e-αξιολόγηση : Εφαρμογές της Κρυπτογραφίας στην Αξιολόγηση μέσω Τεχνολογιών Πληροφορικής και Επικοινωνιών

Βασίλειος Ι. Γαλάνης

Διπλωματική Εργασία

Πανεπιστήμιο Πατρών
Σχολή Θετικών Επιστημών
Τμήμα Μαθηματικών
Πάτρα

Επιβλέπων: Καθηγητής Μιχαήλ Ν. Βραχάτης

(Μάϊος 2009)

Αυτή η διπλωματική εργασία στοιχειοθετήθηκε με το πρόγραμμα LaTeXΗ συγγραφή έγινε με τη βοήθεια του προγράμματος Kile στο λειτουργικό σύστημα Ubuntu Linux. Το style που χρησιμοποιήθηκε είναι το ελληνικό LaTeXstyle του Β. Π. Πλαγιανάκου (από τη σελίδα του http://www.math.upatras.gr/∼vpp/)

Ευχαριστίες

Για την πραγματοποίηση της εργασίας αυτής καθοριστική υπήρξε η βοήθεια και η συμπαράσταση πολλών ανθρώπων. Κατάρχάς, θα ήθελα να ευχαριστήσω θερμά τον Δάσκαλό μου, καθηγητή κ. Μ.Ν. Βραχάτη στον οποίο οφείλεται κατά ένα πολύ μεγάλο βαθμό η υλοποίηση της εργασίας αυτής. Η ουσιαστική καθοδήγησή του στο ξεπέρασμα των ποικίλων δυσκολιών που συνάντησα κατά της εκπόνησης της, οι πολύτιμες συμβουλές και υποδείξεις του, και η ηθική του συμπαράσταση με βοήθησαν τα μέγιστα. Ευχαριστώ επίσης και τα άλλα δύο μέλη της Τριμελούς Συμβουλευτικής Επιτροπής μου, τους καθηγητές κ.κ. Γ. Κ. Μελετίου και Ε. Γαλλόπουλο, των οποίων η βοήθεια ήταν επίσης καθοριστική.

Αισθάνομαι, επίσης, την υποχρέωση να ευχαριστήσω και τους υπόλοιπους συνεργάτες μου, μέλη του Εργαστηρίου Υπολογιστικής Νοημοσύνης (CILAB) και μεταπτυχιακούς φοιτητές του Τμήματος Μαθηματικών του Πανεπιστημίου Πατρών, κ.κ. Μ. Γ. Επιτροπάκη, Μ. Κ. Οικονομάκη, Γ. Σ. Αντζουλάτο και Ε. Κ. Λάσκαρη.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για την αμέριστη στήριξη και υπομονή τους όλα αυτά τα χρόνια.

Βασίλειος Ι. Γαλάνης

Πάτρα, 2009.

Περιεχόμενα

Μέρος Ι

Εισαγωγή

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή - Η έννοια της αξιολόγησης

Με τον όρο αξιολόγηση εννοούμε τη συστηματική αποτίμηση της αξίας ή της σημαντικότητας μίας διαδικασίας ή ενός αντικειμένου κάνοντας χρήση συγκεκριμένων προαποφασισμένων κριτηρίων. Η έννοια της αξιολόγησης αποτελεί από μόνη της αντικείμενο μελέτης καθώς υπάρχουν πολλοί και διαφορετικοί τρόποι προσέγγισης της αξιολόγησης ενός υποκειμένου. Συγκεκριμενα, στα [28], [58] βλέπουμε ότι υπάρχει σαφής διαχωρισμός των διαφορετικών προσεγγίσεων για τη διενέργεια της διαδικασίας αξιολόγησης, ανάλογα με τον προσανατολισμό και τους στόχους του οργανισμού που διενεργεί την αξιολόγηση, καθώς και την επιστημολογική προσέγγιση την οποία ακολουθεί.

