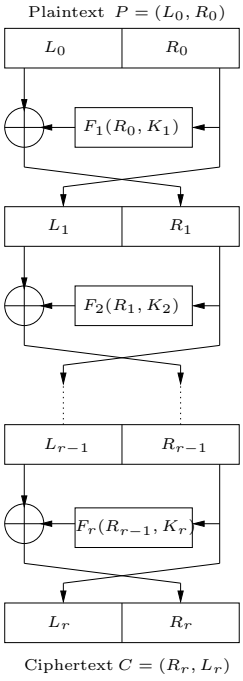
Κρυπτογραφία και Κρυπτανάλυση με μεθόδους Υπολογιστικής Νοημοσύνης και Υπολογιστικών Μαθηματικών και εφαρμογές

Έλενα Χ. Λάσκαρη

Διδακτορική Διατριβή



Πανεπιστήμιο Πατρών
Τμήματα Μαθηματικών και Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής
Πάτρα

Επιβλέπων: Καθηγητής Μιχαήλ Ν. Βραχάτης

(Φεβρουάριος 2010)

Η παρουσα Διδακτορικη Διατριβη στοιχειοθετηθηκε με το προγραμμα LaTeX. Η συγγραφη εγινε με το προγραμμα vim στο λειτουργικο συστημα Fedora Linux και με χρηση του style του Εργαστηριου Υπολογιστικης Νοημοσυνης (CI Lab), το οποιο δημιουργηθηκε απο τον Β.Π. Πλαγιανακο. Η τελικη ηλεκτρονικη μορφη (Portable Document Format – PDF) δημιουργηθηκε με το προγραμμα DVIPDF. Η αναπτυξη των προγραμματων εγινε σε Matlab, C++ και Fortran. Οι γραφικες παραστασεις εγιναν σε Matlab, και η επεξεργασια των σχηματων εγινε με τα προγραμματα Gimp και Adobe Photoshop.

Στο εξώφυλλο απεικονίζεται η διαδικασία κρυπτογράφησης των κρυπτοσυστημάτων Feistel

Στον δάσκαλό μου και στους γονείς μου για την στήριξη και την υπομονή τους.

Περίληψη

Στην παρούσα διατριβή μελετάμε προβλήματα κρυπτογραφίας και κρυπτανάλυσης με μεθόδους Υπολογιστικής Νοημοσύνης και υπολογιστικών μαθηματικών, καθώς και εφαρμογές νέων πρωτοκόλλων εξασφάλισης ιδιωτικότητας. Η παρουσίαση των επιμέρους θεμάτων και αποτελεσμάτων της διατριβής οργανώνεται ως εξής.

Στο Κεφάλαιο 1 παρουσιάζεται μια ιστορική αναδρομή για την χρήση της κρυπτογραφίας από την αρχή της εμφάνισή της ως σήμερα, παρέχονται τα βασικά στοιχεία και έννοιες της κρυπτογραφίας και της κρυπτανάλυσης και δίνονται οι βασικοί στόχοι, τα υπό θεώρηση προβλήματα και η συνεισφορά της παρούσας διατριβής.

Το Μέρος Ι της διατριβής αφιερώνεται στη χρήση μεθόδων Υπολογιστικής Νοημοσύνης για την επίλυση προβλημάτων κρυπτογραφίας και κρυπτανάλυσης. Πιο συγκεκριμένα, στο Κεφάλαιο 2 δίνονται τα απαραίτητα εισαγωγικά στοιχεία για τις μεθόδους Υπολογιστικής Νοημοσύνης, δηλαδή των μεθόδων Εξελικτικού Υπολογισμού και των Τεχνητών Νευρωνικών Δικτύων, και παρουσιάζονται αναδρομικά στοιχεία για την χρήση της Υπολογιστικής Νοημοσύνης στην κρυπτολογία μέχρι σήμερα.

Στο Κεφάλαιο 3 αρχικά μελετώνται τρία διαφορετικά προβλήματα κρυπτανάλυσης ως προβλήματα διακριτής βελτιστοποίησης και ερευνάται η επίλυσή τους με μεθόδους Εξελικτικού Υπολογισμού. Τα αποτελέσματα δείχνουν ότι λόγω της αποδεδειγμένης πολυπλοκότητας των αρχικών κρυπτογραφικών προβλημάτων, ο μετασχηματισμός τους σε προβλήματα διακριτής βελτιστοποίησης διατηρεί την πολυπλοκότητά τους καθιστώντας δύσκολη την εξόρυξη πληροφοριών για την δυναμική τους από τις μεθόδους Εξελικτικού Υπολογισμού. Το γεγονός αυτό υποδεικνύει ότι η κατασκευή της αντικειμενικής συνάρτησης που θα χρησιμοποιηθεί από τις μεθόδους για την επίλυση των υπό μελέτη προβλημάτων κρυπτογραφίας αποτελεί πολύ κρίσιμο σημείο για την αποτελεσματικότητα των μεθόδων στον κλάδο αυτό.

Στη συνέχεια του κεφαλαίου, μελετάμε την κρυπτανάλυση κρυπτοσυστημάτων Feistel με μεθόδους Εξελικτικού Υπολογισμού (ΕΥ) και συγκεκριμένα μοντελοποιούμε κατάλληλα το πρόβλημα και εφαρμόζουμε τις μεθόδους ΕΥ για τον εντοπισμό δυαδικών ψηφίων του κλειδιού του κρυπτοσυστήματος DES με τέσσερις και έξι γύρους, αντίστοιχα. Τα αποτελέσματα δείχνουν ότι οι μέθοδοι μπορούν να επιλύσουν αποδοτικά και αποτελεσματικά τα υπό μελέτη προβλήματα με χαμηλό κόστος και αυτοματοποιημένα, δηλαδή χωρίς να απαιτείται η επέμβαση εξωτερικού χρήστη στην διαδικασία επίλυσης όπως γίνεται από άλλες μεθοδολογίες επίλυσης.

Το Κεφάλαιο 3 ολοκληρώνεται με την έρευνα για την κατασκευή κυτίων αντικατάστασης (S-boxes) με μεθόδους Εξελικτικού Υπολογισμού. Και στην περίπτωση αυτή τα αποτελέσματα είναι θετικά καθώς οι μέθοδοι επιτυγχάνουν με απλή μεθοδολογία να εντοπίσουν τις βέλτιστες τιμές επίλυσης με χαμηλό κόστος.

Στο Κεφάλαιο 4 μελετάται η χρήση Τεχνητών Νευρωνικών Δικτύων (ΤΝΔ) για την επίλυση προβλημάτων κρυπτογραφίας. Αρχικά, τα ΤΝΔ εφαρμόζονται για την επίλυση κλασικών προβλημάτων κρυπτογραφίας ως μέτρο ελέγχου της σθεναρότητάς τους. Τα αποτελέσματα δείχνουν ότι παρά τη χρήση διαφορετικών τοπολογιών δικτύων, μεθόδων εκπαίδευσης αλλά και θεώρησης των προβλημάτων, τα νευρωνικά δίκτυα είναι σε θέση να επιλύσουν ικανοποιητικά τα υπό μελέτη προβλήματα μόνο για μικρές τιμές των παραμέτρων τους.

Στη συνέχεια, μελετάται η χρήση ΤΝΔ για τον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες που αποτελεί σημαντικό πρόβλημα για τις κρυπτογραφικές εφαρμογές. Τα αποτελέσματα είναι ενθαρρυντικά καθώς η προτεινόμενη μοντελοποίηση και η μεθοδολογία έδωσε πολύ ικανοποιητική εκπαίδευση των δικτύων

και μάλιστα παρατηρήθηκε ότι τα δίκτυα μπορούν να μάθουν τα πρότυπα εκπαίδευσης χρησιμοποιώντας λιγότερη μνήμη από αυτήν που απαιτείται για την αποθήκευση του αντίστοιχου συνόλου δεδομένων. Ωστόσο, αναφορικά με την γενίκευση των δικτύων, τα αποτελέσματα είναι λίγο καλύτερα από την τυχαία αναζήτηση.

Το Κεφάλαιο 4 ολοκληρώνεται με την θεωρητική μελέτη της εφαρμογής Πολυωνυμικών Δικτύων Ridge στο πρόβλημα εντοπισμού του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου, όπου και παρέχονται ενδιαφέροντα συμπεράσματα.

Το Μέρος ΙΙ της διατριβής περιλαμβάνει τα Κεφάλαια 5 και 6 στα οποία εφαρμόζονται μέθοδοι υπολογιστικών μαθηματικών σε διάφορα προβλήματα κρυπτογράφησης. Συγκεκριμένα, στο Κεφάλαιο 5 μελετάται η χρήση μεθόδων πολυωνυμικής παρεμβολής για αντίστροφη παρεμβολή σε προβλήματα κρυπτογραφίας στα πεπερασμένα σώματα αλλά και στο λογάριθμο του Lucas. Τα αποτελέσματα δείχνουν ότι στα προβλήματα που μελετώνται το υπολογιστικό κόστος επίλυσης είναι αρκετά υψηλό. Ωστόσο, οι λύσεις που παρέχονται παρουσιάζουν θεωρητικό ενδιαφέρον καθώς εντοπίζονται πολυώνυμα χαμηλού βαθμού ικανά να παρεμβάλλουν τις τιμές των υπό μελέτη προβλημάτων.

Στο Κεφάλαιο 6 προτείνεται ένα νέο κρυπτοσύστημα συμμετρικού κλειδιού με χρήση χαοτικών περιοδικών τροχιών. Αρχικά, δίνεται η βασική μορφή του νέου κρυπτοσυστήματος και μελετάται η ποιότητα των κλειδιών αυτού, και στη συνέχεια παρουσιάζονται τρεις τροποποιήσεις του που αυξάνουν την σθεναρότητά του σε κρυπταναλυτικές επιθέσεις. Θέματα αποδοτικότητας του νέου κρυπτοσυστήματος αναλύονται στο τέλος του κεφαλαίου.

Τέλος, στο Μέρος ΙΙΙ της διατριβής, στο Κεφάλαιο 7, προτείνονται δύο πρωτόκολλα για ασφαλή ηλεκτρονική συγκέντρωση δεδομένων. Αρχικά, αναλύονται οι απαιτήσεις για την εξασφάλιση της ιδιωτικότητας σε αυτού του είδους τα πρωτόκολλα και στη συνέχεια περιγράφονται αναλυτικά τα δύο πρωτόκολλα, που αποτελούν τροποποιήσεις και βελτιώσεις πρωτοκόλλων ηλεκτρονικών εκλογών, και μελετάται η ασφάλεια και η πολυπλοκότητά τους.

Η διατριβή ολοκληρώνεται με το Κεφάλαιο 8 στο οποίο δίνονται τα συμπεράσματα και οι προοπτικές που προκύπτουν από την παρούσα διατριβή.

Synopsis

In this PhD thesis we study problems of cryptography and cryptanalysis through Computational Intelligence methods and computational mathematics. Furthermore, we examine the establishment and security of new privacy preserving protocols for electronic data gathering.

The analytical presentation of all issues and results of the thesis are organized as follows.

Part I is dedicated to the application of Computational Intelligence (CI) methods for solving problems of cryptology. Specifically, Chapter 2 is a brief introduction to Computational Intelligence methods, i.e., Evolutionary Computation (EC) and Artificial Neural Networks (ANNs), and reports previous work on this subject. In Chapter 3, three different problems of cryptanalysis are formulated as discrete optimization tasks and Evolutionary Computation methods are utilized to address them. The reported results suggest that due to the proven complexity of the initial cryptographic problems their direct formulation as discrete optimization tasks preserves their complexity which makes it difficult for the methods to extract pieces of information. Thus, the first conclusion derived by these experiments is that when EC methods are applied to cryptanalysis special attention must be paid to the design of the fitness function so as to include as much information as possible for the target problem. The second conclusion is that when EC methods (and CI methods in general) can be used as a quick practical assessment for the efficiency and the effectiveness of proposed cryptographic systems.

In Chapter 3, we also apply EC methods for the cryptanalysis of Feistel ciphers. Specifically, the problem of finding some missing bits of the key that is used in a simple Feistel cipher, namely the Data Encryption Standard with four and six rounds, respectively, is studied. The two instances are complementary, since every problem of missing bits of keys in Differential Cryptanalysis of Feistel ciphers can be categorized into one of the two cases. The results show that the proposed methods are able to tackle the problem efficiently and effectively with low cost and in automated way.

Chapter 3 concludes with a new methodology with EC methods for designing strong Substitution boxes (S-boxes) for cryptographic applications. The obtained results are promising and indicate that this novel approach is effective.

Chapter 4 examines the use of ANNs for cryptographic problems. Initially, ANNs are employed for classical problems of cryptography as a measure of their robustness. The results show that although different topologies, training methods and formulation of the problems were tested, ANNs were able to obtain the solution of the problems at hand only for small values of their parameters.

Next, we study the performance of ANNs on the computation of a Boolean function derived from the use of elliptic curves in cryptographic applications. Specifically, the considered Boolean function outputs the least significant bit of the discrete logarithm over elliptic curves. The results indicate that ANNs are able to adapt to the data presented with high accuracy, while their response to unknown data is slightly better than a random selection. Another important finding is that ANNs require a small amount of storage for the known patterns in contrast to the storage needed of the data itself.

Chapter 4 concludes with a theoretical study of the application of Ridge Polynomial Networks for the computation of the least significant bit of the discrete logarithm.

Part II of the thesis includes Chapters 5 and 6 where computational mathematics are utilized for different cryptographic problems. In Chapter 5 we consider the Aitken and Neville inverse interpolation methods for a discrete exponential function and the Lucas logarithm function. The results indicate that the computational cost for addressing the problems through this approach remains high, however interesting features regarding the degree of the resulting interpolation polynomials are reported.

In Chapter 6 a new symmetric key cryptosystem that exploits the idea of nonlinear mappings and their fixed points to encrypt information is presented. Furthermore, a measure of the quality of the keys used is introduced. The experimental results indicate that the proposed cryptosystem is efficient and secure to ciphertext-only attacks. Finally, three modifications of the basic cryptosystem that render it more robust are presented and efficiency issues are discussed.

Finally, at Part III of the thesis, in Chapter 7, two protocols for privacy preserving electronic data gathering are proposed. The security requirements that must be met for data gathering with privacy are presented and then two protocols, based on electronic voting protocols, are analytically described. Security and complexity issues are also discussed.

The thesis concludes with Chapter 8 where conclusions of all issues presented are given and ideas for future work are proposed.

Ευχαριστίες

Η παρούσα διδακτορική διατριβή δεν θα είχε ολοκληρωθεί με την σημερινή της μορφή χωρίς την βοήθεια και την στήριξη κάποιων ανθρώπων που θα ήθελα να ευχαριστήσω θερμά. Κατ΄ αρχήν, θέλω να εκφράσω τις θερμές μου ευχαριστίες στον καθηγητή κ. Μιχαήλ Βραχάτη, επιβλέποντα της διδακτορικής μου διατριβής, του οποίου η συμπαράσταση και οι συμβουλές ήταν ανεκτίμητες καθ΄ όλη την διάρκεια ολοκλήρωσης της μελέτης μου. Επίσης, τον ευχαριστώ γιατί πέρα από τις επιστημονικές του γνώσεις και εμπειρία μου μετέδωσε επιστημονικό ήθος και στάθηκε δίπλα μου σαν αληθινός δάσκαλος και άνθρωπος.

Θα ήθελα επίσης να ευχαριστήσω θερμά τα άλλα δύο μέλη της Τριμελούς Συμβουλευτικής Επιτροπής μου, τον αναπληρωτή καθηγητή κ. Ιωάννη Σταματίου και τον καθηγητή κ. Χρήστο Ζαρολιάγκη, καθώς και τον καθηγητή του Α.Τ.Ε.Ι. Ηπείρου κ. Γεράσιμο Μελετίου για την εξαιρετική μας συνεργασία, τις υποδείξεις και τις πολύτιμες συμβουλές τους, χωρίς τις οποίες το αποτέλεσμα αυτής της διατριβής θα ήταν πολύ διαφορετικό.

Επίσης, ευχαριστώ πολύ όλους τους εξαίρετους συνεργάτες και φίλους Κ. Παρσόπουλο, Δ. Τασουλή, Ν. Παυλίδη, Μ. Επιτροπάκη, Ι. Πεταλά, Β. Γαλάνη και Γ. Αντζουλάτο, με τους οποίους είχα την χαρά να συνεργαστώ κατά την εκπόνηση της διατριβής μου, για την στήριξη, την αγάπη και την συμπαράσταση που μου έδειξαν όλο αυτό τον καιρό.

Ευχαριστίες πρέπει να αποδοθούν και στο Τμήμα Μαθηματικών του Πανεπιστημίου Πατρών για την υλικοτεχνική υποδομή που μου παρείχε ώστε να είναι εφικτή η εκπόνηση αυτής της διατριβής. Η παρούσα διατριβή στηρίχθηκε οικονομικά από το πρόγραμμα Αρχιμήδης που συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση και το ΥΠ.Ε.Π.Θ.

Έλενα Λάσκαρη

Πάτρα, 2010.

Περιεχόμενα

Περίληψη **v**

Synopsis **ιι**

Ευχαριστίες **ix**

Κατάλογος Συντομεύσεων Ορολογίας **xix**

1 Εισαγωγή **1**
1.1 Ιστορικά στοιχεία της κρυπτογραφίας και της κρυπτανάλυσης 1
1.2 Εισαγωγή στην κρυπτογραφία και στην κρυπτανάλυση 3
1.2.1 Βασική ορολογία και έννοιες 4
1.2.1.1 Κρυπτανάλυση 4
1.2.2 Κρυπτοσυστήματα συμμετρικού κλειδιού 6
1.2.2.1 Κρυπτοσυστήματα τμηματικής κρυπτογράφησης 6
1.2.2.2 Κρυπτοσυστήματα ροής 8
1.2.3 Κρυπτοσυστήματα δημοσίου κλειδιού 9
1.2.4 Κρυπτοσυστήματα Ελλειπτικών Καμπυλών 11
1.3 Προβλήματα υπό θεώρηση στην παρούσα διατριβή 12
1.4 Συνεισφορά της παρούσας διδακτορικής διατριβής 13
1.5 Δομή της διδακτορικής διατριβής 15

I Κρυπτογραφία και κρυπτανάλυση με μεθόδους Υπολογιστικής Νοημοσύνης **17**

2 Εισαγωγή στην Υπολογιστική Νοημοσύνη **19**
2.1 Εισαγωγή στις μεθόδους Εξελικτικού Υπολογισμού 19
2.1.1 Γενετικοί Αλγόριθμοι 20
2.1.2 Γενετικός Προγραμματισμός 22
2.1.3 Εξελικτικός Προγραμματισμός 24
2.1.4 Εξελικτικές Στρατηγικές 25
2.1.5 Διαφοροεξελικτικός Αλγόριθμος 29
2.1.6 Βελτιστοποίηση με Σμήνος Σωματιδίων 31
2.1.7 Βελτιστοποίηση με Αποικίες Μυρμηγκιών 35
2.2 Εισαγωγή στα Τεχνητά Νευρωνικά Δίκτυα 36
2.2.1 Υπολογιστικό μοντέλο ενός νευρώνα 38
2.2.2 Αρχιτεκτονική ενός Τεχνητού Νευρωνικού Δικτύου 39
2.2.3 Εκπαίδευση των Τεχνητών Νευρωνικών Δικτύων 39
2.2.4 Πολυστρωματικά Τεχνητά Νευρωνικά Δίκτυα πρόσθιας τροφοδότησης 42
2.3 Η Υπολογιστική Νοημοσύνη στην κρυπτολογία 44

3 Κρυπτογραφία και Κρυπτανάλυση με μεθόδους ΕΥ **47**
3.1 Εξελικτικός Υπολογισμός και κρυπτολογία 47
3.2 Προβλήματα κρυπτογραφίας ως διακριτής βελτιστοποίησης 48
3.2.1 Θεώρηση των υπό μελέτη προβλημάτων 48
3.2.2 Πειραματική θεώρηση και αποτελέσματα 51
3.3 Μέθοδοι ΕΥ για την κρυπτανάλυση κρυπτοσυστημάτων Feistel 56
3.3.1 Θεωρητικά στοιχεία για το κρυπτοσύστημα DES 56
3.3.2 Θεώρηση προβλήματος 59
3.3.3 Πειραματική θεώρηση και αποτελέσματα 60
3.4 Κατασκευή S-boxes με μεθόδους Εξελικτικού Υπολογισμού 65
3.4.1 Θεωρητικά στοιχεία για τα S-boxes 66
3.4.2 Θεώρηση του προβλήματος 67
3.4.3 Προτεινόμενη μεθοδολογία 68
3.4.4 Πειραματική θεώρηση και αποτελέσματα 69
3.5 Συμπεράσματα 70

4 Μελέτη προβλημάτων κρυπτογραφίας με χρήση ΤΝΔ **73**
4.1 Τεχνητά Νευρωνικά Δίκτυα και κρυπτολογία 73
4.2 ΤΝΔ για κρυπτανάλυση κλασικών κρυπτοσυστημάτων 74
4.2.1 Πειραματική θεώρηση και αποτελέσματα 74
4.3 ΤΝΔ για κρυπτανάλυση κρυπτοσυστημάτων ελλειπτικών καμπυλών 77
4.3.1 Θεώρηση προβλήματος 77
4.3.2 Πειραματική θεώρηση και αποτελέσματα 78
4.4 Θεωρητική μελέτη της εφαρμογής ΠΔR στην κρυπτογραφία 79
4.5 Συμπεράσματα 84

II Υπολογιστικά Μαθηματικά και Κρυπτολογία **85**

5 Πολυωνυμική παρεμβολή σε προβλήματα κρυπτογραφίας **87**
5.1 Εισαγωγή 87
5.2 Μέθοδοι παρεμβολής σε πεπερασμένα σώματα 87
5.3 Οι μέθοδοι παρεμβολής Aitken και Neville 88
5.4 Οι μέθοδοι Aitken και Neville στα πεπερασμένα σώματα 89
5.5 Συμπεράσματα 91
5.6 Αντίστροφη παρεμβολή για το λογάριθμο του Lucas 96
5.7 Εισαγωγικά στοιχεία 96
5.8 Θεώρηση του προβλήματος 97
5.9 Πειραματική θεώρηση και αποτελέσματα 97
5.10 Συμπεράσματα 101

6 Νέα κρυπτοσυστήματα βασιζόμενα σε περιοδικές τροχιές **103**
6.1 Εισαγωγή 103
6.2 Βασικά στοιχεία μη γραμμικών δυναμικών απεικονίσεων 104
6.3 Βασική μορφή του προτεινόμενου κρυπτοσυστήματος 106
6.3.1 Κατασκευή του κλειδιού 106
6.3.2 Αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης 107
6.4 Ποιότητα των κλειδιών 108
6.5 Τροποποιήσεις του κρυπτοσυστήματος και αποδοτικότητα 109
6.5.1 Πρώτη τροποποίηση 109
6.5.2 Δεύτερη τροποποίηση 109
6.5.3 Τρίτη τροποποίηση 110

6.5.4 Θέματα αποδοτικότητας 110
6.6 Πειραματική θεώρηση και αποτελέσματα 110
6.7 Συμπεράσματα - Συνεισφορά 111

III Πρωτόκολλα εξασφάλισης ιδιωτικότητας 115

7 Πρωτόκολλα για ασφαλή ηλεκτρονική συγκέντρωση δεδομένων 117
7.1 Εισαγωγή 117
7.2 Τροποποίηση πρωτοκόλλων ηλεκτρονικών εκλογών 118
7.3 Ανάλυση ασφάλειας του προτεινόμενου σχήματος με Συλλέκτη 120
7.4 Θέματα πολυπλοκότητας του σχήματος με Συλλέκτη 122
7.5 Ηλεκτρονική συγκέντρωση δεδομένων χωρίς Συλλέκτη 124
7.5.1 Πρωτόκολλο ηλεκτρονικών εκλογών χωρίς κάλπη 124
7.5.2 Δεύτερο προτεινόμενο σχήμα 126
7.6 Ανάλυση ασφάλειας του προτεινόμενου σχήματος χωρίς Συλλέκτη 128
7.7 Θέματα πολυπλοκότητας του σχήματος χωρίς Συλλέκτη 129
7.8 Συμπεράσματα - Συνεισφορά 130

8 Συμπεράσματα και προοπτικές 131

IV Βιβλιογραφία – Ευρετήριο 135

Βιβλιογραφία 137

Κατάλογος Δημοσιεύσεων Υποψήφιας 151

Ευρετήριο 169

Κατάλογος Σχημάτων

3.1 Απεικόνιση της συνάρτησης $f(x) = \alpha^x - \beta \pmod p$, για $p = 101, \alpha = 2$ και $\beta = 34$. 49

3.2 Απεικόνιση της συνάρτησης $f(x) = \alpha^x - \beta \pmod p$, για $p = 1009, \alpha = 11$ και $\beta = 337$, γύρω από το ολικό ελάχιστο (αριστερά), και για $p = 2003, \alpha = 5$ και $\beta = 668$, γύρω από το ολικό ελάχιστο (δεξιά) 50

3.3 Απεικόνιση της συνάρτησης $g(x, y) = x^2 - y^2 \pmod N$, για $N = 143$ (αριστερά), και οι ισοϋψείς της συνάρτησης $g(x, y) = x^2 - y^2 \pmod N$, για $N = 143$ στην τιμή 0 (δεξιά). 51

3.4 Απεικόνιση της συνάρτησης $h_e(x) = (x-1)(x-2) \pmod N$, για $N = 667$ (αριστερά), και απεικόνιση της συνάρτησης $w_e(x) = (x+1)(x-1)(x-2) \pmod N$, για $N = 667$ (δεξιά). 51

3.5 Η διαδικασία κρυπτογράφησης των κρυπτοσυστημάτων Feistel 57

4.1 Ένα Δίκτυο Πί-Σίγμα (ΠΣΔ) με έναν νευρώνα εξόδου 81

4.2 Ένα Πολυωνυμικό Δίκτυο Ridge (ΡΠΔ) με έναν γραμμικό νευρώνα εξόδου 83

5.1 Συχνότητα εμφάνισης πολυωνυμικών βαθμών για όλα τα στιγμιότυπα του προβλήματος με (a) την μέθοδο Aitken και (b) την μέθοδο Neville. . . . 91

6.1 Η διδιάστατη απεικόνιση του Hénon στο χώρο (x_1, x_2) για (α) $\cos\alpha = 0.24$, $g(x_1) = -x_1^2$, (β) $\cos\alpha = 0.24$, $g(x_1) = -0.9x_1^2$, (γ) $\cos\alpha = 0.2$, $g(x_1) = -x_1^2$, (δ) $\cos\alpha = 0.2$, $g(x_1) = -0.9x_1^2$ 105

6.2 (α) Σταθερά σημεία της διδιάστατης απεικόνισης του Hénon με $\cos\alpha = 0.24$ και $g(x_1) = -x_1^2$, χρησιμοποιούμενα ως κλειδιά του κρυπτοσυστήματος, (β) λεπτομέρεια των κλειδιών που χρησιμοποιούνται στην (α), (γ) κλειδιά της (α) τοποθετημένα στην διδιάστατη απεικόνιση του Hénon με $\cos\alpha = 0.15$ και $g(x_1) = -x_1^2$, (δ) κλειδιά της (α) τοποθετημένα στην διδιάστατη απεικόνιση του Hénon με $\cos\alpha = 0.35$ και $g(x_1) = -x_1^2$. 112

Κατάλογος Πινάκων

2.1 Η εξελικτική διαδικασία ενός Γενετικού Αλγορίθμου. 21
2.2 Τελεστές διασταύρωσης των Γενετικών Αλγορίθμων. 22
2.3 Η γενική μορφή του Εξελικτικού Προγραμματισμού. 24
2.4 Ο γενικός αλγόριθμος των Εξελικτικών Στρατηγικών. 26
2.5 Η τυπική μορφή του Διαφοροεξελικτικού Αλγορίθμου. 30
2.6 Η γενική μορφή της μεθόδου Βελτιστοποίησης με Σμήνος Σωματιδίων. . 34
2.7 Η διαδικασία εκπαίδευσης ενός δικτύου perceptron. 41
2.8 Ο αλγόριθμος της οπισθοδρομικής μετάδοσης του σφάλματος. 43

3.1 Ποσοστά επιτυχίας της κάθε μεθόδου για την ελαχιστοποίηση της συνάρτησης f για δύο κατώφλια συναρτησιακών υπολογισμών και $p = 1009$ ως $p = 1000003$. 53
3.2 Αποτελέσματα για την ελαχιστοποίηση της συνάρτησης g (βλέπε Εξίσωση (3.2)). 55
3.3 Αποτελέσματα για τις συναρτήσεις h_e (βλέπε Εξίσωση (3.4)) και w_e (βλέπε Εξίσωση (3.6)), για $N = 103 \times 107$ 56
3.4 Αποτελέσματα για το κρυπτοσύστημα DES με τέσσερις γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 20$ ζεύγη δοκιμών. 61
3.5 Αποτελέσματα για το κρυπτοσύστημα DES με τέσσερις γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 50$ ζεύγη δοκιμών. 62
3.6 Αποτελέσματα για το κρυπτοσύστημα DES με έξι γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 200$ ζεύγη δοκιμών. 64
3.7 Οι βέλτιστες τιμές μη-γραμμικότητας και αυτοσυσχέτισης, αντίστοιχα, για S-boxes μεγέθους n. 69
3.8 Βέλτιστες συνδεδεμένες τιμές μη-γραμμικότητας και αυτοσυσχέτισης για S-boxes μεγέθους n για όλες τις μεθόδους. 70
3.9 Συχνότητα επίτευξης των διαφορετικών τιμών μη-γραμμικότητας στα 100 ανεξάρτητα πειράματα. 70

4.1 Αποτελέσματα της εκπαίδευσης Τεχνητών Νευρωνικών Δικτύων για το ΠΔΛ και το ΠΑΔΗ 75
4.2 Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για το Πρόβλημα Διακριτού Λογαρίθμου με την δεύτερη θεώρηση του προβλήματος 76
4.3 Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για την απεικόνιση $\phi(N)$ όπου $N = p \times q \leqslant 10^4$ 76
4.4 Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για το πρόβλημα της παραγοντοποίησης με την δεύτερη θεώρηση και για N από 143 μέχρι 1003 76
4.5 Αποτελέσματα για p με μήκος 14ων δυαδικών ψηφίων και τοπολογία $56-3-2$ 79
4.6 Αποτελέσματα για p με μήκος 20 δυαδικών ψηφίων και τοπολογία $80-3-2$ 80
4.7 Αποτελέσματα για p με μήκος 32 δυαδικών ψηφίων και τοπολογία $128-3-2$ 80
4.8 Αποτελέσματα συμπίεσης δεδομένων 81

5.1 Περιπτώσεις παραμέτρων του προβλήματος που μελετήθηκαν. 90

5.2 Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το πλήθος των απαιτούμενων επαληθεύσεων σε 100 ανεξάρτητα πειράματα. 92
5.3 Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το πλήθος των χρησιμοποιούμενων σημείων σε 100 ανεξάρτητα πειράματα. 93
5.4 Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το βαθμό του τελικού πολυωνύμου σε 100 ανεξάρτητα πειράματα. . . . 94
5.5 Αποτελέσματα από 100 ανεξάρτητα πειράματα για $p = 2003$, $\alpha = 5$ και διαφορετικές τιμές της παραμέτρου b. 95
5.6 Στιγμιότυπα των προβλημάτων που θεωρήθηκαν για την περίπτωση ριζών του χαρακτηριστικού πολυωνύμου της ακολουθίας του Lucas στο σώμα $\mathbb{F}_p$ (Ρίζες στο $\mathbb{F}_p$) και στο σώμα $\mathbb{F}_{p^2}$ (Ρίζες στο $\mathbb{F}_{p^2}$). 98
5.7 Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville σε 100 ανεξάρτητα πειράματα για την περίπτωση ριζών στο σώμα $\mathbb{F}_p$. 99
5.8 Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville σε 100 ανεξάρτητα πειράματα για την περίπτωση ριζών στο σώμα $\mathbb{F}_{p^2}$. 100

6.1 Πειραματικά αποτελέσματα για διάφορα είδη αρχικών κειμένων 111

Κατάλογος Συντομεύσεων Ορολογίας

DES - Data Encryption Standard

ΡΠΔ - Πολυωνυμικό Δίκτυο Ridge

S-boxes - Substitution boxes

ΒΑΜ - Βελτιστοποίηση με Αποικίες Μυρμηγκιών

ΒΣΣ - Βελτιστοποίηση με Σμήνος Σωματιδίων

ΒΣΣΟΒ - Βελτιστοποίηση με Σμήνος Σωματιδίων ολική παραλλαγή με βάρος αδράνειας

ΒΣΣΟΠ - Βελτιστοποίηση με Σμήνος Σωματιδίων ολική παραλλαγή με παράγοντα περιορισμού

ΒΣΣΤΒ - Βελτιστοποίηση με Σμήνος Σωματιδίων τοπική παραλλαγή με βάρος αδράνειας

ΒΣΣΤΠ - Βελτιστοποίηση με Σμήνος Σωματιδίων τοπική παραλλαγή με παράγοντα περιορισμού

ΓΑ - Γενετικοί Αλγόριθμοι

ΓΠ - Γενετικός Προγραμματισμός

ΔΕ - Διαφοροεξελικτικός Αλγόριθμος

ΔΚ - Διαφορική Κρυπτανάλυση

ΕΠ - Εξελικτικός Προγραμματισμός

ΕΣ - Εξελικτικές Στρατηγικές

ΕΥ - Εξελικτικός Υπολογισμός

ΝΣ - Νοημοσύνη Σμηνών

ΠΑDH - Πρόβλημα Απεικόνισης Diffie-Hellman

ΠΑΚDH - Πρόβλημα Ανταλλαγής Κλειδιών Diffie-Hellman

ΠΔΛ - Πρόβλημα Διακριτού Λογαρίθμου

ΠΔΛΕΚ - Πρόβλημα Διακριτού Λογαρίθμου Ελλειπτικών Καμπυλών

ΠΣΔ - Δίκτυο Πί-Σίγμα

ΤΑ - Τυχαία Αναζήτηση

ΤΝΔ - Τεχνητό Νευρωνικό Δίκτυο

ΥΝ - Υπολογιστική Νοημοσύνη

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Ιστορικά στοιχεία της κρυπτογραφίας και της κρυπτανάλυσης

Η κρυπτογραφία έχει μια μακρά και εντυπωσιακή ιστορία. Οι ρίζες της ξεκινούν πριν από 4000 χρόνια περίπου όταν στην αρχαία Αίγυπτο το 2000 π.Χ. χρησιμοποιήθηκαν τα ιερογλυφικά για να διακοσμήσουν τους τάφους εκλιπόντων κυβερνώντων ή βασιλέων. Τα ιερογλυφικά αυτά εξιστορούσαν την ζωή του εκλιπόντος και εξυμνούσαν τις σπουδαίες πράξεις του. Ήταν σκόπιμα περίπλοκη γραφή χωρίς όμως να σκοπεύει στην απόκρυψη του κειμένου. Αντίθετα, σκοπός της ήταν να αποδώσει στο κείμενο σπουδαιότητα. Με το πέρασμα του χρόνου τα ιερογλυφικά γίνονταν όλο και περισσότερο πολύπλοκα ώσπου τελικά οι άνθρωποι έχασαν το ενδιαφέρον της αποκρυπτογράφησής τους. Στην Ινδία η μυστική γραφή εξελίχθηκε περισσότερο καθώς η κυβέρνηση χρησιμοποιούσε μυστικούς κώδικες για την επικοινωνία με ένα δίκτυο κατασκόπων διασκορπισμένων σε ολόκληρη τη χώρα. Οι κώδικες αυτοί αποτελούνταν ως επί το πλείστον από απλές αλφαβητικές αντικαταστάσεις που βασίζονταν στα φωνήεντα. Η ιστορία της κρυπτογραφίας στην Μεσοποταμία είναι παρόμοια με αυτήν της Αιγύπτου καθώς η σφηνοειδής γραφή χρησιμοποιήθηκε για την κρυπτογράφηση κειμένου. Η ίδια τεχνική παρουσιάστηκε στην Βαβυλωνία και στην Ασσυρία.

Στην Ελλάδα τα πρώτα στοιχεία κρυπτογραφίας εμφανίζονται στο κείμενο της Ιλιάδας, στην Ιστορία του Ηροδότου αλλά και στην ιστορία του Περίανδρου της Κορίνθου. Η γνωστή «σκυτάλη» της Σπάρτης ανάγεται στον 5ο π.Χ. αιώνα. Αποτελούνταν από μια ξύλινη ράβδο γύρω από την οποία τύλιγαν μια λωρίδα περγαμηνής ή δέρματος. Το μήνυμα γραφόταν από τον αποστολέα πάνω στη λωρίδα κατά μήκος της σκυτάλης και στη συνέχεια ξετύλιγαν τη λωρίδα η οποία φαινόταν να περιέχει μια σειρά γραμμάτων χωρίς νόημα καθώς το μήνυμα είχε αναδιαταχθεί. Προκειμένου να διαβάσει το μήνυμα ο παραλήπτης έπρεπε απλώς να τυλίξει την λωρίδα σε μια σκυτάλη ίδιας διαμέτρου με αυτήν που χρησιμοποιήθηκε κατά την γραφή. Με την κρυπτογραφική μέθοδο της σκυτάλης ο Λύσανδρος το 404 π.Χ. απέκρουσε με επιτυχία μια επίθεση του Πέρση σατράπη Φαρνάβαζου. Τον 4ο π.Χ. αιώνα ο Αινείας ο Τακτικός από την Μεγαλόπολη έγραψε ένα από τα πρώτα βιβλία κρυπτολογίας στο οποίο περιέχεται και μια τεχνική, παραλλαγή της οποίας εφαρμόστηκε από τους Γερμανούς στον 2ο παγκόσμιο πόλεμο. Επίσης, ο Πολύβιος τον 2ο π.Χ. αιώνα δημιούργησε ένα κρυπτοσύστημα που ονομάστηκε το «τετράγωνο του Πολύβιου». Στο σύστημα αυτό κάθε γράμμα του κειμένου αντικαθίσταται από ζεύγη αριθμών με βάση έναν πίνακα διάστασης 5×5. Ο Ιούλιος Καίσαρας χρησιμοποίησε τη μυστική αυτή γραφή αλλά και κρυπτογράφηση μετατόπισης κατά τρεις χαρακτήρες δεξιά.

Κατά την περίοδο $400 - 1200$ μ.Χ. η Ευρώπη διανύει τον μεσαίωνα κατά τον οποίο όλες οι επιστήμες, και μεταξύ αυτών και η κρυπτογραφία, ήταν σε παρακμή. Έτσι, την περίοδο αυτή η κρυπτογραφία αναπτύσσεται μόνο στην Ινδία και στις ισλαμικές χώρες. Τον 9ο μ.Χ. αιώνα ο πλέον σημαντικός Άραβας κρυπτολόγος Al Kindi ανέπτυξε τη μέθοδο κρυπτανάλυσης που βασίζεται στη συχνότητα εμφάνισης των χαρακτήρων κάθε γλώσσας.

Το 1404 μ.Χ. ο Ιταλός αρχιτέκτονας και συγγραφέας L.B. Alberti ήταν ο πρώτος που ανέπτυξε ένα πολυαλφαβητικό σύστημα αντικατάστασης για κρυπτογράφηση. Πολυαλφαβητικό

σύστημα αντικατάστασης ονομάζεται κάθε τεχνική που επιτρέπει διαφορετικά κρυπτογραφήματα να αναπαριστούν το ίδιο αρχικό μη κρυπτογραφημένο σύμβολο, γεγονός που καθιστά δυσκολότερη την κρυπτανάλυση καθώς δεν διατηρούνται οι συχνότητες των γραμμάτων. Για την υλοποίηση αυτού του κρυπτοσυστήματος επινόησε και την πρώτη κρυπτογραφική μηχανή μετά την σκυτάλη που ονομάζεται «δίσκοι του Alberti». Η μηχανή αυτή περιλάμβανε δύο ομόκεντρους χάλκινους δίσκους διαφορετικής διαμέτρου πάνω στην περιφέρεια των οποίων ήταν χαραγμένο ένα αλφάβητο. Ο ένας δίσκος αναφερόταν στο αρχικό μήνυμα και ο άλλος στο κρυπτογράφημα. Κάθε δίσκος περιστρεφόταν ανεξάρτητα και έτσι διαφορετικά μέρη του μηνύματος κρυπτογραφούνταν θέτοντας σε διαφορετικές θέσεις τον κρυπτογραφικό δίσκο.

Το 1518 μ.Χ. ο Trithemius έγραψε την «Πολυγραφία», το πρώτο τυπωμένο βιβλίο κρυπτογραφίας, το οποίο περιείχε τα πρώτα κρυπτοσυστήματα κυκλικών μεταθέσεων και στη συνέχεια ο Cardano δημιούργησε την κρυπτογράφηση με τη μέθοδο της μάσκας. Αυτή η κλάση κρυπτοσυστημάτων παρέμεινε σθεναρή μέχρι το 1800.

Τα μεταγενέστερα χρόνια η κρυπτογραφία άρχισε να εξελίσσεται. Όλες οι κυβερνήσεις της Δυτικής Ευρώπης χρησιμοποιούσαν την κρυπτογραφία με διαφόρους τρόπους. Έως το 1860 μεγάλοι κώδικες ήταν πλέον συνήθεις για την κρυπτογράφηση των διπλωματικών επικοινωνιών. Η εφεύρεση του τηλέγραφου και του ραδιοφώνου εξώθησε την ανάπτυξη της κρυπτογραφικής προστασίας των τηλεπικοινωνιών, καθώς η ταχύτητα και το μέγεθος των μεταδιδόμενων δεδομένων κατέστησαν τις τηλεπικοινωνίες περισσότερο ευάλωτες στις μεσολαβήσεις και στην αποκρυπτογράφηση.

Τον 19ο αιώνα ο Ch. Babbage κατάφερε να κρυπταναλύσει διγραφικά κρυπτογραφήματα, δηλαδή συστήματα όπου κρυπτογραφούνται ζεύγη γραμμάτων. Το 1918 ο Γερμανός A. Serbious δημιούργησε ένα μηχανικό κρυπτοσύστημα που μπορεί να θεωρηθεί ως ηλεκτρική παραλλαγή των δίσκων του Alberti, και είναι γνωστή με το όνομα «Αίνιγμα». Η βασική εκδοχή του Αινίγματος αποτελείται από ένα πληκτρολόγιο για την εισαγωγή του κειμένου, από μια αναδιατακτική μονάδα που κρυπτογραφεί κάθε χαρακτήρα του κειμένου σε έναν αντίστοιχο χαρακτήρα του κρυπτογραφήματος και έναν ηλεκτρικό πίνακα που δείχνει τον αντίστοιχο χαρακτήρα του τελικού κρυπτογραφημένου κειμένου. Στη βασική αυτή εκδοχή του κρυπτοσυστήματος σύντομα προστέθηκαν περισσότεροι αναδιατάκτες και ανακλαστές καθιστώντας την διαδικασία αρκετά πολύπλοκη μέχρι το Αίνιγμα να φτάσει να έχει πάνω από 10^{16} πιθανά κλειδιά. Ωστόσο, το 1938 ο Πολωνός μαθηματικός M. Rejewski με την ομάδα του κατάφεραν να σπάσουν το Αίνιγμα στην απλή μορφή που τότε είχε και τα αποτελέσματά τους βοήθησαν μεταγενέστερα στην πλήρη κρυπτανάλυση του Αινίγματος από Άγγλους κρυπταναλυτές. Μεταξύ των κρυπταναλυτών του Αινίγματος ήταν και ο γνωστός Άγγλος μαθηματικός Alan Turing, ο οποίος κατά την διάρκεια του δεύτερου παγκόσμιου πολέμου εργαζόταν στο Βρετανικό κέντρο κρυπτανάλυσης, δημιούργησε διάφορες τεχνικές κρυπτανάλυσης Γερμανικών κρυπτοσυστημάτων μεταξύ των οποίων και το Αίνιγμα, αλλά υπήρξε και επικεφαλής του Hut8, του τομέα που ήταν υπεύθυνος για την ανάγνωση των Γερμανικών ναυτικών σημάτων.

Τα μεταπολεμικά χρόνια η κρυπτογραφία γνώρισε μεγαλύτερη ανάπτυξη κυρίως λόγω της τεχνολογίας των υπολογιστών και της δυνατότητας ταχύτερων υπολογισμών. Ωστόσο, τα κλασικά κρυπτοσυστήματα που χρησιμοποιούνταν χαρακτηρίζονταν από το πρόβλημα της μυστικής ανταλλαγής κλειδιών, δηλαδή την δημιουργία ενός ασφαλούς διαύλου επικοινωνίας μέσω του οποίου ο αποστολέας και ο παραλήπτης θα μπορούσαν να συμφωνήσουν για το χρησιμοποιούμενο μυστικό κλειδί. Εκτός από το πρόβλημα της ασφάλειας του διαύλου επικοινωνίας, υπήρχαν περιπτώσεις όπου η επικοινωνία έπρεπε να είναι γρήγορη, φθηνή και να βοηθά στην συχνή ανταλλαγή κλειδιών.

Το 1874 στο βιβλίο του W. S. Jevons [78] περιγράφηκε για πρώτη φορά η σχέση των μονόδρομων συναρτήσεων με την κρυπτογραφία, που αποτέλεσε τον πρόδρομο για την κρυπτογραφία δημοσίου κλειδιού. Το 1976 οι W. Diffie και M. Hellman πρότειναν μια καινοτόμο μέθοδο κρυπτογράφησης σύμφωνα με την οποία μπορούσε να υπάρξει επικοινωνία χωρίς την ανάγκη ανταλλαγής κλειδιών μέσω ασφαλούς διαύλου. Η ασφάλεια της μεθόδου ανταλλαγής

κλειδιών που πρότειναν βασιζόταν στο πρόβλημα επίλυσης του διακριτού λογαρίθμου και έγινε γνωστή ως ανταλλαγή κλειδιών Diffie-Hellman. Αυτή ήταν η πρώτη δημοσιευμένη πρακτική μέθοδος που καθιέρωσε ένα δημόσιο κλειδί που μεταδίδεται μέσω ενός εξουσιοδοτημένου αλλά όχι ιδιωτικού καναλιού επικοινωνιών, χωρίς να χρησιμοποιείται πριν κάποιο μυστικό κλειδί. Επίσης, η τεχνική συμφωνίας δημοσίου κλειδιού του Merkle έγινε γνωστή ως Merkle's Puzzles, εφευρέθηκε το 1974 και δημοσιεύθηκε το 1978.

Η ιδέα των W. Diffie και M. Hellman υλοποιήθηκε ολοκληρωμένα το 1978 από τους R. Rivest, A. Shamir και L. Adleman που επινόησαν το κρυπτοσύστημα RSA. Η ασφάλεια του RSA βασίζεται σε ένα άλλο δύσκολο μαθηματικό πρόβλημα αυτό της παραγοντοποίησης μεγάλων ακέραιων αριθμών, για το οποίο δεν είναι γνωστή κάποια αποδοτική, δηλαδή πρακτικά γρήγορη, γενική τεχνική επίλυση. Το RSA πραγματοποιεί κρυπτογράφηση δημοσίου κλειδιού αλλά και ψηφιακή υπογραφή δημοσίου κλειδιού.

Μετά το 1970, αναπτύχθηκε ένα μεγάλο πλήθος και ποικιλία κρυπτογραφήσεων, ψηφιακών υπογραφών, τεχνικές συμφωνίας κλειδιών και άλλες στο πεδίο της κρυπτογραφίας δημοσίου κλειδιού. Το κρυπτοσύστημα ElGamal δημιουργήθηκε το 1985 και βασίζεται στην δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου, όπως και το σχετικό κρυπτοσύστημα DSA που αναπτύχθηκε από την Αμερικανική Υπηρεσία Εθνικής Ασφάλειας (NSA).

Η εισαγωγή στην κρυπτογραφία ελλειπτικών καμπυλών από τον N. Koblitz και τον V. Miller ανεξάρτητα και συγχρόνως στα μέσα του 1980 οδήγησε σε νέα κρυπτοσυστήματα δημοσίου κλειδιού που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου. Παρότι είναι μαθηματικά πολυπλοκότερα, τα κρυπτοσυστήματα ελλειπτικών καμπυλών παρέχουν κλειδιά μικρότερου μεγέθους και γρηγορότερους υπολογισμούς για ισοδύναμα επίπεδα ασφάλειας.

Η έρευνα για νέα σχήματα κρυπτογράφησης, για βελτίωση των ήδη υπαρχόντων, καθώς και για αποδείξεις της ασφάλειάς τους συνεχίζει με ραγδαίο ρυθμό. Παλαιότερες κρυπτογραφικές δομές εγκαταλείπονται και νέα προϊόντα ασφαλείας δημιουργούνται προκειμένου να καλύψουν τις ανάγκες των ευαίσθητων πληροφοριακών δεδομένων της σύγχρονης κοινωνίας.

1.2 Εισαγωγή στην κρυπτογραφία και στην κρυπτανάλυση

Η κρυπτογραφία ξεκίνησε ως η τέχνη και επιστήμη της κρυπτογράφησης, «από αρχαία τέχνη σε σύγχρονη επιστήμη» όπως αναφέρει και ο U. Maurer [122], και αφορούσε στη δημιουργία τεχνικών μεταβολής ενός μηνύματος με τέτοιο τρόπο που να διατηρείται μυστικό το περιεχόμενό του.

Σήμερα η κρυπτογραφία είναι η επιστήμη που μελετά μαθηματικές μεθόδους σχετιζόμενες με διάφορους τομείς της ασφάλειας πληροφορίας, όπως είναι η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η πιστοποίηση οντοτήτων και η πιστοποίηση της πηγής δεδομένων μεταξύ άλλων.

Κρυπτανάλυση είναι η μελέτη μαθηματικών μεθόδων για την ανατροπή της ασφάλειας των κρυπτογραφικών τεχνικών και των υπηρεσιών ασφαλούς επικοινωνίας γενικότερα. Στην κρυπτανάλυση θεωρούμε πάντα ότι το χρησιμοποιούμενο σύστημα κρυπτογράφησης είναι γνωστό σε όλους και οι μέθοδοι κρυπτανάλυσης αποσκοπούν στην εύρεση κρίσιμων σημείων του συστήματος μέσω των οποίων μπορεί να καταρρεύσει η ασφάλειά τους.

Στις ακόλουθες ενότητες θα δώσουμε τα εισαγωγικά στοιχεία και τις βασικές έννοιες της κρυπτογραφίας, των κρυπτοσυστημάτων και της κρυπτανάλυσης. Στη συνέχεια θα περιγράψουμε πιο αναλυτικά την λειτουργία διαφόρων κρυπτοσυστημάτων, και των αντίστοιχων μαθηματικών προβλημάτων στα οποία βασίζονται, με τα οποία θα ασχοληθούμε στην διατριβή, καθώς και των υπαρχουσών μεθόδων κρυπτανάλυσής τους.

1.2.1 Βασική ορολογία και έννοιες

Προκειμένου να ορίσουμε τις βασικές έννοιες της κρυπτογραφίας, ας θεωρήσουμε το απλό πρόβλημα κατά το οποίο ένας αποστολέας θέλει να στείλει ένα μήνυμα σε έναν παραλήπτη, διατηρώντας το περιεχόμενο του μηνύματος κρυφό από τρίτους. Στην κρυπτογραφία το αρχικό μήνυμα που πρόκειται να στείλει ο αποστολέας ονομάζεται *πρωτότυπο ή καθαρό κείμενο (plaintext, cleartext)*. Η διαδικασία κατά την οποία το πρωτότυπο κείμενο μεταβάλλεται για να αποκρύψουμε την σημασία του και να διατηρηθεί κρυφό το περιεχόμενό του καλείται *κρυπτογράφηση*. Ένα κρυπτογραφημένο μήνυμα ονομάζεται και *κρυπτογράφημα (ciphertext)*, ενώ η διαδικασία μετατροπής του κρυπτογραφήματος στο αρχικό μήνυμα ονομάζεται *αποκρυπτογράφηση*. *Αντίπαλος (adversary)* θεωρείται οποιαδήποτε οντότητα, εκτός του αποστολέα και του παραλήπτη, η οποία προσπαθεί να ανατρέψει την ασφάλεια του συστήματος επικοινωνίας μεταξύ τους. Ένας αντίπαλος σε πολλές περιπτώσεις μπορεί να προσπαθήσει να υποδυθεί τον έγκυρο αποστολέα ή παραλήπτη.

Θεωρούμε ένα πεπερασμένο σύνολο $\mathcal{A}$ ως το αλφάβητο των μηνυμάτων. Ο χώρος των μηνυμάτων συμβολίζεται με $\mathcal{M}$ και αποτελείται από όλες τις δυνατές σειρές συμβόλων από το αλφάβητο $\mathcal{A}$. Ένα στοιχείο του συνόλου $\mathcal{M}$ είναι πρωτότυπο κείμενο και μπορεί για παράδειγμα να αποτελείται από δυαδικές συμβολοσειρές, Αγγλικό κείμενο, κώδικα υπολογιστών κ.τ.λ. Το σύνολο $\mathcal{C}$ συμβολίζει το χώρο των κρυπτογραφημάτων και αποτελείται από σειρές συμβόλων από ένα αλφάβητο που μπορεί να είναι είτε το $\mathcal{A}$ είτε να διαφέρει από αυτό. Συμβολίζουμε με $\mathcal{K}$ το σύνολο που αποτελεί το χώρο των κλειδιών. Κάθε στοιχείο $e \in \mathcal{K}$ ορίζει μοναδικά μια αμφιμονοσήμαντη συνάρτηση $E_e : \mathcal{M} \mapsto \mathcal{C}$ που καλείται συνάρτηση κρυπτογράφησης και μια αντίστοιχη αμφιμονοσήμαντη συνάρτηση $D_d : \mathcal{C} \mapsto \mathcal{M}$, με $d \in \mathcal{K}$, που καλείται συνάρτηση αποκρυπτογράφησης. Η διαδικασία εφαρμογής της συνάρτησης κρυπτογράφησης E_e σε ένα μήνυμα $m \in \mathcal{M}$ ονομάζεται κρυπτογράφηση του m και η διαδικασία εφαρμογής της συνάρτησης D_d σε ένα κρυπτογράφημα $c \in \mathcal{C}$ ονομάζεται αποκρυπτογράφηση του c.

Ένα σχήμα κρυπτογράφησης αποτελείται από ένα σύνολο $\{E_e : e \in \mathcal{K}\}$ συναρτήσεων κρυπτογράφησης και το αντίστοιχο σύνολο $\{D_d : d \in \mathcal{K}\}$ συναρτήσεων αποκρυπτογράφησης, με την ιδιότητα ότι για κάθε $e \in \mathcal{K}$ υπάρχει μοναδικό κλειδί $d \in \mathcal{K}$ τέτοιο ώστε $D_d = E_e^{-1}$ δηλαδή $D_d(E_e(m)) = m, \forall m \in \mathcal{M}$. Ένα σχήμα κρυπτογράφησης καλείται *κρυπτοσύστημα (cryptosystem, cipher)*. Το ζεύγος κλειδιών e και d συμβολίζονται και (e, d) και σε κάποιες περιπτώσεις κρυπτοσυστημάτων τα δύο κλειδιά είναι ίδια. Για την κατασκευή ενός κρυπτοσυστήματος απαιτείται η επιλογή ενός χώρου μηνυμάτων $\mathcal{M}$, ενός χώρου κρυπτογραφημάτων $\mathcal{C}$, ένας χώρος κλειδιών $\mathcal{K}$, ένα σύνολο συναρτήσεων κρυπτογράφησης $\{E_e : e \in \mathcal{K}\}$ και το αντίστοιχο σύνολο συναρτήσεων αποκρυπτογράφησης $\{D_d : d \in \mathcal{K}\}$. Γενικά, τα κρυπτοσυστήματα ανάλογα με το είδος των κλειδιών που περιλαμβάνουν χωρίζονται σε δύο κατηγορίες: τα κρυπτοσυστήματα συμμετρικού κλειδιού και τα κρυπτοσυστήματα δημοσίου κλειδιού.

1.2.1.1 Κρυπτανάλυση

Η *κρυπτανάλυση* είναι η μελέτη μαθηματικών μεθόδων για την ανατροπή της ασφάλειας των κρυπτοσυστημάτων και των υπηρεσιών ασφαλούς επικοινωνίας γενικότερα. Θεμελιώδης υπόθεση της κρυπτανάλυσης είναι η *υπόθεση του Kerckhoff*, σύμφωνα με την οποία η μυστικότητα πρέπει να βασίζεται ολοκληρωτικά στο κλειδί της κρυπτογράφησης [185], δηλαδή, θεωρούμε πάντα ότι το χρησιμοποιούμενο σύστημα κρυπτογράφησης είναι γνωστό σε όλους. Κατά συνέπεια οι μέθοδοι κρυπτανάλυσης αποσκοπούν στην εύρεση κρίσιμων σημείων του συστήματος μέσω των οποίων μπορεί να καταρρεύσει η ασφάλειά του. Ουσιαστικά, η κρυπτανάλυση αποσκοπεί στην αποκάλυψη του πρωτότυπου κειμένου χωρίς να υπάρχει πρόσβαση στο κλειδί και η επιτυχής κρυπτανάλυση μπορεί να αποκαλύψει είτε το αρχικό μήνυμα είτε το κλειδί που χρησιμοποιείται για την κρυπτογράφησή του, μέσω των αδύναμων σημείων του κρυπτοσυστήματος.

Μια προσπάθεια κρυπτανάλυσης καλείται *επίθεση (attack)*. Υπάρχουν διάφοροι γενικοί

τύποι κρυπταναλυτικών επιθέσεων, οι πιο σημαντικοί και συνήθως χρησιμοποιούμενοι περιγράφονται στη συνέχεια. Σε κάθε περίπτωση θεωρούμε ότι ο κρυπταναλυτής έχει πλήρη γνώση του αλγορίθμου κρυπτογράφησης που χρησιμοποιείται.

1. *Επίθεση μόνο κρυπτογραφήματος (ciphertext-only attack).* Στην περίπτωση αυτή ο κρυπταναλυτής έχει τα κρυπτογραφήματα από κάποια πρωτότυπα κείμενα, τα οποία έχουν όλα κρυπτογραφηθεί χρησιμοποιώντας τον ίδιο αλγόριθμο κρυπτογράφησης. Σκοπός του κρυπταναλυτή είναι να αποκαλύψει το πρωτότυπο κείμενο από όσο περισσότερα κρυπτογραφήματα είναι δυνατόν ή καλύτερα να εξάγει από αυτά το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφησή τους προκειμένου να αποκρυπτογραφήσει και άλλα μηνύματα που κρυπτογραφούνται με το ίδιο κλειδί. Δηλαδή, δοθέντων των $C_1 = E_k(P_1), C_2 = E_k(P_2), \ldots, C_i = E_k(P_i)$, παρήγαγε είτε τα $P_1, P_2, \ldots, P_i, k$ είτε έναν αλγόριθμο που θα παράγει το P_{i+1} από το $C_{i+1} = E_k(P_{i+1})$.

2. *Επίθεση γνωστού πρωτότυπου κειμένου (known-plaintext attack).* Στην περίπτωση αυτή ο κρυπταναλυτής έχει πρόσβαση σε κρυπτογραφήματα αλλά και στα πρωτότυπα κείμενα αυτών των κρυπτογραφημάτων. Σκοπός του είναι να αποκαλύψει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση κάθε μηνύματος ή έναν αλγόριθμο που θα αποκρυπτογραφεί κάθε νέο μήνυμα που κρυπτογραφείται με το ίδιο κλειδί με τα προηγούμενα. Δηλαδή, δοθέντος των $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, C_i = E_k(P_i)$, παρήγαγε είτε το k είτε έναν αλγόριθμο που εξάγει το P_{i+1} από το $C_{i+1} = E_k(P_{i+1})$.

3. *Επίθεση επιλεγμένου πρωτότυπου κειμένου (chosen-plaintext attack).* Ο κρυπταναλυτής έχει πρόσβαση σε κρυπτογραφήματα και τα αντίστοιχα πρωτότυπα κείμενα αλλά επιπλέον μπορεί να επιλέξει τα πρωτότυπα κείμενα για τα οποία θα έχει τα αντίστοιχα κρυπτογραφήματα. Αυτό το είδος επίθεσης είναι πιο ισχυρό από την επίθεση γνωστού πρωτότυπου κειμένου καθώς ο κρυπταναλυτής μπορεί να επιλέξει τα πρωτότυπα κείμενα που μπορεί να του δώσουν περισσότερες πληροφορίες για το κλειδί. Σκοπός του κρυπταναλυτή είναι να εξάγει το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων ή έναν αλγόριθμο που θα αποκρυπτογραφεί κάθε νέο μήνυμα που κρυπτογραφείται με το ίδιο κλειδί. Δηλαδή, δοθέντων των $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, C_i = E_k(P_i)$, όπου ο κρυπταναλυτής επιλέγει τα $P_1, P_2, \ldots, P_i$, παρήγαγε είτε το κλειδί k, είτε έναν αλγόριθμο για την εξαγωγή του P_{i+1} από το $C_{i+1} = E_k(P_{i+1})$.

4. *Επίθεση μεταβαλλόμενου επιλεγμένου πρωτότυπου κειμένου (adaptive-chosen-plaintext attack).* Αυτή είναι μια ειδική περίπτωση επίθεσης επιλεγμένου πρωτότυπου κειμένου. Ο κρυπταναλυτής δεν επιλέγει απλά τα πρωτότυπα κείμενα που θα κρυπτογραφηθούν αλλά μπορεί επίσης να μεταβάλλει την επιλογή του βασιζόμενος στα αποτελέσματα της προηγούμενης κρυπτογράφησης. Στην επίθεση επιλεγμένου πρωτότυπου κειμένου, ο κρυπταναλυτής μπορεί απλά να επιλέξει ένα μεγάλο τμήμα πρωτότυπου κειμένου προς κρυπτογράφηση ενώ στην επίθεση μεταβαλλόμενου επιλεγμένου πρωτότυπου κειμένου μπορεί να επιλέξει ένα μικρότερο τμήμα πρωτότυπου κειμένου και μετά να επιλέξει ένα άλλο ανάλογα με το αποτέλεσμα που πήρε από το πρώτο κ.ο.κ.

5. *Επίθεση επιλεγμένου κρυπτογραφήματος (chosen-ciphertext attack).* Στην περίπτωση αυτή ο κρυπταναλυτής μπορεί να επιλέξει διάφορα κρυπτογραφήματα που θα αποκρυπτογραφηθούν και έχει πρόσβαση στο αποκρυπτογραφημένο μήνυμα που προκύπτει. Σκοπός του κρυπταναλυτή είναι να ανακαλύψει το κλειδί. Δηλαδή, δοθέντος των $C_1, P_1 = D_k(C_1), C_2, P_2 = D_k(C_2), \ldots, C_i, P_i = D_k(C_i)$, να βρεθεί το κλειδί k.

Οι επιθέσεις γνωστού πρωτότυπου κειμένου και επιλεγμένου πρωτότυπου κειμένου είναι αρκετά συνηθισμένες και χρησιμοποιήθηκαν επιτυχώς και κατά την διάρκεια του 2ου παγκοσμίου πολέμου.

1.2.2 Κρυπτοσυστήματα συμμετρικού κλειδιού

Από την εμφάνιση της κρυπτογραφίας μέχρι και το 1976 η κρυπτογράφηση των μηνυμάτων γινόταν ουσιαστικά με την πρότερη επικοινωνία του αποστολέα και του παραλήπτη μέσω ασφαλούς διαύλου, δηλαδή διαύλου μη προσβάσιμου σε κάποιον αντίπαλο, κατά την οποία συμφωνούσαν για το χρησιμοποιούμενο μυστικό κλειδί. Αυτό το κλειδί χρησιμοποιούνταν κατά την κρυπτογράφηση του μηνύματος από τον αποστολέα και στη συνέχεια το κρυπτογράφημα αποστελλόταν μέσω μη ασφαλούς διαύλου επικοινωνίας προς τον παραλήπτη. Ο παραλήπτης με τη βοήθεια του μυστικού κλειδιού αποκρυπτογραφούσε το κρυπτογράφημα και λάμβανε το αρχικό μήνυμα. Αυτό το είδος κρυπτογράφησης κατά την οποία απαιτείται η ανταλλαγή κλειδιών μέσω ασφαλούς διαύλου επικοινωνίας καλείται κρυπτογράφηση συμμετρικού κλειδιού (symmetric key cryptography) και ορίζεται ως εξής

Ορισμός 1.1 *Θεωρούμε ένα σχήμα κρυπτογράφησης που αποτελείται από το σύνολο συναρτήσεων κρυπτογράφησης* $\{E_e : e \in \mathcal{K}\}$ *και το σύνολο συναρτήσεων αποκρυπτογράφησης* $\{D_d : d \in \mathcal{K}\}$*, αντίστοιχα, όπου* $\mathcal{K}$ *είναι ο χώρος κλειδιών. Το σχήμα κρυπτογράφησης καλείται κρυπτογράφηση συμμετρικού κλειδιού (symmetric key cryptography) αν για κάθε σχετιζόμενο ζεύγος κλειδιών* (e, d)*, είναι υπολογιστικά εύκολο να καθοριστεί το* d *γνωρίζοντας μόνο το* e *και αντίστροφα.*

Στα περισσότερα πρακτικά κρυπτοσυστήματα συμμετρικού κλειδιού το κλειδί κρυπτογράφησης e είναι ίδιο με το κλειδί αποκρυπτογράφησης d.

Ένα σημαντικό πρόβλημα στα κρυπτοσυστήματα συμμετρικού κλειδιού είναι η εύρεση μιας αποτελεσματικής μεθόδου ασφαλούς ανταλλαγής κλειδιών. Το πρόβλημα αυτό αναφέρεται και ως *πρόβλημα διανομής (ανταλλαγής) κλειδιών (key distribution problem)* και αποτελεί επιμέρους κλάδο της κρυπτογραφίας. Σε όλα τα συστήματα κρυπτογράφησης θεωρούμε ότι το σύνολο συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης, δηλαδή το σχήμα κρυπτογράφησης, είναι γνωστό σε όλους και η μόνη πληροφορία που απαιτείται να παραμένει κρυφή είναι το κλειδί αποκρυπτογράφησης d. Καθώς όμως στην κρυπτογράφηση συμμετρικού κλειδιού το κλειδί αποκρυπτογράφησης d υπολογίζεται εύκολα από το κλειδί κρυπτογράφησης e συνεπάγεται ότι στην περίπτωση αυτή και το κλειδί e πρέπει να παραμένει κρυφό. Υπάρχουν δύο βασικές κλάσεις σχημάτων κρυπτογράφησης συμμετρικού κλειδιού, τα *κρυπτοσυστήματα τμηματικής κρυπτογράφησης (block ciphers)* και τα *κρυπτοσυστήματα ροής (stream ciphers).*

1.2.2.1 Κρυπτοσυστήματα τμηματικής κρυπτογράφησης (Block ciphers)

Ορισμός 1.2 *Ένα κρυπτοσύστημα τμηματικής κρυπτογράφησης (block cipher) είναι ένα σχήμα κρυπτογράφησης το οποίο χωρίζει το πρωτότυπο κείμενο που πρόκειται να αποσταλεί σε συμβολοσειρές που καλούνται τμήματα (blocks) συγκεκριμένου μήκους* t *επί του αλφάβητου* $\mathcal{A}$ *και κρυπτογραφεί κάθε ένα τμήμα χωριστά.*

Οι δύο βασικές κλάσεις κρυπτοσυστημάτων τμηματικής κρυπτογράφησης είναι τα *κρυπτοσυστήματα αντικατάστασης (substitution ciphers)* και τα *κρυπτοσυστήματα μετάθεσης (transposition ciphers).* Τα *κρυπτοσυστήματα γινομένου (product ciphers)* είναι συνδυασμός των δύο προηγούμενων κλάσεων.

Κρυπτοσυστήματα αντικατάστασης (Substitution ciphers) Τα κρυπτοσυστήματα αντικατάστασης είναι κρυπτοσυστήματα τμηματικής κρυπτογράφησης που αντικαθιστούν σύμβολα ή ομάδες συμβόλων του πρωτότυπου κειμένου με άλλα σύμβολα ή ομάδες συμβόλων. Υπάρχουν διάφορα είδη κρυπτοσυστημάτων αντικατάστασης όπως τα κρυπτοσυστήματα απλής αντικατάστασης, τα κρυπτοσυστήματα ομοφωνικής αντικατάστασης και τα κρυπτοσυστήματα πολυαλφαβητικής αντικατάστασης.

Ορισμός 1.3 *Έστω $\mathcal{A}$ ένα αλφάβητο q συμβόλων και $\mathcal{M}$ το σύνολο όλων των συμβολοσειρών του $\mathcal{A}$ μήκους t. Έστω $\mathcal{K}$ το σύνολο όλων των αντιμεταθέσεων του συνόλου $\mathcal{A}$. Για κάθε $e \in \mathcal{K}$ ορίζουμε μια συνάρτηση κρυπτογράφησης E_e ως $E_e(m) = (e(m_1)e(m_2)\cdots e(m_t)) = (c_1c_2\cdots c_t) = c$, όπου $m = (m_1m_2\cdots m_t) \in \mathcal{M}$. Δηλαδή κάθε σύμβολο σε μια $t-$άδα αντικαθίσταται με ένα άλλο σύμβολο του $\mathcal{A}$ σύμφωνα με μια συγκεκριμένη αντιμετάθεση e. Για να αποκρυπτογραφήσουμε το $c = (c_1c_2\cdots c_t)$ υπολογίζουμε την αντίστροφη αντιμετάθεση $d = e^{-1}$ και τότε είναι $D_d(c) = (d(c_1)d(c_2)\cdots d(c_t)) = (m_1m_2\cdots m_t) = m$. Η συνάρτηση E_e καλείται κρυπτοσύστημα απλής αντικατάστασης ή μονοαλφαβητικής αντικατάστασης (simple substitution cipher, mono-alphabetic substitution cipher).*

Ο αριθμός των διαφορετικών κρυπτοσυστημάτων αντικατάστασης είναι $q!$ και είναι ανεξάρτητος από το μέγεθος του τμήματος (block) που χρησιμοποιεί το κρυπτοσύστημα. Τα κρυπτοσυστήματα απλής αντικατάστασης για μικρά μεγέθη t του τμήματος δεν είναι ιδιαίτερα ασφαλή ακόμα κι αν ο χώρος των κλειδιών είναι πολύ μεγάλος. Αυτό προκύπτει εύκολα παρατηρώντας ότι η κατανομή των συχνοτήτων των συμβόλων του πρωτότυπου κειμένου διατηρείται και στο κρυπτογράφημα και συνεπώς ένας κρυπταναλυτής μπορεί να προσδιορίσει το κλειδί αναλύοντας έναν μικρό αριθμό κρυπτογραφημένων τμημάτων.

Ορισμός 1.4 *Με κάθε σύμβολο $a \in \mathcal{A}$ συσχετίζουμε ένα σύνολο $H(a)$ συμβολοσειρών t συμβόλων με τον περιορισμό τα σύνολα $H(a), a \in \mathcal{A}$ να είναι ανά δύο ξένα. Ένα κρυπτοσύστημα ομοφωνικής αντικατάστασης (homophonic substitution cipher) αντικαθιστά κάθε σύμβολο a σε ένα τμήμα πρωτότυπου κειμένου με μια τυχαία επιλεγμένη συμβολοσειρά από το σύνολο $H(a)$. Για την αποκρυπτογράφηση μιας συμβολοσειράς c, t συμβόλων, πρέπει να καθοριστεί ένα $a \in \mathcal{A}$ τέτοιο ώστε $c \in H(a)$. Το κλειδί του κρυπτοσυστήματος αποτελείται από τα σύνολα $H(a)$.*

Ένα κρυπτοσύστημα ομοφωνικής αντικατάστασης μπορεί να χρησιμοποιηθεί για να κάνει περισσότερο ομοιόμορφη την συχνότητα εμφάνισης των συμβόλων του κρυπτογραφήματος σε σχέση με την αντίστοιχη στο κρυπτοσύστημα απλής αντικατάστασης με το κόστος της επέκτασης των δεδομένων. Κατ' αυτό τον τρόπο η κρυπτανάλυση γίνεται δυσκολότερη.

Ορισμός 1.5 *Ένα κρυπτοσύστημα πολυαλφαβητικής αντικατάστασης (polyalphabetic substitution cipher) είναι ένα κρυπτοσύστημα τμηματικής κρυπτογράφησης με μήκος t για τα τμήματα επί ενός αλφάβητου $\mathcal{A}$ με τις ακόλουθες ιδιότητες:*

1. *ο χώρος των κλειδιών $\mathcal{K}$ αποτελείται από όλα τα διατεταγμένα σύνολα t αντιμεταθέσεων $(p_1, p_2, \ldots, p_t)$, όπου κάθε αντιμετάθεση p_i ορίζεται επί του συνόλου $\mathcal{A}$,*
2. *η κρυπτογράφηση του πρωτότυπου κειμένου $m = (m_1m_2\cdots m_t)$ με το κλειδί $e = (p_1, p_2, \ldots, p_t)$ δίνεται ως $E_e(m) = (p_1(m_1)p_2(m_2)\cdots p_t(m_t))$ και*
3. *το κλειδί αποκρυπτογράφησης που αντιστοιχεί στο $e = (p_1, p_2, \ldots, p_t)$ είναι το $d = (p_1^{-1}, p_2^{-1}, \ldots, p_t^{-1})$.*

Παράδειγμα των κρυπτοσυστημάτων πολυαλφαβητικής αντικατάστασης είναι το κρυπτοσύστημα Vigenére [201]. Τα κρυπτοσυστήματα πολυαλφαβητικής αντικατάστασης έχουν το πλεονέκτημα σε σχέση με τα κρυπτοσυστήματα απλής αντικατάστασης ότι δεν διατηρούν τις συχνότητες εμφάνισης των συμβόλων. Ωστόσο, δεν είναι πολύ δύσκολο να κρυπταναλυθούν με τρόπο παρόμοιο με αυτό των κρυπτοσυστημάτων απλής αντικατάστασης. Συγκεκριμένα, αφού καθοριστεί το μήκος t των τμημάτων, τα σύμβολα του κρυπτογραφήματος χωρίζονται σε t ομάδες (όπου η ομάδα $i, 1 \leqslant i \leqslant t$, αποτελείται από αυτά τα σύμβολα του κρυπτογραφήματος που προκύπτουν χρησιμοποιώντας την αντιμετάθεση p_i) και η ανάλυση συχνοτήτων μπορεί να εφαρμοστεί σε κάθε ομάδα χωριστά.

Κρυπτοσυστήματα μετάθεσης (Transposition ciphers) Μια άλλη κλάση κρυπτοσυστημάτων συμμετρικού κλειδιού είναι τα *κρυπτοσυστήματα απλής μετάθεσης (simple transposititon ciphers)* τα οποία απλά αντιμεταθέτουν τα σύμβολα σε ένα τμήμα πρωτότυπου κειμένου.

Ορισμός 1.6 *Θεωρούμε ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού με τμήματα μήκους t. Έστω $\mathcal{K}$ το σύνολο όλων των αντιμεταθέσεων του συνόλου $\{1, 2, \ldots, t\}$. Για κάθε $e \in \mathcal{K}$ ορίζουμε την συνάρτηση κρυπτογράφησης $E_e(m) = (m_{e(1)} m_{e(2)} \cdots m_{e(t)})$, όπου $m = (m_1 m_2 \cdots m_t) \in \mathcal{M}$ που είναι ο χώρος των μηνυμάτων. Το σύνολο όλων αυτών των συναρτήσεων καλείται κρυπτοσύστημα απλής μετάθεσης. Το κλειδί αποκρυπτογράφησης που αντιστοιχεί στο e είναι η αντίστροφη αντιμετάθεση $d = e^{-1}$. Για να αποκρυπτογραφήσουμε το $c = (c_1 c_2 \cdots c_t)$ υπολογίζουμε το $D_d(c) = (c_{d(1)} c_{d(2)} \cdots c_{d(t)})$.*

Ένα κρυπτοσύστημα απλής μετάθεσης διατηρεί τον αριθμό των συμβόλων μέσα στο τμήμα και συνεπώς μπορεί εύκολα να κρυπταναλυθεί.

Κρυπτοσυστήματα γινομένου (Product ciphers) Τα κρυπτοσυστήματα απλής αντικατάστασης και απλής μετάθεσης ανεξάρτητα δεν παρέχουν πολύ υψηλό επίπεδο ασφάλειας. Ωστόσο, συνδυάζοντας τους μετασχηματισμούς που χρησιμοποιούν είναι δυνατό να δημιουργήσουμε ισχυρά κρυπτοσυστήματα. Ένα παράδειγμα κρυπτοσυστημάτων γινομένου είναι μια σύνθεση των $t \geqslant 2$ μετασχηματισμών $E_{k_1} E_{k_2} \cdots E_{k_t}$, όπου κάθε $E_{k_i}, 1 \leqslant i \leqslant t$, είναι είτε ένα κρυπτοσύστημα αντικατάστασης είτε ένα κρυπτοσύστημα μετάθεσης. Ας θεωρήσουμε ότι η σύνθεση μιας αντικατάστασης και μιας μετάθεσης καλείται *γύρος (round)*. Σε ένα γύρο μια αντικατάσταση προσθέτει *σύγχυση (confusion)* στη διαδικασία κρυπτογράφησης ενώ μια μετάθεση προσθέτει *διάχυση (diffusion)*. Η σύγχυση έχει σκοπό να κάνει περισσότερο σύνθετη τη σχέση μεταξύ του κλειδιού και του κρυπτογραφήματος. Η διάχυση αναφέρεται στην αναδιάταξη και τον διαχωρισμό των δυαδικών ψηφίων του μηνύματος έτσι ώστε κάθε συσσώρευση στο πρωτότυπο κείμενο να διαχέεται στο κρυπτογράφημα. Τα σύγχρονα συστήματα τμηματικής κρυπτογράφησης εφαρμόζουν διαδοχικά έναν αριθμό γύρων για την κρυπτογράφηση του πρωτότυπου κειμένου.

1.2.2.2 Κρυπτοσυστήματα ροής (Stream ciphers)

Τα κρυπτοσυστήματα ροής αποτελούν μια σημαντική κλάση των κρυπτοσυστημάτων συμμετρικού κλειδιού. Μπορούμε να θεωρήσουμε ότι είναι κρυπτοσυστήματα τμηματικής κρυπτογράφησης με μήκος τμήματος ίσο με ένα. Είναι χρήσιμα υπό την έννοια ότι ο μετασχηματισμός κρυπτογράφησης μπορεί να αλλάζει για κάθε σύμβολο του πρωτότυπου κειμένου που κρυπτογραφείται. Σε περιπτώσεις όπου τα σφάλματα μετάδοσης είναι αρκετά πιθανά τα κρυπτοσυστήματα ροής πλεονεκτούν καθώς δεν έχουν διάδοση του σφάλματος. Μπορούν επίσης να χρησιμοποιηθούν όταν τα δεδομένα πρέπει να διαχειρίζονται κατά ένα σύμβολο κάθε φορά όταν για παράδειγμα ο εξοπλισμός δεν έχει επαρκή μνήμη για διαχείριση μεγαλύτερων τμημάτων δεδομένων.

Ορισμός 1.7 *Έστω $\mathcal{K}$ ο χώρος των κλειδιών για ένα σύνολο συναρτήσεων κρυπτογράφησης. Μια ακολουθία συμβόλων $e_1 e_2 \cdots e_i \in \mathcal{K}$ καλείται σειρά (ροή) κλειδιών (keystream).*

Ορισμός 1.8 *Έστω $\mathcal{A}$ ένα αλφάβητο q συμβόλων και E_e ένα κρυπτοσύστημα απλής αντικατάστασης με μήκος τμήματος ίσο με 1, όπου $e \in \mathcal{K}$. Έστω $m_1 m_2 m_3 \cdots$ μια συμβολοσειρά του πρωτότυπου κειμένου και $e_1 e_2 e_3 \cdots$ μια σειρά κλειδιών του $\mathcal{K}$. Ένα κρυπτοσύστημα ροής παίρνει τη συμβολοσειρά του πρωτότυπου κειμένου και παράγει μια συμβολοσειρά κρυπτογραφήματος $c_1 c_2 c_3 \cdots$, όπου $c_i = E_{e_i(m_i)}$. Αν το d_i συμβολίζει το αντίστροφο του e_i τότε το $D_{d_i}(c_i) = m_i$ αποκρυπτογραφεί τη συμβολοσειρά του κρυπτογραφήματος.*

Ένα κρυπτοσύστημα ροής εφαρμόζει απλούς κρυπτογραφικούς μετασχηματισμούς ανάλογα με τη σειρά κλειδιών που χρησιμοποιείται. Η σειρά κλειδιών πρέπει να δημιουργείται τυχαία ή από έναν αλγόριθμο που παράγει σειρά κλειδιών από μια αρχική μικρή σειρά κλειδιών που ονομάζεται σπόρος (seed) ή από έναν σπόρο και προηγούμενα σύμβολα του κρυπτογραφήματος. Ένας τέτοιος αλγόριθμος καλείται γεννήτορας σειράς κλειδιών (keystream generator). Παράδειγμα των κρυπτοσυστημάτων ροής είναι το κρυπτοσύστημα Vernam [201].

1.2.3 Κρυπτοσυστήματα δημοσίου κλειδιού

Μέχρι τα τέλη της δεκαετίας του '70 όλες οι εκπομπές κρυπτογραφημένων μηνυμάτων γίνονταν με χρήση κρυπτοσυστημάτων συμμετρικού κλειδιού. Το 1976 ο W. Diffie και ο M. Hellman [46] εφεύραν ένα καινοτόμο είδος κρυπτογράφησης την *κρυπτογράφηση δημοσίου κλειδιού (public key cryptography)*. Η ιδέα του νέου αυτού είδους κρυπτογράφησης βασίζεται στη χρήση *μονόδρομων συναρτήσεων (one-way functions)*.

Ορισμός 1.9 *Μια συνάρτηση $f : X \mapsto Y$ καλείται μονόδρομη συνάρτηση εάν η τιμή της $f(x)$ μπορεί να υπολογιστεί εύκολα για οποιοδήποτε $x \in X$, αλλά για τα περισσότερα τυχαία επιλεγμένα $y \in \mathrm{Im}(f)$ είναι υπολογιστικά ανέφικτο να βρεθεί κάποιο $x \in X$ τέτοιο ώστε $f(x) = y$.*

Μια ειδική μορφή μονόδρομων συναρτήσεων είναι οι *μονόδρομες συναρτήσεις κερκόπορτας (trapdoor one-way functions)*.

Ορισμός 1.10 *Μια μονόδρομη συνάρτηση κερκόπορτας είναι μια μονόδρομη συνάρτηση $f : X \mapsto Y$ με την εξής επιπρόσθετη ιδιότητα: δοθείσης κάποιας επιπλέον πληροφορίας είναι εφικτό να βρεθεί για δοθέν $y \in \mathrm{Im}(f)$ ένα $x \in X$ τέτοιο ώστε $f(x) = y$.*

Έστω $\{E_e : e \in \mathcal{K}\}$ ένα σύνολο συναρτήσεων κρυπτογράφησης και $\{D_d : d \in \mathcal{K}\}$ το σύνολο των αντίστοιχων συναρτήσεων αποκρυπτογράφησης, όπου $\mathcal{K}$ ο χώρος των κλειδιών. Θεωρούμε ένα οποιοδήποτε ζεύγος σχετιζόμενων συναρτήσεων κρυπτογράφησης / αποκρυπτογράφησης (E_e, D_d) και υποθέτουμε ότι κάθε ζεύγος έχει την ακόλουθη ιδιότητα: δοθέντος του E_e και ενός τυχαίου κρυπτογραφήματος $c \in C$ είναι υπολογιστικά ανέφικτο να βρεθεί ένα μήνυμα $m \in M$ τέτοιο ώστε $E_e(m) = c$. Αυτό σημαίνει ότι δοθέντος του e είναι ανέφικτο να υπολογιστεί το αντίστοιχο κλειδί αποκρυπτογράφησης d. Στην κρυπτογράφηση δημοσίου κλειδιού η συνάρτηση E_e είναι μια μονόδρομη συνάρτηση κερκόπορτας, όπου το e είναι το κλειδί κρυπτογράφησης και καλείται *δημόσιο κλειδί (public key)* και το d είναι η επιπλέον πληροφορία (κερκόπορτα) που απαιτείται για τον υπολογισμό της αντίστροφης συνάρτησης, δηλαδή για την αποκρυπτογράφηση, και καλείται *ιδιωτικό κλειδί (private key)*.

Υπό τις παραπάνω προϋποθέσεις ας θεωρήσουμε την επικοινωνία δύο μελών, Α και Β. Ο Β επιλέγει ένα ζεύγος κλειδιών (e, d). Ο Β στέλνει το κλειδί κρυπτογράφησης e στον Α μέσω οποιουδήποτε καναλιού και κρατά κρυφό το κλειδί αποκρυπτογράφησης d. Ο Α μπορεί στη συνέχεια να στείλει ένα μήνυμα m στον Β εφαρμόζοντας σε αυτό την συνάρτηση κρυπτογράφησης που ορίζεται από το δημόσιο κλειδί του Β, δηλαδή στέλνει το κρυπτογράφημα $c = E_e(m)$. Ο Β αποκρυπτογραφεί το κρυπτογράφημα c εφαρμόζοντας την αντίστροφη συνάρτηση D_d που ορίζεται κατά μοναδικό τρόπο από το d.

Κατά τον ίδιο τρόπο, η συνάρτηση κρυπτογράφησης μπορεί να υπολογιστεί εύκολα από οποιονδήποτε ο οποίος έχει το δημόσιο κλειδί του Β, αλλά η αντίστροφη συνάρτηση (που αποκρυπτογραφεί τα κρυπτογραφημένα μηνύματα) δεν μπορεί να υπολογιστεί σε εφικτό χρόνο χωρίς το ιδιωτικό κλειδί d. Αυτό σημαίνει ότι οποιοσδήποτε μπορεί να στείλει ένα μήνυμα στον Β χρησιμοποιώντας για κρυπτογράφηση το ίδιο κλειδί, δηλαδή το δημόσιο κλειδί του Β, το οποίο μπορεί βρίσκεται σε έναν δημόσιο φάκελο με πιστοποιημένα περιεχόμενα. Στη συνέχεια ο Β και μόνο αυτός χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το

μήνυμα του αποστολέα. Συνεπώς, σε αντίθεση με την κρυπτογράφηση συμμετρικού κλειδιού, στην κρυπτογράφηση δημοσίου κλειδιού ο αποστολέας δεν χρειάζεται να έχει καμία εκ των προτέρων επικοινωνία με τον παραλήπτη γεγονός που αποτελεί ένα από τα σημαντικότερα χαρακτηριστικά αυτού του είδους κρυπτογράφησης.

Μια πιθανή αιτία για την αργή εμφάνιση του είδους της κρυπτογράφησης δημοσίου κλειδιού είναι ότι μέχρι το 1970 η χρήση της κρυπτογραφίας γινόταν κυρίως για στρατιωτικούς και διπλωματικούς σκοπούς, για τους οποίους η κρυπτογράφηση συμμετρικού κλειδιού ήταν επαρκής. Ωστόσο, με την αύξηση της χρήσης υπολογιστών στον τομέα της οικονομίας προέκυψαν νέες ανάγκες στην κρυπτογραφία. Σε αντίθεση με τους στρατιωτικούς ή τους διπλωματικούς κόλπους με τις αυστηρές ιεραρχίες, τις λίστες εξουσιοδοτημένων χρηστών και τα συστήματα αγγελιοφόρων, στις εμπορικές συναλλαγές και στην ιδιωτικότητα δεδομένων συναντάται μεγαλύτερη και περισσότερο ρευστή δομή χρηστών που χρησιμοποιούν κρυπτογράφηση. Ίσως για αυτό το λόγο η κρυπτογράφηση δημοσίου κλειδιού αναπτύχθηκε όταν υπήρξε πλέον η ανάγκη για αυτό το είδος κρυπτοσυστημάτων.

Μερικοί από τους τομείς εφαρμογής της κρυπτογράφησης δημοσίου κλειδιού είναι οι ακόλουθοι,

1. *μετάδοση εμπιστευτικών μηνυμάτων*,
2. *συστήματα ταυτοποίησης (identification systems)*, στα οποία οι χρήστες αποδεικνύουν ότι είναι εξουσιοδοτημένοι για πρόσβαση σε δεδομένα ή σε κάποια υπηρεσία, ή ότι είναι αυτοί που ισχυρίζονται,
3. *πιστοποίηση (authentication)*, η οποία επιβεβαιώνει ότι το μήνυμα έχει αποσταλεί από τον πραγματικό αποστολέα και δεν έχει παρέμβει κάποιος άλλος,
4. *μη-αποκήρυξη (nonrepudiation)*, η οποία προφυλάσσει από άτομα που ισχυρίζονται ότι δεν έχουν συμφωνήσει σε κάτι για το οποίο πραγματικά έχουν συμφωνήσει,
5. *ορισμός κλειδιού (key establishment)*, όπου δύο άτομα θέλουν να συμφωνήσουν σε ανοικτή επικοινωνία για ένα μυστικό κλειδί που θα χρησιμοποιήσουν σε συμμετρικά κρυπτοσυστήματα,
6. *μηχανισμοί ηλεκτρονικών χρηματικών συναλλαγών (electronic cash)*, που διατηρούν την ανωνυμία του καταναλωτή,
7. *σχήματα ηλεκτρονικών εκλογών (electronic voting)*, που εξασφαλίζουν την μυστικότητα των ψήφων και το έγκυρο αποτέλεσμα της ψηφοφορίας,
8. *σχήματα ηλεκτρονικών δημοπρασιών (electronic auctions)*, που εξασφαλίζουν την μυστικότητα των τιμών δημοπράτησης, δημόσια επαλήθευση του αποτελέσματος της δημοπρασίας και ανωνυμία των συμμετεχόντων και του νικητή στους υπόλοιπους συμμετέχοντες.

Τα βασικότερα μαθηματικά προβλήματα που χρησιμοποιήθηκαν για τη δημιουργία κρυπτοσυστημάτων δημόσιου κλειδιού είναι το πρόβλημα του διακριτού λογαρίθμου, το πρόβλημα Diffie-Hellman και το πρόβλημα παραγοντοποίησης, τα οποία περιγράφονται αναλυτικά στη συνέχεια.

Το Πρόβλημα του Διακριτού Λογαρίθμου (ΠΔΛ) [4,148,166] αφορά στην ανάπτυξη ενός αποδοτικού αλγορίθμου για τον υπολογισμό ενός ακέραιου αριθμού $x > 0$ που ικανοποιεί την σχέση

$$\alpha^x = \beta,$$

όπου τα α, β είναι στοιχεία μιας πεπερασμένης κυκλικής ομάδας και το α αποτελεί γεννήτορα της ομάδας αυτής. Υποθέτουμε ότι το x είναι ο μικρότερος μη αρνητικός ακέραιος αριθμός

τέτοιος ώστε να ισχύει $\alpha^x = \beta$. Τότε, το x ονομάζεται *δείκτης (index)* ή *διακριτός λογάριθμος* του β. Στην ειδική περίπτωση ενός πεπερασμένου σώματος $\mathbb{Z}_p$ πρώτης τάξης p, επιλέγεται μια πρωτεύουσα ρίζα $g \, modulo \, p$. Έτσι, αν u είναι ο μικρότερος μη αρνητικός ακέραιος τέτοιος ώστε να ισχύει $g^u \equiv h \pmod{p}$, τότε το u καλείται *δείκτης* ή *διακριτός λογάριθμος* του h. Το πρόβλημα του διακριτού λογαρίθμου είναι υπολογιστικά αδύνατο, δηλαδή δεν υπάρχει γνωστός αποδοτικός αλγόριθμος για την επίλυση του διακριτού λογαρίθμου.

Η ασφάλεια πολλών κρυπτοσυστημάτων δημοσίου αλλά και ιδιωτικού κλειδιού [4, 38, 53, 127, 128, 144, 146, 148, 166, 216, 217], βασίζεται στην υπόθεση ότι το ΠΔΛ είναι υπολογιστικά αδύνατο. Συγκεκριμένα, θα αναφερθούμε στο

(1) πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman [46], και στο

(2) κρυπτοσύστημα δημοσίου κλειδιού του El Gamal, καθώς και στο σχήμα ψηφιακών υπογραφών του El Gamal [53].

Το πρόβλημα ανταλλαγής κλειδιών των Diffie-Hellman (ΠΑΚDH) [38, 123, 216] ορίζεται ως εξής. Έστω α ένα σταθερό πρωτεύον στοιχείο ενός πεπερασμένου σώματος $\mathbb{F}_q$, τα x, y, συμβολίζουν τα ιδιωτικά κλειδιά δύο χρηστών που ικανοποιούν την σχέση $0 \leqslant x, y \leqslant q-2$, και τα $\beta = \alpha^x, \gamma = \alpha^y$ αναπαριστούν τα αντίστοιχα δημόσια κλειδιά. Τότε, το ΠΑΚDH αφορά στον υπολογισμό του α^{xy} από τα στοιχεία β, γ, όπου α^{xy} είναι το συμμετρικό κλειδί για την μυστική επικοινωνία μεταξύ των δύο χρηστών.

Θεωρούμε την ειδική περίπτωση του ΠΑΚDH, όπου $\beta = \gamma$. Ο όρος απεικόνιση των Diffie-Hellman αναφέρεται στην απεικόνιση

$$\beta = \alpha^x \mapsto \alpha^{x^2}.$$

Ο ορισμός του προβλήματος απεικόνισης των Diffie-Hellman (ΠΑDH) προκύπτει άμεσα από τον προηγούμενο ορισμό του ΠΑΚDH. Τα δύο αυτά προβλήματα ΠΑΚDH και ΠΑDH, είναι υπολογιστικά ισοδύναμα, καθώς ισχύει η ακόλουθη σχέση

$$\alpha^{x^2}\alpha^{y^2}\alpha^{2xy} = \alpha^{(x+y)^2},$$

και ο υπολογισμός του α^{xy} από το α^{2xy} είναι εφικτός (τετραγωνικές ρίζες σε πεπερασμένα σώματα).

Το πρόβλημα παραγοντοποίησης σχετίζεται με το κρυπτοσύστημα RSA [178]. Η ασφάλεια του κρυπτοσυστήματος αυτού βασίζεται στο γεγονός ότι είναι υπολογιστικά μη εφικτή η παραγοντοποίηση ενός θετικού ακεραίου $N = pq$, όπου p και q είναι δύο διαφορετικοί περιττοί πρώτοι αριθμοί [130]. Η παραγοντοποίηση του N είναι ισοδύναμη με τον προσδιορισμό του $\phi(N)$ από το N, όπου $\phi(N) = (p-1)(q-1)$ [178].

1.2.4 Κρυπτοσυστήματα Ελλειπτικών Καμπυλών

Κρυπτοσυστήματα που βασίζονται στις ελλειπτικές καμπύλες προτάθηκαν στις μελέτες [89, 139] ως εναλλακτική λύση σε σχέση με τα παραδοσιακά κρυπτοσυστήματα δημοσίου κλειδιού. Το σημαντικότερο πλεονέκτημά τους είναι η χρήση μικρών παραμέτρων (αναφορικά με το μέγεθός τους σε δυαδικά ψηφία) σε σχέση με τα συνήθη κρυπτοσυστήματα (για παράδειγμα το RSA). Αυτό οφείλεται στην ιδιαίτερα μεγάλη δυσκολία επίλυσης του προβλήματος διακριτού λογαρίθμου των ελλειπτικών καμπυλών (ΠΔΛΕΚ), που αποτελεί το μαθηματικό υπόβαθρο αυτών των κρυπτοσυστημάτων ελλειπτικών καμπυλών. Το ΠΔΛΕΚ θεωρείται ότι απαιτεί περισσότερο χρόνο επίλυσης από τον αντίστοιχο χρόνο επίλυσης του προβλήματος του διακριτού λογαρίθμου (ΠΔΛ), που είναι το ανάλογό του στο χώρο των πεπερασμένων σωμάτων. Η ασφάλεια των κρυπτοσυστημάτων που χρησιμοποιούν τους διακριτούς λογάριθμους, βασίζεται στην υπόθεση ότι τα προβλήματα αυτά δεν μπορούν να επιλυθούν σε πολυωνυμικό χρόνο.

Πολλές τεχνικές που αξιοποιούν αλγεβρικές και αριθμοθεωρητικές μεθόδους, αλλά και μεθόδους προσέγγισης και παρεμβολής [38, 102, 123, 128, 216] έχουν προταθεί για την επιτάχυνση της επίλυσης των δύο αυτών τύπων των διακριτών λογαρίθμων.

Μια ελλειπτική καμπύλη σε ένα πεπερασμένο σώμα $\mathbb{F}_p$, όπου $p > 3$ και πρώτος αριθμός, συμβολίζεται με $E(\mathbb{F}_p)$ και ορίζεται ως το σύνολο όλων των ζευγών $(x, y) \in \mathbb{F}_p$ που ικανοποιούν την εξίσωση $y^2 = x^3 + \alpha x + b$, όπου $\alpha, b \in \mathbb{F}_p$, με τον περιορισμό $4\alpha^3 + 27b^2 \neq 0$. Τα σημεία αυτά, μαζί με ένα ειδικό σημείο που συμβολίζεται ως $\mathcal{O}$, και καλείται σημείο στο άπειρο, και έναν κατάλληλο τελεστή πρόσθεσης σημείων, ορίζουν μια Αβελιανή ομάδα. Αυτή είναι η ομάδα ελλειπτικής καμπύλης και το σημείο $\mathcal{O}$ είναι το ταυτοτικό σημείο της ομάδας [16, 195]. Η τάξη m μιας ελλειπτικής καμπύλης ορίζεται ως ο αριθμός των σημείων της $E(\mathbb{F}_p)$. Σύμφωνα με το θεώρημα του Hasse [16, 195] ισχύει ότι $p + 1 - 2\sqrt{p} \leqslant m \leqslant p + 1 + 2\sqrt{p}$. Η τάξη ενός σημείου $P \in E(\mathbb{F}_p)$ είναι ο μικρότερος θετικός ακέραιος, n, για τον οποίο ισχύει $nP = \mathcal{O}$. Από το θεώρημα του Lagrange, ισχύει ότι η τάξη ενός σημείου είναι διαιρέτης της τάξης της ελλειπτικής καμπύλης.

Αν E είναι μια ελλειπτική καμπύλη σε ένα πεπερασμένο σώμα $\mathbb{F}_q$, P ένα σημείο της $E(\mathbb{F}_q)$ τάξης n και Q ένα σημείο της $E(\mathbb{F}_q)$, τέτοιο ώστε $Q = tP$, με $0 \leqslant t \leqslant (n-1)$, τότε το πρόβλημα του διακριτού λογαρίθμου της ελλειπτικής καμπύλης είναι ο προσδιορισμός της τιμής t. Οι βέλτιστοι αλγόριθμοι επίλυσης του ΠΔΛΕΚ απαιτούν εκθετικό αριθμό απαραίτητων βημάτων, σε αντίθεση με τους βέλτιστους αλγορίθμους επίλυσης του απλού διακριτού λογαρίθμου επί της πολλαπλασιαστικής ομάδας $\mathbb{F}_q$, που απαιτούν υπο-εκθετικό χρόνο του μεγέθους της χρησιμοποιούμενης ομάδας [5].

1.3 Προβλήματα υπό θεώρηση στην παρούσα διατριβή

Τις τελευταίες δεκαετίες, ο κλάδος της υπολογιστικής νοημοσύνης έχει παρουσιάσει πολύ μεγάλη εξέλιξη και οι μέθοδοί του έχουν εφαρμοστεί με μεγάλη επιτυχία σε προβλήματα προερχόμενα από διαφορετικούς επιστημονικούς τομείς όπως η ιατρική, η μηχανική, η οικονομία κ.ο.κ. Στα πλεονεκτήματα των μεθόδων υπολογιστικής νοημοσύνης συγκαταλέγεται ότι είναι σχετικά απλές στην εφαρμογή τους, ότι είναι αυτοματοποιημένες σε μεγάλο βαθμό και το σημαντικότερο ότι δεν απαιτούν «καλές» μαθηματικές ιδιότητες από το προς επίλυση πρόβλημα γεγονός που τις καθιστά κατάλληλες για επίλυση προβλημάτων που προέρχονται από πραγματικές εφαρμογές. Η ύπαρξη αυτοματοποιημένων και σχετικά απλών τεχνικών για τον σχεδιασμό και την κρυπτανάλυση κρυπτοσυστημάτων είναι ιδιαίτερα σημαντική καθώς επιτρέπει την γρήγορη εφαρμογή τους και χωρίς την ανάγκη ανθρώπινης αλληλεπίδρασης για την αξιολόγηση πολλών πιθανών λύσεων των υπό μελέτη προβλημάτων.

Έχοντας ως κίνητρο τα παραπάνω στοιχεία, το πρώτο πρόβλημα που θεωρούμε στην παρούσα διατριβή είναι η δυνατότητα εφαρμογής των μεθόδων της υπολογιστικής νοημοσύνης για την αντιμετώπιση προβλημάτων από τον πολύ απαιτητικό κλάδο της κρυπτολογίας. Πιο αναλυτικά, στόχος της διατριβής είναι να αναδείξει τα κρίσιμα σημεία κατά την εφαρμογή της υπολογιστικής νοημοσύνης στον κλάδο αυτό, να μελετήσει την δυνατότητα αυτοματοποίησης διαδικασιών κρυπτανάλυσης και τον συνδυασμό υπαρχόντων τεχνικών με πιο σύγχρονες μεθόδους όπως αυτές της υπολογιστικής νοημοσύνης, να ερευνήσει την εφαρμογή των μεθόδων αυτών ως εργαλείο ελέγχου της σθεναρότητας κρυπτοσυστημάτων και τέλος να καταγράψει την αποτελεσματικότητα και την αποδοτικότητα των μεθόδων σε σύγχρονα προβλήματα κρυπτογραφίας.

Για το σκοπό αυτό, στο πρώτο μέρος της παρούσας διατριβής θεωρούμε τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με σμήνος σωματιδίων από τους Εξελικτικούς Αλγορίθμους και νευρωνικά δίκτυα πρόσθιας τροφοδότησης και Πολυωνυμικά Δίκτυα Ridge από τα τεχνητά νευρωνικά δίκτυα και μελετάμε την εφαρμογή τους και την απόδοσή τους στο πρόβλημα του διακριτού λογαρίθμου στα πεπερασμένα σώματα [99, 105, 106] και στις ελλειπτικές καμπύλες [98], στο πρόβλημα παραγοντοποίησης ακεραίων [108], στην κρυπτανά-

λυση του Feistel κρυπτοσυστήματος DES τεσσάρων και έξι γύρων [100] και στην κατασκευή ισχυρών S-boxes [101, 109].

Το δεύτερο πρόβλημα που θεωρούμε στην παρούσα διατριβή είναι η εφαρμογή μεθόδων αντίστροφης πολυωνυμικής παρεμβολής για την μελέτη θεμελιωδών προβλημάτων κρυπτογραφίας, όπως είναι το πρόβλημα του διακριτού λογαρίθμου, η απεικόνιση Diffie-Hellman και το πρόβλημα του λογαρίθμου του Lucas, στα πεπερασμένα σώματα [103, 110]. Τα προβλήματα αυτά έχουν μελετηθεί με τη βοήθεια πολλών τεχνικών, αλγεβρικών, αριθμοθεωρητικών, παρεμβολής και άλλων. Η μελέτη για την πολυωνυμική προσέγγιση των προβλημάτων αυτών έχει αποδείξει ότι υπάρχουν μοναδικά πολυώνυμα παρεμβολής για την αναπαράστασή τους, ωστόσο τα πολυώνυμα αυτά είναι ιδιαίτερα υψηλού βαθμού ώστε να μπορούν να χρησιμοποιηθούν για την κρυπτανάλυση συστημάτων που βασίζονται στα προβλήματα αυτά. Στόχος της διατριβής είναι να μελετήσει υπολογιστικά την δυνατότητα αναπαράστασης των αντίστοιχων συναρτήσεων με την μορφή πολυωνύμων χρησιμοποιώντας μεθόδους αντίστροφης παρεμβολής οι οποίες είναι κατασκευαστικές και επιτρέπουν την πρόσθεση νέων σημείων παρεμβολής με μικρό υπολογιστικό κόστος.

Το επόμενο πρόβλημα που μελετάται στα πλαίσια της διατριβής είναι η κατασκευή νέων συμμετρικών κρυπτοσυστημάτων που βασίζονται σε τεχνικές υπολογιστικών μαθηματικών και συγκεκριμένα στις χαοτικές περιοδικές τροχιές και τις μεθόδους υπολογισμού τους [208]. Η αξιοποίηση των μη-γραμμικών δυναμικών συστημάτων και ειδικότερα του χάους στην κρυπτογραφία έχει αποτελέσει θέμα έρευνας τα τελευταία χρόνια λόγω της προφανούς πολυπλοκότητάς του και των στατιστικών ιδιοτήτων του. Ωστόσο, στις περισσότερες εργασίες που αφορούν στο συγκεκριμένο αντικείμενο δεν παρέχεται προσεκτική αξιολόγηση των κρυπτογραφικών ιδιοτήτων των υπό σχεδίαση συστημάτων και της σθεναρότητάς τους απέναντι σε διάφορες τακτικές κρυπτανάλυσης [40]. Σκοπός αυτού του μέρους της διατριβής είναι να παρέχει ένα νέο συμμετρικό κρυπτοσύστημα το οποίο βασίζεται σε περιοδικές τροχιές και ταυτόχρονα είναι σθεναρό σε διάφορες κρυπταναλυτικές επιθέσεις.

Τέλος, στο τρίτο μέρος της διατριβής θεωρούμε το πρόβλημα δημιουργίας πρωτοκόλλων για ασφαλή ηλεκτρονική συγκέντρωση δεδομένων τροποποιώντας πρωτόκολλα ηλεκτρονικών εκλογών [104, 107]. Η ηλεκτρονική συγκέντρωση δεδομένων είναι ιδιαίτερα σημαντική στη σύγχρονη εποχή, καθώς η συγκέντρωση και ανάλυση των δεδομένων που βρίσκονται οργανωμένα σε διάφορες βάσεις μπορούν να δώσουν πολύ σημαντικά καθολικά συμπεράσματα για την γνώση που αυτά εμπεριέχουν και τα οποία δεν θα μπορούσαν να ληφθούν από την επιμέρους μελέτη των δεδομένων. Στόχος της διατριβής στο μέρος αυτό είναι, τροποποιώντας πρωτόκολλα ηλεκτρονικών εκλογών που ικανοποιούν τα κριτήρια εξασφάλισης ιδιωτικότητας, να παρέχει ασφαλή πρωτόκολλα και για την ηλεκτρονική συγκέντρωση δεδομένων.

Συνοπτικά, τα προβλήματα που θεωρούμε στην παρούσα διατριβή είναι τα ακόλουθα: (α) η δυνατότητα εφαρμογής των μεθόδων υπολογιστικής νοημοσύνης σε προβλήματα κρυπτογραφίας και κρυπτανάλυσης, (β) η εφαρμογή μεθόδων αντίστροφης παρεμβολής για την μελέτη θεμελιωδών προβλημάτων κρυπτογραφίας, (γ) η δημιουργία σθεναρών συμμετρικών κρυπτοσυστημάτων με τη χρήση χαοτικών τροχιών και (δ) η δημιουργία πρωτοκόλλων ηλεκτρονικής συγκέντρωσης δεδομένων.

1.4 Συνεισφορά της παρούσας διδακτορικής διατριβής

Η παρούσα διατριβή συνεισφέρει σημαντικά σε όλα τα παραπάνω προβλήματα. Πιο αναλυτικά, αναφορικά με την δυνατότητα εφαρμογής των μεθόδων υπολογιστικής νοημοσύνης στην κρυπτολογία, αρχικά θεωρούμε τρία θεμελιώδη προβλήματα της κρυπτογραφίας και συγκεκριμένα, το πρόβλημα του διακριτού λογαρίθμου σε πεπερασμένα σώματα, το πρόβλημα της απεικόνισης Diffie-Hellman, και το πρόβλημα της παραγοντοποίησης ακεραίων και χρησιμοποιούμε δύο μεθόδους Εξελικτικού Υπολογισμού, τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με Σμήνος σωματιδίων, αλλά και Νευρωνικά Δίκτυα πρόσθιας

τροφοδότησης για την αντιμετώπισή τους. Λόγω της πολυπλοκότητας των κρυπτογραφικών αυτών προβλημάτων, ο μετασχηματισμός τους σε προβλήματα βελτιστοποίησης δεν παρέχει αρκετή πληροφορία για την δυναμική τους ώστε να μπορούν να επιλυθούν αποδοτικά από τις εξελικτικές μεθόδους. Το γεγονός αυτό υποδεικνύει ότι ένα πολύ κρίσιμο σημείο για την εφαρμογή και την αποδοτικότητα των μεθόδων της Υπολογιστικής Νοημοσύνης στην κρυπτολογία είναι η δημιουργία της αντικειμενικής συνάρτησης που μοντελοποιεί το υπό μελέτη πρόβλημα. Η συνάρτηση θα πρέπει να δημιουργείται με τρόπο που να εμπεριέχει όσο το δυνατόν περισσότερη πληροφορία για την δυναμική του προβλήματος και να παρέχει ουσιαστική αξιολόγηση της κάθε πιθανής λύσης. Ωστόσο, υπό αυτό το πρίσμα γίνεται σαφές ότι οι μέθοδοι Υπολογιστικής Νοημοσύνης μπορούν να αποτελέσουν ένα γρήγορο πρώτο μέτρο ελέγχου της σθεναρότητας νέων κρυπτογραφικών σχημάτων πριν την λεπτομερέστερη μελέτη τους με άλλες πιο σύνθετες μεθόδους κρυπτανάλυσης. Τα παραπάνω θέματα επισημάνθηκαν αργότερα και στην μελέτη [75].

Στη συνέχεια, θεωρούμε την κρυπτανάλυση κρυπτοσυστημάτων Feistel και πιο συγκεκριμένα του κρυπτοσυστήματος DES με την χρήση του Διαφοροεξελικτικού αλγορίθμου και της μεθόδου Βελτιστοποίησης με Σμήνος σωματιδίων. Η κρυπτανάλυση του DES των τεσσάρων και έξι γύρων βασίζεται κυρίως στην Διαφορική Κρυπτανάλυση, η οποία αποκαλύπτει ένα αρκετά μεγάλο πλήθος δυαδικών ψηφίων του κλειδιού. Και για τις δύο περιπτώσεις γύρων, τα υπολειπόμενα δυαδικά ψηφία του κλειδιού είναι 14 και δεν μπορούν να αποκαλυφθούν με την Διαφορική Κρυπτανάλυση οπότε χρησιμοποιείται είτε επίθεση εξαντλητικής αναζήτησης, είτε η χρήση επιπλέον χαρακτηριστικών τεσσάρων και έξι γύρων αντίστοιχα και ιδιαίτερα προσεκτική καταμέτρηση των ψηφίων των υποκλειδιών που προκύπτουν. Στην παρούσα μελέτη θεωρούμε το πρόβλημα εύρεσης των 14 δυαδικών ψηφίων του κλειδιού για τις δύο περιπτώσεις γύρων του DES, το μοντελοποιούμε ως πρόβλημα βελτιστοποίησης και το επιλύουμε με τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με Σμήνος σωματιδίων. Τα αποτελέσματα και για τις δύο περιπτώσεις είναι πολύ καλά και δείχνουν ότι οι μέθοδοι Υπολογιστικής Νοημοσύνης μπορούν να είναι αποτελεσματικές και αποδοτικές σε αυτή την περίπτωση και το κυριότερο ότι μπορούν να χρησιμοποιηθούν σε συνδυασμό με άλλες μεθόδους κρυπτανάλυσης για την αυτοματοποίηση κάποιων διαδικασιών που θα απαιτούσαν ανθρώπινη παρέμβαση.

Ένα ακόμα πρόβλημα κρυπτογραφίας στο οποίο μελετάμε την απόδοση των μεθόδων Υπολογιστικής Νοημοσύνης είναι η κατασκευή ισχυρών S-boxes. Τα S-boxes αποτελούν δομικό στοιχείο πολλών σύγχρονων κρυπτοσυστημάτων συμμετρικού κλειδιού και η επιλογή τους είναι πολύ σημαντική καθώς καθορίζει την ιδιότητα σύγχυσης (confusion) των αντίστοιχων κρυπτοσυστημάτων. Σε προηγούμενες μελέτες χρησιμοποιήθηκαν ευρετικές μέθοδοι όπως η μέθοδος ανάβασης λόφου, η μέθοδος της Προσομοιωμένης Ανόπτησης αλλά και οι Γενετικοί Αλγόριθμοι από τις μεθόδους Υπολογιστικής Νοημοσύνης για την επίλυση του συγκεκριμένου προβλήματος με αρκετά καλά αποτελέσματα. Στην παρούσα μελέτη θεωρούμε τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με Σμήνος σωματιδίων, που είναι οι νεότερες μέθοδοι Εξελικτικού Υπολογισμού και δεν χρειάζονται προεργασία για την ρύθμιση των παραμέτρων τους, για την δημιουργία ισχυρών S-boxes και συγκρίνουμε την απόδοσή τους με την αντίστοιχη των παραπάνω μεθόδων. Τα αποτελέσματα δείχνουν ότι οι προτεινόμενες μέθοδοι είναι αποτελεσματικές και αποδοτικές στην εύρεση βέλτιστων S-boxes και γενικά απαιτούν μικρότερο υπολογιστικό κόστος στις περισσότερες περιπτώσεις που δοκιμάζονται σε σχέση με τις άλλες μεθόδους.

Με την βοήθεια των Νευρωνικών Δικτύων μελετάμε επίσης το πρόβλημα υπολογισμού του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες. Η επίλυση του προβλήματος αυτού είναι αρκετά σημαντική για τις κρυπτογραφικές εφαρμογές καθώς οδηγεί στον υπολογισμό όλων των δυαδικών ψηφίων του διακριτού λογαρίθμου. Τα αποτελέσματα δείχνουν ότι για τρία διαφορετικά μήκη δυαδικών ψηφίων του διακριτού λογαρίθμου τα Νευρωνικά Δίκτυα μπορούν να προσαρμοστούν και να εκπαιδευτούν στα δεδομένα με αρκετά

υψηλό ποσοστό επιτυχίας. Μια ακόμα ενδιαφέρουσα παρατήρηση που προκύπτει αναφορικά με τα σύνολα εκπαίδευσης είναι ότι το δίκτυο παρουσιάζει συμπεριφορά συμπίεσης δεδομένων, καθώς είναι σε θέση να μάθει τα δεδομένα και να απαντά σωστά χρησιμοποιώντας λιγότερη μνήμη από αυτήν που απαιτείται για την αποθήκευση του αντίστοιχου συνόλου δεδομένων. Παρόλ΄ αυτά, τα δίκτυα δεν παρουσίασαν την ίδια καλή απόδοση και στα σύνολα ελέγχου, καθώς τα ποσοστά επιτυχίας τους σε αυτά είναι λίγο υψηλότερα από την τυχαία επιλογή.

Τέλος, σε αυτό το μέρος της διατριβής μελετήθηκε θεωρητικά η εφαρμογή των Πολυωνυμικών Δικτύων Ridge για τον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου και οδήγησε σε πόρισμα ύπαρξης Πολυωνυμικών Δικτύων Ridge που υλοποιούν τα πολυώνυμα υπολογισμού του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου και δόθηκε ένα φράγμα για την τάξη των Δικτύων Πι-Σίγμα που απαιτούνται για την κατασκευή αυτών των πολυωνυμικών δικτύων.

Η παρούσα διατριβή επίσης συνεισφέρει στη μελέτη του προβλήματος του διακριτού λογαρίθμου, της απεικόνισης Diffie-Hellman και του λογαρίθμου του Lucas με μεθόδους παρεμβολής. Συγκεκριμένα, στο δεύτερο μέρος της διατριβής μελετήθηκαν υπολογιστικά τα παραπάνω προβλήματα χρησιμοποιώντας τις μεθόδους αντίστροφης πολυωνυμικής παρεμβολής, Aitken και Neville. Οι μέθοδοι αυτές έχουν το πλεονέκτημα σε σχέση με τις κλασικές μεθόδους παρεμβολής ότι είναι κατασκευαστικές και παρέχουν την δυνατότητα προσθήκης νέων σημείων παρεμβολής επαναληπτικά με μικρό υπολογιστικό κόστος μέχρι να επιτευχθεί η απαιτούμενη ακρίβεια υπολογισμού. Τα αποτελέσματα που προκύπτουν δείχνουν ότι το συνολικό υπολογιστικό κόστος για την επίλυση των παραπάνω προβλημάτων με την προτεινόμενη μεθοδολογία παραμένει υψηλό όπως έχουν δείξει και οι μέχρι τώρα μελέτες, ωστόσο μια ενδιαφέρουσα παρατήρηση που προέκυψε είναι ότι ο βαθμός των τελικών πολυωνύμων που παρεμβάλλουν την λύση του προβλήματος είναι σχετικά χαμηλός.

Στη συνέχεια, η διατριβή συνεισφέρει στη δημιουργία ισχυρών κρυπτοσυστημάτων που βασίζονται στις ιδιότητες του χάους παρουσιάζοντας ένα νέο κρυπτοσύστημα συμμετρικού κλειδιού που βασίζεται σε περιοδικές τροχιές. Το προτεινόμενο κρυπτοσύστημα ελέγχεται ως προς την ποιότητα των κλειδιών του και ως προς την ασφάλειά του και παρέχονται επιπλέον τρεις τροποποιήσεις της βασικής του μορφής που αυξάνουν την σθεναρότητά του σε συνήθεις κρυπταναλυτικές επιθέσεις. Το κρυπτοσύστημα μελετάται επίσης ως προς την αποδοτικότητά του και δοκιμάζεται πειραματικά ως προς τον απαιτούμενο χρόνο κρυπτογράφησης και αποκρυπτογράφησης αλλά και την τελική μορφή που παρουσιάζουν τα κρυπτογραφήματά του.

Στο τελευταίο μέρος της διατριβής, προτείνονται δύο πρωτόκολλα ηλεκτρονικής συγκέντρωσης δεδομένων με ασφάλεια, τα οποία βασίζονται σε πρωτόκολλα ηλεκτρονικών εκλογών. Η δημιουργία πρωτοκόλλων συγκέντρωσης δεδομένων που εξασφαλίζουν την ιδιωτικότητα των φορέων που παρέχουν τα δεδομένα αυτά είναι πολύ σημαντική καθώς εξασφαλίζει την ανωνυμία των φορέων και την ιδιωτικότητά τους παρέχοντας ταυτόχρονα την δυνατότητα για ανακάλυψη γνώσης που ενυπάρχει στις επιμέρους βάσεις δεδομένων και η οποία δεν θα ήταν εύκολο να εξαχθεί από την ανεξάρτητη ανάλυση των πληροφοριών. Η διατριβή αυτή συνεισφέρει παρέχοντας δύο διαφορετικά πρωτόκολλα (με χρήση έμπιστου τρίτου φορέα και μη) που εξασφαλίζουν τις απαιτήσεις της πληρότητας, ιδιωτικότητας, νομιμότητας, αυθεντικοποίησης και επιβεβαίωσης των δεδομένων. Για κάθε μια περίπτωση, παρουσιάζεται ανάλυση της ασφάλειας του προτεινόμενου σχήματος αλλά και της υπολογιστικής πολυπλοκότητάς του.

1.5 Δομή της διδακτορικής διατριβής

Το υπόλοιπο της διατριβής οργανώνεται ως εξής: στο Μέρος Ι και στο Κεφάλαιο 2 παρουσιάζονται τα βασικά εισαγωγικά στοιχεία των μεθόδων Υπολογιστικής Νοημοσύνης και της χρήσης της στην κρυπτολογία μέχρι σήμερα. Στο Κεφάλαιο 3 μελετώνται τα προβλήματα κρυπτογραφίας και κρυπτανάλυσης με τις μεθόδους Εξελικτικού Υπολογισμού, ενώ στο Κεφάλαιο 4 ερευνάται η χρήση Τεχνητών Νευρωνικών Δικτύων για την κρυπτολογία.

Στο Μέρος ΙΙ της διατριβής και στο Κεφάλαιο 5 εφαρμόζονται οι μέθοδοι αντίστροφης πολυωνυμικής παρεμβολής στα προβλήματα του διακριτού λογαρίθμου, στην απεικόνιση Diffie-Hellman και στο πρόβλημα του Lucas, ενώ στο Κεφάλαιο 6 παρουσιάζεται το νέο προτεινόμενο συμμετρικό κρυπτοσύστημα που βασίζεται στις περιοδικές τροχιές.

Τέλος, στο Μέρος ΙΙΙ της διατριβής, στο Κεφάλαιο 7, αναλύονται τα δύο νέα πρωτόκολλα ασφαλούς ηλεκτρονικής συγκέντρωσης δεδομένων. Η διατριβή ολοκληρώνεται με το Κεφάλαιο 8 στο οποίο δίνονται τα συμπεράσματα από την μελέτη όλων των προβλημάτων που πραγματεύεται η διατριβή αλλά και οι προοπτικές που προκύπτουν για περαιτέρω έρευνα.

Μέρος I

Κρυπτογραφία και κρυπτανάλυση με μεθόδους Υπολογιστικής Νοημοσύνης

ΚΕΦΑΛΑΙΟ **2**

Εισαγωγή στην Υπολογιστική Νοημοσύνη

Το 1950 ο Alan Turing εξέφρασε την υπόθεση ότι μπορούν να αναπτυχθούν υπολογιστές που θα μιμούνται την λειτουργία του ανθρώπινου εγκεφάλου. Η υπόθεση αυτή υπονοεί ότι οποιαδήποτε λογική σκέψη μπορεί να πραγματοποιηθεί σε έναν αρκετά μεγάλο ντετερμινιστικό υπολογιστή. Η υπόθεση του Turing παραμένει ακόμα ένα όραμα, ωστόσο έχει εμπνεύσει τεράστια ερευνητική προσπάθεια προκειμένου οι υπολογιστές να παρουσιάσουν χαρακτηριστικά νοημοσύνης. Παρότι δεν υπάρχει κοινά αποδεκτός ορισμός, η *Υπολογιστική Νοημοσύνη* (ΥΝ) (Computational Intelligence) μπορεί να θεωρηθεί ως η μελέτη των προσαρμόσιμων μηχανισμών που κάνουν δυνατή την ευφυή συμπεριφορά ενός συστήματος σε ένα πολύπλοκο και μεταβαλλόμενο περιβάλλον [52, 54]. Οι μηχανισμοί αυτοί εκδηλώνουν την ικανότητα μάθησης ή προσαρμογής σε νέες καταστάσεις έτσι ώστε το σύστημα να θεωρείται ότι έχει μια ή περισσότερες ιδιότητες της λογικής σκέψης, όπως η γενίκευση, η αφαιρετική, η ανακάλυψη και η συσχέτιση. Για να κάνουν δυνατή την ευφυή συμπεριφορά, τα συστήματα ΥΝ συχνά σχεδιάζονται με τέτοιο τρόπο ώστε να μοντελοποιούν απόψεις της βιολογικής νοημοσύνης και της νοημοσύνης που παρουσιάζεται στη φύση.

Στη συνέχεια του Κεφαλαίου παρουσιάζονται οι δύο βασικότεροι κλάδοι της Υπολογιστικής Νοημοσύνης, ο Εξελικτικός Υπολογισμός και τα Τεχνητά Νευρωνικά Δίκτυα.

2.1 Εισαγωγή στις μεθόδους Εξελικτικού Υπολογισμού

Ο *Εξελικτικός Υπολογισμός* (ΕΥ) (Evolutionary Computation) αποτελεί τον κλάδο της Υπολογιστικής Νοημοσύνης που εμπνεύστηκε από τους εξελικτικούς μηχανισμούς που συναντούνται στη φύση, όπως η *φυσική επιλογή* και η *προσαρμόσιμη συμπεριφορά*, για το σχεδιασμό μεθόδων βελτιστοποίησης και ομαδοποίησης. Η έννοια της φυσικής επιλογής αναφέρεται στην επιβίωση του καλύτερου αντιπροσώπου κάθε είδους μέσω της αναπαραγωγής, καθώς ένας απόγονος πρέπει να διατηρήσει τα καλύτερα χαρακτηριστικά των γονέων του προκειμένου να επιβιώσει. Παραδείγματα του ΕΥ που ανήκουν σε αυτήν την κλάση είναι οι *Γενετικοί Αλγόριθμοι* (ΓΑ) (Genetic Algorithms) [10], ο *Γενετικός Προγραμματισμός* (ΓΠ) (Genetic Programming) [94], ο *Εξελικτικός Προγραμματισμός* (ΕΠ) (Evolutionary Programming) [59], οι *Εξελικτικές Στρατηγικές* (ΕΣ) (Evolution Strategies) [189] και ο *Διαφοροεξελικτικός Αλγόριθμος* (ΔΕ) (Differential Evolution Algorithm) [202]. Η κοινωνική και προσαρμόσιμη συμπεριφορά των οργανισμών που οργανώνονται σε ομάδες οδήγησε στην δημιουργία μιας δεύτερης κλάσης μεθόδων ΕΥ, τις μεθόδους *Νοημοσύνης Σμηνών* (ΝΣ) (Swarm Intelligence). Οι μέθοδοι αυτές μοντελοποιούν τις κοινωνικές διεργασίες των ζώντων οργανισμών που οργανώνονται σε ομάδες και δρουν για έναν κοινό σκοπό. Τυπικά παραδείγματα τέτοιων διεργασιών αποτελούν οι μηχανισμοί αναζήτησης τροφής στα σμήνη πτηνών, στα κοπάδια ψαριών και στις αποικίες μυρμηγκιών. Η μελέτη πολλών βιολογικών διεργασιών κοινωνικής και προσαρμόσιμης συμπεριφοράς οδήγησε στην άποψη ότι ο κοινωνικός μερισμός των πληροφοριών μεταξύ των ατόμων ενός πληθυσμού μπορεί να αποφέρει εξελικτικό πλεονέκτημα [52]. Παραδείγματα μεθόδων ΕΥ που ανήκουν σε αυτή την κλάση είναι η μέθοδος *Βελτιστοποίησης με Σμήνος Σωματιδίων* (ΒΣΣ) (Particle Swarm Optimization) [83] και η μέθοδος

Βελτιστοποίησης με Αποικίες Μυρμηγκιών (BAM) (Ant Colony Optimization) [48].

Κοινό χαρακτηριστικό όλων των μεθόδων ΕΥ είναι η χρήση ενός *πληθυσμού* (population) *ατόμων* (individuals), όπου κάθε άτομο αναπαριστά μια πιθανή λύση του προς επίλυση προβλήματος. Για τον εντοπισμό καλύτερων πιθανών λύσεων του προβλήματος, κάθε μέθοδος ΕΥ εξελίσσει τα άτομα του πληθυσμού αναπαράγοντάς τον, χρησιμοποιώντας κάποιους εξελικτικούς τελεστές, όπως για παράδειγμα ο *ανασυνδυασμός* (recombination), η *διασταύρωση* (crossover), η *μετάλλαξη* (mutation) και η *επιλογή* (selection). Για την αξιολόγηση των ατόμων του πληθυσμού κάθε μέθοδος χρειάζεται μια συνάρτηση αξιολόγησης, η οποία καλείται και *αντικειμενική συνάρτηση*, καθώς εξαρτάται άμεσα από το υπό μελέτη αντικείμενο (πρόβλημα). Οι μέθοδοι ΕΥ δεν απαιτούν την χρήση πληροφοριών των παραγώγων της αντικειμενικής συνάρτησης και μπορούν να εφαρμοστούν σε περιπτώσεις προβλημάτων με ασυνεχείς αντικειμενικές συναρτήσεις, ακόμα και σε μη συνεκτικούς χώρους αναζήτησης. Λόγω αυτών των χαρακτηριστικών, έχουν χρησιμοποιηθεί επιτυχώς σε πολλές περιπτώσεις πραγματικών εφαρμογών, όπως για παράδειγμα σε προβλήματα εξόρυξης δεδομένων, συνδυαστικής βελτιστοποίησης, διάγνωσης σφαλμάτων, ομαδοποίησης, χρονοπρογραμματισμού και προσέγγισης χρονοσειρών.

Στις ακόλουθες παραγράφους δίνουμε μια συνοπτική περιγραφή των διαφόρων μεθόδων Εξελικτικού Υπολογισμού.

2.1.1 Γενετικοί Αλγόριθμοι

Οι Γενετικοί Αλγόριθμοι (ΓΑ) προήλθαν από την προσπάθεια των βιολόγων το 1950 να προσομοιώσουν σε υπολογιστές γενετικά συστήματα που απαντώνται στη φύση. Ως δημιουργός του πεδίου των ΓΑ θεωρείται ο John Holland, ο οποίος το 1975 μελέτησε την ευφυΐα και την εκπαίδευση των μηχανών και ανέπτυξε τις ιδιότητες των ΓΑ στα τεχνητά συστήματα [72]. Τα συστήματα αυτά είχαν την ικανότητα να προσαρμόζονται στις αλλαγές του περιβάλλοντος και παρουσίασαν αυτοπροσαρμογή με την έννοια ότι μπορούσαν να προσαρμόσουν τις λειτουργίες τους σύμφωνα με την αλληλεπιδράσεις τους με το περιβάλλον. Μεταξύ των νεωτερισμών του Holland ήταν και η χρήση ενός πληθυσμού ατόμων για την διαδικασία της αναζήτησης αντί για τη συνήθη χρήση ενός μόνο σημείου αναζήτησης.

Τα βασικά χαρακτηριστικά των ΓΑ είναι η *φυσική εξέλιξη* και η *γενετική κληρονομικότητα*. Στη φυσική εξέλιξη κάθε βιολογικό είδος πρέπει να αναζητήσει τις πιο κατάλληλες προσαρμογές σε ένα πολύπλοκο και μεταβαλλόμενο περιβάλλον προκειμένου να επιβιώσει. Οι ΓΑ βασίζονται στην ιδέα ότι η γνώση και η εμπειρία που αποκτά κάθε είδος περνά μέσα στα χρωμοσώματα των μελών του. Για το λόγο αυτό, οι έννοιες και το λεξιλόγιο που χρησιμοποιούν οι ΓΑ προέρχονται από το πεδίο της γενετικής. Έτσι, τα άτομα του πληθυσμού καλούνται *χρωμοσώματα ή γονότυποι* (chromosomes). Κάθε χρωμόσωμα είναι ένα μέλος του πληθυσμού και αποτελείται από τμήματα που καλούνται *γονίδια* (genes). Καθένα από τα γονίδια ρυθμίζει την κληρονομικότητα ενός ή περισσοτέρων χαρακτηριστικών. Τα διαφορετικά χρωμοσώματα που μπορούν να καταλαμβάνουν ένα τμήμα του χρωμοσώματος καλούνται *αλληλόμορφα* (alleles).

Η διαδικασία εξέλιξης ενός πληθυσμού χρωμοσωμάτων αντιστοιχεί σε μια αναζήτηση στο χώρο των πιθανών λύσεων. Μια τέτοια αναζήτηση απαιτεί την εξισορρόπηση δύο αλληλοσυγκρουόμενων στόχων, την αξιοποίηση των καλύτερων λύσεων και την ευρεία εξερεύνηση του χώρου αναζήτησης. Η διαδικασία αναζήτησης στους ΓΑ γίνεται με τη χρήση δύο τελεστών, της *διασταύρωσης* και της *μετάλλαξης*. Οι τελεστές αυτοί επιδρούν στα χρωμοσώματα και τα μεταβάλλουν με στόχο την εύρεση καλύτερων χρωμοσωμάτων. Η επιλογή του νέου πληθυσμού γίνεται χρησιμοποιώντας ως κριτήριο την συνάρτηση αξιολόγησης. Η διαδικασία εξέλιξης του πληθυσμού επαναλαμβάνεται μέχρι να ικανοποιηθεί κάποιο κριτήριο τερματισμού του αλγορίθμου. Το κριτήριο τερματισμού μπορεί να είναι είτε ένα μέγιστο πλήθος γενεών, είτε η ακρίβεια εύρεσης της βέλτιστης λύσης. Στον Πίνακα 2.1 συνοψίζεται η δομή ενός κλασικού ΓΑ.

Πίνακας 2.1: Η εξελικτική διαδικασία ενός Γενετικού Αλγορίθμου.

1. Έστω $g = 0$.
2. Αρχικοποίησε έναν αρχικό πληθυσμό χρωμοσωμάτων C_g.
3. Υπολόγισε την τιμή της συνάρτησης αξιολόγησης για κάθε χρωμόσωμα $\vec{C}_{g,n} \in C_g$, του πληθυσμού.
4. Θέσε $g = g + 1$.
5. Επέλεξε τα χρωμοσώματα προς αναπαραγωγή (γονείς) από τον πληθυσμό C_{g-1}.
6. Διασταύρωσε τους επιλεγμένους γονείς μέσω του τελεστή της διασταύρωσης για τη δημιουργία των απογόνων O_g.
7. Μετάλλαξε μέσω του τελεστή μετάλλαξης τους απογόνους του πληθυσμού O_g.
8. Επέλεξε την νέα γενιά C_g από την προηγούμενη γενιά C_{g-1} και τους απογόνους O_g με βάση τον τελεστή της επιλογής.
9. Επανάλαβε την διαδικασία από το βήμα 3, μέχρι να ικανοποιηθεί το κριτήριο τερματισμού.

Οι ΓΑ συνήθως χρησιμοποιούν δυαδική αναπαράσταση για τα χρωμοσώματα του πληθυσμού. Ωστόσο, οι διάφορες μέθοδοι ΓΑ που έχουν αναπτυχθεί, μπορούν να εφαρμοστούν και με βάση οποιοδήποτε σύστημα αριθμών, συμπεριλαμβανομένου και αυτού των αριθμών κινητής υποδιαστολής [132].

Ο τελεστής της διασταύρωσης στους ΓΑ έχει ως σκοπό την παραγωγή απογόνου από δύο γονείς, ο οποίος επιλέγεται τελικά χρησιμοποιώντας τον τελεστή της επιλογής. Ωστόσο, η διασταύρωση πραγματοποιείται με βάση μια πιθανότητα που ονομάζεται *βαθμός διασταύρωσης* (crossover rate) $p_c \in [0, 1]$, και συνεπώς δεν παράγουν απόγονο όλες οι δυνατές ομάδες γονέων. Οι τρεις σημαντικότεροι τελεστές διασταύρωσης που εφαρμόζονται στους ΓΑ με δυαδική αναπαράσταση είναι η *ομοιόμορφη διασταύρωση* (uniform crossover), η *διασταύρωση ενός σημείου* (one-point crossover) και η *διασταύρωση δύο σημείων* (two-point crossover). Σε κάθε περίπτωση, επιλέγονται δύο γονείς και ανάλογα με το βαθμό διασταύρωσης υπόκεινται σε διασταύρωση κατά την οποία ανταλλάσσουν τμήματα των δυαδικών συμβολοσειρών τους, παράγοντας δύο συμπληρωματικούς απογόνους. Στην περίπτωση της ομοιόμορφης διασταύρωσης, κάθε ψηφίο (bit) της συμβολοσειράς των απογόνων επιλέγεται μέσω της ανταλλαγής των αντίστοιχων ψηφίων των δύο γονέων με βάση μια ομοιόμορφη πιθανότητα. Στην περίπτωση της διασταύρωσης ενός σημείου επιλέγεται τυχαία ένα ψηφίο στο χρωμόσωμα των γονέων και οι απόγονοι προκύπτουν από την ανταλλαγή των ψηφίων των γονέων από το συγκεκριμένο ψηφίο και πέρα. Τέλος, στην περίπτωση της διασταύρωσης δύο σημείων, επιλέγονται δύο ψηφία στο χρωμόσωμα των γονέων και οι γονείς ανταλλάσσουν τα τμήματα των χρωμοσωμάτων τους μεταξύ των δύο αυτών ψηφίων. Στον Πίνακα 2.2 απεικονίζονται παραδείγματα των τριών τελεστών διασταύρωσης.

Ο σκοπός του *τελεστή μετάλλαξης* είναι η δημιουργία νέου γενετικού υλικού σε ένα υπάρχον χρωμόσωμα ώστε να προσθέσει ποικιλότητα στα γενετικά χαρακτηριστικά του πληθυσμού. Επίσης, σε συνδυασμό με τον τελεστή της διασταύρωσης φροντίζει ώστε όλες οι πιθανές αλληλόμορφες τιμές των γονιδίων να είναι εφικτές κατά την αναζήτηση. Πιο συγκεκριμένα, ο

Πίνακας 2.2: Τελεστές διασταύρωσης των Γενετικών Αλγορίθμων.

Γονέας 1	1010010001	101001 | 0001	101 | 001 | 0001
Γονέας 2	0101101101	010110 | 1101	010 | 110 | 1101
	↓	↓	↓
Απόγονος 1	0110100101	101001 1101	101 110 0001
Απόγονος 2	1001011001	010110 0001	010 001 1101
	ομοιόμορφη διασταύρωση	**διασταύρωση ενός σημείου**	**διασταύρωση δύο σημείων**

τελεστής της μετάλλαξης μεταβάλλει ένα ή περισσότερα ψηφία του χρωμοσώματος, σύμφωνα με μια πιθανότητα που καλείται *βαθμός μετάλλαξης* (mutation rate) p_m. Συνήθως χρησιμοποιείται μικρή τιμή για τον βαθμό μετάλλαξης ώστε να μην διαταράσσονται πολύ τα καλά χρωμοσώματα. Ωστόσο, ερευνητικές μελέτες έχουν δείξει ότι η αρχική θεώρηση του βαθμού μετάλλαξης σε μια μεγάλη τιμή και η σταδιακή εκθετική μείωση της τιμής του αναφορικά με το πλήθος των γενεών, βελτιώνει την ταχύτητα σύγκλισης της μεθόδου και την ακρίβειά της [54].

Για την επιλογή του νέου πληθυσμού σε κάθε γενεά των ΓΑ έχουν αναπτυχθεί διάφορες τεχνικές [54]. Μια από τις πιο σημαντικές τεχνικές επιλογής είναι και ο *ελιτισμός* (elitism). Κατά την ελιτιστική τεχνική η επιλογή ενός χρωμοσώματος γίνεται με βάση την συναρτησιακή του τιμή με σκοπό την μεταβίβαση των καλύτερων χρωμοσωμάτων στη νέα γενεά. Η στρατηγική αυτή δεν εξασφαλίζει πάντα την ισορροπία μεταξύ εξαντλητικής αναζήτησης και αποδοτικότητας του ΓΑ, καθώς ενέχει τον κίνδυνο της γρήγορης κυριαρχίας του πληθυσμού από ένα χρωμόσωμα που δεν είναι απαραίτητα η καθολικά βέλτιστη λύση, παρουσιάζει όμως ενδιαφέρον σε περιπτώσεις τοπικής αναζήτησης καθώς μπορεί να βελτιώσει αξιοσημείωτα την απόδοση του ΓΑ. Εναλλακτικά, έχουν προταθεί και άλλες τεχνικές επιλογής που χαρακτηρίζονται από μεγαλύτερη διασπορά του πληθυσμού και χαμηλούς ρυθμούς σύγκλισης των ΓΑ, όπως είναι η *τυχαία επιλογή* (random selection), η *αναλογική επιλογή* (proportional selection) και η τεχνική επιλογής του νέου πληθυσμού μόνο μεταξύ των απογόνων [54, 133].

Οι ΓΑ έχουν εφαρμοστεί με επιτυχία μεταξύ των άλλων και σε προβλήματα Βελτιστοποίησης από τον τομέα της εφαρμοσμένης μηχανικής και του μηχανολογικού σχεδιασμού, στο χρονοπρογραμματισμό, σε προβλήματα μεταφορών όπως το πρόβλημα του πλανόδιου πωλητή, σε προβλήματα βέλτιστου ελέγχου και ρομποτικής, καθώς και στην οικονομία [10, 13, 42, 59, 66, 133, 206, 207]

2.1.2 Γενετικός Προγραμματισμός

Ο *Γενετικός Προγραμματισμός* (ΓΠ) αναπτύχθηκε σχετικά πρόσφατα από τον Koza [94] και όμοια με τους Γενετικούς Αλγορίθμους, επικεντρώνεται στην εξέλιξη των γονότυπων. Η βασική τους διαφορά είναι στον τρόπο αναπαράστασης που χρησιμοποιούν. Ενώ οι ΓΑ χρησιμοποιούν δυαδική αναπαράσταση, ο ΓΠ θεωρεί ως άτομα (χρωμοσώματα) εκτελέσιμα υπολογιστικά προγράμματα τα οποία αναπαριστά χρησιμοποιώντας δενδροειδή δομή. Για το σκοπό αυτό ορίζεται μια «γραμματική» η οποία ανταποκρίνεται με ακρίβεια στο προς επίλυση πρόβλημα. Στη γραμματική αυτή περιλαμβάνεται ένα σύνολο συναρτήσεων και ένα σύνολο όρων. Το σύνολο όρων καθορίζει όλες τις μεταβλητές και σταθερές, ενώ το σύνολο συναρτήσεων περιέχει όλες τις συναρτήσεις που μπορούν να εφαρμοστούν στα στοιχεία του συνόλου όρων. Τα στοιχεία του συνόλου όρων αποτελούν τα φύλλα του δένδρου και τα στοιχεία του συνόλου συναρτήσεων αποτελούν τους υπόλοιπους κόμβους του δένδρου.

Κάθε άτομο στον πληθυσμό του ΓΠ αναπαριστά ένα πρόγραμμα, το οποίο είναι ένα στοιχείο

του χώρου προγραμμάτων. Ο χώρος προγραμμάτων αποτελείται από όλα τα εφικτά προγράμματα που προκύπτουν από τη δοθείσα γραμματική. Σκοπός του ΓΠ είναι η αναζήτηση ενός προγράμματος από το χώρο προγραμμάτων που δίνει την καλύτερη προσέγγιση στην πραγματική λύση του προβλήματος.

Τα δένδρα που αναπαριστούν τα άτομα του πληθυσμού μπορούν να είναι σταθερού ή μεταβλητού μεγέθους. Συνήθως χρησιμοποιούνται δένδρα μεταβλητού μεγέθους, για τα οποία δίνεται περιορισμός του μέγιστου βάθους. Επίσης μπορούν να χρησιμοποιηθούν σχήματα όπου το μέγιστο βάθος αυξάνεται ανάλογα με τον αριθμό των γενεών.

Η αρχικοποίηση του πληθυσμού στο ΓΠ γίνεται τυχαία υπό τους περιορισμούς του μέγιστου βάθους και των εννοιών όπως αυτές εκφράζονται από τη δοθείσα γραμματική. Για κάθε άτομο επιλέγεται τυχαία μια ρίζα από το σύνολο των συναρτήσεων. Ο αριθμός των κλάδων της ρίζας και κάθε άλλος κόμβος εκτός των φύλλων καθορίζονται από τον αριθμό των παραμέτρων της επιλεγμένης συνάρτησης. Για κάθε κόμβο, εκτός της ρίζας, ο αλγόριθμος αρχικοποίησης επιλέγει τυχαία ένα στοιχείο είτε από το σύνολο συναρτήσεων είτε από το σύνολο όρων. Αν επιλεγεί στοιχείο από το σύνολο όρων τότε ο κόμβος γίνεται φύλλο και δεν λαμβάνεται υπ' όψιν για περαιτέρω ανάπτυξη.

Η συνάρτηση αξιολόγησης στον ΓΠ εξαρτάται από το προς επίλυση πρόβλημα και εμπεριέχει την αξιολόγηση κάθε προβλήματος από το χώρο - στόχο. Αυτό συνήθως απαιτεί την αξιολόγηση κάθε ατόμου για ένα σύνολο περιπτώσεων και ο μέσος όρος της απόδοσής του επί αυτού του συνόλου χρησιμοποιείται ως μέτρο απόδοσης. Τα μη αποδοτικά προγράμματα γίνονται ανενεργά, ενώ τα καλύτερα «αναπαράγονται» με τη βοήθεια τελεστών.

Οι τελεστές που εφαρμόζονται στο ΓΠ είναι η *διασταύρωση*, η *μετάλλαξη* και η *επιλογή* και χρησιμοποιούνται όπως και στους ΓΑ. Αναφορικά με την διασταύρωση υπάρχουν δύο διαφορετικοί τρόποι δημιουργίας απογόνων οι οποίοι διαφέρουν στον αριθμό των απογόνων που παράγονται. Ο πρώτος τρόπος είναι η **δημιουργία ενός απογόνου** κατά την οποία επιλέγεται τυχαία ένας κόμβος από κάθε γονέα και η διασταύρωση επιτελείται αντικαθιστώντας το υποδένδρο του ενός γονέα από το αντίστοιχο του άλλου γονέα. Ο δεύτερος τρόπος είναι η **δημιουργία δύο απογόνων** κατά την οποία επιλέγεται τυχαία ένας κόμβος από κάθε γονέα και τα αντίστοιχα υποδένδρα αντιμετατίθονται για τη δημιουργία δύο απογόνων.

Υπάρχουν διάφοροι τελεστές μετάλλαξης στο ΓΠ. Οι πιο συνήθεις είναι οι ακόλουθοι.

(α) **Μετάλλαξη κόμβου συνάρτησης:** επιλέγεται τυχαία ένας κόμβος συνάρτησης και αντικαθίσταται από έναν κόμβο της ίδιας τάξης που επιλέγεται τυχαία από το σύνολο συναρτήσεων.

(β) **Μετάλλαξη κόμβου όρων:** επιλέγεται τυχαία ένας κόμβος - φύλλο και αντικαθίσταται από έναν νέο όρο τυχαία επιλεγμένο από το σύνολο όρων.

(γ) **Μετάλλαξη αντιμετάθεσης (swap):** επιλέγεται τυχαία ένας κόμβος συνάρτησης και τα ορίσματα του κόμβου αντιμετατίθονται.

(δ) **Μετάλλαξη αύξησης (grow):** επιλέγεται τυχαία ένας οποιοσδήποτε κόμβος και αντικαθίσταται από ένα τυχαία δημιουργημένο υποδένδρο. Το νέο υποδένδρο περιορίζεται από ένα προκαθορισμένο βάθος.

(ε) **Gaussian μετάλλαξη:** ένας κόμβος - φύλλο (όρος) που αναπαριστά μια σταθερά, επιλέγεται τυχαία και μεταλλάσσεται προσθέτοντας μια Gaussian τυχαία τιμή σε αυτόν.

(στ) **Μετάλλαξη κλάδου (trunc):** επιλέγεται τυχαία ένας κόμβος συνάρτησης και αντικαθίσταται από έναν τυχαίο κόμβο όρου. Αυτός ο τελεστής μετάλλαξης επιτελεί «κλάδεμα» (pruning) του δένδρου.

Τα προς μετάλλαξη άτομα επιλέγονται τυχαία σύμφωνα με μια πιθανότητα μετάλλαξης p_m. Επιπρόσθετα, κόμβοι μέσα στο επιλεγμένο δένδρο μεταλλάσσονται σύμφωνα με μια πιθανότητα

p_n. Όσο μεγαλύτερη είναι η πιθανότητα p_n τόσο η γενετική δομή του ατόμου μεταλλάσσεται. Αναφορικά με την πιθανότητα p_m, όσο μεγαλύτερη είναι τόσο περισσότερα άτομα υπόκεινται σε μετάλλαξη.

Σε μία υλοποίηση ΓΠ μπορούν να επιλεγούν τυχαία και να χρησιμοποιηθούν ένας ή περισσότεροι τελεστές μετάλλαξης. Στη δεύτερη περίπτωση οι τελεστές μπορούν να εφαρμοστούν διαδοχικά.

2.1.3 Εξελικτικός Προγραμματισμός

Παράλληλα με τη δημιουργία των ΓΑ, αναπτύχθηκε από τον Larry Fogel το πεδίο του Εξελικτικού Προγραμματισμού [60]. Ο *Εξελικτικός Προγραμματισμός* (ΕΠ) διαφέρει ουσιαστικά από τους Γενετικούς Αλγορίθμους και τον Γενετικό Προγραμματισμό καθώς επικεντρώνεται στην ανάπτυξη μοντέλων που βασίζονται στην συμπεριφορά και όχι σε γενετικά μοντέλα. Δηλαδή, ο ΕΠ προήλθε από την προσομοίωση της προσαρμόσιμης συμπεριφοράς στην εξέλιξη και για το λόγο αυτό συσχετίζεται με την εξέλιξη του *φαινοτύπου*, του συνόλου δηλαδή των χαρακτηριστικών που παρατηρούνται εξωτερικά και προκύπτουν από την αλληλεπίδραση με το περιβάλλον. Η διαδικασία της εξέλιξης αφορά στην εύρεση του συνόλου των βέλτιστων συμπεριφορών από το χώρο των παρατηρούμενων συμπεριφορών. Για το σκοπό αυτό, η συνάρτηση αξιολόγησης μετρά το «σφάλμα συμπεριφοράς» ενός ατόμου αναφορικά με το περιβάλλον του ατόμου αυτού.

Επίσης, ο ΕΠ διαφέρει από τους Γενετικούς Αλγορίθμους και τον Γενετικό Προγραμματισμό στο ότι δεν εφαρμόζεται ο τελεστής της διασταύρωσης. Χρησιμοποιείται μόνο η μετάλλαξη για την δημιουργία νέου πληθυσμού. Στον Πίνακα 2.3 παρουσιάζεται με ψευδοκώδικα η γενική μορφή του ΕΠ.

Πίνακας 2.3: Η γενική μορφή του Εξελικτικού Προγραμματισμού.

1. Θέσε τον αριθμό γενεών $g = 0$.
2. Αρχικοποίησε έναν αρχικό πληθυσμό $C_g = \{\vec{C}_{g,n} | n = 1, \ldots, N\}$, όπου N είναι ο συνολικός αριθμός ατόμων του πληθυσμού.
3. Υπολόγισε την τιμή της συνάρτησης αξιολόγησης για κάθε άτομο $\vec{C}_{g,n} \in C_g$ του πληθυσμού.
4. Μετάλλαξε κάθε άτομο $\vec{C}_{g,n}$ για τη δημιουργία απογόνου $\vec{O}_{g,n}$.
5. Επέλεξε το νέο πληθυσμό $C_{g+1,n}$ από τους πληθυσμούς C_g και O_g.
6. Θέσε $g = g + 1$.
7. Επανάλαβε την διαδικασία από το βήμα 3, μέχρι να ικανοποιηθεί το κριτήριο τερματισμού.

Η μετάλλαξη εφαρμόζεται σε κάθε άτομο σύμφωνα με συγκεκριμένη πιθανότητα p_m. Ο τελεστής μετάλλαξης που χρησιμοποιείται εξαρτάται από το προς επίλυση πρόβλημα. Οι απόγονοι που παράγονται μέσω της μετάλλαξης ανταγωνίζονται τα άτομα - γονείς για επιβίωση στην επόμενη γενεά. Μετά την μετάλλαξη ο νέος πληθυσμός επιλέγεται με έναν από τους ακόλουθους τρόπους:

1. Όλα τα άτομα, γονείς και απόγονοι, έχουν την ίδια πιθανότητα να επιλεγούν.

2. Ένας ελιτιστικός μηχανισμός χρησιμοποιείται για τη μεταφορά ενός συνόλου από τους καλύτερους γονείς στην επόμενη γενεά. Το υπόλοιπο του πληθυσμού επιλέγεται από το υπόλοιπο των γονέων και τους απογόνους.

3. Αρχικά αποκλείονται οι χειρότεροι γονείς και απόγονοι από την διαδικασία επιλογής. Στη συνέχεια επιλέγεται ο νέος πληθυσμός από τα υπόλοιπα "καλά" άτομα. Η διαδικασία αυτή εξασφαλίζει ότι τα αδύναμα άτομα δεν θα επιβιώσουν στην επόμενη γενεά.

4. Η επιλογή γίνεται με συνδυασμό των δύο προηγούμενων στρατηγικών.

Ο ΕΠ μπορεί να αντιμετωπίσει προβλήματα Βελτιστοποίησης και ομαδοποίησης με εφαρμογές σε διάφορα επιστημονικά πεδία, όπως για παράδειγμα η οικονομία [58, 59].

2.1.4 Εξελικτικές Στρατηγικές

Οι *Εξελικτικές Στρατηγικές* (ΕΣ) αναπτύχθηκαν το 1960 από τον Rechenberg [174], μελετήθηκαν περαιτέρω από τον Schwefel [187, 189] και βασίζονται στην ιδέα «εξέλιξη της εξέλιξης». Στις ΕΣ θεωρείται και η γονοτυπική και η φαινοτυπική εξέλιξη, ωστόσο δίνεται έμφαση στη φαινοτυπική συμπεριφορά των ατόμων. Κάθε άτομο αναπαριστάται από τα γενετικά δομικά στοιχεία του και ένα σύνολο παραμέτρων στρατηγικής (strategy parameters) που μοντελοποιούν την συμπεριφορά του ατόμου στο περιβάλλον του. Η εξέλιξη, στη συνέχεια, αποτελείται από ανάπτυξη και των γενετικών χαρακτηριστικών και των παραμέτρων στρατηγικής, κατά την οποία η εξέλιξη των γενετικών χαρακτηριστικών ελέγχεται από τις παραμέτρους στρατηγικής. Μια επιπρόσθετη διαφορά μεταξύ των ΕΣ και των άλλων μεθόδων Εξελικτικού Υπολογισμού έγκειται στο ότι οι αλλαγές που οφείλονται στην μετάλλαξη γίνονται αποδεκτές μόνο στην περίπτωση επιτυχίας αναφορικά με την απόδοση του ατόμου. Δηλαδή, τα μεταλλαγμένα άτομα γίνονται δεκτά μόνο αν η μετάλλαξη επιφέρει βελτίωση στην αξιολόγηση του ατόμου. Επίσης, ενδιαφέρον σημείο των ΕΣ είναι ότι οι απόγονοι μπορούν να δημιουργηθούν από περισσότερους από δύο γονείς. Στον Πίνακα 2.4 δίνεται ο γενικός αλγόριθμος των Εξελικτικών Στρατηγικών.

Η αναπαράσταση κάθε ατόμου του πληθυσμού αποτελείται από δύο τύπους πληροφοριών, τον γονοτυπικό και τον φαινοτυπικό. Κάθε άτομο αναπαριστάται από μία δυάδα $C_n = (\vec{G}_n, S_n)$, όπου $\vec{G}_n$ αναπαριστά το γενετικό υλικό και το S_n αναπαριστά τις παραμέτρους στρατηγικής (δηλαδή τα χαρακτηριστικά συμπεριφοράς). Οι παράμετροι στρατηγικής περιλαμβάνουν κυρίως πληροφορίες για τη μετάλλαξη και αποσκοπούν στην εφαρμογή της με αυτοπροσαρμοζόμενο μέγεθος βήματος. Οι παράμετροι στρατηγικής που έχουν χρησιμοποιηθεί στις ΕΣ περιλαμβάνουν τυπικές αποκλίσεις του μεγέθους βήματος της μετάλλαξης και γωνίες στροφής:

(α) Μια τυπική απόκλιση συσχετιζόμενη με κάθε άτομο C_n, το οποίο αναπαριστάται ως $C_n = (\vec{G}_n, \sigma_n) \in \mathbb{R}^I \times \mathbb{R}_+$, με $\vec{G}_n \in \mathbb{R}^I$ (δηλαδή το άτομο έχει I γενετικές μεταβλητές) και $\sigma_n \in \mathbb{R}_+$ (μια θετική βαθμωτή τιμή).

(β) Μια τυπική απόκλιση για κάθε γενετική μεταβλητή ενός ατόμου και γωνίες στροφής σχετιζόμενες με κάθε άτομο, αναπαρίστανται ως $C_n = (\vec{G}_n, \vec{\sigma}_n, \vec{\omega}_n) \in \mathbb{R}^I \times \mathbb{R}_+^I \times \mathbb{R}_+^{I(I-1)/2}$, όπου $\vec{\omega}$ είναι ένα διάνυσμα αποτελούμενο από $I(I-1)/2$ γωνίες στροφής με $\omega_{nk} \in (0, 2\pi]$.

Με την ανάθεση μιας τυπικής απόκλισης σ_{ni} σε κάθε γενετική μεταβλητή G_{ni}, οι προτιμώμενες κατευθύνσεις αναζήτησης μπορούν να βρίσκονται μόνο πάνω στους άξονες του συστήματος συντεταγμένων. Ωστόσο, γενικά η καλύτερη κατεύθυνση αναζήτησης δεν βρίσκεται σε αυτούς τους άξονες. Για το λόγο αυτό, η βέλτιστη σύγκλιση επιτυγχάνεται μόνο τυχαία όταν κατάλληλες μεταλλάξεις συσχετιστούν. Οι συσχετιζόμενες μεταλλάξεις πραγματοποιούνται χρησιμοποιώντας γωνίες στροφής αποφεύγοντας

Πίνακας 2.4: Ο γενικός αλγόριθμος των Εξελικτικών Στρατηγικών.

1. Θέσε τον αριθμό γενεών $g = 0$.
2. Αρχικοποίησε έναν αρχικό πληθυσμό $C_g = \{\vec{C}_{g,n} \,|n = 1, \ldots, \mu\}$, όπου μ είναι ο συνολικός αριθμός των ατόμων - γονέων.
3. Υπολόγισε την απόδοση κάθε ατόμου του πληθυσμού σύμφωνα με την συνάρτηση αξιολόγησης f.
4. Για $l = 1, \ldots, \lambda$, όπου λ ο αριθμός των απογόνων, κάνε τα ακόλουθα:
   α. διάλεξε τυχαία ρ γονείς, όπου $\rho \geqslant 2 \geqslant \mu$,
   β. διασταύρωσε τα γενετικά δομικά στοιχεία και τις παραμέτρους στρατηγικής των ρ γονέων,
   γ. μετάλλαξε το γενετικό υλικό και τις παραμέτρους στρατηγικής των απογόνων που προέκυψαν από την διασταύρωση,
   δ. υπολόγισε την απόδοση των απογόνων.
5. Επέλεξε τα μ καλύτερα άτομα, από τον πληθυσμό των λ απογόνων ή από τον πληθυσμό των μ γονέων και των λ απογόνων, για τη δημιουργία της επόμενης γενεάς.
6. Θέσε $g = g + 1$.
7. Επανάλαβε την διαδικασία από το βήμα 4, μέχρι να ικανοποιηθεί το κριτήριο τερματισμού.

έτσι τις απότομες αλλαγές κατεύθυνσης της τροχιάς αναζήτησης πάνω στην κλίση της αντικειμενικής συνάρτησης [188].

Οι γωνίες στροφής χρησιμοποιούνται για την αναπαράσταση των συνδιασπορών μεταξύ των I γενετικών μεταβλητών στο γενετικό διάνυσμα $\vec{G}_n$. Καθώς το μητρώο συνδιασπορών είναι συμμετρικό, μπορεί να χρησιμοποιηθεί ένα διάνυσμα για την αναπαράσταση των γωνιών στροφής αντί για ένα μητρώο. Οι γωνίες στροφής χρησιμοποιούνται για τον υπολογισμό ενός ορθογώνιου μητρώου στροφής, $T(\vec{\omega}_n)$, ως

$$T(\vec{\omega}_n) = \prod_{i=1}^{I-1} \prod_{j=i+1}^{I} R_{ij}(\vec{\omega}_n), \tag{2.1}$$

που είναι το γινόμενο των $I(I-1)/2$ μητρώων στροφής. Κάθε μητρώο στροφής $R_{ij}(\vec{\omega}_n)$ είναι ένα μητρώο με στοιχεία $r_{ii} = \cos(\omega_{nk})$ και $r_{ij} = -r_{ji} = -\sin(\omega_{nk})$, με $k = 1 \Leftrightarrow (i = 1, j = 2)$, $k = 2 \Leftrightarrow (i = 1, j = 3)$, κ.ο.κ.

Η τυπική απόκλιση και το ορθογώνιο μητρώο στροφής χρησιμοποιούνται για τον καθορισμό του μεγέθους βήματος της μετάλλαξης.

Ο αρχικός πληθυσμός κατασκευάζεται τυχαία, με τυχαία αρχικοποίηση του γενετικού υλικού και των παραμέτρων στρατηγικής.

Αναφορικά με τον τελεστή της διασταύρωσης, αυτός εφαρμόζεται στις γενετικές μεταβλητές αλλά και στις παραμέτρους στρατηγικής αλλά με τρόπο διαφορετικό από τον αντίστοιχο σε

άλλες μεθόδους ΕΥ. Πιο συγκεκριμένα, υπάρχουν δύο βασικές τεχνικές διασταύρωσης στις ΕΣ και είναι οι ακόλουθες.

(α) Η τοπική διασταύρωση, όπου ένας απόγονος δημιουργείται από δύο γονείς χρησιμοποιώντας τυχαία επιλεγμένες συνιστώσες των γονέων.

(β) Η ολική διασταύρωση, όπου ολόκληρος ο πληθυσμός των ατόμων λαμβάνει μέρος στη δημιουργία ενός απογόνου. Οι συνιστώσες επιλέγονται τυχαία από τυχαία επιλεγμένα άτομα για τη δημιουργία του απογόνου.

Και στις δύο περιπτώσεις, ο *ανασυνδυασμός* των γενετικών και των παραμέτρων στρατηγικής γίνεται με

(α) διακριτό ανασυνδυασμό, όπου τα πραγματικά αλληλόμορφα των γονέων χρησιμοποιούνται για την κατασκευή απογόνου, ή με

(β) μέσο ανασυνδυασμό, όπου τα αλληλόμορφα του απογόνου είναι ο αριθμητικός μέσος των αντίστοιχων γονιδίων των γονέων (στον μέσο ανασυνδυασμό χρησιμοποιείται αναπαράσταση κινητής υποδιαστολής).

Αναφορικά με τον τελεστή της μετάλλαξης στις ΕΣ, όπως και στον ΕΠ, χρησιμοποιείται Gaussian θόρυβος με μέση τιμή μηδέν για τον καθορισμό της εμβέλειας της μετάλλαξης. Η μετάλλαξη εφαρμόζεται στις γενετικές μεταβλητές αλλά και στις παραμέτρους στρατηγικής. Το σχήμα μετάλλαξης εξαρτάται από τον τύπο των παραμέτρων στρατηγικής που χρησιμοποιείται.

Για την αναπαράσταση $C_n = (\vec{G}_n, \sigma_n)$, στην οποία δεν περιλαμβάνεται πληροφορία συσχέτισης, η διαδικασία της μετάλλαξης εφαρμόζεται σε δύο στάδια:

1. Μετάλλαξε την τυπική απόκλιση $\sigma_{g,n}$ για την τρέχουσα γενεά g και κάθε άτομο C_n. Υπάρχουν διάφορες μέθοδοι μετάλλαξης των αποκλίσεων, εκ των οποίων ο κανόνας επιτυχίας του 1/5 του Rechenberg ήταν η πρώτη ευρετική μέθοδος που χρησιμοποιήθηκε [174]. Ο κανόνας αυτός αναφέρει ότι το ποσοστό επιτυχών μεταλλάξεων πρέπει να είναι 1/5. Επομένως, αν το ποσοστό είναι μεγαλύτερο από 1/5, τότε η απόκλιση πρέπει να αυξηθεί, αλλιώς η απόκλιση πρέπει να μειωθεί. Δηλαδή,

$$\sigma_{g+t,n} = \begin{cases} c_d \sigma_{g,n}, & \text{αν } s_g < 1/5, \\ c_i \sigma_{g,n}, & \text{αν } s_g > 1/5, \\ \sigma_{g,n}, & \text{αν } s_g = 1/5, \end{cases}$$

   όπου s_g είναι η συχνότητα επιτυχών μεταλλάξεων επί των t επαναλήψεων, και c_d, c_i σταθερές. Μια μετάλλαξη είναι επιτυχής αν έχει ως αποτέλεσμα απόγονο με καλύτερη απόδοση από τον γονέα.

   Ο Schwefel πρότεινε την ακόλουθη στρατηγική μετάλλαξης για τυπικές αποκλίσεις [187]:

$$\sigma_{g+1,n} = \sigma_{g,n} e^{\tau \xi_\tau},$$

   όπου $\tau = \sqrt{I}$ και $\xi_\tau \sim N(0,1)$.

   Μια διαφορετική στρατηγική προτάθηκε από τον Fogel [58] και είναι η εξής:

$$\sigma_{g+1,n} = \sigma_{g,n}(1 + \tau \xi_\tau).$$

2. Μετάλλαξε το γενετικό υλικό $\vec{G}_{g,n}$ κάθε ατόμου ως εξής:

$$\vec{G}_{g+1,n} = \vec{G}_{g,n} + \vec{\sigma}_{g+1,n} \vec{\xi},$$

   όπου $\vec{\xi} \in \mathbb{R}_+^I$, με συνιστώσες $\xi_i \sim N(0,1)$.

Για την αναπαράσταση $C_n = (\vec{G}_n, \vec{\sigma}_n, \omega_n)$, όπου χρησιμοποιούνται και οι τυπικές αποκλίσεις και πληροφορίες συσχέτισης, η μετάλλαξη εφαρμόζεται στα ακόλουθα τρία στάδια.

1. Μετάλλαξε τις γωνίες στροφής $\omega_{g,nk}$ για κάθε άτομο C_n:

$$\omega_{g+1,nk} = (\omega_{g,nk} + \phi\xi_{\omega,k}) \mod 2\pi,$$

όπου $\phi > 0$ και $\xi_{\omega,ki} \sim N(0,1)$, για $k = 1, \ldots, I(I-1)/2$.

2. Έστω ότι το διάνυσμα $\vec{\sigma}_{g,n} \in \mathbb{R}_+^I$ αναπαριστά τις τυπικές αποκλίσεις όλων των γονιδίων, δηλαδή $\vec{\sigma}_{g,n} = (\sigma_{g,n1}, \ldots, \sigma_{g,nI})$. Έστω $S(\sigma) = diag(\sigma_{g,n1}, \ldots, \sigma_{g,nI})$ το διαγώνιο μητρώο που αναπαριστά αυτές τις αποκλίσεις. Τότε, κάθε τυπική απόκλιση μεταλλάσσεται ως

$$\sigma_{g+1,ni} = \sigma_{g,ni} e^{(\tau\xi_\tau + \eta\xi_{\sigma,i})},$$

όπου $\tau, \eta \in \mathbb{R}_+$ και $\xi_{\sigma,i} \sim N(0,1)$.

3. Μετάλλαξε τα γονίδια, χρησιμοποιώντας την ακόλουθη σχέση

$$G_{g+1,n} = G_{g,n} + T(\omega_{g+1,n})S(\sigma_{g+1,n})\xi,$$

όπου $T(\omega_{g,n})$ είναι το ορθογώνιο μητρώο στροφής που υπολογίζεται από την Σχέση 2.1 και ξ ένα τυχαίο διάνυσμα με $\xi_i \sim N(0,1)$, για $i = 1, \ldots, I$.

Ο Schwefel στην εργασία [189] μελέτησε τις τιμές των παραμέτρων και βρήκε ότι οι τιμές $(\phi, \tau, \eta) = (5\pi/180, (2\pi)^{-1/2}, (4\pi)^{-1/4})$ μπορούν να χρησιμοποιηθούν ως καλές ευρετικές τιμές.

Τα μεταλλαγμένα άτομα γίνονται αποδεκτά μόνο αν η απόδοση τους είναι καλύτερη από την αντίστοιχη των αρχικών ατόμων. Δηλαδή, για την περίπτωση ελαχιστοποίησης της συνάρτησης αξιολόγησης, f, ισχύει

$$G_{g+1,n} = \begin{cases} G_{g,n} + \sigma_{g+1,n\xi}, & \text{αν } f(G_{g,n} + \sigma_{g+1,n\xi}) < f(G_{g,n}), \\ G_{g,n}, & \text{αλλιώς}, \end{cases}$$

στην περίπτωση που χρησιμοποιούνται μόνο τυπικές αποκλίσεις ως παράμετροι στρατηγικής, και

$$G_{g+1,n} = \begin{cases} G_{g,n} + T(\omega_{g+1,n})S(\sigma_{g+1,n})\xi, & \text{αν } f(G_{g,n} + T(\omega_{g+1,n})S(\sigma_{g+1,n})\xi) < f(G_{g,n}), \\ G_{g,n}, & \text{αλλιώς}, \end{cases}$$

αν χρησιμοποιείται πληροφορία συσχέτισης.

Τέλος, για κάθε γενεά από μ γονείς παράγονται λ απόγονοι, οι οποίοι μεταλλάσσονται. Μετά τον ανασυνδυασμό και την μετάλλαξη επιλέγονται τα άτομα για την επόμενη γενεά, σύμφωνα με μια από τις ακόλουθες δύο στρατηγικές επιλογής.

(α) $(\mu+\lambda)$ΕΣ: στην περίπτωση αυτή, η ΕΣ παράγει λ απογόνους από μ γονείς, με $1 \leqslant \mu \leqslant l \leqslant \infty$. Η επόμενη γενεά αποτελείται από τα μ καλύτερα άτομα μεταξύ των μ γονέων και των λ απογόνων. Η $(\mu+\lambda)$ΕΣ χρησιμοποιεί την τεχνική του ελιτισμού για την επιβίωση των πιο αποδοτικών γονέων στην επόμενη γενεά.

(β) (μ, λ)ΕΣ: στην περίπτωση αυτή, η επόμενη γενεά αποτελείται από τα μ καλύτερα άτομα επιλεγμένα από τους λ απογόνους. Η στρατηγική αυτή απαιτεί πλεονασματική γέννηση, δηλαδή $1 \leqslant \mu < \lambda < \infty$.

2.1.5 Διαφοροεξελικτικός Αλγόριθμος

Ο *Διαφοροεξελικτικός Αλγόριθμος* (ΔΕ), παρότι δεν έχει την προέλευσή του σε φυσικές ή κοινωνικές διεργασίες, έχει αρκετά κοινά σημεία με τους Εξελικτικούς Αλγόριθμους και πληθώρα εφαρμογών με εξαιρετικά αποτελέσματα. Ο ΔΕ αναπτύχθηκε από τους Storn και Price [202] και χρησιμοποιεί ένα πληθυσμό από σημεία, ο οποίος εξελίσσεται και μπορεί να εντοπίσει ολικά βέλτιστα γρήγορα και με μικρό υπολογιστικό κόστος.

Ο ΔΕ χρησιμοποιεί έναν πληθυσμό C_g, που αποτελείται από N, D-διάστατα, διανύσματα

$$\vec{x}_{i,g}, \quad i = 1, 2, ..., N, \tag{2.2}$$

για κάθε γενιά g. Το πλήθος N, δεν μεταβάλλεται κατά την διαδικασία της βελτιστοποίησης και ο αρχικός πληθυσμός επιλέγεται τυχαία και κατά τέτοιο τρόπο ώστε να καλύπτει ολόκληρο τον χώρο αναζήτησης. Κατά κανόνα χρησιμοποιείται η ομοιόμορφη κατανομή σε κάθε περίπτωση τυχαίας δειγματοληψίας. Ο ΔΕ παράγει τα νέα διανύσματα παραμέτρων προσθέτοντας την σταθμητή διαφορά μεταξύ δύο διανυσμάτων του πληθυσμού, σε ένα τρίτο διάνυσμα. Η διαδικασία αυτή ονομάζεται *μετάλλαξη (mutation)*. Οι παράμετροι του μεταλλαγμένου διανύσματος στη συνέχεια συνδυάζονται με τις παραμέτρους ενός άλλου προκαθορισμένου διανύσματος, που καλείται *διάνυσμα στόχος* (target vector), για την παραγωγή ενός *διανύσματος δοκιμής* (trial vector). Ο συνδυασμός αυτός των παραμέτρων καλείται *διασταύρωση* (crossover). Εάν το διάνυσμα δοκιμής έχει καλύτερη απόδοση, αναφορικά με την συνάρτηση αξιολόγησης, από το διάνυσμα στόχο τότε το αντικαθιστά στην επόμενη γενιά. Η διαδικασία αυτή καλείται *επιλογή* (selection). Κάθε διάνυσμα του πληθυσμού οφείλει να αποτελέσει διάνυσμα-στόχο μια φορά, έτσι ώστε να έχουμε N συγκρίσεις σε κάθε γενιά.

Ένας ΔΕ χρησιμοποιεί τρεις διαφοροεξελικτικούς τελεστές: την *μετάλλαξη*, την *διασταύρωση* και την *επιλογή*. Οι διαφορετικές εκδοχές ΔΕ διαχωρίζονται ανάλογα με τη μορφή των τελεστών που χρησιμοποιούνται.

Για κάθε διάνυσμα στόχο $\vec{x}_{i,g}$, $i = 1, 2, ..., N$, παράγεται ένα μεταλλαγμένο διάνυσμα σύμφωνα με την σχέση

$$\vec{v}_{i,g+1} = \vec{x}_{r_1,g} + F(\vec{x}_{r_2,g} - \vec{x}_{r_3,g}), \tag{2.3}$$

όπου οι δείκτες r_1, r_2 και r_3, είναι ακέραιοι τυχαία επιλεγμένοι από το σύνολο $\{1, 2, ..., N\}$, διαφορετικοί μεταξύ τους καθώς και από τον τρέχοντα δείκτη i. Επομένως το μέγεθος N του πληθυσμού πρέπει να είναι μεγαλύτερο ή ίσο από 4, ώστε να ικανοποιείται η προηγούμενη συνθήκη. Η παράμετρος F είναι πραγματική και σταθερή, με $F > 0$ και $F \in [0, 2]$, και καθορίζει το εύρος της επίδρασης του αντίστοιχου παράγοντα διαφοράς $(\vec{x}_{r_2,g} - \vec{x}_{r_3,g})$.

Για να αυξηθεί η διασπορά του πληθυσμού σε κάθε νέα γενιά, ώστε να γίνεται καλύτερη αναζήτηση, χρησιμοποιείται ο τελεστής της διασταύρωσης. Συγκεκριμένα, παράγεται το διάνυσμα δοκιμής

$$\vec{u}_{i,g} = (u_{1i,g}, u_{2i,g}, ..., u_{Di,g}), \tag{2.4}$$

όπου

$$u_{ji,g} = \begin{cases} v_{ji,g}, & \text{αν } (randb(j) \leq CR) \text{ ή } j = rnbr(i), \\ x_{ji,g}, & \text{αν } (randb(j) > CR) \text{ ή } j \neq rnbr(i), \end{cases} \tag{2.5}$$

για $j = 1, 2, ..., D$. Στη σχέση (2.5), ο όρος $randb(j)$ είναι η j-οστή τιμή μιας ομοιόμορφης γεννήτριας τυχαίων αριθμών εντός του κλειστού διαστήματος $[0, 1]$ και το CR είναι μια *σταθερά διασταύρωσης* (crossover constant), η οποία καθορίζεται από το χρήστη της μεθόδου. Το $rnbr(i)$ είναι ένας ακέραιος τυχαία επιλεγμένος από το σύνολο $\{1, 2, ..., D\}$, ο οποίος εξασφαλίζει ότι το $\vec{u}_{i,g}$ θα περιέχει τουλάχιστον μία από τις συνιστώσες του μεταλλαγμένου διανύσματος $\vec{v}_{i,g}$. Αυτό το σχήμα διασταύρωσης καλείται *δυαδικό* (binary crossover).

Η επιλογή των μελών του πληθυσμού για την γενιά $g + 1$, γίνεται μετά από σύγκριση του διανύσματος δοκιμής $\vec{u}_{i,g+1}$ και του διανύσματος στόχου $\vec{x}_{i,g}$. Εάν το διάνυσμα $\vec{u}_{i,g+1}$ έχει καλύτερη απόδοση από το διάνυσμα $\vec{x}_{i,g}$, τότε ως διάνυσμα $\vec{x}_{i,g+1}$ επιλέγεται το $\vec{u}_{i,g+1}$,

αλλιώς διατηρείται το $\vec{x}_{i,g}$. Δηλαδή, για την περίπτωση ελαχιστοποίησης της συνάρτησης αξιολόγησης, f, ισχύει

$$\vec{x}_{i,g+1} = \begin{cases} \vec{u}_{i,g+1}, & \text{αν } f(\vec{u}_{i,g+1}) < f(\vec{x}_{i,g}), \\ \vec{x}_{i,g}, & \text{αλλιώς.} \end{cases} \tag{2.6}$$

Η τυπική μορφή του Διαφοροεξελικτικού Αλγορίθμου, όπως αυτή περιγράφηκε παραπάνω, δίνεται στον Πίνακα 2.5.

Πίνακας 2.5: Η τυπική μορφή του Διαφοροεξελικτικού Αλγορίθμου.

1. Θέσε τον αριθμό γενεών $g = 0$ και αρχικοποίησε τις παραμέτρους F, CR.
2. Αρχικοποίησε έναν αρχικό πληθυσμό $C_g = \{\vec{x}_{i,g} \,|i = 1, \ldots, N\}$, όπου N είναι ο συνολικός αριθμός των ατόμων - γονέων.
3. Υπολόγισε την απόδοση κάθε ατόμου του πληθυσμού σύμφωνα με την συνάρτηση αξιολόγησης, f.
4. Για κάθε άτομο $\vec{x}_{i,g}$, $i = 1, \ldots, N$, του πληθυσμού, κάνε τα ακόλουθα:
   - α. επέλεξε $r_1, r_2, r_3 \sim U(1, \ldots, N)$, με $r_1 \neq r_2 \neq r_3 \neq i$
   - β. επέλεξε $rnbr(i) \sim U(1, \ldots, D)$
   - γ. για $j = 1, \ldots, D$,
     επέλεξε $randb(j) \sim U[0, 1]$
     αν $randb(j) \leqslant CR$ ή $j = rnbr(i)$, τότε
     $$u_{ji,g} = x_{jr_1,g} + F(x_{jr_2,g} - x_{jr_3,g}),$$
     αλλιώς
     $$u_{ji,g} = x_{ji,g}.$$
5. Επέλεξε τον νέο πληθυσμό C_{g+1} των N ατόμων ως εξής:
   $$\vec{x}_{i,g+1} = \begin{cases} \vec{u}_{i,g+1}, & \text{αν } f(\vec{u}_{i,g+1}) < f(\vec{x}_{i,g}), \\ \vec{x}_{i,g}, & \text{αλλιώς.} \end{cases}$$
6. Θέσε $g = g + 1$.
7. Επανάλαβε την διαδικασία από το βήμα 4, μέχρι να ικανοποιηθεί το κριτήριο τερματισμού.

Οι Διαφοροεξελικτικοί τελεστές παρουσιάζονται με κάποιες παραλλαγές, οι οποίες δημιουργούν την ποικιλία εκδοχών του ΔΕ. Για την ταξινόμηση των παραλλαγών αυτών χρησιμοποιείται ο ακόλουθος συμβολισμός:

$$DE/x/y/z,$$

όπου το x καθορίζει το διάνυσμα που θα μεταλλαχθεί, το οποίο μπορεί να είναι «rand» δηλαδή ένα τυχαία επιλεγμένο διάνυσμα του πληθυσμού ή «best», δηλαδή το διάνυσμα με τη χαμηλότερη συναρτησιακή τιμή του τρέχοντος πληθυσμού. Το y είναι ο αριθμός των διαφορών που

χρησιμοποιούνται για τον παράγοντα διαφοράς στη μετάλλαξη και το z συμβολίζει το σχήμα της διασταύρωσης.

Χρησιμοποιώντας τον συμβολισμό αυτό, η μέθοδος με τον τελεστή μετάλλαξης της Σχέσης (2.3), μπορεί να συμβολιστεί ως $DE/rand/1/bin$. Διαφορετικοί τελεστές μετάλλαξης που έχουν χρησιμοποιηθεί για τον ΔΕ με ενδιαφέροντα αποτελέσματα [202], είναι οι ακόλουθοι:

$$\vec{v}_{i,g+1} = \vec{x}_{best,g} + F(\vec{x}_{r_1,g} - \vec{x}_{r_2,g}), \tag{2.7}$$

$$\vec{v}_{i,g+1} = \vec{x}_{i,g} + F(\vec{x}_{best,g} - \vec{x}_{i,g}) + F(\vec{x}_{r_1,g} - \vec{x}_{r_2,g}), \tag{2.8}$$

$$\vec{v}_{i,g+1} = \vec{x}_{best,g} + F(\vec{x}_{r_1,g} + \vec{x}_{r_2,g} - \vec{x}_{r_3,g} - \vec{x}_{r_4,g}), \tag{2.9}$$

$$\vec{v}_{i,g+1} = \vec{x}_{r_1,g} + F(\vec{x}_{r_2,g} + \vec{x}_{r_3,g} - \vec{x}_{r_4,g} - \vec{x}_{r_5,g}), \tag{2.10}$$

όπου $\vec{x}_{best,g}$ είναι το καλύτερο άτομο της g-ιοστής γενεάς, r_1, r_2, r_3, r_4, $r_5 \in \{1, 2, \ldots, N\}$, είναι ανά δύο διαφορετικοί τυχαίοι δείκτες και $\vec{x}_{i,g}$ είναι το τρέχον άτομο της γενεάς g.

Η χρήση δύο διανυσμάτων διαφορών στις μεθόδους $DE/best/2/bin$ και $DE/rand/2/bin$, των Σχέσεων (2.9) και (2.10), αντίστοιχα, βοηθά στην βελτίωση της διασποράς του πληθυσμού όταν το μέγεθος του πληθυσμού, N, είναι αρκετά μεγάλο.

2.1.6 Βελτιστοποίηση με Σμήνος Σωματιδίων

Η Βελτιστοποίηση με Σμήνος Σωματιδίων (ΒΣΣ) είναι μια σχετικά νέα εξελικτική μέθοδος, η οποία αναπτύχθηκε από τους Eberhart και Kennedy [50], ανήκει στις μεθόδους Νοημοσύνης Σμηνών και βασίζεται στην προσομοίωση της κοινωνικής συμπεριφοράς των πτηνών μέσα σε ένα σμήνος. Πρόδρομο της μεθόδου ΒΣΣ αποτέλεσε η προσπάθεια για προσομοίωση της κίνησης σμηνών, με σκοπό την εύρεση μοτίβων που επιτρέπουν στα πτηνά να πετούν συγχρονισμένα και να αλλάζουν ξαφνικά κατεύθυνση αναδιοργανωμένα σε έναν βέλτιστο σχηματισμό.