Η τεχνολογία της πληροφορικής και των επικοινωνιών αναπτύσσεται με ραγδαίους ρυθμούς και έχει εφαρμογές σε ένα πολύ μεγάλο και διαρκώς αυξανόμενο εύρος δραστηριοτήτων, καθώς προσφέρει τη δυνατότητα άμεσης ανταλλαγής πληροφορίας ανεξαρτήτως της απόστασης που χωρίζει τον αποστολέα από τον παραλήπτη. Το σημείο συνάντησης τους, το διαδίκτυο, είναι πλέον πλήρως ενσωματωμένο στην καθημερινότητα του μέσου ανθρώπου και παρέχει ένα καινούριο περιβάλλον επικοινωνίας. Οι δυνατότητες του διαδικτύου στην αποστολή όχι μόνο κειμένου αλλά και ήχου και βίντεο σε πραγματικό χρόνο το έχουν καταστήσει απαραίτητο εργαλείο στην εκπαίδευση, τη βιομηχανία και το εμπόριο.

Μεγάλη μερίδα των διαθέσιμων εφαρμογών του διαδικτύου είναι εφαρμογές που απευθύνονται σε ομάδες ατόμων και οι οποίες έχουν κοινά αντικείμενα και στόχους για την ομάδα στην οποία απευθύνονται, με πιο χαρακτηριστικό παράδειγμα τις εφαρμογές εξ αποστάσεως εκπαίδευσης. Η μέτρηση της αποτελεσματικότητας για κάθε τέτοια εφαρμογή, τόσο στο σύνολο της όσο και στα επί μέρους χαρακτηριστικά της, είχε σαν αποτέλεσμα την εμφάνιση ενός νέου προβλήματος το οποίο έχει να κάνει με την αξιολόγηση μέσω διαδικτύου τόσο των εφαρμογών αυτών όσο και των συμμετεχώντων στις δραστηριότητες τις οποίες προσφέρει κάθε εφαρμογή.

Με την ευρεία διάδοση της χρήσης του διαδικτύου, οι δυνατότητες για διενέργεια μαζικής αξιολόγησης στα πλαίσια μιας διαρκώς διευρυνόμενης γκάμας δραστηριοτήτων έχει γίνει εφικτή σε παγκόσμια κλίμακα. Ανάλογα με τον επιστημολογικό τύπο αξιολόγησης που διενεργείται, δηλαδή είτε αυτός είναι ¨προσανατολισμένος προς τον καταναλωτή¨ (αντικειμενική επιστημολογική προσέγγιση) είτε είναι ¨πελατοκεντρικός¨ ή ¨αξιολόγηση από αντίπαλο¨(υποκειμενική επιστημολογική προσέγγιση), το διαδίκτυο μπορεί να προσφέρει πολλούς και διαφορετικούς τύπους αξιολόγησης, οι οποίοι μπορούν να χρησιμοποιηθούν είτε μεμονωμένα είτε σε συνδυασμό σε πολλές και διαφορετικής φύσης εφαρμογές.

1.1 Ο σκοπός της εργασίας

Η εργασία αυτή έχει σα σκοπό τη διερεύνηση των εφαρμογών της κρυπτογραφίας στην ασφάλεια της διαδικασίας της αξιολόγησης σε περιβάλλοντα όπου γίνεται χρήση τεχνολογιών επικοινωνίας και πληροφορικής. Πιό συγκεκριμένα, ξεκινώντας από την όσο το δυνατόν πλήρη περιγραφή ενός συστήματος e-αξιολόγησης τόσο σε επίπεδο hardware όσο και σε επίπεδο software, σκοπός μας είναι να εισάγουμε κατάλληλες κρυπτογραφικές τεχνικές έτσι ώστε να καλύπτουμε τις απαιτήσεις ασφαλείας της διαδικασίας της ηλεκτρονικής αξιολόγησης και να δώσουμε παραδείγματα αντίστοιχων εφαρμογών όπου είναι γίνεται χρήση της ηλεκτρονικής αξιολόγησης.