Παρόμοια με τις υπόλοιπες μεθόδους ΕΥ, η ΒΣΣ χρησιμοποιεί έναν πληθυσμό σημείων στο χώρο αναζήτησης, τα οποία αποτελούν πιθανές λύσεις του προβλήματος. Σύμφωνα με την ορολογία της μεθόδου ΒΣΣ, ο πληθυσμός αυτός καλείται *σμήνος* (swarm) και κάθε μέλος αυτού καλείται *σωματίδιο* (particle). Αντίθετα με τις προηγούμενες μεθόδους ΕΥ, στην ΒΣΣ οι αλλαγές των θέσεων των σωματιδίων του πληθυσμού μέσα στο χώρο αναζήτησης βασίζονται στην κοινωνικο-ψυχολογική τάση των ατόμων να «μιμηθούν» την επιτυχία των άλλων ατόμων. Για το λόγο αυτό, οι αλλαγές της κίνησης ενός σωματιδίου μέσα στο σμήνος καθορίζονται από την δική του προηγούμενη εμπειρία αλλά και από την εμπειρία των γειτονικών του σωματιδίων. Συγκεκριμένα, κάθε μέλος του πληθυσμού «θυμάται» τις καλύτερες περιοχές του χώρου αναζήτησης που έχει επισκεπτεί, αλλά συγχρόνως γνωρίζει και την καλύτερη περιοχή που έχουν εντοπίσει τα γειτονικά του σωματίδια, και μεταβάλλει την κίνησή του συνδυάζοντας και τους δύο αυτούς παράγοντες. Συνεπώς η συμπεριφορά αναζήτησης ενός σωματιδίου εξαρτάται από την αντίστοιχη των υπόλοιπων μελών του πληθυσμού. Η μοντελοποίηση αυτής της κοινωνικής συμπεριφοράς έχει ως αποτέλεσμα την στοχαστική επιστροφή των σωματιδίων προς προηγούμενες ελπιδοφόρες περιοχές του χώρου αναζήτησης.

Το χαρακτηριστικό που καθοδηγεί την λειτουργία της μεθόδου ΒΣΣ είναι η κοινωνική αλληλεπίδραση. Τα σωματίδια του σμήνους μαθαίνουν το ένα από το άλλο και βασιζόμενα στην αποκτώμενη γνώση, κινούνται με τέτοιο τρόπο ώστε να «μοιάσουν» στους καλύτερους γείτονές τους. Συνεπώς, η κοινωνική δομή της μεθόδου καθορίζεται από το σχηματισμό των γειτονιών, καθώς σωματίδια από την ίδια γειτονιά επικοινωνούν μεταξύ τους. Έχουν αναπτυχθεί και μελετηθεί διάφορα σχήματα γειτονιών, στις οποίες η έννοια της γειτονιάς είναι τοπολογική αναφορικά με τη θέση (αρίθμηση) των σωματιδίων μέσα στον πληθυσμό και όχι ως προς την θέση τους στο χώρο αναζήτησης [82]. Τα πιο σημαντικά σχήματα γειτονιών που συνήθως χρησιμοποιούνται για τη μέθοδο ΒΣΣ, είναι τα ακόλουθα.

(α) Η *τοπολογία αστεριού* (star topology), η οποία βασίζεται στην έννοια της *ολικής γειτονιάς* (global neighborhood), δηλαδή κάθε σωματίδιο επικοινωνεί με κάθε άλλο σωματίδιο του σμήνους. Σύμφωνα με αυτή την παραλλαγή της μεθόδου, κάθε σωματίδιο κινείται προς την κατεύθυνση της καλύτερης προηγούμενης θέσης του αλλά και της καλύτερης προηγούμενης θέσης ολόκληρου του σμήνους.

(β) Η *τοπολογία δακτυλιδιού* (ring topology), η οποία βασίζεται στην έννοια της *τοπικής γειτονιάς* (local neighborhood), δηλαδή κάθε σωματίδιο επικοινωνεί μόνο με τα σωματίδια που ανήκουν στην περιορισμένη γειτονιά του. Σύμφωνα με αυτή την παραλλαγή της μεθόδου, κάθε μέλος του πληθυσμού κινείται προς την κατεύθυνση της καλύτερης προηγούμενης θέσης του αλλά και προς την θέση του καλύτερου σωματιδίου που ανήκει στην περιορισμένη γειτονιά του [52]. Για παράδειγμα, εάν το μέγεθος της γειτονιάς είναι 2, τότε το i-οστό μέλος του πληθυσμού κινείται προς το καλύτερο σωματίδιο μεταξύ τριών, του $(i-1)$-οστού, του $(i+1)$-οστού και του ιδίου. Το πλεονέκτημα της τοπολογίας αυτής είναι ότι ερευνάται μεγαλύτερο μέρος του χώρου αναζήτησης και η σύγκλιση της μεθόδου είναι πιο αργή.

Η παραλλαγή της μεθόδου με ολική γειτονιά είναι μια ειδική περίπτωση της μεθόδου με τοπική γειτονιά αν θεωρήσουμε ως γειτονιά ολόκληρο το σμήνος. Στην περίπτωση της ολικής γειτονιάς, η μέθοδος ΒΣΣ είναι περισσότερο επιρρεπής στη σύγκλιση σε τοπικά ακρότατα καθώς όλα τα σωματίδια κινούνται προς αυτή την λύση. Όσο μικρότερο είναι το μέγεθος της γειτονιάς και περισσότερες οι γειτονιές που χρησιμοποιούνται, τόσο λιγότερο επηρεάζεται η μέθοδος από τα τοπικά ακρότατα. Στην περίπτωση αυτή ερευνάται μεγαλύτερο μέρος του χώρου αναζήτησης και καμία λύση δεν επηρεάζει όλα τα σωματίδια του σμήνους. Ωστόσο, όσο μεγαλύτερος είναι ο αριθμός των γειτονιών, τόσο αργότερη είναι η σύγκλιση της μεθόδου στη τελική λύση.

Σε αντιστοιχία με τις υπόλοιπες μεθόδους ΕΥ, κάθε μέλος του σμήνους είναι ένα σημείο του D-διάστατου χώρου, οπότε το i-οστό μέλος του πληθυσμού στην t επανάληψη του αλγορίθμου μπορεί να παρασταθεί από ένα διάνυσμα $\vec{x}_{i,t} = (x_{i1,t}, x_{i2,t}, \ldots, x_{iD,t})^\top$. Η καλύτερη θέση που είχε κατά την κίνησή του στο χώρο το i-οστό μέλος μέχρι την τρέχουσα επανάληψη t του αλγορίθμου, παριστάνεται από το διάνυσμα $\vec{p}_{i,t} = (p_{i1,t}, p_{i2,t}, \ldots, p_{iD,t})^\top$, και η ταχύτητά του (αλλαγή θέσης), στην τρέχουσα επανάληψη t, από το διάνυσμα $\vec{v}_{i,t} = (v_{i1,t}, v_{i2,t}, \ldots, v_{iD,t})^\top$. Επιπλέον, συμβολίζουμε με δείκτη *best*, το καλύτερο μέλος της γειτονιάς (ολικής ή τοπικής) του σωματιδίου i, μέχρι της τρέχουσα επανάληψη. Η κίνηση του σμήνους περιγράφεται από τις ακόλουθες εξισώσεις

$$\vec{v}_{i,t+1} = w\vec{v}_{i,t} + c_1 r_1 \big(\vec{p}_{i,t} - \vec{x}_{i,t}\big) + c_2 r_2 \big(\vec{p}_{best,t} - \vec{x}_{i,t}\big), \tag{2.11}$$

$$\vec{x}_{i,t+1} = \vec{x}_{i,t} + \vec{v}_{i,t+1}, \tag{2.12}$$

όπου $i = 1, 2, \ldots, N$, όταν N είναι το μέγεθος του πληθυσμού, t είναι ο αριθμός της τρέχουσας επανάληψης, c_1 και c_2 δύο θετικές σταθερές και r_1, r_2 τυχαίοι αριθμοί ομοιόμορφα κατανεμημένοι στο διάστημα [0,1]. Το w είναι μια παράμετρος που καλείται *βάρος αδράνειας* (inertia weight) της μεθόδου.

Η σχέση (2.11) χρησιμοποιείται για τον καθορισμό της νέας ταχύτητας του κάθε σωματιδίου και περιλαμβάνει τρεις βασικούς όρους

(α) την τρέχουσα ταχύτητα του σωματιδίου,

(β) την απόσταση του σωματιδίου από την καλύτερη μέχρι τώρα θέση του και

(γ) την απόσταση του από την καλύτερη θέση της γειτονιάς του (ολικής ή τοπικής).

Στη συνέχεια το σωματίδιο μετακινείται σε μια νέα θέση σύμφωνα με τη σχέση (2.12). Η απόδοση κάθε σωματιδίου μετράται, με μια συνάρτηση αξιολόγησης, η οποία στα προβλήματα Βελτιστοποίησης χωρίς περιορισμούς, είναι η προς βελτιστοποίηση συνάρτηση.

Το βάρος αδράνειας w, έχει ιδιαίτερα σημαντικό ρόλο στη σύγκλιση της μεθόδου. Χρησιμοποιείται ως ρυθμιστικός παράγοντας της συμβολής της τρέχουσας ταχύτητας στη νέα, καθορίζοντας με τον τρόπο αυτό την ισορροπία μεταξύ της ολικής και της τοπικής αναζήτησης. Μεγάλες τιμές του w διευκολύνουν την ολική αναζήτηση και τον εντοπισμό νέων περιοχών στο χώρο αναζήτησης, ενώ οι μικρές τιμές διευκολύνουν την τοπική αναζήτηση, δηλαδή την λεπτομερέστερη εξερεύνηση των ήδη ευρεθέντων περιοχών. Κατάλληλη επιλογή του w παρέχει ισορροπία μεταξύ της ολικής και τοπικής αναζήτησης και έχει ως αποτέλεσμα την μείωση κατά μέσο όρο των επαναλήψεων που απαιτούνται για τον εντοπισμό της βέλτιστης λύσης. Αρχικά η παράμετρος w που χρησιμοποιήθηκε ήταν σταθερή. Πειραματικά όμως απεδείχθη ότι υψηλές τιμές του w στα αρχικά βήματα του αλγορίθμου και χαμηλότερες στα επόμενα οδηγούν σε καλύτερες επιδόσεις της μεθόδου [191, 192]. Για το λόγο αυτό στις εφαρμογές συνήθως χρησιμοποιείται παράμετρος w, η οποία μεταβάλλει την τιμή της από την αρχική τιμή 1.2 μέχρι την τιμή 0.

Οι παράμετροι c_1 και c_2 στη σχέση (2.11), καλούνται *κοινωνική* (social) και *γνωστική* (cognitive) παράμετρος, αντίστοιχα. Ο ρόλος τους στην σύγκλιση της ΒΣΣ δεν είναι τόσο κρίσιμος, ωστόσο κατάλληλη ρύθμισή τους μπορεί να συντελέσει σε γρηγορότερη σύγκλιση και διαφυγή από τοπικά ακρότατα. Οι τυπικές τιμές που προτείνονται για τις c_1, c_2 στην εκδοχή της μεθόδου με βάρος αδράνειας, είναι $c_1 = c_2 = 2$.

Οι παράμετροι r_1 και r_2 χρησιμοποιούνται για την διατήρηση της ποικιλότητας του πληθυσμού και είναι τυχαίοι αριθμοί ομοιόμορφα κατανεμημένοι στο διάστημα $[0, 1]$.

Η χρήση ενός μηχανισμού ελέγχου της ταχύτητας των σωματιδίων συνήθως διευκολύνει στη σύγκλιση της μεθόδου καθώς αποτρέπει την πολύ γρήγορη κίνηση των σωματιδίων μεταξύ διαφορετικών περιοχών του χώρου αναζήτησης. Για το σκοπό αυτό χρησιμοποιείται μια παράμετρος, $V_{\max}$, η οποία περιορίζει τη μέγιστη επιτρεπτή ταχύτητα των σωματιδίων. Εάν η ταχύτητα ενός σωματιδίου ξεπεράσει το κατώφλι αυτής της μέγιστης επιτρεπτής ταχύτητας, τότε τίθεται ίση με την τιμή $V_{\max}$. Η τιμή της παραμέτρου αυτής συνήθως αρχικοποιείται ως συνάρτηση του εύρους του πεδίου ορισμού του προβλήματος. Είναι σημαντικό να σημειωθεί ότι η παράμετρος $V_{\max}$ δεν αποτελεί όριο για την θέση των σωματιδίων αλλά μόνο για το μέγεθος των βημάτων κίνησης μέσα στο χώρο αναζήτησης.

Μια πιο πρόσφατη εκδοχή της μεθόδου ΒΣΣ χρησιμοποιεί μια νέα παράμετρο για τον έλεγχο της ταχύτητας των σωματιδίων, η οποία καλείται *παράγοντας περιορισμού* (constriction factor), και στην περίπτωση αυτή το σμήνος κινείται σύμφωνα με τις εξισώσεις

$$\vec{v}_{i,t+1} = \chi\Big(\vec{v}_{i,t} + c_1 r_1 \big(\vec{p}_{i,t} - \vec{x}_{i,t}\big) + c_2 r_2 \big(\vec{p}_{best,t} - \vec{x}_{i,t}\big)\Big), \tag{2.13}$$

$$\vec{x}_{i,t+1} = \vec{x}_{i,t} + \vec{v}_{i,t+1}, \tag{2.14}$$

όπου $i = 1, 2, \ldots, N$, χ είναι ο παράγοντας περιορισμού, c_1 και c_2 είναι η κοινωνική και η γνωστική παράμετρος, αντίστοιχα, r_1, r_2 είναι τυχαίοι αριθμοί ομοιόμορφα κατανεμημένοι στο διάστημα $[0, 1]$ και t είναι ο αριθμός της τρέχουσας επανάληψης.

Σύμφωνα με τη θεωρητική μελέτη της μεθόδου [36], και προκειμένου να υπάρχει σύγκλιση των τροχιών των σωματιδίων, πρέπει να ισχύει $c_1 + c_2 > 4$. Στην περίπτωση αυτή, η βέλτιστη τιμή του παράγοντα περιορισμού δίνεται από την σχέση

$$\chi = \frac{2\kappa}{|2 - \phi - \sqrt{\phi^2 - 4\phi}|}, \tag{2.15}$$

όπου η μεταβλητή κ ανήκει στο διάστημα $[0, 1]$ και η παράμετρος $\phi = c_1 + c_2$, δηλαδή $\phi > 4$. Οι τιμές $\kappa = 1$ και $\phi = 4.1$, με $c_1 = c_2 = 2.05$, που ικανοποιούν τη σχέση (2.15), δίνουν για την

παράμετρο χ την τιμή 0.729 και είναι οι τυπικές τιμές των παραμέτρων που χρησιμοποιούνται στη σχετική βιβλιογραφία.

Η αρχικοποίηση του πληθυσμού και των ταχυτήτων των μελών του συνήθως γίνεται τυχαία μέσα στον χώρο αναζήτησης, ωστόσο διαφορετικές τεχνικές αρχικοποίησης μπορούν να βελτιώσουν την συνολική απόδοση του αλγορίθμου [157]. Για ομοιόμορφη τυχαία αρχικοποίηση στον πολυδιάστατο χώρο αναζήτησης μπορεί να χρησιμοποιηθεί η μέθοδος Sobol [169].

Γενικά, η επιλογή κάποιων παραμέτρων για την υλοποίηση της μεθόδου ΒΣΣ, όπως είναι το μέγεθος του σμήνους, η σύγχρονη ή ασύγχρονη ενημέρωση του σμήνους κ.α., έχουν αποτελέσει θέμα έρευνας αλλά είναι ακόμη ανοικτά. Μια αρχική ανάλυση τέτοιων θεμάτων μπορεί να βρεθεί στην εργασία [23]. Η γενική μορφή της μεθόδου Βελτιστοποίησης με Σμήνος Σωματιδίων δίνεται στον Πίνακα 2.6.

Πίνακας 2.6: Η γενική μορφή της μεθόδου Βελτιστοποίησης με Σμήνος Σωματιδίων.

1. Θέσε τον αριθμό επαναλήψεων $t = 0$ και αρχικοποίησε το σμήνος, P_t, των σωματιδίων έτσι ώστε η θέση $\vec{x}_{i,t}$ κάθε σωματιδίου i του σμήνους να είναι τυχαία μέσα στο χώρο αναζήτησης. Θέσε τις τιμές των παραμέτρων της μεθόδου.

2. Υπολόγισε την απόδοση κάθε σωματιδίου του πληθυσμού σύμφωνα με την συνάρτηση αξιολόγησης, f.

3. Σύγκρινε την απόδοση κάθε σωματιδίου με την καλύτερη απόδοσή του μέχρι την τρέχουσα επανάληψη, και, για την περίπτωση ελαχιστοποίησης,

   αν $f(\vec{x}_{i,t}) < f(\vec{p}_{i,t})$, τότε $f(\vec{p}_{i,t}) = f(\vec{x}_{i,t})$ και $\vec{p}_{i,t} = \vec{x}_{i,t}$.

4. Σύγκρινε την απόδοση κάθε σωματιδίου με την απόδοση του καλύτερου σωματιδίου της γειτονιάς του (ολικής ή τοπικής) μέχρι την τρέχουσα επανάληψη, και, για την περίπτωση ελαχιστοποίησης,

   αν $f(\vec{x}_{i,t}) < f(\vec{p}_{best,t})$, τότε $f(\vec{p}_{best,t}) = f(\vec{x}_{i,t})$ και $\vec{p}_{best,t} = \vec{x}_{i,t}$.

5. Για κάθε σωματίδιο του σμήνους υπολόγισε το διάνυσμα της ταχύτητάς του (χρησιμοποιώντας την Σχέση (2.11) ή την Σχέση (2.13) ανάλογα με την χρησιμοποιούμενη εκδοχή της μεθόδου).

6. Υπολόγισε τη νέα θέση κάθε σωματιδίου του σμήνους σύμφωνα με τη σχέση

   $$\vec{x}_{i,t+1} = \vec{x}_{i,t} + \vec{v}_{i,t+1}.$$

7. Θέσε τον αριθμό επαναλήψεων $t = t + 1$.

8. Επανάλαβε την διαδικασία από το βήμα 2, μέχρι να ικανοποιηθεί το κριτήριο τερματισμού.

Η μέθοδος ΒΣΣ παρουσιάζει κάποιες φορές το πρόβλημα παγίδευσης σε τοπικά ακρότατα. Πρόσφατα όμως αναπτύχθηκε για τη μέθοδο αυτή μια τεχνική για την αποφυγή των τοπικών ακροτάτων, η οποία καλείται *τεχνική εφελκυσμού* (Streching). Ο συνδυασμός της τεχνικής αυτής με την μέθοδο ΒΣΣ οδήγησε σε μεγάλη βελτίωση των αποτελεσμάτων της μεθόδου για μια ποικιλία προβλημάτων με πολλά τοπικά ελάχιστα [153, 154]. Επίσης, η τεχνική αυτή χρησιμοποιείται για τον εντοπισμό πολλαπλών ολικών βέλτιστων [155].

Οι μέθοδοι ΕΥ εμπλέκουν τρεις κύριους τελεστές, την διασταύρωση ή ανασυνδυασμό, την μετάλλαξη και την επιλογή. Η μέθοδος ΒΣΣ δεν διαθέτει άμεσο τελεστή ανασυνδυασμού. Ωστόσο, η στοχαστική επιτάχυνση των σωματιδίων του σμήνους προς την προηγούμενη καλύτερη θέση τους, καθώς και προς την καλύτερη θέση όλου του σμήνους ή προς την κατεύθυνση του καλύτερου της γειτονιάς στην τοπική εκδοχή, παρομοιάζεται με την διαδικασία ανασυνδυασμού [51, 175, 187, 189]. Επίσης, η πρόσθεση της ταχύτητας στην τρέχουσα θέση για τη δημιουργία της νέας είναι παρόμοια με την μετάλλαξη των ΓΑ, με την διαφορά ότι στην ΒΣΣ η μετάλλαξη κατευθύνεται από την εμπειρία του κάθε ατόμου αλλά και όλου του πληθυσμού. Δηλαδή μπορούμε να πούμε ότι η μέθοδος ΒΣΣ κάνει *μετάλλαξη με συνείδηση* [83]. Τέλος, η ΒΣΣ δεν χρησιμοποιεί άμεσα τελεστή επιλογής για την επιβίωση του καλύτερου μέλους. Ως συνέπεια αυτού, σωματίδια με χαμηλότερη τιμή απόδοσης μπορούν να επιβιώσουν κατά την διαδικασία της Βελτιστοποίησης και είναι πιθανόν να οδηγηθούν σε οποιοδήποτε σημείο του χώρου αναζήτησης [51].

Η μέθοδος ΒΣΣ παρουσιάζει ιδιαίτερο ενδιαφέρον και έχει αποδειχθεί πολύ ικανή στην αντιμετώπιση πολύπλοκων προβλημάτων, όπως είναι η Βελτιστοποίηση με περιορισμούς, η Βελτιστοποίηση σε συνεχώς μεταβαλλόμενα περιβάλλοντα με εμφάνιση θορύβου, προβλήματα με πολλές συναρτήσεις (multiobjective), ακέραιου προγραμματισμού, minimax, αλλά και πραγματικές εφαρμογές [2, 3, 6, 37, 62, 83, 111, 112, 115, 150, 156, 158, 159, 173, 184, 203].

2.1.7 Βελτιστοποίηση με Αποικίες Μυρμηγκιών

Η μέθοδος Βελτιστοποίησης με Αποικίες Μυρμηγκιών (ΒΑΜ) ανήκει στα συστήματα της Νοημοσύνης Σμηνών και προσομοιάζει μέρος της λειτουργίας των φυσικών αποικιών μυρμηγκιών.

Η λειτουργία μιας φυσικής αποικίας μυρμηγκιών περιλαμβάνει αρκετές διαφορετικές εργασίες που πραγματοποιούνται από διαφορετικές ομάδες μυρμηγκιών. Οι κύριες εργασίες είναι η αναπαραγωγή που πραγματοποιείται από την βασίλισσα, η άμυνα που γίνεται από μυρμήγκια - στρατιώτες, η συλλογή τροφής που πραγματοποιείται από εξειδικευμένα μυρμήγκια - εργάτες, η επώαση που γίνεται από εξειδικευμένα μυρμήγκια - εργάτες, το καθάρισμα της φωλιάς που γίνεται από εξειδικευμένα μυρμήγκια - εργάτες και το χτίσιμο και η συντήρηση της φωλιάς που επίσης πραγματοποιείται από εξειδικευμένα μυρμήγκια - εργάτες. Η διανομή και η εκτέλεση των εργασιών γίνεται αυτόματα και βασίζεται στις ανατομικές διαφορές των ατόμων και στην στιγμεργία (*stigmergy*). Ο όρος στιγμεργία δηλώνει την διαφοροποιημένη συμπεριφορά των ατόμων μέσα σε μία αποικία και τον συντονισμό των δραστηριοτήτων τους. Η φυσική στιγμεργία σε μια αποικία χαρακτηρίζεται ως [48]:

1. η έλλειψη κεντρικής καθοδήγησης,
2. η επικοινωνία και ο συντονισμός μεταξύ των ατόμων της αποικίας με βάση τις τοπικές μεταβολές του περιβάλλοντος,
3. η θετική απόκριση με βάση την ενίσχυση των δράσεων των ατόμων.

Η αλγοριθμική μοντελοποίηση των αποικιών μυρμηγκιών βασίζεται στην αρχή της τεχνητής στιγμεργίας, η οποία ορίζεται ως η «*έμμεση επικοινωνία που επιτυγχάνεται από αριθμητικές μεταβολές των περιβαλλοντολογικών καταστάσεων οι οποίες είναι μόνο τοπικά προσβάσιμες από τα επικοινωνούντα μυρμήγκια*» [48]. Ο σκοπός της μοντελοποίησης τμημάτων της λειτουργίας των αποικιών μυρμηγκιών είναι η εύρεση ενός μαθηματικού μοντέλου το οποίο θα περιγράφει με ακρίβεια τα χαρακτηριστικά της στιγμεργίας των αντίστοιχων ατόμων - μυρμηγκιών. Σε αντίθεση με την μέθοδο Βελτιστοποίησης με Σμήνος Σωματιδίων, όπου όλα τα άτομα (σωματίδια) του σμήνους εμφανίζουν την ίδια συμπεριφορά και χαρακτηριστικά, στη μοντελοποίηση των αποικιών μυρμηγκιών θεωρούνται «σμήνη» που αποτελούνται από μεγάλο αριθμό ατόμων και τα άτομα αυτά συνήθως έχουν διαφορετική δομή και εργασίες αλλά όλα συνεισφέρουν σε έναν κοινό στόχο.

Ένα από τα πρώτα ερωτήματα που ερευνήθηκαν αναφορικά με την συμπεριφορά των μυρμηγκιών ήταν η συλλογή τροφής. Τα μυρμήγκια έχουν την ιδιότητα να βρίσκουν πάντα το πιο σύντομο μονοπάτι μεταξύ της φωλιάς και της πηγής τροφής. Τα πειράματα έδειξαν ότι αρχικά τα μονοπάτια επιλέγονται τυχαία. Καθώς όμως ο χρόνος περνάει όλο και περισσότερα μυρμήγκια ακολουθούν το συντομότερο μονοπάτι. Η εμφάνιση αυτής της ικανότητας γίνεται δυνατή με τη βοήθεια μιας έμμεσης μορφής επικοινωνίας μεταξύ των μελών της αποικίας, η οποία πραγματοποιείται με την εναπόθεση από τα μυρμήγκια στο περιβάλλον μιας χημικής ουσίας, της *φερομόνης*. Συγκεκριμένα, κατά την διάρκεια αναζήτησης τροφής και κατά την επιστροφή στη φωλιά κάθε μυρμήγκι εναποθέτει φερομόνη στο μονοπάτι που ακολουθεί. Για την επιλογή μονοπατιού τα μυρμήγκια ακολουθούν αυτό με την μεγαλύτερη συγκέντρωση φερομόνης. Το συντομότερο μονοπάτι θα έχει περισσότερα αποθέματα φερομόνης καθώς τα μυρμήγκια επιστρέφουν από αυτό το μονοπάτι προς την φωλιά γρηγορότερα, αφήνοντας έτσι περισσότερη φερομόνη από αυτή που αφήνουν τα μυρμήγκια που γυρνούν από το μακρύτερο μονοπάτι. Επιπλέον, οι εναποθέσεις φερομόνης εξατμίζονται με το χρόνο συνεπώς η συγκέντρωση φερομόνης στο μακρύτερο μονοπάτι μειώνεται γρηγορότερα από την αντίστοιχη στο συντομότερο μονοπάτι. Αυτή ακριβώς η απλή ιδέα υλοποιείται από την μέθοδο BAM για την επίλυση προβλημάτων συνδυαστικής Βελτιστοποίησης με εφαρμογές μεταξύ άλλων στη δρομολόγηση δικτύων και στο χρονοπρογραμματισμό εργασιών [19, 48, 49].

Η μελέτη της συμπεριφοράς των μυρμηγκιών γενικότερα οδήγησε στην ανάπτυξη αλγορίθμων που εφαρμόζονται σε ποικιλία προβλημάτων. Εκτός από την μέθοδο BAM που μοντελοποιεί τη συμπεριφορά των μυρμηγκιών για τη συλλογή τροφής για την επίλυση προβλημάτων συνδυαστικής Βελτιστοποίησης, η ιδιότητα των μυρμηγκιών να κατανέμουν δυναμικά το φόρτο εργασίας οδήγησε σε στρατηγικές προσαρμόσιμης ανάθεσης εργασιών, η διαδικασία καθαρισμού της φωλιάς και κατανομής της επώασης οδήγησε σε αλγορίθμους για την επίλυση του προβλήματος χρωματισμού γράφων και αλγορίθμους ταξινόμησης και τα χαρακτηριστικά συντονισμού για συνεργατική μεταφορά έδωσαν αλγορίθμους για ρομποτικές υλοποιήσεις που βασίζονται σε ομάδες [48].

2.2 Εισαγωγή στα Τεχνητά Νευρωνικά Δίκτυα

Στην ενότητα αυτή παρουσιάζονται εισαγωγικά στοιχεία και βασικές έννοιες των Τεχνητών Νευρωνικών Δικτύων (ΤΝΔ), των μεθόδων εκπαίδευσής τους, καθώς και τα σημαντικότερα θεωρητικά αποτελέσματα που έχουν αποδειχθεί για τις δυνατότητες και την εφαρμογή των ΤΝΔ σε διάφορα προβλήματα.

Την αφορμή για την δημιουργία των ΤΝΔ αποτέλεσε ο ανθρώπινος εγκέφαλος, η λειτουργία του και οι δυνατότητές του. Ο ανθρώπινος εγκέφαλος είναι ένας πολύπλοκος μη-γραμμικός και παράλληλος υπολογιστής. Έχει την ικανότητα να εκτελεί εργασίες όπως η αναγνώριση προτύπων και ο έλεγχος μηχανών και γενικότερα να αντιλαμβάνεται πολύ γρηγορότερα από οποιονδήποτε υπολογιστή, παρά το γεγονός ότι οι ψηφιακές πύλες λειτουργούν σε επίπεδο νανοδευτερολέπτων ενώ τα βιολογικά νευρικά συστήματα σε χιλιοστά του δευτερολέπτου. Επιπλέον, ο ανθρώπινος εγκέφαλος έχει την ικανότητα να μαθαίνει, να απομνημονεύει και να γενικεύει, στοιχεία που οδήγησαν σε έρευνα για την αλγοριθμική μοντελοποίηση των βιολογικών νευρικών συστημάτων.

Υπολογίζεται ότι υπάρχουν νευρώνες πλήθους τάξης $10 - 500$ δισεκατομμυρίων στον ανθρώπινο εγκέφαλο με 60 τρισεκατομμύρια συνάψεις. Οι νευρώνες οργανώνονται σε περίπου 1000 κεντρικές ομάδες κάθε μια εκ των οποίων έχει περίπου 500 νευρωνικά δίκτυα. Προς το παρόν είναι αδύνατο να μοντελοποιήσουμε πραγματικά τον ανθρώπινο εγκέφαλο. Ωστόσο, είναι εφικτή η μοντελοποίηση μικρών τεχνητών νευρωνικών δικτύων (ΤΝΔ) με στόχο την επίλυση συγκεκριμένων προβλημάτων. Με τον τρόπο αυτό μπορούμε να επιλύσουμε κάποια προβλήματα με ΤΝΔ που περιορίζονται από τις δυνατότητες της σύγχρονης υπολογιστικής ισχύος και του αποθηκευτικού χώρου.

Τα βασικά δομικά στοιχεία των βιολογικών νευρικών συστημάτων είναι τα νευρικά κύτταρα που ονομάζονται νευρώνες. Ένας νευρώνας αποτελείται από ένα κυτταρικό σώμα, δενδρίτες και έναν άξονα. Οι νευρώνες είναι μαζικά διασυνδεδεμένοι, και η σύνδεση γίνεται μεταξύ του άξονα ενός νευρώνα και ενός δενδρίτη ενός άλλου νευρώνα. Η σύνδεση αυτή καλείται σύναψη. Τα σήματα μεταφέρονται από τους δενδρίτες μέσω του κυτταρικού σώματος στον άξονα από τον οποίο στη συνέχεια μεταβιβάζονται προς όλους τους συνδεδεμένους δενδρίτες. Ένα σήμα όμως μεταδίδεται στον άξονα ενός νευρώνα μόνο αν «πυροδοτήσει» το κύτταρο. Ένας νευρώνας μπορεί είτε να περιορίσει είτε να προωθήσει ένα σήμα.

Ένας τεχνητός νευρώνας είναι μοντέλο ενός βιολογικού νευρώνα. Κάθε τεχνητός νευρώνας λαμβάνει σήματα από το περιβάλλον ή άλλους τεχνητούς νευρώνες. Τα εισερχόμενα σήματα είτε περιορίζονται είτε αυξάνονται μέσω αρνητικών ή θετικών αριθμητικών βαρών που συσχετίζονται με κάθε σύνδεση προς τον τεχνητό νευρώνα. Η πυροδότηση ενός τεχνητού νευρώνα και η ισχύς του εξερχόμενου σήματος ελέγχονται μέσω μιας συνάρτησης που καλείται *συνάρτηση ενεργοποίησης*. Ο τεχνητός νευρώνας συγκεντρώνει όλα τα εισερχόμενα σήματα και υπολογίζει το εισερχόμενο σήμα του δικτύου ως συνάρτηση των αντιστοίχων βαρών. Το σήμα του δικτύου είναι η είσοδος της συνάρτησης ενεργοποίησης από την οποία υπολογίζεται το σήμα εξόδου του τεχνητού νευρώνα.

Ένα τεχνητό νευρωνικό δίκτυο (ΤΝΔ) είναι ένα διαστρωματομένο δίκτυο τεχνητών νευρώνων. Ένα ΤΝΔ μπορεί να αποτελείται από ένα στρώμα εισόδου, κρυφά στρώματα και ένα στρώμα εξόδου. Οι τεχνητοί νευρώνες ενός στρώματος συνδέονται πλήρως ή μερικώς με τους νευρώνες του επόμενου στρώματος. Είναι επίσης δυνατή η ανάδραση δηλαδή η σύνδεση προς τα προηγούμενα στρώματα.

Έχουν αναπτυχθεί διάφοροι τύποι ΤΝΔ, όπως

1. ΤΝΔ μονοστρωματικά, όπως τα Hopfield ΤΝΔ,
2. ΤΝΔ πολυστρωματικά εμπρόσθιας τροφοδότησης, μεταξύ των οποίων είναι τα τυπικά δίκτυα backpropagation, functional link και τα product unit δίκτυα,
3. temporal ΤΝΔ, όπως τα Elman και Jordan απλά recurrent δίκτυα αλλά και τα δίκτυα χρονικής υστέρησης (time-delay),
4. τα self-organizing ΤΝΔ,
5. συνδυασμένα δίκτυα εμπρόσθιας τροφοδότησης και self-organizing δίκτυα, όπως τα radial basis function δίκτυα και άλλα.

Αυτοί οι τύποι ΤΝΔ έχουν χρησιμοποιηθεί σε ένα μεγάλο εύρος εφαρμογών παρουσιάζοντας αποτελεσματικότητα και αποδοτικότητα στην επίλυση πολύπλοκων προβλημάτων. Μερικές κλάσεις εφαρμογών των ΤΝΔ είναι οι ακόλουθες.

1. Ομαδοποίηση, όπου στόχος είναι η πρόβλεψη της ομάδας στην οποία ανήκει ένα πρότυπο.
2. Συσχέτιση προτύπων, όπου στόχος είναι η παραγωγή του προτύπου που σχετίζεται καλύτερα με ένα δοθέν πρότυπο.
3. Συμπλήρωση προτύπων, όπου στόχος είναι η συμπλήρωση ελλιπών τμημάτων δοθέντων προτύπων.
4. Βελτιστοποίηση, που στοχεύει στην εύρεση των βέλτιστων τιμών των παραμέτρων ενός προβλήματος βελτιστοποίησης.
5. Έλεγχος, όπου δοθέντος ενός προτύπου προτείνεται η καταλληλότερη ενέργεια.
6. Προσέγγιση συναρτήσεων και μοντελοποίηση χρονοσειρών, όπου στόχος είναι η εκμάθηση των συναρτησιακών σχέσεων μεταξύ των προτύπων εισόδου και των επιθυμητών προτύπων εξόδου.

7. Εξόρυξη δεδομένων, με στόχο την ανακάλυψη κρυμμένων δομών σε δεδομένα, το οποίο αναφέρεται και ως ανακάλυψη γνώσης.

Από μαθηματική σκοπιά, ένα ΤΝΔ είναι ουσιαστικά η υλοποίηση μιας μη γραμμικής απεικόνισης από το χώρο $\mathbb{R}^I$ στον $\mathbb{R}^K$, $F : \mathbb{R}^I \mapsto \mathbb{R}^K$, όπου τα I, K είναι οι διαστάσεις του χώρου εισόδου και εξόδου αντίστοιχα. Η συνάρτηση F είναι συνήθως μια πολύπλοκη συνάρτηση ενός συνόλου μη γραμμικών συναρτήσεων, μια για κάθε νευρώνα του δικτύου.

2.2.1 Υπολογιστικό μοντέλο ενός νευρώνα

Οι McCulloch και Pitts στην μελέτη [124] πρότειναν ένα δυαδικό κατώφλι ως υπολογιστικό μοντέλο για έναν νευρώνα. Αυτός ο μαθηματικός νευρώνας υπολογίζει ένα άθροισμα με βάρη των n σημάτων εισόδου, x_j, $j = 1, 2, \ldots, n$, και παράγει μια έξοδο $y = 1$ αν το άθροισμα είναι μεγαλύτερο από ένα συγκεκριμένο κατώφλι μ, και μια έξοδο $y = 0$ διαφορετικά. Δηλαδή, η έξοδος του νευρώνα είναι

$$y = \theta\Big(\sum_{j=1}^{n} w_j x_j - \mu\Big),$$

όπου $\theta(\cdot)$ είναι μια συνάρτηση κατώφλι, και w_j είναι το βάρος σύναψης που σχετίζεται με την $j-$οστή είσοδο. Πολλές φορές, για απλότητα του συμβολισμού, το κατώφλι μ θεωρείται ως ένα επιπλέον βάρος $w_0 = -\mu$, το οποίο προσαρμόζεται στον νευρώνα με μια σταθερή είσοδο, $x_0 = 1$. Οι McCulloch και Pitts απέδειξαν ότι με κατάλληλα επιλεγμένα βάρη μια σύγχρονη ρύθμιση τέτοιων νευρώνων είναι, κατ΄ αρχήν, ικανή για καθολικό υπολογισμό. Το μοντέλο των McCulloch και Pitts περιέχει ένα πλήθος απλουστευμένων υποθέσεων που δεν εκφράζουν την πραγματική συμπεριφορά των βιολογικών νευρώνων. Μερικές από αυτές τις διαφορές είναι οι ακόλουθες:

1. Οι βιολογικοί νευρώνες δεν αποτελούν συσκευές κατωφλικής λειτουργίας αλλά έχουν διαβαθμιζόμενη ανταπόκριση (ουσιαστικά η έξοδός τους είναι μια μη γραμμική συνάρτηση των εισόδων τους),

2. οι βιολογικοί νευρώνες πραγματοποιούν ένα μη γραμμικό άθροισμα των εισόδων και είναι σε θέση να πραγματοποιήσουν και λογική επεξεργασία,

3. οι βιολογικοί νευρώνες παράγουν μια σειρά παλμών και όχι μόνο μια απλή τιμή εξόδου,

4. οι βιολογικοί νευρώνες ενημερώνονται ασύγχρονα.

Ωστόσο, το μοντέλο νευρώνων των McCulloch και Pitts ξεκίνησε μια νέα εποχή για τα υπολογιστικά μοντέλα των νευρωνικών δικτύων. Το παραπάνω μοντέλο νευρώνα γενικεύτηκε με πάρα πολλούς τρόπους. Μια προφανής γενίκευσή του είναι η χρήση συναρτήσεων ενεργοποίησης διαφορετικών από το κατώφλι, όπως για παράδειγμα, η μερικώς γραμμική συνάρτηση, η σιγμοειδής και η συνάρτηση του Gauss. Η σιγμοειδής είναι η πιο συχνά χρησιμοποιούμενη συνάρτηση στα ΤΝΔ, καθώς είναι αυστηρά αύξουσα και παρουσιάζει ομαλότητα και ασυμπτωτικές ιδιότητες. Η τυπική σιγμοειδής συνάρτηση είναι η λογιστική συνάρτηση, που ορίζεται ως

$$g(x) = \frac{1}{(1 + \exp(-\lambda_1 x))},$$

όπου λ_1 είναι η παράμετρος κλίσης της συνάρτησης.

2.2.2 Αρχιτεκτονική ενός Τεχνητού Νευρωνικού Δικτύου

Η σύνδεση πολλών νευρώνων μεταξύ τους αποτελεί ένα ΤΝΔ. Τα ΤΝΔ μπορούν να θεωρηθούν ως κατευθυνόμενοι γράφοι με βάρη στα οποία οι κόμβοι είναι τεχνητοί νευρώνες και οι κατευθυνόμενες ακμές (με βάρη) είναι συνδέσεις από τις εξόδους των νευρώνων στις εισόδους των νευρώνων. Ανάλογα με τον τρόπο σύνδεσης των νευρώνων (αρχιτεκτονική), τα ΤΝΔ μπορούν να ομαδοποιηθούν σε δύο μεγάλες κατηγορίες:

(α) τα ΤΝΔ εμπρόσθιας τροφοδότησης, στα οποία δεν υπάρχουν κλειστοί βρόγχοι στο γράφο, και

(β) στα feedback (recurrent) ΤΝΔ, στα οποία υπάρχουν κλειστοί βρόχοι προς τα πίσω τροφοδότησης.

Η πιο κοινή οικογένεια ΤΝΔ εμπρόσθιας τροφοδότησης είναι τα στρωματοποιημένα δίκτυα (layered networks) στα οποία οι νευρώνες οργανώνονται σε στρώματα με συνδέσεις αυστηρά από ένα στρώμα σε ένα άλλο. Γενικότερα, όλα τα δίκτυα που δεν περιέχουν κλειστούς βρόγχους μπορούν να αναδιαταχθούν σε μορφή στρωματοποιημένων δικτύων πρόσθιας τροφοδότησης (όχι απαραίτητα πλήρως διασυνδεδεμένων). Τα τυπικά δίκτυα αυτής της κατηγορίας είναι τα μονοστρωματικά perceptrons, τα πολυστρωματικά perceptrons και τα Radial Basis Function δίκτυα. Αντίστοιχα, τα τυπικά δίκτυα της κατηγορίας των feedback δικτύων είναι τα Competitive δίκτυα, τα δίκτυα Hopfield και τα Kohonen's SOMs.

Διαφορετικές συνδέσεις των δικτύων οδηγούν σε διαφορετική συμπεριφορά. Γενικά, τα δίκτυα πρόσθιας τροφοδότησης είναι στατικά δίκτυα, δηλαδή, δοθείσης μιας εισόδου, παράγουν μόνο ένα σύνολο τιμών εξόδου και όχι μια ακολουθία τιμών. Τα δίκτυα πρόσθιας τροφοδότησης δεν έχουν μνήμη με την έννοια ότι η απόκριση του δικτύου σε μια είσοδο είναι ανεξάρτητη από την προηγούμενη κατάσταση του δικτύου. Μια εξαίρεση αποτελούν τα δίκτυα πρόσθιας τροφοδότησης χρονικής υστέρησης (time delay feedforward networks) στα οποία η δυναμική παρουσιάζεται λόγω των διαφορετικών παραγόντων υστέρησης των νευρώνων στο δίκτυο.

Τα recurrent δίκτυα είναι ουσιαστικά δυναμικά συστήματα. Με την παρουσίαση ενός νέου προτύπου εισόδου, υπολογίζονται οι έξοδοι των νευρώνων. Λόγω των συνδέσεων προς τα πίσω τροφοδότησης, οι είσοδοι σε κάθε νευρώνα τροποποιούνται, γεγονός που οδηγεί το δίκτυο σε μια νέα κατάσταση. Η διαδικασία αυτή επαναλαμβάνεται μέχρι την σύγκλιση. Αυτοί οι δύο διαφορετικοί τύποι δικτύων απαιτούν διαφορετικά μαθηματικά εργαλεία για την διαχείρισή τους, όπως για παράδειγμα η χρήση διαφορικών εξισώσεων για την περιγραφή των δυναμικών συστημάτων.

Οι διαφορετικές αρχιτεκτονικές δικτύων απαιτούν και διαφορετικούς αλγορίθμους εκπαίδευσης. Στην παράγραφο που ακολουθεί δίνονται τα βασικά στοιχεία της διαδικασίας εκπαίδευσης των ΤΝΔ.

2.2.3 Εκπαίδευση των Τεχνητών Νευρωνικών Δικτύων

Η ικανότητα μάθησης είναι ένα θεμελιώδες χαρακτηριστικό της ευφυΐας. Παρότι η έννοια της εκπαίδευσης είναι συχνά δύσκολο να αποδοθεί, η διαδικασία εκπαίδευσης υπό το πλαίσιο των ΤΝΔ μπορεί να περιγραφεί ως το πρόβλημα ενημέρωσης της αρχιτεκτονικής του δικτύου και των βαρών των συνδέσεών του με τέτοιο τρόπο ώστε το δίκτυο να μπορεί να αποδώσει αποτελεσματικά ένα συγκεκριμένο έργο. Τυπικά, η εκπαίδευση των ΤΝΔ πραγματοποιείται με δύο τρόπους. Κάποιες φορές τα βάρη μπορούν να τεθούν a priori από τον σχεδιαστή του δικτύου μέσω κατάλληλης θεώρησης του προβλήματος προς επίλυση. Ωστόσο, τις περισσότερες φορές το δίκτυο πρέπει να «μάθει» τα βάρη των συνδέσεών του από ένα δοθέν σύνολο προτύπων εκπαίδευσης. Η βελτίωση της απόδοσης επιτυγχάνεται με το χρόνο μέσω επαναλαμβανόμενης ανανέωσης των βαρών του δικτύου. Η δυνατότητα των ΤΝΔ αυτόματης εκμάθησης από παραδείγματα αποτελεί ένα από τα μεγαλύτερα πλεονεκτήματά τους σε

σχέση με τα παραδοσιακά expert systems, καθώς δεν χρειάζεται ο καθορισμός ενός συνόλου κανόνων για την αποδοτική λειτουργία τους.

Υπάρχουν τρεις βασικοί τρόποι εκπαίδευσης,

(α) η εκπαίδευση με επίβλεψη,

(β) η εκπαίδευση χωρίς επίβλεψη και

(γ) η υβριδική εκπαίδευση.

Στην εκπαίδευση με επίβλεψη, παρέχεται στο δίκτυο ένα σύνολο προτύπων για εκπαίδευση με τις αντίστοιχες σωστές αποκρίσεις του δικτύου. Στην περίπτωση αυτή τα βάρη καθορίζονται με τέτοιο τρόπο ώστε το δίκτυο να μπορεί να παράγει εξόδους όσο το δυνατόν πιο κοντά στις γνωστές ορθές αποκρίσεις. Η reinforcement εκπαίδευση είναι ειδική περίπτωση της εκπαίδευσης με επίβλεψη, κατά την οποία παρέχονται στο δίκτυο όχι οι σωστές έξοδοι αλλά κρίσεις ως προς την ορθότητα των αποκρίσεών του. Αντιθέτως, η εκπαίδευση χωρίς επίβλεψη δεν απαιτεί την συσχέτιση σωστών εξόδων με τις αντίστοιχες τιμές εισόδου του συνόλου προτύπων εκπαίδευσης, αλλά μελετά την υποκείμενη δομή των δεδομένων εισόδου ή τις συσχετίσεις μεταξύ των προτύπων εισόδου και οργανώνει τα πρότυπα σε κατηγορίες ανάλογα με αυτές τις συσχετίσεις. Η υβριδική εκπαίδευση συνδυάζει την εκπαίδευση με επίβλεψη και χωρίς επίβλεψη. Τυπικά, μια αναλογία βαρών του δικτύου καθορίζονται χρησιμοποιώντας την εκπαίδευση με επίβλεψη ενώ τα υπόλοιπα καθορίζονται από την χωρίς επίβλεψη εκπαίδευση.

Αναφορικά με την εκπαίδευση με επίβλεψη των ΤΝΔ, υπάρχουν τρία θεμελιώδη και πρακτικά ζητήματα που μελετώνται και είναι η μέγιστη ικανότητα του δικτύου να μάθει από τα πρότυπα εκπαίδευσης, το πλήθος των προτύπων που απαιτούνται για την εκπαίδευση και η απαιτούμενη πολυπλοκότητα χρόνου για την εκπαίδευση του δικτύου. Το πρώτο ζήτημα αφορά στο αν η πραγματική λύση περιέχεται στο σύνολο των λύσεων που το δίκτυο μπορεί να παρέχει, δηλαδή αν υπάρχει στον εφικτό χώρο λύσεων του δικτύου. Το πρόβλημα αυτό είναι αρκετά δύσκολο και παραμένει ανοικτό σε αρκετές περιπτώσεις εκπαίδευσης. Η ικανότητα προσέγγισης των ΤΝΔ πρόσθιας τροφοδότησης έχει μελετηθεί αρκετά και ένα από τα πιο θεμελιώδη αποτελέσματα αυτών των ερευνών είναι ότι τα τυπικά δίκτυα πρόσθιας τροφοδότησης με ένα μόνο κρυφό στρώμα μπορούν να προσεγγίσουν οποιαδήποτε συνεχή συνάρτηση ομοιόμορφα σε οποιοδήποτε συμπαγές σύνολο και οποιαδήποτε μετρήσιμη συνάρτηση σε οποιοδήποτε επιθυμητό βαθμό ακρίβειας [73, 215]. Δυστυχώς, οι περισσότερες θεωρητικές μελέτες αγνοούν το πρόβλημα εκπαίδευσης, δηλαδή αν υπάρχει μέθοδος ικανή να εκπαιδεύσει τα βάρη του δικτύου από εμπειρικές παρατηρήσεις των απεικονίσεων.

Το δεύτερο ζήτημα που αφορά στην πολυπλοκότητα του συνόλου προτύπων εκπαίδευσης, καθορίζει των αριθμό των προτύπων που είναι απαραίτητα για την εκπαίδευση του δικτύου ώστε να είναι εγγυημένη η γενίκευσή του. Η ύπαρξη πολύ λίγων προτύπων εκπαίδευσης μπορεί να προκαλέσει πρόβλημα over-fitting κατά το οποίο το δίκτυο αποδίδει καλά στο σύνολο εκπαίδευσης αλλά άσχημα σε ανεξάρτητα πρότυπα ελέγχου τα οποία ωστόσο ανήκουν στην ίδια κατανομή με το σύνολο εκπαίδευσης.

Το τρίτο ζήτημα αφορά στην υπολογιστική πολυπλοκότητα του αλγορίθμου εκπαίδευσης που χρησιμοποιείται για την εκτίμηση μιας λύσης από το σύνολο των προτύπων εκπαίδευσης.

Υπάρχουν τέσσερις βασικοί τύποι κανόνων εκπαίδευσης:

(α) οι κανόνες διόρθωσης σφάλματος (error-correction),

(β) οι κανόνες Boltzmann,

(γ) οι κανόνες Hebbian και

(δ) οι κανόνες competitive learning.

Από τους παραπάνω τύπους, οι κανόνες διόρθωσης σφάλματος είναι οι πλέον χρησιμοποιούμενοι για πολυστρωματικά ΤΝΔ πρόσθιας τροφοδότησης τα οποία θα χρησιμοποιηθούν στα επόμενα κεφάλαια για την επίλυση προβλημάτων κρυπτανάλυσης.

Γενικά, στην εκπαίδευση με επίβλεψη δίνεται στο δίκτυο η επιθυμητή έξοδος για κάθε είσοδο. Κατά τη διαδικασία της εκπαίδευσης, η πραγματική έξοδος, y, που παράγεται από το δίκτυο μπορεί να διαφέρει από την επιθυμητή έξοδο, d. Η βασική αρχή των κανόνων εκπαίδευσης διόρθωσης σφάλματος είναι η χρήση του σφάλματος $(d - y)$ για την μεταβολή των βαρών του δικτύου με τέτοιο τρόπο ώστε το σφάλμα αυτό σταδιακά να μειωθεί.

Για παράδειγμα, ο κανόνας εκπαίδευσης του perceptron βασίζεται στην αρχή της διόρθωσης του σφάλματος. Ένα δίκτυο perceptron αποτελείται από έναν νευρώνα με μεταβλητά βάρη, $w_j, j = 1, 2, \ldots, n$, και κατώφλι μ. Δοθέντος ενός διανύσματος $\mathbf{x} = (x_1, x_2, \ldots, x_n)^\top$, η είσοδος του δικτύου είναι

$$v = \sum_{j=1}^{n} w_j x_j - \mu.$$

Η έξοδος y του perceptron είναι $(+1)$ αν $v > 0$, και 0 αλλιώς. Σε ένα πρόβλημα κατηγοριοποίησης σε δύο κλάσεις, το perceptron αντιστοιχεί ένα πρότυπο εισόδου σε μια κλάση αν $y = 1$, και στην άλλη κλάση αν $y = 0$. Η γραμμική εξίσωση

$$\sum_{j=1}^{n} w_j x_j - \mu = 0,$$

ορίζει το σύνολο συνοριακών τιμών (ένα υπερεπίπεδο στον n-διάστατο χώρο εισόδων) το οποίο διαιρεί το χώρο σε δύο τμήματα.

Ο Rosenblatt [179] ανέπτυξε μια διαδικασία εκπαίδευσης για τον καθορισμό των βαρών και του κατωφλιού σε ένα perceptron, δοθέντος ενός συνόλου προτύπων εκπαίδευσης. Η διαδικασία αυτή περιγράφεται στον Πίνακα 2.7.

Πίνακας 2.7: Η διαδικασία εκπαίδευσης ενός δικτύου perceptron.

1. Αρχικοποίησε τα βάρη και το κατώφλι σε μικρές τυχαίες τιμές.
2. Δώσε ως είσοδο στο δίκτυο ένα διάνυσμα εισόδου $(x_1, x_2, \ldots, x_n)^T$, και υπολόγισε την έξοδο του νευρώνα.
3. Ενημέρωσε τις τιμές των βαρών σύμφωνα με την σχέση

   $$w_j(t + 1) = w_j(t) + \eta(d - y)x_j,$$

   όπου d είναι η επιθυμητή έξοδος, t είναι ο αριθμός των επαναλήψεων, και η $(0 < \eta < 1)$ είναι το μήκος του βήματος.

Η εκπαίδευση πραγματοποιείται μόνο όταν υπάρχει σφάλμα από το δίκτυο. Ο Rosenblatt απέδειξε ότι αν τα πρότυπα εισόδου είναι από δύο γραμμικά ανεξάρτητες κλάσεις, τότε η διαδικασία εκπαίδευσης του perceptron θα συγκλίνει μετά από πεπερασμένο αριθμό επαναλήψεων (Θεώρημα σύγκλισης του perceptron). Έχουν προταθεί πολλές παραλλαγές αυτού του αλγορίθμου εκπαίδευσης [71]. Επίσης μπορούν να χρησιμοποιηθούν άλλες συναρτήσεις ενεργοποίησης που οδηγούν σε διαφορετικά χαρακτηριστικά εκπαίδευσης. Ωστόσο, ένα perceptron ενός μόνο στρώματος μπορεί να διαχωρίσει μόνο γραμμικά διαχωρίσιμα πρότυπα,

εφόσον χρησιμοποιεί μια μονότονη συνάρτηση ενεργοποίησης. Μια μη-μονότονη συνάρτηση ενεργοποίησης, όπως για παράδειγμα η συνάρτηση Gauss, μπορεί να διαμορφώσει μη-γραμμικά συνοριακά σύνολα.

Ο αλγόριθμος εκπαίδευσης της οπισθοδρομικής μετάδοσης του σφάλματος (backpropagation), ο οποίος είναι από τους πλέον διαδεδομένους αλγορίθμους εκπαίδευσης ΤΝΔ ανήκει επίσης στην κατηγορία διόρθωσης σφάλματος.

2.2.4 Πολυστρωματικά Τεχνητά Νευρωνικά Δίκτυα πρόσθιας τροφοδότησης

Τα πολυστρωματικά ΤΝΔ πρόσθιας τροφοδότησης είναι τα πιο συχνά χρησιμοποιούμενα ΤΝΔ. Ένα δίκτυο πρόσθιας τροφοδότησης είναι ένα δίκτυο με ακυκλικές και μονόδρομες κατευθυνόμενες συνδέσεις μεταξύ των νευρώνων, και στο οποίο οι νευρώνες μπορούν να ομαδοποιηθούν σε στρώματα. Κατά συνέπεια, η τοπολογία του δικτύου μπορεί να περιγραφεί με μια σειρά ακέραιων αριθμών που αναπαριστούν το πλήθος των νευρώνων που ανήκουν στο αντίστοιχο στρώμα.

Έχει αποδειχθεί ότι τα πολυστρωματικά δίκτυα πρόσθιας τροφοδότησης είναι ικανά να διαμορφώσουν οποιαδήποτε σύνθετα συνοριακά φράγματα και να αναπαραστήσουν κάθε συνάρτηση Boole [140]. Επίσης έχει αποδειχθεί ότι ένα δίκτυο πρόσθιας τροφοδότησης με ένα κρυφό στρώμα και έναν σταθερό αριθμό νευρώνων στο κρυφό στρώμα, έχει ένα κατώτερο φράγμα στο βαθμό προσέγγισης οποιασδήποτε συνάρτησης [165]. Το πρόβλημα του κάτω φράγματος μπορεί να εξαλειφθεί αν χρησιμοποιηθούν περισσότερα κρυφά στρώματα. Οι Mairov και Pinkus στην εργασία [165] απέδειξαν ότι στον μοναδιαίο κύβο στον χώρο $\mathbb{R}^n$ οποιαδήποτε συνεχής συνάρτηση μπορεί να προσεγγιστεί ομοιόμορφα, ως προς οποιοδήποτε σφάλμα χρησιμοποιώντας ένα δίκτυο με δύο κρυφά στρώματα και $2n+1$ νευρώνες στο πρώτο στρώμα και $4n+3$ νευρώνες στο δεύτερο στρώμα. Επιπλέον, ο Anthony στην εργασία [9] απέδειξε ότι υπάρχει ένα δίκτυο με δύο στρώματα και συνάρτηση ενεργοποίησης το κατώφλι ικανό να υπολογίσει οποιαδήποτε συνάρτηση Boole.

Η ανάπτυξη του αλγορίθμου εκπαίδευσης της οπισθοδρομικής μετάδοσης του σφάλματος (backpropagation) για τα πολυστρωματικά δίκτυα πρόσθιας τροφοδότησης κατέστησε τα δίκτυα αυτά ως τα πλέον γνωστά από όλα τα δίκτυα.

Γενικά, ένα τυπικό ΤΝΔ πρόσθιας τροφοδότησης με L στρώματα, αποτελείται από ένα στρώμα εισόδου, $L-1$ κρυφά (ενδιάμεσα) στρώματα, και ένα στρώμα εξόδου, με νευρώνες οι οποίοι είναι διαδοχικά συνδεδεμένοι (πλήρως ή μερικώς) με πρόσθια κατεύθυνση, χωρίς συνδέσεις μεταξύ των νευρώνων του ίδιου στρώματος και χωρίς συνδέσεις ανάδρασης μεταξύ των στρωμάτων. Συμβολίζουμε με $w_{ij}^{(l)}$ το βάρος της σύνδεσης μεταξύ του i-οστού νευρώνα του στρώματος $(l-1)$ και του j-οστού νευρώνα του στρώματος l. Ο στόχος ενός αλγορίθμου εκπαίδευσης είναι ο προσδιορισμός των βαρών του δικτύου με τέτοιο τρόπο ώστε να ελαχιστοποιείται μια συγκεκριμένη συνάρτηση κόστους.

Έστω $\{(\mathbf{x}^{(1)}, \mathbf{d}^{(1)}), (\mathbf{x}^{(2)}, \mathbf{d}^{(2)}), \ldots, (\mathbf{x}^{(p)}, \mathbf{d}^{(p)})\}$ ένα σύνολο p προτύπων εκπαίδευσης (δηλαδή ζεύγη εισόδων - εξόδων), όπου $\mathbf{x}^{(i)} \in \mathbb{R}^n$ είναι το διάνυσμα εισόδου στον n-διάστατο χώρο, και $\mathbf{d}^{(i)} \in [0,1]^m$ είναι το επιθυμητό διάνυσμα εξόδου στον m-διάστατο υπερκύβο. Σε περιπτώσεις προβλημάτων κατηγοριοποίησης το m τίθεται ίσο με το πλήθος των κλάσεων. Η τετραγωνική συνάρτηση σφάλματος, η οποία συνήθως χρησιμοποιείται για τα ΤΝΔ στην βιβλιογραφία, ορίζεται ως

$$E = \frac{1}{2} \sum_{i=1}^{p} \left\| \mathbf{y}^{(i)} - \mathbf{d}^{(i)} \right\|^2.$$

Η αλγόριθμος της οπισθοδρομικής μετάδοσης του σφάλματος είναι μια μέθοδος μείωσης της κλίσης για την ελαχιστοποίηση της παραπάνω συνάρτησης κόστους, και μπορεί να περιγραφεί όπως δίνεται στον Πίνακα 2.8 [76].

Πίνακας 2.8: Ο αλγόριθμος της οπισθοδρομικής μετάδοσης του σφάλματος.

1. Αρχικοποίησε τα βάρη σε μικρές τυχαίες τιμές
2. Επέλεξε τυχαία ένα πρότυπο εισόδου $\mathbf{x}^{(\mu)}$
3. Μετάδωσε το σήμα μπροστά μέσω του δικτύου
4. Υπολόγισε το δ_i^L στο στρώμα εξόδου, όπου

$$\delta_i^L = g'(h_i^L)[d_i^\mu - y_i^L],$$

όπου το h_i^l αναπαριστά την είσοδο του δικτύου στον i-οστό νευρώνα του l-οστού στρώματος.

5. Υπολόγισε τα αντίστοιχα δ για τα προηγούμενα στρώματα μεταδίδοντας τα σφάλματα προς τα πίσω, δηλαδή

$$\delta_i^l = g'(h_i^l) \sum_j w_{ij}^{l+1} \delta_j^{l+1},$$

για $l = (L-1), \ldots, 1$.

6. Ανανέωσε τα βάρη χρησιμοποιώντας την σχέση

$$\Delta w_{ji}^l = \eta \delta_i$$

7. Πήγαινε στο βήμα 2 και επανέλαβε για το επόμενο πρότυπο εισόδου μέχρι το σφάλμα στο στρώμα εξόδου να γίνει μικρότερο από ένα προκαθορισμένο κατώφλι ή μέχρι να πραγματοποιηθεί το μέγιστο πλήθος επιτρεπτών επαναλήψεων.

Υπάρχουν πολλά ανοικτά θέματα για τον σχεδιασμό των ΤΝΔ πρόσθιας τροφοδότησης. Μερικά από αυτά είναι η επιλογή του πλήθους των στρωμάτων που απαιτούνται για ένα δοθέν πρόβλημα, ο αριθμός των νευρώνων ανά στρώμα και το κατάλληλο μέγεθος του συνόλου εκπαίδευσης ώστε να επιτρέπει την καλή γενίκευση του δικτύου. Παρότι τα ΤΝΔ πρόσθιας τροφοδότησης με την μέθοδο της οπισθοδρομικής μετάδοσης του σφάλματος έχουν χρησιμοποιηθεί ευρέως για προβλήματα κατηγοριοποίησης και προσέγγισης συναρτήσεων, υπάρχουν πάντα πολλοί παράγοντες σχεδιασμού του δικτύου που πρέπει να καθοριστούν με μια μέθοδο δοκιμής και διόρθωσης. Για το λόγο αυτό, κατά την επίλυση ενός προβλήματος με τη χρήση ΤΝΔ δοκιμάζονται διάφορες αρχιτεκτονικές δικτύου, σύνολα προτύπων εκπαίδευσης αλλά και διαφορετικές μέθοδοι εκπαίδευσης προκειμένου να δοθεί μια ολοκληρωμένη εικόνα για την απόδοση των ΤΝΔ στο συγκεκριμένο πρόβλημα.

Εκτός από την τυπική μέθοδο της οπισθοδρομικής μετάδοσης του σφάλματος [181] έχουν αναπτυχθεί και παραλλαγές αυτής, όπως η μέθοδος της προς τα πίσω μετάδοσης με μεταβλητό μέγεθος βήματος [117], η μέθοδος Resilient Backpropagation [176] και η Online Adaptive Backpropagation [116], καθώς και άλλες μέθοδοι εκπαίδευσης που βασίζονται στην μείωση της κλίση της συνάρτησης κόστους, όπως η Scaled Conjugate Gradient μέθοδος [143]. Επίσης, τα τελευταία χρόνια αξιοποιούνται σημαντικά για την εκπαίδευση των ΤΝΔ και μέθοδοι που δεν απαιτούν τον υπολογισμό της κλίσης της συνάρτησης κόστους και κατά συνέπεια επι-

τρέπουν την χρήση και διαφορετικών συναρτήσεων κόστους με όχι τόσο «καλές» μαθηματικές ιδιότητες. Οι μέθοδοι αυτές είναι οι μέθοδοι Εξελικτικού Υπολογισμού.

2.3 Η Υπολογιστική Νοημοσύνη στην κρυπτολογία

Τα τελευταία χρόνια τεχνικές της Υπολογιστικής Νοημοσύνης εμφανίζονται όλο και πιο συχνά στην επιστημονική περιοχή της ασφάλειας υπολογιστών αλλά και στην πολύ απαιτητική περιοχή της κρυπτολογίας [75]. Αλγόριθμοι που αξιοποιούν μεθοδολογίες προερχόμενες από τον Εξελικτικό Υπολογισμό και τα Τεχνητά Νευρωνικά Δίκτυα έχουν προταθεί για την αντιμετώπιση διαφόρων προβλημάτων κρυπτογραφίας και κρυπτανάλυσης, όπως για παράδειγμα για το σχεδιασμό και την ανάλυση νέων κρυπτογραφικών αρχέτυπων, για γεννήτριες ψευδοτυχαίων αριθμών μέχρι τμηματικά (block) κρυπτοσυστήματα, για την κρυπτανάλυση κλασικών κρυπτοσυστημάτων αλλά και για τον εντοπισμό επιθετικών μοτίβων σε δίκτυα υπολογιστών. Ωστόσο, παρά το αυξανόμενο ενδιαφέρον της επιστημονικής κοινότητας για την εφαρμογή μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτολογία υπάρχει στο πεδίο αυτό ένα σύνολο ανοικτών προβλημάτων που πρέπει να επιλυθούν.

Ένα κρίσιμο σημείο κατά την εφαρμογή μεθόδων Εξελικτικού Υπολογισμού στην κρυπτανάλυση είναι ο ορισμός των αντικειμενικών συναρτήσεων που θα χρησιμοποιηθούν ώστε να αποφευχθεί το πρόβλημα των παραπλανητικών χώρων αναζήτησης των λύσεων (fitness landscapes). Οι χώροι αναζήτησης λύσεων των προβλημάτων που σχετίζονται με τα σύγχρονα κρυπτοσυστήματα είναι σχεδόν κατά κανόνα δελτοειδή και η απευθείας εφαρμογή ευρετικών για την αναζήτηση σε ένα τέτοιο χώρο δεν παράγει απαραίτητα αποτελέσματα καλύτερα από την τυχαία αναζήτηση.

Γενικότερα, μια σημαντική απαίτηση για μια ευρετική μέθοδο βελτιστοποίησης είναι ο τρόπος αξιολόγησης κάθε πιθανής λύσης του προς επίλυση προβλήματος, δηλαδή ο προσδιορισμός της ποιότητάς της. Σε πολλές περιπτώσεις η εύρεση κατάλληλου τρόπου αξιολόγησης είναι το πιο δύσκολο μέρος της επίλυσης ενός συγκεκριμένου προβλήματος και κάποιες φορές είναι ανέφικτο λόγω της φύσης του προβλήματος. Είναι ιδιαίτερα σημαντικό η επιλεγμένη τεχνική αξιολόγησης μιας λύσης να παρέχει ουσιώδη και ακριβή σύγκριση μεταξύ δύο τυχαίων λύσεων. Συγκεκριμένα, η έννοια μιας «καλής» λύσης είναι ανούσια αν δεν είναι δυνατόν να αποφανθούμε αν μια λύση είναι καλύτερη από οποιαδήποτε άλλη. Η μη-ύπαρξη μιας κατάλληλης μεθόδου εκτίμησης στην περίπτωση αυτή σημαίνει ότι ο χώρος των λύσεων μπορεί να θεωρηθεί ως μια επίπεδη επιφάνεια με μια μόνο κορυφή στο σημείο που βρίσκεται το βέλτιστο. Συνεπώς, η εφαρμογή ευρετικών μεθόδων αναζήτησης για επίλυση θα είναι μάταιη καθώς δεν μπορεί να είναι αποτελεσματική.

Τα κλασικά κρυπτοσυστήματα που έχουν κρυπταναλυθεί πλήρως μέχρι σήμερα, έχουν γενικά την ιδιότητα όταν χρησιμοποιούν κλειδιά κρυπτογράφησης/αποκρυπτογράφησης που διαφέρουν λίγο μεταξύ τους να παράγουν κρυπτογραφήματα/αποκρυπτογραφήματα που επίσης διαφέρουν λίγο μεταξύ τους. Κατ' αυτόν τον τρόπο, βοηθούν σημαντικά στον ορισμό των αντικειμενικών συναρτήσεων που μετρούν για παράδειγμα την εγγύτητα ενός δοθέντος κειμένου με την αγγλική γλώσσα. Αντίθετα, τα σύγχρονα κρυπτοσυστήματα δεν εμφανίζουν την προηγούμενη ιδιότητα και αυτό αποτελεί σημαντικό πρόβλημα και αιτία της σχετικής αποτυχίας των εφαρμογών ευρετικών τεχνικών στα κρυπτοσυστήματα αυτά, καθώς δοκιμάζοντας ένα κλειδί που έχει 255 σωστά δυαδικά ψηφία από τα 256, δηλαδή κλειδί σωστό κατά $99,61\%$, αυτό παράγει αποκρυπτογραφημένο κείμενο που μοιάζει εντελώς τυχαίο. Το γεγονός αυτό οφείλεται στο χαρακτηριστικό που ονομάζεται avalanche effect, κατά το οποίο ένα κρυπτοσύστημα είναι ισχυρό όταν μια μικρή αλλαγή στην είσοδό του επιφέρει μεγάλη αλλαγή στην έξοδό του και προέρχεται σαν ιδέα από τη θεωρία διάχυσης του Shannon [190].

Η παραπάνω ιδιότητα των σύγχρονων κρυπτοσυστημάτων (avalanche effect), σε συνδυασμό με την απαίτηση των ευρετικών μεθόδων για ουσιώδη και ακριβή μέθοδο εκτίμησης των διαφόρων πιθανών λύσεων συνεπάγεται ότι η αντιμετώπιση προβλημάτων κρυπτολογίας με

μεθόδους Εξελικτικού Υπολογισμού είναι ιδιαίτερα δύσκολη λόγω της φύσης των προβλημάτων αυτών και εξαρτάται σημαντικά από την ύπαρξη και δημιουργία κατάλληλης μεθόδου αξιολόγησης των πιθανών λύσεων.

Μέχρι τώρα, δύο κύριες εφαρμογές των μεθόδων Εξελικτικού Υπολογισμού έχουν μελετηθεί ιδιαίτερα και είναι ο σχεδιασμός καλών γεννητριών ψευδοτυχαίων αριθμών και ο σχεδιασμός S-boxes για τμηματικά (block) κρυπτοσυστήματα. Το πρώτο πρόβλημα είναι αρκετά απατηλό καθώς όλες οι τεχνικές που έχουν ερευνηθεί βασίζονται στην χρήση γεννητριών με αντικειμενική συνάρτηση που μετριέται παρατηρώντας τις ψευδοτυχαίες ιδιότητες τμήματος των εξόδων τους. Αυτή η μέθοδος μέτρησης της τυχαιότητας όμως είναι αρκετά παραπλανητική καθώς για να είναι καλή μια γεννήτρια πρέπει συνήθως να έχει μια πολύ μακρά περίοδο και στις μελέτες αυτές μπορεί κανείς να παρατηρήσει αποτελεσματικά μόνο ένα μικρό τμήμα της. Επίσης, η χρήση αυτής της τεχνικής μέτρησης χαρακτηρίζεται πλέον ως πολύ περιορισμένη κυρίως επειδή η τυχαιότητα είναι μια αόριστη έννοια η οποία δεν έχει έναν αποδοτικά μετρήσιμο ορισμό. Αυτός είναι και ο λόγος που τα τελευταία χρόνια αυτός ο ερευνητικός τομέας εστιάζει στην δημιουργία καλών γεννητριών ψευδοτυχαίων αριθμών για συγκεκριμένες εφαρμογές όπου οι απαιτούμενες ιδιότητες της γεννήτριας είναι γνωστές και εύκολα μετρήσιμες, εγκαταλείποντας την ιδέα της δημιουργίας καλών γεννητριών για κάθε περίπτωση.

Το δεύτερο πρόβλημα σε αντίθεση με ότι αναμενόταν παρουσιάζει μεγάλη επιτυχία. Ο σχεδιασμός S-boxes είναι ένα κρίσιμο στοιχείο για την κατασκευή των τμηματικών (block) κρυπτοσυστημάτων. Κατά την κατασκευή ενός νέου block κρυπτοσυστήματος πολλοί ερευνητές ακολουθούν τις συστάσεις των κρυπτοσυστημάτων Feistel. Τα κρυπτοσυστήματα Feistel είναι πολλά και μπορεί όχι βέλτιστα αλλά αρκετά σθεναρά. Από το πρωταρχικό DES μέχρι το πρόσφατο CAST-256, οι περισσότεροι σχεδιαστές τμηματικών κρυπτοσυστημάτων προτιμούν αυτού του είδους τα σχήματα λόγω της απλότητάς τους, των καλών ιδιοτήτων τους και την σθεναρότητά τους που είναι εγγυημένη από την πολύχρονη και εξαντλητική δοκιμή τους. Συνεπώς, η ύπαρξη καλών αλγορίθμων για την αυτοματοποιημένη δημιουργία S-boxes δίνει την δυνατότητα για αυτοματοποιημένη δημιουργία καλών νέων τμηματικών κρυπτοσυστημάτων και αυτή είναι η αιτία για το αυξανόμενο ενδιαφέρον στο πεδίο αυτό.

Η χρήση αυτοματοποιημένων τεχνικών για τον σχεδιασμό κρυπτογραφικών συναρτήσεων και κρυπτοσυστημάτων γενικότερα, αποτελεί ένα σημαντικό κίνητρο για την εφαρμογή των μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτογραφία. Τα περισσότερα κρυπτοσυστήματα αποτελούνται από συνδυασμό ενός πλήθους σχετικά απλών λειτουργιών και ένα μεγάλο μέρος της επιστημονικής έρευνας έχει πραγματοποιηθεί για τον προσδιορισμό καλών κρυπτογραφικών ιδιοτήτων αυτών των λειτουργιών. Οι αυτοματοποιημένες ευρετικές τεχνικές αναζήτησης μπορούν να εφαρμοστούν για την γρήγορη αναζήτηση ενός μεγάλου πλήθους δυνατών κρυπτογραφικών λειτουργιών ώστε να βρουν ποιες από αυτές ικανοποιούν τις επιθυμητές ιδιότητες.

Η χρήση αυτοματοποιημένων τεχνικών για την κρυπτανάλυση κρυπτοσυστημάτων είναι επίσης πολύ σημαντικό κίνητρο για την εφαρμογή των ερευτικών μεθόδων στον τομέα αυτό, καθώς αφαιρεί την ανάγκη για ανθρώπινη αλληλεπίδραση με την διαδικασία αναζήτησης που είναι αρκετά χρονοβόρα. Λόγω της πολυπλοκότητας των κρυπτοσυστημάτων η εύρεση αδυναμιών σε αυτά είναι γενικά επίπονο χειρωνακτικό έργο και η διαδικασία αξιοποίησης των αδυναμιών των κρυπτοσυστημάτων είναι σπάνια γρήγορη και απλή ακόμα και όταν χρησιμοποιούνται οι υπολογιστές για την υλοποίηση της αξιοποίησης (εκτός από περιπτώσεις κρυπτοσυστημάτων με σημαντικά ελαττώματα). Καθώς όμως η ισχύς επεξεργασίας των υπολογιστών συνεχώς αυξάνεται και τα κατανεμημένα υπολογιστικά συστήματα γίνονται ολοένα και επικρατέστερα, αυτοματοποιημένες τεχνικές ανάλυσης μπορούν να εφαρμοστούν γρήγορα σε μεγάλο αριθμό πιθανών λύσεων ώστε να αποκλειστούν άμεσα «κακές» υποψήφιες λύσεις.

Τέλος, οι ευρετικές μέθοδοι βελτιστοποίησης και η παράλληλη υλοποίησή τους μπορεί να βελτιώσει δραματικά την απόδοση και να αυξήσει την συνολική αποτελεσματικότητα μεγάλου εύρους κρυπταναλυτικών επιθέσεων δημιουργώντας νέες συνδυαστικές μεθοδολογίες κρυπτανάλυσης.

ΚΕΦΑΛΑΙΟ 3

Κρυπτογραφία και Κρυπτανάλυση με μεθόδους Εξελικτικού Υπολογισμού

Σε αυτό το κεφάλαιο παρουσιάζουμε τη μελέτη διαφορετικών προβλημάτων κρυπτογραφίας και κρυπτανάλυσης με τη χρήση μεθόδων Εξελικτικού Υπολογισμού (ΕΥ). Αρχικά, τέσσερα προβλήματα κρυπτογραφίας κλασικών κρυπτοσυστημάτων δημοσίου κλειδιού μετασχηματίζονται σε προβλήματα διακριτής βελτιστοποίησης και εφαρμόζονται μέθοδοι ΕΥ για την επίλυσή τους. Στη συνέχεια, η μερική κρυπτανάλυση κρυπτοσυστημάτων Feistel διαφορετικού πλήθους γύρων μοντελοποιείται ως πρόβλημα βελτιστοποίησης και επιλύεται με μεθόδους ΕΥ. Τέλος, οι μέθοδοι ΕΥ εφαρμόζονται για την κατασκευή κρυπτογραφικά ισχυρών S-boxes.

3.1 Εξελικτικός Υπολογισμός και κρυπτολογία

Ως πρόδρομος της εφαρμογής των μεθόδων Εξελικτικού Υπολογισμού (ΕΥ) στην κρυπτανάλυση μπορούν να θεωρηθούν οι εργασίες των Peleg και Rosenfeld [163] το 1979, των Hunter και McKenzie [74] το 1983, των Carrol και Martin [24] το 1986 και των King και Bahler [85] το 1992. Στις εργασίες αυτές χρησιμοποιήθηκαν για πρώτη φορά αυτοματοποιημένες ευρετικές μέθοδοι για κρυπτανάλυση και πιο συγκεκριμένα αλγόριθμοι χαλάρωσης (relaxation algorithms) για την κρυπτανάλυση κρυπτογραφημάτων απλής αντικατάστασης. Το 1993 οι Spillman *et al.* [199,200] και ο Mathews [118] εισήγαγαν την χρήση γενετικών αλγορίθμων για την επίλυση προβλημάτων απλής αντικατάστασης, μετάθεσης και knapsack κρυπτογραφημάτων, ενώ επίσης την ίδια χρονιά προτάθηκε από τους Forsyth και Safavi-Naini [61] η χρήση της μεθόδου προσομοιωμένης ανόπτησης (simulated annealing) για την αντιμετώπιση κρυπτογραφημάτων απλής αντικατάστασης.

Το 1995 ο Jakobsen [77] πρότεινε μερικές απλοποιημένες *τεχνικές ανάβασης λόφου* (hill-climbing) για την επίλυση των προβλημάτων των εργασιών [61,200] και το 1996 οι Vertan και Geangala [205] χρησιμοποίησαν γενετικούς αλγορίθμους για την κρυπτανάλυση του Merkle–Hellman κρυπτοσυστήματος. Επίσης, το 1997 οι Bagnall *et al.* [11] παρουσίασαν μια επίθεση μόνο με κρυπτογράφημα (ciphertext-only) για μια απλοποιημένη εκδοχή του κρυπτοσυστήματος Αίνιγμα (Enigma rotor machine) χρησιμοποιώντας γενετικούς αλγόριθμους.

Το 1998 ο A. Clark δημοσίευσε την διατριβή του [31] με τίτλο «Optimization Heuristics for Cryptology» στην οποία εισήγαγε την χρήση της μεθόδου *αποτρεπτικής αναζήτησης* (tabu search) για κρυπτανάλυση, σύγκρινε διάφορες ευρετικές τεχνικές, συμπεριλαμβανομένων των γενετικών αλγορίθμων, για την κρυπτανάλυση κλασικών κρυπτοσυστημάτων και απέδειξε ότι η επίθεση στα knapsack κρυπτογραφήματα της εργασίας [199] ήταν ελλιπής. Επίσης, οι Millan, A. Clark και Dawson πρότειναν την κατασκευή συναρτήσεων Boole με καλές κρυπτογραφικές ιδιότητες αξιοποιώντας ευφυείς τεχνικές ανάβασης λόφου και γενετικούς αλγόριθμους [136–138].

Συνεχίζοντας την έρευνα των Millan, A. Clark και Dawson, οι J. Clark και Jacob παρουσίασαν το 2000 στην εργασία [32] μια μεθοδολογία με δύο επίπεδα βελτιστοποίησης για τη δημιουργία συναρτήσεων Boole και πιο πρόσφατα πρότειναν νέες τεχνικές επίθεσης σε σχήματα αναγνώρισης (identification schemes) χρησιμοποιώντας την μέθοδο της προσομοιωμένης

ανόπτησης [33].

Το 2001, οι Burnett *et al.* στην εργασία [22] σχεδίασαν τα S-boxes για το κρυπτοσύστημα MARS, το οποίο ήταν μεταξύ των πέντε υποψήφιων κρυπτοσυστημάτων AES, χρησιμοποιώντας γενετικούς αλγορίθμους και τεχνικές ανάβασης λόφου. Το 2002 οι Hernández *et al.* πρότειναν μια νέα τεχνική κρυπτανάλυσης για το κρυπτοσύστημα TEA με μειωμένο αριθμό γύρων, εφαρμόζοντας γενετικούς αλγορίθμους [69,70]. Η τεχνική αυτή χρησιμοποιήθηκε επίσης για τον διαχωρισμό ενός κρυπτογραφήματος τμηματικής κρυπτογράφησης από μια τυχαία μετάθεση.

Επίσης, το 2004, οι J. Clark, Jacob και Stepney στη μελέτη [34] όρισαν νέες συναρτήσεις κόστους για προβλήματα κρυπτογραφίας, ενώ στην εργασία [35] βελτίωσαν τον σχεδιασμό μικρών S-boxes με τη χρήση της μεθόδου προσομοιωμένης ανόπτησης. Τέλος, οι Barbieri *et al.* περιέγραψαν μια μέθοδο για την κατασκευή καλών γραμμικών κωδίκων διόρθωσης σφαλμάτων σε block μορφή (linear block error-correcting codes) που χρησιμοποιεί γενετικούς αλγορίθμους [12], ακολουθώντας την ιδέα για την δημιουργία κωδίκων με χρήση γενετικών των Dontas και Jong [47].

3.2 Προβλήματα κρυπτογραφίας ως προβλήματα διακριτής βελτιστοποίησης

Στην παρούσα ενότητα μετασχηματίζουμε τέσσερα προβλήματα από το χώρο της κρυπτογραφίας σε προβλήματα διακριτής βελτιστοποίησης. Στη συνέχεια θεωρούμε δύο μεθόδους ΕΥ, και πιο συγκεκριμένα την μέθοδο βελτιστοποίησης με σμήνος σωματιδίων (ΒΣΣ) και την μέθοδο διαφορικής εξέλιξης (ΔΕ), για την αντιμετώπιση τεσσάρων προβλημάτων [106, 108].

Τα πειραματικά αποτελέσματα δείχνουν ότι ο μετασχηματισμός των προβλημάτων σε προβλήματα διακριτής βελτιστοποίησης διατηρεί την πολυπλοκότητά τους καθιστώντας δύσκολη για τις μεθόδους την εξόρυξη πληροφοριών για τη δυναμική των υπό μελέτη συναρτήσεων [106, 108]. Το γεγονός αυτό υποδεικνύει ότι ένα κρίσιμο στοιχείο για την εφαρμογή των μεθόδων ΕΥ στην κρυπτανάλυση είναι ο ορισμός κατάλληλης αντικειμενικής συνάρτησης, δηλαδή η αποφυγή παραπλανητικών χώρων αναζήτησης οι οποίοι οδηγούν σε αποτελέσματα που δεν είναι καλύτερα από αυτά της τυχαίας αναζήτησης. Το θέμα αυτό επισημάνθηκε επίσης αργότερα στην εργασία [75].

Το πρώτο συμπέρασμα που συνάγεται από τα πειράματα αυτά είναι ότι, λόγω της αποδεδειγμένης πολυπλοκότητας των κρυπτογραφικών προβλημάτων, όταν οι μέθοδοι ΕΥ εφαρμόζονται στην κρυπτανάλυση θα πρέπει να δίνεται ιδιαίτερη προσοχή στη δημιουργία της αντικειμενικής συνάρτησης έτσι ώστε αυτή να εμπεριέχει όσο το δυνατόν περισσότερη πληροφορία για το προς επίλυση πρόβλημα. Το δεύτερο συμπέρασμα είναι ότι οι μέθοδοι ΕΥ, αλλά και οι μέθοδοι Υπολογιστικής Νοημοσύνης γενικότερα, μπορούν να χρησιμοποιηθούν ως ένα γρήγορο και πρακτικό μέτρο της αποτελεσματικότητας και της αξιοπιστίας προτεινόμενων κρυπτογραφικών συστημάτων. Πιο συγκεκριμένα, οι μέθοδοι αυτές δείχνουν να μπορούν να εντοπίσουν γρήγορα ασθενή κρυπτογραφικά σχήματα και κατά συνέπεια μπορούν να χρησιμοποιηθούν για αυτό το σκοπό σαν ένα πρώτο μέτρο σθεναρότητας πριν από άλλες πιο σύνθετες μεθόδους ανάλυσης κρυπτοσυστημάτων.

3.2.1 Θεώρηση των υπό μελέτη προβλημάτων

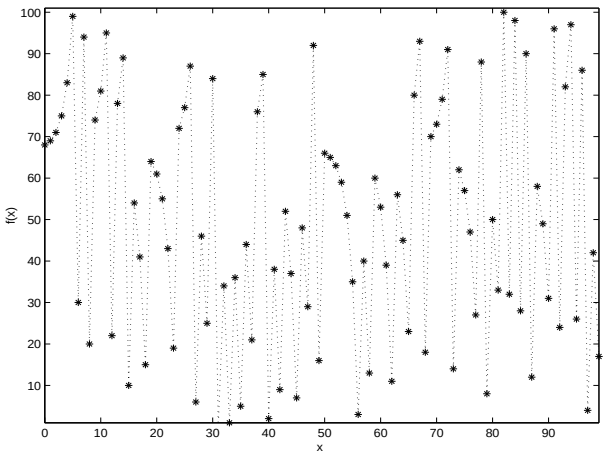
Το πρώτο πρόβλημα που θεωρούμε σε αυτή την ενότητα προέρχεται από το πρόβλημα του διακριτού λογαρίθμου (ΠΔΛ), ενώ τα υπόλοιπα τρία προκύπτουν από το πρόβλημα της παραγοντοποίησης. Πιο συγκεκριμένα, το πρώτο πρόβλημα αφορά στο πρόβλημα του διακριτού λογαρίθμου, το οποίο μπορεί να μετασχηματιστεί σε ελαχιστοποίηση της συνάρτησης

$$f : \mathbb{Z}_p^* \mapsto \{0, 1, \ldots, p-1\},$$

όπου

$$f(x) = \alpha^x - \beta \pmod{p},$$

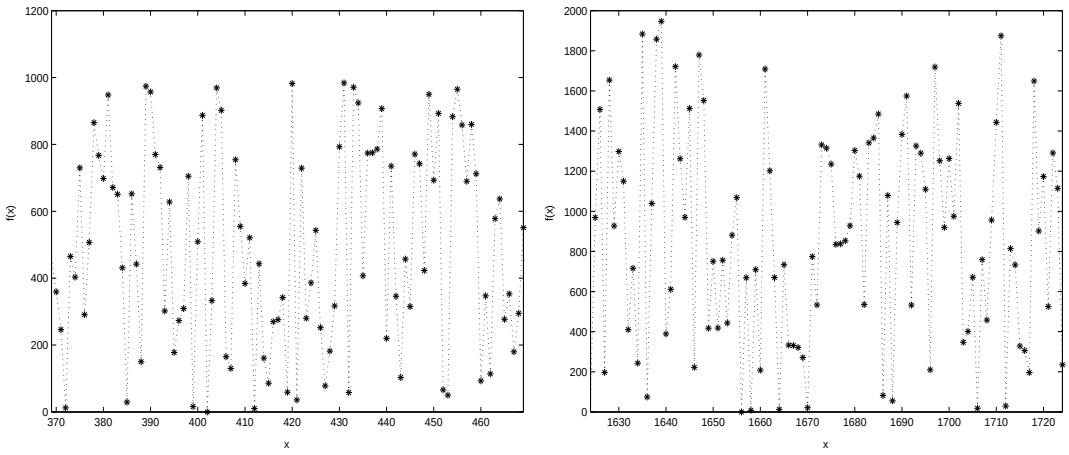
p είναι ένας δοθείς πρώτος αριθμός, α είναι ο γεννήτορας του συνόλου $\mathbb{Z}_p^*$ και το $\beta \in \mathbb{Z}_p^*$ επίσης δίνεται. Στη συνέχεια θα αναφερόμαστε στο πρόβλημα της ελαχιστοποίησης της συνάρτησης f ως **Πρόβλημα 1**. Το ολικό ελάχιστο της συνάρτησης f είναι το μηδέν και ο αντίστοιχος καθολικός ελαχιστοποιητής είναι ο διακριτός λογάριθμος του β ως προς βάση τη α modulo p. Με τον τρόπο αυτό το πρόβλημα του διακριτού λογαρίθμου μετασχηματίζεται σε πρόβλημα ακέραιου προγραμματισμού σε ένα φραγμένο σύνολο. Ο καθολικός ελαχιστοποιητής της συνάρτησης f είναι μοναδικός καθώς το α είναι γεννήτορας. Σημειώνουμε ότι η τιμή της συνάρτησης f για δοθέν x μπορεί να υπολογιστεί εύκολα μέσω του αλγορίθμου επαναλαμβανόμενου τετραγωνισμού και πολλαπλασιασμού για εκθετοποίηση στο χώρο $\mathbb{Z}_n$ (square-and-multiply algorithm). Παρότι το πρόβλημα του διακριτού λογαρίθμου μπορεί να θεωρηθεί ως μονοδιάστατο πρόβλημα ελαχιστοποίησης, δεν είναι ένα εύκολο πρόβλημα προς επίλυση. Η συνάρτηση f που παράγεται από το πρόβλημα του διακριτού λογαρίθμου παρουσιάζει πολύπλοκη συμπεριφορά. Επιπλέον, η ασφάλεια των κρυπτοσυστημάτων που βασίζονται στο ΠΔΛ απαιτεί τη χρήση μεγάλων κλειδιών κρυπτογράφησης. Το μέγεθος των κλειδιών είναι ανάλογο με το πλήθος των ψηφίων του πρώτου αριθμού p του ΠΔΛ. Για το λόγο αυτό στην ελαχιστοποίηση της συνάρτησης f ενδιαφερόμαστε περισσότερο για μεγάλους πρώτους αριθμούς p, γεγονός που καθιστά την διαδικασία της επίλυσης αρκετά δύσκολη. Ένας αλγόριθμος βελτιστοποίησης ικανός για την εύρεση του ολικού ελαχίστου της συνάρτησης f για μεγάλους πρώτους αριθμούς p με χαμηλό κόστος, επαρκεί για την κρυπτανάλυση όλων των κρυπτοσυστημάτων που βασίζονται στους αντίστοιχους διακριτούς λογαρίθμους. Απεικονίσεις της συνάρτησης f για $p = 101, \alpha = 2, \beta = 34$, $p = 1009, \alpha = 11, \beta = 337$ και $p = 2003, \alpha = 5, \beta = 668$, δίνονται στα Σχήματα 3.1 και 3.2 (α) και (β), αντίστοιχα, όπου οι τιμές της συνάρτησης συμβολίζονται με «∗».



Σχήμα 3.1: Απεικόνιση της συνάρτησης $f(x) = \alpha^x - \beta \pmod{p}$, για $p = 101, \alpha = 2$ και $\beta = 34$.

Το δεύτερο πρόβλημα ορίζεται ως εξής: δοθέντος ενός σύνθετου ακέραιου αριθμού N, να βρεθεί ένα ζεύγος αριθμών $x^2 \equiv y^2 \pmod{N}$, με $x \not\equiv \pm y \pmod{N}$. Το πρόβλημα αυτό είναι ισοδύναμο με την εύρεση μη-τετριμμένων παραγόντων του ακεραίου N, καθώς ο αριθμός N διαιρεί το $x^2 - y^2 = (x - y)(x + y)$, αλλά δεν διαιρεί ούτε το $x - y$ αλλά ούτε και το $x + y$. Επομένως, ο μ.κ.δ.$(x - y, N)$ είναι μη-τετριμμένος παράγοντας του N [130].

Μετασχηματίζουμε το προηγούμενο πρόβλημα σε πρόβλημα διακριτής βελτιστοποίησης ορίζοντας την συνάρτηση ελαχιστοποίησης $F : \{1, 2, \ldots, N-1\} \times \{1, 2, \ldots, N-1\} \mapsto$



Σχήμα 3.2: Απεικόνιση της συνάρτησης $f(x) = \alpha^x - \beta \pmod p$, για $p = 1009, \alpha = 11$ και $\beta = 337$, γύρω από το ολικό ελάχιστο (αριστερά), και για $p = 2003, \alpha = 5$ και $\beta = 668$, γύρω από το ολικό ελάχιστο (δεξιά)

$\{0, 1, \ldots, N-1\}$, με

$$F(x, y) = x^2 - y^2 \pmod N, \tag{3.1}$$

υπό τους περιορισμούς $x \neq \pm y \pmod N$. Ο περιορισμός $x \equiv -y \pmod N$ μπορεί να ενσωματωθεί στο πρόβλημα αλλάζοντας το πεδίο ορισμού της συνάρτησης. Στην περίπτωση αυτή, το πρόβλημα μειώνεται στην ελαχιστοποίηση της συνάρτησης $g : \{2, 3, \ldots, (N-1)/2\} \times \{2, 3, \ldots, (N-1)/2\} \mapsto \{0, \ldots, N-1\}$, με

$$g(x, y) = x^2 - y^2 \pmod N, \tag{3.2}$$

υπό τον περιορισμό $x \not\equiv y \pmod N$. Αυτό είναι ένα διδιάστατο πρόβλημα ελαχιστοποίησης και το καθολικό ελάχιστο της συνάρτησης g είναι το μηδέν. Για λόγους απλότητας στη συνέχεια θα καλούμε το πρόβλημα ελαχιστοποίησης της συνάρτησης g, δηλαδή την εύρεση του ολικού ελαχιστοποιητή (x^*, y^*) της συνάρτησης g, υπό τον περιορισμό $x \not\equiv y \pmod N$, ως **Πρόβλημα 2**. Μια απεικόνιση της συνάρτησης $g(x, y)$ για $N = 11 \times 13 = 143$, δίνεται στο Σχήμα 3.3 (αριστερά) και οι ισοϋψείς της συνάρτησης g για την τιμή $g(x, y) = 0$ απεικονίζονται στο Σχήμα 3.3 (δεξιά).

Επίσης θεωρούμε τα ακόλουθα προβλήματα ελαχιστοποίησης. Ορίζουμε την συνάρτηση $h : \{1, 2, \ldots, N-1\} \mapsto \{0, 1, \ldots, N-1\}$, με

$$h(x) = (x - a)(x - b) \pmod N, \tag{3.3}$$

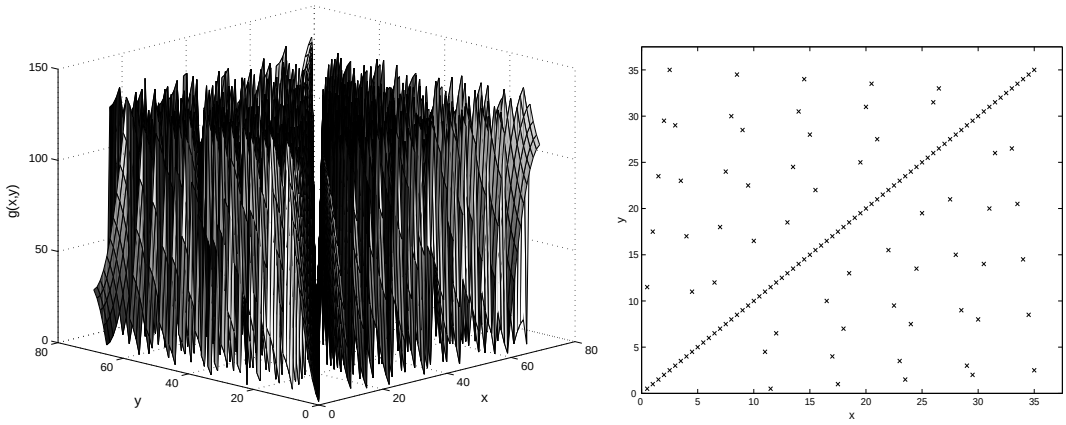
όπου a, b μη μηδενικοί ακέραιοι και $x \not\equiv a \pmod N$, $x \not\equiv b \pmod N$. Μια περίπτωση μελέτης για το πρόβλημα αυτό είναι η συνάρτηση

$$h_e(x) = (x - 1)(x - 2), \tag{3.4}$$

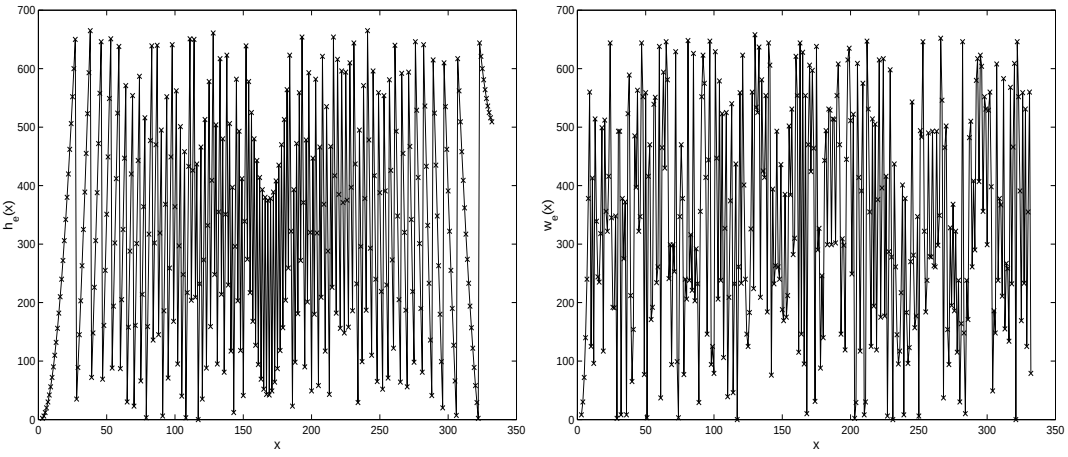
όπου $x \not\equiv 1 \pmod N$ και $x \not\equiv 2 \pmod N$. Αυτό είναι ένα πρόβλημα μονοδιάστατης ελαχιστοποίησης με ολικό ελάχιστο της συνάρτησης h_e είναι το μηδέν. Στη συνέχεια θα αναφερόμαστε στο πρόβλημα ελαχιστοποίησης της συνάρτησης $h_e(x)$, υπό τους περιορισμούς $x \not\equiv 1 \pmod N$ και $x \not\equiv 2 \pmod N$, ως **Πρόβλημα 3**. Στο Σχήμα 3.4 αριστερά απεικονίζεται η συνάρτηση $h_e(x)$ για μια μικρή τιμή του $N = 23 \times 29 = 667$.

Γενικότερα μπορούμε να θεωρήσουμε την ελαχιστοποίηση της συνάρτησης

$$w(x) = (x - a)(x - b) \cdots (x - m) \pmod N, \tag{3.5}$$



Σχήμα 3.3: Απεικόνιση της συνάρτησης $g(x, y) = x^2 - y^2 \pmod N$, για $N = 143$ (αριστερά), και οι ισοϋψείς της συνάρτησης $g(x, y) = x^2 - y^2 \pmod N$, για $N = 143$ στην τιμή 0 (δεξιά).



Σχήμα 3.4: Απεικόνιση της συνάρτησης $h_e(x) = (x-1)(x-2) \pmod N$, για $N = 667$ (αριστερά), και απεικόνιση της συνάρτησης $w_e(x) = (x+1)(x-1)(x-2) \pmod N$, για $N = 667$ (δεξιά).

όπου $x \in \{0, 1, \ldots, N-1\}$ και $x \not\equiv \{a, b, \ldots, m\} \pmod N$. Θα μελετήσουμε την περίπτωση

$$w_e(x) = (x+1)(x-1)(x-2) \pmod N, \tag{3.6}$$

με $x \not\equiv \{-1, 1, 2\} \pmod N$. Θα αναφερόμαστε στο μονοδιάστατο πρόβλημα ελαχιστοποίησης της συνάρτησης $w_e(x)$ υπό τους περιορισμούς $x \not\equiv \{-1, 1, 2\} \pmod N$ ως **Πρόβλημα 4**. Στο Σχήμα 3.4 δεξιά απεικονίζεται η συνάρτηση $w_e(x)$ για μικρή τιμή του $N = 23 \times 29 = 667$.

3.2.2 Πειραματική θεώρηση και αποτελέσματα

Για την αντιμετώπιση των τεσσάρων προβλημάτων ελαχιστοποίησης που ορίσαμε παραπάνω εφαρμόσαμε την μέθοδο ΒΣΣ και την μέθοδο ΔΕ και συγκρίναμε τα αποτελέσματά τους με τα αντίστοιχα αποτελέσματα που λάβαμε με την εφαρμογή της τεχνικής της απλής τυχαίας αναζήτησης. Για τα πειράματα χρησιμοποιήθηκαν η ολική και η τοπική παραλλαγή της μεθόδου ΒΣΣ με βάρος αδράνειας αλλά και με παράγοντα περιορισμού, καθώς και οι εκδοχές $DE/rand/1/bin$ και $DE/best/2/bin$ της μεθόδου ΔΕ. Για τις εκδοχές της μεθόδου

ΒΣΣ χρησιμοποιήθηκαν οι τυπικές τιμές παραμέτρων που δίνονται από την βιβλιογραφία της μεθόδου, και για την τοπική παραλλαγή δοκιμάστηκε μέγεθος της γειτονιάς ίσο με 1.

Αναφορικά με την μέθοδο ΒΣΣ, προκαταρκτικά πειράματα στα συγκεκριμένα προβλήματα έδειξαν ότι η τιμή της ελάχιστης και μέγιστης ταχύτητας, $V_{\min}$ και $V_{\max}$, των σωματιδίων επηρεάζει σημαντικά της απόδοση της μεθόδου σε κάθε περίπτωση. Συγκεκριμένα, το κάτω φράγμα στην τιμή της ταχύτητας των σωματιδίων εμπόδιζε την πρόωρη σύγκλιση της μεθόδου σε τοπικό ακρότατο για το Πρόβλημα 1, ενώ το άνω φράγμα στην τιμή της ταχύτητας των σωματιδίων προστάτευε τη μέθοδο από τη λήψη μεγάλων τιμών των ταχυτήτων που οδηγεί σε έκρηξη του σμήνους και καταστροφή της δυναμικής της μεθόδου για τα Προβλήματα 2, 3 και 4. Τα πιο ενθαρρυντικά αποτελέσματα ελήφθησαν χρησιμοποιώντας την τιμή $V_{\min} = 1$ για το Πρόβλημα 1 και $V_{\max} = \lfloor(\text{UpBound} - \text{LoBound})/5\rfloor$, όπου το UpBound συμβολίζει το άνω όριο του πεδίου ορισμού της συνάρτησης και το LoBound συμβολίζει το κάτω όριο, για τα Προβλήματα 2, 3, 4. Δηλαδή, η τιμή της μέγιστης ταχύτητας των σωματιδίων τέθηκε σε $V_{\max} = ((N-7)/10, (N-7)/10)$ για το Πρόβλημα 2 και $V_{\max} = (N-4)/5$ για τα Προβλήματα 3 και 4 για όλα τα πειράματα. Οι τιμές των παραμέτρων που χρησιμοποιήθηκαν για την μέθοδο ΔΕ είναι $F = 0.5$ και $CR = 0.5$. Σε όλες τις περιπτώσεις οι πληθυσμοί των μεθόδων περιορίστηκαν μέσα στον εφικτό χώρο λύσεων του αντίστοιχου προβλήματος.

Για την ελαχιστοποίηση της συνάρτησης f (Πρόβλημα 1), η απόδοση των μεθόδων μελετήθηκε για πρώτους αριθμούς p, στο διάστημα $[1009, 1000003]$. Για κάθε πρώτο αριθμό p που θεωρήθηκε, πραγματοποιήθηκαν 100 ανεξάρτητα πειράματα και τα αντίστοιχα αποτελέσματα παρουσιάζονται στον Πίνακα 3.1. Αναφορικά με τον συμβολισμό που χρησιμοποιείται στον πίνακα, ο συμβολισμός ΒΣΣΟΒ αντιστοιχεί στην ολική παραλλαγή της μεθόδου ΒΣΣ με βάρος αδράνειας, το ΒΣΣΟΠ είναι η ολική παραλλαγή της μεθόδου ΒΣΣ με παράγοντα περιορισμού, το ΒΣΣΤΒ είναι η τοπική παραλλαγή της μεθόδου με βάρος αδράνειας, το ΒΣΣΤΠ είναι η τοπική παραλλαγή της μεθόδου με παράγοντα περιορισμού, το ΔΕ1 αντιστοιχεί στην εκδοχή $DE/rand/1/bin$ της μεθόδου ΔΕ και το ΔΕ2 στην εκδοχή $DE/best/2/bin$ της μεθόδου ΔΕ. Τα αποτελέσματα της τεχνικής τυχαίας αναζήτησης συμβολίζονται ως ΤΑ.

Ένα πείραμα θεωρείται επιτυχές αν η μέθοδος εντοπίζει τον καθολικό ελαχιστοποιητή χρησιμοποιώντας συναρτησιακούς υπολογισμούς λιγότερους ή ίσους με ένα προκαθορισμένο όριο. Για το Πρόβλημα 1, θεωρήσαμε δύο διαφορετικά κατώφλια συναρτησιακών υπολογισμών, $\log_2^2 p$ και $\log_2^3 p$, αντίστοιχα.

Για το Πρόβλημα 1, τα ποσοστά επιτυχίας για κάθε μέθοδο, δηλαδή ο αριθμός των πειραμάτων στα οποία η μέθοδος εντόπισε τον καθολικό ελαχιστοποιητή εντός των προκαθορισμένων ορίων συναρτησιακών υπολογισμών δίνονται στον Πίνακα 3.1. Από την αναλογία $c\%$ των ποσοστών επιτυχίας που παρουσιάζονται, είναι σαφές ότι το ΠΔΛ μπορεί να σπάσει αν χρησιμοποιηθούν συναρτησιακοί υπολογισμοί πλήθους $100/c$ φορές επί το αντίστοιχο κατώφλι.

Τα πειραματικά αποτελέσματα δείχνουν ότι το φράγμα των $\log_2^2 p$ συναρτησιακών υπολογισμών δεν επιτρέπει στις μεθόδους να εντοπίσουν τον καθολικό ελαχιστοποιητή, καθώς τα ποσοστά επιτυχίας είναι ιδιαίτερα χαμηλά για όλες τις παραλλαγές των μεθόδων ακόμα και για την τυχαία αναζήτηση. Όταν το φράγμα των συναρτησιακών υπολογισμών αυξάνεται σε $\log_2^3 p$, τα ποσοστά επιτυχίας των μεθόδων αυξάνουν αρκετά για μικρούς πρώτους αριθμούς και μειώνονται προοδευτικά καθώς το μέγεθος των πρώτων αριθμών που μελετώνται αυξάνει.

Για την ελαχιστοποίηση της συνάρτησης g (Πρόβλημα 2), η απόδοση των μεθόδων μελετήθηκε για διάφορες τιμές του ακεραίου N, μεταξύ των τιμών $N = 199 \times 211 = 41989$ και $N = 691 \times 701 = 484391$. Για κάθε διαφορετική τιμή του ακεραίου N που μελετήθηκε, εκτελέστηκαν 100 ανεξάρτητα πειράματα. Τα αντίστοιχα αποτελέσματα δίνονται στον Πίνακα 3.2.

Για τα προβλήματα 2, 3 και 4 το όριο των προκαθορισμένων συναρτησιακών υπολογισμών που μπορεί να χρησιμοποιήσει κάθε μέθοδος για τον εντοπισμό του καθολικού ελαχιστοποιητή τέθηκε ίσο με τον πληθάριθμο των ακεραίων που ανήκουν στο πεδίο ορισμού της αντίστοιχης υπό μελέτη συνάρτησης. Τα ποσοστά επιτυχίας για κάθε μέθοδο, δηλαδή ο αριθμός των

Πίνακας 3.1: Ποσοστά επιτυχίας της κάθε μεθόδου για την ελαχιστοποίηση της συνάρτησης f για δύο κατώφλια συναρτησιακών υπολογισμών και $p = 1009$ ως $p = 1000003$.

		Ποσοστά επιτυχίας για συναρτ. υπολογ.	
	Μέθοδος	$\leqslant \log_2^2 p$	$\leqslant \log_2^3 p$
$p = 1009$ $\alpha = 11$ $\beta = 337$	ΒΣΣΟΒ	7%	61%
	ΒΣΣΟΠ	6%	63%
	ΒΣΣΤΒ	3%	55%
	ΒΣΣΤΠ	7%	60%
	ΔΕ1	4%	37%
	ΔΕ2	1%	45%
	ΤΑ	15%	68%
$p = 2003$ $\alpha = 5$ $\beta = 668$	ΒΣΣΟΒ	4%	60%
	ΒΣΣΟΠ	7%	68%
	ΒΣΣΤΒ	5%	63%
	ΒΣΣΤΠ	6%	63%
	ΔΕ1	5%	23%
	ΔΕ2	1%	24%
	ΤΑ	9%	46%
$p = 3001$ $\alpha = 14$ $\beta = 1001$	ΒΣΣΟΒ	3%	20%
	ΒΣΣΟΠ	2%	21%
	ΒΣΣΤΒ	3%	17%
	ΒΣΣΤΠ	2%	18%
	ΔΕ1	1%	15%
	ΔΕ2	1%	8%
	ΤΑ	3%	36%
$p = 4001$ $\alpha = 3$ $\beta = 1334$	ΒΣΣΟΒ	3%	28%
	ΒΣΣΟΠ	3%	14%
	ΒΣΣΤΒ	2%	27%
	ΒΣΣΤΠ	3%	15%
	ΔΕ1	1%	8%
	ΔΕ2	1%	10%
	ΤΑ	2%	33%
$p = 9973$ $\alpha = 11$ $\beta = 3324$	ΒΣΣΟΒ	1%	20%
	ΒΣΣΟΠ	2%	35%
	ΒΣΣΤΒ	2%	15%
	ΒΣΣΤΠ	3%	28%
	ΔΕ1	1%	11%
	ΔΕ2	0%	5%
	ΤΑ	5%	21%
$p = 10007$ $\alpha = 5$ $\beta = 3336$	ΒΣΣΟΒ	1%	23%
	ΒΣΣΟΠ	1%	20%
	ΒΣΣΤΒ	1%	24%
	ΒΣΣΤΠ	1%	20%
	ΔΕ1	1%	10%
	ΔΕ2	0%	6%
	ΤΑ	2%	27%
$p = 99991$ $\alpha = 6$ $\beta = 33330$	ΒΣΣΟΒ	0%	3%
	ΒΣΣΟΠ	1%	7%
	ΒΣΣΤΒ	0%	3%
	ΒΣΣΤΠ	1%	5%
	ΔΕ1	0%	4%
	ΔΕ2	0%	2%
	ΤΑ	1%	3%
$p = 500029$ $\alpha = 6$ $\beta = 166676$	ΒΣΣΟΒ	0%	2%
	ΒΣΣΟΠ	0%	2%
	ΒΣΣΤΒ	0%	2%
	ΒΣΣΤΠ	0%	3%
	ΔΕ1	0%	2%
	ΔΕ2	0%	0%
	ΤΑ	0%	2%
$p = 1000003$ $\alpha = 2$ $\beta = 333334$	ΒΣΣΟΒ	0%	1%
	ΒΣΣΟΠ	0%	2%
	ΒΣΣΤΒ	0%	1%
	ΒΣΣΤΠ	0%	2%
	ΔΕ1	0%	0%
	ΔΕ2	0%	0%
	ΤΑ	0%	0%

πειραμάτων στα οποία η μέθοδος εντόπισε τον καθολικό ελαχιστοποιητή εντός του προκαθορισμένου ορίου συναρτησιακών υπολογισμών, η ελάχιστη τιμή, η διάμεσος, η μέση τιμή και η τυπική απόκλιση των συναρτησιακών υπολογισμών που απαιτήθηκαν για την επιτυχία της μεθόδου, δίνονται στους αντίστοιχους πίνακες.

Τα πειραματικά αποτελέσματα για το Πρόβλημα 2 δείχνουν ότι οι εκδοχές της μεθόδου ΒΣΣ αποδίδουν καλύτερα από τις εκδοχές της μεθόδου ΔΕ για τις συγκεκριμένες τιμές των παραμέτρων. Επιπλέον, η απόδοση της μεθόδου ΔΕ μειώνεται καθώς αυξάνεται η τιμή του ακεραίου N σε αντίθεση με την μέθοδο ΒΣΣ η οποία παρουσιάζει πιο σταθερή συμπεριφορά αναφορικά με τις παραμέτρους του προβλήματος. Ωστόσο, σε αντίθεση με την απόδοση των μεθόδων ΕΥ εν γένει, η τεχνική της τυχαίας αναζήτησης ξεπερνά σε απόδοση και τις δύο μεθόδους ΕΥ στις συγκεκριμένες περιπτώσεις του προβλήματος που μελετήθηκαν. Το γεγονός αυτό υποδεικνύει ότι η σχεδόν τυχαία μορφή των συγκεκριμένων υποπροβλημάτων καθιστά δύσκολη για τις μεθόδους την εξόρυξη πληροφοριών για τη δυναμική των συναρτήσεων. Στις περιπτώσεις όπου οι μέθοδοι ΕΥ εντόπισαν τον καθολικό ελαχιστοποιητή απαιτήθηκε ένας σχετικά μικρός αριθμός συναρτησιακών υπολογισμών αναφορικά με τον πληθάριθμο του πεδίου ορισμού της υπό μελέτη συνάρτησης. Επίσης, είναι σημαντικό να παρατηρήσουμε ότι στα πειράματα όπου οι μέθοδοι ΕΥ απέτυχαν να εντοπίσουν τον καθολικό ελαχιστοποιητή, εντόπισαν κάποιον τοπικό ελαχιστοποιητή με τιμή πολύ κοντά στο ολικό ελάχιστο.

Παρόμοια αποτελέσματα λήφθηκαν από την ελαχιστοποίηση της συνάρτησης h_e (Πρόβλημα 3) και της w_e (Πρόβλημα 4). Για $N = 103 \times 107$ τα αποτελέσματα αυτά δίνονται στον Πίνακα 3.3. Για το Πρόβλημα 4, τα ποσοστά επιτυχίας της μεθόδου ΒΣΣ και των παραλλαγών της είναι αρκετά υψηλά (περίπου 82%) ενώ η απόδοση των παραλλαγών της μεθόδου ΔΕ παραμένει χαμηλή. Ωστόσο, η μέθοδος της τυχαίας αναζήτησης και σε αυτή την περίπτωση ξεπερνά την απόδοση των μεθόδων ΕΥ αναφορικά με τα ποσοστά επιτυχίας.

Πίνακας 3.2: Αποτελέσματα για την ελαχιστοποίηση της συνάρτησης g (βλέπε Εξίσωση (3.2)).

N	Μέθοδος	Ποσοστό Επιτυχίας	Συναρτησιακοί Υπολογισμοί Μέση Τιμή	Τυπ.Απόκ.	Διάμεσος	Ελάχ.Τιμή
$N = 199 \times 211$	ΒΣΣΟΒ	56%	8844.643	5992.515	8325.000	660
	ΒΣΣΟΠ	48%	7149.375	5272.590	5355.000	330
	ΒΣΣΤΒ	51%	8329.412	6223.142	7050.000	270
	ΒΣΣΤΠ	51%	7160.588	6001.276	5940.000	420
	ΔΕ1	4%	517.500	115.866	465.000	450
	ΔΕ2	9%	5476.667	6455.651	1830.000	60
	ΤΑ	66%	9104.015	5862.358	8700.500	22
$N = 293 \times 307$	ΒΣΣΟΒ	41%	16210.244	11193.375	15090.000	120
	ΒΣΣΟΠ	45%	16818.667	12664.632	13800.000	630
	ΒΣΣΤΒ	58%	18455.690	12870.897	14520.000	270
	ΒΣΣΤΠ	50%	16374.000	13597.782	13365.000	120
	ΔΕ1	7%	1598.571	1115.488	1470.000	120
	ΔΕ2	19%	17815.263	12484.580	16290.000	2730
	ΤΑ	64%	21548.531	13926.751	20852.500	57
$N = 397 \times 401$	ΒΣΣΟΒ	53%	31965.849	24423.975	27570.000	780
	ΒΣΣΟΠ	45%	32532.667	22652.983	33210.000	1740
	ΒΣΣΤΒ	55%	31472.182	23394.791	22620.000	720
	ΒΣΣΤΠ	54%	38156.111	22925.970	37665.000	750
	ΔΕ1	1%	1680.000	0.000	1680.000	1680
	ΔΕ2	12%	27722.500	17498.736	28620.000	180
	ΤΑ	60%	27302.567	21307.031	23607.500	145
$N = 499 \times 503$	ΒΣΣΟΒ	56%	49893.750	37515.327	44640.000	930
	ΒΣΣΟΠ	55%	49975.636	36727.380	41760.000	300
	ΒΣΣΤΒ	55%	49207.091	34053.904	50430.000	2010
	ΒΣΣΤΠ	46%	48443.478	34677.039	43470.000	1920
	ΔΕ1	1%	2480.000	0.000	2480.000	2480
	ΔΕ2	8%	67245.000	35114.316	64770.000	14730
	ΤΑ	61%	54139.443	38642.970	48743.000	140
$N = 599 \times 601$	ΒΣΣΟΒ	52%	72175.000	48653.823	71550.000	600
	ΒΣΣΟΠ	51%	81476.471	53666.543	75100.000	5000
	ΒΣΣΤΒ	49%	78651.020	48197.105	67400.000	11200
	ΒΣΣΤΠ	52%	69542.308	48837.949	53050.000	2500
	ΔΕ1	2%	4700.000	4808.326	4700.000	1300
	ΔΕ2	5%	8620.000	8078.180	9300.000	800
	ΤΑ	64%	86123.656	47504.284	89392.500	904
$N = 691 \times 701$	ΒΣΣΟΒ	46%	207443.478	163585.340	214800.000	800
	ΒΣΣΟΠ	46%	175426.086	138118.794	149200.000	800
	ΒΣΣΤΒ	60%	196993.334	146204.518	144500.000	9200
	ΒΣΣΤΠ	52%	209307.692	163833.606	200100.000	1800
	ΔΕ1	2%	23800.000	25000.000	23800.000	21000
	ΔΕ2	10%	71000.000	95357.642	15200.000	1600
	ΤΑ	60%	185932.334	126355.926	154999.000	2828

Πίνακας 3.3: Αποτελέσματα για τις συναρτήσεις h_e (βλέπε Εξίσωση (3.4)) και w_e (βλέπε Εξίσωση (3.6)), για $N = 103 \times 107$

Συνάρτηση	Μέθοδος	Ποσοστό Επιτυχίας	Συναρτησιακοί Υπολογισμοί Μέση Τιμή	Τυπ.Απόκ.	Διάμεσος	Ελάχ.Τιμή
h_e	ΒΣΣΟΒ	51%	2013.333	1483.535	1500.000	100
	ΒΣΣΟΠ	57%	1974.035	1609.228	1420.000	60
	ΒΣΣΤΒ	59%	1677.288	1254.688	1420.000	60
	ΒΣΣΤΠ	58%	2385.862	1676.898	2040.000	120
	ΔΕ1	1%	100.000	0.000	100.000	100
	ΔΕ2	1%	80.000	0.000	80.000	80
	ΤΑ	65%	2099.646	1448.007	2056.000	6
w_e	ΒΣΣΟΒ	79%	1382.785	1265.927	820.000	40
	ΒΣΣΟΠ	84%	1402.857	1442.194	930.000	40
	ΒΣΣΤΒ	80%	1757.750	1544.267	1110.000	40
	ΒΣΣΤΠ	85%	1416.000	1329.034	880.000	40
	ΔΕ1	1%	60.000	0.000	60.000	60
	ΔΕ2	1%	80.000	0.000	80.000	80
	ΤΑ	96%	1507.969	1328.913	1104.000	7

3.3 Μέθοδοι Εξελικτικού Υπολογισμού για την κρυπτανάλυση κρυπτοσυστημάτων Feistel

Στην ενότητα αυτή θεωρούμε ως προβλήματα βελτιστοποίησης δύο διαφορετικές περιπτώσεις ενός προβλήματος που εισάγεται από την Διαφορική Κρυπτανάλυση ενός κρυπτοσυστήματος Feistel. Πιο συγκεκριμένα, μελετάμε το πρόβλημα εύρεσης μερικών δυαδικών ψηφίων (bits) του κλειδιού που χρησιμοποιείται από ένα απλό κρυπτοσύστημα Feistel, το Data Encryption Standard (DES) με τέσσερις και έξι γύρους, αντίστοιχα [99, 100]. Οι δύο περιπτώσεις του προβλήματος είναι συμπληρωματικές καθώς οποιοδήποτε πρόβλημα εύρεσης δυαδικών ψηφίων ενός κλειδιού στην Διαφορική Κρυπτανάλυση για κρυπτοσυστήματα Feistel μπορεί να κατηγοριοποιηθεί σε μια από αυτές τις δύο περιπτώσεις.

Για την επίλυση των προαναφερθέντων προβλημάτων βελτιστοποίησης χρησιμοποιούμε τις μεθόδους ΒΣΣ και ΔΕ. Τα πειραματικά αποτελέσματα για το DES με τέσσερις γύρους δείχνουν ότι οι μέθοδοι εντοπίζουν την λύση αποδοτικά και αποτελεσματικά καθώς απαιτούν αρκετά μικρότερο αριθμό συναρτησιακών υπολογισμών σε σχέση με την προσέγγιση της επίθεσης εξαντλητικής αναζήτησης (brute force attack). Για την περίπτωση του DES με έξι γύρους τα αποτελέσματα δείχνουν ότι η αποδοτικότητα των μεθόδων εξαρτάται από την κατασκευή της αντικειμενικής συνάρτησης του προβλήματος.

3.3.1 Θεωρητικά στοιχεία για το κρυπτοσύστημα DES

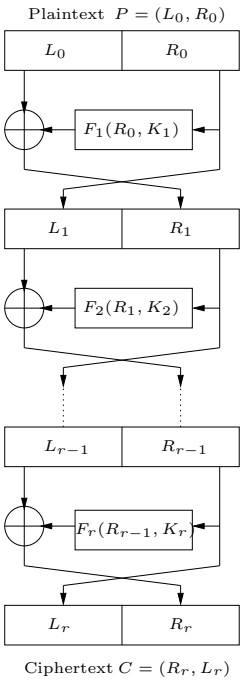
Ένα τμηματικό κρυπτοσύστημα (block cipher) είναι μια συνάρτηση που απεικονίζει τμήματα πρωτότυπου κειμένου n δυαδικών ψηφίων σε τμήματα κρυπτογραφήματος n δυαδικών ψηφίων, όπου n είναι ένα επιλεγμένο μήκος τμήματος. Η συνάρτηση αυτή παραμετροποιείται χρησιμοποιώντας ένα κλειδί K, με k δυαδικά ψηφία, το οποίο παίρνει τιμές από ένα υποσύνολο $\mathcal{K}$ του συνόλου όλων των διανυσμάτων k δυαδικών ψηφίων, που καλείται χώρος των κλειδιών. Η συνάρτηση πρέπει να είναι αντιστρέψιμη ώστε να επιτρέπει μοναδική αποκρυπτογράφηση. Τα τμηματικά κρυπτοσυστήματα μπορούν να είναι είτε συμμετρικού κλειδιού είτε δημοσίου κλειδιού [130].

Ένα κρυπτοσύστημα Feistel είναι ένα επαναλαμβανόμενο τμηματικό κρυπτοσύστημα που

βασίζεται στον επαναληπτικό υπολογισμό για έναν προκαθορισμένο αριθμό γύρων απλών συναρτήσεων, που καλούνται *συναρτήσεις γύρων (round functions)*. Η τελική συνάρτηση κρυπτογράφησης απεικονίζει ένα πρωτότυπο τμήμα κειμένου P, n δυαδικών ψηφίων, σε ένα κρυπτογράφημα C. Σε ένα κρυπτοσύστημα Feistel, η τρέχουσα υπολογισμένη (από την συνάρτηση γύρου) λέξη n δυαδικών ψηφίων χωρίζεται σε τμήματα των $(n/2)$ δυαδικών ψηφίων, το αριστερό τμήμα L_i και το δεξί τμήμα R_i [57]. Έπειτα, ο i-οστός γύρος, όπου $1 \leqslant i \leqslant r$, έχει το ακόλουθο αποτέλεσμα:

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus F_i(R_{i-1}, K_i),$$

όπου K_i είναι το υποκλειδί που χρησιμοποιείται στον i-οστό γύρο (προκύπτει από το κλειδί κρυπτογράφησης K), και F_i είναι μια τυχαία συνάρτηση γύρου για τον i-οστό γύρο. Μετά την εφαρμογή της συνάρτησης του τελευταίου γύρου, τα δύο τμήματα αντιμετατίθονται και το αποτέλεσμα είναι το κρυπτογράφημα C του κρυπτοσυστήματος Feistel, δηλαδή $C = (R_r, L_r)$. Η διαδικασία κρυπτογράφησης των κρυπτοσυστημάτων Feistel απεικονίζεται στην Εικόνα 3.5.



Σχήμα 3.5: Η διαδικασία κρυπτογράφησης των κρυπτοσυστημάτων Feistel

Στα κρυπτοσυστήματα Feistel η συνάρτηση αποκρυπτογράφησης προκύπτει απλά από την συνάρτηση κρυπτογράφησης εφαρμόζοντας τα υποκλειδιά, K_i, και τις συναρτήσεις γύρων, F_i, με την αντίστροφη σειρά. Το γεγονός αυτό καθιστά την δομή Feistel μια ελκυστική επιλογή για υλοποιήσεις λογισμικές αλλά και υλικές.

Ένα από τα πιο ευρέως χρησιμοποιούμενα κρυπτοσυστήματα Feistel είναι το Data Encryption Standard (DES) [145]. Το DES είναι ένα κρυπτοσύστημα συμμετρικού κλειδιού, δηλαδή τα μέλη που ανταλλάσσουν πληροφορίες κατέχουν το ίδιο κλειδί. Χρησιμοποιεί πρωτότυπα τμήματα κειμένου μήκους $n = 64$ δυαδικών ψηφίων και παράγει τμήματα κρυπτογραφήματος 64 δυαδικών ψηφίων. Το αποτελεσματικό μήκος κλειδιού είναι $k = 64$ δυαδικά ψηφία, 8 από τα οποία μπορούν να χρησιμοποιηθούν ως ψηφία ελέγχου ισοτιμίας (parity bits). Το κύριο μέρος της συνάρτησης γύρου είναι η συνάρτηση F, η οποία εφαρμόζεται στο δεξί τμήμα των δεδομένων, χρησιμοποιώντας ένα υποκλειδί 48 δυαδικών ψηφίων και 8 S-boxes. Τα S-boxes είναι απεικονίσεις που μετασχηματίζουν τα 6 δυαδικά ψηφία σε 4 δυαδικά ψηφία με έναν μη-γραμμικό τρόπο και αποτελούν το μόνο μη-γραμμικό μέρος του κρυπτοσυστήματος DES. Στην

έξοδο των 32 δυαδικών ψηφίων της συνάρτησης F και στο αριστερό τμήμα των δεδομένων εφαρμόζεται η λογική πράξη XOR και τα δύο μισά ανταλλάσσονται διαδοχικά [130, 201].

Δύο από τις πιο ισχυρές κρυπταναλυτικές επιθέσεις για τα κρυπτοσυστήματα Feistel βασίζονται στην αξιοποίηση συγκεκριμένων αδυναμιών των S-boxes των υποκείμενων κρυπτοσυστημάτων. Οι επιθέσεις αυτές είναι η *Γραμμική Κρυπτανάλυση* [119,120] και η *Διαφορική Κρυπτανάλυση* [14,15], οι οποίες εφαρμόστηκαν επιτυχώς πρώτα στην κρυπτανάλυση του DES. Η Διαφορική Κρυπτανάλυση (ΔΚ) είναι μια επίθεση επιλεγμένου πρωτότυπου κειμένου. Στις επιθέσεις επιλεγμένου πρωτότυπου κειμένου ο αντίπαλος έχει προσωρινή πρόσβαση στην συνάρτηση κρυπτογράφησης και μπορεί να επιλέξει μερικά πρωτότυπα κείμενα για τα οποία θα δημιουργήσει τα αντίστοιχα κρυπτογραφήματα. Η ΔΚ αναλύει την επίδραση συγκεκριμένων αλλαγών σε ζεύγη πρωτότυπων κειμένων στις αλλαγές των αντίστοιχων κρυπτογραφημένων ζευγών. Αυτές οι αλλαγές μπορούν να χρησιμοποιηθούν για να αποδοθούν πιθανότητες στα πιθανά κλειδιά αλλά και για να αναγνωριστούν ψηφία του κλειδιού που χρησιμοποιήθηκε κατά την διαδικασία της κρυπτογράφησης. Η μέθοδος αυτή συνήθως εφαρμόζεται με ένα πλήθος ζευγών πρωτότυπου κειμένου που έχουν μια συγκεκριμένη διαφορά και βασίζεται μόνο στα αντίστοιχα ζεύγη κρυπτογραφήματος. Για κρυπτοσυστήματα παρόμοια με το κρυπτοσύστημα DES, η διαφορά επιλέγεται να είναι μια συγκεκριμένη τιμή της λογικής πράξης XOR μεταξύ των δύο πρωτότυπων κειμένων που αποτελούν κάθε ζεύγος.

Για τον εντοπισμό του πιο πιθανού κλειδιού, η ΔΚ χρησιμοποιεί *χαρακτηριστικές*. Για την κατανόηση της έννοιας της χαρακτηριστικής πρέπει να παρατηρηθεί ότι κάθε ζεύγος κρυπτογραφημένων πρωτότυπων κειμένων συσχετίζεται με την XOR τιμή των δύο πρωτότυπων κειμένων του, την XOR τιμή των δύο κρυπτογραφημάτων του, τις XOR τιμές των εισόδων κάθε γύρου κατά τις δύο κρυπτογραφήσεις και τις XOR τιμές των εξόδων κάθε γύρου κατά τις δύο κρυπτογραφήσεις. Αυτές οι XOR τιμές σχηματίζουν μια χαρακτηριστική r-γύρων [14]. Πιο τυπικά, μια χαρακτηριστική r-γύρων είναι μια τριάδα $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_C)$, όπου Ω_P και Ω_C είναι αριθμοί n δυαδικών ψηφίων και Ω_Λ είναι μια λίστα r στοιχείων $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \ldots, \Lambda_r)$, καθένα από τα οποία είναι ένα ζεύγος της μορφής $\Lambda_i = (\lambda_I^i, \lambda_O^i)$, όπου λ_I^i και λ_O^i είναι αριθμοί $n/2$ δυαδικών ψηφίων και n είναι το μήκος τμήματος του κρυπτοσυστήματος [14]. Μια χαρακτηριστική ικανοποιεί τις ακόλουθες απαιτήσεις:

(1) λ_I^1 είναι το δεξί μισό τμήμα του Ω_P,

(2) λ_I^2 είναι το αριστερό μισό τμήμα του $\Omega_P \oplus \lambda_O^1$,

(3) λ_I^r είναι το δεξί μισό τμήμα του Ω_C,

(4) λ_I^{r-1} είναι το αριστερό μισό τμήμα του $\Omega_C \oplus \lambda_O^r$, και

(5) για κάθε i, $2 \leqslant i \leqslant r-1$, ισχύει ότι $\lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1}$.

Σε κάθε χαρακτηριστική αποδίδεται η πιθανότητα ένα τυχαίο ζεύγος με επιλεγμένη XOR τιμή πρωτότυπου κειμένου, Ω_P, να έχει τις XOR τιμές των γύρων, Λ_i, και την XOR τιμή κρυπτογραφήματος, Ω_C, που καθορίζονται από την χαρακτηριστική. Κάθε χαρακτηριστική επιτρέπει την αναζήτηση ενός συγκεκριμένου συνόλου των ψηφίων του υποκλειδιού του τελευταίου γύρου, και είναι τα ψηφία που πηγαίνουν σε συγκεκριμένα S-boxes, ανάλογα με την επιλεγμένη χαρακτηριστική. Οι χαρακτηριστικές που είναι περισσότερο χρήσιμες είναι αυτές που έχουν μια μέγιστη πιθανότητα και τον μέγιστο αριθμό ψηφίων του υποκλειδιού των οποίων οι εμφανίσεις μπορούν να μετρηθούν.

Η ΔΚ είναι μια στατιστική μέθοδος που σπάνια αποτυγχάνει και ήταν η πρώτη θεωρητική κρυπτανάλυση του DES που απαιτούσε (κατά μέσο όρο) λιγότερα βήματα από την εξαντλητική αναζήτηση, δηλαδή τον έλεγχο όλων των $2^{56} = 72\,057\,594\,037\,927\,936$ πιθανών κλειδιών. Παρότι αυτός ο αριθμός μοιάζει απαγορευτικός, μια επίθεση εξαντλητικής αναζήτησης στο DES 56 δυαδικών ψηφίων χρησιμοποιώντας τα τεχνολογικά δεδομένα των προηγούμενων δεκαετιών

επιχειρήθηκε επιτυχώς. Ένα ειδικό σύστημα με κατάλληλο λογισμικό, κατασκευασμένο από τις Cryptography Research, Advanced Wireless Technologies και EFF (Electronic Frontier Foundation) έφτασε τον βαθμό αναζήτησης κλειδιών στα 90 δισεκατομμύρια κλειδιά ανά δευτερόλεπτο.

3.3.2 Θεώρηση προβλήματος

DES με τέσσερις γύρους: Για το κρυπτοσύστημα DES με τέσσερις γύρους η Διαφορική Κρυπτανάλυση (ΔΚ) χρησιμοποιεί μια χαρακτηριστική ενός γύρου με πιθανότητα 1, η οποία στο πρώτο στάδιο κρυπτανάλυσης αποκαλύπτει 42 ψηφία του υποκλειδιού του τελευταίου γύρου. Στην περίπτωση που τα υποκλειδιά υπολογίζονται με βάση τον αλγόριθμο DES key scheduling, τα 42 ψηφία που λαμβάνονται από την ΔΚ είναι ακριβή ψηφία του κλειδιού και υπολείπονται ακόμα 14 ψηφία προκειμένου να συμπληρωθούν όλα τα ψηφία του κλειδιού.

Με την προσέγγιση της επίθεσης εξαντλητικής αναζήτησης, δηλαδή με την αναζήτηση μεταξύ όλων των πιθανών 14 ψηφίων, απαιτείται η δοκιμή 2^{14} δυνατών περιπτώσεων για την εύρεση των υπολειπόμενων ψηφίων του κλειδιού. Το σωστό κλειδί θα πρέπει να ικανοποιεί την γνωστή από την χαρακτηριστική XOR τιμή πρωτότυπων κειμένων (plaintext XOR) για όλα τα ζεύγη πρωτότυπων κειμένων που χρησιμοποιούνται από την ΔΚ. Μια εναλλακτική προσέγγιση για την εύρεση των 14 ψηφίων του κλειδιού που υπολείπονται είναι η χρήση μιας δεύτερης χαρακτηριστικής που αντιστοιχεί στα υπολειπόμενα ψηφία και η προσπάθεια για μια πιο προσεκτική καταμέτρηση των ψηφίων των υποκλειδιών των δύο τελευταίων γύρων, η οποία καθιστά αρκετά σύνθετη την προσέγγιση αυτή.

Στην παρούσα μελέτη, αντί να χρησιμοποιήσουμε τις προαναφερθείσες προσεγγίσεις για την εύρεση των υπολειπόμενων 14 ψηφίων του κλειδιού, προτείνουμε το μετασχηματισμό του προβλήματος σε πρόβλημα διακριτής βελτιστοποίησης και την επίλυσή του με μεθόδους ΕΥ. Καθώς το σωστό κλειδί θα πρέπει να ικανοποιεί την γνωστή από την χαρακτηριστική XOR τιμή πρωτότυπων κειμένων για όλα τα ζεύγη που χρησιμοποιούνται από την ΔΚ, τα κρυπτογραφήματα αυτά μπορούν να χρησιμοποιηθούν για την αξιολόγηση πιθανών λύσεων που προτείνονται από τις μεθόδους βελτιστοποίησης. Θεωρούμε ότι το $\mathbf{X}$ είναι ένα 14–διάστατο διάνυσμα, στο οποίο κάθε συνιστώσα αντιστοιχεί σε ένα από τα 14 άγνωστα δυαδικά ψηφία του κλειδιού. Ένα τέτοιο διάνυσμα αναπαριστά μια πιθανή λύση στο πρόβλημα βελτιστοποίησης. Επίσης, έστω ότι np είναι ο αριθμός των ζευγών κρυπτογραφημάτων που χρησιμοποιούνται από την ΔΚ για την εύρεση των 42 ψηφίων του κλειδιού. Τότε, μπορούμε να κατασκευάσουμε το κλειδί με τα 56 ψηφία που χρησιμοποιεί το DES, χρησιμοποιώντας τα 42 ψηφία που αποκαλύπτει η ΔΚ και τις 14 συνιστώσες του $\mathbf{X}$, με την κατάλληλη σειρά. Με το εξαγόμενο κλειδί των 56 ψηφίων, αποκρυπτογραφούμε τα np ζεύγη κρυπτογραφημάτων και μετράμε τον αριθμό των αποκρυπτογραφημένων ζευγών που ικανοποιούν την γνωστή από την χαρακτηριστική XOR τιμή πρωτότυπων κειμένων, την οποία συμβολίζουμε $cnp_{\mathbf{X}}$. Κατ΄ αυτόν τον τρόπο, ως αντικειμενική συνάρτηση f ορίζεται η διαφορά μεταξύ του επιθυμητού αποτελέσματος np και του πραγματικού αποτελέσματος $cnp_{\mathbf{X}}$, δηλαδή $f(\mathbf{X}) = np - cnp_{\mathbf{X}}$. Το ολικό ελάχιστο της συνάρτησης f είναι το μηδέν και ο ολικός ελαχιστοποιητής είναι το σωστό κλειδί με υψηλή πιθανότητα.

DES με έξι γύρους: Η κρυπτανάλυση του κρυπτοσυστήματος DES με έξι γύρους είναι, όπως ήταν αναμενόμενο, πιο πολύπλοκη από την αντίστοιχη για τους τέσσερις γύρους, καθώς η καλύτερη χαρακτηριστική που μπορεί να χρησιμοποιηθεί από την ΔΚ έχει πιθανότητα μικρότερη από 1. Συγκεκριμένα, η ΔΚ χρησιμοποιεί δύο χαρακτηριστικές με πιθανότητα $p_{sr} = 1/16$ για να δώσει 42 ψηφία του σωστού κλειδιού. Και σε αυτή την περίπτωση υπολείπονται 14 ψηφία για την συμπλήρωση ολόκληρου του κλειδιού. Ωστόσο, στην περίπτωση αυτή το σωστό κλειδί μπορεί να μην προκύπτει από όλα τα ζεύγη κρυπτογραφημάτων. Αυτό συμβαίνει γιατί δεν είναι όλα τα αντίστοιχα ζεύγη πρωτότυπου κειμένου (plaintext) *σωστά ζεύγη* (right pairs).

Ορισμός 3.1 *Ένα ζεύγος καλείται σωστό ζεύγος αναφορικά με μια χαρακτηριστική r γύρων $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_C)$ και ένα ανεξάρτητο κλειδί K, αν ισχύει ότι $P' = \Omega_P$, όπου P' είναι η XOR τιμή του ζεύγους, και για τους πρώτους r γύρους της κρυπτογράφησης του ζεύγους χρησιμοποιώντας το ανεξάρτητο κλειδί K τα XORs εισόδου και εξόδου του i-οστού γύρου είναι ίσα με λ_I^i και λ_O^i, αντίστοιχα [14].*

Η πιθανότητα ένα ζεύγος πρωτότυπων κειμένων με XOR τιμή ίση με την τιμή Ω_P της χαρακτηριστικής να είναι σωστό ζεύγος χρησιμοποιώντας ένα σταθερό κλειδί, είναι περίπου ίση με την πιθανότητα της χαρακτηριστικής. Ένα ζεύγος το οποίο δεν είναι σωστό ζεύγος καλείται *λανθασμένο ζεύγος* (wrong pair) και δεν υποδεικνύει πάντα το σωστό κλειδί σαν πιθανή τιμή. Η μελέτη των σωστών και λανθασμένων ζευγών έχει δείξει ότι το σωστό κλειδί εμφανίζεται με την πιθανότητα της χαρακτηριστικής από τα σωστά ζεύγη και μερικές άλλες τυχαίες φορές από τα λανθασμένα ζεύγη. Συμπερασματικά, αν όλα τα ζεύγη της ΔΚ (σωστά και λανθασμένα) χρησιμοποιηθούν για την συνάρτηση f που ορίσαμε προηγουμένως, η ελάχιστη τιμή της συνάρτησης θα μεταβάλλεται ανάλογα με τα συγκεκριμένα ζεύγη που θα χρησιμοποιηθούν. Αντιθέτως, αν τα σωστά ζεύγη διαχωριστούν από τα λανθασμένα και χρησιμοποιηθούν αποκλειστικά στην αντικειμενική συνάρτηση f, τότε το ολικό ελάχιστο της συνάρτησης θα είναι σταθερό με τιμή μηδέν, όπως και στην περίπτωση του DES με τέσσερις γύρους. Καθώς ο διαχωρισμός των σωστών κλειδιών δεν είναι πάντα εφικτός και εύκολος, μελετάμε την συμπεριφορά της προτεινόμενης προσέγγισης χρησιμοποιώντας της αντικειμενική συνάρτηση f με όλα τα ζεύγη της ΔΚ.

3.3.3 Πειραματική θεώρηση και αποτελέσματα

Για την εξαγωγή των πειραματικών αποτελεσμάτων εφαρμόσαμε τις μεθόδους ΒΣΣ και ΔΕ θεωρώντας κάθε συνιστώσα της πιθανής λύσης ως πραγματικό αριθμό μέσα στο διάστημα $[0, 1]$ και όλοι οι πληθυσμοί περιορίστηκαν μέσα στον εφικτό χώρο του προβλήματος. Για την αξιολόγηση των προτεινόμενων λύσεων εφαρμόσαμε την τεχνική της στρογγυλοποίησης των πραγματικών τιμών της λύσης στον κοντινότερο ακέραιο. Η τεχνική αυτή θεωρήθηκε ως προσέγγιση για την διακριτή βελτιστοποίηση στη μελέτη [171] και προτάθηκε για εφαρμογή στις μεθόδους ΒΣΣ και ΔΕ στην εργασία [111] με υψηλά ποσοστά επιτυχίας σε προβλήματα ελέγχου (benchmarks) αλλά και άλλες εφαρμογές.

Για την μέθοδο ΒΣΣ μελετήθηκαν και οι δύο παραλλαγές ολικής και τοπικής γειτονιάς και για την μέθοδο ΔΕ θεωρήθηκαν και οι πέντε διαφορετικές περιπτώσεις τελεστών που περιγράφονται στο Κεφάλαιο 2. Στη μέθοδο ΒΣΣ θέσαμε ως μέγιστη τιμή ταχυτήτων την τιμή $V_{\max} = 0.5$. Η τεχνική αυτή περιορισμού της μέγιστης τιμής των ταχυτήτων προτείνεται από την σχετική βιβλιογραφία της μεθόδου για την αποφυγή του φαινομένου έκρηξης του σμήνους. Δηλαδή, η προαναφερθείσα τιμή χρησιμοποιείται για την αποφυγή λήψης από τη μέθοδο πολύ μεγάλων τιμών ταχυτήτων που οδηγούν τα σωματίδια στο σύνορο του χώρου αναζήτησης και καταστρέφουν την δυναμική της [52]. Επίσης, οι τιμές των παραμέτρων για τη μέθοδο ΒΣΣ τέθηκαν στις τυπικές τιμές, δηλαδή $\chi = 0.729$ και $c_1 = c_2 = 2.05$, που δίνονται στη βιβλιογραφία [36], και για τη μέθοδο ΔΕ στις τιμές $CR = F = 0.5$.

Η προτεινόμενη μεθοδολογία δοκιμάστηκε για πολλά διαφορετικά αρχικά κλειδιά και αριθμό ζευγών np. Για κάθε περίπτωση, το μέγεθος του πληθυσμού ήταν ίσο με 100 και η απόδοση των μεθόδων μελετήθηκε με 100 ανεξάρτητα πειράματα. Ένα πείραμα θεωρείται επιτυχές αν η μέθοδος εντοπίζει τον ολικό ελαχιστοποιητή χρησιμοποιώντας μέχρι ένα προκαθορισμένο αριθμό συναρτησιακών υπολογισμών. Το όριο αυτό των συναρτησιακών υπολογισμών και για το κρυπτοσύστημα DES με τέσσερις γύρους αλλά και για το DES με έξι γύρους τέθηκε ίσο με 2^{14}. Για τα υπολειπόμενα ψηφία του κλειδιού του DES με τέσσερις γύρους, τα αποτελέσματα για έξι διαφορετικά κλειδιά, k_i, $i = 1, 2, \ldots, 6$, και για ζεύγη δοκιμών πλήθους, np, ίσο με 20 και 50, δίνονται στους Πίνακες 3.4, 3.5, αντίστοιχα.

Αναφορικά με το συμβολισμό που χρησιμοποιείται στους πίνακες των αποτελεσμάτων,

Πίνακας 3.4: Αποτελέσματα για το κρυπτοσύστημα DES με τέσσερις γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 20$ ζεύγη δοκιμών.

Κλειδί	Μέθοδος	Ποσοστό Επιτυχίας	Μέση Τιμή Συναρτ.Υπολογ.
k_1	ΒΣΣΟΠ	99%	742.42
	ΒΣΣΤΠ1	100%	1773.00
	ΒΣΣΤΠ2	100%	1255.00
	ΔΕ1	100%	614.00
	ΔΕ2	100%	1406.00
	ΔΕ3	100%	780.00
	ΔΕ4	100%	588.00
	ΔΕ5	100%	1425.00
k_2	ΒΣΣΟΠ	99%	911.11
	ΒΣΣΤΠ1	100%	2665.00
	ΒΣΣΤΠ2	100%	1650.00
	ΔΕ1	100%	603.00
	ΔΕ2	100%	1518.00
	ΔΕ3	100%	879.00
	ΔΕ4	100%	615.00
	ΔΕ5	100%	1649.00
k_3	ΒΣΣΟΠ	94%	1117.02
	ΒΣΣΤΠ1	99%	2447.48
	ΒΣΣΤΠ2	100%	1688.00
	ΔΕ1	99%	693.94
	ΔΕ2	100%	1497.00
	ΔΕ3	100%	805.00
	ΔΕ4	100%	690.00
	ΔΕ5	100%	1427.00
k_4	ΒΣΣΟΠ	96%	876.04
	ΒΣΣΤΠ1	100%	2089.00
	ΒΣΣΤΠ2	100%	1418.00
	ΔΕ1	99%	701.01
	ΔΕ2	100%	1378.00
	ΔΕ3	100%	843.00
	ΔΕ4	100%	568.00
	ΔΕ5	100%	1362.00
k_5	ΒΣΣΟΠ	97%	900.00
	ΒΣΣΤΠ1	99%	1979.80
	ΒΣΣΤΠ2	100%	1496.00
	ΔΕ1	100%	662.00
	ΔΕ2	100%	1493.00
	ΔΕ3	100%	848.00
	ΔΕ4	100%	662.00
	ΔΕ5	100%	1542.00
k_6	ΒΣΣΟΠ	93%	1457.00
	ΒΣΣΤΠ1	95%	4475.79
	ΒΣΣΤΠ2	99%	2913.13
	ΔΕ1	100%	651.00
	ΔΕ2	100%	1717.00
	ΔΕ3	100%	1063.00
	ΔΕ4	99%	725.25
	ΔΕ5	100%	1583.00

Πίνακας 3.5: Αποτελέσματα για το κρυπτοσύστημα DES με τέσσερις γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 50$ ζεύγη δοκιμών.

Κλειδί	Μέθοδος	Ποσοστό Επιτυχίας	Μέση Τιμή Συναρτ.Υπολογ.
k_1	ΒΣΣΟΠ	99%	860.61
	ΒΣΣΤΠ1	100%	1698.00
	ΒΣΣΤΠ2	100%	1141.00
	ΔΕ1	100%	485.00
	ΔΕ2	100%	1215.00
	ΔΕ3	100%	785.00
	ΔΕ4	100%	553.00
	ΔΕ5	100%	1382.00
k_2	ΒΣΣΟΠ	94%	741.49
	ΒΣΣΤΠ1	100%	1367.00
	ΒΣΣΤΠ2	100%	1100.00
	ΔΕ1	99%	490.91
	ΔΕ2	100%	1081.00
	ΔΕ3	100%	669.00
	ΔΕ4	100%	521.00
	ΔΕ5	100%	1128.00
k_3	ΒΣΣΟΠ	99%	631.31
	ΒΣΣΤΠ1	100%	1217.00
	ΒΣΣΤΠ2	100%	1035.00
	ΔΕ1	100%	385.00
	ΔΕ2	100%	1006.00
	ΔΕ3	100%	546.00
	ΔΕ4	100%	409.00
	ΔΕ5	100%	1016.00
k_4	ΒΣΣΟΠ	90%	947.78
	ΒΣΣΤΠ1	98%	2292.88
	ΒΣΣΤΠ2	100%	1588.00
	ΔΕ1	98%	666.33
	ΔΕ2	100%	1342.00
	ΔΕ3	100%	838.00
	ΔΕ4	99%	649.50
	ΔΕ5	100%	1294.00
k_5	ΒΣΣΟΠ	100%	707.00
	ΒΣΣΤΠ1	100%	1763.00
	ΒΣΣΤΠ2	100%	1193.00
	ΔΕ1	100%	445.00
	ΔΕ2	100%	1127.00
	ΔΕ3	100%	684.00
	ΔΕ4	100%	465.00
	ΔΕ5	100%	1131.00
k_6	ΒΣΣΟΠ	96%	880.21
	ΒΣΣΤΠ1	100%	2009.00
	ΒΣΣΤΠ2	100%	1390.00
	ΔΕ1	100%	507.00
	ΔΕ2	100%	1250.00
	ΔΕ3	100%	692.00
	ΔΕ4	100%	563.00
	ΔΕ5	100%	1230.00

ΒΣΣΟΠ είναι η παραλλαγή ολικής γειτονιάς της μεθόδου ΒΣΣ με παράγοντα περιορισμού, ΒΣΣΤΠ1 είναι η παραλλαγή τοπικής γειτονιάς μεγέθους 1 της μεθόδου ΒΣΣ με παράγοντα περιορισμού, ΒΣΣΤΠ2 είναι η παραλλαγή τοπικής γειτονιάς μεγέθους 2 της μεθόδου ΒΣΣ με παράγοντα περιορισμού, και ΔΕ1, ΔΕ2, ΔΕ3, ΔΕ4, ΔΕ5 είναι οι πέντε διαφορετικές εκδοχές της μεθόδου ΔΕ που δίνονται από τις Εξισώσεις (2.3),(2.7),(2.8),(2.9),(2.10), αντίστοιχα. Σε κάθε πίνακα καταγράφεται το ποσοστό επιτυχίας κάθε μεθόδου, δηλαδή ο αριθμός των φορών που η μέθοδος ήταν επιτυχής στον εντοπισμό του ολικού ελαχιστοποιητή με το προκαθορισμένο όριο συναρτησιακών υπολογισμών, καθώς και η μέση τιμή των συναρτησιακών υπολογισμών που απαιτήθηκαν για τα επιτυχή πειράματα.

Για τα υπολειπόμενα ψηφία του DES με έξι γύρους, όπου και τα σωστά και τα λανθασμένα ζεύγη χρησιμοποιούνται για την κατασκευή της αντικειμενικής συνάρτησης, τα αποτελέσματα για τα ίδια έξι κλειδιά που δοκιμάστηκαν για την περίπτωση του DES με τέσσερις γύρους και για πλήθος ζευγών δοκιμών, np, ίσο με 200, δίνονται στον Πίνακα 3.6.

Τα αποτελέσματα για το πρόβλημα εύρεσης των υπολειπόμενων (μετά την εφαρμογή της ΔΚ) ψηφίων του κλειδιού του DES με τέσσερις γύρους δείχνουν ότι οι χρησιμοποιούμενες μέθοδοι μπορούν να εντοπίσουν τον ολικό ελαχιστοποιητή, δηλαδή τα 14 υπολειπόμενα ψηφία του κλειδιού, με σχετικά χαμηλό υπολογιστικό κόστος σε σχέση με την μέθοδο της εξαντλητικής αναζήτησης. Τα ποσοστά επιτυχίας για όλες τις εκδοχές των δύο μεθόδων που μελετήθηκαν είναι υψηλά. Για πλήθος ζευγών np ίσο με 20 τα ποσοστά επιτυχίας κυμαίνονται από 93% έως 100%, με μέσο όρο 99.3%. Για πλήθος ζευγών np ίσο με 50 τα ποσοστά επιτυχίας ήταν μεταξύ 90% και 100%, με μέσο όρο 99.4%. Η βελτίωση των ποσοστών επιτυχίας καθώς το πλήθος των ζευγών κρυπτογραφημάτων np που δοκιμάζονται αυξάνεται είναι αναμενόμενη καθώς όσο μεγαλύτερος είναι ο αριθμός των ζευγών που χρησιμοποιούνται για την αξιολόγηση των πιθανών λύσεων τόσο μειώνεται η πιθανότητα μια λανθασμένη 14-άδα ψηφίων να αξιολογηθεί ως σωστή. Η μέση τιμή των συναρτησιακών υπολογισμών που απαιτούνται για τον εντοπισμό του ολικού ελαχιστοποιητή από όλες τις εκδοχές των μεθόδων είναι 1309 στην περίπτωση όπου $np = 20$ και 982 στην περίπτωση όπου $np = 50$. Αυτό σημαίνει ότι καθώς περισσότερα ζεύγη κρυπτογραφημάτων ενσωματώνονται στην αντικειμενική συνάρτηση, η αξιολόγηση των πιθανών λύσεων είναι πιο ακριβής αλλά και ο εντοπισμός του ολικού ελαχιστοποιητή γίνεται ευκολότερα. Ωστόσο, ο αριθμός των ζευγών κρυπτογραφημάτων που χρησιμοποιούνται από την προτεινόμενη μεθοδολογία δεν θα πρέπει να ξεπερνά τον αντίστοιχο αριθμό ζευγών που χρησιμοποιούνται από την ΔΚ για το αρχικό πρόβλημα, καθώς αυτό θα σήμαινε αύξηση του συνολικού κόστους της κρυπτανάλυσης ως προς τις κρυπτογραφήσεις και τις αποκρυπτογραφήσεις.

Αναφορικά με τις διαφορετικές παραλλαγές της μεθόδου ΒΣΣ, η τοπική παραλλαγή με μέγεθος γειτονιάς 2 (ΒΣΣΤΠ2) είχε ποσοστά επιτυχίας κοντά στο 100%, για όλες τις περιπτώσεις του πρώτου προβλήματος, με μέση τιμή συναρτησιακών υπολογισμών ίση με 1489. Η ολική παραλλαγή της ΒΣΣ (ΒΣΣΟΠ) πέτυχε ποσοστά επιτυχίας από 93% έως 100% στις διαφορετικές περιπτώσεις του προβλήματος, αλλά με μέσο όρο 898 συναρτησιακών υπολογισμών. Αυτό σημαίνει ότι παρά το γεγονός ότι η ολική παραλλαγή της μεθόδου ΒΣΣ επιτυγχάνει συνολικά χαμηλότερα ποσοστά επιτυχίας, στις περιπτώσεις όπου και οι δύο παραλλαγές της μεθόδου, ολική και τοπική, καταφέρνουν να εντοπίσουν τον ελαχιστοποιητή, η ολική παραλλαγή απαιτεί λιγότερους συναρτησιακούς υπολογισμούς από την τοπική παραλλαγή.

Οι διαφορετικές εκδοχές της μεθόδου ΔΕ παρουσίασαν σταθερή και παρόμοια μεταξύ τους συμπεριφορά, με μέσο όρο ποσοστών επιτυχίας 100% σε όλες τις περιπτώσεις. Μια μικρή εξαίρεση αποτέλεσε η εκδοχή ΔΕ4 που πέτυχε ποσοστό επιτυχίας 99% σε δύο περιπτώσεις του προβλήματος. Ο ΔΕ1 απαίτησε τον χαμηλότερο μέσο όρο συναρτησιακών υπολογισμών (576) μεταξύ όλων των θεωρούμενων μεθόδων και των παραλλαγών τους.

Από τους Πίνακες 3.4, 3.5 και 3.6, παρατηρούμε ότι υπάρχει σημαντική διαφορά στα ποσοστά επιτυχίας των μεθόδων για το κρυπτοσύστημα DES με τέσσερις γύρους και το DES με έξι γύρους. Αυτό αποδίδεται στο γεγονός ότι στην πρώτη περίπτωση χρησιμοποιούμε μια

Πίνακας 3.6: Αποτελέσματα για το κρυπτοσύστημα DES με έξι γύρους για έξι διαφορετικά κλειδιά χρησιμοποιώντας $np = 200$ ζεύγη δοκιμών.

Κλειδί	Μέθοδος	Ποσοστό Επιτυχίας	Μέση Τιμή Συναρτ.Υπολογ.
k_1	ΒΣΣΟΠ	26%	7038.46
	ΒΣΣΤΠ1	9%	2188.89
	ΒΣΣΤΠ2	8%	3862.50
	ΔΕ1	36%	5191.67
	ΔΕ2	52%	5515.39
	ΔΕ3	41%	5807.32
	ΔΕ4	51%	6364.71
	ΔΕ5	59%	6855.93
k_2	ΒΣΣΟΠ	24%	5037.50
	ΒΣΣΤΠ1	3%	1500.00
	ΒΣΣΤΠ2	7%	2357.14
	ΔΕ1	34%	6535.29
	ΔΕ2	58%	6968.97
	ΔΕ3	40%	5945.00
	ΔΕ4	39%	6897.44
	ΔΕ5	61%	6932.79
k_3	ΒΣΣΟΠ	41%	4902.44
	ΒΣΣΤΠ1	6%	4533.33
	ΒΣΣΤΠ2	5%	7340.00
	ΔΕ1	48%	5070.83
	ΔΕ2	61%	6967.21
	ΔΕ3	53%	6698.11
	ΔΕ4	48%	5889.58
	ΔΕ5	56%	7926.79
k_4	ΒΣΣΟΠ	47%	4912.77
	ΒΣΣΤΠ1	13%	4407.69
	ΒΣΣΤΠ2	23%	4134.78
	ΔΕ1	57%	6491.23
	ΔΕ2	76%	7594.74
	ΔΕ3	66%	6418.18
	ΔΕ4	72%	5741.67
	ΔΕ5	76%	7001.32
k_5	ΒΣΣΟΠ	36%	5575.00
	ΒΣΣΤΠ1	4%	1950.00
	ΒΣΣΤΠ2	5%	4700.00
	ΔΕ1	51%	5688.24
	ΔΕ2	62%	7803.23
	ΔΕ3	57%	5229.83
	ΔΕ4	53%	5377.36
	ΔΕ5	64%	6387.50
k_6	ΒΣΣΟΠ	37%	5624.32
	ΒΣΣΤΠ1	5%	2920.00
	ΒΣΣΤΠ2	9%	3377.78
	ΔΕ1	49%	5681.63
	ΔΕ2	63%	7380.95
	ΔΕ3	50%	7048.00
	ΔΕ4	51%	5621.57
	ΔΕ5	64%	7679.69

χαρακτηριστική με πιθανότητα 1 ενώ στην δεύτερη περίπτωση η χαρακτηριστική έχει μικρότερη πιθανότητα (1/16). Αυτό σημαίνει ότι στο σύνολο των 200 ζευγών κρυπτογραφημάτων που χρησιμοποιούνται στην αντικειμενική συνάρτηση, περίπου 12 ζεύγη είναι σωστά και προτείνουν την σωστή 14-άδα ψηφίων, ενώ τα υπόλοιπα 188 ζεύγη προτείνουν τυχαία 14-άδες ψηφίων μειώνοντας κατ΄ αυτόν τον τρόπο την πιθανότητα η προτεινόμενη 14-άδα να είναι σωστή. Συνεπώς, καθώς η αντικειμενική συνάρτηση γίνεται περισσότερο αξιόπιστη όταν περισσότερα σωστά ζεύγη είναι διαθέσιμα, ή ισοδύναμα όταν η πιθανότητα της χρησιμοποιούμενης χαρακτηριστικής είναι μεγάλη, είναι αναμενόμενο ότι στην περίπτωση των τεσσάρων γύρων η απόδοση των μεθόδων θα να είναι καλύτερη από ότι στην περίπτωση των έξι γύρων. Παρότι τα λανθασμένα ζεύγη που συμπεριλαμβάνονται στην αντικειμενική συνάρτηση του DES με έξι γύρους είναι παραπλανητικά για την αξιολόγηση της σωστής 14-άδας υπολειπόμενων ψηφίων, η ολική παραλλαγή της μεθόδου ΒΣΣ (ΒΣΣΟΠ) και όλες οι εκδοχές της μεθόδου ΔΕ (ΔΕ1-ΔΕ5) κατάφεραν να εντοπίσουν τα σωστά ψηφία κατά μέσο όρο στο 35% των ανεξάρτητων πειραμάτων η μέθοδος ΒΣΣ και στο 55% των πειραμάτων οι εκδοχές της ΔΕ για όλα τα έξι διαφορετικά κλειδιά που μελετήθηκαν (Πίνακας 3.6). Οι συναρτησιακοί υπολογισμοί που απαιτήθηκαν για τον εντοπισμό της σωστής 14-άδας ψηφίων του κλειδιού στην περίπτωση του DES με έξι γύρους ήταν κατά μέσο όρο 5600 για όλες τις μεθόδους.

Τέλος, μια ενδιαφέρουσα παρατήρηση που προέκυψε από τα αποτελέσματα της προτεινόμενης μεθοδολογίας είναι ότι στην περίπτωση του κρυπτοσυστήματος DES με τέσσερις γύρους όλες οι μέθοδοι σε ανεξάρτητα πειράματα εντόπισαν τέσσερις διαφορετικές 14-άδες που ικανοποιούν το κριτήριο της αντικειμενικής συνάρτησης. Οι τέσσερις αυτές λύσεις διέφεραν σε δύο σταθερές θέσεις, το 10-ο και το 36-ο ψηφίο του κλειδιού του DES. Στην περίπτωση του DES με έξι γύρους μόνο μία λύση, η σωστή, εντοπίστηκε από όλες τις μεθόδους.

Τα αποτελέσματα δείχνουν ότι η προτεινόμενη μεθοδολογία είναι αποτελεσματική στην αντιμετώπιση τέτοιου είδους προβλημάτων, καθώς για το κρυπτοσύστημα DES με τέσσερις γύρους κατάφερε να επιλύσει το πρόβλημα χρησιμοποιώντας κατά μέσο όρο 576 συναρτησιακούς υπολογισμούς σε αντίθεση με την περίπτωση της μεθοδολογίας εξαντλητικής αναζήτησης που απαιτεί $2^{14} = 16384$ υπολογισμούς. Επιπλέον, τα αποτελέσματα του DES με έξι γύρους δείχνουν ότι η αποδοτικότητά της εξαρτάται κυρίως από την κατασκευή της αντικειμενικής συνάρτησης. Τέλος, είναι σημαντικό ότι η μεθοδολογία αυτή μπορεί να εφαρμοστεί για όλα τα κρυπτοσυστήματα Feistel που υπόκεινται σε ΔΚ και ενδιαφέρον παρουσιάζει η πιθανή εφαρμογή της για την εύρεση ολόκληρου του κλειδιού των κρυπτοσυστημάτων Feistel.

3.4 Κατασκευή S-boxes με μεθόδους Εξελικτικού Υπολογισμού

Ένα από τα σημαντικότερα δομικά στοιχεία πολλών σύγχρονων κρυπτοσυστημάτων συμμετρικού κλειδιού είναι τα *κυτία (κουτιά) αντικατάστασης (substitution boxes (S-boxes))*. Ουσιαστικά, τα S-boxes είναι μη-γραμμικές απεικονίσεις που λαμβάνουν ως ορίσματα έναν αριθμό δυαδικών ψηφίων και τα μετασχηματίζουν σε κάποιου πλήθους δυαδικά ψηφία. Τα S-boxes έχουν ιδιαίτερα σημαντικό ρόλο στην κρυπτογραφία καθώς χρησιμοποιούνται για να παρέχουν την ιδιότητα της σύγχυσης (confusion) στο αντίστοιχο κρυπτοσύστημα και σε πολλές περιπτώσεις αποτελούν το μόνο μη-γραμμικό κομμάτι του κρυπτοσυστήματος (για παράδειγμα στο κρυπτοσύστημα DES). Καθώς η ασφάλεια των κρυπτοσυστημάτων που περιλαμβάνουν S-boxes βασίζεται κυρίως στην επιλογή τους, ένα μεγάλο τμήμα της ερευνητικής δραστηριότητας από το πεδίο της κρυπτογραφίας αφιερώνεται στην κατασκευή ισχυρών S-boxes. Πρόσφατα, η απόδοση εξελικτικών ευρετικών μεθόδων, όπως η μέθοδος ανάβασης λόφου (hill climbing) [134], οι Γενετικοί Αλγόριθμοι [135] και η μέθοδος Προσομοιωμένης Ανόπτησης (Simulated Annealing) [34], στην κατασκευή ισχυρών S-boxes μελετήθηκε με αρκετά καλά αποτελέσματα.

Στην εργασία αυτή προτείνουμε μια νέα μεθοδολογία για την κατασκευή ισχυρών S-boxes

και εφαρμόζουμε δύο μεθόδους ΕΥ, την μέθοδο Βελτιστοποίησης με Σμήνος Σωματιδίων (ΒΣΣ) και τον Διαφοροεξελικτικό Αλγόριθμο (ΔΕ) για την επίλυση του προβλήματος.

3.4.1 Θεωρητικά στοιχεία για τα S-boxes

Έστω ότι η $f : \mathbb{B}^n \mapsto \mathbb{B}^m$ είναι ένα S-box που απεικονίζει n Boolean τιμές σε m Boolean τιμές. Στην περίπτωση που είναι $m = 1$, η f είναι συνάρτηση Boole απλής εξόδου και αν ο αριθμός των εισόδων που απεικονίζονται στην τιμή 0 είναι ίσος με τον αριθμό των εισόδων που απεικονίζονται στην τιμή 1 τότε η συνάρτηση Boole καλείται *ισορροπημένη (balanced)*. Η ισορροπία είναι μια ιδιότητα πολύ σημαντική για τις συναρτήσεις Boole που χρησιμοποιούνται σε εφαρμογές της κρυπτογραφίας καθώς εξασφαλίζει ότι η συνάρτηση δεν προσεγγίζεται από καμία σταθερή συνάρτηση. Γενικεύοντας την έννοια της ισορροπίας για συναρτήσεις πολλαπλής εξόδου, αν κάθε δυνατή τιμή εξόδου αποτελούμενη από m δυαδικά ψηφία εμφανίζεται ίσο αριθμό φορών ως έξοδος της συνάρτησης, δηλαδή 2^{n-m} φορές, τότε η συνάρτηση καλείται *κανονική (regular)*. Στην περίπτωση όπου $n = m$, το S-box καλείται *αμφιμονοσήμαντο (bijective)* και όλες οι πιθανές τιμές εξόδου εμφανίζονται ακριβώς μια φορά. Για λόγους απλότητας στη συνέχεια θα αναφέρουμε τις συναρτήσεις Boole απλής εξόδου απλά ως συναρτήσεις Boole και τις περιπτώσεις συναρτήσεων Boole πολλαπλής εξόδου ως S-boxes.

Για τον σχεδιασμό κρυπτογραφικά ισχυρών συναρτήσεων Boole και S-boxes κατάλληλων για κρυπτογραφικές εφαρμογές, υπάρχουν δύο κλασικά μέτρα ποιότητας, η *μη-γραμμικότητα (nonlinearity)* και η *αυτοσυσχέτιση (autocorrelation)*. Προκειμένου να δώσουμε τους ορισμούς των δύο αυτών μέτρων είναι απαραίτητο να δούμε τις έννοιες των γραμμικών και affine (ομοπαραλληλικών) συναρτήσεων Boole, τον μετασχηματισμό Walsh Hadamard, τον πίνακα αλήθειας πολικότητας (polarity truth table) και το θεώρημα του Parseval.

Μια γραμμική συνάρτηση Boole επιλεγμένη από το $\omega \in \mathbb{B}^n$ συμβολίζεται με L_ω και είναι $L_\omega(x) = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus w_n x_n$, όπου το $w_i x_i$, για $i = 1, 2, \ldots, n$, συμβολίζει την λογική πράξη AND των i-οστών δυαδικών ψηφίων του ω και του x, και το $\oplus$ συμβολίζει τη λογική πράξη XOR. Το σύνολο των affine συναρτήσεων Boole αποτελείται από το σύνολο των γραμμικών συναρτήσεων Boole και του συμπληρώματός του.

Για μια συνάρτηση Boole f μια χρήσιμη αναπαράσταση είναι ο πίνακας αλήθειας πολικότητας που δίνεται ως $\hat{f}(x) = (-1)^{f(x)}$. Ο μετασχηματισμός Walsh Hadamard μιας συνάρτησης Boole f ορίζεται ως

$$\hat{F}_f(\omega) = \sum_{x \in \mathbb{B}^n} \hat{f}(x)\hat{L}_\omega(x).$$

Ο μετασχηματισμός Walsh Hadamard είναι ένα μέτρο της συσχέτισης (correlation) της συνάρτησης Boole f με το σύνολο των γραμμικών συναρτήσεων Boole. Γενικά, δύο συναρτήσεις Boole f, h θεωρούνται *μη-συσχετισμένες (uncorrelated)* όταν ισχύει ότι

$$\sum_x \hat{f}(x)\hat{h}(x) = 0.$$

Η μέγιστη απόλυτη τιμή που λαμβάνεται από τον μετασχηματισμό Walsh Hadamard συμβολίζεται ως

$$WH_{\max}(f) = \max_{\omega \in \mathbb{B}^n} \left|\hat{F}_f(\omega)\right|$$

και συνδέεται με την μη-γραμμικότητα της συνάρτησης f. Συγκεκριμένα, η μη-γραμμικότητα N_f μιας συνάρτησης Boole f ορίζεται ως

$$N_f = (2^n - WH_{\max}(f))/2.$$

Αναφορικά με τον μετασχηματισμό Walsh Hadamard, όπως αποδεικνύεται από το θεώρημα του Parseval ισχύει ότι $\sum_{\omega \in \mathbb{B}^n} (\hat{F}_f(\omega))^2 = 2^{2^n}$, που συνεπάγεται ότι

$$WH_{\max}(f) \geqslant 2^{n/2}.$$

Το σύνολο των συναρτήσεων με μη-γραμμικότητα ίση με αυτό το κατώτερο φράγμα καλούνται *Bent συναρτήσεις* αλλά δεν είναι ποτέ ισορροπημένες. Το σύνολο των ισορροπημένων συναρτήσεων με τη μέγιστη μη-γραμμικότητα και ο προσδιορισμός των αντίστοιχων φραγμάτων για τις ισορροπημένες συναρτήσεις αποτελούν σημαντικά ανοικτά ερευνητικά προβλήματα [134].

Η αυτοσυσχέτιση μιας συνάρτησης Boole f είναι ένα μέτρο της αυτοομοιότητάς της και ορίζεται ως

$$\hat{r}_f(s) = \sum_{x \in \mathbb{B}^n} \hat{f}(x)\hat{f}(x \oplus s),$$

όπου $s \in \mathbb{B}^n$. Η μέγιστη απόλυτη τιμή που λαμβάνεται από την αυτοσυσχέτιση συμβολίζεται ως $AC_{\max}$ και είναι

$$AC_{\max}(f) = \max_{s \in \mathbb{B}^n \setminus \{0^n\}} \big| \sum_{x \in \mathbb{B}^n} \hat{f}(x)\hat{f}(x \oplus s) \big|.$$

Η μη-γραμμικότητα και η αυτοσυσχέτιση ως μέτρα των συναρτήσεων Boole μπορούν να επεκταθούν στα S-boxes ορίζοντας το σύνολο των συναρτήσεων f_β, που είναι γραμμικοί συνδυασμοί των ψηφίων εξόδου του αντίστοιχου S-box. Συγκεκριμένα, για ένα S-box $f : \mathbb{B}^n \mapsto \mathbb{B}^m$, μια συνάρτηση $f_\beta(x)$, για κάθε $\beta \in \mathbb{B}^m$, που είναι γραμμικός συνδυασμός των m ψηφίων εξόδου της f, ορίζεται ως

$$f_\beta(x) = \beta_1 f_1(x) \oplus \cdots \oplus \beta_m f_m(x),$$

όπου $f_j(x)$, για $j = 1, \ldots, m$ συμβολίζει το j-οστό δυαδικό ψηφίο της εξόδου του S-box. Υπάρχουν $2^m - 1$ μη τετριμμένες συναρτήσεις f_β, και για κάθε τέτοια συνάρτηση η τιμή του μετασχηματισμού Walsh Hadamard, που συμβολίζεται ως $\hat{F}_\beta(\omega)$ και η τιμή αυτοσυσχέτισης που συμβολίζεται ως $\hat{r}_\beta(s)$, προκύπτουν άμεσα από τους προηγούμενους ορισμούς. Κατ΄ αυτό τον τρόπο, η μη-γραμμικότητα ενός S-box είναι η χαμηλότερη μη-γραμμικότητα μεταξύ όλων των $2^m - 1$ αντίστοιχων $f_\beta(x)$ συναρτήσεων, και η αυτοσυσχέτιση του S-box είναι η υψηλότερη αυτοσυσχέτιση μεταξύ των ίδιων $f_\beta(x)$ συναρτήσεων.

3.4.2 Θεώρηση του προβλήματος

Η έρευνα για τον σχεδιασμό συναρτήσεων Boole και S-boxes που αντιμετωπίζει το πρόβλημα ως πρόβλημα βελτιστοποίησης, στοχεύει στην εύρεση συναρτήσεων με υψηλή μη-γραμμικότητα ή/και χαμηλή αυτοσυσχέτιση. Το πρόβλημα εύρεσης της συνάρτησης Boole f^* με τη μέγιστη μη-γραμμικότητα, μπορεί να δοθεί ως πρόβλημα μεγιστοποίησης, δηλαδή μεγιστοποίησε ως προς f την συνάρτηση

$$N_f = (2^n - WH_{\max}(f))/2,$$

ή ισοδύναμα, ως πρόβλημα ελαχιστοποίησης μέσω της μέγιστης απόλυτης τιμής του μετασχηματισμού Walsh Hadamard, δηλαδή ελαχιστοποίησε ως προς f την συνάρτηση

$$WH_{\max}(f) = \max_{\omega \in \mathbb{B}^n} \big|\hat{F}_f(\omega)\big|.$$

Για την συνάρτηση Boole f^{**} με την χαμηλότερη αυτοσυσχέτιση, το πρόβλημα θεωρείται ως ελαχιστοποίηση ως προς f της συνάρτησης

$$AC_{\max}(f) = \max_{s \in \mathbb{B}^n \setminus \{0^n\}} \big| \sum_{x \in \mathbb{B}^n} \hat{f}(x)\hat{f}(x \oplus s) \big|.$$

Για την περίπτωση των S-boxes, οι παραπάνω αντικειμενικές συναρτήσεις γενικεύονται ως εξής. Αναφορικά με τη μη-γραμμικότητα ενός S-box, το πρόβλημα είναι η ελαχιστοποίηση ως προς f της συνάρτησης

$$\max_{\beta \in \mathbb{B}^m,\, \omega \in \mathbb{B}^n} \big|\hat{F}_\beta(\omega)\big|, \tag{3.7}$$

και για την αυτοσυσχέτιση ενός S-box, το πρόβλημα είναι η ελαχιστοποίηση ως προς f της συνάρτησης

$$\max_{\beta\in\mathbb{B}^m\setminus\{0^m\},\, s\in\mathbb{B}^n\setminus\{0^n\}} \left|\hat{r}_\beta(s)\right|. \tag{3.8}$$

3.4.3 Προτεινόμενη μεθοδολογία

Για την επίλυση του προβλήματος σχεδίασης των S-boxes ως πρόβλημα βελτιστοποίησης, εφαρμόζουμε δύο μεθόδους Εξελικτικού Υπολογισμού, την μέθοδο Βελτιστοποίησης με Σμήνος Σωματιδίων και τον Διαφοροεξελικτικό Αλγόριθμο. Σε αυτή την ενότητα περιγράφονται οι λεπτομέρειες της προτεινόμενης μεθοδολογίας.

Προκειμένου να υλοποιήσουμε τις μεθόδους βελτιστοποίησης για την επίλυση του προβλήματος κατασκευής των S-boxes, είναι απαραίτητο να θεωρήσουμε την κατάλληλη αναπαράσταση κάθε πιθανής λύσης. Σκοπός μας είναι η εύρεση του S-box $f : \mathbb{B}^n \mapsto \mathbb{B}^m$, με n Boolean ψηφία εισόδου και m Boolean ψηφία εξόδου, που ικανοποιεί την ιδιότητα της υψηλότερης δυνατής μη-γραμμικότητας ή την ιδιότητα της χαμηλότερης δυνατής αυτοσυσχέτισης ή και τα δύο. Η αναπαράσταση που χρησιμοποιούμε για κάθε πιθανή λύση είναι ο πίνακας αλήθειας των εξόδων του αντίστοιχου S-box σε δεκαδική μορφή. Δηλαδή, η αναπαράσταση της πιθανής λύσης γίνεται μέσω ενός 2^n-διάστατου διανύσματος ακέραιων συνιστωσών, όπου κάθε συνιστώσα αναπαριστά την αντίστοιχη έξοδο m δυαδικών ψηφίων του S-box σε δεκαδική μορφή. Με τον τρόπο αυτό το αρχικό πρόβλημα βελτιστοποίησης μετατρέπεται σε πρόβλημα ακέραιης βελτιστοποίησης. Για την επίλυση του προβλήματος θεωρήσαμε τις μεθόδους ΒΣΣ και ΔΕ. Οι δύο αυτές μέθοδοι αρχικά σχεδιάστηκαν για την επίλυση προβλημάτων βελτιστοποίησης πραγματικών αριθμών, όμως η αποτελεσματικότητά τους στην επίλυση προβλημάτων ακέραιης βελτιστοποίησης μέσω της τεχνικής της στρογγυλοποίησης στον πλησιέστερο ακέραιο έχει επίσης αποδειχθεί πειραματικά [111].

Όπως προαναφέραμε, η ισορροπία (balance) είναι μια πολύ σημαντική ιδιότητα για τις συναρτήσεις Boole που χρησιμοποιούνται σε εφαρμογές κρυπτογραφίας. Η ιδιότητα αυτή κληρονομείται στα S-boxes μέσω της κανονικότητας (regularity), καθώς ένα S-box είναι κανονικό αν και μόνο αν όλοι οι μη μηδενικοί γραμμικοί συνδυασμοί της εξόδου του είναι ισορροπημένες συναρτήσεις Boole. Για το λόγο αυτό αναζητούμε κανονικά S-boxes με υψηλή μη-γραμμικότητα ή/ και χαμηλή αυτοσυσχέτιση. Η αναπαράσταση της πιθανής λύσης που χρησιμοποιήθηκε συνεπάγεται την αναζήτηση πιθανών λύσεων στο χώρο όλων των S-boxes της μορφής $f : \mathbb{B}^n \mapsto \mathbb{B}^m$, κανονικών ή μη. Στη σχετική βιβλιογραφία [34,134,135] προκειμένου να επιτευχθούν κανονικά S-boxes ως λύσεις, γίνεται μια αρχικοποίηση με τυχαία κανονικά S-boxes ως υποψήφιες λύσεις και στη συνέχεια η μέθοδος βελτιστοποίησης που χρησιμοποιείται είναι υπεύθυνη για την διατήρηση της κανονικότητας των λύσεων στους παραγόμενους απογόνους. Στην παρούσα μελέτη, για την κατασκευή κανονικών S-boxes, προτείναμε μια εναλλακτική τεχνική που την ονομάσαμε «*Τεχνική Κατασκευής Κανονικότητας*» (*Regularity Constraction Technique*). Με την χρήση της τεχνικής αυτής επιτρέπεται η εξερεύνηση ολόκληρου του χώρου αναζήτησης από την μέθοδο που εφαρμόζεται, δηλαδή επιτρέπεται στη μέθοδο η αναζήτηση μεταξύ εφικτών λύσεων (κανονικών S-boxes) και μη-εφικτών λύσεων (μη κανονικών S-boxes). Για την αξιολόγηση της πιθανής λύσης στην περίπτωση που αυτή είναι μη-εφικτή, η προτεινόμενη υποψήφια λύση μετασχηματίζεται στην κοντινότερη, αναφορικά με την απόσταση Hamming, εφικτή λύση. Δηλαδή, κάθε συνιστώσα στο διάνυσμα της προτεινόμενης λύσης με τιμή που διαταράσσει την κανονικότητα της λύσης μετατρέπεται στην πλησιέστερη δυνατή τιμή που αποδίδει κανονικότητα στη προτεινόμενη λύση. Με την τεχνική αυτή η μέθοδος διατηρεί την δυναμική της και μπορεί να επιτελέσει καλύτερη αναζήτηση.

Για την αρχικοποίηση του πληθυσμού των εφαρμοζόμενων μεθόδων χρησιμοποιείται η διαδικασία που προτείνεται και στη σχετική βιβλιογραφία [135], σύμφωνα με την οποία κατασκευάζεται ένα διάνυσμα που περιέχει 2^{n-m} αντίγραφα όλων των 2^m δυνατών εξόδων και στη συνέχεια οι συνιστώσες του μετατίθενται τυχαία ώστε να δημιουργηθεί ο τυχαίος αρχικός

πληθυσμός.