1.2 Η διάρθρωση της εργασίας

Η διάρθρωση της εργασίας αυτής γίνεται με τον εξής τρόπο :

- Στο πρώτο μέρος θα διερευνήσουμε το τρόπο με τον οποίο ενσωματώνεται η έννοια της ασφάλειας στη διαδικασία της αξιολόγησης, τους λόγους για τους οποίους υπάρχει ανάγκη για ενσωμάτωση τεχνικών ασφαλείας στην e-αξιολόγηση και τα οφέλη που αποκομίζουμε από αυτες καθώς και μία γρήγορη παρουσίαση του συνόλου των τεχνικών που χρησιμοποιούνται. Στη συνέχεια του κεφαλαίου αυτού, θα δούμε που και πως ενσωματώνονται εφαρμογές κρυπτογραφίας στο σύνολο των τεχνικών ασφαλείας που χρησιμοποιούνται στη διαδικασία αξιολόγησης.

- Στο δεύτερο μέρος θα κάνουμε μια παρουσίαση των κρυπτογραφικών πρωτοκόλλων και τεχνικών που έχουν εφαρμογή στην e-αξιολόγηση, καθώς και μια παρουσίαση του μαθηματικού τους υπόβαθρου.

- Στο τρίτο μέρος θα κάνουμε μια παρουσίαση των εφαρμογών της ηλεκτρονικής αξιολόγησης στην εκπαίδευση.

Μέρος ΙΙ

Ασφάλεια δεδομένων και κρυπτογραφία στην e-αξιολόγηση

ΚΕΦΑΛΑΙΟ 2

Ασφάλεια στην e-αξιολόγηση

2.1 e-αξιολόγηση : ορισμός

Με τον όρο e-αξιολόγηση εννοούμε τη διαδικασία εξ αποστάσεως αξιολόγησης με τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών. Η διαδικασία της αξιολόγησης μπορεί να αφορά διαφορετικά αντικείμενα σε διαφορετικά περιβάλλοντα και με διαφορετικούς στόχους.

Με βάση τον ορισμό της αξιολόγησης τον οποίο δώσαμε στην εισαγωγή και τη φύση του προβλήματος το οποίο καλούμαστε να αντιμετωπίσουμε με εφαρμογές e-αξιολόγησης, πιθανά αντικείμενα αξιολόγησης είναι οι επιδόσεις μαθητών και καθηγητών σε ένα πρόγραμμα εξ αποστάσεως εκπαίδευσης, το επίπεδο οργάνωσης ενός ιδρύματος, το εκπαιδευτικό υλικό ή ακόμα και η αξιολόγηση της επίτευξης των εκπαιδευτικών ή τυχόν οικονομικών στόχων του προγραμματος αυτού.

2.2 Η έννοια της ασφάλειας στην e-αξιολόγηση

Στην e-αξιολόγηση, η χρήση σύγχρονων τεχνολογιών όπως το διαδίκτυο γεννά μια σειρά από προβλήματα τα οποία έχουν να κάνουν τόσο με τη φύση τις διαδικάσιας της αξιολόγησης, όσο και με τη βαθμό εμπιστευτικότητας των δεδομένων που διακινούνται μέσω του διαδικτύου στα πλαίσια της διαδικασίας αυτής. Με την ενσωμάτωση της ασφάλειας στην e-αξιολόγηση επιχειρούμε να αποτρέψουμε :

- Την αυθαίρετη πρόσβαση σε δεδομένα εμπιστευτικού χαρακτήρα τα οποία διακινούνται στα πλαίσια της διαδικασίας της e-αξιολόγησης τα οποία μπορούν να αφορούν από βαθμούς μέχρι και εμπορικά, τραπεζικά ή και βιομηχανικά δεδομένα μεγάλης εμπορικής αξίας.

- Τη μεταβολή είτε των δεδομένων της e-αξιολόγησης είτε της διαδικασίας αυτής καθεαυτής καθιστώντας τη μη αξιόπιστη, και άρα μη χρήσιμη.