3.4.4 Πειραματική θεώρηση και αποτελέσματα

Για την επίλυση του προβλήματος εφαρμόστηκαν οι μέθοδοι ΒΣΣ και ΔΕ θεωρώντας κάθε συνιστώσα της πιθανής λύσης ως πραγματικό αριθμό στο διάστημα $[0, 2^m - 1]$ και όλοι οι πληθυσμοί που χρησιμοποιήθηκαν περιορίστηκαν στο διάστημα αυτό. Για την αξιολόγηση των προτεινόμενων λύσεων, εφαρμόστηκε η τεχνική της στρογγυλοποίησης των πραγματικών συνιστωσών της λύσης στους κοντινότερους ακέραιους [171], ακολουθούμενη από την Τεχνική Κατασκευής Κανονικότητας. Αναφορικά με την μέθοδο ΒΣΣ, θεωρήθηκε η ολική παραλλαγή της μεθόδου με παράγοντα περιορισμού (ΒΣΣΟΠ) και οι τοπικές παραλλαγές με παράγοντα περιορισμού και μέγεθος γειτονιάς 1 (ΒΣΣΤΠ1) και 2 (ΒΣΣΤΠ2), αντίστοιχα. Για την μέθοδο ΔΕ χρησιμοποιήθηκαν και οι πέντε διαφορετικοί τελεστές μετάλλαξης (ΔΕ1 - ΔΕ5) που περιγράφονται από τις Εξισώσεις (2.3),(2.7),(2.8),(2.9),(2.10), αντίστοιχα. Οι τιμές των παραμέτρων για τη μέθοδο ΒΣΣ τέθηκαν στις τυπικές τιμές, δηλαδή $\chi = 0.729$ και $c_1 = c_2 = 2.05$, που δίνονται στη βιβλιογραφία [36], και για τη μέθοδο ΔΕ στις τιμές $CR = F = 0.5$.

Η προτεινόμενη μεθοδολογία δοκιμάστηκε για αμφιμονοσήμαντα S-boxes μεγέθους $5 \times 5, 6 \times 6, 7 \times 7$ και 8×8. Για κάθε περίπτωση, το μέγεθος του πληθυσμού που χρησιμοποιήθηκε ήταν 20 και η απόδοση των μεθόδων μελετήθηκε με 100 ανεξάρτητα πειράματα. Για κάθε πείραμα χρησιμοποιήθηκε ένα κατώφλι 1000 συναρτησιακών υπολογισμών, επιτρέποντας έτσι 50 επαναλήψεις για κάθε παραλλαγή.

Στον Πίνακα 3.7 δίνονται οι βέλτιστες τιμές για την μη-γραμμικότητα και την αυτοσυσχέτιση των S-boxes, που επιτεύχθηκαν από τις μεθόδους χρησιμοποιώντας ως αντικειμενικές συναρτήσεις αυτές που περιγράφονται από τις Εξισώσεις (3.7) και (3.8), αντίστοιχα.

Πίνακας 3.7: Οι βέλτιστες τιμές μη-γραμμικότητας και αυτοσυσχέτισης, αντίστοιχα, για S-boxes μεγέθους n.

	Μη-γραμμικότητα							
n	ΒΣΣΟΠ	ΒΣΣΤΠ1	ΒΣΣΤΠ2	ΔΕ1	ΔΕ2	ΔΕ3	ΔΕ4	ΔΕ5
5	10	10	10	10	10	10	10	10
6	20	20	20	20	20	20	20	20
7	46	46	46	46	46	44	44	44
8	98	98	98	98	98	98	98	98
	Αυτοσυσχέτιση							
n	ΒΣΣΟΠ	ΒΣΣΤΠ1	ΒΣΣΤΠ2	ΔΕ1	ΔΕ2	ΔΕ3	ΔΕ4	ΔΕ5
5	16	16	16	16	16	16	16	16
6	32	32	32	32	32	32	32	32
7	56	56	56	56	56	56	56	56
8	80	88	80	88	88	80	88	88

Η προτεινόμενη μεθοδολογία απέδωσε τις ίδιες βέλτιστες τιμές μη-γραμμικότητας που βρέθηκαν και με τη μέθοδο Ανάβασης Λόφου (Hill Climbing) στη μελέτη [134] στην οποία χρησιμοποιήθηκαν οι ίδιες αντικειμενικές συναρτήσεις αλλά μέγεθος δείγματος 10000. Εξαίρεση αποτέλεσε μόνο η περίπτωση $n = 8$ για την οποία η μέθοδος Ανάβασης Λόφου πέτυχε καλύτερη τιμή μη-γραμμικότητας (100). Αυτό μπορεί να οφείλεται στο μικρότερο μέγεθος δείγματος ή πληθυσμού που χρησιμοποιήθηκε με την προτεινόμενη μεθοδολογία καθώς η διάσταση του προβλήματος αυξάνεται. Ωστόσο, συνολικά τα αποτελέσματα δείχνουν ότι η συγκεκριμένη νέα μεθοδολογία είναι αποτελεσματική στην εύρεση καλών κανονικών αμφιμονοσήμαντων S-boxes. Επιπλέον, η προτεινόμενη μεθοδολογία είναι απλή, απαιτεί μόνο τον υπολογισμό των τιμών

της αντικειμενικής συνάρτησης για τις προτεινόμενες λύσεις και μπορεί εύκολα να συνδυαστεί με εναλλακτικές τεχνικές κατασκευής κανονικότητας των λύσεων.

Στον Πίνακα 3.8 δίνονται οι βέλτιστες συνδεδεμένες τιμές μη-γραμμικότητας και αυτοσυσχέτισης που επιτεύχθηκαν από όλες τις θεωρούμενες μεθόδους και στις δύο περιπτώσεις του κριτηρίου αναζήτησης. Είναι σημαντικό να παρατηρήσουμε ότι τα αποτελέσματα υποδεικνύουν ότι υπάρχει ένας «συμβιβασμός» μεταξύ των τιμών των δύο ποσοτήτων.

Πίνακας 3.8: Βέλτιστες συνδεδεμένες τιμές μη-γραμμικότητας και αυτοσυσχέτισης για S-boxes μεγέθους n για όλες τις μεθόδους.

	(N_f, AC_{max})	
n	Κριτήριο N_f	Κριτήριο AC_{max}
5	$(10, 24)$	$(8, 16)$
6	$(20, 32)$	$(20, 32)$
7	$(46, 64)$	$(44, 56)$
8	$(98, 88)$	$(96, 80)$

Στον Πίνακα 3.9 παρουσιάζεται η συχνότητα επίτευξης των διαφορετικών τιμών μη-γραμμικότητας στα 100 ανεξάρτητα πειράματα που επιτελέστηκαν από κάθε μέθοδο. Στον πίνακα δίνονται όλες οι τιμές μη-γραμμικότητας που βρέθηκαν ακολουθούμενες από την συχνότητα εμφάνισής τους μέσα σε παρένθεση.

Αναφορικά με την απόδοση των διαφορετικών παραλλαγών των δύο εφαρμοζόμενων μεθόδων, σε όλες τις περιπτώσεις επιτεύχθηκαν οι ίδιες βέλτιστες τιμές, με εξαίρεση τις παραλλαγές ΔΕ3, ΔΕ4 και ΔΕ5 στην περίπτωση με $n = 7$, όπου η βέλτιστη τιμή μη-γραμμικότητας ήταν 44, και τις παραλλαγές ΒΣΣΤΠ1, ΔΕ1, ΔΕ2, ΔΕ4 και ΔΕ5 στην περίπτωση με $n = 8$ όπου η τιμή αυτοσυσχέτισης που επιτεύχθηκε ήταν 88.

Πίνακας 3.9: Συχνότητα επίτευξης των διαφορετικών τιμών μη-γραμμικότητας στα 100 ανεξάρτητα πειράματα.

n	5	6	7	8
ΒΣΣΟΠ	8(99) 10(1)	20(100)	44(99) 46(1)	96(28) 98(72)
ΒΣΣΤΠ1	8(99) 10(1)	20(100)	44(98) 46(2)	96(19) 98(81)
ΒΣΣΤΠ2	8(99) 10(1)	20(100)	44(99) 46(1)	96(19) 98(81)
ΔΕ1	8(99) 10(1)	20(100)	44(99) 46(1)	96(28) 98(72)
ΔΕ2	8(99) 10(1)	20(100)	44(99) 46(1)	96(31) 98(69)
ΔΕ3	8(99) 10(1)	20(100)	44(100)	96(17) 98(83)
ΔΕ4	8(99) 10(1)	20(100)	44(100)	96(42) 98(58)
ΔΕ5	8(99) 10(1)	20(100)	44(100)	96(36) 98(64)

3.5 Συμπεράσματα

Στο κεφάλαιο αυτό μελετήσαμε διάφορα προβλήματα κρυπτογραφίας και κρυπτανάλυσης με μεθόδους Εξελικτικού Υπολογισμού. Πιο αναλυτικά, αρχικά μελετήσαμε την εφαρμογή των μεθόδων ΕΥ σε τέσσερα προβλήματα κρυπτανάλυσης, μετασχηματίζοντάς τα σε προβλήματα διακριτής βελτιστοποίησης. Τα αποτελέσματα έδειξαν ότι ο μετασχηματισμός αυτών των προβλημάτων διατηρεί την πολυπλοκότητά τους καθιστώντας την εξόρυξη πληροφοριών για την δυναμική τους δύσκολη. Υποδεικνύει όμως ότι για την εφαρμογή των ΕΥ στην κρυπτανάλυση,

ένα πολύ κρίσιμο σημείο αφορά στην δημιουργία της κατάλληλης αντικειμενικής συνάρτησης ώστε αυτή να περιέχει όσο δυνατόν περισσότερη πληροφορία για το προς επίλυση πρόβλημα.

Στη συνέχεια του κεφαλαίου μελετήθηκε η χρήση των μεθόδων ΕΥ για την κρυπτανάλυση κρυπτοσυστημάτων Feistel και συγκεκριμένα για τον εντοπισμό ψηφίων του κλειδιού του κρυπτοσυστήματος DES με τέσσερις και έξι γύρους, αντίστοιχα. Τα αποτελέσματα για τα δύο αυτά προβλήματα είναι σημαντικά καθώς οι μέθοδοι εντόπισαν αποδοτικά και αποτελεσματικά την λύση και μάλιστα με τρόπο που δεν απαιτεί την παρέμβαση του χρήστη όπως συμβαίνει με άλλες μεθοδολογίες επίλυσης. Επίσης, και σε αυτή την εφαρμογή υποδεικνύεται η κρισιμότητα της αντικειμενικής συνάρτησης που περιγράφει το υπό μελέτη πρόβλημα στην απόδοση των μεθόδων ΕΥ.

Τέλος, στο κεφάλαιο αυτό μελετήθηκε η κατασκευή S-boxes με τη βοήθεια των μεθόδων ΕΥ. Τα S-boxes αποτελούν σημαντικό δομικό στοιχείο των σύγχρονων κρυπτοσυστημάτων συμμετρικού κλειδιού και η κατασκευή ισχυρών S-boxes αποτελεί κρίσιμο τμήμα της ερευνητικής δραστηριότητας του κλάδου της κρυπτογραφίας. Τα αποτελέσματα της μελέτης αυτής είναι σημαντικά καθώς η προτεινόμενη μεθοδολογία που είναι πιο απλή από τις ήδη υπάρχουσες μεθόδους επίλυσης, απέδωσε τις βέλτιστες δυνατές τιμές με μικρότερο υπολογιστικό κόστος.

ΚΕΦΑΛΑΙΟ **4**

Μελέτη προβλημάτων κρυπτογραφίας με χρήση Τεχνητών Νευρωνικών Δικτύων

4.1 Τεχνητά Νευρωνικά Δίκτυα και κρυπτολογία

Τα τελευταία δεκαπέντε χρόνια έχουν δημοσιευθεί σχετικά λίγες ερευνητικές μελέτες που συσχετίζουν τα Τεχνητά Νευρωνικά Δίκτυα (ΤΝΔ) με την κρυπτογραφία και την κρυπτανάλυση. Το 1991 ο R. Rivest παρουσίασε μια εργασία επισκόπησης που αφορούσε στη σχέση της κρυπτογραφίας και της εκπαίδευσης μηχανών [177], δίνοντας έμφαση στον τρόπο με τον οποίο τα δύο αυτά πεδία θα μπορούσαν να συνεισφέρουν ιδέες το ένα στο άλλο. Οι Blum, Furst, Kearns και Lipton στην εργασία [18] μελέτησαν πως μπορούν να δημιουργηθούν καλά κρυπτογραφικά αρχέτυπα βασισμένα σε προβλήματα εκπαίδευσης που θεωρούνται μη επιλύσιμα. Εργαζόμενος στην ίδια ιδέα, ο Pointcheval στις εργασίες [167, 168] χρησιμοποίησε ένα NP-Complete πρόβλημα βασισμένο στα ΤΝΔ για τον σχεδιασμό συγκεκριμένου τύπου ασφαλών προβλημάτων αναγνώρισης αλλά αργότερα οι Knudsen και Meier στο άρθρο [88] έδειξαν ότι το σχήμα αυτό ήταν λιγότερο ασφαλές από ότι αρχικά θεωρήθηκε.

Το 1998 ο Ramzan στη διδακτορική του διατριβή [170] «έσπασε» το κρυπτοσύστημα Unix Crypt, μια απλοποιημένη μορφή του κρυπτοσυστήματος Αίνιγμα, χρησιμοποιώντας ΤΝΔ. Το 2001 μια εφαρμογή της κρυπτολογίας στο πεδίο των ΤΝΔ προτάθηκε από τους Chang και Lu [26]. Συγκεκριμένα, πρότειναν πρωτόκολλα για «oblivious polynomial evaluation» που μπορούσαν να λειτουργήσουν κατευθείαν με αριθμούς κινητής υποδιαστολής και έδωσαν σαν παράδειγμα την μη φανερή εκπαίδευση των ΤΝΔ. Επίσης, στην εργασία [220] παρουσιάστηκε ένα γενικό παράδειγμα δημιουργίας ΤΝΔ για εφαρμογή στην οπτική κρυπτογραφία. Στις δημοσιεύσεις [80, 81] οι Δ. Καρράς και Β. Ζορκάδης χρησιμοποίησαν ΤΝΔ πρόσθιας τροφοδότησης και Hopfield για να βελτιώσουν και να ενδυναμώσουν κλασικές γεννήτριες ψευδοτυχαίων αριθμών για την ασφαλή διαχείριση συστημάτων επικοινωνίας.

Τα ΤΝΔ χρησιμοποιήθηκαν επίσης για την δημιουργία ενός νέου συστήματος ανταλλαγής κλειδιών που βασίστηκε σε ένα νέο φαινόμενο, τον συγχρονισμό των ΤΝΔ [86,87]. Ο συγχρονισμός των ΤΝΔ είναι ένα είδος αμοιβαίας εκπαίδευσης των ΤΝΔ σε κοινές εισόδους. Ωστόσο, στην μελέτη [87] αποδείχθηκε ότι το νέο πρωτόκολλο ανταλλαγής κλειδιών μπορεί να καταρρεύσει με τρεις διαφορετικούς τρόπους, χρησιμοποιώντας Γενετικούς Αλγορίθμους, γενετικές επιθέσεις και πιθανοτικές επιθέσεις, αντίστοιχα. Αργότερα, στις εργασίες [141, 182, 183] παρουσιάστηκαν μερικές τεχνικές βελτίωσης του αρχικά προτεινόμενου πρωτοκόλλου. Τέλος, η ιδέα για εφαρμογή των ΤΝΔ στην κατασκευή S-boxes παρουσιάστηκε το 2005 στην εργασία [93].

Στη συνέχεια του κεφαλαίου παρουσιάζεται η μελέτη της αποδοτικότητας των ΤΝΔ στην επίλυση κλασικών προβλημάτων κρυπτογραφίας και προβλημάτων από το πεδίο της κρυπτογραφίας των ελλειπτικών καμπυλών. Επίσης, μελετάται θεωρητικά η συσχέτιση ΤΝΔ ειδικής μορφής, των Πολυωνυμικών Δικτύων Ridge, με την επίλυση συγκεκριμένου προβλήματος κρυπτογραφίας και παρουσιάζονται τα αποτελέσματά της.

4.2 Τεχνητά Νευρωνικά Δίκτυα για κρυπτανάλυση κλασικών κρυπτοσυστημάτων

Στην ενότητα αυτή μελετάμε την απόδοση των Τεχνητών Νευρωνικών Δικτύων (ΤΝΔ) στην επίλυση μερικών κλασικών προβλημάτων κρυπτανάλυσης. Συγκεκριμένα, με την βοήθεια των ΤΝΔ μελετάμε την προσέγγιση των συναρτήσεων που σχετίζονται με το Πρόβλημα του Διακριτού Λογαρίθμου (ΠΔΛ) και το Πρόβλημα Ανταλλαγής Κλειδιών με το πρωτόκολλο Diffie-Hellman (ΠΑΚDH), στο χώρο $\mathbb{Z}_p$, όπου p είναι πρώτος αριθμός, καθώς και το πρόβλημα παραγοντοποίησης που σχετίζεται με το κρυπτοσύστημα RSA.

4.2.1 Πειραματική θεώρηση και αποτελέσματα

Αλγόριθμοι εκπαίδευσης: Στην μελέτη αυτή οι αλγόριθμοι εκπαίδευσης ΤΝΔ που χρησιμοποιήθηκαν είναι η τυπική μέθοδος οπισθοδρομικής διάδοσης σφάλματος (Standard Back Propagation) [181], η μέθοδος οπισθοδρομικής διάδοσης σφάλματος με μεταβλητό βήμα (Back Propagation with Variable Stepsize) [117], η μέθοδος Resilient Back Propagation [176], η μέθοδος οπισθοδρομικής διάδοσης σφάλματος με προσαρμοζόμενο βήμα για εκπαίδευση ανά πρότυπο εισόδου (Adaptive On-line Back Propagation) [116] και η μέθοδος Scaled Conjugate Gradient [143]. Όλες οι μέθοδοι δοκιμάστηκαν αναλυτικά για πολλές διαφορετικές τιμές των παραμέτρων τους. Στις περισσότερες πειραματικές θεωρήσεις, οι αλγόριθμοι δεν παρουσίασαν σημαντικές αποκλίσεις στην απόδοσή τους με εξαίρεση την τυπική μέθοδος οπισθοδρομικής διάδοσης σφάλματος η οποία παρουσίασε δυσκολίες στην εκπαίδευση τις περισσότερες φορές.

Αρχιτεκτονική δικτύου: Καθώς ο ορισμός μιας «βέλτιστης» αρχιτεκτονικής δικτύου για οποιοδήποτε συγκεκριμένο πρόβλημα είναι αρκετά δύσκολος και παραμένει ένα ανοικτό πρόβλημα των ΤΝΔ, στην παρούσα μελέτη δοκιμάσαμε μια ποικιλία τοπολογιών με διαφορετικό πλήθος κρυφών στρωμάτων και διαφορετικό αριθμό νευρώνων σε κάθε στρώμα. Τα αποτελέσματα που παρουσιάζονται αφορούν στην βέλτιστη απόδοση των ΤΝΔ μεταξύ όλων των διαφορετικών θεωρήσεων και δοκιμών που πραγματοποιήθηκαν για κάθε πρόβλημα. Η αρχιτεκτονική που χρησιμοποιήθηκε σε κάθε περίπτωση που παρουσιάζεται περιγράφεται με μια σειρά ακέραιων αριθμών που συμβολίζουν το πλήθος των νευρώνων σε κάθε στρώμα του ΤΝΔ.

Κανονικοποίηση δεδομένων: Για την ευκολότερη προσαρμογή του δικτύου, τα δεδομένα μετασχηματίστηκαν μέσω μιας διαδικασίας κανονικοποίησης πριν την εκπαίδευση του δικτύου. Για την περίπτωση όπου τα δεδομένα που παρουσιάζονται στο δίκτυο ανήκουν στον χώρο $\mathbb{Z}_p$, με p πρώτο αριθμό, το διάστημα $S = [-1, 1]$, διαιρείται σε p υποδιαστήματα. Κατ΄ αυτό τον τρόπο, οι αριθμοί από το σύνολο δεδομένων μετασχηματίζονται στους αντίστοιχους του διαστήματος S. Συγχρόνως, η τιμή εξόδου του δικτύου μετασχηματίζεται σε έναν αριθμό του $\mathbb{Z}_p$ χρησιμοποιώντας της αντίστροφη διαδικασία.

Αξιολόγηση του δικτύου: Για την αξιολόγηση της απόδοσης του δικτύου, αρχικά μετρήθηκε το ποσοστό των δεδομένων εκπαίδευσης για τα οποία το δίκτυο πέτυχε να δώσει ως αποτέλεσμα την ακριβή τιμή του στόχου. Το μέτρο αυτό συμβολίζεται ως μ_0. Ωστόσο, καθώς η τιμή εξόδου του δικτύου περιορίζεται στο διάστημα $[-1, 1]$, πολύ μικρές διακυμάνσεις της τιμής εξόδου οδηγούν το δίκτυο σε υπολογισμό όχι της ακριβούς τιμής στόχου αλλά μιας τιμής πολύ κοντά σε αυτήν. Το γεγονός αυτό καθιστά το μέτρο μ_0 ανεπαρκές για την αξιολόγηση της απόδοσης του δικτύου. Για το λόγο αυτό χρησιμοποιήσαμε το μέτρο $\mu_{\pm v}$. Το μέτρο αυτό καταγράφει το ποσοστό των δεδομένων για τα οποία η διαφορά ανάμεσα στην επιθυμητή και την πραγματική έξοδο δεν ξεπερνά κατά $\pm v$ την τιμή του ακριβούς στόχου. Πρέπει να παρατηρήσουμε ότι το μέτρο $\mu_{\pm v}$ έχει διαφορετική σημασία για το ΠΔΛ και το ΠΑΚDH. Συγκεκριμένα, το μέτρο $\mu_{\pm v}$ είναι πολύ σημαντικό στην περίπτωση του ΠΔΛ. Αν το μέγεθος του διαστήματος $(\pm v)$ είναι $\mathcal{O}(\log(p))$ τότε το μέτρο $\mu_{\pm v}$ μπορεί να αντικαταστήσει το ακριβές μέτρο μ_0. Γενικά, για κάποιες μικρές τιμές του v το μέτρο $\mu_{\pm v}$ είναι

αποδεκτό καθώς ο υπολογισμός του διακριτού λογαρίθμου μπορεί να επιβεβαιωθεί μέσω του εκθετικού υπολογισμού στα πεπερασμένα σώματα [166]. Ωστόσο, η επαλήθευση της λύσης για το πρόβλημα της Απεικόνισης Diffie-Hellman είναι ανοικτό. Σύνολα πιθανών τιμών της Απεικόνισης Diffie-Hellman μπορούν να χρησιμοποιηθούν για τον υπολογισμό πιθανών τιμών για το ΠΑΚΔΗ. Οι τιμές για το ΠΑΚΔΗ μπορούν να δοκιμαστούν στην πράξη, καθώς είναι συμμετρικά κλειδιά επικοινωνίας μεταξύ δύο χρηστών. Τα ποσοστά επιτυχίας με το μέτρο $\mu_{\pm v}$ για το ΠΑΔΗ μπορούν να συγκριθούν με τα αντίστοιχα για το ΠΔΛ. Τα αποτελέσματα της σύγκρισης μπορούν να συσχετιστούν με την εικασία της υπολογιστικής ισοδυναμίας των δύο προβλημάτων.

Στην εργασία [129], μελετήθηκαν τα δύο προβλήματα ΠΔΛ και ΠΑΔΗ για πολλούς διαφορετικούς μικρούς αριθμούς p. Τα πρότυπα εισόδου ήταν διαφορετικές τιμές της μεταβλητής της συνάρτησης του διακριτού λογαρίθμου και της απεικόνισης Diffie-Hellman αντίστοιχα, και ως τιμές στόχου λήφθηκαν οι τιμές των αντίστοιχων συναρτήσεων, για σταθερές επιλεγμένες τιμές γεννητόρων g και πρώτων αριθμών p. Τα ΤΝΔ στην περίπτωση αυτή έδωσαν αποτελέσματα εκπαίδευσης και γενίκευσης που έφταναν σε ποσοστό επιτυχίας 100%. Στη συνέχεια, η απόδοση των ΤΝΔ μελετήθηκε για μεγαλύτερους πρώτους αριθμούς οι οποίοι έκαναν την διαδικασία εκπαίδευσης των ΤΝΔ δυσκολότερη. Η ύπαρξη μεγάλου πλήθους αριθμών που κανονικοποιούνταν στο διάστημα $[-1, 1]$ δημιούργησε προβλήματα στην προσαρμογή των ΤΝΔ. Αυτό είχε ως αποτέλεσμα μικρές διαφορές στην έξοδο του δικτύου να οδηγούν σε πλήρη αποτυχία απαιτώντας την χρήση μεγαλύτερης αρχιτεκτονικής. Σε περιπτώσεις πολύ μεγάλων πρώτων αριθμών η απόδοση των ΤΝΔ στην εκπαίδευση ήταν πολύ χαμηλή. Μερικά ενδεικτικά αποτελέσματα της εκπαίδευσης δίνονται στον Πίνακα 4.1.

Πίνακας 4.1: Αποτελέσματα της εκπαίδευσης Τεχνητών Νευρωνικών Δικτύων για το Πρόβλημα Διακριτού Λογαρίθμου και το Πρόβλημα Απεικόνισης Diffie-Hellman

p	Τοπολογία	Εποχές	μ_0	$\mu_{\pm 2}$	$\mu_{\pm 5}$	$\mu_{\pm 10}$	Πρόβλημα
83	$1-5-5-1$	20000	20%	30%	48%	70%	ΠΔΛ
	$1-5-5-1$	20000	20%	35%	51%	70%	ΠΑΔΗ
97	$1-5-5-1$	25000	20%	30%	48%	70%	ΠΔΛ
	$1-5-5-1$	20000	20%	35%	51%	70%	ΠΑΔΗ

Στην παρούσα μελέτη το ΠΔΛ μελετήθηκε υπό διαφορετική θεώρηση. Συγκεκριμένα, μελετήσαμε την περίπτωση όπου για διάφορες τιμές πρώτου αριθμού p και γεννήτορα g, η τιμή $h = g^u \pmod p$ παραμένει σταθερή. Τα πρότυπα εισόδου αποτελούνταν από ζεύγη πρώτων αριθμών p και των αντίστοιχων γεννητόρων g και τα πρότυπα στόχου ήταν οι αντίστοιχες τιμές u, έτσι ώστε $\log_g h \equiv u \pmod p$, για μια σταθερή τιμή h. Υπό την θεώρηση αυτή μελετήθηκε το ΠΔΛ για πρώτους αριθμούς με τιμές από 101 μέχρι 2003, με διαφορετικές τοπολογίες δικτύου και μεθόδους εκπαίδευσης. Στην περίπτωση αυτή, υπήρξε μια διαφοροποίηση μεταξύ των αποτελεσμάτων που λήφθηκαν από διαφορετικές μεθόδους. Για μικρές τιμές του p, δηλαδή για p από 101 μέχρι 199, τα καλύτερα αποτελέσματα για την προσέγγιση της τιμής του u δόθηκαν από την μέθοδο οπισθοδρομικής διάδοσης σφάλματος για εκπαίδευση ανά πρότυπο εισόδου με προσαρμοζόμενο βήμα. Για μεγαλύτερες τιμές του p, τα καλύτερα αποτελέσματα λήφθηκαν από την μέθοδο Scaled Conjugate Gradient. Αποτελέσματα για την νέα θεώρηση του ΠΔΛ δίνονται στον Πίνακα 4.2. Όλα τα αποτελέσματα αναφέρονται στην εκπαίδευση των ΤΝΔ για την προσέγγιση της τιμής του διακριτού λογαρίθμου u. Συγκρίνοντας τα αποτελέσματα της απόδοσης των ΤΝΔ για το ΠΔΛ υπό τις δύο διαφορετικές θεωρήσεις συμπεραίνουμε ότι για το ΠΔΛ η προσεγγιστική ικανότητα των ΤΝΔ είναι καλύτερη με την

δεύτερη θεώρηση του προβλήματος.

Πίνακας 4.2: Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για το Πρόβλημα Διακριτού Λογαρίθμου με την δεύτερη θεώρηση του προβλήματος

Εύρος p	Τοπολογία	Εποχές	μ_0	$\mu_{\pm 15}$	$\mu_{\pm 20}$	$\mu_{\pm 30}$	$\mu_{\pm 40}$
$101-199$	$2-15-1$	600000	100%	100%	100%	100%	100%
$503-1009$	$2-25-1$	600000	82%	93%	96%	96%	98%
$1009-2003$	$2-30-1$	600000	17%	40%	46.7%	51.8%	54.1%
$1009-2003$	$2-3-3-3-1$	20000	7.5%	34.3%	44.8%	64.2%	71.6%

Στην εργασία [129] εκτός από το ΠΔΛ και το ΠΑDH μελετήθηκε επίσης η απόδοση των ΤΝΔ στην προσέγγιση της $\phi(N)$ απεικόνισης, $N \mapsto \phi(N)$, με πρότυπα εισόδου αριθμούς $N = p \times q$, όπου p και q πρώτοι αριθμοί, και πρότυπα στόχους τις αντίστοιχες τιμές της απεικόνισης $\phi(N) = (p-1)\times(q-1)$. Στην περίπτωση αυτή το πρόβλημα της κανονικοποίησης των δεδομένων δεν αποτέλεσε εμπόδιο. Τα αποτελέσματα της μελέτης για το πρόβλημα αυτό παρουσίασαν πολύ ενδιαφέρον, καθώς τα ΤΝΔ ήταν σε θέση όχι μόνο να προσαρμοστούν στα δεδομένα εκπαίδευσης αλλά επιπλέον παρουσίασαν πολύ καλή απόδοση αναφορικά με το σύνολο ελέγχου [129]. Ενδεικτικά αποτελέσματα της εκπαίδευσης των ΤΝΔ για την προσέγγιση της απεικόνισης $\phi(N)$ παρουσιάζονται στον Πίνακα 4.3.

Πίνακας 4.3: Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για την απεικόνιση $\phi(N)$ όπου $N = p \times q \leqslant 10^4$

Τοπολογία	Εποχές	μ_0	$\mu_{\pm 2}$	$\mu_{\pm 5}$	$\mu_{\pm 10}$	$\mu_{\pm 20}$
$1-5-5-1$	80000	3%	15%	35%	65%	90%
$1-7-8-1$	50000	6%	20%	50%	70%	100%

Στην παρούσα μελέτη το πρόβλημα της παραγοντοποίησης επίσης ερευνήθηκε χρησιμοποιώντας διαφορετική θεώρηση. Συγκεκριμένα, η προσέγγιση της τιμής της συνάρτησης $p^2 + q^2$, δοθείσης της τιμής του N, οδηγεί άμεσα στην παραγοντοποίηση του N στους παράγοντες p και q. Για το λόγο αυτό, μελετήσαμε τα ΤΝΔ αναφορικά με την προσέγγιση της παραπάνω συνάρτησης για διάφορες τιμές του N. Τα καλύτερα αποτελέσματα του προβλήματος της παραγοντοποίησης υπό την νέα θεώρηση δίνονται στον Πίνακα 4.4.

Πίνακας 4.4: Αποτελέσματα της εκπαίδευσης των Τεχνητών Νευρωνικών Δικτύων για το πρόβλημα της παραγοντοποίησης με την δεύτερη θεώρηση και για N από 143 μέχρι 1003

Τοπολογία	Εποχές	μ_0	$\mu_{\pm 15}$	$\mu_{\pm 20}$	$\mu_{\pm 30}$	$\mu_{\pm 40}$
$1-15-1$	200000	35.1%	36.8%	42.1%	43.8%	45.6%
$1-20-1$	600000	35.1%	43.8%	45.6%	52.6%	56.2%

Από την σύγκριση των αποτελεσμάτων της εκπαίδευσης των ΤΝΔ για το πρόβλημα της

παραγοντοποίησης υπό τις δύο διαφορετικές θεωρήσεις προκύπτει ότι ενώ με τη δεύτερη θεώρηση τα ΤΝΔ δείχνουν να πετυχαίνουν μεγαλύτερα ποσοστά επιτυχίας για το μέτρο μ_0 ωστόσο χρειάζονται μεγαλύτερο αριθμό εποχών για να δώσουν τα αποτελέσματα αυτά ενώ αντίστοιχα η απόδοση κατά το μέτρο $\mu_{\pm v}$ δεν αυξάνεται ανάλογα. Επιπλέον, τα καλύτερα αποτελέσματα που προέκυψαν υπό την πρώτη θεώρηση αναφέρονται σε μεγαλύτερες τιμές του N, σε σχέση με αυτά της δεύτερης θεώρησης. Συμπερασματικά, παρότι οι δύο διαφορετικές θεωρήσεις του προβλήματος παραγοντοποίησης είναι υπολογιστικά ισοδύναμες, η απόδοση των ΤΝΔ για την προσέγγιση του προβλήματος είναι καλύτερη υπό την πρώτη θεώρηση.

Συνολικά, τα αποτελέσματα της μελέτης για την απόδοση των ΤΝΔ στο ΠΔΛ και στο πρόβλημα της παραγοντοποίησης που σχετίζεται με το κρυπτοσύστημα RSA, υποδεικνύουν ότι το πρόβλημα του διακριτού λογαρίθμου δεν είναι ευκολότερο στην επίλυσή του από το πρόβλημα της παραγοντοποίησης. Το γεγονός αυτό έρχεται σε συμφωνία με τα θεωρητικά αποτελέσματα, καθώς αν δοθεί μια μέθοδος υπολογισμού δεικτών στα πεπερασμένα σώματα τότε το κρυπτοσύστημα RSA καταρρέει.

4.3 Τεχνητά Νευρωνικά Δίκτυα για κρυπτανάλυση κρυπτοσυστημάτων ελλειπτικών καμπυλών

Στην ενότητα αυτή μελετάμε την απόδοση των ΤΝΔ στο πρόβλημα υπολογισμού του λιγότερο σημαντικού δυαδικού ψηφίου του διακριτού λογαρίθμου ενός σημείου ελλειπτικών καμπυλών. Ο υπολογισμός του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες με γνωστή περιττή τάξη είναι σημαντικός για τις κρυπτογραφικές εφαρμογές, καθώς οδηγεί στον υπολογισμό όλων των δυαδικών ψηφίων του διακριτού λογαρίθμου. Τα αποτελέσματα της μελέτης αυτής δείχνουν ότι τα ΤΝΔ είναι δυνατόν να προσαρμοστούν στα δεδομένα που λαμβάνουν με μεγάλη επιτυχία, ενώ η απόκρισή τους σε άγνωστα δεδομένα είναι λίγο καλύτερη από την τυχαία επιλογή. Ένα άλλο σημαντικό εύρημα είναι ότι τα ΤΝΔ απαιτούν λιγότερο χώρο αποθήκευσης για τα γνωστά πρότυπα σε σχέση με τον χώρο που απαιτείται για την αποθήκευση του ίδιου του συνόλου δεδομένων.

4.3.1 Θεώρηση προβλήματος

Για το πρόβλημα του διακριτού λογαρίθμου επί των ελλειπτικών καμπυλών, η ακόλουθη πρόταση προκύπτει από την ασφάλεια των δυαδικών ψηφίων των διακριτών λογαρίθμων επί των κυκλικών ομάδων [164,201].

Πρόταση 4.1 *Δοθείσης μιας ελλειπτικής καμπύλης, E, σε ένα πεπερασμένο σώμα, $\mathbb{F}_q$, με γνωστή τάξη n, και μιας oracle για ένα δυαδικό ψηφίο του διακριτού λογαρίθμου που δεν αντιστοιχεί σε καμία δύναμη του 2 που διαιρεί την τάξη n, τότε όλα τα δυαδικά ψηφία του διακριτού λογαρίθμου μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο.*

Παρατήρηση 4.1 *Μέχρι τώρα δεν υπάρχει αλγόριθμος που να βρίσκει την τάξη μιας ελλειπτικής καμπύλης σε πολυωνυμικό χρόνο. Επιπλέον, η πολυπλοκότητα για τον υπολογισμό του διακριτού λογαρίθμου επί ελλειπτικών καμπυλών χωρίς γνώση της τάξης τους, είναι εκθετική και συνεπώς το πρόβλημα του διακριτού λογαρίθμου σε αυτή την περίπτωση παραμένει ένα υπολογιστικά δύσκολο πρόβλημα.*

Από την Πρόταση 4.1 προκύπτει ότι στην περίπτωση μιας ελλειπτικής καμπύλης με περιττή τάξη n, μια oracle που δίνει το λιγότερο σημαντικό δυαδικό ψηφίο του διακριτού λογαρίθμου ενός σημείου της ελλειπτικής καμπύλης, οδηγεί στον υπολογισμό όλων των ψηφίων του διακριτού λογαρίθμου σε πολυωνυμικό χρόνο. Επιπλέον, οι ελλειπτικές καμπύλες με τάξη πρώτο αριθμό θεωρούνται πιο ασφαλείς για κρυπτογραφικές εφαρμογές. Για τους παραπάνω λόγους, μελετάμε τον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου

ενός σημείου ελλειπτικής καμπύλης με περιττή τάξη. Στις εργασίες [38, 194] παρουσιάζονται εκτιμήσεις για την πολυπλοκότητα υπολογισμού των ψηφίων του διακριτού λογαρίθμου σε διαφορετικά σώματα.

Αναφορικά με το υπό μελέτη πρόβλημα, ορίζουμε την ακόλουθη συνάρτηση Boole. Έστω μια ελλειπτική καμπύλη $E(\mathbb{F}_q)$ και $P = (x_P, y_P), Q = (x_Q, y_Q)$ δύο σημεία της καμπύλης $E(\mathbb{F}_q)$, τέτοια ώστε $Q = tP$, με $0 \leqslant t \leqslant (n-1)$. Ορίζουμε την συνάρτηση Boole $f : \{0,1\}^{4\lceil \log p \rceil} \mapsto \{0,1\}$, με

$$f(x_P, y_P, x_Q, y_Q) = \lambda\sigma\psi(t), \tag{4.1}$$

που έχει ως είσοδο τις συντεταγμένες x_P, y_P, x_Q, y_Q, σε δυαδική αναπαράσταση, και δίνει ως έξοδο το λιγότερο σημαντικό ψηφίο (λσψ) του t, δηλαδή 1 αν το λιγότερο σημαντικό ψηφίο του t είναι 1, και 0 αν το λιγότερο σημαντικό ψηφίο του t είναι 0. Γενικά, ένα κύκλωμα Boole που υπολογίζει την παραπάνω συνάρτηση μπορεί να είναι εκθετικά μεγάλο ως προς το $\lceil \log p \rceil$ [38]. Για τον υπολογισμό αυτής της συνάρτησης Boole χρησιμοποιούμε τα ΤΝΔ. Στη συγκεκριμένη μελέτη, χρησιμοποιούμε τα ΤΝΔ πρόσθιας τροφοδότησης για την προσέγγιση της συνάρτησης που ορίζεται στην (4.1). Για το γενικό πρόβλημα υπολογισμού μιας συνάρτησης Boole με τη χρήση ΤΝΔ πρόσθιας τροφοδότησης, στην εργασία [9] έχει αποδειχθεί το ακόλουθο θεώρημα που στηρίζει την αποτελεσματικότητα της προτεινόμενης προσέγγισης.

Θεώρημα 4.1 *Για κάθε μια συνάρτηση Boole υπάρχει ένα τεχνητό νευρωνικό δίκτυο με ένα κρυφό στρώμα και συνάρτηση ενεργοποίησης κατώφλι ικανό να την υπολογίσει.*

4.3.2 Πειραματική θεώρηση και αποτελέσματα

Η εκπαίδευση ΤΝΔ με νευρώνες που χρησιμοποιούν ως συνάρτηση ενεργοποίησης κατώφλι απαιτεί την χρήση μεθόδων εκπαίδευσης που δεν χρησιμοποιούν πληροφορία των παραγώγων της συνάρτησης σφάλματος. Επιπλέον, όπως έχει αποδειχθεί στην εργασία [41], τα αναλογικά ΤΝΔ μπορούν να είναι πιο ισχυρά από τα ΤΝΔ που χρησιμοποιούν κατώφλια, ακόμα και για τον υπολογισμό συναρτήσεων Boole. Για τους παραπάνω λόγους, μελετάμε την απόδοση των ΤΝΔ χρησιμοποιώντας ως συνάρτηση ενεργοποίησης την συνάρτηση της υπερβολικής εφαπτομένης

$$f(x) = \tanh(\lambda_2 x),$$

η οποία προσεγγίζει μια συνάρτηση κατώφλι καθώς η παράμετρος λ_2 τείνει στο άπειρο. Σε όλα τα πειράματα, το στρώμα εξόδου αποτελείται από δύο νευρώνες και ο νευρώνας με την υψηλότερη τιμή εξόδου καθορίζει την κλάση στην οποία ανήκει το υπολογιζόμενο δυαδικό ψηφίο. Κατ' αυτό τον τρόπο, αν η τιμή εξόδου του πρώτου νευρώνα είναι μικρότερη από την τιμή εξόδου του δεύτερου νευρώνα, τότε το ψηφίο θεωρείται ότι ανήκει στην Κλάση 0, που αντιστοιχεί σε μηδενική τιμή του ψηφίου και αντίστροφα. Αυτή η θεώρηση μας επιτρέπει να χρησιμοποιήσουμε μεθόδους εκπαίδευσης που μεταχειρίζονται παραγώγους της συνάρτησης σφάλματος του δικτύου. Συγκεκριμένα, μελετήσαμε την απόδοση τριών αλγορίθμων εκπαίδευσης, έναν από κάθε διαφορετική κατηγορία αλγορίθμων, την μέθοδο Resilient Back Propagation [176], την μέθοδο οπισθοδρομικής διάδοσης σφάλματος με προσαρμοζόμενο βήμα για εκπαίδευση ανά πρότυπο εισόδου (Adaptive On-line Back Propagation) [116] και την μέθοδο του Διαφοροεξελικτικού Αλγορίθμου [202]. Αναφορικά με την τοπολογία των ΤΝΔ, δοκιμάστηκε ποικιλία τοπολογιών με διαφορετικό πλήθος στρωμάτων και νευρώνων σε κάθε στρώμα. Στους πίνακες δίνονται οι τοπολογίες με τις οποίες επιτεύχθηκαν τα καλύτερα αποτελέσματα για κάθε πρόβλημα.

Για την κατασκευή των συνόλων δεδομένων χρησιμοποιήθηκε η βιβλιοθήκη ECC_LIB για κρυπτογραφία ελλειπτικών καμπυλών [91]. Η απόδοση των ΤΝΔ μελετήθηκε για τρία διαφορετικά σύνολα δεδομένων της υπό θεώρηση συνάρτησης Boole που αντιστοιχούν σε τυχαία επιλεγμένα p με μήκος ψηφίων 14, 20 και 32, αντίστοιχα, όπου $\mathbb{F}_p$ είναι το πεπερασμένο σώμα επί του οποίου κατασκευάζεται η ελλειπτική καμπύλη.

Σε κάθε πείραμα το σύνολο δεδομένων διαχωρίστηκε τυχαία σε σύνολο εκπαίδευσης και σύνολο ελέγχου. Τα δύο τρίτα του συνόλου δεδομένων τέθηκαν στο σύνολο εκπαίδευσης και το υπόλοιπο ένα τρίτο αποτέλεσε το σύνολο ελέγχου. Για την αξιολόγηση της απόδοσης του ΤΝΔ, αρχικά μετρήσαμε το ποσοστό του συνόλου εκπαίδευσης για το οποίο το ΤΝΔ πρόβλεψε σωστά το λιγότερο σημαντικό ψηφίο του διακριτού λογαρίθμου κατά μέσο όρο από 10 πειράματα. Στη συνέχεια η απόδοση του δικτύου αξιολογήθηκε μετρώντας το μέσο όρο του ποσοστού επιτυχίας για το σύνολο ελέγχου για όλα τα πειράματα.

Τα καλύτερα αποτελέσματα για την παραπάνω θεώρηση και για την τιμή της παραμέτρου $\lambda_2 = 1$, λήφθηκαν χρησιμοποιώντας την μέθοδο οπισθοδρομικής διάδοσης σφάλματος με προσαρμοζόμενο βήμα για εκπαίδευση ανά πρότυπο εισόδου και δίνονται στους Πίνακες 4.5, 4.6 και 4.7, αντίστοιχα. Τα αποτελέσματα δείχνουν ότι για τα τρία διαφορετικά μήκη δυαδικών ψηφίων, τα ΤΝΔ μπόρεσαν να προσαρμοστούν στα δεδομένα εκπαίδευσης με μέση επιτυχία 90%. Αναφορικά με τα σύνολα ελέγχου, τα ΤΝΔ πέτυχαν και για τα τρία διαφορετικά μήκη ψηφίων μέση επιτυχία 57%, δηλαδή λίγο υψηλότερη από την τυχαία επιλογή. Σχετικά με τις απαιτούμενες εποχές για την εκπαίδευση των ΤΝΔ, καθώς το μήκος ψηφίων του p αυξανόταν χρειάζονταν περισσότερες εποχές για να επιτευχθεί η ίδια επιτυχία.

Πίνακας 4.5: Αποτελέσματα για p με μήκος 14ων δυαδικών ψηφίων και τοπολογία $56-3-2$

Εποχές		Εκπαίδευση			Έλεγχος		
		Κλάση 0	Κλάση 1	Επιτυχία	Κλάση 0	Κλάση 1	Επιτυχία
500	Κλάση 0	168	33	83.58%	30	24	55.56%
	Κλάση 1	48	151	75.88%	23	23	50.00%
650	Κλάση 0	184	17	91.54%	33	21	61.11%
	Κλάση 1	32	167	83.92%	23	23	50.00%
700	Κλάση 0	183	18	91.04%	33	21	61.11%
	Κλάση 1	30	169	84.92%	21	25	54.35%
1000	Κλάση 0	186	15	92.54%	33	21	61.11%
	Κλάση 1	25	174	87.44%	18	28	60.87%

Μια άλλη ενδιαφέρουσα παρατήρηση που προέκυψε αναφορικά με το σύνολο εκπαίδευσης είναι ότι το δίκτυο μπορεί να μάθει τα πρότυπα εκπαίδευσης και να απαντά σωστά ως προς το λιγότερο σημαντικό ψηφίο του διακριτού λογαρίθμου χρησιμοποιώντας λιγότερη μνήμη από αυτήν που απαιτείται για την αποθήκευση του αντίστοιχου συνόλου δεδομένων. Τα αποτελέσματα για τη συμπίεση των δεδομένων δίνονται στον Πίνακα 4.8. Στον Πίνακα 4.8, το «ΠΔΨ(p) » συμβολίζει το πλήθος δυαδικών ψηφίων του p, με «ΠΔΨ Δεδομένων» συμβολίζεται το πλήθος δυαδικών ψηφίων που απαιτείται για την αποθήκευση του συνόλου δεδομένων της εκπαίδευσης, το «ΠΔΨ Δικτύου» συμβολίζει το πλήθος των δυαδικών ψηφίων που απαιτούνται για την αποθήκευση των βαρών του δικτύου και «Επιτυχία» είναι το ποσοστό επιτυχίας του δικτύου στην αναγνώριση της σωστής κλάσης για τα δεδομένα εκπαίδευσης.

4.4 Θεωρητική μελέτη της εφαρμογής Πολυωνυμικών Δικτύων Ridge στην κρυπτογραφία

Στην ενότητα αυτή παρουσιάζονται μερικά θεωρητικά αποτελέσματα για την εφαρμογή ΤΝΔ ειδικής μορφής σε προβλήματα κρυπτογραφίας. Πιο συγκεκριμένα, μελετάμε θεωρητικά

Πίνακας 4.6: Αποτελέσματα για p με μήκος 20 δυαδικών ψηφίων και τοπολογία $80-3-2$

Εποχές		Εκπαίδευση			Έλεγχος		
		Κλάση 0	Κλάση 1	Επιτυχία	Κλάση 0	Κλάση 1	Επιτυχία
2000	Κλάση 0	186	14	93.0%	32	26	55.17%
	Κλάση 1	23	177	88.5%	17	25	59.52%
3000	Κλάση 0	191	9	95.5%	30	28	51.72%
	Κλάση 1	19	181	90.5%	21	21	50.00%
4000	Κλάση 0	194	6	98.0%	32	26	55.17%
	Κλάση 1	18	182	91.0%	19	23	54.76%
6000	Κλάση 0	196	4	98.0%	33	25	56.90%
	Κλάση 1	17	183	91.5%	20	22	52.38%

Πίνακας 4.7: Αποτελέσματα για p με μήκος 32 δυαδικών ψηφίων και τοπολογία $128-3-2$

Εποχές		Εκπαίδευση			Έλεγχος		
		Κλάση 0	Κλάση 1	Επιτυχία	Κλάση 0	Κλάση 1	Επιτυχία
4000	Κλάση 0	193	5	97.47%	36	21	63.16%
	Κλάση 1	16	186	92.08%	20	23	53.49%
5000	Κλάση 0	193	5	97.47%	36	21	63.16%
	Κλάση 1	15	187	92.57%	19	24	55.81%
8000	Κλάση 0	193	5	97.47%	35	22	61.40%
	Κλάση 1	14	188	93.07%	18	25	58.14%
9000	Κλάση 0	193	5	97.47%	35	22	61.40%
	Κλάση 1	14	188	93.07%	16	27	62.79%

την δυνατότητα εφαρμογής των Πολυωνυμικών Δικτύων Ridge (Ridge Polynomial Networks) για τον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου. Ο υπολογισμός του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου είναι σημαντικός για τις κρυπτογραφικές εφαρμογές καθώς σχετίζεται μεταξύ άλλων και με τον υπολογισμό όλων των ψηφίων του διακριτού λογαρίθμου [67].

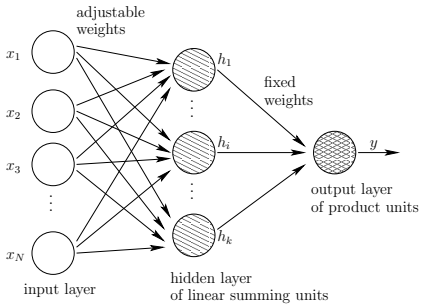
Τα Πολυωνυμικά Δίκτυα Ridge (ΡΠΔ) ανήκουν στην κλάση των ΤΝΔ που βασίζονται σε νευρώνες πολλαπλασιαστικού τύπου, δηλαδή οι νευρώνες εφαρμόζουν την συνάρτηση ενεργοποίησής τους στο γινόμενο των βαρών επί των εισόδων τους. Τα δομικά στοιχεία των ΡΠΔ είναι τα Δίκτυα Πί-Σίγμα (Pi-Sigma Networks). Ένα Δίκτυο Πί-Σίγμα (ΠΣΔ) είναι ένα τεχνητό νευρωνικό δίκτυο πρόσθιας τροφοδότησης με ένα κρυφό στρώμα γραμμικών νευρώνων που χρησιμοποιεί πολλαπλασιαστικούς νευρώνες στο στρώμα εξόδου, δηλαδή χρησιμοποιεί *γινόμενα αθροισμάτων* των συνιστωσών της εισόδου του. Η παρουσία ενός μόνο στρώματος προσαρμοζόμενων βαρών στα ΠΣΔ έχει ως αποτέλεσμα την γρήγορη εκπαίδευσή τους. Υπάρχουν δύο ειδών Δίκτυα Πί-Σίγμα, τα Αναλογικά Δίκτυα Πί-Σίγμα (Analog Pi-Sigma Networks) και τα Δυαδικά Δίκτυα Πί-Σίγμα (Binary Pi-Sigma Networks). Μια γενίκευση των Αναλογικών Δικτύων Πί-Σίγμα είναι τα Πολυωνυμικά Δίκτυα Ridge για τα οποία έχει αποδειχθεί ότι έχουν ικανότητες καθολικού προσεγγιστή [65]. Αντίστοιχα, τα Δυαδικά Δίκτυα

Πίνακας 4.8: Αποτελέσματα συμπίεσης δεδομένων

ΠΔΨ(p)	ΠΔΨ Δεδομένων	ΠΔΨ Δικτύου	Επιτυχία
14	23200	8400	89.99%
20	32800	11856	94.75%
32	52000	18768	95.27%

Πί-Σίγμα μπορούν να υλοποιούν οποιαδήποτε συνάρτηση Boole [193].

Στο Σχήμα 4.1 παρουσιάζεται ένα Δίκτυο Πί-Σίγμα με μια έξοδο. Το δίκτυο αυτό είναι ένα πλήρως συνδεδεμένο δίκτυο πρόσθιας τροφοδότησης με δύο στρώματα. Ωστόσο, το στρώμα με τους αθροιστικούς νευρώνες δεν είναι κρυφό όπως στην περίπτωση των πολυστρωματικών Perceptrons, καθώς τα βάρη από αυτό το δίκτυο προς το στρώμα εξόδου έχουν σταθερή τιμή 1. Αυτή η ιδιότητα συνεισφέρει στην μείωση του απαιτούμενου χρόνου για εκπαίδευση.



Σχήμα 4.1: Ένα Δίκτυο Πί-Σίγμα (ΠΣΔ) με έναν νευρώνα εξόδου

Έστω $\mathbf{x} = (1, x_1, \ldots, x_N)^\top$ ένα διάνυσμα στήλη $N+1$ διάστασης, είσοδος του δικτύου επαυξημένη κατά 1, όπου το x_k συμβολίζει την k-οστή συνιστώσα του $\mathbf{x}$. Κάθε είσοδος πολλαπλασιάζεται με K διανύσματα βαρών διάστασης $N+1$, $\mathbf{w}_j = (w_{0j}, w_{1j}, \ldots, w_{Nj})^\top$, $j = 1, 2, \ldots, K$ και τα αποτελέσματα αθροίζονται από ένα στρώμα K αθροιστικών γραμμικών νευρώνων, όπου K είναι η επιθυμητή τάξη του δικτύου. Η έξοδος, h_j, του j-οστού αθροιστικού νευρώνα, δίνεται ως εξής:

$$h_j = \mathbf{w}_j^\top \mathbf{x} = \sum_{k=1}^{N} w_{kj} x_k + w_{0j}, \quad j = 1, 2, \ldots, K, \tag{4.2}$$

όπου w_{kj} είναι ένα προσαρμοζόμενο βάρος από την συνιστώσα x_k της εισόδου προς τον j-οστό αθροιστικό νευρώνα και w_{0j} είναι το κατώφλι του j-οστό αθροιστικό νευρώνα. Τα βάρη μπορούν να λάβουν αυθαίρετες πραγματικές τιμές.

Η έξοδος y του Δικτύου Πί-Σίγμα δίνεται ως:

$$y = \sigma\left(\prod_{j=1}^{K} h_j\right) = \sigma(net), \tag{4.3}$$

όπου $\sigma(\cdot)$ είναι μια κατάλληλη συνάρτηση ενεργοποίησης και $net = \prod_{j=1}^{K} h_j$.

Το δίκτυο που απεικονίζεται στο Σχήμα 4.1 ονομάζεται K τάξης Δίκτυο Πί-Σίγμα καθώς περιλαμβάνει K αθροιστικούς νευρώνες. Ο συνολικός αριθμός συνδέσεων με προσαρμοζόμενα βάρη, συμπεριλαμβανομένων των προσαρμοζόμενων κατωφλιών, για ένα K τάξης Δίκτυο Πί-Σίγμα με N διάστασης διανύσματα εισόδου είναι $(N+1)K$. Αν απαιτούνται έξοδοι πολλών συνιστωσών, για κάθε μια συνιστώσα της εξόδου χρειάζεται ένα ανεξάρτητο στρώμα αθροιστικών νευρώνων. Έτσι, για ένα διάνυσμα εξόδου $\mathbf{y}$, M διάστασης υπάρχουν συνολικά στο

δίκτυο $\sum_{i=1}^{M}(N+1)K_i$ συνδέσεις προσαρμοζόμενων βαρών, όπου K_i είναι ο αριθμός των αθροιστικών νευρώνων για την i-οστή συνιστώσα εξόδου. Το γεγονός αυτό καθιστά το δίκτυο επεκτάσιμο, καθώς η τάξη του μπορεί να αυξηθεί προσθέτοντας και άλλους αθροιστικούς νευρώνες με τα σχετιζόμενα βάρη τους χωρίς να καταστραφεί κάποια σύνδεση που υπήρχε πριν στο δίκτυο. Τα ΠΣΔ μπορούν να χειριστούν και αναλογικές και δυαδικές εισόδους και εξόδους χρησιμοποιώντας μια κατάλληλη μη-γραμμική συνάρτηση ενεργοποίησης $\sigma(\cdot)$.

Αναφορικά με τις προσεγγιστικές ικανότητες των ΠΣΔ, παρότι η συνάρτηση ενεργοποίησης εφαρμόζεται σε ένα K τάξης πολυώνυμο όταν χρησιμοποιούνται K αθροιστικοί νευρώνες, αυτό δεν σημαίνει ότι μπορούν να χρησιμοποιηθούν μόνο K τάξης όροι καθώς εισάγοντας στην είσοδο μια επιπλέον συνιστώσα με σταθερή τιμή 1 μπορούν να δημιουργηθούν όροι με τάξη μικρότερη από K. Ωστόσο, το K τάξης πολυώνυμο που δημιουργείται δεν έχει πλήρη βαθμό ελευθερίας καθώς οι συνιστώσες του αποτελούνται από αθροίσματα και γινόμενα των w_{kj} και συνεπώς δεν είναι ανεξάρτητες. Για το λόγο αυτό, ένα ΠΣΔ δεν μπορεί να προσεγγίσει ομοιόμορφα όλες τις συνεχείς συναρτήσεις πολλών μεταβλητών που μπορούν να οριστούν σε ένα συμπαγές σύνολο. Παρόλα αυτά, η θεωρία των πολυωνύμων Ridge μπορεί να χρησιμοποιηθεί για να αποδειχθεί ότι η ιδιότητα του καθολικού προσεγγιστή μπορεί να επιτευχθεί απλά προσθέτοντας τις εξόδους Αναλογικών ΠΣΔ διαφορετικών τάξεων. Το δίκτυο που προκύπτει με αυτή τη διαδικασία είναι μια γενίκευση του ΠΣΔ που ονομάζεται Πολυωνυμικό Δίκτυο Ridge και κατασκευάζεται ως εξής.

Για $\mathbf{x} = (x_1, x_2, \ldots, x_N)^\top$ και $\mathbf{w} = (w_1, w_2 \ldots, w_N)^\top \in \mathbb{R}^N$, συμβολίζουμε με $\langle \mathbf{x}, \mathbf{w} \rangle$ το εσωτερικό τους γινόμενο, δηλαδή $\langle \mathbf{x}, \mathbf{w} \rangle = \sum_{i=1}^{N} x_i w_i$. Για ένα δοθέν συμπαγές σύνολο $C \subset \mathbb{R}^N$, όλες οι συναρτήσεις που ορίζονται στο C με την μορφή $f(\langle \mathbf{x}, \mathbf{w} \rangle)$, όπου f είναι μια συνεχής συνάρτηση μιας μεταβλητής, ονομάζονται συναρτήσεις ridge. Ένα *ridge πολυώνυμο* είναι μία ridge συνάρτηση που μπορεί να αναπαρασταθεί ως

$$\sum_{i=0}^{n} \sum_{j=1}^{m} a_{ij} \langle \mathbf{x}, \mathbf{w} \rangle^i, \tag{4.4}$$

για $a_{ij} \in \mathbb{R}$ και $\mathbf{w}_{ij} \in \mathbb{R}^N$.

Στις εργασίες [29,30] αποδείχθηκε ότι κάθε πολυώνυμο στο χώρο $\mathbb{R}^N$ με βαθμό μικρότερο ή ίσο με k μπορεί να αναπαρασταθεί με ένα πολυώνυμο Ridge και επιπλέον μπορεί να υλοποιηθεί με ένα Πολυωνυμικό Δίκτυο Ridge [65]. Από τα αποτελέσματα αυτά και το θεώρημα Stone-Weierstrass προκύπτει ότι τα πολυώνυμα Ridge της μορφής (4.4) έχουν την ιδιότητα καθολικού προσεγγιστή [65].

Ένα Πολυωνυμικό Δίκτυο Ridge (ΡΠΔ) ορίζεται ως ένα ΤΝΔ πρόσθιας τροφοδότησης που βασίζεται στην γενικευμένη μορφή των ridge πολυωνύμων [65]

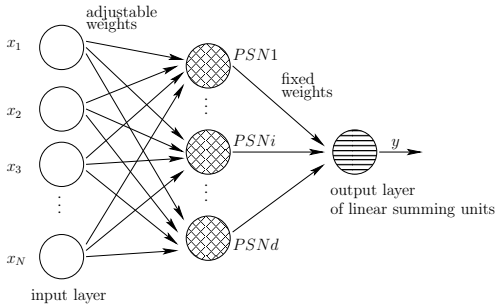
$$p(\mathbf{x}) = \sum_{j=1}^{n_{\text{total}}} \prod_{i=1}^{j} (\langle \mathbf{x}, \mathbf{w}_{ji} \rangle + w_{ji}), \tag{4.5}$$

όπου $n_{\text{total}} = \sum_{l=0}^{k} n_l$, και $n_l = \binom{N+l-1}{l}$, είναι ο συνολικός αριθμός πολυωνύμων βαθμού l N-μεταβλητών, και προσεγγίζει μια άγνωστη συνάρτηση f σε ένα συμπαγές σύνολο $C \subset \mathbb{R}^N$ ως εξής

$$\begin{aligned} f(\mathbf{x}) \quad \approx \quad & (\langle \mathbf{x}, \mathbf{w}_{11} \rangle + w_{11}) + (\langle \mathbf{x}, \mathbf{w}_{21} \rangle + w_{21})(\langle \mathbf{x}, \mathbf{w}_{22} \rangle + w_{22}) + \cdots \\ & + (\langle \mathbf{x}, \mathbf{w}_{n_{\text{total}}1} \rangle + w_{n_{\text{total}}1}) \cdots (\langle \mathbf{x}, \mathbf{w}_{n_{\text{total}}n_{\text{total}}} \rangle + w_{n_{\text{total}}n_{\text{total}}}). \end{aligned} \tag{4.6}$$

Κάθε όρος γινομένου της (4.6) μπορεί να επιτευχθεί ως έξοδος ενός Δικτύου Πί-Σίγμα με γραμμικούς νευρώνες εξόδου. Για το λόγο αυτό, η μορφή των Πολυωνυμικών Δικτύων Ridge μπορεί να θεωρηθεί ως γενίκευση των Δικτύων Πί-Σίγμα. Στο Σχήμα 4.2 αναπαριστάται η γενική αρχιτεκτονική των ΡΠΔ που χρησιμοποιεί τα ΠΣΔ ως δομικά στοιχεία. Το ΡΠΔ έχει ένα μόνο στρώμα προσαρμοζόμενων βαρών το οποίο αποτελεί πλεονέκτημα για την ταχύτητα

εκπαίδευσής του. Η Σχέση (4.6) αποτελεί τη βάση για έναν αλγόριθμο «αυξητικής» εκπαίδευσης όπου Δίκτυα Πί-Σίγμα υψηλότερης τάξης μπορούν να προστεθούν διαδοχικά μέχρι να επιτευχθεί το επιθυμητό επίπεδο ακρίβειας του δικτύου.



Σχήμα 4.2: Ένα Πολυωνυμικό Δίκτυο Ridge (ΡΠΔ) με έναν γραμμικό νευρώνα εξόδου

Η ικανότητα καθολικού προσεγγιστή των ΡΠΔ, η γρηγορότερη εκπαίδευσή τους σε σύγκριση με άλλα είδη ΤΝΔ, και η δυνατότητά τους να εκπαιδεύονται «αυξητικά», τα καθιστά μια σημαντική μεθοδολογία για εφαρμογή σε διάφορα προβλήματα όπως για παράδειγμα προβλήματα προσέγγισης και εύρεσης ριζών [55], αλλά και προβλήματα κρυπτογραφίας.

Στην παρούσα μελέτη θεωρούμε το πρόβλημα υπολογισμού του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου με πραγματικά πολυώνυμα, για το οποίο ισχύει το ακόλουθο θεώρημα.

Θεώρημα 4.2 ([194]) *Έστω $0 \leqslant M < M + H \leqslant p - 1$ και έστω ένα πολυώνυμο $f(X) \in \mathbb{R}[X]$ τέτοιο ώστε, $f(x) \geqslant 0$ αν το x είναι τετραγωνικό υπόλοιπο modulo p, και $f(x) < 0$ αλλιώς, για κάθε στοιχείο $x \in S$ από κάποιο σύνολο $S \subseteq \{M+1, \ldots, M+H\}$ με πληθάριθμο $|S| \geqslant H - s$. Τότε, για οποιοδήποτε $\varepsilon > 0$, ισχύει για το βαθμό του πολυωνύμου f το ακόλουθο φράγμα*

$$\deg f \geqslant \begin{cases} H/2 - 2s - 1 - p^{1/2}\log p, & \text{για οποιοδήποτε } H, \\ \mathcal{C}(\varepsilon)\min\{H, H^2 p^{-1/2}\} - 2s - 1, & \text{αν } p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2+\varepsilon}, \\ (p-1)/2 - 2s - 1, & \text{αν } M = 0, H = p-1, \end{cases} \tag{4.7}$$

όπου το $\mathcal{C}(\varepsilon) > 0$ εξαρτάται μόνο από το ε.

Επίσης, για τα πραγματικά πολυώνυμα πολλών μεταβλητών που υπολογίζουν το λιγότερο σημαντικό ψηφίο του διακριτού λογαρίθμου, ισχύει το ακόλουθο θεώρημα.

Θεώρημα 4.3 ([194]) *Έστω α_0, α_1 δύο διακριτοί πραγματικοί αριθμοί, $r = \lfloor \log p \rfloor$, και έστω ένα πολυώνυμο $f(X_1, \ldots, X_r) \in \mathbb{R}[X_1, \ldots, X_r]$ τέτοιο ώστε, $f(\alpha_{u_1}, \ldots, \alpha_{u_r}) \geqslant 0$, αν x είναι τετραγωνικό υπόλοιπο modulo p, και $f(\alpha_{u_1}, \ldots, \alpha_{u_r}) < 0$, αλλιώς, όπου $x = u_1 u_2 \ldots u_r$ είναι η δυαδική αναπαράσταση του x, και $1 \leqslant x \leqslant 2^r - 1$. Τότε το πολυώνυμο f έχει βαθμό $\deg f \geqslant \log r + o(\log r)$ και περιέχει τουλάχιστον $spr\, f \geqslant 0.25r + o(r)$ διακριτά μονώνυμα.*

Καθώς η ικανότητα καθολικού προσεγγιστή των ΡΠΔ επιτυγχάνεται αθροίζοντας τις εξόδους ΠΣΔ διαφορετικών τάξεων, για την προσέγγιση των πραγματικών πολυωνύμων που υπολογίζουν το λιγότερο σημαντικό ψηφίο του διακριτού λογαρίθμου προκύπτει το ακόλουθο πόρισμα.

Πόρισμα 4.1 *Έστω το πολυώνυμο $f(X) \in \mathbb{R}[X]$ που ικανοποιεί τις συνθήκες του Θεωρήματος 4.2, δηλαδή είναι τέτοιο ώστε $f(x) \geqslant 0$ αν το x είναι τετραγωνικό υπόλοιπο modulo p, και $f(x) < 0$ αλλιώς, για κάθε στοιχείο $x \in S$ από κάποιο σύνολο $S \subseteq \{M+1, \ldots, M+H\}$ με πληθάριθμο $|S| \geqslant H - s$, και το πολυώνυμο $f(X_1, \ldots, X_r)$ που ικανοποιεί τις συνθήκες*

του Θεωρήματος 4.3, δηλαδή είναι τέτοιο ώστε $f(\alpha_{u_1},\ldots,\alpha_{u_r}) \geqslant 0$, *αν* x *είναι τετραγωνικό υπόλοιπο modulo* p, *και* $f(\alpha_{u_1},\ldots,\alpha_{u_r}) < 0$, *αλλιώς, όπου* $x = u_1u_2\ldots u_r$ *είναι η δυαδική αναπαράσταση του* x, *και* $1 \leqslant x \leqslant 2^r - 1$. *Τότε, ισχύουν οι ακόλουθες προτάσεις:*
(*a*) *Υπάρχουν δύο Πολυωνυμικά Δίκτυα Ridge που υλοποιούν το πολυώνυμο* $f(X)$ *και το πολυώνυμο* $f(X_1, X_2\ldots, X_r)$, *αντίστοιχα, και*
(*b*) *Η μέγιστη τάξη των Δικτύων Πί-Σίγμα που αποτελούν καθένα από τα ΡΠΔ του* (*a*), *απαιτείται να είναι για την πρώτη περίπτωση ίση με*

$$\deg f \geqslant \begin{cases} H/2 - 2s - 1 - p^{1/2}\log p, & \text{για οποιοδήποτε } H, \\ \mathcal{C}(\varepsilon)\min\{H, H^2p^{-1/2}\} - 2s - 1, & \text{αν } p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2+\varepsilon}, \\ (p-1)/2 - 2s - 1, & \text{αν } M = 0, H = p-1, \end{cases} \tag{4.8}$$

όπου το $\mathcal{C}(\varepsilon) > 0$ *εξαρτάται μόνο από το* ε, *και ίση με*

$$\deg f(X_1, X_2\ldots, X_r) \geqslant \log r + o(\log r), \tag{4.9}$$

για την δεύτερη περίπτωση.

Επιπροσθέτως, η εγγενής ιδιότητα των ΡΠΔ να αναπαριστούν το τελικό πολυώνυμο που υλοποιούν μετά την εκπαίδευση, ως ένα πολυώνυμο πολλών μεταβλητών, μπορεί να αποβεί ιδιαίτερης σημασίας για το πεδίο της κρυπτογραφίας. Τέλος, η συσχέτιση πολλών κρυπτογραφικών αποτελεσμάτων που θεωρούν τη χρήση συναρτήσεων Boole με την ιδιότητα των Δυαδικών Δικτύων Πί-Σίγμα να υλοποιούν οποιαδήποτε συνάρτηση Boole, μπορούν να οδηγήσει σε θεωρητικά αποτελέσματα που αφορούν και αυτή την κλάση συναρτήσεων.

4.5 Συμπεράσματα

Στο κεφάλαιο αυτό μελετήθηκαν τρεις διαφορετικές εφαρμογές των ΤΝΔ στην κρυπτολογία. Η πρώτη εφαρμογή αφορά στην κρυπτανάλυση κλασικών κρυπτοσυστημάτων όπως το πρόβλημα του διακριτού λογαρίθμου (ΠΔΛ), το πρόβλημα ανταλλαγής κλειδιών Diffie-Hellman (ΠΑΚDH) και το πρόβλημα της παραγοντοποίησης. Τα τρία προβλήματα δόθηκαν με δύο διαφορετικές θεωρήσεις και μελετήθηκαν με διάφορες τοπολογίες και μεθόδους εκπαίδευσης των ΤΝΔ. Τα αποτελέσματα έδειξαν ότι τα ΤΝΔ είναι ικανά να εκπαιδευτούν σε μεγάλο βαθμό για μικρές τιμές των παραμέτρων των προβλημάτων και να παρουσιάσουν καλή γενίκευση. Ωστόσο, όσο οι τιμές των παραμέτρων αυξάνονται η απόδοση των ΤΝΔ πέφτει σημαντικά ακόμα και ως προς την εκπαίδευσή τους. Επίσης, οι διαφορετικές θεωρήσεις των προβλημάτων παρουσίασαν μια διακύμανση των αποτελεσμάτων ανάλογα με το υπό μελέτη πρόβλημα.

Η δεύτερη εφαρμογή των ΤΝΔ που μελετήθηκε ήταν για την κρυπτανάλυση κρυπτοσυστημάτων ελλειπτικών καμπυλών και συγκεκριμένα για τον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου. Τα αποτελέσματα έδειξαν ότι τα ΤΝΔ μπορούν να προσαρμοστούν στα δεδομένα που λαμβάνουν με μεγάλη επιτυχία ενώ αντίθετα η απόκρισή τους σε άγνωστα δεδομένα είναι λίγο καλύτερη από την τυχαία αναζήτηση. Ωστόσο ένα σημαντικό εύρημα είναι η απαίτηση από τα ΤΝΔ λιγότερου χώρου αποθήκευσης για τα γνωστά πρότυπα σε σχέση με το χώρο που απαιτείται για την αποθήκευση του ίδιου του συνόλου.

Τέλος, μελετήθηκε θεωρητικά η εφαρμογή Πολυωνυμικών Δικτύων Ridge στον υπολογισμό του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου που έχει ως απόρροια ένα θεώρημα ύπαρξης Πολυωνυμικών Δικτύων Ridge για την υλοποίηση των υπό μελέτη συναρτήσεων - πολυωνύμων και ένα κάτω φράγμα για την μέγιστη τάξη των δικτύων αυτών.

Μέρος II

Υπολογιστικά Μαθηματικά και Κρυπτολογία

ΚΕΦΑΛΑΙΟ 5

Πολυωνυμική παρεμβολή σε προβλήματα κρυπτογραφίας

5.1 Εισαγωγή

Η κρυπτογραφία δημοσίου κλειδιού είναι άμεσα συνδεδεμένη με ένα σύνολο δύσκολων και πολύπλοκων μαθηματικών προβλημάτων από τα πεδία της υπολογιστικής άλγεβρας, της θεωρίας αριθμών, της θεωρίας πιθανοτήτων, της μαθηματικής λογικής, της Διοφαντικής πολυπλοκότητας και της αλγεβρικής γεωμετρίας. Τέτοια προβλήματα είναι η παραγοντοποίηση [178], ο διακριτός λογάριθμος [4,148,166], ο λογάριθμος του Lucas [197,198] και άλλα [131]. Τα κρυπτοσυστήματα βασίζονται στην υπόθεση ότι τα προβλήματα αυτά είναι υπολογιστικά αδύνατα υπό την έννοια ότι ο υπολογισμός τους δεν μπορεί να ολοκληρωθεί σε πολυωνυμικό χρόνο.

Πολλές τεχνικές, όπως αλγεβρικές, αριθμοθεωρητικές, παρεμβολής και άλλες, έχουν προταθεί για την αντιμετώπιση των παραπάνω προβλημάτων [4,38,96,123,126–128,144,146,148, 166,194,216,217]. Στην μελέτη αυτή εστιάζουμε σε τεχνικές παρεμβολής εφαρμοσμένες σε πεπερασμένα σώματα. Συγκεκριμένα, θεωρούμε τις μεθόδους Aitken και Neville για αντίστροφη πολυωνυμική παρεμβολή σε μια μετατοπισμένη διακριτή εκθετική συνάρτηση και στη συνέχεια στη συνάρτηση του Lucas.

Στην ενότητα που ακολουθεί παρουσιάζονται προηγούμενες μελέτες για μεθόδους παρεμβολής σε πεπερασμένα σώματα, εστιάζοντας στη συνάρτηση του διακριτού λογαρίθμου και στην απεικόνιση Diffie-Hellman. Στη συνέχεια, περιγράφονται οι μέθοδοι παρεμβολής Aitken και Neville και αναλύεται η προτεινόμενη τεχνική για αντίστροφη παρεμβολή στα πεπερασμένα σώματα, παρουσιάζοντας τα αποτελέσματα της εφαρμογής της για μια μετατοπισμένη διακριτή εκθετική συνάρτηση. Η αντίστροφη παρεμβολή με τις μεθόδους Aitken και Neville μελετάται επίσης αναλυτικά για το πρόβλημα του λογαρίθμου του Lucas.

5.2 Μέθοδοι παρεμβολής σε πεπερασμένα σώματα

Σε ένα πεπερασμένο σώμα $\mathbb{F}_q$, όπου $q = p^n$, με p πρώτο αριθμό και n έναν θετικό ακέραιο, κάθε συνάρτηση μπορεί να αναπαρασταθεί ως πολυώνυμο μέσω της παρεμβολής Lagrange. Για κάθε συνάρτηση, $f : \mathbb{F}_q \mapsto \mathbb{F}_q$, υπάρχει μοναδικό πολυώνυμο $p(x)$ βαθμού το πολύ $(q-1)$ που συμπίπτει με την f. Η παρεμβολή είναι υπολογιστικά «ελκυστική» μόνο στην περίπτωση ενός πολυωνύμου με μικρό αριθμό μη-μηδενικών συντελεστών (δηλαδή με υψηλή αραιότητα). Καθώς στην κρυπτογραφία οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης ορίζονται ως συναρτήσεις σε πεπερασμένα σώματα, η προσπάθεια έκφρασής τους ως πολυώνυμα είναι ιδιαίτερα επιθυμητή.

Αναφορικά με την συνάρτηση του διακριτού λογαρίθμου, υπάρχει η πολύ γνωστή έκφραση του Wells [213]:

$$\log_\alpha(x) = \sum_{i=1}^{p-2} \frac{x^i}{1-\alpha^i},$$

όπου $x \neq 0, \alpha, x \in \mathbb{Z}_p$, και α είναι ένας γεννήτορας του $\mathbb{Z}_p^*$. Ο τύπος αυτός μπορεί να γενικευθεί για την περίπτωση ενός σώματος $\mathbb{F}_q$ πρώτης τάξης δύναμης και επιπλέον, για την περίπτωση όπου το α δεν είναι γεννήτορας της πολλαπλασιαστικής ομάδας του σώματος [127, 128, 144]. Ένας διακριτός μετασχηματισμός Fourier μπορεί επίσης να χρησιμοποιηθεί ως εξής [128]:

$$\log_\alpha(x) = (1, 2, \ldots, p-1) \underset{1 \leqslant i,j \leqslant p-1}{(\alpha^{-ij})} \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{pmatrix}.$$

Για την απεικόνιση Diffie-Hellman, έχει προταθεί η ακόλουθη έκφραση [216]:

$$K(x, y) = - \sum_{1 \leqslant i,j \leqslant p-1} x^i y^j \alpha^{-ij}.$$

Η έκφραση αυτή μπορεί να αναπαρασταθεί μέσω ενός διακριτού μετασχηματισμού Fourier ως εξής:

$$K(x, y) = (y, y^2, \ldots, y^{p-1}) \underset{1 \leqslant i,j \leqslant p-1}{(-\alpha^{-ij})} \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{pmatrix}.$$

Η ανταλλαγή κλειδιών του Diffie-Hellman βασίζεται στο γεγονός ότι δεν έχει βρεθεί απλή αναπαράσταση της απεικόνισης Diffie-Hellman $F(g^u, g^v) = g^{uv}$, με $0 \leqslant u, v < d$ και g μη μηδενικό στοιχείο του $\mathbb{F}_q$ τάξης $d|q-1$. Εύκολα μπορεί να επαληθευθεί [216] ότι το πολυώνυμο:

$$F(x, y) = e \sum_{i,j=0}^{d-1} g^{-ij} x^i y^j, \quad ed \equiv 1 \pmod{p},$$

αναπαριστά την απεικόνιση ανταλλαγής κλειδιών Diffie-Hellman στο σώμα $\mathbb{F}_q$, όπου $q = p^n$. Το πολυώνυμο F μπορεί να είναι βαθμού το πολύ $2(d-1)$, ενώ ο μέγιστος αριθμός μη-μηδενικών συντελεστών του F είναι d^2. Για την επίλυση του ΠΑΚDH και την κατάρρευση του κρυπτοσυστήματος Diffie-Hellman θα αρκούσε η εύρεση ενός απλού πολυωνύμου που θα ικανοποιούσε την $F(g^u, g^v) = g^{uv}$, για όλα τα ζεύγη $(u, v) \in \mathcal{W}$ ενός μεγάλου υποσυνόλου $\mathcal{W} \subseteq [0, d-1]^2$.

5.3 Οι μέθοδοι παρεμβολής Aitken και Neville

Οι μέθοδοι παρεμβολής τύπου Lagrange επιτυγχάνουν την επιθυμητή ακρίβεια χρησιμοποιώντας τον μικρότερο δυνατό αριθμό σημείων παρεμβολής. Ωστόσο, ο κατάλληλος αριθμός σημείων παρεμβολής δεν είναι γνωστός εκ των προτέρων. Συνήθως, θεωρείται ένας αριθμός αρχικών σημείων παρεμβολής και, αν τα σημεία αυτά δεν είναι επαρκή νέα σημεία προστίθενται επαναληπτικά μέχρι να επιτευχθεί η απαιτούμενη ακρίβεια. Η πρόσθεση ενός νέου σημείου παρεμβολής στην περίπτωση της παρεμβολής Lagrange δεν μπορεί να πραγματοποιηθεί απευθείας, καθώς το πολυώνυμο παρεμβολής αλλάζει, και συνεπώς όλοι οι υπολογισμοί πρέπει να γίνουν από την αρχή.

Οι μέθοδοι παρεμβολής Aitken και Neville είναι πολύ γνωστές και θεωρούνται ως κλασικές μέθοδοι για την παρεμβολή συναρτήσεων στο σύνολο των πραγματικών αριθμών [21]. Επιπλέον, οι μέθοδοι Aitken και Neville είναι κατασκευαστικές κατά τρόπο τέτοιο που επιτρέπει την πρόσθεση ενός νέου σημείου παρεμβολής με χαμηλό υπολογιστικό κόστος. Αυτό το πλεονέκτημα των προαναφερθέντων μεθόδων παρεμβολής σε σχέση με την μέθοδο Lagrange,

καθώς και το γεγονός ότι οι τύποι παρεμβολής τους μπορούν να εφαρμοστούν σε οποιοδήποτε σώμα αποτέλεσε το κίνητρο για την μελέτη της απόδοσης τους στα πεπερασμένα σώματα.

Έστω $f(x)$ μια συνάρτηση ορισμένη σε ένα σώμα $\mathbb{F}, x_i \in \mathbb{F}, i = 0, 1, \ldots, n$, σημεία παρεμβολής ανά δύο διαφορετικά μεταξύ τους, και $f_i = f(x_i)$. Τότε, το πολυώνυμο παρεμβολής του Aitken ορίζεται ως:

$$P_{0,1,\ldots,m,i}(x) = \frac{1}{(x_i - x_m)} \begin{vmatrix} P_{0,1,\ldots,m}(x) & x_m - x \\ P_{0,1,\ldots,m-1,i}(x) & x_i - x \end{vmatrix}, \quad \text{για} \begin{cases} m = 0, 1, \ldots, n-1, \\ i = (m+1), \ldots, n, \end{cases}$$

όπου, γενικά το $P_{0,1,\ldots,k}$ συμβολίζει το πολυώνυμο Aitken που παρεμβάλλει όλα τα σημεία $x_0, x_1, \ldots, x_k$.

Το αντίστοιχο πολυώνυμο παρεμβολής του Neville είναι:

$$P_{i,i+1,\ldots,i+m}(x) = \frac{1}{(x_{i+m} - x_i)} \begin{vmatrix} P_{i,i+1,\ldots,i+m-1}(x) & x_i - x \\ P_{i+1,i+2,\ldots,i+m}(x) & x_{i+m} - x \end{vmatrix}, \text{για} \begin{cases} m = 1, 2, \ldots, n, \\ i = 0, \ldots, (n-m), \end{cases}$$

όπου, γενικά το $P_{i,i+1,\ldots,i+k}$ συμβολίζει το πολυώνυμο Neville που παρεμβάλλει όλα τα σημεία $x_i, x_{i+1}, \ldots, x_{i+k}$.

Σε πολλές εφαρμογές οι τιμές $f_i, i = 0, 1, \ldots, n$, μιας συνάρτησης $y = f(x)$ στα αντίστοιχα σημεία $x_i, i = 0, 1, \ldots, n$, δίνονται, και ζητείται να βρεθεί το σημείο x^* για το οποίο ισχύει ότι $f(x^*) = y^*$. Το πρόβλημα αυτό ονομάζεται πρόβλημα αντίστροφης παρεμβολής της συνάρτησης f. Και οι δύο μέθοδοι παρεμβολής Aitken και Neville μπορούν να εφαρμοστούν για το πρόβλημα της αντίστροφης παρεμβολής απλώς ανταλλάσσοντας τα x_i και $y_i = f_i$ στους αντίστοιχους τύπους παρεμβολής [21]. Κατ' αυτό τον τρόπο, η έκφραση για την μέθοδο Aitken για αντίστροφη παρεμβολή είναι:

$$P_{0,1,\ldots,m,i}(y) = \frac{1}{(y_i - y_m)} \begin{vmatrix} P_{0,1,\ldots,m}(y) & y_m - y \\ P_{0,1,\ldots,m-1,i}(y) & y_i - y \end{vmatrix}, \quad \text{για} \begin{cases} m = 0, 1, \ldots, n-1, \\ i = (m+1), \ldots, n, \end{cases}$$

ενώ η αντίστοιχη έκφραση της μεθόδου Neville για αντίστροφη παρεμβολή είναι:

$$P_{i,i+1,\ldots,i+m}(y) = \frac{1}{(y_{i+m} - y_i)} \begin{vmatrix} P_{i,i+1,\ldots,i+m-1}(y) & y_i - y \\ P_{i+1,i+2,\ldots,i+m}(y) & y_{i+m} - y \end{vmatrix}, \text{για} \begin{cases} m = 1, 2, \ldots, n, \\ i = 0, \ldots, (n-m). \end{cases}$$

5.4 Οι μέθοδοι Aitken και Neville για αντίστροφη παρεμβολή στα πεπερασμένα σώματα

Στην ενότητα αυτή μελετάμε τις μεθόδους Aitken και Neville για αντίστροφη παρεμβολή στα πεπερασμένα σώματα. Συγκεκριμένα, μελετάμε την τεχνική της αντίστροφης παρεμβολής στις τιμές της μετατοπισμένης διακριτής εκθετικής συνάρτησης:

$$f(x) = \alpha^x - b \pmod{p},$$

στο χώρο $\mathbb{Z}_p$ με p έναν πρώτο αριθμό και α ένα πρωτεύον στοιχείο του $\mathbb{Z}_p$. Η συνάρτηση αυτή είναι αμφιμονοσήμαντη, αφού το α είναι πρωτεύον στοιχείο.

Επειδή οι θεωρούμενες μέθοδοι είναι κατασκευαστικές, δεν χρησιμοποιούνται όλα τα σημεία του πεδίου ορισμού της συνάρτησης ως σημεία παρεμβολής, αλλά τόσα σημεία όσα είναι απαραίτητα για την κατασκευή ενός πολυωνύμου που παρεμβάλλει την συναρτησιακή τιμή $f(x^*) = 0 \pmod{p}$. Η διαδικασία ξεκινά παρεμβάλλοντας δύο συναρτησιακές τιμές της συνάρτησης $f(x)$ για δύο τυχαίες τιμές του x. Το πολυώνυμο που προκύπτει υπολογίζεται στο μηδέν και αν το σημείο x που προκύπτει δεν είναι ο διακριτός λογάριθμος του b επί του $\alpha modulo p$, τότε η συναρτησιακή τιμή του σημείου αυτού αποτελεί το νέο σημείο παρεμβολής.

Πίνακας 5.1: Περιπτώσεις παραμέτρων του προβλήματος που μελετήθηκαν.

# Πρόβλημα	p	α	b
1	101	2	30
2	599	7	200
3	1759	6	500
4	2003	5	100
5	2411	6	700
6	2801	3	300
7	3001	14	100
8	3313	10	400
9	3631	15	3600
10	4001	3	1000
11	4441	21	500
12	4751	19	4500
13	5003	2	1000
14	5209	17	300
15	5881	31	3000
16	6007	3	2000
17	6841	22	4000
18	7001	3	500
19	7841	12	3500
20	8011	14	40
21	8761	23	6000
22	8929	11	3000
23	9001	7	200
24	10007	5	1000

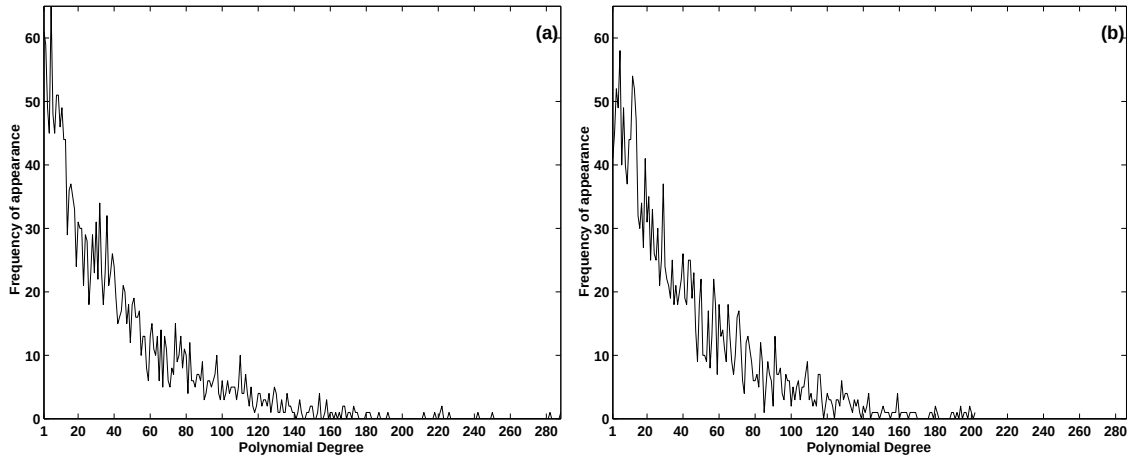
Η αποδοτικότητα και τα χαρακτηριστικά των θεωρούμενων μεθόδων αντίστροφης παρεμβολής σε πεπερασμένα σώματα πρώτης τάξης δοκιμάστηκαν για διαφορετικούς πρώτους αριθμούς, p και τιμές του b. Οι διάφορες περιπτώσεις τιμών των παραμέτρων του προβλήματος που δοκιμάστηκαν δίνονται στον Πίνακα 5.1.

Τα αποτελέσματα για 100 ανεξάρτητα πειράματα για τα παραπάνω στιγμιότυπα του προβλήματος παρουσιάζονται στους Πίνακες 5.2, 5.3, 5.4. Στους πίνακες δίνεται ο αριθμός επαληθεύσεων που πραγματοποιήθηκαν (# Επαληθεύσεων), το πλήθος των σημείων παρεμβολής που χρησιμοποιήθηκαν (# Σημείων) και ο βαθμός του πολυωνύμου που προέκυψε ως αποτέλεσμα (Βαθμός Πολ/μου). Οι επαληθεύσεις αναφέρονται στο πλήθος υπολογισμών του πολυωνύμου στο μηδέν που πραγματοποιούνται για να διαπιστωθεί αν το αποτέλεσμα - σημείο είναι ο διακριτός λογάριθμος. Κάθε επαλήθευση απαιτεί έναν υπολογισμό της μετατοπισμένης διακριτής εκθετικής συνάρτησης, f, για μια συγκεκριμένη τιμή του x. Ο αριθμός των σημείων που χρησιμοποιούνται αναφέρεται στο πλήθος των σημείων παρεμβολής, $y = f(x)$, που χρειάζονται κατά τη διαδικασία, και συνεπώς υπολογίζονται, μέχρι να βρεθεί το κατάλληλο πολυώνυμο παρεμβολής. Πρέπει να παρατηρηθεί ότι το τελικό πολυώνυμο παρεμβολής δεν παρεμβάλλει κατ' ανάγκη όλα τα σημεία που χρησιμοποιούνται από την διαδικασία. Τέλος, η τρίτη ποσότητα (Βαθμός Πολ/μου) αντιστοιχεί στον βαθμό του τελικού πολυωνύμου που παρεμβάλλει την τιμή του διακριτού λογαρίθμου. Το πλήθος των σημείων παρεμβολής που χρησιμοποιούνται για την κατασκευή του τελικού πολυωνύμου είναι (Βαθμός Πολ/μου +1). Για κάθε πείραμα, δύο αρχικά σημεία παρεμβολής επιλέγονται τυχαία στο πεδίο $[1, p-1]$. Για κάθε μια από τις τρεις ποσότητες που καταμετρώνται, στους πίνακες δίνονται η μέση τιμή (Μέση Τ.), η διάμε-

σος (Διάμ.), η τυπική απόκλιση (Τυπ.Απ.), καθώς και η ελάχιστη (Ελάχ.Τ.) και μέγιστη τιμή (Μέγ.Τ.).