Ξεκινώντας την εισαγωγή στην έννοια της ασφάλειας στην e-αξιολόγηση, θα πρέπει αρχικά να ορίσουμε το αντικείμενο στο οποίο αυτή διενεργείται. Το αντικείμενο αυτό είναι η παρεχόμενη πληροφορία στις διάφορες μορφές τις, από την οποία καλούμαστε να βγάλουμε μια σειρά από συμπεράσματα κάνοντας χρήση της e-αξιολόγησης. Γενικά, η πληροφορία μπορεί να έχει τρεις μορφές:

- Δεδομένα : Σταθερή πληροφορία για αντικείμενα και φαινόμενα.

- Πληροφορία : Επεξεργασμένα δεδομένα σε κατάλληλη μορφή για λήψη αποφάσεων και αναλυτική έρευνα.

- Γνώση : Επεξεργασμένη πληροφορία που χρησιμοποιείται για την επίλυση προβλημάτων και τη λήψη αποφάσεων, καθώς επίση και μέτα-πληροφορία για τους τρόπους επεξεργασίας και μετατροπής της πληροφορίας για τη λήψη αποφάσεων.

Η ασφάλεια στην e-αξιολόγηση απότελείται από δύο ξεχωριστά κομμάτια καθώς περιλαμβάνει τόσο την ασφάλεια σε επίπεδο εξοπλισμού (hardware, δηλ. του δικτύου, των υπολογιστικών συστημάτων κτλ.) όσο και την ασφάλεια σε επίπεδο λογισμικού (software, δηλ. τα προγράμματα, τις πλατφόρμες και τις διαδικτυακές εφαρμογές).

Για την αντιμετώπιση των δύο παραπάνω προβλημάτων, όχι μόνο σε εφαρμογές e-αξιολόγησης, αλλά και γενικά σε οποιοδήποτε τύπο ηλεκτρονικού δικτύου έχει, ήδη από το 1989, θεσπιστεί το πρότυπο ISO 7498-2 [18], το οποίο καθορίζει μία σειρά από κριτήρια ασφαλείας τα οποία και πρέπει να ακολουθούνται για τη δημιουργία ενός ασφαλούς περιβάλλοντος δικτύωσης:

- Εμπιστευτικότητα : τα δεδομένα που είναι αποθηκευμένα στις βάσεις δεδομένων και διακινούνται στο δίκτυο δεν είναι αναγνώσιμα από τρίτους.
- Ακεραιότητα : τα δεδομένα που είναι αποθηκευμένα στις βάσεις δεδομένων και διακινούνται στο δίκτυο δεν είναι δυνατό να μεταβληθούν από τρίτους
- Διαθεσιμότητα : τα δεδομένα είναι πάντα διαθέσιμα σε διαπίστευμένα μέλη του δικτύου.
- Αναγνωρισιμότητα και εξακρίβωση ταυτότητας για τα διαπιστευμένα μέλη του δικτύου.
- Εξουσιοδότηση (έλεγχος τοπικής πρόσβασης): τα διαπιστευμένα μέλη έχουν πρόσβαση μόνο στα σχετικά με αυτά δεδομένα και όχι σε άλλα.
- Μη δυνατότητα αποκύρηξης πράξης : κάθε χρήστης του δικτύου μπορεί να καταστεί υπεύθυνος για κάθε πράξη την οποία έχει τελέσει χρησιμοποιώντας το δίκτυο.

Το πρώτο βήμα το οποίο θα πρέπει να κάνουμε για να θεμελιώσουμε την προσέγγιση μας είναι μια μελέτη του είδους των απειλών ασφαλείας τις οποίες θα πρέπει να μπορεί να αντιμετωπίσει ένα σύστημα e-αξιολόγησης.

2.3 Μοντελοποίηση των απειλών ασφαλείας για ένα σύστημα e-αξιολόγησης

Η θεμελίωση της ασφάλειας σε ένα σύστημα είναι αλληλένδυτη με τον προσδιορισμό του τύπου των απειλών σε αυτό αλλά και με το μέγεθος της ζημιάς η οποία μπορεί να προκληθεί από μια πετυχημένη επίθεση στο σύστημα. Για να το κάνουμε αυτό πρέπει αρχικά να περιγράψουμε τη δομή ενός συστήματος e-αξιολόγησης όσο και το προφίλ των συμμετέχοντων σε ένα τέτοιο σύστημα, διαμορφώνοντας έτσι ένα γενικό θεωρητικό μοντέλο ενός συστήματος e-αξιολόγησης. Η μοντελοποίηση αυτή βασίζεται στην εργασία [41].

2.3 Μοντελοποίηση των απειλών ασφαλείας για ένα σύστημα e-αξιολόγησης

Οι οντότητες οι οποίες απαρτίζουν το μοντέλο ενός συστήματος e-αξιολόγησης είναι οι αξιολογητές, οι αρχές που συντονίζουν τη διαδικασία της e-αξιολόγησης και οι επιλογές που γίνονται σχετικά με τον τύπο e-αξιολόγησης. Πιο αναλυτικά έχουμε :

- Οι αξιολογητές : Οι αξιολογητές είναι οι οντότητες οι οποίες παρέχουν τις αναγκαίες πληροφορίες για τα προς αξιολόγηση αντικείμενα κατά τη διαδικασία της e-αξιολόγησης. Οι αξιολογητές μπορεί να λαμβάνουν οποιαδήποτε μορφή ανάλογα με τη φύση και τους στόχους της διαδικασίας αξιολόγησης στην οποία μετέχουν. Μπορούν να αποτελούν είτε μέρος ενός κλειστού προγράμματος, όπως π.χ. ενός προγράμματος εξ αποστάσεως εκπαίδευσης είτε να μετέχουν σε μια ανοιχτή διαδικασία όπως, π.χ. σε ένα γκάλλοπ ή σε μια μέτρηση του βαθμού ικανοποιήσης παρεχόμενων υπηρεσιών από μια εταιρία. Ανάλογα με τον τύπο και τους σκοπούς της αξιολόγησης, οι αξιολογητές θα πρέπει να έχουν την δυνατότητα διακοπής ή ακόμη και ανάκλησης της επιλογής τους μέχρι και τον τερματισμό της αξιολόγησης.

- Οι αρχές (authorities) : Οι αρχές διαχειρίζονται τη διαδικασία της αξιολόγησης αλλά και τα αποτελέσματα τα οποία αυτή παράγει. Καθώς το περιβάλλον διεξαγωγής της διαδικασίας e-αξιολόγησης είναι το διαδίκτυο, το ρόλο της αρχής παίζουν αυτοματοποιημένες διαδικτυακές υποδομές (τα υπολογιστικά συστήματα και το λογισμικό που χρησιμοποιείται για τη διενέργεια της e-αξιολόγησης) οι οποίες χρησιμοποιούνται τόσο για τη διανομή των πληροφοριών στους αξιολογητές όσο και για τη συγκέντρωση και επεξεργασία των αξιολογήσεων που δίνουν οι αξιολογητές. Αξίζει επίσης να σημειωθεί ότι οι αρχές μπορούν να ενεργούν και ως αξιολογητές, αφού με το πέρας της διαδικασίας (ή ακόμα και παράλληλα εαν είναι δυναμική) της e-αξιολόγησης μπορούν να εξάγουν μέτα-πληροφορία με κατάλληλη επεξεργασία των αποτελεσμάτων. Οι αρχές παίζουν, συνήθως το όλο της εμπιστευτικής τρίτης αρχής (Trusted Third Party-TTP) όπως καλείται στη βιβλιογραφία της κρυπτογραφίας. Αξίζει να σημειωθεί ότι υπάρχει και η δυνατότητα αξιολόγησης με μη έμπιστες αρχές ή χωρίς καν τη διαμεσολάβηση αρχών με χρήση συγκεκριμένων κρυπτογραφικών πρωτοκόλλων.