Τα αποτελέσματα δείχνουν ότι το υπολογιστικό κόστος για την επίλυση του προβλήματος του διακριτού λογαρίθμου, αναφορικά με το πλήθος των απαιτούμενων επαληθεύσεων, είναι υψηλό και για τις δύο μεθόδους αντίστροφης παρεμβολής. Ωστόσο, ο σχετικά μικρός βαθμός των τελικών πολυωνύμων που προκύπτουν από την διαδικασία της αντίστροφης παρεμβολής συνιστά ενδιαφέρον αποτέλεσμα καθώς δείχνει ότι στις περισσότερες περιπτώσεις υπάρχει ένα πολυώνυμο χαμηλού βαθμού που παρεμβάλλει τον διακριτό λογάριθμο. Για το λόγο αυτό, η εύρεση των κατάλληλων σημείων παρεμβολής είναι κρίσιμη για την μείωση του υπολογιστικού κόστους για την επίλυση του προβλήματος του διακριτού λογαρίθμου.

Ένα ακόμα ενδιαφέρον αποτέλεσμα αποτελεί η υψηλή συχνότητα με την οποία πολυώνυμα μικρού βαθμού προκύπτουν από τα διαφορετικά πειράματα για κάθε στιγμιότυπο του προβλήματος. Το συμπέρασμα αυτό διαφαίνεται από τις χαμηλές τιμές της διαμέσου για τον βαθμό του τελικού πολυωνύμου που δίνονται στον Πίνακα 5.4, σε αντίθεση με τις αντίστοιχες μέγιστες τιμές οι οποίες εμφανίζονται πολύ αραιά. Η συχνότητα εμφάνισης των διαφορετικών βαθμών των τελικών πολυωνύμων για όλα τα πειράματα και των δύο μεθόδων απεικονίζονται στο Σχήμα 5.1. Αναφορικά με την αποτελεσματικότητα της κάθε μεθόδου στην εύρεση του κατάλληλου πολυωνύμου, η μέθοδος Aitken ήταν λίγο καλύτερη από την μέθοδο Neville στις περισσότερες περιπτώσεις.



Σχήμα 5.1: Συχνότητα εμφάνισης πολυωνυμικών βαθμών για όλα τα στιγμιότυπα του προβλήματος με (a) την μέθοδο Aitken και (b) την μέθοδο Neville.

Η απόδοση των δύο μεθόδων αντίστροφης παρεμβολής μελετήθηκε επίσης για διάφορες τιμές του b, κρατώντας σταθερή την τιμή του p. Τα αποτελέσματα αναφορικά με αυτή την πειραματική θεώρηση παρουσιάζονται στον Πίνακα 5.5. Συνολικά, η συμπεριφορά και των δύο μεθόδων είναι αρκετά σταθερή αναφορικά με την παράμετρο b.

5.5 Συμπεράσματα

Στην προηγούμενη ενότητα μελετήθηκε η απόδοση δύο μεθόδων αντίστροφης παρεμβολής, συγκεκριμένα των μεθόδων Aitken και Neville, για μια μετατοπισμένη διακριτή εκθετική συνάρτηση σε πεπερασμένα σώματα. Τα αποτελέσματα δείχνουν ότι το υπολογιστικό κόστος για την επίλυση του ΠΔΛ με αυτή την μεθοδολογία είναι υψηλό και για τις δύο μεθόδους. Συνολικά, η μέθοδος Aitken απεδείχθη λίγο καλύτερη από την μέθοδο Neville. Σημαντικό αποτέλεσμα ωστόσο αποτελεί το γεγονός ότι τα τελικά πολυώνυμα που προκύπτουν από την

Πίνακας 5.2: Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το πλήθος των απαιτούμενων επαληθεύσεων σε 100 ανεξάρτητα πειράματα.

Πρόβλημα	# Επαληθεύσεων									
	AITKEN					**NEVILLE**				
	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.
1	51.06	49.50	27.24	4.00	98.00	53.57	54.50	26.47	5.00	100.00
2	304.34	298.50	190.44	9.00	598.00	313.76	308.00	168.96	11.00	593.00
3	845.33	776.50	505.70	52.00	1741.00	961.97	960.00	502.37	32.00	1748.00
4	885.76	858.50	577.26	4.00	1978.00	1030.32	1076.00	544.13	113.00	1970.00
5	1185.38	1233.50	698.64	6.00	2385.00	1076.98	1060.50	626.18	6.00	2352.00
6	1251.48	1225.00	813.69	39.00	2800.00	1406.53	1362.00	789.02	18.00	2742.00
7	1490.59	1434.00	871.58	7.00	2996.00	1472.15	1438.00	893.62	8.00	2979.00
8	1727.81	1689.50	886.54	80.00	3280.00	1682.65	1556.50	978.54	42.00	3206.00
9	1701.35	1536.50	1109.06	29.00	3578.00	1830.08	1894.00	1040.59	5.00	3625.00
10	1953.68	1758.00	1228.28	41.00	3996.00	2134.41	2023.00	1191.16	14.00	3994.00
11	2297.73	2430.00	1298.40	18.00	4438.00	2197.55	2415.00	1265.07	17.00	4370.00
12	2092.47	1744.00	1452.38	6.00	4613.00	2451.19	2322.00	1361.64	27.00	4625.00
13	2569.09	2992.00	1450.74	48.00	4875.00	2681.18	2864.00	1461.67	28.00	4916.00
14	2538.64	2831.00	1437.81	44.00	5203.00	2485.72	2675.50	1511.98	109.00	5192.00
15	3140.46	3172.50	1686.20	116.00	5730.00	2936.12	2825.50	1826.41	28.00	5861.00
16	3227.38	3088.50	1684.70	38.00	5993.00	3139.66	2867.00	1757.40	45.00	5988.00
17	3725.76	4058.00	2022.05	184.00	6838.00	3429.21	3255.00	1932.10	158.00	6805.00
18	3238.45	2996.50	2019.04	60.00	6926.00	3177.59	3110.00	1939.81	9.00	6990.00
19	3794.16	3498.00	2256.09	98.00	7831.00	3697.39	3648.50	2259.73	181.00	7796.00
20	3801.96	3979.50	2289.30	10.00	7989.00	4025.00	4266.50	2322.49	94.00	7985.00
21	4253.92	4782.00	2463.25	146.00	8704.00	4592.02	5090.50	2732.54	115.00	8611.00
22	4823.47	5221.00	2403.39	57.00	8916.00	4463.26	4737.00	2378.70	7.00	8723.00
23	4350.66	4492.00	2364.91	104.00	8919.00	4719.24	4997.00	2690.34	58.00	8878.00
24	4927.91	5450.50	2932.47	92.00	9734.00	4932.99	4711.50	2988.91	58.00	9963.00

Πίνακας 5.3: Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το πλήθος των χρησιμοποιούμενων σημείων σε 100 ανεξάρτητα πειράματα.

Πρόβλημα	# Σημείων									
	AITKEN					**NEVILLE**				
	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.
1	12.36	11.50	6.15	2.00	27.00	12.78	12.00	5.93	2.00	30.00
2	31.95	29.00	19.01	4.00	96.00	31.43	29.00	15.31	4.00	72.00
3	50.97	44.50	27.15	10.00	126.00	57.22	53.00	28.57	8.00	134.00
4	50.15	47.00	28.76	2.00	138.00	56.97	55.50	26.52	15.00	124.00
5	59.90	58.00	31.35	3.00	147.00	55.07	53.00	27.40	3.00	135.00
6	60.21	56.50	35.48	9.00	220.00	65.74	61.00	31.44	6.00	145.00
7	68.81	62.50	36.85	3.00	190.00	67.51	62.00	36.23	3.00	172.00
8	74.44	68.00	35.10	12.00	170.00	72.76	64.50	37.08	9.00	150.00
9	72.75	63.00	43.54	7.00	176.00	75.23	73.50	39.30	2.00	216.00
10	79.38	68.50	45.88	9.00	224.00	86.02	75.00	46.77	5.00	233.00
11	86.37	84.50	45.71	6.00	272.00	81.52	83.50	41.62	5.00	195.00
12	78.01	66.00	44.95	3.00	181.00	87.62	80.50	42.45	7.00	189.00
13	88.88	95.50	43.22	10.00	193.00	94.79	91.50	48.01	7.00	202.00
14	87.19	90.00	44.47	9.00	284.00	88.97	86.00	51.54	15.00	252.00
15	100.56	96.00	48.11	15.00	210.00	98.40	88.50	56.98	7.00	264.00
16	103.76	93.00	50.98	9.00	269.00	102.50	88.50	54.64	9.00	265.00
17	113.78	111.00	60.69	19.00	343.00	103.87	94.00	52.77	18.00	265.00
18	98.18	88.50	52.63	11.00	252.00	95.84	90.50	52.48	4.00	301.00
19	108.69	96.50	59.65	14.00	329.00	105.62	100.00	57.46	19.00	281.00
20	107.27	105.00	58.25	4.00	312.00	112.37	110.50	59.54	14.00	303.00
21	112.20	117.50	56.97	17.00	299.00	121.49	122.50	63.21	15.00	266.00
22	125.86	124.00	59.34	10.00	353.00	115.79	116.50	53.26	3.00	261.00
23	113.89	111.50	56.05	14.00	290.00	123.24	120.50	64.18	11.00	280.00
24	121.69	125.50	62.27	13.00	268.00	123.68	113.00	66.22	11.00	332.00

Πίνακας 5.4: Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville για το βαθμό του τελικού πολυωνύμου σε 100 ανεξάρτητα πειράματα.

Πρόβλημα	Βαθμός Πολ/μου									
	AITKEN					**NEVILLE**				
	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.	Μέση Τ.	Διάμ.	Τυπ.Απ.	Ελάχ.Τ.	Μέγ.Τ.
1	6.27	5.00	4.44	1.00	25.00	7.61	6.50	5.39	1.00	29.00
2	16.19	11.00	14.25	1.00	80.00	16.92	13.00	12.02	1.00	49.00
3	23.82	18.00	20.77	1.00	113.00	29.43	22.50	24.09	1.00	109.00
4	26.62	19.50	23.10	1.00	113.00	29.95	22.50	22.53	1.00	95.00
5	30.07	21.00	28.41	1.00	125.00	26.16	19.00	22.84	1.00	121.00
6	33.38	24.50	28.74	1.00	121.00	32.41	25.00	27.40	1.00	111.00
7	29.91	25.00	24.50	1.00	116.00	33.91	26.00	27.82	1.00	112.00
8	37.70	32.00	25.80	2.00	123.00	31.71	23.00	26.33	1.00	115.00
9	38.66	31.50	34.32	1.00	143.00	40.04	34.00	32.91	1.00	135.00
10	39.24	29.00	35.27	2.00	168.00	43.19	42.00	33.19	1.00	177.00
11	47.17	35.50	34.66	1.00	127.00	35.95	26.00	29.54	1.00	128.00
12	35.35	25.00	36.91	1.00	174.00	44.07	34.00	34.27	2.00	143.00
13	43.37	36.00	34.83	1.00	130.00	45.92	35.00	38.28	1.00	145.00
14	44.20	35.00	38.53	3.00	282.00	44.92	31.50	38.03	1.00	211.00
15	54.73	44.00	44.67	1.00	180.00	49.17	38.00	44.79	1.00	209.00
16	45.27	36.00	36.94	1.00	173.00	54.55	49.50	43.29	1.00	190.00
17	55.38	40.00	45.02	1.00	218.00	53.58	39.00	48.15	1.00	230.00
18	48.93	38.50	43.07	1.00	212.00	52.54	46.50	40.90	1.00	196.00
19	53.68	44.00	44.84	1.00	192.00	46.34	34.50	39.05	1.00	168.00
20	54.72	38.50	48.85	1.00	242.00	61.39	45.50	53.68	2.00	288.00
21	59.54	42.00	55.87	1.00	296.00	67.06	56.50	50.40	1.00	200.00
22	63.53	51.50	54.91	2.00	259.00	62.33	52.00	46.77	1.00	209.00
23	56.89	43.50	51.90	3.00	288.00	60.18	51.50	48.67	1.00	202.00
24	64.41	51.50	50.12	2.00	222.00	56.21	42.50	54.51	1.00	258.00

Πίνακας 5.5: Αποτελέσματα από 100 ανεξάρτητα πειράματα για $p = 2003$, $\alpha = 5$ και διαφορετικές τιμές της παραμέτρου b.

Πρόβλημα	μέτρο (%)	# Σημείων	Βαθμός Πολ/μου
	Μέση Τιμή	61.07	29.25
$p = 2003$	Διάμεσος	60.00	25.00
$a = 5$	Ελάχ.Τ.	5.00	1.00
$b = 9$	Μέγ.Τ.	142.00	112.00
	Μέση Τιμή	58.86	26.87
$p = 2003$	Διάμεσος	57.00	19.00
$a = 5$	Ελάχ.Τ.	13.00	1.00
$b = 100$	Μέγ.Τ.	180.00	140.00
	Μέση Τιμή	57.41	29.52
$p = 2003$	Διάμεσος	51.00	21.00
$a = 5$	Ελάχ.Τ.	10.00	1.00
$b = 600$	Μέγ.Τ.	153.00	108.00
	Μέση Τιμή	54.07	27.46
$p = 2003$	Διάμεσος	51.00	21.00
$a = 5$	Ελάχ.Τ.	8.00	2.00
$b = 900$	Μέγ.Τ.	110.00	78.00
	Μέση Τιμή	55.89	28.86
$p = 2003$	Διάμεσος	49.00	20.00
$a = 5$	Ελάχ.Τ.	8.00	1.00
$b = 1300$	Μέγ.Τ.	173.00	133.00
	Μέση Τιμή	55.48	28.09
$p = 2003$	Διάμεσος	50.00	23.00
$a = 5$	Ελάχ.Τ.	5.00	2.00
$b = 1550$	Μέγ.Τ.	145.00	123.00
	Μέση Τιμή	55.11	27.88
$p = 2003$	Διάμεσος	51.00	23.00
$a = 5$	Ελάχ.Τ.	9.00	2.00
$b = 1900$	Μέγ.Τ.	162.00	121.00
	Μέση Τιμή	52.23	23.82
$p = 2003$	Διάμεσος	48.00	20.00
$a = 5$	Ελάχ.Τ.	3.00	1.00
$b = 2000$	Μέγ.Τ.	138.00	100.00

μεθοδολογία είναι συνήθως χαμηλού βαθμού. Αυτό σημαίνει ότι στις περισσότερες περιπτώσεις υπάρχει ένα πολυώνυμο χαμηλού βαθμού το οποίο παρεμβάλλει την τιμή του διακριτού λογαρίθμου. Για το λόγο αυτό, η εύρεση των κατάλληλων σημείων παρεμβολής είναι κρίσιμη για την μείωση του υπολογιστικού κόστους της μεθοδολογίας αυτής για την επίλυση του προβλήματος του διακριτού λογαρίθμου.

5.6 Αντίστροφη παρεμβολή με τις μεθόδους Aitken και Neville για το λογάριθμο του Lucas

Η συνάρτηση του Lucas είναι μια μονόδρομη συνάρτηση που πρόσφατα προτάθηκε για χρήση στην κρυπτογραφία δημοσίου κλειδιού. Η ασφάλεια των κρυπτοσυστημάτων που βασίζονται στη συνάρτηση του Lucas οφείλεται στην δυσκολία επίλυσης του προβλήματος λογαρίθμου του Lucas. Στη μελέτη αυτή, το πρόβλημα λογαρίθμου του Lucas ερευνάται χρησιμοποιώντας τεχνικές παρεμβολής. Συγκεκριμένα, οι μέθοδοι Aitken και Neville για αντίστροφη παρεμβολή εφαρμόζονται σε τιμές της ακολουθίας του Lucas ώστε να βρεθεί ένα πολυώνυμο που θα παρεμβάλλει το λογάριθμο του Lucas.

5.7 Εισαγωγικά στοιχεία

Ένα ουσιαστικό κομμάτι της κρυπτογραφίας δημοσίου κλειδιού είναι η χρήση μονόδρομων συναρτήσεων. Οι συναρτήσεις αυτές μπορούν να υπολογιστούν εύκολα αλλά οι αντίστροφές τους είναι πολύ δύσκολο να υπολογιστούν. Οι μονόδρομες συναρτήσεις συνήθως προέρχονται από υπολογιστικά δύσκολα προβλήματα της θεωρίας αριθμών, όπως το πρόβλημα του διακριτού λογαρίθμου και το πρόβλημα της παραγοντοποίησης μεταξύ άλλων. Η πιο γνωστή και συχνά χρησιμοποιούμενη μονόδρομη συνάρτηση είναι η διακριτή εκθετική συνάρτηση, η οποία αποτελεί τη βάση για διάφορα κρυπτοσυστήματα δημοσίου κλειδιού [46,53].

Οι Smith και Lennon στις εργασίες τους [197,198] πρότειναν μια νέα μονόδρομη συνάρτηση για το σχεδιασμό κρυπτοσυστημάτων δημοσίου κλειδιού, την συνάρτηση του Lucas, η οποία ορίζεται ως εξής. Έστω p ένας περιττός πρώτος αριθμός και $\mathbb{F}_p$ ένα πεπερασμένο σώμα τάξης p. Για ένα σταθερό στοιχείο $m \in \mathbb{F}_p$, θεωρούμε την ακόλουθη επαναληπτική γραμμική σχέση δεύτερης τάξης

$$\begin{aligned} V_0(m) &= 2, \quad V_1(m) = m, \\ V_t(m) &= mV_{t-1}(m) - V_{t-2}(m), \quad t \geqslant 2. \end{aligned} \tag{5.1}$$

Η ακολουθία $\{V_t(m)\}, t = 0, 1, \ldots$, ονομάζεται *ακολουθία του Lucas παραγόμενη από το* m και η απεικόνιση,

$$t \mapsto V_t(m), \quad t \geqslant 0,$$

καλείται *συνάρτηση του Lucas*.

Οι Smith και Lennon στην εργασία [197] απέδειξαν ότι ισχύει $V_t(m) = \mu^t + \mu^{-t}$, $t \geqslant 0$, όπου μ και μ^{-1} είναι οι ρίζες του χαρακτηριστικού πολυωνύμου της Εξίσωσης 5.1, δηλαδή του $f(X) = X^2 - mX + 1$. Οι ρίζες μ και μ^{-1} δίνονται από τις ακόλουθες σχέσεις,

$$\mu = \frac{m + \sqrt{m^2 - 4}}{2}, \quad \mu^{-1} = \frac{m - \sqrt{m^2 - 4}}{2}.$$

Αν το $m^2 - 4$ είναι τετραγωνικό υπόλοιπο ως προς μέτρο p ή μηδέν, τότε και οι δύο ρίζες βρίσκονται στο $\mathbb{F}_p$, διαφορετικά και οι δύο ρίζες ανήκουν στο $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Η ασφάλεια των κρυπτοσυστημάτων που χρησιμοποιούν την συνάρτηση του Lucas βασίζεται στην δυσκολία επίλυσης του προβλήματος λογαρίθμου του Lucas ως προς βάση m το οποίο

ορίζεται ως εξής. Δοθέντων ενός πρώτου αριθμού p, οποιουδήποτε $m \in \mathbb{F}_p$ και $z \in \{V_t(m)\}$, όπου $\{V_t(m)\}$, με $t \geqslant 0$, είναι η ακολουθία του Lucas που παράγεται από το m, να βρεθεί ένας ακέραιος αριθμός x τέτοιος ώστε $V_x(m) = z$.

Το πρόβλημα του λογαρίθμου του Lucas είναι ιδιαίτερα σημαντικό για την σύγχρονη κρυπτογραφία [8, 17, 95, 197, 198]. Επιπλέον, η συνάρτηση του Lucas μπορεί να θεωρηθεί ως μια γενίκευση της διακριτής εκθετικής συνάρτησης, καθώς, όπως αποδείχθηκε στην μελέτη [8], αποτελεί μια ειδική μορφή του πολυωνύμου του Dickson. Το γεγονός αυτό πυροδότησε την έρευνα για την υπολογιστική ισοδυναμία του λογαρίθμου του Lucas και του προβλήματος του διακριτού λογαρίθμου [17, 95] και αποδείχθηκε στην εργασία [95] ότι η ασφάλεια της συνάρτησης του Lucas είναι σε πολυωνυμικό χρόνο ισοδύναμη με τα γενικευμένα προβλήματα του διακριτού λογαρίθμου. Η δυσκολία του προβλήματος του διακριτού λογαρίθμου στηρίζεται από πολλές ερευνητικές μελέτες [38, 84, 92, 97, 125, 127, 144, 147, 217, 218] και όπως αποδείχθηκε στις [38, 147, 217] δεν υπάρχουν χαμηλού βαθμού πολυώνυμα παρεμβολής του διακριτού λογαρίθμου για ένα μεγάλο σύνολο δοθέντων δεδομένων. Αντίστοιχη μελέτη για πολυωνυμική αναπαράσταση και κάτω φράγματα στον βαθμό των πολυωνύμων παρεμβολής για μια συνάρτηση που σχετίζεται με το πρόβλημα λογαρίθμου του Lucas παρουσιάζεται στην εργασία [8]. Συγκεκριμένα, στην εργασία αυτή παρουσιάζεται η ακριβής έκφραση ενός πολυωνύμου βαθμού $p-1$ που αναπαριστά το λογάριθμο του Lucas και δίνονται κάτω φράγματα για το βαθμό πολυωνύμων που παρεμβάλλουν τον λογάριθμο του Lucas σε υποσύνολα δοθέντων δεδομένων.

Η εύρεση ενός πολυωνύμου χαμηλού βαθμού ή υψηλής αραιότητας το οποίο να αναπαριστά το λογάριθμο του Lucas αποτελεί μια μέθοδο για τον γρήγορο υπολογισμό του. Για το λόγο αυτό, στην παρούσα μελέτη ερευνούμε το πρόβλημα λογαρίθμου του Lucas υπό μια διαφορετική σκοπιά. Συγκεκριμένα, θεωρούμε τις μεθόδους Aitken και Neville για αντίστροφη παρεμβολή για την αντιμετώπιση του συγκεκριμένου προβλήματος, αξιοποιώντας το ιδιαίτερο χαρακτηριστικό τους ότι καθορίζουν εσωτερικά το πεδίο της παρεμβαλλόμενης συνάρτησης.

5.8 Θεώρηση του προβλήματος

Μελετάμε τις μεθόδους Aitken και Neville για αντίστροφη παρεμβολή σε μια μετατόπιση της συνάρτησης του Lucas, και συγκεκριμένα για την συνάρτηση

$$f(t) = V_t(m) - z, \quad t \geqslant 0,$$

όπου $z \in \mathbb{F}_p$, η οποία δεν είναι αμφιμονοσήμαντη. Ουσιαστικά, αναζητούμε ένα πολυώνυμο που παρεμβάλλει την τιμή $f(t^*) = 0$ της συνάρτησης. Καθώς οι δύο μέθοδοι είναι κατασκευαστικές, η διαδικασία της παρεμβολής ξεκινά παρεμβάλλοντας δύο συναρτησιακές τιμές της συνάρτησης $f(t)$ για δύο τυχαίες τιμές του t. Το πολυώνυμο που δημιουργείται υπολογίζεται στο μηδέν και η τιμή t_0 που προκύπτει επαληθεύεται υπολογίζοντας την συναρτησιακή τιμή $f(t_0)$. Αν ισχύει ότι $f(t_0) = 0$ τότε το t_0 είναι ο λογάριθμος του Lucas ως προς βάση m και η διαδικασία τερματίζεται, διαφορετικά η συναρτησιακή τιμή $f(t_0)$ αποτελεί το νέο σημείο παρεμβολής.

Για τον υπολογισμό της συνάρτησης $f(t)$ θεωρούνται δύο περιπτώσεις ανάλογα με τις ρίζες του χαρακτηριστικού πολυωνύμου της ακολουθίας του Lucas. Εάν οι ρίζες ανήκουν στο σώμα $\mathbb{F}_p$ τότε όλοι οι υπολογισμοί πραγματοποιούνται στο σώμα $\mathbb{F}_p$. Διαφορετικά, αν οι ρίζες ανήκουν στο σώμα $\mathbb{F}_{p^2}$, τότε οι απαραίτητοι υπολογισμοί διακριτής εκθετοποίησης για την εύρεση της τιμής $V_t(m)$ πραγματοποιούνται στο σώμα $\mathbb{F}_{p^2}$.

5.9 Πειραματική θεώρηση και αποτελέσματα

Οι δύο μέθοδοι αντίστροφης παρεμβολής δοκιμάστηκαν για το πρόβλημα λογαρίθμου του Lucas για διάφορες τιμές πρώτων αριθμών p, πρωτευόντων ριζών g ως προς μέτρο p, τιμές

βάσης m και τιμές του z, και για τις δύο περιπτώσεις ριζών, δηλαδή στο σώμα $\mathbb{F}_p$ και στο $\mathbb{F}_{p^2}$, αντίστοιχα. Τα στιγμιότυπα των προβλημάτων που θεωρήθηκαν παρουσιάζονται στον Πίνακα 5.6, όπου οι τιμές του πεδίου «Ρίζες στο $\mathbb{F}_p$» αντιστοιχούν στην περίπτωση όπου οι ρίζες ανήκουν στο σώμα $\mathbb{F}_p$, και οι τιμές του πεδίου «Ρίζες στο $\mathbb{F}_{p^2}$» αντιστοιχούν στην περίπτωση όπου οι ρίζες ανήκουν στο σώμα $\mathbb{F}_{p^2}$.

Πίνακας 5.6: Στιγμιότυπα των προβλημάτων που θεωρήθηκαν για την περίπτωση ριζών του χαρακτηριστικού πολυωνύμου της ακολουθίας του Lucas στο σώμα $\mathbb{F}_p$ (Ρίζες στο $\mathbb{F}_p$) και στο σώμα $\mathbb{F}_{p^2}$ (Ρίζες στο $\mathbb{F}_{p^2}$).

			Ρίζες στο $\mathbb{F}_p$		Ρίζες στο $\mathbb{F}_{p^2}$	
# Πρόβλημα	p	g	m	z	m	z
1	101	2	3	82	4	14
2	599	7	3	365	5	23
3	1759	6	5	1701	4	14
4	2003	5	4	14	3	7
5	2411	6	3	7	6	34
6	2801	3	3	7	4	14
7	3001	14	4	2261	5	23
8	3313	10	4	902	5	23
9	3631	15	3	3419	4	14
10	4001	3	3	2990	4	14
11	4751	19	5	2178	11	119
12	5003	2	5	23	3	7
13	5881	31	4	3362	9	79
14	6007	3	5	1681	3	7
15	7001	3	3	5739	4	14
16	7841	12	3	6924	4	14
17	8011	14	3	7	5	23
18	8929	11	4	545	6	34
19	9001	7	4	8403	5	23
20	10007	5	4	2627	5	23

Τα αποτελέσματα για 100 ανεξάρτητα πειράματα για κάθε στιγμιότυπο του προβλήματος δίνονται στους Πίνακες 5.7,5.8. Και στους δύο πίνακες, δίνονται ο αριθμός των επαληθεύσεων (# Επαληθεύσεων), ο αριθμός των σημείων που χρησιμοποιήθηκαν (# Σημείων), και ο βαθμός των τελικών πολυωνύμων (Βαθμός Πολ/μου). Οι επαληθεύσεις αφορούν στον αριθμό των φορών υπολογισμού ενός πολυωνύμου στο μηδέν ώστε να επαληθευθεί αν το αποτέλεσμα - σημείο ισούται με τον λογάριθμο του Lucas ως προς βάση m. Κάθε επαλήθευση απαιτεί έναν υπολογισμό της συνάρτησης $f(t)$, για μια συγκεκριμένη τιμή του t.

Η ποσότητα «# Σημείων» αναφέρεται στο πλήθος των σημείων παρεμβολής, $y = f(t)$, που χρησιμοποιούνται από την διαδικασία (και συνεπώς υπολογίστηκαν) μέχρι να βρεθεί το κατάλληλο πολυώνυμο παρεμβολής. Ωστόσο, λόγω του κατασκευαστικού χαρακτήρα των μεθόδων παρεμβολής, το τελικό πολυώνυμο μπορεί να μην παρεμβάλλει όλα τα σημεία αυτά. Τέλος, ο «Βαθμός Πολ/μου» αντιστοιχεί στο βαθμό του τελικού πολυωνύμου που παρεμβάλλει την τιμή του λογαρίθμου του Lucas. Ο αριθμός των σημείων παρεμβολής που χρησιμοποιούνται για την κατασκευή του τελικού πολυωνύμου είναι (Βαθμός Πολ/μου +1).

Για κάθε πείραμα, δύο αρχικά σημεία παρεμβολής επιλέγονται τυχαία στο πεδίο $[1, p-1]$. Για κάθε μια από τις τρεις ποσότητες που καταγράφονται (# Επαληθεύσεων, # Σημείων, Βαθμός Πολ/μου), η μέση τιμή (Μ.Τ.), η διάμεσος (Διάμ.), η τυπική απόκλιση (Τ.Α.), καθώς και η ελάχιστη (Ελ.) και μέγιστη τιμή (Μέγ.) υπολογίζονται.

Πίνακας 5.7: Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville σε 100 ανεξάρτητα πειράματα για την περίπτωση ριζών στο σώμα $\mathbb{F}_p$.

AITKEN															
Πρόβλημα	# Επαληθεύσεων					# Σημείων					Βαθμός Πολ/μου				
	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.
1	46.97	30.00	51.12	0.00	326.00	32.47	28.50	23.48	1.00	97.00	4.73	4.00	3.77	0.00	14.00
2	134.58	105.00	126.94	0.00	661.00	112.55	96.50	85.81	1.00	407.00	7.66	5.50	6.34	0.00	31.00
3	464.38	314.50	500.02	0.00	3495.00	365.39	293.50	302.84	1.00	1524.00	13.61	11.00	10.70	0.00	52.00
4	84.05	52.50	102.85	0.00	584.00	80.43	53.00	90.57	1.00	478.00	5.75	5.00	4.66	0.00	24.00
5	601.71	396.50	557.74	2.00	2849.00	489.61	368.50	370.75	4.00	1677.00	18.50	16.00	14.20	1.00	74.00
6	243.02	164.50	231.45	0.00	898.00	225.30	162.50	203.31	1.00	764.00	9.36	7.00	7.89	0.00	37.00
7	66.05	44.00	65.70	0.00	335.00	65.67	45.00	62.01	1.00	314.00	5.35	4.00	4.67	0.00	19.00
8	414.79	291.00	399.04	15.00	2483.00	372.23	279.00	313.86	17.00	1744.00	14.34	11.00	10.95	1.00	68.00
9	574.65	439.00	520.08	2.00	2558.00	502.32	420.00	403.84	4.00	1803.00	16.19	13.00	12.13	1.00	61.00
10	81.65	52.00	88.25	0.00	575.00	80.91	53.50	83.38	1.00	534.00	6.13	5.00	4.65	0.00	20.00
11	1115.85	594.00	1318.30	0.00	7572.00	876.33	565.50	828.60	1.00	3786.00	19.45	14.00	18.84	0.00	87.00
12	1237.94	1036.50	1023.22	2.00	4789.00	1021.75	941.00	727.05	4.00	3078.00	23.59	20.00	16.60	1.00	74.00
13	1529.05	959.00	1694.05	3.00	7310.00	1187.00	891.00	1087.87	5.00	4202.00	21.93	16.00	19.67	1.00	98.00
14	1527.72	947.50	1852.38	8.00	9698.00	1176.03	887.00	1051.08	10.00	4769.00	23.84	18.50	20.97	1.00	107.00
15	1671.58	1029.00	1724.95	0.00	8898.00	1343.99	957.00	1132.74	1.00	5041.00	26.37	21.00	23.21	0.00	120.00
16	3715.67	3104.00	3289.47	65.00	18856.00	2597.46	2553.50	1722.80	67.00	7104.00	36.50	28.00	31.03	1.00	135.00
17	401.51	247.00	454.12	1.00	2715.00	380.71	245.00	404.40	3.00	2295.00	12.99	10.00	10.67	0.00	47.00
18	2371.20	1656.50	2296.85	19.00	10017.00	1883.87	1518.00	1521.90	21.00	6039.00	28.75	21.00	25.50	1.00	109.00
19	1048.29	651.50	1199.67	31.00	7100.00	926.81	627.00	924.16	33.00	4871.00	19.92	15.00	17.25	1.00	82.00
20	2353.83	1845.50	1898.68	47.00	8071.00	1965.46	1692.00	1398.36	49.00	5515.00	27.60	22.0	22.80	1.00	102.00

NEVILLE															
Πρόβλημα	# Επαληθεύσεων					# Σημείων					Βαθμός Πολ/μου				
	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.
1	47.61	47.50	49.23	0.00	278.00	33.02	31.50	23.10	1.00	89.00	4.61	3.50	3.89	0.00	16.00
2	181.90	152.00	176.20	0.00	968.00	142.16	114.00	107.05	1.00	478.00	9.24	7.00	7.28	0.00	28.00
3	443.11	380.50	435.98	0.00	1958.00	355.42	269.50	294.37	1.00	1192.00	11.37	9.00	8.83	0.00	42.00
4	88.90	90.00	86.86	0.00	438.00	86.28	59.00	79.70	1.00	395.00	5.25	3.50	4.57	0.00	18.00
5	627.15	554.00	519.77	13.00	3125.00	514.05	474.00	357.92	15.00	1760.00	15.23	11.50	12.00	1.00	46.00
6	240.76	171.00	238.60	0.00	1092.00	223.14	147.50	207.55	1.00	901.00	9.63	7.00	7.86	0.00	34.00
7	64.05	56.00	53.57	0.00	265.00	63.49	53.00	50.62	1.00	246.00	5.83	4.00	4.65	0.00	18.00
8	406.36	367.50	434.64	2.00	2431.00	360.96	245.00	346.01	4.00	1689.00	11.96	9.50	10.60	1.00	48.00
9	594.15	535.50	489.96	2.00	2448.00	523.27	417.50	391.60	4.00	1801.00	17.59	15.00	14.02	1.00	56.00
10	75.33	46.00	83.51	0.00	419.00	74.92	44.50	79.66	1.00	398.00	5.60	4.00	4.56	0.00	21.00
11	1203.58	990.50	1413.61	0.00	7020.00	926.54	635.00	874.09	1.00	3645.00	19.15	15.00	17.59	0.00	117.00
12	1139.67	837.00	1305.51	2.00	9144.00	911.31	648.50	790.61	4.00	4167.00	22.20	18.50	19.20	1.00	99.00
13	1465.15	1181.50	1509.38	6.00	8697.00	1169.27	901.00	972.77	8.00	4533.00	22.94	17.50	18.60	1.00	76.00
14	1540.68	1527.00	1379.59	18.00	6942.00	1250.55	1023.00	932.83	20.00	4072.00	24.29	20.50	19.00	1.00	79.00
15	1974.82	1880.00	2009.95	0.00	10388.00	1534.43	1291.00	1281.68	1.00	5434.00	29.09	21.00	23.76	0.00	94.00
16	3835.49	2762.00	3987.39	16.00	23017.00	2560.39	2389.50	1850.69	18.00	7430.00	39.72	32.50	33.01	1.00	138.00
17	357.01	286.50	375.17	1.00	2473.00	341.58	238.00	339.51	3.00	2122.00	10.96	8.00	10.22	0.00	58.00
18	2405.76	1619.50	2704.83	6.00	18320.00	1862.98	1382.00	1557.72	8.00	7764.00	32.41	25.00	27.33	1.00	175.00
19	978.87	627.00	1087.30	11.00	7372.00	875.50	677.00	844.18	13.00	5012.00	17.90	14.00	17.09	1.00	112.00
20	2476.01	2530.00	2554.21	18.00	19746.00	1994.78	2044.50	1551.64	20.00	8634.00	28.85	25.50	22.83	1.00	89.00

Πίνακας 5.8: Αποτελέσματα των μεθόδων αντίστροφης παρεμβολής Aitken και Neville σε 100 ανεξάρτητα πειράματα για την περίπτωση ριζών στο σώμα $\mathbb{F}_{p^2}$.

AITKEN															
Πρόβλημα	# Επαληθεύσεων					# Σημείων					Βαθμός Πολ/μου				
	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.
1	8.46	5.50	10.04	0.00	52.00	8.79	7.00	7.70	1.00	38.00	1.78	2.00	1.68	0.00	7.00
2	259.60	217.50	216.44	0.00	1029.00	188.77	183.50	125.91	1.00	485.00	11.70	9.50	8.61	0.00	39.00
3	792.54	625.50	666.09	2.00	2592.00	568.34	537.50	378.71	4.00	1367.00	18.39	16.50	12.93	1.00	47.00
4	1002.74	725.50	1053.57	6.00	7133.00	669.78	616.50	461.80	8.00	1948.00	19.34	15.00	17.28	1.00	112.00
5	1221.30	816.50	1236.63	0.00	8447.00	819.35	703.00	555.48	1.00	2333.00	21.43	18.50	16.93	0.00	73.00
6	1216.80	800.50	1328.68	2.00	7059.00	828.70	692.50	642.93	4.00	2583.00	19.48	17.00	15.38	1.00	84.00
7	1306.25	894.50	1394.61	5.00	10001.00	906.64	777.00	658.66	7.00	2904.00	24.78	23.00	20.42	1.00	131.00
8	460.96	325.00	444.91	2.00	2506.00	406.35	311.00	350.57	4.00	1775.00	14.92	13.00	11.39	1.00	52.00
9	1852.59	968.50	2190.82	65.00	13735.00	1169.41	850.50	920.04	66.00	3557.00	28.13	20.50	23.27	1.00	107.00
10	517.33	367.00	491.07	3.00	3244.00	462.29	350.50	377.75	5.00	2190.00	14.25	12.00	10.63	1.00	48.00
11	641.66	490.50	710.80	4.00	5491.00	562.10	469.00	508.02	6.00	3246.00	16.57	15.00	12.05	1.00	56.00
12	2322.47	2016.00	2028.76	3.00	11154.00	1637.83	1645.00	1089.07	5.00	4450.00	36.11	31.50	25.07	1.00	128.00
13	3349.57	2301.50	3346.93	25.00	16341.00	2124.32	1896.50	1499.86	27.00	5527.00	35.01	27.50	27.40	1.00	131.00
14	2314.08	1489.50	2559.03	31.00	15257.00	1640.25	1329.50	1285.18	33.00	5537.00	27.70	23.00	24.11	1.00	126.00
15	3167.17	2457.50	3003.33	9.00	13716.00	2205.43	2077.50	1568.08	11.00	6065.00	35.16	25.50	29.45	1.00	130.00
16	3875.90	3470.50	3187.13	54.00	15872.00	2716.24	2797.00	1649.76	56.00	6795.00	41.02	32.50	34.22	1.00	158.00
17	943.05	691.00	862.04	5.00	3881.00	852.02	665.50	722.69	7.00	3117.00	20.60	14.50	17.55	1.00	68.00
18	2272.53	1853.50	2076.25	10.00	11965.00	1841.48	1679.50	1397.48	12.00	6589.00	32.23	29.00	26.49	1.00	112.00
19	3751.20	2800.50	3565.80	33.00	17037.00	2673.58	2415.00	1959.90	35.00	7579.00	37.28	26.50	34.72	1.00	168.00
20	4972.11	3962.50	4461.65	2.00	16878.00	3384.46	3297.50	2388.80	4.00	8165.00	50.69	39.50	41.17	1.00	174.00

NEVILLE															
Πρόβλημα	# Επαληθεύσεων					# Σημείων					Βαθμός Πολ/μου				
	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.	Μ.Τ.	Διάμ.	Τ.Α.	Ελ.	Μέγ.
1	7.36	8.00	7.57	0.00	33.00	7.93	6.00	6.17	1.00	29.00	1.77	2.00	1.58	0.00	6.00
2	269.56	164.00	343.32	0.00	2083.00	178.21	147.50	137.31	1.00	581.00	10.07	7.00	7.89	0.00	37.00
3	851.42	900.50	840.22	3.00	5562.00	580.66	463.00	403.11	5.00	1677.00	21.04	15.50	18.03	1.00	102.00
4	1133.77	1005.00	1110.86	4.00	5971.00	729.59	666.00	493.48	6.00	1901.00	22.38	18.00	17.16	1.00	85.00
5	1316.51	1312.50	1225.28	0.00	5497.00	868.04	790.00	574.28	1.00	2157.00	21.65	17.50	16.85	0.00	75.00
6	1634.80	1316.50	1623.25	57.00	6694.00	1022.62	921.50	736.33	57.00	2526.00	24.51	21.00	20.67	1.00	91.00
7	1502.49	1171.00	1403.31	5.00	6676.00	1014.02	950.00	709.49	7.00	2684.00	23.92	19.50	17.91	2.00	79.00
8	365.08	334.50	368.11	2.00	1871.00	330.31	249.00	301.13	4.00	1439.00	12.18	10.00	9.37	1.00	46.00
9	1825.26	1353.00	2055.20	18.00	9359.00	1166.45	863.50	912.58	20.00	3335.00	28.32	20.50	26.26	1.00	122.00
10	729.39	660.50	715.29	7.00	3595.00	619.75	506.50	516.94	9.00	2365.00	18.89	16.50	14.89	1.00	74.00
11	841.00	761.00	770.95	5.00	3295.00	724.86	633.00	591.19	7.00	2399.00	20.08	16.00	15.18	1.00	69.00
12	2179.27	1727.50	2342.17	2.00	12466.00	1490.78	1290.50	1154.39	4.00	4572.00	26.64	20.00	23.14	1.00	112.00
13	3227.29	2515.00	2925.22	97.00	16257.00	2159.17	1978.00	1312.52	98.00	5489.00	35.71	31.00	28.66	1.00	147.00
14	2952.24	1982.00	3670.16	10.00	21967.00	1852.00	1375.00	1521.13	12.00	5844.00	29.04	21.00	24.87	1.00	112.00
15	3352.11	3112.00	3736.95	32.00	22103.00	2218.47	1899.50	1638.08	34.00	6685.00	33.77	29.00	28.86	1.00	158.00
16	3952.63	3453.50	4181.73	29.00	25482.00	2603.54	2453.50	1891.57	31.00	7552.00	39.48	31.50	32.31	1.00	150.00
17	951.18	1125.50	939.90	3.00	5047.00	851.16	668.00	767.83	5.00	3723.00	21.73	16.50	18.31	1.00	97.00
18	2132.81	1954.50	2372.73	25.00	18035.00	1709.60	1362.50	1370.63	27.00	7732.00	25.69	19.50	21.77	1.00	102.00
19	4891.85	3395.00	5014.92	94.00	27638.00	3171.10	2881.50	2126.46	96.00	8569.00	48.10	39.50	39.87	1.00	206.00
20	4221.56	4179.50	4096.85	35.00	20638.00	2999.15	2767.00	2112.28	37.00	8723.00	40.68	31.50	31.38	1.00	146.00

Τα αποτελέσματα δείχνουν ότι και οι δύο μέθοδοι Aitken και Neville παρουσιάζουν παρόμοια συμπεριφορά στην εύρεση του πολυωνύμου που παρεμβάλλει την τιμή του λογαρίθμου του Lucas (και για τις δύο περιπτώσεις του πεδίου ορισμού των ριζών) και χρειάζονται περίπου το ένα τρίτο του πληθάριθμου του σώματος επαληθεύσεις για να το βρουν, που είναι αρκετά μεγάλο κόστος. Ωστόσο, ενδιαφέρον παρουσιάζει το γεγονός που παρατηρήθηκε και για το πρόβλημα του διακριτού λογαρίθμου (Ενότητα 5.4) ότι ο βαθμός των τελικών πολυωνύμων είναι χαμηλός. Αυτό σημαίνει ότι υπάρχει ένα πολυώνυμο χαμηλού βαθμού που παρεμβάλλει την τιμή του λογαρίθμου του Lucas.

Συγκριτικά με τα αποτελέσματα που προέκυψαν για το πρόβλημα του διακριτού λογαρίθμου και περιγράφονται στην αρχή του κεφαλαίου, στην περίπτωση του λογαρίθμου του Lucas ο αριθμός των επαληθεύσεων που απαιτούνται για την εύρεση του κατάλληλου πολυωνύμου είναι μικρότερος από τον αντίστοιχο αριθμό που χρειάζεται για το πρόβλημα του διακριτού λογαρίθμου. Το ίδιο ισχύει και για τον βαθμό των τελικών πολυωνύμων, δηλαδή οι βαθμοί των πολυωνύμων που παρεμβάλλουν την τιμή του διακριτού λογαρίθμου είναι υψηλότεροι από τους αντίστοιχους βαθμούς των πολυωνύμων που παρεμβάλλουν την τιμή του λογαρίθμου του Lucas. Ωστόσο, δεν ισχύει το ίδιο για τον αριθμό των σημείων παρεμβολής που χρησιμοποιούνται από την διαδικασία, καθώς περισσότερα σημεία υπολογίζονται και χρησιμοποιούνται για το πρόβλημα του λογαρίθμου του Lucas.

5.10 Συμπεράσματα

Το πρόβλημα του λογαρίθμου του Lucas είναι ιδιαίτερα σημαντικό για την σύγχρονη κρυπτογραφία καθώς η ασφάλεια πολλών κρυπτοσυστημάτων βασίζεται σε αυτό. Η εύρεση ενός πολυωνύμου χαμηλού βαθμού ή χαμηλής sparsity που αναπαριστά το λογάριθμο του Lucas είναι κρίσιμη για την επίλυση του προβλήματος. Για το σκοπό αυτό, στην παρούσα μελέτη δύο μέθοδοι αντίστροφης παρεμβολής, οι μέθοδοι Aitken και Neville εφαρμόζονται για την αντιμετώπιση του προβλήματος του λογαρίθμου του Lucas. Συγκεκριμένα, μελετάται η αντίστροφη παρεμβολή στις τιμές της συνάρτησης του Lucas για την εύρεση ενός πολυωνύμου που παρεμβάλλει την τιμή του λογαρίθμου του Lucas. Και οι δύο μέθοδοι έχουν κατασκευαστικό χαρακτήρα που επιτρέπει να ξεκινά η διαδικασία με δύο σημεία παρεμβολής και να προστίθενται νέα σημεία παρεμβολής απευθείας με χαμηλό υπολογιστικό κόστος. Τα αποτελέσματα δείχνουν ότι το υπολογιστικό κόστος για την αντιμετώπιση του προβλήματος λογαρίθμου του Lucas με την μεθοδολογία αυτή παραμένει υψηλό. Ωστόσο, υπάρχουν πολυώνυμα χαμηλού βαθμού που παρεμβάλλουν την τιμή του λογαρίθμου του Lucas για κάθε στιγμιότυπο του προβλήματος που μελετάται. Τέλος, τα αποτελέσματα συγκρινόμενα με τα αντίστοιχα για το πρόβλημα του διακριτού λογαρίθμου παρέχουν μια ενδιαφέρουσα παρατήρηση αναφορικά με την υπολογιστική ισοδυναμία των δύο προβλημάτων.

ΚΕΦΑΛΑΙΟ **6**

Νέα κρυπτοσυστήματα συμμετρικού κλειδιού βασιζόμενα σε περιοδικές τροχιές

6.1 Εισαγωγή

Τα τελευταία χρόνια οι ερευνητικές μελέτες στο πεδίο των μη γραμμικών δυναμικών συστημάτων και ειδικά των συστημάτων με χαοτική συμπεριφορά οδήγησαν και στη διερεύνηση πιθανών εφαρμογών τους. Μεταξύ των εφαρμογών αυτών εμφανίστηκε και το πεδίο της χαοτικής κρυπτογράφησης. Στα πλαίσια της χαοτικής κρυπτογράφησης αρχικά μελετήθηκαν αυτόνομα χαοτικά συστήματα ως γεννήτριες ψευδοτυχαίων αριθμών και στη συνέχεια ο συγχρονισμός χαοτικών συστημάτων οδήγησε στην διερεύνηση μη-αυτόνομων χαοτικών συστημάτων με σήματα συνεχών τιμών για την μετάδοση πληροφοριών [121,142,162,214].

Συγκεκριμένα, αναπτύχθηκαν διάφορα σχήματα για το μετασχηματισμό των σημάτων πληροφορίας σε χαοτική κυματομορφή για κρυπτογράφηση και την άντληση της πληροφορίας από μεταδιδόμενη κυματομορφή για την αποκρυπτογράφηση. Τα πιο σημαντικά από αυτά είναι τα συστήματα χαοτικής μετατροπής (chaotic masking), τα συστήματα χαοτικής μετάθεσης κλειδώματος (chaos shift keying) και τα συστήματα χαοτικής αλλοίωσης ή αντίστροφα συστήματα. Στα συστήματα χαοτικής μετατροπής το σύστημα κρυπτογράφησης αποτελείται από ένα αυτόνομο χαοτικό σύστημα, η έξοδος του οποίου προστίθεται στην πληροφορία προς κρυπτογράφηση. Το άθροισμά τους μεταδίδεται μέσω του καναλιού. Το σύστημα αποκρυπτογράφησης χρησιμοποιεί το μεταδιδόμενο σήμα για τον συγχρονισμό ενός ισοδύναμου χαοτικού συστήματος με το αντίστοιχο της κρυπτογράφησης. Το ανακατασκευασμένο χαοτικό σήμα αφαιρείται στη συνέχεια από το μεταδιδόμενο σήμα οπότε προκύπτει η πληροφορία. Προκειμένου να είναι εγγυημένος ο συγχρονισμός του αποδέκτη η πληροφορία που μεταδίδεται πρέπει να είναι επαρκώς μικρή σε σχέση με το χαοτικό σήμα. Στα συστήματα χαοτικής μετάθεσης κλειδώματος (chaos shift keying), το σύστημα κρυπτογράφησης αποτελείται από δύο ή περισσότερα αυτόνομα χαοτικά συστήματα με διαφορετικές παραμέτρους. Σύμφωνα με το σήμα της πληροφορίας ένα από τα συστήματα αυτά επιλέγεται και η έξοδός του μεταδίδεται στο κανάλι. Το σύστημα αποκρυπτογράφησης αποτελείται από τον ίδιο αριθμό χαοτικών συστημάτων, τα οποία προσπαθούν να συγχρονιστούν με τα αντίστοιχα της κρυπτογράφησης. Οι παράμετροι ρυθμίζονται έτσι ώστε μόνο ένα ζεύγος χαοτικών συστημάτων να συγχρονίζεται κάθε φορά. Η ανίχνευση του συγχρονισμού αυτού αποκωδικοποιεί την πληροφορία. Τέλος, στα συστήματα χαοτικής αλλοίωσης (ή αντίστροφα συστήματα) η κρυπτογράφηση γίνεται από ένα μη αυτόνομο χαοτικό σύστημα του οποίου η κατάσταση επηρεάζεται από την πληροφορία. Ο αποκωδικοποιητής συγχρονίζεται με τον κωδικοποιητή μέσω ανακατασκευής της κατάστασής του χρησιμοποιώντας το μεταδιδόμενο σήμα. Η πληροφορία ανακτάται εφαρμόζοντας την αντίστροφη διαδικασία κρυπτογράφησης στην ανακατασκευασμένη κατάσταση και στο μεταδιδόμενο σήμα. Όλα τα παραπάνω συστήματα έχουν μελετηθεί αναλυτικά και πειραματικά τόσο σε εφαρμογές συνεχούς χρόνου όσο και σε διακριτού χρόνου στις εργασίες [63,151,221].

Το ενδιαφέρον για την εφαρμογή του χάους στην διαδικασία της κρυπτογράφησης προέκυψε από την προφανή πολυπλοκότητα του γεωμετρικού σήματος και τις στατιστικές ιδιότητες που παρατηρούνται στα μη γραμμικά δυναμικά συστήματα [90, 219]. Κατ' αυτό τον τρόπο,

τα χαοτικά σήματα μπορούν να θεωρηθούν ως συνεχών τιμών ισοδύναμα των ψευδοτυχαίων ακολουθιών διακριτών τιμών που χρησιμοποιούνται στην κλασική κρυπτογραφία [40].

Στο κεφάλαιο αυτό παρουσιάζουμε ένα νέο κρυπτοσύστημα συμμετρικού κλειδιού που βασίζεται σε μη γραμμικά δυναμικά συστήματα. Το κρυπτοσύστημα αξιοποιεί τις ιδιότητες των μη γραμμικών απεικονίσεων και των σταθερών σημείων τους για την κρυπτογράφηση της πληροφορίας. Συγκεκριμένα, το πρωτότυπο μήνυμα αποτελείται από συμβολοσειρές (χαρακτήρες) από ένα γνωστό αλφάβητο (για παράδειγμα ASCII), ενώ το κρυπτογράφημα αποτελείται από σταθερά σημεία μη γραμμικών απεικονίσεων. Επιπλέον, εισάγουμε ένα μέτρο της ποιότητας των κλειδιών που χρησιμοποιούνται. Τέλος, παρουσιάζουμε και αναλύουμε τρεις τροποποιήσεις του βασικού κρυπτοσυστήματος που το καθιστούν πιο σθεναρό σε διάφορες κρυπταναλυτικές επιθέσεις.

6.2 Βασικά στοιχεία μη γραμμικών δυναμικών απεικονίσεων

Γενικά, οι διδιάστατες μη γραμμικές απεικονίσεις παρουσιάζουν την ακόλουθη μορφή:

$$\Phi : \begin{cases} \widehat{x}_1 &= \varphi_1(x_1, x_2), \\ \widehat{x}_2 &= \varphi_2(x_1, x_2). \end{cases} \tag{6.1}$$

Σε μια μη γραμμική απεικόνιση της μορφής (6.1) υπάρχουν σημεία τα οποία είναι αμετάβλητα ή σταθερά υπό την απεικόνιση. Τα σημεία αυτά συνήθως αποκαλούνται περιοδικές τροχιές της απεικόνισης. Ένα σημείο $X = (x_1, x_2)^\top$ καλείται σταθερό σημείο της απεικόνισης Φ αν $\Phi(X) = X$. Επίσης, καλείται *σταθερό σημείο τάξης* p, *ή περιοδική τροχιά περιόδου* p, αν ισχύει

$$X = \Phi_p^p(X) \equiv \underbrace{\Phi(\Phi \cdots (\Phi(X)) \cdots)}_{p \text{ φορές}}. \tag{6.2}$$

Ένα τυπικό παράδειγμα μιας μη γραμμικής απεικόνισης είναι η διδιάστατη απεικόνιση του Hénon [68,211]:

$$\Phi : \begin{pmatrix} \widehat{x}_1 \\ \widehat{x}_2 \end{pmatrix} = R(a) \begin{pmatrix} x_1 \\ x_2 + g(x_1) \end{pmatrix}, \tag{6.3}$$

όπου $(x_1, x_2)^\top \in \mathbb{R}^2$ και

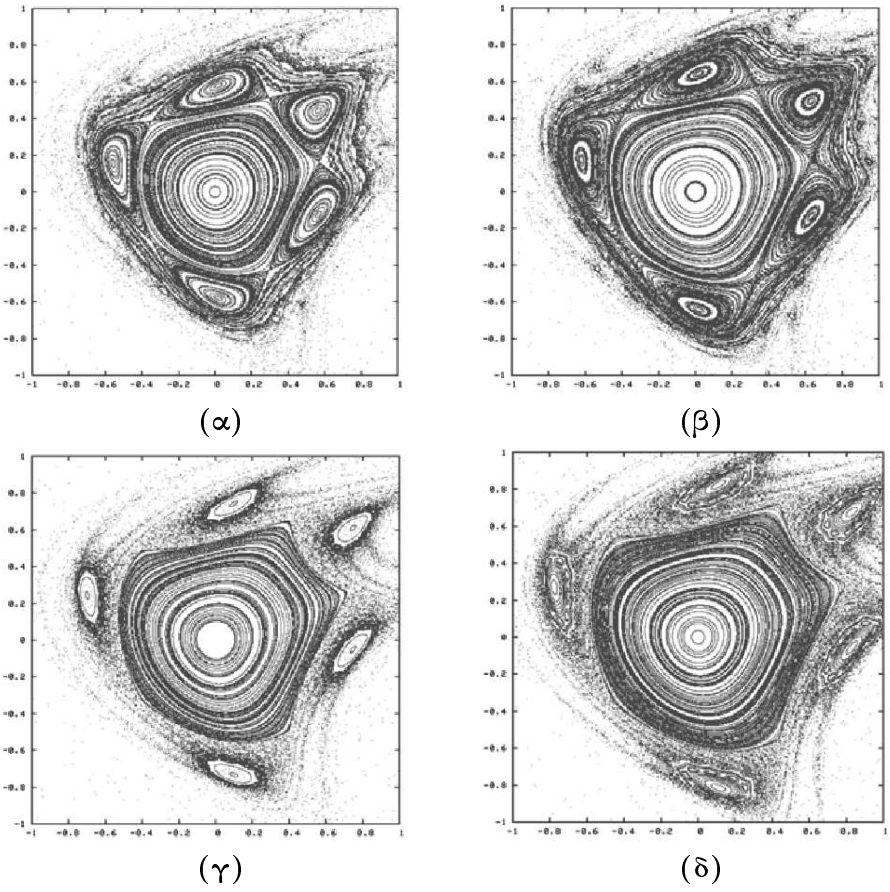
$$R(a) = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix},$$

όπου $a \in [0, \pi]$ είναι η γωνία περιστροφής και $g(x_1) = -x_1^2$. Στο Σχήμα 6.1 παρουσιάζεται η διδιάστατη απεικόνιση του Hénon για διαφορετικές τιμές των παραμέτρων της.

Παρότι χρησιμοποιούμε την διδιάστατη απεικόνιση του Hénon, μια μεγάλη ποικιλία απεικονίσεων μπορούν να χρησιμοποιηθούν μεταξύ των οποίων και οι απεικονίσεις Standard Map [172], Gingerbreadman Map [45], Predator-Prey Map [196], καθώς και απεικονίσεις μεγαλύτερης διάστασης όπως η απεικόνιση του Lorenz [114], του Rössler [180] και η 4-διάστατη απεικόνιση του Hénon [212].

Για τον υπολογισμό των περιοδικών τροχιών μιας απεικόνισης έχουν προταθεί διάφορες μέθοδοι. Για παράδειγμα, χρησιμοποιώντας το πακέτο CHABIS [209,210] για την απεικόνιση του Hénon με $a = \cos^{-1}(0.24)$ και $g(x_1) = -x_1^2$, υπολογίζεται το ακόλουθο σταθερό σημείο με περίοδο $p = 5$

$$X_1^5 = (0.5672405470221847, -0.1223202134278941)^\top.$$



Σχήμα 6.1: Η διδιάστατη απεικόνιση του Hénon στο χώρο (x_1, x_2) για (α) $\cos\alpha = 0.24$, $g(x_1) = -x_1^2$, (β) $\cos\alpha = 0.24$, $g(x_1) = -0.9x_1^2$, (γ) $\cos\alpha = 0.2$, $g(x_1) = -x_1^2$, (δ) $\cos\alpha = 0.2$, $g(x_1) = -0.9x_1^2$

Για να λάβουμε τα υπόλοιπα σταθερά σημεία της ίδιας τροχιάς απαιτούνται απλές επαναλήψεις εφαρμογής της απεικόνισης στο σταθερό σημείο που έχει ήδη υπολογιστεί,

$$\begin{aligned} X_2^5 &= \Phi(X_1^5) = (0.5672405470221847, 0.4440820516139216)^\top, \\ X_3^5 &= \Phi(X_2^5) = (0.0173925844399303, 0.5800185952239573)^\top, \\ X_4^5 &= \Phi(X_3^5) = (-0.5585984457571741, 0.1560161118011652)^\top, \\ X_5^5 &= \Phi(X_4^5) = (0.0173925844399305, -0.5797160932304572)^\top. \end{aligned}$$

Κατ' αυτό τον τρόπο, αν μια απεικόνιση και ένα σταθερό της σημείο με περίοδο p είναι γνωστά, τα υπόλοιπα $(p-1)$ σταθερά σημεία της ίδιας περιοδικής τροχιάς μπορούν εύκολα να υπολογιστούν. Το πακέτο CHABIS δίνει την δυνατότητα υπολογισμού ευσταθών ή ασταθών περιοδικών τροχιών με πολύ μεγάλες τιμές περιόδων [211,212].

Σε κάθε περιοδική τροχιά αντιστοιχεί ένας *αριθμός περιστροφής* $\sigma = \nu/(2\pi) = i_1/i_2$, όπου ν είναι η συχνότητα της τροχιάς και i_1, i_2 είναι δύο θετικοί ακέραιοι. Από την ακολουθία με την οποία τα παραπάνω σταθερά σημεία δημιουργούνται στον χώρο (x_1, x_2), μπορούμε να συμπεράνουμε ότι ο αριθμός περιστροφής της τροχιάς είναι $\sigma = 1/5$, το οποίο σημαίνει ότι η τροχιά παράγει $i_2 = 5$ σημεία, περιστρεφόμενη γύρω από το κέντρο $i_1 = 1$ φορά.

6.3 Βασική μορφή του προτεινόμενου κρυπτοσυστήματος

Η κεντρική ιδέα του προτεινόμενου κρυπτοσυστήματος είναι η απόκρυψη της πληροφορίας στα σταθερά σημεία μιας τροχιάς (συμβολίζεται με O) μιας μη γραμμικής απεικόνισης. Έστω $X_0, \Phi_1^p(X_0), \Phi_2^p(X_0), \ldots, \Phi_{p-1}^p(X_0)$ σταθερά σημεία της τροχιάς O. Όλα τα σταθερά σημεία της τροχιάς O αποθηκεύονται με τη σειρά με την οποία εμφανίζονται εφαρμόζοντας επαναληπτικά $p-1$ φορές την απεικόνιση Φ χρησιμοποιώντας το αρχικό σταθερό σημείο X_0. Μια τέτοια τροχιά O μπορεί να υπολογιστεί χρησιμοποιώντας την γενικευμένη μέθοδο διχοτόμησης [209–211], καθώς επίσης και μεθόδους υπολογιστικής νοημοσύνης [160, 161], ή άλλες παραδοσιακές μεθόδους εύρεσης ριζών (όπως οι μέθοδοι Newton και Broyden).

Ισοδύναμα, ας θεωρήσουμε την ομάδα $G_o = \langle \mathbb{Z}_p, + \rangle$, με στοιχεία, $r_i \in \mathbb{Z}_p$, τα οποία εκφράζουν το πλήθος των επαναλήψεων της απεικόνισης Φ επί οποιουδήποτε αρχικού σταθερού σημείου X_0 μιας περιοδικής τροχιάς με περίοδο p. Ο τελεστής «+» συμβολίζει το πλήθος των επαναλήψεων της απεικόνισης Φ επί ενός αρχικού σταθερού σημείου X_0 και αντιστοιχεί στην σύνθεση της απεικόνισης Φ, δηλαδή

$$\Phi_{r_i}^p(X_0) \circ \Phi_{r_j}^p(X_0) = (\Phi_{r_i}^p \circ \Phi_{r_j}^p)(X_0) = \Phi_{r_i+r_j}^p(X_0).$$

Συνεπώς, η πρόσθεση των επαναλήψεων της απεικόνισης Φ αντιστοιχεί στην πρόσθεση στοιχείων modulo p, δηλαδή $r_i + r_j \pmod p$, όπου p είναι η περίοδος της περιοδικής τροχιάς O.

Αν η μη γραμμική απεικόνιση Φ, η τροχιά O και ένα σταθερό σημείο X_0 της O (το οποίο θεωρείται ως αρχικό σταθερό σημείο της τροχιάς O) είναι γνωστά, μπορούμε να υπολογίσουμε το πλήθος επαναλήψεων της απεικόνισης Φ που απαιτούνται για να λάβουμε οποιοδήποτε σταθερό σημείο της ίδιας τροχιάς ξεκινώντας από το αρχικό σταθερό σημείο X_0. Είναι σημαντικό να παρατηρήσουμε ότι τα στοιχεία της τροχιάς O, μπορούν να τοποθετηθούν σε μια συνδεδεμένη λίστα, καθώς έχουν συγκεκριμένη σειρά εμφάνισης η οποία είναι γνωστή μόνο αν η μη γραμμική απεικόνιση είναι γνωστή. Όπως περιγράφουμε στις ακόλουθες ενότητες, η σειρά εμφάνισης των σταθερών αυτών σημείων αποτελεί τη βάση για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης του προτεινόμενου κρυπτοσυστήματος.

6.3.1 Κατασκευή του κλειδιού

Στη βασική του μορφή το κρυπτοσύστημα δέχεται ένα μήνυμα m ως είσοδο (για παράδειγμα μια ακολουθία χαρακτήρων ASCII) και παράγει ένα μητρώο $C \in \mathbb{R}^{length(m)\times 2}$ ως έξοδο. Αυτό σημαίνει ότι κάθε χαρακτήρας του αρχικού μηνύματος κρυπτογραφείται σε ένα σταθερό σημείο μιας συγκεκριμένης περιοδικής τροχιάς. Θεωρώντας την απεικόνιση του Hénon σαν παράδειγμα για την δημιουργία του κλειδιού, το κλειδί k του κρυπτοσυστήματος αποτελείται από τα ακόλουθα στοιχεία

α) Μια μη γραμμική απεικόνιση Φ με τα ακόλουθα χαρακτηριστικά: (i) την τιμή του $\alpha \in [0, \pi]$ και (ii) έναν μη γραμμικό όρο $g(x_1)$,

β) ένα σταθερό σημείο X_0,

γ) έναν θετικό ακέραιο p (αρκετά μεγάλο, για παράδειγμα, $p \geqslant 300$, και κατά προτίμηση πρώτο αριθμό) που δηλώνει την τάξη της τροχιάς O στην οποία ανήκει το σταθερό σημείο X_0.

Παρατηρούμε ότι είναι απαραίτητο να επιλέγονται περιοδικές τροχιές των οποίων η περίοδος ξεπερνά κατά το ήμισυ τον πληθάριθμο του συνόλου χαρακτήρων που χρησιμοποιείται. Για παράδειγμα, αν χρησιμοποιείται το σύνολο χαρακτήρων ASCII για το μήνυμα, πρέπει $p \geqslant 128$.

Ο αλγόριθμος κατασκευής του κλειδιού αποτελείται από τα ακόλουθα βήματα.

Αλγόριθμος κατασκευής κλειδιού:

1. Επέλεξε τυχαία μια γωνία στροφής $\alpha \in [0, \pi]$.
2. Επέλεξε έναν μη γραμμικό όρο $g(x_1)$.
3. Επέλεξε έναν αρκετά μεγάλο θετικό ακέραιο p (κατά προτίμηση ο p πρέπει να είναι πρώτος αριθμός).
4. Επέλεξε μια περιοχή του χώρου στην οποία θα πρέπει να βρίσκεται το σταθερό σημείο X_0.
5. Χρησιμοποίησε μια μέθοδο (για παράδειγμα το CHABIS [209]) για τον εντοπισμό ενός σταθερού σημείου X_0.
6. Έλεγξε αν ο p είναι ο μικρότερος ακέραιος που ικανοποιεί την σχέση $X_0 = \Phi_p^p(X_0)$ και τερμάτισε.

Παρατηρούμε ότι όταν ο p είναι πρώτος αριθμός το έκτο βήμα του αλγορίθμου κατασκευής του κλειδιού μπορεί να παραλειφθεί. Επίσης, οι επιλογές των βημάτων $1-4$ μπορεί να μην δώσουν ένα σταθερό σημείο X_0 και στην περίπτωση αυτή απαιτείται νέα επιλογή των παραμέτρων του κλειδιού.

6.3.2 Αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης

Ο αλγόριθμος κρυπτογράφησης δέχεται ως είσοδο ένα μήνυμα m, $m_1 m_2 \dots m_n$, με n χαρακτήρες (για παράδειγμα χαρακτήρες ASCII), και ένα κλειδί k, και επιστρέφει ένα κρυπτογράφημα $C \in \mathbb{R}^{n \times 2}$. Ο αλγόριθμος περιγράφεται στα ακόλουθα βήματα.

Αλγόριθμος κρυπτογράφησης:

1. Αρχικοποίησε το $C_0 = X_0$, $i = 1$.
2. Εφάρμοσε $ASCII(m_i)$ φορές την θεωρούμενη μη γραμμική απεικόνιση Φ ξεκινώντας από το σταθερό σημείο C_{i-1}, ώστε να επιτευχθεί το $C_i = \Phi^p_{ASCII(m_i)}(C_{i-1})$.
3. Προχώρησε στον επόμενο χαρακτήρα, θέτοντας $i = (i + 1)$.
4. **Αν** $i < n$ **τότε** πήγαινε στο Βήμα 2, **αλλιώς** τερμάτισε.

Αντίστροφα, ο αλγόριθμος αποκρυπτογράφησης δέχεται ως είσοδο ένα κρυπτογράφημα $C \in \mathbb{R}^{n \times 2}$ και ένα κλειδί k και παρέχει ως έξοδο το αρχικό κείμενο m, μέσω της ακόλουθης διαδικασίας.

Αλγόριθμος αποκρυπτογράφησης:

1. Αρχικοποίησε το $C_0 = X_0$, $i = 1$.
2. Ξεκινώντας από το σταθερό σημείο C_{i-1}, μέτρησε το πλήθος των επαναλήψεων, noi, της θεωρούμενης μη γραμμικής απεικόνισης Φ που απαιτούνται για να ικανοποιηθεί για πρώτη φορά η σχέση $C_i = \Phi^p_{noi}(C_{i-1})$. Ο χαρακτήρας m_i του αρχικού κειμένου επιτυγχάνεται από την ισότητα, $noi = ASCII(m_i)$.
3. Προχώρησε στον επόμενο χαρακτήρα, θέτοντας $i = (i + 1)$.
4. **Αν** $i < n$ **τότε** πήγαινε στο Βήμα 2, **αλλιώς** τερμάτισε.

6.4 Ποιότητα των κλειδιών

Στο προτεινόμενο κρυπτοσύστημα, το ουσιαστικό στοιχείο του κλειδιού είναι το αρχικό σταθερό σημείο που χρησιμοποιείται, καθώς όλα τα υπόλοιπα σταθερά σημεία της ίδιας περιοδικής τροχιάς της μη γραμμικής απεικόνισης παράγονται από αυτό. Είναι σημαντικό να παρατηρήσουμε ότι το αρχικό σταθερό σημείο δεν είναι χρήσιμο αν η απεικόνιση δεν είναι γνωστή. Το αρχικό σταθερό σημείο που χρησιμοποιείται για το κλειδί μπορεί να αποτελέσει ένα μέτρο για την ποιότητα του κλειδιού. Αυτό οφείλεται στην ιδιότητα ευαισθησίας των σταθερών σημείων μιας περιοδικής τροχιάς σε διαταραχές. Συγκεκριμένα, όσο μεγαλύτερες είναι οι πραγματικές ιδιοτιμές της Ιακωβιανής υπολογιζόμενης στο σταθερό σημείο (Βήμα 2 του ακόλουθου αλγόριθμου ελέγχου ευστάθειας), τόσο πιο ευαίσθητο είναι το κλειδί σε μικρές διαταραχές. Τα σταθερά σημεία που είναι ευαίσθητα σε μικρές διαταραχές συνιστούν περιοδικές τροχιές που ονομάζονται *ασταθείς*. Στην περίπτωση αυτή, όλα τα σταθερά σημεία μιας ασταθούς περιοδικής τροχιάς μπορούν να επιτευχθούν με ακρίβεια μόνο αν το αρχικό σταθερό σημείο είναι γνωστό με μεγάλη ακρίβεια. Οποιαδήποτε μικρή διαταραχή στις συντεταγμένες ενός σταθερού σημείου οδηγεί σε μεγάλες μεταβολές σε όλα τα υπόλοιπα σταθερά σημεία της ίδιας περιοδικής τροχιάς. Για το λόγο αυτό, ακόμα και αν κάποιος αντίπαλος αποκτήσει γνώση για κάποια ψηφία του αρχικού σταθερού σημείου μιας ασταθούς περιοδικής τροχιάς δεν μπορεί να παράγει τα υπόλοιπα σταθερά σημεία της συγκεκριμένης τροχιάς. Σύμφωνα με την παραπάνω ιδιότητα, δίνεται ο ακόλουθος ορισμός για *ισχυρά κλειδιά*.

Ορισμός 6.1 *Ένα κλειδί του προτεινόμενου κρυπτοσυστήματος καλείται ισχυρό, αν το αρχικό σταθερό σημείο που χρησιμοποιείται ανήκει σε μια ασταθή περιοδική τροχιά της δοθείσης μη γραμμικής απεικόνισης.*

Για την επιβεβαίωση του είδους μιας περιοδικής τροχιάς, δηλαδή ευσταθής ή ασταθής, μπορεί να χρησιμοποιηθεί ο ακόλουθος αλγόριθμος ελέγχου ευστάθειας. Ο αλγόριθμος δέχεται ως είσοδο τη μη γραμμική απεικόνιση Φ και το αρχικό σταθερό σημείο X_0 που χρησιμοποιούνται, την περίοδο p της περιοδικής τροχιάς στην οποία ανήκει το σημείο X_0 και το Ιακωβιανό μητρώο της απεικόνισης Φ.

Αλγόριθμος ελέγχου ευστάθειας:

1. Υπολόγισε το Ιακωβιανό μητρώο της απεικόνισης Φ για το αρχικό σταθερό σημείο X_0, και θέσε $J = \text{Jacobian}(X_0)$.
2. **Για** $i = 2 : p$ **κάνε**
   $X_i = \Phi(X_{i-1})$
   $J = \text{Jacobian}(X_i)J$.
3. Υπολόγισε τις ιδιοτιμές $\lambda_1, \lambda_2, \ldots, \lambda_{dim} \in \mathbb{C}$ του μητρώου J.
4. **Αν** $\Im(\lambda_i) \neq 0$ **και** $(\Re(\lambda_i)^2 + \Im(\lambda_i)^2)^{1/2} = 1$, για κάθε $i = 1, 2, \ldots, dim$
   τότε η τροχιά είναι «ΕΥΣΤΑΘΗΣ»
   αλλιώς αν $\Im(\lambda_i) \neq 0$ **και** $(\Re(\lambda_i)^2 + \Im(\lambda_i)^2)^{1/2} \neq 1$, για οποιοδήποτε $i \in \{1, 2, \ldots, dim\}$ **τότε** η τροχιά είναι «ΜΙΓΑΔΙΚΗ ΑΣΤΑΘΗΣ»
   αλλιώς αν $\Im(\lambda_i) = 0$ **και** $\Re(\lambda_i) \neq 1$ για κάθε $i = 1, 2, \ldots, dim$
   τότε η τροχιά είναι «ΑΣΤΑΘΗΣ»

Αν όλες οι ιδιοτιμές του Ιακωβιανού μητρώου J είναι μιγαδικές και βρίσκονται πάνω στον μοναδιαίο κύκλο τότε η τροχιά είναι *ευσταθής*. Διαφορετικά, αν έστω μία ιδιοτιμή είναι μιγαδική και δεν βρίσκεται στον μοναδιαίο κύκλο τότε η τροχιά είναι *μιγαδική ασταθής*. Τέλος, αν όλες οι ιδιοτιμές είναι πραγματικές και οι τιμές τους είναι διάφορες της μονάδας τότε η τροχιά καλείται *ασταθής*. Στην τελευταία περίπτωση, όσο μεγαλύτερη είναι η τιμή μιας ιδιοτιμής, τόσο πιο ασταθής θεωρείται η τροχιά.

6.5 Τροποποιήσεις της βασικής μορφής του κρυπτοσυστήματος και θέματα αποδοτικότητας

Στην παρούσα ενότητα παρουσιάζονται τρεις τροποποιημένες εκδοχές του προτεινόμενου κρυπτοσυστήματος. Οι τροποποιήσεις αυτές έχουν ως στόχο να καταστήσουν το κρυπτοσύστημα περισσότερο σθεναρό σε πιθανές επιθέσεις.

6.5.1 Πρώτη τροποποίηση

Ας θεωρήσουμε την περίπτωση όπου κάποιος αντίπαλος γνωρίζει δύο κρυπτογραφήματα C_i και C_j (δηλαδή δύο σταθερά σημεία που κρυπτογραφούν τους χαρακτήρες m_i και m_j του κειμένου αντίστοιχα) και το πλήθος των επαναλήψεων της απεικόνισης Φ που απαιτούνται για να λάβουμε το C_j από το C_i. Τότε, ο αντίπαλος μπορεί να λάβει τον χαρακτήρα m_j του αρχικού κειμένου. Για να αποφευχθεί η περίπτωση αυτή μπορεί να χρησιμοποιηθεί ένα κρυφό αρχικό σταθερό σημείο για την κρυπτογράφηση του κάθε χαρακτήρα του αρχικού κειμένου, και ορίζεται ως εξής.

Ορισμός 6.2 *Ένα σταθερό σημείο καλείται αρχικό σταθερό σημείο για την κρυπτογράφηση ενός χαρακτήρα m_i αν χρησιμοποιείται ως σημείο εκκίνησης για να λάβουμε $ASCII(m_i)$ επαναλήψεις της απεικόνισης Φ.*

Χρησιμοποιώντας ένα κρυφό αρχικό σταθερό σημείο για την κρυπτογράφηση ενός χαρακτήρα m_i, έχουμε ότι

$$\text{Κρυπτογράφηση}(m_i) = \Phi^p_{ASCII(m_i)}(X_{initial\, m_i}).$$

Στη βασική μορφή του κρυπτοσυστήματος θεωρείται ότι το αρχικό σταθερό σημείο για κάθε χαρακτήρα είναι το σταθερό σημείο που κρυπτογραφεί τον προηγούμενο χαρακτήρα, δηλαδή είναι

$$\text{Κρυπτογράφηση}(m_i) = \Phi^p_{ASCII(m_i)}(\Phi^p_{ASCII(m_{i-1})}(X_0)).$$

Για τον υπολογισμό των αρχικών σταθερών σημείων για κάθε χαρακτήρα του κειμένου, προτείνονται οι ακόλουθες σχέσεις:

$$\begin{cases} X_{initial\, m_1} = \Phi^p_{\beta H(m) \pmod p}(X_0), \\ X_{initial\, m_i} = \Phi^p_{\gamma ASCII(m_{i-1}) \pmod p}(C_{i-1}), \quad \text{για } i = 2, \ldots \end{cases}$$

όπου β, γ είναι δύο θετικοί και μεγάλοι ακέραιοι αριθμοί οι οποίοι πρέπει να προσαρτώνται στο κλειδί k, και $H(m)$ είναι το αποτέλεσμα μιας μονόδρομης συνάρτησης hash επί του μηνύματος m (για παράδειγμα MD5 [185]). Για $\beta = \gamma = 0$, λαμβάνουμε τη βασική μορφή του προτεινόμενου κρυπτοσυστήματος. Τέλος, μπορεί να προστεθεί ένας τυχαίος χαρακτήρας μπροστά από το μήνυμα m έτσι ώστε να λαμβάνεται πάντα ένα τελείως διαφορετικό κρυπτογράφημα.

6.5.2 Δεύτερη τροποποίηση

Ας θεωρήσουμε την περίπτωση όπου κάποια πληροφορία σχετική με την σειρά των σταθερών σημείων της περιοδικής τροχιάς που χρησιμοποιείται έχει αποκαλυφθεί σε κάποιον αντίπαλο. Για να αντιμετωπιστεί μια επίθεση βασιζόμενη στη ανάλυση της συχνότητας εμφάνισης των κρυπτογραφημάτων, στην δεύτερη τροποποίηση, κάθε χαρακτήρας του αρχικού κειμένου κρυπτογραφείται από ένα σταθερό σημείο που είναι ανεξάρτητο από τα σταθερά σημεία που έχουν χρησιμοποιηθεί προηγουμένως (που κρυπτογραφούν τους προηγούμενους χαρακτήρες). Για την υλοποίηση αυτής της νέας τροποποίησης, δύο μεγάλοι θετικοί ακέραιοι αριθμοί β, γ επιλέγονται και προσαρτώνται στο κλειδί k. Επιπλέον, χρησιμοποιείται μια μονόδρομη συνάρτηση hash, H που εφαρμόζεται στο κείμενο m και δίνει την τιμή $H(m)$. Τότε,

υπολογίζεται το γινόμενο $H(m)\beta$ και χρησιμοποιείται για την αρχικοποίηση μιας γεννήτριας ομοιόμορφων τυχαίων αριθμών. Υποθέτουμε ότι κάθε φορά, i, καλείται η γεννήτρια αριθμών και επιστρέφει έναν τυχαίο αριθμό $\mathrm{rand}(i) \in [0,1]$. Μετά από κάθε κλήση υπολογίζεται η τιμή $\mathrm{rand}_p(i) = \lceil \mathrm{rand}(i) \rceil p$. Κατά συνέπεια, το αρχικό σταθερό σημείο για κάθε χαρακτήρα για κρυπτοσυστήματα ροής δίνεται από τη σχέση

$$X_{initial\, m_i} = \Phi_{rand_p(i)\gamma \pmod p}(X_0),$$

και για άλλα κρυπτοσυστήματα δίνεται από τη σχέση

$$\begin{cases} X_{initial\, m_1} = \Phi_{rand_p(1)\gamma \pmod p}(X_0), \\ X_{initial\, m_i} = \Phi_{rand_p(i)ASCII(m_{i-1})\gamma \pmod p}(X_0), \quad \text{για } i = 2,3,\ldots \end{cases}$$

6.5.3 Τρίτη τροποποίηση

Στην τροποποίηση αυτή θεωρούμε το ακόλουθο πρόβλημα. Δοθέντων p σταθερών σημείων μιας τροχιάς O με τυχαία σειρά, να βρεθεί μια απεικόνιση Φ η οποία έχει την τροχιά O ως περιοδική της τροχιά. Σε αυτή την περίπτωση, η εύρεση μιας απεικόνισης Φ που θα ικανοποιούσε το παραπάνω πρόβλημα θα αποκάλυπτε και τα υπόλοιπα σταθερά σημεία της ίδιας τροχιάς και κατά συνέπεια το αποκρυπτογραφημένο κείμενο. Η υποθετική αυτή περίπτωση μπορεί να εξαλειφθεί εφαρμόζοντας τον τελεστή XOR (κατά ψηφίο) μεταξύ του σταθερού σημείου που κρυπτογραφεί τον χαρακτήρα του αρχικού κειμένου και του αρχικού σταθερού σημείου του. Κατά αυτό τον τρόπο, τα σταθερά σημεία της τροχιάς O δεν μπορούν να αποκαλυφθούν. Επιπλέον, το σύνολο των κρυπτογραφημάτων γίνεται μεγέθους $Card(ASCII)p$ που αντιστοιχεί σε $Card(ASCII)p!$ μεταθέσεις για επίθεση εξαντλητικής αναζήτησης (brute force).

6.5.4 Θέματα αποδοτικότητας

Στην παρούσα ενότητα δίνεται ο αριθμός των FLOPs που απαιτούνται για την κρυπτογράφηση ή την αποκρυπτογράφηση ενός χαρακτήρα του αρχικού κειμένου. Για την απεικόνιση του Hénon και για την κρυπτογράφηση (ή αποκρυπτογράφηση) του χαρακτήρα m_i, χρησιμοποιώντας την βασική μορφή του κρυπτοσυστήματος, είναι

$$\mathrm{FLOPs}\,(C(m_i)) = ASCII(m_i)(6 + \mathrm{FLOPs}\,(g(x_1))).$$

Για τις τροποποιήσεις του αλγορίθμου κρυπτογράφησης/αποκρυπτογράφησης μόνο ένας μικρός αριθμός FLOPs χρειάζεται να προστεθεί. Συγκεκριμένα, τα επιπλέον FLOPs είναι

$$\mathrm{FLOPs}\,(C(m_i)) \leqslant p\,(6 + \mathrm{FLOPs}\,(g(x_1))) + t,$$

όπου t είναι ένας μικρός σταθερός αριθμός.

6.6 Πειραματική θεώρηση και αποτελέσματα

Για την αξιολόγηση του προτεινόμενου κρυπτοσυστήματος, εκτός από τον αριθμό των απαιτούμενων FLOPs που παρουσιάστηκαν στην ενότητα 6.5.4, καταμετράται και ο χρόνος (CPU) που απαιτείται για την κρυπτογράφηση (και αποκρυπτογράφηση) πολλών διαφορετικών αρχικών κειμένων (κρυπτογραφημάτων). Επιπλέον, δίνεται η αναλογία των δυαδικών ψηφίων που περιέχονται στα κρυπτογραφήματα που παράγονται από τις παραπάνω κρυπτογραφήσεις.

Για τα πειράματα και για λόγους σύγκρισης δοκιμάστηκαν τριών διαφορετικών ειδών αρχικά κείμενα, και συγκεκριμένα, δοκιμάστηκαν κοινά κείμενα Αγγλικών, κείμενα που περιείχαν τυχαίους χαρακτήρες και κείμενα που επαναλάμβαναν τον ίδιο χαρακτήρα. Τα αποτελέσματα

για το τελευταίο είδος κειμένων είναι σημαντικά καθώς επιβεβαιώνουν ότι ακόμα και στην περίπτωση που τα αρχικά κείμενα περιέχουν κάποιου είδους μοτίβα (δομές) το κρυπτογραφημένο κείμενο δεν παρέχει καμία πληροφορία για το χαρακτηριστικό αυτό. Τα αποτελέσματα καταγράφονται στον Πίνακα 6.1, αφορούν στη βασική μορφή του κρυπτοσυστήματος και πραγματοποιήθηκαν σε έναν υπολογιστή P4 με 512MB μνήμης RAM χρησιμοποιώντας κώδικα του Matlab6.5.

Πίνακας 6.1: Πειραματικά αποτελέσματα για διάφορα είδη αρχικών κειμένων

Είδος αρχικού κειμένου	χρόνος CPU για κρυπτογρ./αποκρυπτ.	Ποσοστό κρυπτογραφήματος σε μηδέν	ένα
10000 τυχαίοι χαρακτήρες	≈ 0.001 *sec*	49.9999%	50.0001%
100000 τυχαίοι χαρακτήρες	≈ 0.00102 *sec*	49.9999%	50.0001%
100000 χαρ. Αγγλικών κειμ.	≈ 0.00103 *sec*	49.9999%	50.0001%
100000 ίδιοι χαρακτήρες	≈ 0.00103 *sec*	49.9999%	50.0001%

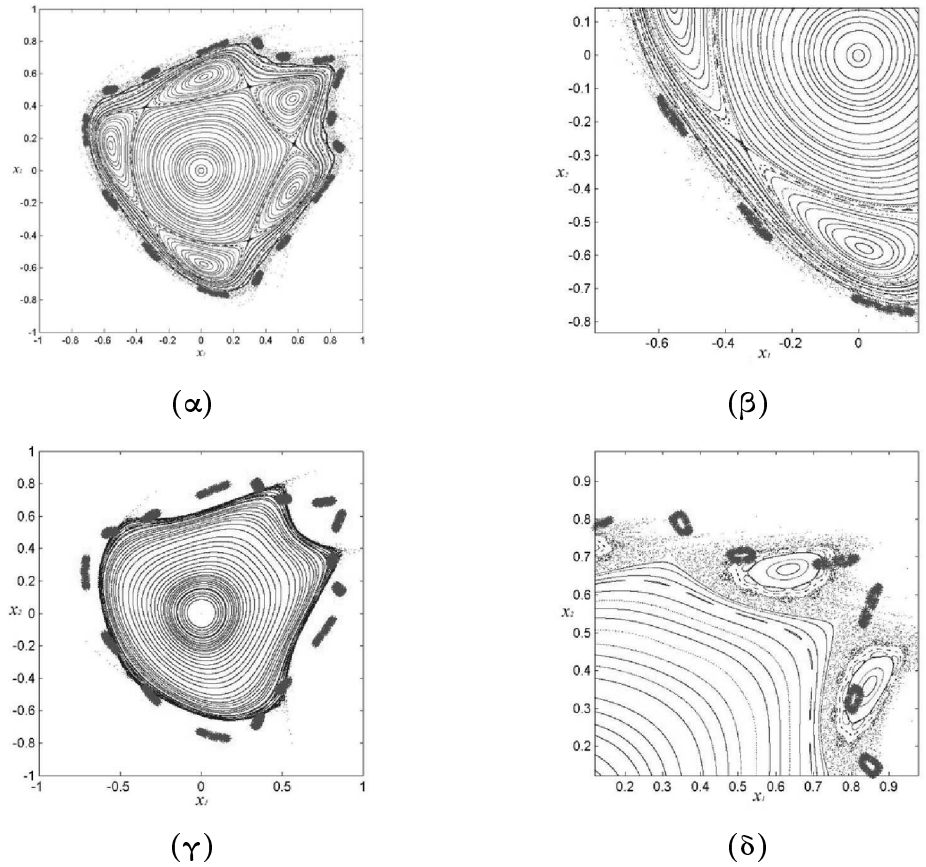
Αναφορικά με τον χρόνο CPU που απαιτείται για την κρυπτογράφηση/αποκρυπτογράφηση των κειμένων χρειάστηκαν μόνο λίγα χιλιοστά του δευτερολέπτου για όλα τα είδη των αρχικών κειμένων, το οποίο ήταν αναμενόμενο καθώς πραγματοποιούνται μόνο μερικές επαναλήψεις της μη γραμμικής απεικόνισης (σημειώνουμε ότι η υλοποίηση δεν ήταν βελτιστοποιημένη για υψηλή απόδοση). Επιπλέον, ο χρόνος CPU που χρειάζεται για τον υπολογισμό του κλειδιού οφείλεται μόνο στον υπολογισμό του αρχικού σταθερού σημείου, καθώς η επιλογή της μη γραμμικής απεικόνισης δεν απαιτεί καθόλου χρόνο. Επιλέγοντας μια κατάλληλη μέθοδο, για παράδειγμα την CHABIS [211], σταθερά σημεία με περίοδο μερικών εκατοντάδων μπορούν να υπολογιστούν σε χρόνο CPU λιγότερο από ένα δευτερόλεπτο σε έναν τυπικό σύγχρονο προσωπικό υπολογιστή.

Αναφορικά με το συνολικό πλήθος μηδενικών και μονάδων που περιέχονται στα κρυπτογραφήματα, τα ποσοστά ήταν περίπου 50% μηδενικά και 50% μονάδες για όλα τα είδη αρχικών κειμένων, δηλαδή τυχαίους χαρακτήρες, κείμενα Αγγλικών και επαναλαμβανόμενους χαρακτήρες. Το αποτέλεσμα αυτό είναι ιδιαίτερα σημαντικό για την ασφάλεια του κρυπτοσυστήματος σε επιθέσεις κρυπτογραφήματος, καθώς τα κρυπτογραφήματα δεν περιέχουν πληροφορίες για πιθανά μοτίβα στα αντίστοιχα αρχικά κείμενα.