- Οι επιλογές αξιολόγησης. Η δομή των επιλογών εξαρτάται από τον τύπο των αξιολόγησης. Πιο συγκεκριμένα, εξαρτάται από τον τύπο των ερωτήσεων και τον τρόπο με τον οποίο αυτές διανέμονται στους αξιολογητές στα πλαίσια της διαδικασίας της e-αξιολόγησης.

Η διαδικασία e-αξιολόγησης έχει τρεις φάσεις λειτουργίας :

- Τη φάση αρχικοποιήσης της διαδικασίας, όπου και γίνεται διανομή των πιστοποιητικών συμμετοχής και του υλικού αξιολόγησης από τις αρχές στους αξιολογητές.

- Τη κύρια φάση, όπου οι αξιολογητές αποστέλλουν ανώνυμα στις αρχές την ατομική τους αξιολόγηση σύμφωνα με τους στόχους της διαδικασίας, τις οποίες και οι αρχές συγκεντρώνουν σε βάσεις δεδομένων.

- Τη φάση κλεισίματος και επεξεργασίας των δεδομένων που παρηχθησαν από τη διαδικασία, όπου και με το πέρας του χρονικού ορίου συμμετοχής στη διαδικασία γίνεται τελική συγκέντρωση των αποτελεσμάτων και περαιτέρω επεξεργασία για την παραγωγή συμπερασμάτων και μέτα-πληροφορίας.

Η παραπάνω αλληλουχία των τριών φάσεων δεν είναι δεσμευτική για ένα σύστημα e-αξιολόγησης. Χαρακτηριστικό παράδειγμα είναι μια διαδικασία αξιολόγησης στην οποία λαμβάνονται δεδομένα αξιολόγησης σε βάθος χρόνου με τέτοιο τρόπο έτσι ώστε να απεικονίζεται η πρόοδος των αντικειμένων αξιολόγησης μέσα στο διάστημα αυτό και να είναι δυνατή η προσαρμογή της διαδικασίας σε καινούριες συνθήκες μέσα στο χρονικό σιάστημα αυτό. Μια τέτοια διαδικασία καλείται δυναμική αξιολόγηση.

Σε περίπτωση δυναμικής αξιολόγησης μπορεί, αναλόγως της μορφής της διαδικασίας ή των απαιτήσεων ασφαλείας, είτε να έχουμε επανάληψη μόνο του δεύτερου μέρους της διαδικασίας, είτε διαδοχικές επαναλήψεις των δύο πρωτων βημάτων. Το τρίτο βήμα ανανεώνεται είτε σε πραγματικό χρόνο είτε μετά από την περάτωση του δεύτερου βήματος κάθε επανάληψης, είτε με το πέρας συνολικά της διαδικασίας. Με τον τρόπο αυτό πραγματώνεται η δυναμική ανανέωση της παρεχόμενης πληροφορίας για κάθε προς αξιολόγηση αντικείμενο αλλά και η παραγωγή αποτελεσμάτων σε βάθος χρόνου.

Ο επιτιθέμενος σε ένα σύστημα e-αξιολόγησης μπορεί να έχει πολλές διαφορετικές μορφές και σκοπούς. Μπορεί να είναι κάποιος ο οποίος σκόπιμα μπορεί να θέλει να κάνει ζημιά στο σύστημα,κάποιος ο οποίος θα ήθελε να αποκτήσει πρόσβαση σε πληροφορίες εμπιστευτικού περιεχομένου ή ακόμα και κάποιος χρήστης του συστήματος ο οποίος θα μπορούσε να το βλάψει κατά λάθος. Ένας επιτιθέμενος ο οποίος μπορεί να επηρεάσει το σύστημα καλείται ενεργός επιτιθέμενος (active adversary) ενώ ένας επιτιθέμενος που απλά αποκτά πρόσβαση στο σύστημα χωρίς να μπορεί να το επηρεάσει καλείται παθητικός επιτιθέμενος.(passive adversary)