Στο Σχήμα 6.2 (α) και (β), απεικονίζονται παραδείγματα πιθανών κλειδιών (μη γραμμικές απεικονίσεις και αρχικά σταθερά σημεία) του προτεινόμενου κρυπτοσυστήματος στο επίπεδο (x_1, x_2). Ακόμα και στην περίπτωση που κάποιος αντίπαλος αποκτήσει γνώση της χρησιμοποιούμενης μη γραμμικής απεικόνισης, η επιλογή λίγο διαφορετικού αρχικού σταθερού σημείου οδηγεί σε μια διαφορετική περιοδική τροχιά (δηλαδή διαφορετικά κρυπτογραφήματα). Επιπλέον, μια συγκεκριμένη περιοδική τροχιά δεν είναι καθόλου χρήσιμη όταν χρησιμοποιηθεί σε διαφορετική απεικόνιση (ακόμα και σε απεικόνιση με τον ίδιο μη γραμμικό όρο αλλά διαφορετική γωνία περιστροφής α). Στο Σχήμα 6.2 (γ) και (δ), η περιοδική τροχιά της εικόνας (α) απεικονίζεται πάνω σε δύο ελαφρά διαφορετικές μη γραμμικές απεικονίσεις. Όπως φαίνεται και στις εικόνες, τα σημεία της αρχικής περιοδικής τροχιάς δεν αποτελούν περιοδική τροχιά για καμία από τις δύο νέες μη γραμμικές απεικονίσεις και, επίσης, ένας αντίπαλος δεν μπορεί να βρει κάποιο σταθερό σημείο των νέων απεικονίσεων χωρίς να έχει κάποια γνώση για αυτές.

6.7 Συμπεράσματα - Συνεισφορά

Στην παραπάνω μελέτη παρουσιάζεται ένα νέο συμμετρικό κρυπτοσύστημα βασισμένο σε περιοδικές τροχιές. Το προτεινόμενο κρυπτοσύστημα αξιοποιεί την ιδέα των μη γραμμικών απεικονίσεων και των σταθερών τους σημείων για κρυπτογράφηση. Συγκεκριμένα, ο αλγόριθμος κρυπτογράφησης δέχεται ως είσοδο μια σειρά χαρακτήρων και δίνει ως έξοδο ένα σύνολο



Σχήμα 6.2: (α) Σταθερά σημεία της διδιάστατης απεικόνισης του Hénon με $\cos\alpha = 0.24$ και $g(x_1) = -x_1^2$, χρησιμοποιούμενα ως κλειδιά του κρυπτοσυστήματος, (β) λεπτομέρεια των κλειδιών που χρησιμοποιούνται στην (α), (γ) κλειδιά της (α) τοποθετημένα στην διδιάστατη απεικόνιση του Hénon με $\cos\alpha = 0.15$ και $g(x_1) = -x_1^2$, (δ) κλειδιά της (α) τοποθετημένα στην διδιάστατη απεικόνιση του Hénon με $\cos\alpha = 0.35$ και $g(x_1) = -x_1^2$.

σταθερών σημείων μιας μη γραμμικής απεικόνισης που καθορίζεται από το κλειδί. Στην μελέτη, εισάγεται και ένα μέτρο αξιολόγησης της ποιότητας των κλειδιών του κρυπτοσυστήματος. Το μέτρο αυτό βασίζεται στην ευαισθησία των σταθερών σημείων μιας περιοδικής τροχιάς σε διαταραχές. Κατά αυτόν τον τρόπο, εφαρμόζοντας τον αλγόριθμο ελέγχου ευστάθειας ελέγχεται αν ένα κλειδί έχει την επιθυμητή ποιότητα.

Η ασφάλεια του προτεινόμενου κρυπτοσυστήματος αποδίδεται κυρίως στην δυσκολία ταξινόμησης των στοιχείων μιας δοθείσης περιοδικής τροχιάς όταν η μη γραμμική απεικόνιση είναι άγνωστη. Οποιουδήποτε είδους επίθεση εξαντλητικής αναζήτησης (brute force) είναι αναποτελεσματική, καθώς μικρές αλλαγές στις παραμέτρους της μη γραμμικής απεικόνισης (για παράδειγμα στην γωνία περιστροφής και στον μη γραμμικό όρο), ή διαταραχές στο αρχικό σταθερό σημείο οδηγούν σε πολύ διαφορετικά αποτελέσματα.

Τα πειραματικά αποτελέσματα δείχνουν ότι το κρυπτοσύστημα είναι αρκετά αποδοτικό καθώς απαιτεί ένα μικρό αριθμό FLOPs για την κρυπτογράφηση / αποκρυπτογράφηση ενός χαρακτήρα και μόνο μερικά χιλιοστά του δευτερολέπτου σε χρόνο CPU για την κρυπτογράφηση και αποκρυπτογράφηση κειμένων με 100.000 χαρακτήρες. Επίσης, η ανάλυση των κρυπτογραφημάτων που προκύπτουν από διαφορετικά είδη αρχικών κειμένων δείχνει ότι καμία πληροφορία μοτίβων δεν μπορεί να προκύψει από τα κρυπτογραφήματα, καθιστώντας έτσι το κρυπτοσύστημα σθεναρό σε επιθέσεις κρυπτογραφημάτων.

Τέλος, στην μελέτη παρουσιάζονται τρεις διαφορετικές τροποποιήσεις της βασικής μορφής του κρυπτοσυστήματος που το καθιστούν περισσότερο αποτελεσματικό σε πολλών ειδών πιθανές επιθέσεις.

Μέρος III

Πρωτόκολλα εξασφάλισης ιδιωτικότητας

ΚΕΦΑΛΑΙΟ 7

Πρωτόκολλα για ασφαλή ηλεκτρονική συγκέντρωση δεδομένων

7.1 Εισαγωγή

Στη σύγχρονη εποχή τόσο οι επιχειρήσεις όσο και οι επιστημονικοί οργανισμοί συγκεντρώνουν πολύ μεγάλο όγκο δεδομένων, τα οποία οργανώνουν σε βάσεις δεδομένων. Η ανάλυση των περιεχομένων αυτών των βάσεων μπορεί να είναι ιδιαίτερα ωφέλιμη, καθώς μπορεί να οδηγήσει σε ανακάλυψη γνώσεων. Για το λόγο αυτό ιδιαίτερη προσπάθεια έχει αφιερωθεί στην ανάπτυξη μεθόδων που συνεισφέρουν στην ανακάλυψη γνώσεων χρησιμοποιώντας τεχνικές εξόρυξης δεδομένων [56]. Οι κανόνες που προκύπτουν από την ανάλυση μιας βάσης δεδομένων εκφράζουν την γνώση που ενυπάρχει στα συγκεκριμένα δεδομένα. Οι κανόνες αυτοί μπορούν να είναι επαρκείς και αποδοτικοί για τις ανάγκες ενός μόνο οργανισμού αλλά πολλοί παράγοντες μπορούν να περιορίζουν την καθολική ισχύ αυτών των κανόνων. Για παράδειγμα, η γνώση που εξάγεται από τη βάση δεδομένων ενός νοσοκομείου μπορεί να περιορίζεται σε ανθρώπους που κατοικούν σε μια σχετικά μικρή γεωγραφική περιοχή, με συγκεκριμένες περιβαλλοντολογικές επιδράσεις, συγκεκριμένες διατροφικές συνήθειες και άλλους περιοριστικούς παράγοντες. Η εφαρμογή τεχνικών ανακάλυψης γνώσης στο σύνολο των βάσεων δεδομένων όλων των οργανισμών που ενεργούν σε συγκεκριμένο πεδίο είναι πιθανό να παράγει πολύ πιο ευρεία γνώση.

Η ανακάλυψη ευρύτερης και ακριβέστερης γνώσης σε πεδία όπως η ιατρική, η εκπαίδευση, η οικονομία, και άλλα, είναι πολύ σημαντική για κάθε οργανισμό μεμονωμένα αλλά και για ολόκληρο το πεδίο. Στην ιδανική περίπτωση, για να εξάγει κάποιος αυτή τη γνώση θα απαιτούσε την συλλογή και ανάλυση των δεδομένων από όλους τους οργανισμούς ενός συγκεκριμένου πεδίου. Ωστόσο, αυτό δεν είναι πάντοτε εφικτό και οι οργανισμοί δεν είναι γενικά πρόθυμοι να εκθέσουν τα δεδομένα τους για λόγους που σχετίζονται κυρίως με θέματα ιδιωτικότητας και εμπιστευτικότητας.

Στην μελέτη αυτή, θεωρούμε την περίπτωση κατά την οποία πολλοί οργανισμοί επιθυμούν να συγκεντρώσουν ηλεκτρονικά όλα τα δεδομένα τους σε μια κοινή βάση, η οποία θα ανακοινωθεί σε όλους τους οργανισμούς. Ωστόσο, τα δεδομένα θα πρέπει να συγκεντρωθούν με κατάλληλο τρόπο έτσι ώστε να μην είναι εφικτό να αποκαλυφθεί ο οργανισμός που αποτέλεσε την πηγή κάθε δεδομένου. Στη συνέχεια του κεφαλαίου, ακολουθώντας την σύμβαση που ευρέως χρησιμοποιείται στην κρυπτογραφία, κάθε οργανισμός θα αναφέρεται ως «Αλίκη». Οι απαιτήσεις ασφαλείας που πρέπει να ικανοποιηθούν από το προτεινόμενο σχήμα για ηλεκτρονική συγκέντρωση δεδομένων με ιδιωτικότητα, είναι οι ακόλουθες.

1. *Πληρότητα:* Όλα τα έγκυρα δεδομένα συγκεντρώνονται σωστά αν όλες οι Αλίκες ακολουθήσουν το πρωτόκολλο.

2. *Ιδιωτικότητα:* Είναι ανέφικτο να συσχετιστούν μεμονωμένες βάσεις με τις Αλίκες.

3. *Νομιμότητα:* Μόνο νόμιμες Αλίκες επιτρέπεται να στείλουν δεδομένα.

4. *Αυθεντικοποίηση:* Κάθε Αλίκη στέλνει έγκυρα δεδομένα.

5. *Επιβεβαίωση:* Κάθε Αλίκη μπορεί να επιβεβαιώσει αν τα δικά της δεδομένα έχουν συμπεριληφθεί σωστά στα συνολικά δεδομένα.

Όλες οι παραπάνω απαιτήσεις με εξαίρεση την τέταρτη, είναι ταυτόσημες με αυτές που χρειάζονται για ασφαλή συστήματα εκλογών σε δημόσιο δίκτυο (για παράδειγμα, βλέπε [20, 27, 39, 64, 186]). Η τέταρτη ιδιότητα της αυθεντικοποίησης των δεδομένων δεν απαιτείται πάντα από τα συστήματα ηλεκτρονικών εκλογών. Επίσης, η απαίτηση που υπάρχει σε κάποια συστήματα ηλεκτρονικών εκλογών για μια μόνο ψήφο ανά ψηφοφόρο δεν είναι απαραίτητη στην περίπτωση της ηλεκτρονικής συγκέντρωσης δεδομένων. Κατά συνέπεια, για να επιτευχθούν οι παραπάνω στόχοι αρκεί να μεταβάλλουμε πρωτόκολλα ηλεκτρονικών εκλογών έτσι ώστε να ικανοποιούν την πρόσθετη απαίτηση της αυθεντικοποίησης των μεταδιδόμενων δεδομένων, χωρίς τον περιορισμό ενός μόνο πακέτου μετάδοσης.

Στο πρώτο προτεινόμενο σχήμα (Ενότητα 7.2) θεωρούμε την ύπαρξη ενός τρίτου μέλους, που ονομάζεται *Συλλέκτης*, και το οποίο είναι υπεύθυνο για την συλλογή των δεδομένων όλων των νόμιμων Αλικών και την διανομή του συνόλου των δεδομένων πίσω στις Αλίκες. Στο δεύτερο προτεινόμενο σχήμα (Ενότητα 7.5), η ασφαλής ηλεκτρονική συγκέντρωση των δεδομένων υλοποιείται χωρίς της ύπαρξη τρίτου μέλους. Και στις δύο περιπτώσεις, τα σχήματα απαιτούν κάποιον που θα επιβεβαιώνει για την εγκυρότητα κάθε καταγεγραμμένου δεδομένου.

Στις επόμενες ενότητες του κεφαλαίου περιγράφουμε αναλυτικά τις δύο προτεινόμενες προσεγγίσεις, δίνοντας επίσης ανάλυση της ασφάλειάς τους καθώς και την υπολογιστική τους πολυπλοκότητα.

7.2 Ηλεκτρονική συγκέντρωση δεδομένων μέσω τροποποίησης πρωτοκόλλων ηλεκτρονικών εκλογών

Η πρώτη προτεινόμενη προσέγγιση για την ηλεκτρονική συγκέντρωση δεδομένων με ιδιωτικότητα, βασίζεται στην τροποποίηση πρόσφατων πρωτοκόλλων ηλεκτρονικών εκλογών. Οι Αλίκες είναι οργανισμοί που ενεργούν σε ένα συγκεκριμένο κοινό πεδίο, όπως για παράδειγμα διαφορετικά νοσοκομεία, φαρμακευτικές εταιρίες, σχολεία, εκπαιδευτικά ιδρύματα, τράπεζες και άλλα. Ο Συλλέκτης μπορεί να είναι είτε μια εθνική αρχή, είτε ένας οργανισμός, ένας διευθυντής οργανισμού ή ακόμα και μια μηχανή. Ο Συλλέκτης διαθέτει μια λίστα με τις ταυτότητες όλων των οργανισμών που θα συμμετέχουν στην ηλεκτρονική συγκέντρωση των δεδομένων.

Κάθε αρχείο δεδομένων σε μια βάση θεωρείται ως ένα διάνυσμα τιμών (αριθμητικών ή κατηγορικών) με την μορφή $\bar{w}_j = (w_{j1}, w_{j2}, \ldots, w_{jm})$. Κάθε Αλίκη πρέπει να στείλει όλα τα αρχεία δεδομένων $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_k$ σε όλες τις άλλες Αλίκες μέσω του Συλλέκτη.

Κάθε αρχείο δεδομένων $\bar{w}_j$ πρέπει να συνοδεύεται από μια ψηφιακή υπογραφή που θα επιβεβαιώνει την εγκυρότητά του. Αυτή η ψηφιακή υπογραφή πρέπει να προέρχεται από έναν ειδικό στο πεδίο, για παράδειγμα, έναν γιατρό για ιατρικά δεδομένα ή έναν διευθυντή τραπέζης για οικονομικά δεδομένα, και θα καλείται *Ειδικός*. Κάθε Αλίκη, σαν οργανισμός, μπορεί να χρησιμοποιήσει έναν ή περισσότερους Ειδικούς. Η ψηφιακή υπογραφή του Ειδικού υλοποιείται χρησιμοποιώντας μια συνάρτηση hash H. Το αρχείο δεδομένων $\bar{w}_j$ υπογράφεται ως

$$Sign_{EU}(\bar{w}_j) = D_{EU}(H(\bar{w}_j)),$$

όπου D_{EU} είναι το ιδιωτικό κλειδί της ένωσης των Ειδικών (κοινό για κάθε Ειδικό) και το $Sign_{EU}$ συμβολίζει την κοινή υπογραφή όλων των Ειδικών. Συνεπώς, ο Ειδικός δημιουργεί τα ζεύγη,

$$[\bar{w}_j, Sign_{EU}(\bar{w}_j)] = A_j,$$

για όλα τα αρχεία του και τα δίνει στην Αλίκη, κρατώντας ένα αντίγραφο ασφαλείας. Η Αλίκη επιβεβαιώνει την υπογραφή της ένωσης των Ειδικών σε κάθε αρχείο δεδομένων και στη συνέχεια υπογράφει για τον Ειδικό το πλήθος των συνολικών αρχείων δεδομένων, που συμβολίζεται ως nor, που της παρέδωσε. Ο Ειδικός επιβεβαιώνει την υπογραφή της Αλίκης στο πλήθος nor.

Όταν ο Ειδικός ολοκληρώσει αυτή τη διαδικασία, στέλνει στον Συλλέκτη ένα μήνυμα που περιέχει,

(α) το πλήθος nor των αρχείων δεδομένων,

(β) την υπογραφή της Αλίκης στο πλήθος nor, και

(γ) την υπογραφή της ένωσης Ειδικών στο πλήθος nor, δηλαδή, μια τριάδα της μορφής,

$$[nor, Sign_A(nor), Sign_{EU}(nor)].$$

Ο Συλλέκτης επιβεβαιώνει την υπογραφή της ένωσης Ειδικών σε κάθε τριάδα και εξάγει από τις τριάδες το συνολικό πλήθος αρχείων δεδομένων που πρέπει να συγκεντρώσει. Ο Συλλέκτης θέτει μια χρονική προθεσμία για την παραλαβή όλων των δεδομένων και επίσης επιλέγει ένα ζεύγος (D_0, E_0) ιδιωτικού και δημοσίου κλειδιού, ανακοινώνοντας το E_0 σε όλες τις Αλίκες. Το δημόσιο κλειδί E_0 χρησιμοποιείται από κάθε Αλίκη για την κρυπτογράφηση όλων των πακέτων A_j σε $z_j = E_0(A_j)$. Στη συνέχεια, κάθε Αλίκη «τυφλώνει» το z_j ως εξής

$$e_j = Blind(z_j, r_j),$$

όπου το r_j είναι ένας τυχαία επιλεγμένος παράγοντας τύφλωσης [28]. Η Αλίκη επίσης υπογράφει τα e_j ως $Sign_A(e_j)$ χρησιμοποιώντας την υπογραφή της. Η τριάδα $[Id_A, e_j, Sign_A(e_j)]$, που περιέχει την ταυτότητα της Αλίκης, τα τυφλά δεδομένα της, και την υπογραφή της, αποστέλλεται από την Αλίκη στον Συλλέκτη. Ο Συλλέκτης επιβεβαιώνει την ταυτότητα της Αλίκης και την υπογραφή της και ελέγχει αν η Αλίκη είναι καταγεγραμμένη στη λίστα των συμμετεχόντων οργανισμών. Αν αυτό ισχύει, υπογράφει τα e_j ως $Sign_C(e_j)$ και τα στέλνει πίσω στην Αλίκη.

Η Αλίκη επιβεβαιώνει την υπογραφή του Συλλέκτη πάνω στα αρχεία δεδομένων της, επαναφέρει τα τυφλά αρχεία $Sign_C(e_j)$, λαμβάνοντας με τον τρόπο αυτό την υπογραφή του Συλλέκτη στα αρχεία z_j, δηλαδή τα $Sign_C(z_j)$. Όλα τα ζεύγη $[z_j, Sign_C(z_j)]$ των υπογεγραμμένων αρχείων δεδομένων αποστέλλονται χωριστά στον Συλλέκτη μέσω ενός *ανώνυμου καναλιού* [1,27,149,152]. Ο Συλλέκτης επιβεβαιώνει την υπογραφή του και λαμβάνει τα z_j ως έγκυρα αρχεία δεδομένων.

Μόλις η χρονική προθεσμία που έχει θέσει ο Συλλέκτης λήξει και όλες οι Αλίκες έχουν στείλει τα δεδομένα τους, ο Συλλέκτης θέτει το σύνολο των κρυπτογραφημένων αρχείων δεδομένων μαζί με την υπογραφή του σε αυτά, σε μια λίστα ως ζεύγη

$$[z_j, Sign_C(z_j)],$$

και τα ανακοινώνει σε όλες τις Αλίκες.

Κάθε Αλίκη επιβεβαιώνει ότι τα δεδομένα της έχουν συμπεριληφθεί σωστά στη λίστα από τα z_j που προήλθαν από την ίδια. Τέλος, ο Συλλέκτης ανακοινώνει το ιδιωτικό του κλειδί D_0 σε όλες τις Αλίκες. Οι Αλίκες αποκρυπτογραφούν όλα τα z_j λαμβάνοντας έτσι όλα τα αρχεία δεδομένων A_j. Στη συνέχεια, επιβεβαιώνουν κάθε αρχείο A_j από την υπογραφή της ένωσης Ειδικών και καθαρίζουν τα δεδομένα απομακρύνοντας από τη λίστα τα μη επιβεβαιωμένα δεδομένα αν υπάρχουν. Από τα επιβεβαιωμένα αρχεία A_j, οι Αλίκες ανακτούν τα $\bar{w}_j$ και ξεκινούν την επεξεργασία των δεδομένων.

Η διαδικασία του προτεινόμενου σχήματος με Συλλέκτη μπορεί να συνοψιστεί στα ακόλουθα βήματα.

- **1η Φάση:** Αρχικοποίηση και Επιβεβαίωση του Ειδικού

(α) Ο Συλλέκτης ανακοινώνει τη χρονική προθεσμία για την παραλαβή όλων των δεδομένων και ένα δημόσιο κλειδί E_0.

(β) Κάθε Ειδικός υπογράφει με την υπογραφή της ένωσης Ειδικών κάθε έγκυρο αρχείο δεδομένων και το παραδίδει στην αντίστοιχη Αλίκη. Η Αλίκη επιβεβαιώνει την υπογραφή της ένωσης Ειδικών σε κάθε αρχείο και υπογράφει το πλήθος nor των αρχείων για τον Ειδικό. Οι Ειδικοί επιβεβαιώνουν την υπογραφή της Αλίκης στο nor.

(γ) Ο Ειδικός στέλνει στον Συλλέκτη το ακριβές πλήθος των αρχείων nor που έχει υπογράψει για την Αλίκη, μαζί με την υπογραφή της και την υπογραφή της ένωσης Ειδικών στο πλήθος nor. Ο Συλλέκτης επιβεβαιώνει την υπογραφή της ένωσης Ειδικών στα nor και τα αποδέχεται.

(δ) Κάθε Αλίκη κρυπτογραφεί τα ζεύγη των αρχείων με τις αντίστοιχες υπογραφές, χρησιμοποιώντας το δημόσιο κλειδί E_0.

- **2η Φάση:** Τυφλή Υπογραφή και Συλλογή Δεδομένων (για κάθε Αλίκη)

(ε) Η Αλίκη τυφλώνει τα κρυπτογραφημένα αρχεία δεδομένων, τα υπογράφει χρησιμοποιώντας το ιδιωτικό της κλειδί, και τα στέλνει μαζί με την ταυτότητά της στον Συλλέκτη.

(στ) Ο Συλλέκτης επιβεβαιώνει την υπογραφή της Αλίκης και την ταυτότητά της και αποδέχεται το πακέτο.

(ζ) Ο Συλλέκτης υπογράφει τα αρχεία δεδομένων και τα στέλνει πίσω στην Αλίκη.

(η) Η Αλίκη επιβεβαιώνει την υπογραφή του Συλλέκτη, επαναφέρει τα τυφλά αρχεία και τα στέλνει πίσω στον Συλλέκτη με τη μορφή χωριστών αρχείων μέσω ενός ανώνυμου καναλιού.

(θ) Ο Συλλέκτης επιβεβαιώνει την υπογραφή του στα κρυπτογραφημένα αρχεία δεδομένων και τα αποδέχεται.

- **3η Φάση:** Διανομή Δεδομένων και Επιβεβαίωση

(ι) Μετά τη λήξη της προθεσμίας και την παραλαβή όλων των δεδομένων, ο Συλλέκτης δημιουργεί μια λίστα με όλα τα κρυπτογραφημένα δεδομένα και την υπογραφή του σε αυτά, και τα στέλνει σε όλες τις Αλίκες.

(κ) Κάθε Αλίκη επιβεβαιώνει ότι τα αρχεία δεδομένων της συμπεριλαμβάνονται σωστά στη λίστα.

- **4η Φάση:** Αποκάλυψη Κλειδιών και Καθαρισμός Δεδομένων

(λ) Ο Συλλέκτης φανερώνει το ιδιωτικό του κλειδί σε όλες τις Αλίκες.

(μ) Κάθε Αλίκη αποκρυπτογραφεί όλα τα αρχεία δεδομένα, κρατώντας μόνο τα έγκυρα. Όλα τα έγκυρα αρχεία δεδομένων είναι διαθέσιμα σε όλες τις Αλίκες.

7.3 Ανάλυση ασφάλειας του προτεινόμενου σχήματος με Συλλέκτη

Στην παρούσα ενότητα, αναλύεται η ασφάλεια του πρώτου προτεινόμενου σχήματος θεωρώντας διάφορες πιθανές επιθέσεις. Συγκεκριμένα, εξετάζονται οι ακόλουθες περιπτώσεις.

Η Αλίκη ως Ενεργός Διαφθορέας:

(1) Υποθέτουμε ότι μια Αλίκη σκοπεύει να εξαπατήσει τις υπόλοιπες Αλίκες με στόχο να λάβει τα δεδομένα τους χωρίς να αποστείλει τα δικά της δεδομένα. Στην περίπτωση αυτή, ο Συλλέκτης μπορεί να αποδείξει ποια Αλίκη δεν έχει στείλει δεδομένα ελέγχοντας την λίστα των συμμετεχόντων και τις αντίστοιχες ταυτότητες Id_A που λαμβάνει στο Βήμα (στ). Κατ΄ αυτό τον τρόπο, μπορεί να ζητήσει από την Αλίκη να του παρέχει την υπογραφή του $Sign_C(e_j)$. Σημειώνεται ότι η Αλίκη δεν μπορεί να πλαστογραφήσει την υπογραφή του.

(2) Υποθέτουμε ότι μια Αλίκη στέλνει τα δεδομένα της στο Βήμα (ε), λαμβάνει την υπογραφή του Συλλέκτη αλλά δεν επιστρέφει τα δεδομένα πίσω στον Συλλέκτη στο Βήμα (η). Μετά την λήξη της προθεσμίας ο Συλλέκτης ελέγχει τα πακέτα της μορφής,

$$[nor, Sign_A(nor), Sign_{EU}(nor)],$$

που έχει λάβει από τους Ειδικούς, και υπολογίζει το άθροισμα,

$$s = \sum_A nor.$$

Έπειτα, το s, που είναι το πλήθος των αναμενόμενων αρχείων δεδομένων, συγκρίνεται με το πλήθος των ληφθέντων αρχείων δεδομένων μέσω του ανώνυμου καναλιού. Αν οι αριθμοί δεν συμφωνούν, δεν φανερώνει το ιδιωτικό του κλειδί και ανακοινώνει σε όλες τις Αλίκες την παραβίαση των κανονισμών και τον ακριβή αριθμό αρχείων που δεν έχουν αποσταλεί. Ο Συλλέκτης ανακοινώνει μια τελική προθεσμία για την λήψη όλων των υπολοίπων δεδομένων. Αν ο συνολικός αριθμός των αρχείων δεδομένων δεν αποσταλεί μέσα στην νέα προθεσμία, τότε η Αλίκη διαφθορέας μπορεί να αποκαλυφθεί από τους Ειδικούς. Η ίδια περίπτωση ισχύει αν η Αλίκη δεν στείλει όλα τα αρχεία δεδομένων της.

(3) Υποθέτουμε ότι η Αλίκη στέλνει μη έγκυρα αρχεία δεδομένων στο Βήμα (η) με στόχο να παραπλανήσει τις άλλες Αλίκες. Τα αρχεία αυτά δεν θα είναι υπογεγραμμένα από τον Ειδικό (μόνο έγκυρα αρχεία δεδομένων υπογράφονται από τον Ειδικό στο Βήμα (β)), και συνεπώς, τα αρχεία δεν θα επιβεβαιωθούν στο τελευταίο βήμα. Τα μη έγκυρα δεδομένα θα καθαριστούν από τη λίστα των δεδομένων. Επιπλέον, η Αλίκη διαφθορέας μπορεί να αποκαλυφθεί άμεσα από τους Ειδικούς. Κατ΄ αυτό τον τρόπο το κριτήριο αυθεντικοποίησης των δεδομένων ικανοποιείται.

(4) Στο Βήμα (δ) η Αλίκη κρυπτογραφεί τα αρχεία της χρησιμοποιώντας το δημόσιο κλειδί του Συλλέκτη. Τα συνήθη κρυπτοσυστήματα για ηλεκτρονικές εκλογές βασίζονται στο κρυπτοσύστημα El Gamal. Για το κρυπτοσύστημα αυτό, η κρυπτογράφηση του $\bar{w}_j$ είναι

$$(g^k \bmod p, E_0^k(\bar{w}_j) \bmod p),$$

όπου το k είναι ένα τυχαίο κλειδί, το p είναι ένας πρώτος αριθμός, και το g είναι γεννήτορας του $\mathbb{Z}_p^*$. Συνεπώς, αν υποθέσουμε ότι μια Αλίκη ή ένας εισβολέας θέλει να εξάγει το ιδιωτικό κλειδί D_0 του Συλλέκτη, θα πρέπει να επιλύσει την εξίσωση,

$$E_0 = g^{D_0} \bmod p,$$

το οποίο είναι ισοδύναμο με την επίλυση του προβλήματος του διακριτού λογαρίθμου. Αν θέλει να αποκρυπτογραφήσει ένα συγκεκριμένο μήνυμα που έχει κρυπτογραφηθεί από κάποια Αλίκη, θα πρέπει να εξάγει το

$$E_0^k = g^{D_0 k} \bmod p,$$

από τις ποσότητες,

$$E_0 = g^{D_0} \bmod p, \quad \text{και} \quad g^k \bmod p.$$

Η επίλυση αυτού του προβλήματος είναι τόσο δύσκολο όσο η επίλυση του προβλήματος Diffie-Hellman [46].

Ο Συλλέκτης ως Παθητικός Διαφθορέας:

Είναι ανέφικτο για τον Συλλέκτη ή για κάποιον εισβολέα να συσχετίσει μεμονωμένα αρχεία δεδομένων με την αντίστοιχη Αλίκη που τα παρείχε στο Βήμα (στ), καθώς κάθε κρυπτογραφημένο αρχείο έχει γίνει τυφλό από την Αλίκη. Είναι επίσης ανέφικτο για τον Συλλέκτη να εντοπίσει την πηγή των δεδομένων κατά το Βήμα (η) καθώς τα λαμβάνει μεμονωμένα μέσω ανώνυμου καναλιού. Συνεπώς, η ασφάλεια των δεδομένων έχει εξασφαλιστεί.

Ο Συλλέκτης ως Ενεργός Διαφθορέας:

(1) Η επικοινωνία στα Βήματα (ε) και (ζ) γίνεται με υπογεγραμμένη αποστολή από τον αποστολέα και συνεπώς ο αποστολέας δεν μπορεί να εξαπατήσει τον παραλήπτη. Συγκεκριμένα, στο Βήμα (ζ), ας υποθέσουμε ότι ο Συλλέκτης προσπαθεί να εξαπατήσει την Αλίκη στέλνοντάς της υπογεγραμμένο αλλά λάθος πακέτο δεδομένων, $Sign_C(e'_j)$. Τότε, στο Βήμα (η) δεν θα γίνει η επιβεβαίωση της υπογραφής του Συλλέκτη στα δεδομένα της Αλίκης και η Αλίκη μπορεί να αποδείξει την απάτη.

(2) Κατά την φάση της επιβεβαίωσης, το ιδιωτικό κλειδί του Συλλέκτη δεν αποκαλύπτεται μέχρι κάθε Αλίκη να επιβεβαιώσει ότι τα δεδομένα της έχουν συμπεριληφθεί σωστά στην λίστα. Αν τα δεδομένα z_i της Αλίκης δεν συμπεριλαμβάνονται στην λίστα τότε η Αλίκη μπορεί να υποχρεώσει τον Συλλέκτη να υπογράψει ξανά όλα τα δεδομένα της λίστας. Δημοσιεύοντας μέσω ανώνυμου καναλιού την υπογραφή του Συλλέκτη στα δικά της κρυπτογραφημένα δεδομένα, $Sign_C(z_i)$, που πραγματοποιείται στο Βήμα (η), μπορεί να αποδείξει ότι για κάθε υπογεγραμμένο αρχείο δεδομένων $Sign_C(z_j)$ της λίστας, ισχύει ότι $Sign_C(z_j) \neq Sign_C(z_i)$. Κατά τον ίδιο τρόπο, αν έχουν αλλοιωθεί τα δεδομένα της Αλίκης στην λίστα, μπορεί να ανακοινώσει μέσω ανώνυμου καναλιού την αλλοίωση των δεδομένων της, και να επιβεβαιώσει το γεγονός αυτό δημοσιεύοντας τα κρυπτογραφημένα δεδομένα της με την υπογραφή του Συλλέκτη, $[z_i, Sign_C(z_i)]$, που λαμβάνει κατά το Βήμα (ζ). Για τις υπόλοιπες Αλίκες είναι πολύ εύκολο να ελέγξουν αν

$$[z_i, Sign_C(z_i)] \neq [z_j, Sign_C(z_j)],$$

για όλα τα i αρχεία δεδομένων της Αλίκης και όλα τα j αρχεία της λίστας. Κατ' αυτό τον τρόπο εξασφαλίζεται η απαίτηση της επιβεβαίωσης.

(3) Ο Συλλέκτης μπορεί να προσπαθήσει να παραπλανήσει τις Αλίκες προσθέτοντας μη έγκυρα δεδομένα στην λίστα δεδομένων. Ωστόσο, οι Αλίκες μπορούν να αναγνωρίσουν τα μη έγκυρα δεδομένα καθώς δεν θα έχουν την υπογραφή των Ειδικών και αυτά θα καθαριστούν από την λίστα στη φάση της επιβεβαίωσης.

7.4 Θέματα πολυπλοκότητας του σχήματος με Συλλέκτη

Για τον υπολογισμό της πολυπλοκότητας του προτεινόμενου σχήματος για ηλεκτρονική συγκέντρωση δεδομένων με Συλλέκτη, θεωρούμε ως μέτρο το πλήθος των απαιτούμενων

1. κρυπτογραφήσεων και αποκρυπτογραφήσεων,

2. υπογραφών και επιβεβαιώσεων,

3. αποστολών,

4. τυφλώσεων και επαναφορών.

Υποθέτουμε ότι κάθε μια από τις παραπάνω λειτουργίες έχει υπολογιστικό κόστος ίσο με ένα.

Έστω ότι το πλήθος όλων των Ειδικών είναι e, n είναι όλες οι Αλίκες και $\sum_A nor$ είναι το άθροισμα όλων των αρχείων δεδομένων που θα συγκεντρωθούν μέσω της διαδικασίας. Τότε, το υπολογιστικό κόστος για κάθε βήμα του προτεινόμενου σχήματος, όπως περιγράφεται στην ενότητα 7.2, είναι

1η: (α) μηδέν,

1η: (β) το πολύ $2\sum_A nor$ υπογραφές και $2\sum_A nor$ επιβεβαιώσεις,

1η: (γ) e υπογραφές + e αποστολές + e επιβεβαιώσεις,

1η: (δ) $\sum_A nor$ κρυπτογραφήσεις,

2η: (ε) $\sum_A nor$ τυφλώσεις + $\sum_A nor$ υπογραφές + $\sum_A nor$ αποστολές,

2η: (στ) $\sum_A nor$ επιβεβαιώσεις,

2η: (ζ) $\sum_A nor$ υπογραφές + $\sum_A nor$ αποστολές,

2η: (η) $\sum_A nor$ επιβεβαιώσεις + $\sum_A nor$ επαναφορές + $f(\sum_A nor, k)$,

2η: (θ) $\sum_A nor$ επιβεβαιώσεις,

3η: (ι) n αποστολές,

3η: (κ) μηδέν,

4η: (λ) n αποστολές,

4η: (μ) $\sum_A nor$ αποκρυπτογραφήσεις.

Συνεπώς, το υπολογιστικό κόστος του σχήματος είναι

$$\mathcal{K} = 15\sum_A nor + 3e + 2n + f\left(\sum_A nor, k\right),$$

όπου οι τρεις πρώτοι παράγοντες μετρούν το υπολογιστικό κόστος της διαδικασίας συγκέντρωσης, ενώ ο όρος $f(\sum_A nor, k)$ είναι το υπολογιστικό κόστος για την χρήση ενός ανώνυμου καναλιού επικοινωνίας με k μείκτες.

Το ανώνυμο κανάλι με k MIXes αρχικά προτάθηκε από τον Chaum στην εργασία [27]. Το υπολογιστικό του κόστος για m αποστολείς και έναν μόνο παραλήπτη, υπολογίζεται ότι είναι

$$z = 3m \times (k+1).$$

Βελτιώσεις για το πρωτόκολλο του Chaum για ανώνυμα κανάλια με k MIXes έχουν προταθεί στις εργασίες [149, 152]. Η υπολογιστική πολυπλοκότητα που σχετίζεται με τη χρήση αυτών των πρωτοκόλλων είναι της ίδιας τάξης.

Στο προτεινόμενο σχήμα, χρησιμοποιείται ένα ανώνυμο κανάλι για n Αλίκες (αποστολείς) με $\sum_A nor$ αρχεία και έναν μόνο παραλήπτη, τον Συλλέκτη. Στην περίπτωση αυτή, το m

αντιστοιχεί στην ποσότητα $\sum_A nor$, καθώς όλα τα αρχεία αποστέλλονται μεμονωμένα. Κατά συνέπεια, το z σε αυτή την περίπτωση είναι

$$z^* = f\Big(\sum_A nor, k\Big) = 3\sum_A nor \times (k+1).$$

Συνδυάζοντας τα προηγούμενα αποτελέσματα προκύπτει ότι το υπολογιστικό κόστος του σχήματος είναι, το πολύ,

$$\mathcal{K}_{total} = 15\sum_A nor + 3e + 2n + \Big(3\sum_A nor \times (k+1)\Big).$$

Το κόστος αυτό μπορεί να μειωθεί σημαντικά αν χρησιμοποιηθεί μια κατάλληλη ομαδοποίηση των αρχείων για τις επικοινωνίες. Ο όρος κατάλληλη ομαδοποίηση αναφέρεται σε ομαδοποίηση που προφυλάσσει την ιδιωτικότητα των δεδομένων. Η ασφαλής ομαδοποίηση μπορεί να χρησιμοποιηθεί και στις απλές αποστολές στα Βήματα (ε) και (ζ), μειώνοντας ακόμα περισσότερο το συνολικό κόστος του σχήματος. Τέλος σημειώνεται ότι το πλήθος e των Ειδικών δεν μπορεί να ξεπερνά το πλήθος των αρχείων $\sum_A nor$.

7.5 Ηλεκτρονική συγκέντρωση δεδομένων χωρίς Συλλέκτη

Στην παρούσα ενότητα παρουσιάζουμε αναλυτικά την δεύτερη προτεινόμενη προσέγγιση για ασφαλή ηλεκτρονική συγκέντρωση δεδομένων, στην οποία δεν απαιτείται η χρήση τρίτου μέλους ως Συλλέκτη. Η προσέγγιση αυτή βασίζεται επίσης στα πρωτόκολλα ηλεκτρονικών εκλογών, αλλά συγκεκριμένα σε μια ειδική κατηγορία αυτών όπου δεν είναι απαραίτητη η χρήση κάλπης. Για λόγους πληρότητας, στην υποενότητα που ακολουθεί περιγράφεται ένα πρωτόκολλο ηλεκτρονικών εκλογών χωρίς κάλπη και στην συνέχεια δίνεται αναλυτικά το δεύτερο προτεινόμενο σχήμα για την ηλεκτρονική συγκέντρωση δεδομένων.

7.5.1 Πρωτόκολλο ηλεκτρονικών εκλογών χωρίς κάλπη

Στη σύγχρονη εποχή, η μελέτη των ηλεκτρονικών ψηφοφοριών είναι αρκετά διαδεδομένη, καθώς ο παραδοσιακός τρόπος εκλογών χαρακτηρίζεται από διάφορα μειονεκτήματα. Οι κλασικές εκλογές αποτελούν μια χρονοβόρα διαδικασία, που απαιτεί πολύ εργασία για την σωστή διεξαγωγή της και την ορθή καταμέτρηση των αποτελεσμάτων, αλλά συγχρόνως απαιτεί μεταξύ άλλων και την μετακίνηση των ψηφοφόρων σε εκλογικά κέντρα. Για τους λόγους αυτούς, έχουν προταθεί πολλά πρωτόκολλα ασφαλών ηλεκτρονικών εκλογών [25, 39, 79, 186]. Τα περισσότερα από τα πρωτόκολλα αυτά χρησιμοποιούν τουλάχιστον μια κεντρική υπηρεσία ορθής συλλογής και ανακοίνωσης αποτελεσμάτων (Central Tabulating Facility). Ένα πρωτόκολλο ηλεκτρονικών εκλογών χωρίς κεντρική υπηρεσία, όπου οι ψηφοφόροι έχουν τον έλεγχο των εκλογών, σχεδιάστηκε από τους Merritt et al. [43, 44] και περιγράφεται στη συνέχεια.

Υποθέτουμε ότι κάθε ψηφοφόρος, i, όπου $i = 1, 2, \ldots, N$, έχει ένα δημόσιο και ένα ιδιωτικό κλειδί, και κάθε ψηφοφόρος γνωρίζει το δημόσιο κλειδί των υπολοίπων.

(1) Κάθε ψηφοφόρος επιλέγει την ψήφο του και ακολουθεί την εξής διαδικασία [185].

   (α) Προσαρμόζει μια τυχαία σειρά αλφαριθμητικών χαρακτήρων, R_0, στην ψήφο του, V.

   (β) Κρυπτογραφεί διαδοχικά την ψήφο του μαζί με το R_0, χρησιμοποιώντας τα δημόσια κλειδιά των ψηφοφόρων 1 έως N, με αυτή τη σειρά, παράγοντας το

$$E_N(E_{N-1}(\cdots(E_1(V, R_0))\cdots),$$

όπου το E_j είναι η συνάρτηση κρυπτογράφησης που χρησιμοποιεί το δημόσιο κλειδί του j-οστού ψηφοφόρου.

(γ) Επαναλαμβάνει το βήμα (β), περιλαμβάνοντας αυτή τη φορά μια τυχαία αλφαριθμητική σειρά σε κάθε επίπεδο κρυπτογράφησης. Κατ΄ αυτόν τον τρόπο, στο σημείο αυτό η ψήφος γίνεται

$$E_N(R_N, E_{N-1}(\cdots(R_2, E_1(R_1, E_N(E_{N-1}(\cdots(E_1(V, R_0))\cdots))))\cdots)),$$

όπου R_i, $i = 1, \ldots, N$, είναι τυχαίες αλφαριθμητικές σειρές. Ο ψηφοφόρος αποθηκεύει τα ενδιάμεσα αποτελέσματα μετά από κάθε διαδοχική κρυπτογράφηση. Τα αποτελέσματα αυτά θα χρησιμοποιηθούν αργότερα στο πρωτόκολλο για να επιβεβαιωθεί ότι η ψήφος του περιλαμβάνεται μεταξύ των καταμετρημένων ψήφων.

(2) Κάθε ψηφοφόρος στέλνει το κρυπτογραφημένο μήνυμά του στον N-οστό ψηφοφόρο. Αυτός αποκρυπτογραφεί όλες τις ψήφους με το δικό του ιδιωτικό κλειδί και αφαιρεί την τυχαία σειρά σε αυτό το επίπεδο. Έπειτα, ανακατεύει την σειρά όλων των ψήφων και στέλνει το αποτέλεσμα στον $N-1$ ψηφοφόρο. Η ίδια διαδικασία επαναλαμβάνεται για όλους τους ψηφοφόρους από τον N-οστό μέχρι τον 1. Συνεπώς, μόνο οι εσωτερικές κρυπτογραφήσεις παραμένουν και κάθε ψήφος έχει την εξής μορφή: $E_N(E_{N-1}(\cdots(E_1(V, R_0))\cdots)$.

(3) Ακολούθως, ο N-οστός ψηφοφόρος αποκρυπτογραφεί όλες τις ψήφους με το ιδιωτικό του κλειδί, επιβεβαιώνει ότι η ψήφος του βρίσκεται μεταξύ του συνόλου των ψήφων, υπογράφει όλες τις ψήφους και στέλνει τα αποτελέσματα σε όλους τους άλλους ψηφοφόρους. Ο $N-1$ ψηφοφόρος επιβεβαιώνει και διαγράφει την υπογραφή του N-οστού ψηφοφόρου. Επιβεβαιώνει ότι η ψήφος του βρίσκεται μεταξύ των ψήφων, υπογράφει τις ψήφους και τις στέλνει σε όλους τους άλλους ψηφοφόρους. Η ίδια διαδικασία επαναλαμβάνεται από όλους τους ψηφοφόρους από τον N-οστό μέχρι τον 1. Κατά τη διάρκεια αυτού του βήματος οι ψήφοι έχουν την μορφή: $\mathrm{Sign}_{i+1}(E_i \cdots (E_1(V, R_0))\cdots)$, όπου Sign_i είναι η υπογραφή του i-οστού ψηφοφόρου.

(4) Όλοι οι ψηφοφόροι επιβεβαιώνουν την υπογραφή του 1-ου ψηφοφόρου, και ότι η ψήφος τους βρίσκεται μεταξύ του συνόλου των ψήφων ελέγχοντας για την δική τους τυχαία αλφαριθμητική σειρά μεταξύ των ψήφων. Έπειτα, όλοι αφαιρούν τις τυχαίες σειρές από κάθε ψήφο και παράγουν το αποτέλεσμα της ψηφοφορίας.

Το παραπάνω πρωτόκολλο δουλεύει και η ορθότητα του αποτελέσματός του αποδεικνύεται από την ίδια την διαδικασία. Ο αριθμός των ψηφοφόρων παραμένει σταθερός κατά την διάρκεια της διαδικασίας, συνεπώς η αύξηση των ψήφων ή η μείωσή τους μπορεί να εντοπισθεί εύκολα. Οι ψήφοι δεν μπορούν να αντικατασταθούν από κάποιον διαφθορέα, καθώς οποιαδήποτε προσπάθεια αντικατάστασης μπορεί να ανακαλυφθεί [185]. Το ανακάτεμα των ψήφων παρέχει ανωνυμία και η εσωτερική σειρά, R_0, επιτρέπει στους συμμετέχοντες να επιβεβαιώσουν ότι η ψήφος τους βρίσκεται στην τελική καταμέτρηση. Ωστόσο, το παραπάνω σχήμα παρουσιάζει τρία προβλήματα. Το πρώτο και το πιο σημαντικό είναι ότι απαιτεί τεράστιο αριθμό υπολογισμών. Η πολυπλοκότητά του περιορίζει την πρακτική εφαρμογή του σε ένα μικρό αριθμό ατόμων και δεν θα μπορούσε να χρησιμοποιηθεί σε πραγματική ψηφοφορία [185]. Το δεύτερο μειονέκτημά του είναι ότι ο 1-ος ψηφοφόρος μαθαίνει το αποτέλεσμα της εκλογής πριν από οποιονδήποτε άλλο, παρόλο που δεν μπορεί να επηρεάσει το αποτέλεσμα. Το τρίτο πρόβλημα είναι ότι ο N-οστός ψηφοφόρος μπορεί να αντιγράψει την ψήφο όλων των υπολοίπων παρά το γεγονός ότι δεν γνωρίζει το περιεχόμενό τους εκ των προτέρων. Αυτό αποτελεί πρόβλημα αν θεωρήσουμε την περίπτωση ψηφοφορίας τριών ατόμων, καθώς το αποτέλεσμα της ψηφοφορίας θα είναι ίδιο με την ψήφο που έχει αντιγραφεί. Για το λόγο αυτό θα πρέπει να ισχύει ότι $N \geqslant 4$, με N σχετικά μικρό.

7.5.2 Προτεινόμενο σχήμα για ηλεκτρονική συγκέντρωση δεδομένων χωρίς Συλλέκτη

Στην μελέτη αυτή τροποποιούμε το παραπάνω πρωτόκολλο ηλεκτρονικών εκλογών για χρήση στην ηλεκτρονική συγκέντρωση δεδομένων, ως εξής: αρχικά χωρίζουμε τους συμμετέχοντες οργανισμούς σε ομάδες κατάλληλου μεγέθους, έτσι ώστε κάθε ομάδα να αποτελείται από τουλάχιστον τέσσερα μέλη οργανισμούς, και ο συνολικός αριθμός ομάδων να διαιρείται με κάποιον αριθμό διάφορο του 2. Αυτό το σχήμα διαχωρισμού εξασφαλίζει και την ασφάλεια και την απλότητα του πρωτοκόλλου, όπως θα αναλύσουμε στη συνέχεια. Επίσης, αυτός ο διαχωρισμός μπορεί να καλύπτει και άλλα ειδικά κριτήρια, όπως για παράδειγμα τον διαχωρισμό κατά περιοχή.

Όπως περιγράψαμε και στο πρωτόκολλο στην ενότητα 7.5.1, κάθε έγγραφο $\bar{w}_j$ πρέπει να συνοδεύεται από μια ψηφιακή υπογραφή που πιστοποιεί την ισχύ του. Αυτή η ψηφιακή υπογραφή προέρχεται από τον ειδικό με την μορφή D_{EU}, το οποίο είναι το κοινό ιδιωτικό κλειδί της ένωσης ειδικών. Η κοινή υπογραφή όλων των ειδικών συμβολίζεται και πάλι ως Sign_{EU}. Οπότε, κάθε ειδικός δημιουργεί το ζεύγος $[\bar{w}_j, \mathrm{Sign}_{EU}(\bar{w}_j)] = A_j$ για κάθε έγγραφό του, και τα περνά στον αντίστοιχο οργανισμό, κρατώντας ένα δικό του αντίγραφο. Ο οργανισμός υπογράφει για τον ειδικό το πλήθος των εγγράφων, nor, που του έχει στείλει. Όταν κάθε ειδικός ολοκληρώσει την διαδικασία, στέλνει σε όλους τους άλλους, ένα μήνυμα που περιέχει: (α) το πλήθος, nor, των εγγράφων που έχει στείλει στον οργανισμό, (β) την υπογραφή του οργανισμού στο πλήθος, nor και (γ) την υπογραφή της ένωσης ειδικών στο πλήθος nor. Κατ' αυτό τον τρόπο, όλοι οι οργανισμοί γνωρίζουν το σύνολο των εγγραφών που πρέπει να στείλει κάθε οργανισμός, καθώς και το συνολικό πλήθος των εγγραφών.

Σε πρώτο επίπεδο, κάθε οργανισμός ακολουθεί το πρωτόκολλο ηλεκτρονικών εκλογών, όπως περιγράφηκε στην ενότητα 7.5.1, εφαρμόζοντας και τα τέσσερα βήματα. Το βήμα 1 εφαρμόζεται χωριστά σε κάθε ζεύγος A_j του οργανισμού. Συνεπώς, στο βήμα 2, όλοι οι ειδικοί λαμβάνουν το συνολικό πλήθος των κρυπτογραφημένων εγγραφών της ομάδας τους. Αν ο αριθμός των ληφθέντων εγγραφών δεν συμφωνεί με το πλήθος των αναμενόμενων εγγραφών, τότε το πρωτόκολλο διακόπτεται. Στη συνέχεια εφαρμόζονται διαδοχικά τα βήματα 3 και 4. Στο τέλος του πρώτου επιπέδου, το σύνολο όλων των εγγραφών των ομάδων έχουν συγκεντρωθεί ιδιωτικά.

Στο δεύτερο επίπεδο, ένας αντιπρόσωπος από κάθε ομάδα (ή όλη η ομάδα σαν μια μονάδα) είναι υπεύθυνος για την περαιτέρω συγκέντρωση των δεδομένων μεταξύ των διαφορετικών ομάδων. Κάθε ομάδα ανακοινώνει τον αντιπρόσωπό της σε όλους τους άλλους οργανισμούς στέλνοντας ένα μήνυμα με την ταυτότητα του αντιπροσώπου, υπογεγραμμένη από όλα τα μέλη της. Στη συνέχεια καθορίζονται υπερ-ομάδες αποτελούμενες από τους αντιπροσώπους και το ίδιο πρωτόκολλο εφαρμόζεται ξανά. Από αυτό το επίπεδο, το βήμα 1 δεν εφαρμόζεται σε κάθε έγγραφο χωριστά αλλά σε πακέτα εγγράφων προκαθορισμένου μεγέθους, με στόχο την μείωση της πολυπλοκότητας του σχήματος. Ο καθορισμός του κατάλληλου μεγέθους του πακέτου αναλύεται στη συνέχεια. Αν υπάρχουν υπόλοιπα έγγραφα στις υπο-ομάδες, αυτά κρυπτογραφούνται και στέλνονται (ένα προς ένα) μεμονωμένα. Τα βήματα 2 έως 4 εφαρμόζονται διαδοχικά. Η διαδικασία του δεύτερου επιπέδου εφαρμόζεται επαναληπτικά, μέχρι όλα τα έγγραφα όλων των οργανισμών να συγκεντρωθούν μαζί. Η δημιουργημένη βάση δεδομένων ανακοινώνεται δημόσια για όλους τους συμμετέχοντες οργανισμούς. Κάθε οργανισμός μπορεί να βεβαιωθεί για την αυθεντικότητα της βάσης επιβεβαιώνοντας τις υπογραφές των τελευταίων αντιπροσώπων (οι αντιπρόσωποι του πάνω επιπέδου), οι οποίες συνοδεύουν κάθε έγγραφο της βάσης. Η παραπάνω διαδικασίες δίνονται περιληπτικά στα ακόλουθα βήματα:

1η φάση: Διαδικασίες 1ου επιπέδου

(α) Όλοι οι συμμετέχοντες οργανισμοί χωρίζονται σε ομάδες κατάλληλου μεγέθους.

(β) Κάθε ειδικός υπογράφει με την υπογραφή της ένωσης ειδικών κάθε έγκυρο έγγραφο δεδομένων, περνά κάθε υπογεγραμμένο έγγραφο στον αντίστοιχο οργανισμό

και λαμβάνει την υπογραφή του, επιβεβαιώνοντας το πλήθος των εγγράφων που παρείχε.

(γ) Ο ειδικός στέλνει σε όλους τους οργανισμούς τον ακριβή αριθμό, nor, των εγγράφων που υπέγραψε για τον συγκεκριμένο οργανισμό, μαζί με την υπογραφή του, καθώς και την υπογραφή της ένωσης ειδικών στο πλήθος nor.

(δ) Κάθε οργανισμός ακολουθεί τα βήματα 1 έως 4 του πρωτοκόλλου ηλεκτρονικών εκλογών χωρίς κάλπη, παρέχοντας έτσι τα έγγραφά του στην ομάδα του. Στο βήμα 1, ο οργανισμός κρυπτογραφεί χωριστά τα ζεύγη του A_j. Στο τέλος αυτής της φάσης, κάθε ομάδα έχει συγκεντρώσει όλα τα έγγραφα δεδομένων της.

2η φάση: Διαδικασίες 2ου επιπέδου

(ε) Ορίζεται ένας αντιπρόσωπος για κάθε ομάδα.

(στ) Οι αντιπρόσωποι χωρίζονται σε υπερ-ομάδες κατάλληλου μεγέθους.

(ζ) Υπολογίζεται το κατάλληλο μέγεθος πακέτου εγγράφων που θα κατανεμηθεί διαδοχικά μεταξύ των αντιπροσώπων κάθε υπερ-ομάδας και ανακοινώνεται σε κάθε υπερ-ομάδα.

(η) Κάθε αντιπρόσωπος ακολουθεί τα βήματα 1 έως 4 του πρωτοκόλλου ηλεκτρονικών εκλογών χωρίς κάλπη, παρέχοντας τα έγγραφα της δικής του υπο-ομάδας στην υπερ-ομάδα του. Στο βήμα 1, οι αντιπρόσωποι κρυπτογραφούν τα έγγραφα της υπο-ομάδας τους σε πακέτα μεγέθους που καθορίζεται από το βήμα (ζ). Αν υπάρχουν εναπομείναντα έγγραφα, οι αντιπρόσωποι τα κρυπτογραφούν μεμονωμένα και τα στέλνουν μετά τα πακέτα τους.

(θ) Η 2η φάση επαναλαμβάνεται μέχρι όλα τα έγγραφα όλων των οργανισμών να συγκεντρωθούν μαζί.

Οι κανόνες διαχωρισμού των συμμετεχόντων οργανισμών σε ομάδες, όπως αναφέραμε και παραπάνω, επιβάλλονται για λόγους ασφάλειας και απλότητας. Οι αρχικές ομάδες απαιτούν τουλάχιστον 4 μέλη προκειμένου να ξεπεραστεί το πρόβλημα του σχήματος ηλεκτρονικών εκλογών με την αντιγραφή των αρχείων. Ωστόσο, ο αριθμός των μελών κάθε ομάδας δεν θα πρέπει να είναι πολύ μεγάλος, καθώς αυτό θα αύξανε την πολυπλοκότητα της 1ης φάσης. Από το 2ο επίπεδο συγκέντρωσης δεδομένων και πάνω, απαιτείται αριθμός ομάδων διάφορος από 2 προκειμένου να αποκαλύπτεται η πηγή των εγγράφων.

Στις διαδικασίες του 1ου επιπέδου, το σχήμα απαιτεί τα έγγραφα να κρυπτογραφούνται μεμονωμένα από κάθε οργανισμό. Αυτό είναι απαραίτητο για να εξασφαλιστεί ότι καμία γνώση που αφορά στην πηγή προέλευσης οποιουδήποτε αρχείου δε μπορεί να αποκαλυφθεί. Συνεπώς, η ιδιωτικότητα των οργανισμών διατηρείται. Από το 2ο επίπεδο και πάνω, η απαίτηση για μεμονωμένη κρυπτογράφηση δεν είναι απαραίτητη, καθώς όλα τα έγγραφα των ομάδων έχουν συγκεντρωθεί και κανείς δεν μπορεί πλέον να συνδέσει ένα συγκεκριμένο έγγραφο με την αρχική του πηγή. Επομένως, οι αντιπρόσωποι μπορούν να κρυπτογραφήσουν τα έγγραφα σε πακέτα προκαθορισμένου μεγέθους, τα οποία δεν μπορούν να αναγνωριστούν καθώς ανακατεύονται. Αυτό γίνεται για να μειωθεί η πολυπλοκότητα του προτεινόμενου σχήματος. Το μέγεθος καθορίζεται για κάθε ομάδα από έναν διαφορετικό ακέραιο, m, έτσι ώστε να δημιουργηθεί ένας λογικός αριθμός πακέτων για κάθε μέλος της ομάδας, και είτε όλα τα μέλη της ομάδας να έχουν εναπομείναντα αρχεία, είτε κανένα. Αν υπάρχουν εναπομείναντα αρχεία κρυπτογραφούνται μεμονωμένα. Για παράδειγμα, έστω x_1, x_2, x_3, x_4, ο αριθμός των εγγράφων των τεσσάρων μελών μιας ομάδας, αντίστοιχα. Τότε, ένας ακέραιος m επιλέγεται έτσι ώστε $x_i = \lambda_i m + \mu_i, i = 1, 2, 3, 4$, όπου λ_i είναι ο αριθμός των πακέτων εγγράφων του μέλους i, και είτε όλα τα μ_i είναι ίσα με μηδέν, είτε όλα είναι διάφορα του μηδενός. Το προτεινόμενο σχήμα δεν χρησιμοποιεί ανώνυμα κανάλια επικοινωνίας. Όλες οι μεταδόσεις γίνονται από συγκεκριμένο αποστολέα προς συγκεκριμένο παραλήπτη και είναι αυθεντικοποιημένες. Επιπλέον, δεν

απαιτούνται πρωτόκολλα ψευδώνυμων (identification tags (alias)) ή secret selling secrets, που χρησιμοποιούνται συνήθως από σχήματα ηλεκτρονικών εκλογών.

7.6 Ανάλυση ασφάλειας του προτεινόμενου σχήματος χωρίς Συλλέκτη

Θεωρώντας διάφορες πιθανές επιθέσεις, η ανάλυση ασφαλείας του προτεινόμενου σχήματος μελετάται στη συνέχεια. Σε αντίθεση με τα σχήματα ηλεκτρονικών εκλογών, στην περίπτωση της ηλεκτρονικής συγκέντρωσης δεδομένων οι οργανισμοί έχουν περιορισμένο κίνητρο εξαπάτησης, καθώς οποιαδήποτε διακοπή του πρωτοκόλλου μπορεί να επιφέρει βαριές ποινές στον υπεύθυνο οργανισμό, καθώς και τον τερματισμό της συνεργασίας του με τους υπόλοιπους οργανισμούς. Σε κάθε περίπτωση διακοπής του πρωτοκόλλου καλούνται οι ειδικοί για την αποκάλυψη της υπεύθυνης για τη διακοπή οντότητας.

Οργανισμός ως ενεργός διαφθορέας:

(1) Ας υποθέσουμε ότι ένας οργανισμός σκοπεύει να εξαπατήσει τους άλλους οργανισμούς με σκοπό να δει τα δεδομένα τους χωρίς να στείλει κανένα από τα δικά του δεδομένα, ή στέλνοντας μόνο μέρος αυτών. Στην περίπτωση αυτή, στο βήμα (δ) του 1ου επιπέδου, και συγκεκριμένα στο εσωτερικό βήμα 2 του πρωτοκόλλου εκλογών, το συνολικό πλήθος των αρχείων της αντίστοιχης ομάδας και ο αριθμός των αναμενόμενων εγγράφων δεν θα συμφωνούν. Κατά συνέπεια, η διαδικασία θα τερματιστεί πριν ολοκληρωθεί και ο οργανισμός διαφθορέας δεν θα λάβει τα αποκρυπτογραφημένα δεδομένα της ομάδας.

(2) Ας υποθέσουμε ότι ένας οργανισμός αντιγράφει ένα από τα έγκυρα αρχεία του και το στέλνει πολλές φορές, στη θέση των υπολοίπων αρχείων του, προκειμένου να εξαπατήσει τους υπόλοιπους οργανισμούς. Στην περίπτωση αυτή, στο τέλος του 1ου επιπέδου, θα υπάρχουν πολλά ίδια αρχεία στην ομάδα. Καθώς τα έγκυρα έγγραφα υπογράφονται από την ένωση ειδικών, εξασφαλίζεται ότι δεν υπάρχουν ίδια έγγραφα. Συνεπώς, η διαδικασία θα τερματιστεί. Σημειώνουμε ότι η μοναδικότητα κάθε εγγράφου μπορεί επίσης να εξασφαλιστεί με την επικόλληση ενός τυχαίου αριθμού σε αυτό από τον ειδικό.

(3) Έστω ότι ένας οργανισμός αντιγράφει τα αρχεία ενός άλλου οργανισμού. Τότε στο εσωτερικό βήμα 2 του πρωτοκόλλου εκλογών (δηλαδή στο βήμα (δ) του 1ου επιπέδου), θα υπάρχουν ίδια κρυπτογραφημένα μηνύματα περασμένα στους οργανισμούς. Αυτό δεν είναι επιτρεπτό και η διαδικασία θα τερματιστεί. Επιπλέον, ο διαφθορέας οργανισμός δεν θα λάβει τα αποκρυπτογραφημένα δεδομένα.

(4) Έστω ότι ένας οργανισμός στέλνει μη έγκυρα δεδομένα με σκοπό να παραπλανήσει τους άλλους οργανισμούς. Τότε, στο τέλος του 1ου επιπέδου, θα λείπουν οι υπογραφές της ένωσης ειδικών από τα μη έγκυρα αρχεία οπότε και θα αποκαλυφθούν.

Αντιπρόσωπος ως ενεργός διαφθορέας:

(1) Έστω ότι ένας αντιπρόσωπος σκοπεύει να εξαπατήσει τους άλλους οργανισμούς με σκοπό να δει τα δεδομένα τους χωρίς να αποστείλει τα δικά του δεδομένα ή αποστέλλοντας μέρος των δικών του δεδομένων. Στην περίπτωση αυτή, στο βήμα (η) του 2ου επιπέδου, ο συνολικός αριθμός των αντίστοιχων δεδομένων που λαμβάνουν οι υπερ-ομάδες και ο συνολικός αριθμός των αναμενόμενων δεδομένων δεν θα συμφωνούν. Συνεπώς, η διαδικασία θα τερματιστεί και η ομάδα μπορεί να αποκαλύψει τον διαφθορέα.

(2) Ας υποθέσουμε ότι ένας αντιπρόσωπος αντιγράφει μερικά από τα έγκυρα αρχεία της ομάδας του και τα στέλνει στη θέση των κανονικών αρχείων του, προκειμένου να εξαπατήσει τους υπόλοιπους αντιπροσώπους. Στην περίπτωση αυτή, στο τέλος του 2ου επιπέδου, θα υπάρχουν πολλά ίδια αρχεία και η ομάδα μπορεί να αποκαλύψει τον διαφθορέα.

(3) Αν ένας αντιπρόσωπος αντιγράψει τα αρχεία ενός άλλου αντιπροσώπου, τότε στο εσωτερικό βήμα 2 του πρωτοκόλλου εκλογών (δηλαδή στο βήμα (η) του 2ου επιπέδου), θα υπάρχουν ίδια κρυπτογραφημένα μηνύματα και η διαδικασία θα τερματιστεί πριν την αποκρυπτογράφηση των δεδομένων. Συνεπώς, ο διαφθορέας αντιπρόσωπος δεν θα λάβει τα αποκρυπτογραφημένα δεδομένα και η ομάδα του μπορεί να τον αποκαλύψει.

(4) Έστω ότι ένας αντιπρόσωπος στέλνει μη έγκυρα δεδομένα με σκοπό να παραπλανήσει τους άλλους αντιπροσώπους. Τότε, στο τέλος του βήματος (η), θα λείπουν οι υπογραφές της ένωσης ειδικών από τα μη έγκυρα αρχεία οπότε και αυτά θα αποκαλυφθούν, το πρωτόκολλο θα τερματιστεί και ο διαφθορέας μπορεί να αποκαλυφθεί από την ομάδα του.

Τρίτο μέλος ως ενεργός διαφθορέας:

(1) Έστω ότι κάποιο τρίτο μέλος ενεργεί ως διαφθορέας προσπαθώντας να περάσει μη έγκυρα έγγραφα στους οργανισμούς. Η υπογραφή αυτού του τρίτου μέλους στο βήμα (δ) δεν θα επιβεβαιωθεί ως υπογραφή έγκυρου οργανισμού και τα δεδομένα του θα απορριφθούν. Γενικά, όλες οι αποστολές δεδομένων γίνονται από συγκεκριμένο αποστολέα προς συγκεκριμένο παραλήπτη και είναι αυθεντικοποιημένες. Κατά συνέπεια, οποιοδήποτε τρίτο μέλος διαφθορέας μπορεί να αποκαλυφθεί άμεσα.

7.7 Θέματα πολυπλοκότητας του προτεινόμενου σχήματος χωρίς Συλλέκτη

Στην παρούσα ενότητα αναλύουμε την πολυπλοκότητα του προτεινόμενου σχήματος ως προς τους υπολογισμούς που απαιτεί. Ως μέτρο πολυπλοκότητας θεωρούμε τον αριθμό των: κρυπτογραφήσεων, αποκρυπτογραφήσεων, υπογραφών, επαληθεύσεων και αποστολών. Θεωρούμε ότι όλες οι παραπάνω λειτουργίες έχουν ίδιο υπολογιστικό κόστος και ίσο με 1.

Το πρωτόκολλο των ηλεκτρονικών εκλογών του Merritt για N ψηφοφόρους, όπως περιγράφεται στο [185], απαιτεί:

1. $2N^2$ κρυπτογραφήσεις,
2. N αποστολές,
3. N^2 αποκρυπτογραφήσεις $+N^2$ αποστολές,
4. N^2 αποκρυπτογραφήσεις $+N^2$ υπογραφές $+N^2(N-1)$ αποστολές $+N^2(N-1)$ επαληθεύσεις.

Συνεπώς, ο συνολικός αριθμός υπολογισμών είναι

$$\#\text{υπολογισμών} = 2N^3 + 4N^2 + N = f(N).$$

Ας υποθέσουμε ότι κάθε ψηφοφόρος είναι ένας οργανισμός και έχουμε συνολικά N οργανισμούς. Έστω ότι κάθε οργανισμός έχει x_i εγγραφές. Τότε, ο συνολικός αριθμός εγγραφών είναι $x = x_1 + x_2 + \cdots + x_N$, και ο συνολικός αριθμός υπολογισμών είναι,

$$\frac{x}{N} f(N).$$

Ας θεωρήσουμε το πρωτόκολλο εκλογών και έστω ότι οι ψηφοφόροι χωρίζονται σε ομάδες μεγέθους n, και οι ομάδες χωρίζονται επίσης σε ομάδες n στοιχείων διαδοχικά. Με τον τρόπο αυτό, δημιουργείται ένα δέντρο s επιπέδων, με πλήθος ψηφοφόρων ίσο με $N = n^s$. Εφαρμόζουμε το προτεινόμενο πρωτόκολλο, και ο αριθμός των υπολογισμός είναι ο ακόλουθος:

$$sn^{s-1}f(n) = \log_n(N) \times N \times \frac{f(n)}{n}.$$

Τέλος, συνδυάζουμε τα παραπάνω αποτελέσματα, υποθέτοντας ότι έχουμε $N = n^s$ οργανισμούς, και κάθε οργανισμός έχει x_i εγγραφές, με $x = x_1 + x_2 + \cdots + x_N$. Ο αριθμός των υπολογισμών είναι:

$$s \times x \times \frac{f(n)}{n}.$$

Ας υποθέσουμε ακόμα ότι έχουμε ένα δέντρο με s επίπεδα, όπου το n δεν είναι σταθερό. Και έστω $n_{\max}$ ο μέγιστος αριθμός των κλάδων ανά κόμβο. Σύμφωνα με το προτεινόμενο σχήμα θα πρέπει να είναι $n_{\max} \approx 5$. Τότε, θα είναι $N \leqslant n_{\max}^s$ και

$$\#\text{υπολογισμών} \leqslant sx\frac{f(n_{\max})}{n_{\max}},$$

όπου, γενικά, είναι $\frac{f(k)}{k} = 2k^2 + 4k + 1$ ένα πολυώνυμο 2ου βαθμού.

7.8 Συμπεράσματα - Συνεισφορά

Στην μελέτη αυτή προτάθηκαν δύο σχήματα για ηλεκτρονική συγκέντρωση δεδομένων με ιδιωτικότητα, τα οποία βασίζονται σε τροποποίηση σύγχρονων πρωτοκόλλων ηλεκτρονικών εκλογών.

Αναφορικά με το πρώτο σχήμα, η τροποποίηση περιλαμβάνει ένα πρόσθετο είδος μελών, τις Αλίκες, που δεν είναι απαραίτητα έμπιστα μέλη. Οι Αλίκες είναι οργανισμοί που χρησιμοποιούν Ειδικούς, οι οποίοι αντιστοιχούν στους ψηφοφόρους ενός συστήματος ηλεκτρονικών εκλογών. Ο Συλλέκτης των δεδομένων αναγνωρίζει την υπογραφή της ένωσης των Ειδικών και την ταυτότητα κάθε Αλίκης, χωρίς να μπορεί να συσχετίσει τις βάσεις δεδομένων με τις αντίστοιχες Αλίκες.

Το δεύτερο προτεινόμενο σχήμα βασίζεται σε τροποποίηση ενός πρωτοκόλλου ηλεκτρονικών εκλογών χωρίς κάλπη. Αυτό σημαίνει ότι δεν απαιτεί την χρήση τρίτου έμπιστου μέλους (Συλλέκτη) για την συγκέντρωση των δεδομένων.

Σχετικές μελέτες για την συγκέντρωση δεδομένων δεν εξασφαλίζουν την ιδιωτικότητα των αποστολέων των δεδομένων ή την αυθεντικοποίηση των δεδομένων. Σημαντική προσπάθεια επίσης έχει γίνει για την επεξεργασία δεδομένων που είναι κατανεμημένα σε πολλές πηγές [7, 113, 204], αλλά στις περιπτώσεις αυτές δεν πραγματοποιείται ηλεκτρονική συγκέντρωση των δεδομένων.

Τα δύο προτεινόμενα σχήματα είναι οι πρώτες προσεγγίσεις που ικανοποιούν και τις πέντε απαιτήσεις της πληρότητας του σχήματος, της ιδιωτικότητας και νομιμότητας των συμμετεχόντων, της αυθεντικοποίησης και της επιβεβαίωσης των δεδομένων, που είναι απαραίτητες για την ηλεκτρονική συγκέντρωση δεδομένων με ιδιωτικότητα (privicy preserving electronic gathering). Επιπλέον, και τα δύο σχήματα μπορούν να συνδυαστούν εύκολα με άλλα συστήματα ανώνυμων καναλιών, πρωτόκολλα ηλεκτρονικών εκλογών αλλά και τεχνικές εξόρυξης δεδομένων. Τέλος, οι προσεγγίσεις αυτές μπορούν να επεκταθούν και για άλλες ενδιαφέρουσες εφαρμογές, όπως η ηλεκτρονική απογραφή με ιδιωτικότητα.

ΚΕΦΑΛΑΙΟ 8

Συμπεράσματα και προοπτικές

Τον 21 ο αιώνα καθώς η τεχνολογία των υπολογιστών προχωρά με ταχύτατους ρυθμούς και οι απαιτήσεις για ασφάλεια και ιδιωτικότητα αυξάνονται, η επιστήμη της κρυπτογραφίας εξελίσσεται όλο και περισσότερο για να καλύψει τις νέες ανάγκες που προκύπτουν. Η αναζήτηση νέων μεθοδολογιών για την ανάπτυξη κρυπτοσυστημάτων αλλά και η παρουσίαση καινοτόμων τεχνικών κρυπτανάλυσης κρίνονται απαραίτητες για την ανάπτυξη του κλάδου αυτού.

Η παρούσα διδακτορική διατριβή επικεντρώθηκε στη μελέτη νέων τεχνικών κρυπτογραφίας και κρυπτανάλυσης, αλλά και στην ανάπτυξη νέων πρωτοκόλλων για την ασφαλή ηλεκτρονική συγκέντρωση δεδομένων.

Πιο αναλυτικά, το πρώτο πρόβλημα το οποίο διερεύνησε η διατριβή ήταν η δυνατότητα εφαρμογής των μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτολογία. Στόχος μας ήταν να ανιχνεύσουμε τα κρίσιμα σημεία κατά την εφαρμογή των μεθόδων αυτών στον πολύ απαιτητικό αυτό τομέα προβλημάτων και να μελετήσουμε την αποτελεσματικότητα και την αποδοτικότητά τους σε διάφορα προβλήματα κρυπτογραφίας και κρυπτανάλυσης. Για το λόγο αυτό, θεωρήσαμε δύο Εξελικτικές μεθόδους, τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με Σμήνος σωματιδίων, αλλά και Τεχνητά Νευρωνικά Δίκτυα πρόσθιας τροφοδότησης και τα εφαρμόσαμε αρχικά για την κρυπτανάλυση θεμελιωδών προβλημάτων κρυπτογραφίας όπως αυτό του διακριτού λογαρίθμου, της απεικόνισης Diffie-Hellman και της παραγοντοποίησης ακεραίων. Τα αποτελέσματα σε κάθε περίπτωση έδειξαν ότι η πολυπλοκότητα και η δυναμική των προβλημάτων αυτών είναι τέτοια που δεν παρέχει αρκετή πληροφορία στις μεθόδους ώστε να είναι αποδοτικές στην επίλυσή τους. Κατά συνέπεια, ένα σημείο το οποίο απαιτεί ιδιαίτερη προσοχή κατά την εφαρμογή μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτανάλυση είναι η δημιουργία της αντικειμενικής συνάρτησης που μοντελοποιεί το υπό μελέτη πρόβλημα με τρόπο που να εμπεριέχει όσο το δυνατόν περισσότερη πληροφορία για το πρόβλημα και να αξιολογεί ικανοποιητικά κάθε δυνατή λύση.

Στη συνέχεια, εφαρμόσαμε τον Διαφοροεξελικτικό αλγόριθμο και την μέθοδο Βελτιστοποίησης με Σμήνος σωματιδίων για την αποκρυπτογράφηση τμήματος του κλειδιού του κρυπτοσυστήματος DES με τέσσερις και έξι γύρους. Τα αποτελέσματα ήταν ιδιαίτερα ενθαρρυντικά καθώς στην περίπτωση των τεσσάρων γύρων και οι δύο μέθοδοι ήταν πολύ αποτελεσματικές και αποδοτικές, ενώ ακόμα και στην δυσκολότερη περίπτωση των έξι γύρων οι μέθοδοι έδωσαν πολύ καλά αποτελέσματα. Επίσης, ο Διαφοροεξελικτικός αλγόριθμος και η μέθοδος Βελτιστοποίησης με Σμήνος σωματιδίων εφαρμόστηκαν για ένα πρόβλημα κρυπτογράφησης και συγκεκριμένα για την δημιουργία ισχυρών S-boxes που χρησιμοποιούνται ως δομικό στοιχείο για τα σύγχρονα κρυπτοσυστήματα συμμετρικού κλειδιού και απέδωσαν βέλτιστα σε όλες σχεδόν τις περιπτώσεις με αρκετά μικρό υπολογιστικό κόστος. Τέλος, με την βοήθεια των νευρωνικών Πολυωνυμικών Δικτύων Ridge διατυπώθηκε ένα πόρισμα για την ύπαρξη νευρωνικών δικτύων τα οποία υλοποιούν το πολυώνυμο για την εύρεση του λιγότερο σημαντικού ψηφίου του διακριτού λογαρίθμου.

Συνοψίζοντας, τα αποτελέσματα της διατριβής για την εφαρμογή μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτολογία υποδεικνύουν ότι παρά το γεγονός ότι η κατασκευή των αντικειμενικών συναρτήσεων είναι πολύ κρίσιμη για την αποδοτικότητα των μεθόδων, η Υπο-

λογιστική Νοημοσύνη μπορεί να προσφέρει σημαντικά πλεονεκτήματα στον κλάδο αυτό όπως είναι η αυτοματοποίηση κάποιων διαδικασιών κρυπτανάλυσης ή κρυπτογράφησης, ο γρήγορος έλεγχος της σθεναρότητας νέων κρυπτοσυστημάτων αλλά και ο συνδυασμός τους με τυπικές μεθόδους που χρησιμοποιούνται μέχρι σήμερα για την αξιοποίηση της απλότητας και της αποδοτικότητάς τους.

Οι προοπτικές για την χρήση των μεθόδων Υπολογιστικής Νοημοσύνης στην κρυπτολογία είναι πολλές καθώς η έρευνα του συγκεκριμένου αντικειμένου βρίσκεται ακόμα στην αρχή. Ένα ενδιαφέρον θέμα μελέτης θα ήταν η αξιοποίηση των πιο εξελιγμένων μεθόδων Εξελικτικού Υπολογισμού για τον σχεδιασμό καλών γεννητριών ψευδοτυχαίων αριθμών χρησιμοποιώντας όσο το δυνατόν μεγαλύτερο κομμάτι της περιόδου αυτών.

Το δεύτερο πρόβλημα που μελετάται στην διατριβή είναι η εφαρμογή μεθόδων αντίστροφης πολυωνυμικής παρεμβολής για την εύρεση της τιμής του διακριτού λογαρίθμου αλλά και του λογαρίθμου του Lucas. Για την μελέτη αυτή χρησιμοποιήθηκαν δύο υπολογιστικές μέθοδοι αντίστροφης πολυωνυμικής παρεμβολής, οι μέθοδοι Aitken και Neville, οι οποίες είναι κατασκευαστικές και επιτρέπουν την πρόσθεση νέων σημείων παρεμβολής για καλύτερη προσέγγιση του πολυωνύμου με μικρό υπολογιστικό κόστος. Μέχρι τώρα η παρεμβολή ως τεχνική επίθεσης στα προβλήματα του διακριτού λογαρίθμου και του λογαρίθμου του Lucas έχει διερευνηθεί κυρίως θεωρητικά και με πιο κλασικές μεθόδους παρεμβολής όπως αυτή του Lagrange. Έχει αποδειχθεί θεωρητικά ότι υπάρχουν πολυώνυμα παρεμβολής τα οποία παρεμβάλλουν τις τιμές των δύο λογαρίθμων ωστόσο ο βαθμός των πολυωνύμων αυτών είναι αρκετά υψηλός ώστε η τεχνική αυτή να παρουσιάζει ενδιαφέρον ως μέθοδος κρυπτανάλυσης. Η παρούσα μελέτη έδειξε ότι και με την προτεινόμενη μεθοδολογία το συνολικό κόστος υπολογισμού της τιμής των λογαρίθμων παραμένει υψηλό, ωστόσο η κατανομή των πολυωνύμων που έδωσαν την λύση των προβλημάτων δείχνει ότι η μεθοδολογία που χρησιμοποιήθηκε είτε εντόπισε την λύση στα πρώτα στάδια κατασκευής των πολυωνύμων είτε εντόπισε πολυώνυμα μικρού σχετικά βαθμού που προσεγγίζουν την αντίστοιχη λύση. Η ένδειξη αυτή παρουσιάζει ενδιαφέρον και μια προοπτική της μελέτης αυτής θα μπορούσε να αποτελέσει η περαιτέρω διερεύνηση των αρχικών σημείων παρεμβολής που χρησιμοποιούνται και το πως αυτή επηρεάζει την αποδοτικότητα της συγκεκριμένης τεχνικής στην επίλυση των δύο προβλημάτων.

Το τρίτο πρόβλημα που πραγματεύεται η παρούσα διατριβή είναι η δημιουργία νέων σθεναρών κρυπτοσυστημάτων με την χρήση μη-γραμμικών δυναμικών απεικονίσεων. Η αξιοποίηση των ιδιοτήτων του χάους στην κρυπτογραφία έχει αποτελέσει αντικείμενο μελέτης τα τελευταία χρόνια από τους ερευνητές λόγω της αποδεδειγμένης πολυπλοκότητας των συστημάτων του και των ιδιαίτερων στατιστικών ιδιοτήτων τους. Η διατριβή συνεισφέρει προτείνοντας ένα νέο συμμετρικό κρυπτοσύστημα που βασίζεται σε περιοδικές δυναμικές τροχιές και παρουσιάζει και τρεις τροποποιήσεις του που το καθιστούν ιδιαίτερα σθεναρό απέναντι στις συνήθεις κρυπταναλυτικές επιθέσεις. Δίνεται επίσης το υπολογιστικό κόστος κρυπτογράφησης και αποκρυπτογράφης του προτεινόμενου σχήματος και παρουσιάζονται πειραματικά αποτελέσματα που δείχνουν ότι η δομή των κρυπτογραφημάτων του κρυπτοσυστήματος δεν παρέχει πληροφορία για την ύπαρξη τυχόν μοτίβων στο αρχικό κείμενο. Μία ενδιαφέρουσα προοπτική της συγκεκριμένης μελέτης θα ήταν η δυνατότητα εφαρμογής της προτεινόμενης μεθοδολογίας για την κατασκευή ενός νέου κρυπτοσυστήματος δημόσιου κλειδιού.

Τέλος, στην διατριβή αυτή προτείνονται δύο πρωτόκολλα για την ασφαλή ηλεκτρονική συγκέντρωση δεδομένων. Η συγκέντρωση δεδομένων από διαφορετικές βάσεις με ασφάλεια και ιδιωτικότητα θα ήταν σημαντική για την μελέτη των γνώσεων που ενυπάρχουν στα δεδομένα αυτά, με διάφορες μεθόδους εξόρυξης δεδομένων και ανάλυσης, καθώς οι γνώσεις αυτές ενδεχομένως δεν θα μπορούσαν να αποκαλυφθούν από την επιμέρους μελέτη των δεδομένων χωριστά από κάθε βάση. Τα δύο πρωτόκολλα που προτείνονται βασίζονται σε τροποποιήσεις πρωτοκόλλων ηλεκτρονικών εκλογών με τρόπο τέτοιο ώστε να ικανοποιούνται τα απαραίτητα κριτήρια ασφάλειας και ιδιωτικότητας που απαιτούνται για την συγκέντρωση των δεδομένων. Η βασική διαφορά των δύο πρωτοκόλλων είναι ότι στο ένα γίνεται χρήση έμπιστου τρίτου

μέλους για την συγκέντρωση των δεδομένων, ενώ στο δεύτερο όχι. Και στις δύο περιπτώσεις, παρουσιάζεται ανάλυση της ασφάλειας των σχημάτων αλλά και της πολυπλοκότητάς τους αναφορικά με το υπολογιστικό τους κόστος.

Μέρος IV

Βιβλιογραφία – Ευρετήριο

Βιβλιογραφία

[1] M. Abe. *Universally verifiable mix-net with verification work independent of the number of mix-servers*, volume 1403 of *Lecture Notes in Computer Science*, pages 437–447. Springer-Verlag, 1998.

[2] M.A. Abido. Optimal design of power system stabilizers using particle swarm optimization. *IEEE Trans. Energy Conversion*, 17(3):406–413, 2002.

[3] M.A. Abido. Optimal power flow using particle swarm optimization. *Electrical Power and Energy Systems*, 24:563–571, 2002.

[4] L. Adleman. A subexponential algorithm for discrete logarithm problem with applications to cryptography. In *Proc. 20th FOCS*, pages 55–60, 1979.

[5] L.M. Adleman and J. DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of Computation*, 61(203):1–15, 1993.

[6] D.K. Agrafiotis and W. Cedeno. Feature selection for structure–activity correlation using binary particle swarms. *Journal of Medicinal Chemistry*, 45(5):1098–1107, 2002.

[7] R. Agrawal and R. Srikant. Privacy-preserving data mining. In *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 439–450, Texas, 2000. ACM Press.

[8] H. Aly and A. Winterhof. Polynomial representations of the Lucas logarithm. *Finite Fields and Their Applications*, 12:413–424, 2006.

[9] M. Anthony. Boolean functions and artificial neural networks. Technical report, CDAM, The London School of Economics and Political Science, 2003. CDAM Research Report LSE-CDAM-2003-01.

[10] T. Bäck. *Evolutionary Algorithms in Theory and Practice*. Oxford University Press, New York, 1996.

[11] T. Bagnall, G. P. McKeown, and V. J. Rayward-Smith. The cryptanalysis of a three rotor machine using a genetic algorithm. In Thomas Bäck, editor, *Proceedings of the 7th International Conference on Genetic Algorithms (ICGA97)*, San Francisco, CA, 1997. Morgan Kaufmann.

[12] A. Barbieri, S. Cagnoni, and G. Colavolpe. A genetic approach for generating good linear block error-correcting codes. *LNCS, GECCO 2004*, 3103:1301–1302, 2004.

[13] K. Bennett, M.C. Ferris, and Y.E. Ioannidis. A genetic algorithm for database query optimization. In *Proceedings of the Fourth International Conference on Genetic Algorithms*, pages 520–526, San Mateo, CA, 1991. Morgan Kaufmann.

[14] E. Biham and A. Shamir. Differential cryptanalysis of des–like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[15] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer–Verlag, 1993.

[16] I. Blake. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Notes Series*. Cambridge University Press, 1999.

[17] D. Bleichenbacher, W. Bosma, and A.K. Lenstra. Some remarks on Lucas-based cryptosystems. In *CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, pages 386–396. Springer-Verlag, 1995.

[18] A. Blum, M. Furst, M. Kearns, and R. J. Lipton. Cryptographic primitives based on hard learning problems. *Lecture Notes in Computer Science*, 773:278–291, 1994.

[19] E. Bonabeau, M. Dorigo, and G. Théraulaz. *From Natural to Artificial Swarm Intelligence*. Oxford University Press, New York, 1999.

[20] C. Boyd. A new multiple key cipher and an improved voting scheme. In *LNCS*, volume 434, pages 617–625. Springer-Verlag, 1989.

[21] R. L. Burden and J. D. Faires. *Numerical Analysis*. Brooks/Cole Publishing Company, 1997.

[22] L. Burnett, G. Carter, E. Dawson, and W. Millan. Efficient methods for generating mars-like s-boxes. *LNCS*, 1978(4):300–313, 2001.

[23] A. Carlisle and G. Dozier. An off-the-shelf pso. In *Proceedings of the Workshop on Particle Swarm Optimization*, pages 1–6, Indianapolis (IN), USA, 2001.

[24] J. Carrol and S. Martin. The automated cryptanalysis of substitution ciphers. *Cryptologia*, 10(4):193–209, 1986.

[25] C. Chang and W. Wu. A secure voting system on a public network. *Networks*, 29:81–87, 1997.

[26] Y.-C. Chang and C.-J. Lu. Oblivious polynomial evaluation and oblivious neural learning. *LNCS, ASIACRYPT'01*, 2248:369–384, 2001.

[27] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[28] D. L. Chaum. Blind signature for untraceable payments. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology, Proceedings of CRYPTO'82*, pages 199–203, Plenum, NY, 1982.

[29] C. K. Chui and X. Li. Realization of neural networks with one hidden layer. Technical report, Center for Approximation Theory, Dept. of Mathematics, Texas A&M University, 1991.

[30] C. K. Chui and X. Li. Approximation by Ridge functions and neural networks with one hidden layer. *Journal of Approximation Theory*, 70:131–141, 1992.

[31] A. Clark. *Optimisation Heuristics for Cryptography*. PhD thesis, Queensland University of Technology, Australia, 1998.

[32] J.A. Clark and J.L. Jacob. Two-stage optimisation in the design of boolean functions. *LNCS*, 1841:242–254, 2000.

[33] J.A. Clark and J.L. Jacob. Fault injection and a timing channel on an analysis technique. *LNCS*, 2332:181–196, 2002.

[34] J.A. Clark, J.L. Jacob, and S. Stepney. The design of s-boxes by simulated annealing. In *CEC 2004: International Conference on Evolutionary Computation, Portland OR, USA, June 2004*, pages 1533–1537. IEEE, 2004.

[35] J.A. Clark, J.L. Jacob, and S. Stepney. Searching for cost functions. In *CEC 2004: International Conference on Evolutionary Computation, Portland OR, USA, June 2004*, pages 1517–1524. IEEE, 2004.

[36] M. Clerc and J. Kennedy. The particle swarm–explosion, stability, and convergence in a multidimensional complex space. *IEEE Transactions on Evolutionary Computation*, 6(1):58–73, 2002.

[37] A.R. Cockshott and B.E. Hartman. Improving the fermentation medium for *Echinocandin B* production part ii: Particle swarm optimization. *Process Biochemistry*, 36:661–669, 2001.

[38] D. Coppersmith and I. Shparlinski. On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping. *Journal of Cryptology*, 13:339–360, 2000.

[39] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. *LNCS*, 1233:103–118, 1997.

[40] F. Dachselt and W. Schwarz. Chaos and cryptography. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 48(12):1498–1509, 2001.

[41] B. DasGupta and G. Schnitger. Analog versus discrete neural networks. *Neural Computation*, 8(4):805–818, 1996.

[42] K.A. De Jong. Genetic algorithms: A 10 year perspective. In *Proceedings of the First International Conference on Genetic Algorithms*, pages 169–177, Hillsdale, NJ, 1985. Lawrence Erlbaum Associates.

[43] R. DeMillo, N. Lynch, and M. Merritt. Cryptographic protocols. In *Proc. 14th ACM Symp. on the Theory of Computing*, pages 383–400, 1982.

[44] R. DeMillo and M. Merritt. Protocols for data security. *IEEE Computer*, 16(2):39–50, 1983.

[45] R.L. Devaney. A piecewise linear model for thezones of instability of an area preserving map. *Physica D*, 10:387–393, 1984.

[46] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[47] K. Dontas and K. Jong. Discovery of maximal distance codes using genetic algorithms. In *Proc. of the Second International IEEE Conference on Tools for Artificial Intelligence*, pages 805–811, 1990.

[48] M. Dorigo and G. Di Caro. The ant colony optimization meta-heuristic. In D. Corne, M. Dorigo, and F. Glover, editors, *New Ideas in Optimization*. McGraw-Hill, 1999.

[49] M. Dorigo and L.M. Gambardella. Ant colonies for the traveling salesman problem. *BioSystems*, 43:73–81, 1997.

[50] R.C. Eberhart and J. Kennedy. A new optimizer using particle swarm theory. In *Proceedings Sixth Symposium on Micro Machine and Human Science*, pages 39–43, Piscataway, NJ, 1995. IEEE Service Center.

[51] R.C. Eberhart and Y. Shi. Comparison between genetic algorithms and particle swarm optimization. In V.W. Porto, N. Saravanan, D. Waagen, and A.E. Eiben, editors, *Evolutionary Programming*, volume VII, pages 611–616. Springer, 1998.

[52] R.C. Eberhart, P. Simpson, and R. Dobbins. *Computational Intelligence PC Tools*. Academic Press, 1996.