Τα προς προστασία στοιχεία του συστήματος e-αξιολόγησης είναι αυτά τα οποία είτε παρέχουν κρίσιμη λειτουργικότητα για το σύστημα είτε έχουν οικονομική αξία λόγω της εμπιστευτικής φύσης τους. Τέτοια στοιχεία είναι :

- Το υλικό της αξιολόγησης (π.χ. πληροφορίες για το προς αξιολόγηση αντικείμενο, συμπληρωμένα ερωτηματολόγια κτλ.).
- Προσωπικα δεδομένα και δεδομένα ταυτοποιήσης (κωδικοί πρόσβασης).
- Όγκος κίνησης στο δίκτυο του συστήματος e-αξιολόγησης.
- Η διαθεσιμότητα των υπηρεσιών του συστήματος.
- Η ακεραιότητα των δεδομένων που ανταλλάσονται στα πλαίσια της διαδικασίας, τόσο μεταξύ του συστήματος και των χρηστών όσο και μεταξύ των χρηστών αυτό καθεαυτό.

Για να ολοκληρώσουμε την περιγραφή της δομής ενός συστήματος e-αξιολόγησης, θα δούμε κάποια σημεία πρόσβασης τα οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να αποκτήσει πρόσβαση στο σύστημα [41] :

1. Χρησιμοποιημένα πρωτόκολλα δικτύου
2. Χρησιμοποιημένα κανάλια πληροφορίας

3. Συστήματα χρηστών

4. Διαδικτυακή υποδομή του συστήματος (servers, terminals κτλ.)

Έχοντας πλέον περιγράψει τη δομή ενός συστήματος e-αξιολόγησης, θα πρέπει να προβάλλουμε σε αυτή τις δύο βασικές κατηγορίες προβλημάτων ασφαλείας για δίκτυα υπολογιστών, όπως τα παρουσιάσαμε παραπάνω, με σκοπό να δούμε ποιές είναι οι απειλές στα διάφορα στάδια της διαδικασίας της e-αξιολόγησης και την πιθανή τους προέλευση.

Οι επιθέσεις σε ένα σύστημα e-αξιολόγησης χωρίζονται σε τεσσερις κατηγορίες [41], στις επιθέσεις ενάντια στη διαθεσιμότητα των υπηρεσιών του δικτύου, στις επιθέσεις ενάντια στην ακεραιότητα της πληροφορίας και της κυκλοφορίας της μέσα στο δίκτυο, τις επιθέσεις ενάντια στην ιδιωτικότητα των χρηστών και επιθέσεις ενάντια στην δυνατότητα ταυτοποίησης του χρήστη.

Στην πρώτη κατηγορία τοποθετούμε :

- τις επιθέσεις άρνησης εξυπηρέτησης, οι οπόιες εξαντλούν το εύρος του καναλιού πληροφορίας (bandwidth) του δικτύου καθιστόντας το ανίκανο να ανταποκριθεί στις απαιτήσεις του δικτύου. Υπάρχει μεγάλη ποικιλία τέτοιου τύπου επιθέσεων.

- τις επιθέσεις στα συστήματα και τους κόμβους της διαδικτυακής υποδομής του συστήματος.

Στη δεύτερη κατηγορία επιθέσεων τοποθετούμε :

- τις επιθέσεις κακόβουλου κώδικα

- τις επιθέσεις που έχουν να κάνουν με τη ροή πληροφορίας στο δίκτυο, είτε μεταβάλλοντας την είτε εκτρέπωντας την.