[53] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[54] A. Engelbrecht. *Computational Intelligence: An Introduction*. John Wiley & Sons, 2002.

[55] M. G. Epitropakis and M. N. Vrahatis. Root finding and approximation approaches through neural networks. *SIGSAM Bulletin: Communications in Computer Algebra*, 39(4):118–121, 2005.

[56] U. M. Fayyad, G. Piatetsky-Shapiro, and P. Smyth. *Advances in Knowledge Discovery and Data Mining*. AAAI. Press/MIT Press, 1996.

[57] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.

[58] D.B. Fogel. Evolving behaviours in the iterated prisoner's dilemma. *Evolutionary Computation*, 1(1):77–97, 1993.

[59] D.B. Fogel. *Evolutionary Computation: Towards a New Philosophy of Machine Intelligence*. IEEE Press, Piscataway, NJ, 1995.

[60] D.B. Fogel, A.J. Owens, and M.J. Walsh. *Artificial Intelligence Through Simulated Evolution*. John Wiley, Chichester, UK, 1966.

[61] W. S. Forsyth and R. Safavi-Naini. Automated cryptanalysis of substitution ciphers. *Cryptologia*, 17(4):407–418, 1993.

[62] P.C. Fourie and A.A. Groenwold. The particle swarm optimization algorithm in size and shape optimization. *Struct. Multidisc. Optim.*, 23:259–267, 2002.

[63] D. R. Frey. Chaotic digital encoding: An approach to secure communication. *IEEE Trans. Circuits Syst. II*, 40:660–666, 1993.

[64] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. *Lecture Notes in Computer Science*, 718:244–251, 1992.

[65] J. Ghosh and Y. Shin. Efficient higher-order neural networks for classification and function approximation. *International Journal of Neural Systems*, 3:323–350, 1992.

[66] D.E. Goldberg. *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison Wesley, Reading, MA, 1989.

[67] Johan Håstad and Mats Näslund. The security of all RSA and discrete log bits. *Journal of the ACM*, 51(2):187–230, 2004.

[68] M. Hénon. Numerical study of quadratic area-preserving mappings. *Quart. Appl. Math.*, 27:291–311, 1969.

[69] J. Hernández, P. Isasi, and A. Ribagorda. An application of genetic algorithms to the cryptoanalysis of one round TEA. In *Proc. of the 2002 Symposium on Artificial Intelligence and its Application*, 2002.

[70] J. Hernández, J. Sierra, P. Isasi, and A. Ribagorda. Genetic cryptoanalysis of two rounds TEA. *LNCS*, 2331:1024–1031, 2002.

[71] J. Hertz, A. Krogh, and R. G. Palmer. *Introduction to the theory of neural computation*. Addison-Wesley, Redwood City, 1991.

[72] J.H. Holland. *Adaptation in Natural and Artificial Systems*. University of Michigan Press, Ann Arbor, 1975.

[73] K. Hornik. Multilayer feedforward networks are universal approximators. *Neural Networks*, 2:359–366, 1989.

[74] D. Hunter and A. McKenzie. Experiments with relaxation algorithms for breaking simple substitution ciphers. *The Computer Journal*, 26(1):68–71, 1983.

[75] P. Isasi and J. Hernández. Introduction to the applications of evolutionary computation in computer security and cryptography. *Computational Intelligence*, 20(3):445–449, 2004.

[76] A. K. Jain, J. Mao, and K. Mohiuddin. Artificial neural networks: a tutorial. *IEEE Computer*, 1996.

[77] T. Jakobsen. A fast method for cryptanalysis of substitution ciphers. *Cryptologia*, 19(3):265–274, 1995.

[78] W. S. Jevons. *The Principles of Science: A Treatise on Logic and Scientific Method*. Macmillan & Co., London, 1874.

[79] M. G. Karagiannopoulos, G. C. Meletiou, and M. N. Vrahatis. A note on a secure voting system on a public network. *Networks*, 43(4):224–225, 2004.

[80] D. Karras and V. Zorkadis. Strong pseudorandom bit sequence generators using neural network techniques and their evaluation for secure communications. *LNAI, AI'02*, 2557:615–626, 2002.

[81] D. Karras and V. Zorkadis. On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. *Neural Networks*, 16:899–905, 2003.

[82] J. Kennedy. The behavior of particles. In V.W. Porto, N. Saravanan, D. Waagen, and A.E. Eiben, editors, *Evolutionary Programming*, volume VII, pages 581–590. Springer, 1998.

[83] J. Kennedy and R.C. Eberhart. *Swarm Intelligence*. Morgan Kaufmann Publishers, 2001.

[84] E. Kiltz and A. Winterhof. Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem. *Discrete Appl. Math.*, 154:326–336, 2006.

[85] J. King and D. Bahler. An implementation of probabilistic relaxation in the cryptanalysis of simple substitution ciphers. *Cryptologia*, 16(3):215–225, 1992.

[86] W. Kinzel and I. Kanter. Interacting neural networks and cryptography. In B. Kramer, editor, *Advances in Solid State Physics*, volume 42, pages 383–391. Springer–Verlag, 2002.

[87] A. Klimov, A. Mityagin, and A. Shamir. Analysis of neural cryptography. *LNCS, Advances in Cryptology – ASIACRYPT'02*, 2501:288–298, 2002.

[88] L. R. Knudsen and W. Meier. A new identification scheme based on the perceptrons problem. *LNCS, EUROCRYPT'99*, 1592:363–374, 1999.

[89] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[90] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz. From chaotic maps to encryption schemes. In *Proceedings of the IEEE Int. Symposium Circuits and Systems (ISCAS98)*, volume 4, pages 514–517, 1998.

[91] E. Konstantinou, Y. Stamatiou, and C. Zaroliagis. A software library for elliptic curve cryptography. *LNCS*, 2461:625–637, 2002.

[92] S. Konyagin, T. Lange, and I. Shparlinski. Linear complexity of the discrete logarithm. *Des. Codes Cryptogr.*, 28:135–146, 2003.

[93] P. Kotlarz and Z. Kotulski. On application of neural networks for s-boxes design. *LNAI, AWIC 2005*, 3528:243–248, 2005.

[94] J.R. Koza. *Genetic Programming: On the Programming of Computers by Means of Natural Selection*. MIT Press, Cambridge, MA, 1992.

[95] C. S. Laih, F. K. Tu, and W. C. Tai. On the security of the Lucas function. *Informations Processing Letters*, 53:243–247, 1995.

[96] T. Lange and A. Winterhof. Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by boolean functions. *Acta Arithmetica*, 101(3):223–229, 2002.

[97] T. Lange and A. Winterhof. Interpolation of the discrete logarithm in f_q by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$. *Discrete Appl. Math.*, 128:193–206, 2003.

[98] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, D. K. Tasoulis, and M. N. Vrahatis. Assessing the effectiveness of artificial neural networks on problems related to elliptic curve cryptography. *Mathematical and Computer Modelling*, 46:174–179, 2007.

[99] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis. Evolutionary computation based cryptanalysis: A first study, nonlinear analysis: Theory, methods and applications. *Nonlinear Analysis: Theory, Methods and Applications*, 63:e823–e830, 2005.

[100] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis. Applying evolutionary computation methods for the cryptanalysis of feistel ciphers. *Applied Mathematics and Computation*, 184:63–72, 2007.

[101] E. C. Laskari, G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis. Cryptography and cryptanalysis through computational intelligence. In N. Nedjah, A. Abraham, and L. de Macedo Mourelle, editors, *Computational Intelligence in Information Assurance and Security*, volume 57 of *Studies in Computational Intelligence*, pages 1–49. Springer Verlag, Berlin / Heidelberg, Germany, May 2007. ISBN: 978-3-540-71077-6.

[102] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Aitken and neville inverse interpolation methods over finite fields. *Applied Numerical Analysis and Computational Mathematics (ANACM)*, 2(1):100–107, 2005.

[103] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Aitken and neville inverse interpolation methods over finite fields. *Applied Numerical Analysis and Computational Mathematics (ANACM)*, 2(1):100–107, 2005.

[104] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Privacy preserving electronic data gathering. *Mathematical and Computer Modelling*, 42(7/8):739–746, 2005.

[105] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Studying the performance of artificial neural networks on problems related to cryptography. *Nonlinear Analysis Series B: Real World Applications*, 7:937–942, 2006.

[106] E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis. The discrete logarithm problem as an optimization task: A first study. In *Proc. of the IASTED International Conference on Artificial Intelligence and Applications (AIA 2004)*, volume 2, pages 817–822. ACTA Press, 2004.

[107] E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis. Recent approaches to electronic data gathering with privacy. In *Proceedings of the 1st International Conference "From Scientific Computing to Computational Engineering" (IC-SCCE)*, Athens, Greece, 2004.

[108] E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis. Problems of cryptography as discrete optimization tasks. *Nonlinear Analysis: Theory, Methods and Applications*, 63:e831–e837, 2005.

[109] E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis. Utilizing evolutionary computation methods for the design of s-boxes. In *Proceedings of the International Conference on Computational Intelligence and Security 2006 (CIS 2006)*, volume 2, pages 1299–1302. IEEE Press, 2006.

[110] E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis. Aitken and neville inverse interpolation methods for the lucas logarithm problem. *Applied Mathematics and Computation*, 209(1):52–56, 2009.

[111] E.C. Laskari, K.E. Parsopoulos, and M.N. Vrahatis. Particle swarm optimization for integer programming. In *Proceedings of the IEEE 2002 Congress on Evolutionary Computation*, pages 1576–1581, Hawaii, HI, 2002. IEEE Press.

[112] E.C. Laskari, K.E. Parsopoulos, and M.N. Vrahatis. Particle swarm optimization for minimax problems. In *Proceedings of the IEEE 2002 Congress on Evolutionary Computation*, pages 1582–1587, Hawaii, HI, 2002. IEEE Press.

[113] Y. Lindell and B. Pinkas. Privacy preserving data mining. *Journal of Cryptology*, 15(3):177–206, 2002.

[114] E.N. Lorenz. Deterministic nonperiodic flow. *J. Atmos. Sci.*, 20:130–141, 1963.

[115] W.Z. Lu, H.Y. Fan, A.Y.T. Leung, and J.C.K. Wong. Analysis of pollutant levels in central hong kong applying neural network method with particle swarm optimization. *Environmental Monitoring and Assessment*, 79:217–230, 2002.

[116] G. D. Magoulas, V. P. Plagianakos, and M. N. Vrahatis. Adaptive stepsize algorithms for on-line training of neural networks. *Nonlinear Analysis T.M.A.*, 47(5):3425–3430, 2001.

[117] G. D. Magoulas, M. N. Vrahatis, and G. S. Androulakis. Effective backpropagation training with variable stepsize. *Neural Networks*, 10(1):69–82, 1997.

[118] R. Mathews. The use of genetic algorithms in cryptanalysis. *Cryptologia*, 17(4):187–201, 1993.

[119] M. Matsui. Linear cryptanalysis method for des cipher. *LNCS*, 765:386–397, 1994.

[120] M. Matsui and A. Yamagishi. A new method for known plaintext attack of feal cipher. *LNCS*, pages 81–91, 1992.

[121] R. A. J. Matthews. On the derivation of a chaotic encryption algorithm. *Cryptologia XIII*, pages 29–42, 1989.

[122] U. Maurer. Cryptography 2000 ± 10. *LNCS 2000*, pages 63–85, 2001.

[123] U. Maurer and S. Wolf. The relationship between breaking the diffie-hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28:1689–1721, 1999.

[124] W. S. McCulloch and W. Pitts. A logical calculus of ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, 5:115–133, 1943.

[125] W. Meidl and A. Winterhof. Lower bounds on the linear complexity of the discrete logarithm in finite fields. *IEEE Trans. Inform. Theory*, 47(1):2807–2811, 2001.

[126] G. C. Meletiou. A polynomial representation for exponents in $\mathbb{Z}_p$. *Bulletin of the Greek Mathematical Society*, 34:59–63, 1992.

[127] G. C. Meletiou. Explicit form for the discrete logarithm over the field $\mathrm{GF}(p, k)$. *Archivum Mathematicum (Brno)*, 29(1–2):25–28, 1993.

[128] G. C. Meletiou and G. L. Mullen. A note on discrete logarithms in finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 3(1):75–79, 1992.

[129] G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis. Cryptography through interpolation approximation and computational inteligence methods. *Bulletin of the Greek Mathematical Society*, 48:61–75, 2003.

[130] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of applied cryptography.* CRC Press series on discrete mathematics and its applications. CRC Press, 1996.

[131] R. C. Merkle and M. E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 24:525–530, 1978.

[132] Z. Michalewicz. *Genetic Algorithms + Data Structures = Evolution Programs.* Springer, Berlin, 1994.

[133] Z. Michalewicz, J. Krawczyk, M. Kazemi, and C. Janikow. Genetic algorithms and optimal control problems. In *Proceedings of the 29th IEEE Conference on Decision and Control*, pages 1664–1666, Honolulu, 1990.

[134] W. Millan. How to improve the nonlinearity of bijective s-boxes. *LUNGS*, 1438:181–192, 1998.

[135] W. Millan, L. Burnett, G. Carter, A. Clark, and E. Dawson. Evolutionary heuristics for finding cryptographically strong s-boxes. *LNCS*, 1726:263–274, 1999.

[136] W. Millan, A. Clark, and E. Dawson. Smart hill climbing finds better boolean functions. In *4th Workshop on Selected Areas in Cryptography SAC'97*, 1997.

[137] W. Millan, A. Clark, and E. Dawson. Heuristic design for cryptographically strong balanced Boolean functions. *LNCS, Advances in Cryptology, EUROCRYPT'98*, 1403:489–499, 1998.

[138] W. Millan, A.J. Clark, and E. Dawson. Boolean function design using hill climbing methods. *LNCS*, 1587:1–11, 1999.

[139] V. Miller. Uses of elliptic curves in cryptography. *LNCS*, 218:417–426, 1986.

[140] M. Minsky and S Papert. *Perceptrons: An introduction to computational geometry.* MIT Press, Cambridge, MA, 1969.

[141] R. Mislovaty, Y. Perchenok, I. Kanter, and W. Kinzel. Secure key-exchange protocol with an absence of injective functions. *Phys. Rev. E*, 66(6):066102–1–066102–5, 2002.

[142] D. Mitchell. Nonlinear key generators. *Cryptologia*, 14:350–354, 1990.

[143] M. F. Møller. A scaled conjugate gradient algorithm for fast supervised learning. *Neural Networks*, 6:525–533, 1993.

[144] G. L. Mullen and D. White. A polynomial representation for logarithms in GF(q). *Acta Arithmetica*, 47:255–261, 1986.

[145] National Bureau of Standards, U.S. Department of Commerce, FIPS pub. 46. *Data Encryption Standard*, January 1977.

[146] H. Niederreiter. A short proof for explicit formulas for discrete logarithms in finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 1:55–57, 1990.

[147] H. Niederreiter. Incomplete character sums and polynomial interpolation of the discrete logarithm. *Finite Fields Appl.*, 8:184–192, 2002.

[148] A. Odlyzko. Discrete logarithms: The past and the future. *Designs, Codes, and Cryptography*, 19(2–3):129–145, 2000.

[149] W. Ogata, K. Kurosawa, K. Sako, and K. Takatani. Fault tolerant anonymous channel. *Lecture Notes in Computer Science*, 1334:440–444, 1997.

[150] C.O. Ourique, E.C. Biscaia, and J. Carlos Pinto. The use of particle swarm optimization for dynamical analysis in chemical processes. *Computers and Chemical Engineering*, 26:1783–1793, 2002.

[151] S. Papadimitriou, T. Bountis, S. Mavaroudi, and A. Bezerianos. A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations. *Int. J. Bifurc. Chaos*, 11:3107–3115, 2001.

[152] C. Park, K. Itoh, and K. Kurosawa. Efficient anonymous channel and all/nothing election scheme. *Lecture Notes in Computer Science*, 765:248–259, 1994.

[153] K.E. Parsopoulos, V.P. Plagianakos, G.D. Magoulas, and M.N. Vrahatis. Improving particle swarm optimizer by function "stretching". In N. Hadjisavvas and P.M. Pardalos, editors, *Advances in Convex Analysis and Global Optimization*, volume 54 of *Nonconvex Optimization and Applications*, chapter 28, pages 445–457. Kluwer Academic Publishers, The Netherlands, 2001.

[154] K.E. Parsopoulos, V.P. Plagianakos, G.D. Magoulas, and M.N. Vrahatis. Objective function "stretching" to alleviate convergence to local minima. *Nonlinear Analysis, Theory, Methods & Applications*, 47(5):3419–3424, 2001.

[155] K.E. Parsopoulos and M.N. Vrahatis. Modification of the particle swarm optimizer for locating all the global minima. In V. Kurkova, N.C. Steele, R. Neruda, and M. Karny, editors, *Artificial Neural Networks and Genetic Algorithms*, Computer Science, pages 324–327. Springer, Wien, 2001.

[156] K.E. Parsopoulos and M.N. Vrahatis. Particle swarm optimizer in noisy and continuously changing environments. In M.H. Hamza, editor, *Artificial Intelligence and Soft Computing*, pages 289–294. IASTED/ACTA Press, 2001.

[157] K.E. Parsopoulos and M.N. Vrahatis. Initializing the particle swarm optimizer using the nonlinear simplex method. In A. Grmela and N.E. Mastorakis, editors, *Advances in Intelligent Systems, Fuzzy Systems, Evolutionary Computation*, pages 216–221. WSEAS Press, 2002.

[158] K.E. Parsopoulos and M.N. Vrahatis. Particle swarm optimization method for constrained optimization problems. In P. Sincak, J. Vascak, V. Kvasnicka, and J. Pospichal, editors, *Intelligent Technologies–Theory and Application: New Trends in Intelligent Technologies*, volume 76 of *Frontiers in Artificial Intelligence and Applications*, pages 214–220. IOS Press, 2002.

[159] K.E. Parsopoulos and M.N. Vrahatis. Particle swarm optimization method in multiobjective problems. In *Proceedins of the 2002 ACM Symposium on Applied Computing (SAC 2002)*, pages 603–607, Madrid, Spain, 2002. ACM Press.

[160] K.E. Parsopoulos and M.N. Vrahatis. Computing periodic orbits of non-differentiable / discontinuous mappings through particle swarm optimization. In *Proc. IEEE 2003 Swarm Intelligence Symposium*, pages 34–41, 2003.

[161] K.E. Parsopoulos and M.N. Vrahatis. On the computation of all global minimizers through particle swarm optimization. *IEEE Trans. Evolutionary Comp.*, 8(3):211–224, 2004.

[162] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Lett. A*, 64:821–824, 1990.

[163] S. Peleg and A. Rosenfeld. Breaking substitution ciphers using a relaxation algorithm. *Communications of the ACM*, 22(11):598–605, 1979.

[164] R. Peralta. Simultaneous security of bits in the discrete log. *LNCS*, 219:62–72, 1986.

[165] A. Pincus. Approximation theory of the mlp model in neural networks. *Acta Numerica*, pages 143–195, 1999.

[166] S. C. Pohlig and M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[167] D. Pointcheval. Neural networks and their cryptographic applications. In *In 1994 P. Charpin Ed. INRIA, Livres de resumes EUROCODE'94*, 1994.

[168] D. Pointcheval. A new identification scheme based on the perceptrons problem. *LNCS*, 950:318–328, 1995.

[169] W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery. *Numerical Recipes in Fortran 77*. Cambridge University Press, 1992.

[170] Z. Ramzan. *On Using Neural Networks to Break Cryptosystems*. PhD thesis, Laboratory of Computer Science, MIT, 1998.

[171] S.S. Rao. *Engineering Optimization–Theory and Practice*. Wiley Eastern, New Delhi, 1996.

[172] S.N. Rasband. *Chaotic Dynamics of Nonlinear Systems*. Wiley, New York, 1990.

[173] T. Ray and K.M. Liew. A swarm metaphor for multiobjective design optimization. *Engineering Optimization*, 34(2):141–153, 2002.

[174] I. Rechenberg. *Evolutionsstrategie: Optimierung technischer Systeme nach Prinzipien der biologischen Evolution*. Frommann-Holzboog Verlag, Stuttgart, Germany, 1973.

[175] I. Rechenberg. Evolution strategy. In J.M. Zurada, R.J. Marks II, and C. Robinson, editors, *Computational Intelligence: Imitating Life*. IEEE Press, Piscataway, NJ, 1994.

[176] M. Riedmiller and H. Braun. A direct adaptive method for faster backpropagation learning: The RPROP algorithm. In *IEEE International Conference on Neural Networks*, pages 586–591, 1993.

[177] R. Rivest. Cryptography and machine learning. *LNCS, Advances in Cryptology – ASIACRYPT'91*, 739:427–439, 1993.

[178] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[179] F. Rosenblatt. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological Review*, 65:386–408, 1958.

[180] O.E. Rössler. An equation for continuous chaos. *Phys. Lett. A.*, 57:397–398, 1976.

[181] D. Rumelhart, G. Hinton, and R. Williams. Learning internal representations by error propagation. In *In: D.E. Rumelhart and J.L. McClelland (Eds.) Parallel distributed processing: Explorations in the microstructure of cognition*, volume 1, pages 318–362. MIT Press, 1986.

[182] A. Ruttor, W. Kinzel, and I. Kanter. Neural cryptography with queries. *Journal of Statistical Mechanics*, page P01009, January 2005.

[183] A. Ruttor, W. Kinzel, L. Shacham, and I. Kanter. Neural cryptography with feedback. *Physical Review E*, 69(4):046110–1–046110–7, 2004.

[184] A. Saldam, I. Ahmad, and S. Al-Madani. Particle swarm optimization for task assignment problem. *Microprocessors and Microsystems*, 26:363–371, 2002.

[185] B. Schneier. *Applied Cryptography*. Wiley, New York, second edition, 1996.

[186] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. *LNCS*, 1666:148–164, 1999.

[187] H.-P. Schwefel. *Evolutionsstrategie und numerische Optimierung*. Dr.-ing. thesis, Technical University of Berlin, Dept. of Process Engineering, 1975.

[188] H.-P. Schwefel. *Numerical Optimization of Computer Models*. Wiley, Chichester, 1981.

[189] H.-P. Schwefel. *Evolution and Optimum Seeking*. Wiley, New York, 1995.

[190] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 27(4):656–715, 1949.

[191] Y. Shi and R.C. Eberhart. A modified particle swarm optimizer. In *Proceedings IEEE Conference on Evolutionary Computation*, Anchorage, AK, 1998. IEEE Service Center.

[192] Y. Shi and R.C. Eberhart. Parameter selection in particle swarm optimization. In V.W. Porto, N. Saravanan, D. Waagen, and A.E. Eiben, editors, *Evolutionary Programming*, volume VII, pages 591–600. Springer, 1998.

[193] Y. Shin and J. Ghosh. Realization of boolean functions using binary pi-sigma networks. In *Conference on Artificial Neural Networks in Engineering*, St. Louis, 1991.

[194] I. Shparlinski, editor. *Cryptographic Applications of Analytic Number Theory*. Progress in Computer Science and Applied Logic. Birkhäuser Verlag, 2003.

[195] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[196] M.J. Smith. *Mathematical Ideas in Biology*. Cambridge University Press, London, 1968.

[197] P. Smith and M. Lennon. LUC: A new public key system. In *Proceedings of the Ninth IFIP International Symposium on Computer Security*, pages 103–117, North-Holland, Amsterdam, 1993.

[198] P. Smith and C. Skinner. A public key cryptosystem and a digital signature system based on the Lucas function analogue to the discrete logarithms. *LNCS*, 917:355–364, 1995.

[199] R. Spillman. Cryptanalysis of knapsack ciphers using genetic algorithms. *Cryptologia*, 17(4):367–377, 1993.

[200] R. Spillman, M. Janssen, B. Nelson, and M. Kepner. Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers. *Cryptologia*, 17(1):31–44, 1993.

[201] D. Stinson. *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*. CRC Press, 1995.

[202] R. Storn and K. Price. Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization*, 11:341–359, 1997.

[203] V. Tandon, H. El-Mounayri, and H. Kishawy. Nc end milling optimization using evolutionary computation. *Int. J. Machine Tools & Manufacture*, 42:595–605, 2002.

[204] J. Vaidya and C. Clifton. Privacy preserving association rule mining in vertically partitioned data. In *Proc. of the Eighth ACM SIGKDD International Conference*, Canada, 2002.

[205] C. Vertan and C. Geangala. Breaking the Merkle-Hellman cryptosystem by genetic algorithms: Locality versus performance. In H. Zimmermann, M. Negoita, and D. Dascalu, editors, *Real World Applications of Intelligent Technologies*, pages 201–208. Editura Academiei Romanie, Bucharest, 1996.

[206] G.A. Vignaux and Z. Michalewicz. Genetic algorithms for the transportation problem. In *Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems*, pages 252–259, Amsterdam, 1989. North-Holland.

[207] G.A. Vignaux and Z. Michalewicz. A genetic algorithm for the linear transportation problem. *IEEE Transactions on Systems, Man, and Cybernetics*, 21(2):445–452, 1991.

[208] M. N. Vrahatis, G. A. Tsirogiannis, and E. C. Laskari. Novel orbit based symmetric cryptosystems. *Mathematical and Computer Modelling*, 51(3/4):239–246, 2010. (online version doi:10.1016/j.mcm.2009.08.011).

[209] M.N. Vrahatis. Chabis: A mathematical software package for locating and evaluating roots of systems of nonlinear equations. *ACM Trans. Math. Soft.*, 14(4):330–336, 1988.

[210] M.N. Vrahatis. Solving systems of nonlinear equations using the nonzero value of topological degree. *ACM Trans. Math. Soft.*, 14(4):312–329, 1988.

[211] M.N. Vrahatis. An efficient method for locating and computing periodic orbits of nonlinear mappings. *J. Comp. Phys.*, 119:105–119, 1995.

[212] M.N. Vrahatis, H. Isliker, and T.C. Bountis. Structure and breakdown of invariant tori in a 4–d mapping model of accelerator dynamics. *Inter. J. Bifurc. Chaos*, 7:2707–2722, 1997.

[213] A. L. Wells. A polynomial form for logarithms modulo a prime. *IEEE Trans. Inform. Theory*, IT-30:845–846, 1985.

[214] D. D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, 13(3):1558–1586, 1989.

[215] H. White. Connectionist nonparametric regression: Multilayer feedforward networks can learn arbitrary mappings. *Neural Networks*, 3:535–549, 1990.

[216] A. Winterhof. A note on the interpolation of the Diffie-Hellman mapping. *Bulletin of Australian Mathematical Society*, 64(3):475–477, 2001.

[217] A. Winterhof. Polynomial interpolation of the discrete logarithm. *Des. Codes Cryptogr.*, 25(1):63–72, 2002.

[218] A. Winterhof. A note on the linear complexity profile of the discrete logarithm in finite fields. *Prog. Comput. Sci. Appl. Logic*, 23:359–367, 2004.

[219] T. Yang, L. B. Yang, and C. M. Yang. Cryptanalyzing chaotic secure communications using return maps. *Phys. Lett. A*, 245:495–510, 1998.

[220] T.-W. Yue and S. Chiang. The general neural-network paradigm for visual cryptography. *LNCS, IWANN 2001*, 2084:196–206, 2001.

[221] H. Zhou and X. Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits Syst. I*, 44:268–271, 1997.

Κατάλογος Δημοσιεύσεων Υποψήφιας

Α. Δημοσιεύσεις σε Επιστημονικά Περιοδικά με Σύστημα Κριτών.

1. Laskari, E.C., Parsopoulos, K.E., Vrahatis, M.N., Utilizing Evolutionary Operators in Global Optimization with Dynamic Search Trajectories, *Numerical Algorithms*, vol. 34 (2-4), pp. 393-403, 2003.
2. Laskari, E.C., Meletiou, G.C., Tasoulis, D.K., Vrahatis, M.N., Privacy Preserving Electronic Data Gathering, *Mathematical and Computer Modelling*, vol. 42 (7/8), pp. 739-746, 2005.
3. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Aitken and Neville Inverse Interpolation Methods over Finite Fields, *Applied Numerical Analysis and Computational Mathematics* (ANACM), vol. 2 (1), pp. 100-107, 2005.
4. Laskari, E.C., Meletiou, G.C., Stamatiou, Y.C., Vrahatis, M.N., Evolutionary Computation Based Cryptanalysis: A First Study, *Nonlinear Analysis: Theory, Methods and Applications*, vol. 63, pp. e823-e830, 2005.
5. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Problems of Cryptography as Discrete Optimization Tasks, *Nonlinear Analysis: Theory, Methods and Applications*, vol. 63, pp. e831-e837, 2005.
6. Laskari, E.C., Meletiou, G.C., Tasoulis, D.K., Vrahatis, M.N., Transformations of two cryptographic problems in terms of matrices, *ACM SIGSAM Bulletin*, vol. 39 (4), pp. 127-130, 2005.
7. Laskari, E.C., Meletiou, G.C., Tasoulis, D.K., Vrahatis, M.N., Studying the performance of artificial neural networks on problems related to cryptography, *Nonlinear Analysis Series B: Real World Applications*, vol. 7, pp. 937-942, 2006.
8. Laskari, E.C., Meletiou, G.C., Stamatiou, Y.C., Vrahatis, M.N., Applying Evolutionary Computation Methods for the Cryptanalysis of Feistel Ciphers, *Applied Mathematics and Computation*, vol. 184, pp. 63-72, 2007.
9. Laskari, E.C., Meletiou, G.C., Stamatiou, Y.C., Tasoulis, D.K., Vrahatis, M.N., Assessing the Effectiveness of Artificial Neural Networks on Problems Related to Elliptic Curve Cryptography, *Mathematical and Computer Modelling*, vol. 46, pp. 174-179, 2007.
10. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Aitken and Neville inverse interpolation methods for the Lucas logarithm problem. *Applied Mathematics and Computation*, 209(1), pp. 52-56, 2009.
11. Vrahatis, M.N., Tsirogiannis, G.A., Laskari, E.C., Novel Orbit Based Symmetric Cryptosystems, *Mathematical and Computer Modelling*, 51(3/4), pp. 239-246, 2010, (online version doi:10.1016/j.mcm.2009.08.011).

Β. Άρθρα και Κεφάλαια σε Βιβλία με Σύστημα Κριτών.

1. Laskari E.C., Meletiou G.C., Stamatiou Y.C. and Vrahatis M.N., Cryptography and cryptanalysis through computational intelligence, In: Computational Intelligence in Information Assurance and Security, N. Nedjah, A. Abraham, L. de

Macedo Mourelle (Eds.), Book Series: *Studies in Computational Intelligence*, vol. 57, Chapter 1, pp.1-49, Springer Verlag, Berlin / Heidelberg, Germany, May 4, 2007, ISBN: 978-3-540-71077-6.

2. Parsopoulos, K.E., Laskari, E.C., Vrahatis, M.N., Solving L1 Norm Errors-In-Variables Problems Using Particle Swarm Optimizer, M.H. Hamza (ed.), *Artificial Intelligence and Applications*, pp. 185-190, IASTED/ACTA Press (Anaheim, CA, USA), 2001, ISBN: 0-88986-301-6, ISSN: 1482-7913.
3. Tasoulis, D.K., Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Privacy preserving unsupervised clustering over vertically partitioned data, M. Gavrilova et al. (Eds.), 2006 International Conference on Computational Science and Its Appications - ICCSA 2006, *Lecture Notes in Computer Science* series, vol. 3984, pp. 635-643, 2006.

Γ. Δημοσιεύσεις σε Διεθνή Επιστημονικά Συνέδρια με Σύστημα Κριτών.

1. Laskari, E.C., Parsopoulos, K.E., Vrahatis, M.N., Particle Swarm Optimization for Integer Programming, *Proceedings of the 2002 IEEE Congress on Evolutionary Computation*, pp. 1582-1587, ISBN: 0-7803-7278-6, ISSN: 1098-7576, IEEE Catalog Number: 02CH37290.
2. Laskari, E.C., Parsopoulos, K.E., Vrahatis, M.N., Particle Swarm Optimization for Minimax Problems, *Proceedings of the IEEE 2002 Congress on Evolutionary Computation*, pp. 1576-1581, ISBN: 0-7803-7278-6, ISSN: 1098-7576, IEEE Catalog Number: 02CH37290.
3. Parsopoulos, K.E., Laskari, E.C., Vrahatis, M.N., Particle Identification by Light Scattering through Evolutionary Algorithms, First International Conference for Mathematics and Informatics for Industry (MII 2003), Thessaloniki, Greece, pp. 97-108, 2003.
4. Laskari, E.C., Meletiou, G.C., Tasoulis, D.K., Vrahatis, M.N., Data Mining and Cryptology, *Proceedings of the International Conference of Computational Methods in Sciences and Engineering 2003* (ICCMSE 2003), T.E. Simos (ed.), Kastoria, Greece, pp. 346-349, World Scientific Publishing, 2003, ISBN: 981-238-595-9.
5. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., The Discrete Logarithm Problem as an Optimization Task: A First Study, *Proceedings of the IASTED International Conference on Artificial Intelligence and Applications (AIA 2004)*, Innsbruck, Austria, ACTA Press, vol. 2, pp. 817-822, ISBN: 0-88986-375-X, ISSN: 1027-2666 (IASTED 2004).
6. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Recent Approaches to Electronic Data Gathering with Privacy, *Proceedings of the 1st International Conference "From Scientific Computing to Computational Engineering"* (IC-SCCE), Athens, Greece, 2004.
7. Laskari, E.C., Meletiou, G.C., Vrahatis, M.N., Utilizing Evolutionary Computation Methods for the Design of S-boxes, *Proceedings of the International Conference on Computational Intelligence and Security 2006* (CIS 2006), IEEE Press, vol. 2, pp. 1299-1302, 2006, ISBN: 1-424 4-0605-6.
8. Laskari, E.C., Meletiou, Stergiou E., Vrahatis M.N., Electronic Evaluation in Open and Distance Education, *Proceedings of 3rd International Conference on Open and Distance Learning* (ICODL 2005), 2005.

9. Galanis V.I., Laskari E.C., Meletiou G.C., Vrahatis M.N., E-evaluation in Open and Distance Learning Environments, *Proceedings of the International Conference on Information Technologies* (InfoTech 2009), pp. 28-33, 2009.

Δ. Αναφορές από άλλους ερευνητές.

1. Για την εργασία Α.1
   (α′) Hu X.-H., A bibliography of Particle Swarm Optimization, Department of Electrical and Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN, U.S.A. Available on-line at: http:// w-eb.ics.purdue.edu/ hux/bibliography.shtml (Updated 07/ 02/2003).
   (β′) Chandila P.K., Agarwal H. and Renaud J.E., An efficient strategy for global optimization using local Kriging approximations, In: *Collection of Technical Papers of the 45th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, April 19-22, 2004, Palm Springs, California, U.S.A., Vol. 5, pp.3860-3882, 2004.
   (γ′) Chen X., O'Neill K., Barrowes B.E., Grzegorczyk T.M. and Kong J.A., Application of a spheroidal mode approach and differential evolution algorithm in inversion of magneto-quasistatic data for UXO discrimination, Inverse Problems, 20, No. 6, pp.S27-S40, December 2004.
   (δ′) Chandila P.K., Strategy for global optimization and post-optimality using local Kriging approximations, *Thesis for the Degree of Master of Science*, Department of Aerospace and Mechanical Engineering, University of Notre Dame, Notre Dame, Indiana, U.S.A., April 2004.
   (ε′) Neumaier A., Online papers in global optimization, August 9, 2004. Available on-line at: http://www.mat.univie.ac.at/ neum/glopt/mss/ gloptpapers.html
   (ϛ′) Rashed R. and Houzel C., Recherche et enseignement des mathematiques au IXe siuecle: Le recueil de propositions geometriques de Naim ibn Musa, Les cahiers du Mideo num. 2, Peeters, Leuven,Belgique, 2004.
   (ζ′) Chen X.-D., Inverse problems in electromagnetics, *Ph.D. thesis*, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, U.S.A., May 2005.
   (η′) Fraga E.S., Hybrid methods for optimisation, In: *Computer Aided Methods for Optimal Designand Operations*, J. Zilinskas and I.D.L. Bogle (Eds.), pp.1-14, World Scientific, New Jersey, U.S.A., 2006 [ISBN: 981256909X].
   (ϑ′) He Y., Wang X. and Kou Y., A binary differential evolution algorithm with hybrid encoding, *Computer Research and Development*, 44, No. 9, pp.1476 - 1484, September 2007.
   (ι′) Dimopoulos Y., Likothanasis S. and Stergiou K., Constraint satisfaction and search, AI Research in Greece, Hellenic Artificial Intelligence Society (EETN), July 2008. Available on-line at: http://www.eetn.gr/english/ main frame page en.htm
   (ια′) Ditthakit P. and Chittaladakorn S., Optimal coastal gate operation method through simulation-optimization approach, Kasetsart *Journal Natural Science*, 42, No. 1, pp.177-190, January 2008.
   (ιβ′) Tang G.-F., Yu L., Zhang G.-J. and Huang H., Design and implementation of hybrid genetic algorithm based on dynamic search trajectories, *Journal of Zhejiang University of Technology*, 36, No. 2, pp.1-4, April 2008.

(ιγ′) Snyman J.A. and Kok S., A reassessment of the Snyman-Fatti dynamic search trajectory method for unconstrained global optimization, *Journal of Global Optimization*, 43, No. 1, pp.67-82, January 2009.

2. Για την εργασία Α.2

(α′) Hu X.-H., A bibliography of Particle Swarm Optimization, Department of Electrical & Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN, U.S.A. Available on-line at: http://web.ics. purdue.edu/ hux/bibliography.shtml (Updated 07/ 02/2003).

(β′) Pei C.-H., Information service, Institute of Finance and Trade Economics, Chinese Academy of Social Sciences (CASS), Beijing, China, May 2007. Available on-line at: http://cms.cass.cn/showNews e.asp?id=12547

(γ′) Mohaisen A., Privacy preserving technologies: Extended bibliography, Electronics and Telecom Research Institute (ETRI), Information Security Research Division, Daejeon, Republic of Korea, 2008. Available on-line at: http://mohaisen.net/pdf/BETbibLong.pdf.

3. Για την εργασία Α.3

(α′) Hu X.-H., A bibliography of Particle Swarm Optimization, Department of Electrical & Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN, U.S.A. Available on-line at: http://web.ics. purdue.edu/ hux/bibliography.shtml (Updated 07/ 02/2003). Dissertation, Vol. 2, Issue 1, 2008.

(β′) Ferrer Moreno E., Acceleration of finite field arithmetic with an application to reverse engineering genetic networks, *Ph.D. Thesis* in Computing and Information Sciences and Engineering, University of Puerto Rico, Mayaguez Campus, Puerto Rico, May 2008, Journal of Dissertation, Vol. 2, Issue 1, 2008.

4. Για την εργασία Α.4

(α′) Hu X.-H., A bibliography of Particle Swarm Optimization, Department of Electrical & Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN, U.S.A. Available on-line at: http://web.ics. purdue.edu/ hux/bibliography.shtml (Updated 07/ 02/2003). Dissertation, Vol. 2, Issue 1, 2008.

(β′) Dimopoulos Y., Likothanasis S. and Stergiou K., Constraint satisfaction and search, AI Research in Greece, Hellenic Artificial Intelligence Society (EETN), July 2008. Available on-line at: http://www.eetn.gr/english/ main frame page en.htm

(γ′) Uddin M.F. and Youssef A.M., Cryptanalysis of simple substitution ciphers using particle swarm optimization, In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (CEC2006), July 16-21, 2006, Vancouver, B.C., Canada, art. no. 1688376, pp.677-680, IEEE 2006.

(δ′) Song J., Zhang H.-G., Meng Q.-S. and Wang Z.-G., Cryptanalysis of two-round DES using genetic algorithms, *Lecture Notes in Computer Science*, 4683, pp.583-590, 2007.

(ε′) Song J., Zhang H.-G., Meng Q.-S. and Wang Z.-G., Cryptanalysis of four-round DES based on genetic algorithm, In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (WiCOM 2007), September 21-25, 2007, Shanghai, art. no. 4340355, pp.2326-2329, IEEE 2007.

(ϛ′) Uddin M.F. and Youssef A.M., Cryptanalysis of Pointcheval's identification scheme using ant colony optimization, In: *Proceedings of the 2007*

IEEE Congress on Evolutionary Computation, (CEC2007), D. Srinivasan and L. Wang, (Eds.), September 25-28, 2007, Singapore, art. no. 4424846, pp.2942-2947, IEEE 2007.

(ζ′) Song J., Yang F., Wang M. and Zhang H., Cryptanalysis of transposition cipher using simulated annealing genetic algorithm, *Lecture Notes in Computer Science*, (LNCS), 5370, pp.795-802, 2008.

(η′) Yang F., Song J. and Zhang H., Quantitative cryptanalysis of six-round DES using evolutionary algorithms, *Lecture Notes in Computer Science*, (LNCS), 5370, pp.134-141, 2008.

(ϑ′) Shahzad W., Siddiqui A.B. and Khan F.A., Cryptanalysis of four-rounded DES using binary particle swarm optimization, In: *Proceedings of the 11th Annual conference on Genetic and evolutionary computation*, (GECCO 2009), July 8-12, 2009, Montreal, Quebec, Canada, pp.2161-2166, ACM 2009.

5. Για την εργασία Α.5

(α′) Hu X.-H., A bibliography of Particle Swarm Optimization, Department of Electrical & Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN, U.S.A. Available on-line at: http://web.ics.purdue.edu/ hux/bibliography.shtml (Updated 07/ 02/2003).

(β′) Uddin M.F. and Youssef A.M., Cryptanalysis of simple substitution ciphers using particle swarm optimization, In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (CEC2006), July 16-21, 2006, Vancouver, B.C., Canada, art. no. 1688376, pp.677-680, IEEE 2006.

(γ′) Uddin M.F. and Youssef A.M., Cryptanalysis of Pointcheval's identification scheme using ant colony optimization, In: *Proceedings of the 2007 IEEE Congress on Evolutionary Computation*, (CEC2007), D. Srinivasan and L. Wang, (Eds.), September 25-28, 2007, Singapore, art. no. 4424846, pp.2942-2947, IEEE 2007.

(δ′) Huang Y.-R., Problems of cryptography as discrete optimization tasks, Soft Computing at Organization Performance Laboratory, Department of Mathematics, Shanghai University, Shanghai, China, March 20, 2006.

(ε′) Redi J., Tecniche di computational intelligence per la fattorizzazione di numeri grandi, Tesi di laurea magistrale, Corso di Laurea in Ingengeria Elettronica, Dipartimento di Ingegeria, Biofisica ed Elettronica, Facoltua di Ingegeria, Universitua degli Studi di Genova, Genova, Italia, 24 Luglio 2006.

(ϛ′) Nalini N. and Rao G.R., Attacks of simple block ciphers via efficient heuristics, *Information Sciences*, 177, No. 12, pp.2553-2569, June 2007.

(ζ′) Qing A., Differential Evolution: Fundamentals and Applications in Electrical Engineering, WILEY, 2009, ISBN 978-0-470-82392-7.

6. Για την εργασία Α.7

(α′) Redi J., Tecniche di computational intelligence per la fattorizzazione di numeri grandi, Tesi di laurea magistrale, Corso di Laurea in Ingengeria Elettronica, Dipartimento di Ingegeria, Biofisica ed Elettronica, Facoltua di Ingegeria, Universitua degli Studi di Genova, Genova, Italia, 24 Luglio 2006.

(β′) Kanta A.F., Planche M.P., Montavon G. and Coddet C., Modeling of the in-flight particles characteristics using neural networks and analytical model, In: *Thermal spray 2007: Global coating solutions*, B.R. Marple, M.M.

Hyland, Y.C. Lau, R.S. Lima and G. Montavon, (Eds.), ASM International, Materials Park, Ohio, U.S.A., pp.173-178, 2007.

(γ′) Wilson A., The Dark Side of the Flat World - Emerging SOA security standards, challenges and opportunities for the federal sector, Chapter: *SOA Security and Cryptography*, pp.24-39, Leading Edge Forum, El Segundo, CA, U.S.A., 2007.

(δ′) Mostafa M.M., Profiling organ donors in Egypt using intelligent modeling techniques, *Marketing Intelligence and Planning*, 26, No. 2, pp.166-188, 2008.

(ε′) Wilson A., The dark side of the Flat world: Emerging SOA security standards, challenges and opportunities for the federal sector, Leading Edge Forum, CSC.COM, Consulting Systems Integration Outsourcing, Experience Results, 2008.

(ϛ′) Kanta A.-F., Planche M.-P., Montavon G. and Coddet C., In-flight and upon impact particle characteristics modelling in plasma spray process, Surface and Coatings Technology, in press, 2009.

(ζ′) Mostafa M.M., A probabilistic neural network approach for modelling and classifying efficiency of GCC banks, *International Journal of Business Performance Management*, 11, No. 3, pp.236-258, April 2009.

(η′) Mostafa M.M., Profiling blood donors in Egypt: A neural network analysis, *Expert Systems with Applications*, 36, No. 3, pp.5031-5038, April 2009.

(ϑ′) Mostafa M.M., Modeling the efficiency of top Arab banks: A DEA-neural network approach, *Expert Systems with Applications*, 36, No. 1, pp.309-320, January 2009.

(ι′) Mostafa M.M., Modeling the competitive market efficiency of Egyptian companies: A probabilistic neural network analysis, *Expert Systems with Applications*, 36, No. 5, pp.8839-8848, July 2009.

(ια′) Mostafa M.M. and Billor N., Recognition of western style musical genres using machine learning techniques, *Expert Systems with Applications*, 36, No. 8, pp.11378-11389, October 2009.

(ιβ′) Mostafa M.M. and Nataraajan R., A neuro-computational intelligence analysis of the ecological footprint of nations, *Computational Statistics and Data Analysis*, 53, No. 9, pp.3516-3531, July 2009.

(ιγ′) Zhang C., Kanta A.-F., Li C.-X., Li C.-J., Planche M.-P., Liao H. and Coddet C., Effect of in-flight particle characteristics on the coating properties of atmospheric plasma-sprayed 8 mol% Y2O3-ZrO2 electrolyte coating studying by artificial neural networks, *Surface and Coatings Technology*, 204, No. 4, pp.463-469, November 2009.

(ιδ′) Zhang G., Kanta A.-F., Li W.-Y., Liao H. and Coddet C., Characterizations of AMT-200 HVOF NiCrAlY coatings, *Materials and Design*, 30, No. 3, pp.622-627, March 2009.

(ιε′) Kotlarz P., Neural Networks for Solving Cryptology Problems, *Ph.D. Thesis*, Institute of Fundamental Technological Research, Polish Academy of Sciences, (IPPT-PAN), Warsaw, Poland, 2008.

7. Για την εργασία Α.8

(α′) Muthuregunathan R., Venkataraman D. and Rajasekaran P., Cryptanalysis of knapsack cipher using parallel evolutionary computing, *International Journal of Recent Trends in Engineering*, 1, No. 1, pp.260-263, May 2009.

8. Για την εργασία Α.9

(α′) Ling C. (Supervisor), Bean A., Dai W., Garland R., Macbeth S., Del Castillo M.S., Selva-ratnarajah S. and Zammit M., History of Cryptography, An ISE2 Project, Imperial College London, February 2008 Available on-line at: www2.ee.imperial.ac.uk/andrew.bean06/yr2proj

9. Για την εργασία B.1

(α′) Ou C.M., Ou, C.R., Multi-Agent Artificial Immune Systems (MAAIS) for Intrusion Detection: Abstraction from Danger Theory, KES-AMSTA 2009, *LNAI* 5559, pp. 11-19, Springer-Verlag 2009.

(β′) Kotlarz P., Neural Networks for Solving Cryptology Problems, *Ph.D. Thesis*, Institute of Fundamental Technological Research, Polish Academy of Sciences, (IPPT-PAN), Warsaw, Poland, 2008.

10. Για την εργασία B.2

(α′) Buckner M.A., Learning from data with localized regression and differential evolution, *Ph.D. Dissertation*, Nuclear Engineering Department, The University of Tennessee, Knoxville, U.S.A., May 2003.

(β′) Fieldsend J.E., Novel algorithms for multi-objective search and their application in multi-objective evolutionary neural network training, *Ph.D. Thesis* in Computer Science, University of Exeter, Exeter, U.K., June 2003.

(γ′) Fealko D.R., Evaluating particle swarm intelligence techniques for solving university examination timetabling problems, *Ph.D. Dissertation*, Graduate School of Computer and Information Sciences, Nova Southeastern University, Florida, U.S.A., August 2005.

(δ′) Schwaab M.. Biscaia E.Ch. Jr., Monteiro J.L. and Pinto J.C., Nonlinear parameter estimation through particle swarm optimization, *Chemical Engineering Science*, 63, No. 6, pp.1542-1552, March 2008.

(ε′) Stiros S.C. and Pirazzoli P.A., Direct determination of tidal levels for engineering applications based on biological observations, *Coastal Engineering*, 55, No. 6, pp.459-467, June 2008.

(ϛ′) Stiros S., Psimoulis P. and Kokkinou E., Errors introduced by fluctuations in the sampling rate of automatically recording instruments: Experimental and theoretical approach, *Journal of Surveying Engineering*, 134, No. 3, pp.89-93, August 2008.

(ζ′) Prata D.M., Schwaab M., Lima E.L. and Pinto J.C., Nonlinear dynamic data reconciliation and parameter estimation through particle swarm optimization: Application for an industrial polypropylene reactor, *Chemical Engineering Science*, 64, No. 18, pp.3953- 3967, September 2009.

11. Για την εργασία B.3

(α′) Mohaisen A., Privacy preserving technologies: Extended bibliography, Electronics and Telecom Research Institute (ETRI), *Information Security Research Division*, Daejeon, Republic of Korea, 2008.

(β′) Mutanen T., Consumer data and privacy in ubiquitous computing, Master's thesis for the degree of Master of Science in Technology, Department of Engineering Physics and Mathematics, Helsinki University of Technology, Espoo, Finland, January 11, 2007.

(γ′) Mutanen T., Consumer data and privacy in ubiquitous computing, VTT Publications 647, VTT Technical Research Centre of Finland, Espoo, Finland, June 21, 2007 [ISBN 978-951-38-7031-7]

(δ′) Hsieh P.-Y., A study of some privacy-preserving clustering schemes, Master's Thesis, College of Electrical Engineering and Computer Science, National Taiwan University, Taiwan, Republic of China, 2008.

(ε′) Kadampur M.A., Somayajulu D.V.L.N., Dhiraj S.S.S. and Satyam S.G.P., Privacy preserving clustering by cluster bulging for information sustenance, In: *Proceedings of the 4th International Conference on Information and Automation for Sustainability*, (ICIAFS 2008), December 12-14, 2008, Kharagpur, India, art. no. 4783947, pp.240-246, IEEE Press 2008.

(ϛ′) Wu X., Yue D., Liu F., Chu C., Distributed Model Based Sampling Technique for Privacy Preserving Clustering, 14th International Conference on Management Science & Engineering, August 20-22, Harbin, P.R.China, 2007.

12. Για την εργασία Γ.1

(α′) Fealko D.R., Evaluating particle swarm intelligence techniques for solving university examination timetabling problems, *Ph.D. Dissertation*, Graduate School of Computer and Information Sciences, Nova Southeastern University, Florida, U.S.A., August 2005.

(β′) Boeringer D.W., Multi-objective particle swarm optimization of a modified Bernstein polynomial for curved phased array synthesis using Bezier curves, surfaces, and volumes, *Ph.D. Thesis* in Electrical Engineering, Department of Electrical Engineering, College of Engineering, The Graduate School, The Pennsylvania State University, University Park, PA, U.S.A., August 2004.

(γ′) Boeringer D.W. and Werner D.H., Particle swarm optimization versus genetic algorithms for phased array synthesis, *IEEE Transactions on Antennas and Propagation*, 52, No. 3, pp.771-779, March 2004.

(δ′) Ratnaweera A., Halgamuge S.K. and Watson H.C., Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients, *IEEE Transactions on Evolutionary Computation*, 8, No. 3, pp. 240-255, June 2004.

(ε′) Wetter M., GenOpt Generic Optimization Program, User Manual Version 2.0.0, Technical Report LBNL-54199, Simulation Research Group, Building Technologies Department, Environmental Energy Technologies Division, Lawrence Berkeley National Laboratory, Berkeley, CA 94720, U.S.A., January 5, 2004.

(ϛ′) Boeringer D.W. and Werner D.H., Efficiency-constrained particle swarm optimization of a modified Bernstein polynomial for conformal array excitation amplitude synthesis, *IEEE Transactions on Antennas and Propagation*, 53, No. 8, pp.2662-2673, August 2005.

(ζ′) Engelbrecht A.P., Fundamentals of Computational Swarm Intelligence, John Wiley and Sons Ltd, Chichester, England, November 4, 2005 [ISBN: 0-470-09191-6].

(η′) Ifeachor E.C., Artificial Intelligence: Particles Swarm Optimisation Links: Papers, Signal Processing and Multimedia Communication (SPMC) research Group, School of Computing, Communications and Electronics Faculty of Technology, University of Plymouth, Plymouth, United Kingdom, May 4, 2005

(ϑ′) Acan A., Unveren A. and Bodur M., The latest vs. averaged recent experience: which better guides a PSO algorithm? In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (CEC2006), July 16-21, 2006, Vancouver, B.C., Canada, pp.414-419, IEEE 2006.

(ι′) Li X., Utilising restricted for-loops in genetic programming, *Ph.D. Thesis*, School of Computer Science and Information Technology, Faculty of

Applied Science, Royal Melbourne Institute of Technology, Melbourne, Victoria, Australia, February 2007.

(ια′) Gao H.M., Tan Y. and Zeng J.C., Cooperative particle swarm optimization for steel making scheduling, *Journal of Systems Engineering*, 23, No. 4, pp.466-471, 2008.

(ιβ′) Ifeachor E.C., Particle swarm optimization papers, Signal Processing and Multimedia Communication (SPMC) research Group, School of Computing, Communications and Electronics, Faculty of Technology, University of Plymouth, Plymouth, United Kingdom, January 2008.

(ιγ′) Acan A. and Unveren A., A memory-based colonization scheme for particle swarm optimization, In: *Proceedings of the IEEE Congress on Evolutionary Computation*, (CEC 2009), May 18-21, 2009, Trondheim, Norway, art. no. 4983181, pp.1965-1972, IEEE 2009.

(ιδ′) Herrera O.E., Nuno L. and Diaz-Morcillo A., Shaping an antenna radiation diagram with discrete weights using the PSO algorithm and periodic and nest spaces, *Mathematical and Computer Modelling*, 50, No. 5-6, pp.840-848, September 2009.

(ιε′) Wetter M., GenOpt (R): Generic Optimization Program, User Manual Version 3.0.0, Simulation Research Group, Building Technologies Department, Environmental Energy Technologies Division, Lawrence Berkeley National Laboratory, Berkeley, California, U.S.A., pp.1-104, May 4, 2009.

(ιϝ′) Yeh L.-W., Optimal procurement policies for multi-product multi-supplier with capacity constraintand price discount, (in Chinese), The DHL Thesis Award in Supply Chain Management (SCM),Global Logistics Lab, Department of Industrial Engineering and Management, Institute of Industrial Engineering and Management, Yuan-Ze University, Taoyuan County, Taiwan, July 2003.

(ιζ′) Chang B.C.H., Ratnaweera A., Halgamuge S.K. and Watson H.C., Particle swarm optimisation for protein Motif discovery, *Genetic Programming and Evolvable Machines*, 5, No. 2, pp.203-214, June 2004.

(ιη′) Gomez-Cabrero D. and Ranasinghe D.N., Fine-tuning the ant colony system algorithm through particle swarm optimization, Technical Report No. TR07-2005, Departamento de Estadistica e Investigacion Operativa, Universitat de Valencia, Burjassot, Spain, December 2005.

(ιϑ′) Gomez-Cabrero D. and Ranasinghe D.N., Fine-tuning the ant colony system algorithm through particle swarm optimization, In: *Proceedings of the IEEE International Conference on Information and Automation*, December 15-18, 2005, Colombo, Sri Lanka, 2005.

(κ′) Li Y., Yao D., Yao J. and Chen W., A particle swarm optimization algorithm for beam angle selection in intensity-modulated radiotherapy planning, *Physics in Medicine and Biology*, 50, No. 15, pp.3491-3514, August 2005.

(κα′) Park J.W., Park S.H., Moon J.J., Yoon Y. and Kim S.J., High-fidelity simulation-based optimum design utilizing computing grid technology, In: *Collection of Technical Papers of the 46th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference*, Austin, Texas, April 18-21, 2005, Vol. 9, pp. 6234-6245, 2005.

(κβ′) Sedlaczek K. and Eberhard P., Constrained particle swarm optimization of mechanical systems, In: *Proceedings of the Sixth World Congresses of Structural and Multidisciplinary Optimization*, May 30 - June 03, 2005, Rio de Janeiro, Brazil, pp.1-10, 2005.

(κγ′) Amer-Baig M.M., Optimization of ideal reactive distillation column using hybrid PSO algorithm, Master of Science Degree, Department of Electrical Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, January 2006.

(κδ′) Del Valle Y., Hernandez J.C., Venayagamoorthy G.K. and Harley R.G., Optimal STATCOM sizing and placement using particle swarm optimization, In: *Proceedings of the IEEE/PES Transmission and Distribution Conference and Exposition: Latin American*, (TDC 2006), August 15-18, 2006, Caracas, Venezuela, pp.1-6, IEEE 2006.

(κε′) Del Valle Y., Hernandez J.C., Venayagamoorthy G.K. and Harley R.G., Multiple STATCOM allocation and sizing using particle swarm optimization, In: *Proceedings of the Power Systems Conference and Exposition*, (PSCE 2006), October 29-November 1, 2006, Atlanta, Georgia, U.S.A., art. no. 4076026, pp.1884-1891, IEEE 2006.

(κϛ′) Gao Y.-L., Xu C.-X. and Li J., Linear programming relax-PSO hybrid bound algorithm for a class of nonlinear integer programming problems, In: *Proceedings of the IEEE International Conference on Computational Intelligence and Security*, (CIS 2006), November 3-6, 2006, Guangzhou, China, Vol. 1, art. no. 4072111, pp.380-383, IEEE 2006.

(κζ′) Gomez-Cabrero D., Armero C. and Ranashinge D.N., A new meta-heuristic framework: A- B - Domain, Technical Report No. TR01-2006, Departamento de Estadistica e Investigacion Operativa, Universitat de Valencia, Spain, May 12, 2006.

(κη′) Hendtlass T., A particle swarm algorithm for complex quantised problem spaces, In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (CEC 2006), July 16-21, 2006, Vancouver, B.C., Canada, pp.1015-1019, IEEE 2006.

(κϑ′) Huang K.-W., Hybrid evolutionary approach for the cellular phone stations allocation problems, Thesis for the Degree of Master of Science in Industrial Engineering and Management, Institute of Industrial Engineering and Management, National Formosa University, Huwei, Yunlin, Taiwan, Republic of China, June 2006.

(λ′) Sedlaczek K. and Eberhard P., Using augmented Lagrangian particle swarm optimization for constrained problems in engineering, *Structural and Multidisciplinary Optimization*, 32, No. 4, pp.277-286, October 2006.

(λα′) Yang Q.-Y., Sun J.-G., Zhang J.-Y. and Wang C.-J., A hybrid particle swarm optimization for binary CSPs, *Lecture Notes in Computer Science*, (LNBI), 4115, pp.39-49, 2006.

(λβ′) Yang Q.-Y., Sun J.-G., Zhang J.-Y. and Wang C.-J., A hybrid discrete particle swarm algorithm for hard binary CSPs, *Lecture Notes in Computer Science*, (LNCS), 4222, pp.184-193, 2006.

(λγ′) Zhao M., PSO resources collection, Zijin Communications, Chongqing Institute of Posts and Telecommunications, Chongqing, Sichuan, People's Republic of China. October 16, 2006.

(λδ′) Ai T.J. and Kachitvichyanukul V., Dispersion and velocity indices for observing dynamic behaviour of particle swarm optimization, In: *Proceedings of the 2007 IEEE Congress on Evolutionary Computation*, (CEC 2007), D. Srinivasan and L. Wang, (Eds.), September 25-28, 2007, Singapore, art.no. 4424891, pp.3264-3271, IEEE 2007.

(λε′) Anthonissen C.A., A population-based approach to sequential ordering problems, Master of Science Thesis, Department of Industrial Engineering, Stellenbosch University, Stellenbosch, South Africa, March 2007.

(λϝ′) Banks A., Vincent J. and Anyakoha C., A review of particle swarm optimization. Part I: background and development, *Natural Computing*, 6, No. 4, pp.467-484, December 2007.

(λζ′) Breaban M., Ionita M. and Croitoru C., A new PSO approach to constraint satisfaction, In: *Proceedings of the 2007 IEEE Congress on Evolutionary Computation*, (CEC 2007), D. Srinivasan and L. Wang, (Eds.), September 25-28, 2007, Singapore, art. no. 4424712, pp.1948-1954, IEEE 2007.

(λη′) Chan F.T.S., Kumar V. and Mishra N., A CMPSO algorithm based approach to solve the multiplant supply chain problem, In: *Swarm Intelligence: Focus on Ant and Particle Swarm Optimization*, F.T.S. Chan and M.K. Tiwari, (Eds.), Chapter 25, pp.447-474, Itech Education and Publishing, Vienna, Austria, December 2007, [ISBN: 978-3-902613-09-7].

(λϑ′) Engelbrecht A.P., Computational intelligence: An introduction, Second Edition, John Wiley & Sons, Ltd., Chichester, England, 2007. [ISBN: 978-0-470-03561-0 (HB)]

(μ′) Gao H.-M. and Zeng J.-C., Cooperative particle swarm optimization for steel making scheduling, In: *Proceedings of the 2007 Third International Conference on Natural Computation*, (ICNC 2007), August 24-27, 2007, Haikou, Hainan, China, Vol. 4, art. no. 4344729, pp.522-526, IEEE 2007.

(μα′) Gao Y.-L., Ren Z.-H. and Xu C.-X., A branch and bound-PSO hybrid algorithm for solving integer separable concave programming problems, *Applied Mathematical Sciences*, 1, No. 11, pp.517-525, 2007.

(μβ′) Gao Y.-L., Xu C.-X. and Li J., Linear programming relax-PSO hybrid bound algorithm for a class of nonlinear integer programming problems, *Lecture Notes in Computer Science*, (LNAI), 4456, pp.29-35, 2007.

(μγ′) Omran M.G.H. and Engelbrecht A.P., Differential evolution for integer programming problems, In: *Proceedings of the 2007 IEEE Congress on Evolutionary Computation*, (CEC 2007), D. Srinivasan and L. Wang, (Eds.), September 25-28, 2007, Singapore, art. no. 4424749, pp.2237-2242, IEEE 2007.

(μδ′) Omran M.G.H., Engelbrecht A.P. and Salman A., Barebones particle swarm for integer programming problems, In: *Proceedings of the 4th IEEE Swarm Intelligence Symposium*, (SIS 2007), April 1-5, 2007, Honolulu, Hawaii, U.S.A., art. no. 4223171, pp.170-175, IEEE 2007.

(με′) Sedlaczek K. and Eberhard P., Augmented Lagrangian particle swarm optimization in mechanism design, *Journal of System Design and Dynamics*, 1, No. 3, pp.410-421, 2007.

(μϝ′) Xu Y.-C. and Xiao R.-B., An improved binary particle swarm optimizer, *Pattern Recognition and Artificial Intelligence*, 20, No. 6, pp.788-793, 2007.

(μζ′) Yare Y. and Venayagamoorthy G.K., Optimal scheduling of generator maintenance using modified discrete particle swarm optimization, In: *Proceedings of the 2007 IEEE iREP Symposium- Bulk Power System Dynamics and Control - VII, Revitalizing Operational Reliability*, (IREP 2007), August 19-24, 2007, Charleston, SC, U.S.A., art. no. 4410521, pp.1-8, IEEE 2007.

(μη′) Zhang G.-F., Jiang J.-G., Qi M.-B. and Su Z.-P., Solutions of nonlinear multilevel programming based on particle swarm optimization, *Pattern*

Recognition and Artificial Intelligence, 20, No. 6, pp.745-750, 2007.

(μθ′) Zhang H.-Z. and Gao Z.-Y., Two-way road network design problem with variable lanes, *Journal of Systems Science and Systems Engineering*, 16, No. 1, pp.50-61, March 2007.

(ν′) Zhang X.-W. and Liu S.-Y., A new interval-genetic algorithm, In: *Proceedings of the 2007 Third International Conference on Natural Computation*, (ICNC 2007), August 24-27, 2007, Haikou, Hainan, China, Vol. 4, art. no. 4344668, pp.193-197, IEEE 2007.

(να′) Zhang Z.-H., Hu W.-D. and Yu W.-X., Design of quantized amplitude weights for low sidelobe phased array antennas, *Acta Electronica Sinica*, 35, No. 3, pp.580-584, 2007.

(νβ′) Del Valle Y., Venayagamoorthy G.K., Mohagheghi S., Hernandez J.-C. and Harley R.G., Particle swarm optimization: Basic concepts, variants and applications in power systems, *IEEE Transactions on Evolutionary Computation*, 12, No. 2, pp.171-195, April 2008.

(νγ′) Omran M.G.H. and Mahdavi M., Global-best harmony search, *Applied Mathematics and Computation*, 198, No. 2, pp.643-656, May 2008.

(νδ′) Tsai C.-Y. and Yeh S.-W., A multiple objective particle swarm optimization approach for inventory classification, *International Journal of Production Economics*, 114, No. 2, pp.656-666, August 2008.

(νε′) Yasuda K., Iwasaki N., Ueno G. and Aiyoshi E., Particle swarm optimization: A numerical stability analysis and parameter adjustment based on swarm activity, *IEEE Transactions on Electrical and Electronic Engineering*, 3, No. 6, pp.642-659, November 2008.

(νϝ′) Anvari M., Mehrabad M.S. and Barzinpour F., Machine-part cell formation using a hybrid particle swarm optimization, *The International Journal of Advanced Manufacturing Technology*, in press, 2009

(νζ′) Chen R.-M., Shiau D.-F. and Lo S.-T., Combined discrete particle swarm optimization and simulated annealing for grid computing scheduling problem, *Lecture Notes in Computer Science*, (LNAI), 5755, pp.242-251, 2009.

(νη′) Del Valle Y.E., Optimization of power system performance using facts devices, *Ph.D. Thesis*, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia, U.S.A., August 2009.

(νθ′) Hassan H.A., Yassin I.M., Halim A.K., Zabidi A., Majid Z.A. and Abidin H.Z., Logical effort using a novel discrete particle swarm optimization algorithm, In: *Proceedings of the 5th International Colloquium on Signal Processing and Its Applications*, (CSPA 2009), March 6-8, 2009, Kuala Lumpur, Malaysia, art.no. 5069266, pp.432-437, IEEE 2009.

(ξ′) Kashan A.H. and Karimi B., A discrete particle swarm optimization algorithm for scheduling parallel machines, *Computers and Industrial Engineering*, 56, No. 1, pp.216-223, February 2009.

(ξα′) Lapizco-Encinas G.C., Kingsford C. and Reggia J.A., A cooperative combinatorial particle swarm optimization algorithm for side-chain packing, In: *Proceedings of the 2009 IEEE Symposium Series on Computational Intelligence*, (SSCI 2009), March 30-April 2, 2009, Nashville, TN, U.S.A., art. no. 22037, pp.22-29, IEEE 2009.

(ξβ′) Omran M.G.H. and Al-Sharhan S., Optimization of discrete values using recent variants of differential evolution, In: *Proceedings of the Fourth IASTED International Conference on Computational Intelligence*, (CI 2009),

August 17-19, 2009, Honolulu, Hawaii, U.S.A., Paper No. 657-046, pp.1-6, ACTA press 2009.

(ξγ′) Park J.W., Park S.H. and Kim S.J., Optimization with high-cost objective function evaluations in a computing grid and an application to simulation-based design, *International Journal of High Performance Computing Applications*, 23, No. 1, pp.62-83, February 2009.

(ξδ′) Wong W.-K., Zeng X.-H. and Au W.M.R., A decision support tool for apparel coordination through integrating the knowledge-based attribute evaluation expert system and the T-S fuzzy neural network, *Expert Systems with Applications*, 36, No. 2, Part 1, pp.2377-2390, March 2009.

(ξε′) Zhan Z.-H., Feng X.-L., Gong Y.-J. and Zhang J., Solving the flight frequency programming problem with particle swarm optimization, In: *Proceedings of the IEEE Congress on Evolutionary Computation*, (CEC 2009), May 18-21, 2009, Trondheim, Norway, art. no. 4983105, pp.1383-1390, IEEE 2009.

13. Για την εργασία Γ.2

(α′) Ge J., Zhang L.-Z., Zhou X.-B. and Dong L., Discussion on AGC units participating ancillary services in electricity market, *Power System Technology*, 26, No. 12, pp.61-65, 2002.

(β′) Mantawy A.H. and Al-Ghamdi M.S., A new reactive power optimization algorithm In: *Proceedings of the 2003 IEEE Bologna PowerTech Conference*, June 23-26, Bologna, Italy, Vol. 4, pp.1-6, 2003.

(γ′) Boeringer D.W., Multi-objective particle swarm optimization of a modified Bernstein polynomial for curved phased array synthesis using Bezier curves, surfaces, and volumes, *Ph.D. Thesis* in Electrical Engineering, Department of Electrical Engineering, College of Engineering, The Graduate School, The Pennsylvania State University, University Park, PA, U.S.A., August 2004.

(δ′) Boeringer D.W. and Werner D.H., Particle swarm optimization versus genetic algorithms for phased array synthesis, *IEEE Transactions on Antennas and Propagation*, 52, No. 3, pp.771-779, March 2004.

(ε′) Jiang H.-M., Xie K. and Wang Y.-F., Design of multi-pumped Raman fiber amplifier by particle swarm optimizationi, *Journal of Optoelectronics Laser*, 15, No. 10, pp.1190-1193, October 2004.

(ϛ′) Lin W., Jiang C. and Qian J., The identification research of nonlinear system based on PSO with fuzzy adaptive inertia weight, In: *Proceedings of the World Congress on Intelligent Control and Automation*, (WCICA), Vol. 1, pp.267-271, 2004.

(ζ′) Rastegar R, Meybodi M.R. and Badie K., A new discrete binary particle swarm optimization based on learning automata, In: *Proceedings of the 2004 International Conference on Machine Learning and Applications*, (ICMLA 2004), December 16-18, 2004, Louisville, Kentucky, U.S.A., pp.456-462, 2004.

(η′) Ratnaweera A., Halgamuge S.K. and Watson H.C., Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients, *IEEE Transactions on Evolutionary Computation*, 8, No. 3, pp. 240-255, June 2004.

(ϑ′) Shi Y.-H. Particle swarm optimization, *IEEE Neural Networks Society Newsletter*, 2, No. 1, pp.8-13, February 2004. [ISSN: 1543-4281]

(ι′) Wetter M., GenOpt Generic Optimization Program, User Manual Version 2.0.0, Technical Report LBNL-54199, Simulation Research Group, Building Technologies Department, Environmental Energy Technologies Division, Lawrence Berkeley National Laboratory, Berkeley, CA 94720, U.S.A., January 5, 2004.

(ια′) Zhang X.-G., Yu L., Zheng Y., Shen Y., Zhou G.-T., Xi L.-X. and Yang B.-J., Adaptive PMD compensation using PSO algorithm, *OSA Trends in Optics and Photonics Series*, 95B, pp.98-100, 2004.

(ιβ′) Zhang X.-G., Yu L., Zheng Y., Shen Y., Zhou G.-T., Xi L.-X. and Yang B.-J., Adaptive PMD compensation using PSO algorithm, In: *Proceedings of the Optical Fiber Communication Conference*, (OFC 2004) February 23-27, 2004, Vol. 2, pp.1-3, 2004 [ISBN: 1-55752-772-5].

(ιγ′) Zhang X.-G., Yu L., Zheng Y., Shen Y., Zhou G.-T., Chen L., Xi L.-X., Yuan T.-C., Zhang J.-Z. and Yang B.-J., Two-stage adaptive PMD compensation in a 10 Gbit/s optical communication system using particle swarm optimization algorithm, *Optics Communications*, 231, No. 1-6, pp.233-242, February 2004.

(ιδ′) Zhang X.-G., Zheng Y., Shen Y., Zhang J.-Z. and Yang B.-J., PSO algorithm used for searching the optimum of automatic PMD compensation, In: *Proceedings of the Optical Networks and Technologies*: IFIP TC6 / WG6.10 First Optical Networks and Technologies Conference (OpNeTec), K.-I. Kitayama, F. Masetti-Placci and G. Prati (Eds), October 18-20, 2004, Pisa, Italy, pp.507-516, Springer, October 13, 2004 [ISBN: 0387231773].

(ιε′) Zheng Y., Zhang X., Zhou G., Shen Y., Chen L., Yu L., Xi L. and Yang B., Automatic PMD compensation experiment with particle swarm optimization and adaptive dithering algorithms for 10-Gb/s NRZ and RZ formats, *IEEE Journal of Quantum Electronics*, 40, No. 4, pp.427-435, April 2004.

(ιϝ′) Acan A. and Gunay A., Enhanced particle swarm optimization through external memory support, In: *Proceedings of the IEEE Congress on Evolutionary Computation*, (CEC 2005), Vol. 2, 2005, pp.1875-1882.

(ιζ′) Asghari V.R. and Ardebilipour M., Spread spectrum code estimation by particle swarm algorithm, *Transactions on Engineering, Computing and Technology*, 7, pp.207-210, World Enformatika Society, August 2005, [ISSN 1305-5313].

(ιη′) Asghari V.R. and Ardebilipour M., Spread spectrum code estimation by particle swarm algorithm, *Proceedings of World Academy of Science*, Engineering and Technology, 7, pp.207-210, WASET Org, August 7, 2005, [ISSN: 1307-6884].

(ιϑ′) Asghari V.R. and Ardebilipour M., Spread spectrum code estimation by particle swarm algorithm, *International Journal of Signal Processing*, 2, No. 4, pp.268-272, 2005.

(κ′) Boeringer D.W. and Werner D.H., Efficiency-constrained particle swarm optimization of a modified Bernstein polynomial for conformal array excitation amplitude synthesis, *IEEE Transactions on Antennas and Propagation*, 53, No. 8, pp.2662-2673, August 2005.

(κα′) Di Chio C., Extended particle swarms to simulate biology-like systems, Full research proposal, Department of Computer Science, University of Essex, U.K., July 4, 2005.

(κβ′) Engelbrecht A.P., Fundamentals of Computational Swarm Intelligence, John Wiley and Sons Ltd, Chichester, England, November 4, 2005 [ISBN: 0-470-

09191-6].

(κγ′) Ifeachor E.C., Artificial Intelligence: Particles Swarm Optimisation Links: Papers, Signal Processing and Multimedia Communication (SPMC) research Group, School of Computing, Communications and Electronics Faculty of Technology, University of Plymouth, Plymouth, United Kingdom, May 4, 2005.

(κδ′) Perez-Lopez J.R., Contribucion a los metodos de optimizacion basados en procesos naturales y su aplicacion a la medida de antenas en campo proximo, Tesis Doctoral, Departamento de Ingenieria de Comunicaciones, Universidad de Cantabria, Santander, Spain, Octubre de 2005.

(κε′) Zhang X., Zheng Y., Shen Y., Zhang J. and Yang B., Particle swarm optimization used as a control algorithm for adaptive PMD compensation, *IEEE Photonics Technology Letters*, 17, No. 1, pp.85-87, January 2005.

(κϝ′) Zheng Y., Zhang X., Shen Y., Zhou G. and Yang B., Automatic polarization-mode dispersion compensation by a particle swarm optimization method and adaptive dithering algorithm, *Journal of Optical Society of America B*, 22, No. 2, pp.336-346, February 2005

(κζ′) Acan A., Unveren A. and Bodur M., The latest vs. averaged recent experience: which better guides a PSO algorithm? In: *Proceedings of the 2006 IEEE Congress on Evolutionary Computation*, (CEC2006), July 16-21, 2006, Vancouver, B.C., Canada, pp.414-419, IEEE 2006.

(κη′) Chen Y. and Zhu Q.-G., A novel adaptive PMD compensation system based on PSO algorithm, In: *Proceedings of the Fifth International Conference on Machine Learning and Cybernetics*, (ICMLC2006), August 13-16, 2006, Dalian, China, art. no. 4028086, pp.344-348, IEEE 2006.

(κθ′) Duan G.-Y., Zhang X.-G., Li X.-H., Yu L., Zhang R. and Yang B.-J., Degree of polarization ellipsoids in feedforward PMD compensation, *Semiconductor Optoelectronics*, 27, No. 4, pp.451-454, 2006.

(λ′) He Y.-C. and Liu K.-Q., A modified particle swarm optimization for solving global optimization problems, In: *Proceedings of the Fifth International Conference on Machine Learning and Cybernetics*, (ICMLC 2006), August 13-16, 2006, Dalian, China, art. no. 4028423, pp.2173-2177, IEEE 2006.

(λα′) Huang F., Fan X.-P. and Qu Z.-H., Reconstruction of extended superquadric models by cooperative evolution parallel PSO algorithm, *Computer Engineering and Applications*, 42, No. 13, pp.15-18, 2006.

(λβ′) Jiang H.-M., Xie K., Ren C. and Wang Y.-F., A novel particle swarm optimization with stochastic stagnation, *Journal of Sichuan University* (Engineering Science Edition), 38, No. 4., pp.117-121, July 2006.

(λγ′) Krohling R.A. and Dos Santos Coelho L., Coevolutionary particle swarm optimization using Gaussian distribution for solving constrained optimization problems, *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 36, No. 6, pp.1407-1416, December 2006.

(λδ′) Min C., Lin C. and Shuangchun W., PMD compensation in WDM system using the worst channel equalization scheme, In: *Proceedings of SPIE - The International Society for Optical Engineering*, Vol. 6353 II, art. no. 635330, 2006.

(λε′) Niu Q. and Gu X.-S., An improved genetic-based particle swarm optimization for no-idle permutation flow shops with fuzzy processing time, *Lecture Notes in Artificial Intelligence*, 4099, pp.757-766, 2006.

(λϝ′) Suganthan P.N. and Qin A.K., Recent advances in real-parameter evolutionary algorithms, Tutorial presentation at the Sixth International Conference on Simulated Evolution And Learning, (SEAL2006), October 15-18, 2006, Hefei, China.

(λζ′) Wang L., Liu Y.-S. and Xu Y.-Q., Multi-objective PSO algorithm based on fitness sharing and online elite archiving, *Lecture Notes in Computer Science*, 4113, pp.964-974, 2006.

(λη′) Yu K.-W. and Hu S.-C., An application of AC servo motor by using particle swarm optimization based sliding mode controller, In: *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, (SMC 2006), October 8-11, 2006, Taipei, Taiwan, pp.4146-4150, IEEE 2006.

(λϑ′) Yu K.-W. and Huang Z.-L., LQ regulator design based on particle swarm optimization, In: *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, (SMC 2006), October 8-11, 2006, Taipei, Taiwan, pp.4142-4145, 2006.

(μ′) Zhang X.-G., Xi L.-X., Duan G.-Y., Yu L., Yu Z.-Y. and Yang B.-J., An intelligent PSO-based control algorithm for adaptive compensation polarization mode dispersion in optical fiber communication systems, *Lecture Notes in Computer Science*, (LNCS), 4233, pp.1090-1100, 2006.

(μα′) Zhang X.-G., Xi L.-X., Duan G.-Y., Yu L., Yu Z.-Y. and Yang B.-J., An application of intelligent PSO algorithm to adaptive compensation for polarization mode dispersion in optical fiber communication systems, *Lecture Notes in Computer Science*, (LNCS), 4247, pp.756-765, 2006.

(μβ′) Zhang Z.-Y., Ge S.-Y. and Liu Z.-F., Particle swarm optimization algorithm and its application in unit commitment, *Electric Power Automation Equipment*, 26, No. 5, pp.28-31, 2006.

(μγ′) Zhu J.-J., Duan G.-Y., Wang Q.-G., Zhang X.-G. and Yang B.-J., Second-order polarization mode dispersion self-adaptive compensation experiment using PSO algorithm, *Photon Technology*, 3, pp.150-155, 2006.

(μδ′) Zhu J.-J., Zhang X.-G., Duan G.-Y. and Wang Q.-G., PSO-based control algorithm for polarization mode dispersion self-adaptive compensation, *Semiconductor Photonics and Technology*, 12, No. 4, pp.217-223, 2006.

(με′) Alfawaer Z.M., Hua G.W., Abdullah M.Y. and Mamady I.D., Power minimization algorithm in wireless ad-hoc networks based on PSO, *Journal of Applied Sciences*, 7, No. 17, pp.2523-2526, September 2007.

(μϝ′) Jafarpour B., Meybodi M.R. and Shiry S., A hybrid method for optimization (Discrete PSO + CLA), In: *Proceedings of the International Conference on Intelligence and Advance Systems*, (ICIAS 2007), November 25-28, 2007, Kuala Lumpor, Malaysia, pp.1-10, 2007.

(μζ′) Li X., Utilising restricted for-loops in genetic programming, *Ph.D. Thesis*, School of Computer Science and Information Technology, Faculty of Applied Science, Royal Melbourne Institute of Technology, Melbourne, Victoria, Australia, February 2007.

(μη′) Prakasvudhisarn C. and Kunnapapdeelert S., Torusity tolerance verification using swarm intelligence, *Industrial Engineering and Management Systems* (IEMS), 6, No. 2, pp.94-105, December 2007.

(μϑ′) Wang L., Liu Y. and Xu Y., Improved MOPSO algorithm for shipping route planning, *Journal of Harbin Institute of Technology* (New Series), 14, SUPPL 2, pp.150-153, January 2007.

(ν′) Wang X.-F., SQP algorithms in balancing rotating machinery, *Mechanical Systems and Signal Processing*, 21, No. 3, pp.1469-1478, April 2007.

(να′) Wang Y.-J. and Fang D.-Z., Research on AGC unit dispatch based on particle swarm optimization algorithm, *Relay*, 35, No. 17, pp.58-61, 2007.

(νβ′) Yu K.-W. and Hsu J.-H., Fuzzy gain scheduling PID control design based on particle swarm optimization method, In: *Proceedings of the 2007 IEEE Second International Conference on Innovative Computing, Information and Control*, (ICICIC 2007), September 5-7, 2007, Kumamoto, Japan, art.no. 4427982, pp.337-340, IEEE 2007.

(νγ′) Espirito Santo I.A.C.P. and Fernandes E.M.G.P., Solving minimax problems using an heuristic pattern search algorithm, In: *13th International Congress on Computational and Applied Mathematics*, (ICCAM 2008), July 7-11, 2008, Ghent, Belgium, 2008.

(νδ′) Gao H.-M., Tan Y. and Zeng J.-C., Cooperative particle swarm optimization for steel making scheduling, *Journal of Systems Engineering*, 23, No. 4, pp.466-471, 2008.

(νε′) Ifeachor E.C., Particle swarm optimization papers, Signal Processing and Multimedia Communication (SPMC) research Group, School of Computing, Communications and Electronics, Faculty of Technology, University of Plymouth, Plymouth, United Kingdom, January 2008.

(νϝ′) Liu D., Wu J. and Yang W., A novel self-calibration approach based on particle swarm optimization for position-based visual position algorithm, *Journal of Xi' an University of Technology*, 24, No. 1, pp.1-7, 2008.

(νζ′) Niu Q. and Gu X.-S., A novel particle swarm optimization for flow shop scheduling with fuzzy processing time, *Journal of Donghua University* (English Edition), 25, No. 2, pp.115-122, 2008.

(νη′) Rad B.F. and Abedi M., An optimal load-shedding scheme during contingency situations using meta-heuristics algorithms with application of AHP method, In: *Proceedings of the 2008 IEEE 11th International Conference on Optimization of Electrical and Electronic Equipment*, (OPTIM 203 2008), May 22-24, 2008, Brasov, Romania, art. no. 4602361, pp.167-172, IEEE 2008.

(νϑ′) Rad B.F. and Abedi M., Application of meta-heuristics algorithms in discrete model of steady-state load-shedding, In: *Proceedings of the 2008 IEEE 11th International Conference on Optimization of Electrical and Electronic Equipment*, (OPTIM 2008), May 22-24, 2008, Brasov, Romania, art. no. 4602362, pp.173-177, IEEE 2008.

(ξ′) Acan A. and Unveren A., A memory-based colonization scheme for particle swarm optimization, In: *Proceedings of the IEEE Congress on Evolutionary Computation*, (CEC 2009), May 18-21, 2009, Trondheim, Norway, art. no. 4983181, pp.1965-1972, IEEE 2009.

(ξα′) Cramer A.M., Sudhoff S.D. and Zivi E.L., Evolutionary algorithms for minimax problems in robust design, *IEEE Transactions on Evolutionary Computation*, 13, No. 2, pp.444-453, April 2009.

(ξβ′) Herrera O.E., Nuno L. and Diaz-Morcillo A., Shaping an antenna radiation diagram with discrete weights using the PSO algorithm and periodic and nest spaces, *Mathematical and Computer Modelling*, 50, No. 5-6, pp.840-848, September 2009.

(ξγ′) Huang X., Zhang J. and Zhan Z.-H., Faster particle swarm optimization with random inertia weight, *Computer Engineering and Design*, 30, No. 3,

pp.1-4, 2009.

(ξδ′) Jiang H.-M, Xie K. and Wang Y.-F., C band single pump photonic crystal fiber Raman amplifier, *Chinese Science Bulletin*, 54, No. 13, pp.1927-1931, 2009.

(ξε′) Wang L., Cao J.-F. and Han C.-Z., Self-calibration of heterogeneous sensors based on particle swarm optimization, In: *Proceedings of the 4th IEEE Conference on Industrial Electronics and Applications*, (ICIEA 2009), May 25-27, 2009, Xian, China, art. no. 5138221, pp.321-325, IEEE 2009.

(ξϛ′) Wetter M., GenOpt (R): Generic Optimization Program, User Manual Version 3.0.0, Simulation Research Group, Building Technologies Department, Environmental Energy Technologies Division, Lawrence Berkeley National Laboratory, Berkeley, California, U.S.A., pp.1-104, May 4, 2009.

14. Για την εργασία Γ.4

(α′) Houstis E.N., Moustakides G.V. and Verykios V.S., Privacy Preserving Data Mining publications, Data Mining and Privacy Group, Department of Computer and Communication Engineering, University of Thessaly, Volos, Greece, July 3, 2006.

15. Για την εργασία Γ.5

(α′) Storn R., Differential evolution research: Trends and open questions, *Studies in Computational Intelligence*, 143, pp.1-31, 2008.

(β′) Redi J., Computational Intelligence Methods for Large Integer Numbers Prime-Factorization, *Ph.D. Thesis*, University of Genova, 2006.

16. Για την εργασία Γ.7

(α′) Storn R., Differential evolution research: Trends and open questions, *Studies in Computational Intelligence*, 143, pp.1-31, 2008.

(β′) Poli R., An analysis of publications on particle swarm optimisation applications, Technical Report CSM-469, Department of Computer Science, University of Essex, UK, May 2007 [ISSN: 1744-8050]

(γ′) Ramamoorthy V., Silaghi M., Constraint Satisfaction Approach to Feistel Cipher Substitution Box Generation, Technical Report, Florida Institute of Technology, 2009.

(δ′) Tang M., Li C., Yu Y., Zhang G.-P., Zhang H.-G., Research and Implementation of Evolution Cipher Chip, Second International Symposium on Computational Intelligence and Design, (ISCID 2009 IEEE), vol. 1.(12-14), pp. 32-35, 2009.

Ευρετήριο

Data Encryption Standard, 56, 57
S-box, 66

αντίστροφη πολυωνυμική παρεμβολή, 89, 96
αριθμός περιστροφής, 105
αρχιτεκτονική ΤΝΔ, 39, 74
ασταθής περιοδική τροχιά, 108
αυθεντικοποίηση δεδομένων, 118
αυτοσυσχέτιση S-box, 67
αυτοσυσχέτιση συνάρτησης Boole, 67

βελτιστοποίηση με αποικίες μυρμηγκιών, 35
βελτιστοποίηση με σμήνος σωματιδίων, 31, 52, 60, 68

δίκτυο πί-σίγμα, 80
διαφορική κρυπτανάλυση, 58
διαφοροεξελικτικός αλγόριθμος, 29, 52, 60, 68

εκπαίδευση ΤΝΔ, 39
ελλειπτική καμπύλη, 12
επίθεση επιλεγμένου κρυπτογραφήματος, 5
επίθεση επιλεγμένου πρωτότυπου κειμένου, 5, 58
επίθεση γνωστού πρωτότυπου κειμένου, 5
επίθεση μόνο κρυπτογραφήματος, 5
επίθεση μεταβαλλόμενου επιλεγμένου πρωτότυπου κειμένου, 5
επιβεβαίωση δεδομένων, 118
ευσταθής περιοδική τροχιά, 108
εξελικτικές στρατηγικές, 25
εξελικτικός υπολογισμός, 19

γενετικός προγραμματισμός, 22
γενετικοί αλγόριθμοι, 20
γραμμική συνάρτηση Boole, 66

ιδιωτικότητα δεδομένων, 118
ισορροπία συνάρτησης Boole, 66, 68
ισχυρά κλειδιά, 108

θεώρημα Parseval, 66

κανονική συνάρτηση Boole, 66
κρυπτογράφημα, 4
κρυπτογράφηση δημοσίου κλειδιού, 9
κρυπτογράφηση συμμετρικού κλειδιού, 6
κρυπτοσύστημα, 4
κρυπτοσύστημα Feistel, 57
κρυπτοσύστημα αντικατάστασης, 6
κρυπτοσύστημα γινομένου, 8
κρυπτοσύστημα μετάθεσης, 8
κρυπτοσύστημα ροής, 8
κρυπτοσύστημα τμηματικής κρυπτογράφησης, 6

μέθοδος παρεμβολής Aitken, 88, 97
μέθοδος παρεμβολής Neville, 88, 97
μετασχηματισμός Walsh Hadamard, 66
μη γραμμική απεικόνιση, 104
μη-γραμμικότητα S-box, 67
μη-γραμμικότητα συνάρτησης Boole, 66
μονόδρομη συνάρτηση, 9, 96
μονόδρομη συνάρτηση κερκόπορτας, 9

νομιμότητα αποστολέα, 118

περιοδική τροχιά, 104
πληρότητα δεδομένων, 118
πολυστρωματικό ΤΝΔ, 37
πολυωνυμική παρεμβολή, 87
πολυωνυμικό δίκτυο Ridge, 80, 82
πρόβλημα ανταλλαγής κλειδιών Diffie-Hellman, 11, 74
πρόβλημα απεικόνισης Diffie-Hellman, 11
πρόβλημα διακριτού λογαρίθμου, 11, 48, 74
πρόβλημα διακριτού λογαρίθμου ελλειπτικών καμπυλών, 11, 77
πρόβλημα λογαρίθμου Lucas, 97
πρόβλημα παραγοντοποίησης, 48, 74
πρωτόκολλο ηλεκτρονικής συγκέντρωσης δεδομένων, 117, 126
πρωτόκολλο ηλεκτρονικών εκλογών, 118
πρωτόκολλο ηλεκτρονικών εκλογών χωρίς κάλπη, 124
πρωτότυπο κείμενο, 4

χαρακτηριστική, 58

σταθερό σημείο, 104
συλλέκτης, 118
συνάρτηση Bent, 67

συνάρτηση Lucas, 96

τεχνητό νευρωνικό δίκτυο, 36

υπόθεση Kerckhoff, 4
υπολογιστική νοημοσύνη, 19