- τις επιθέσεις πλαστογράφησης πληροφορίας

Στην τρίτη κατηγορία τοποθετούμε :

- την κατασκόπευση ομάδας χρηστών

- την ανάλυση της ροής του δικτύου για εξαγωγή πληροφορίας

- την απόκτηση των προσωπικών δεδομένων των χρηστών του συστήματος

Στην τέταρτη κατηγορία τοποθετούμε :

- τις επιθέσεις ενάντια στους κωδικούς που χρησιμοποιούν οι χρήστες για την πρόβαση τους στο σύστημα

- τις επιθέσεις πλαστοπρωσοπίας (man-in-the-middle attacks, session hijacking, επιθέσεις επανάληψης συνεδρίας, επιθέσεις αποκύρηξης κτλ.)

Το παραπάνω μοντέλο μας υποδεικνύει τις πιθανες απειλές τις οποίες μπορεί να αντιμετωπίσει ένα σύστημα e-αξιολόγησης. Στη συνέχεια θα κάνουμε μια μικρή παρουσίαση στα πρότυπα υλοποίησης δικτύων για συστήματα e-αξιολόγησης.

2.4 Τα υπάρχοντα πρότυπα και η ασφάλεια σε επίπεδο hardware

Η ασφάλεια στην e-αξιολόγηση, όντας μια απευθείας εφαρμογή της ασφάλειας δικτύων, απότελείται από δύο ξεχωριστά κομμάτια και περιλαμβάνει την ασφάλεια σε επίπεδο εξοπλισμού (hardware, δηλ. του φυσικού δικτύου, των υπολογιστικών συστημάτων κτλ.) και την ασφάλεια σε επίπεδο λογισμικού (software, δηλ. τα προγράμματα, τις πλατφόρμες και τις διαδικτυακές εφαρμογές).

Ένα σύστημα e-αξιολόγησης είναι μια εφαρμογή βασισμένη σε πρωτόκολλα που επιτρέπουν τόσο την ανώνυμη επικοινωνία μεταξύ των αξιολογητών και της αρχής όσο και πολλές και διαφορετικές μορφές ανώνυμης επικοινωνίας και ανταλλαγής αρκετών διαφορετικών μορφών δεδομένων (π.χ. απλές φόρμες-ερωτηματολόγια, εφαρμογές flash, εφαρμογές τηλεσυνδιάσκεψης κτλ.). Αυτό σημαίνει ότι ένα τέτοιο σύστημα θα πρέπει, ανάλογα με τη φύση του προγράμματος e-αξιολόγησης να μπορεί να ικανοποιεί αυτές τις ανάγκες. Καθώς οι ανάγκες αυτες διαφέρουν από ίδρυμα σε ίδρυμα, ή ακόμα και από σχολή σε σχολή, μπορούμε να έχουμε συστήματα e-αξιολόγησης με πολύ διαφορετικά χαρακτηριστικά.

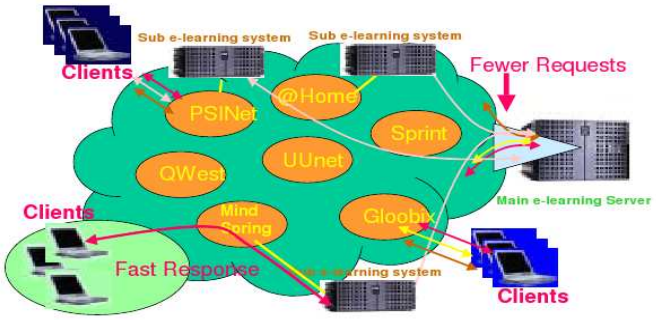
Ένα καλό σημείο αναφοράς για συστήματα τέτοιου τύπου είναι τα συστήματα τα οποία χρησιμοποιούνται σε εφαρμογές e-learning. Τυπικά, τέτοια συστήματα είναι δομημένα με βάση την εξής αρχιτεκτονική :

- Ένας κύριος εξυπηρετητής (server) ο οποίος περιέχει το κύριο μέρος της λειτουργικότητας του συστήματος όπως μαθησιακό περιεχόμενο, πρωτόκολλα επικοινωνίας, το portal του προγράμματος κτλ.

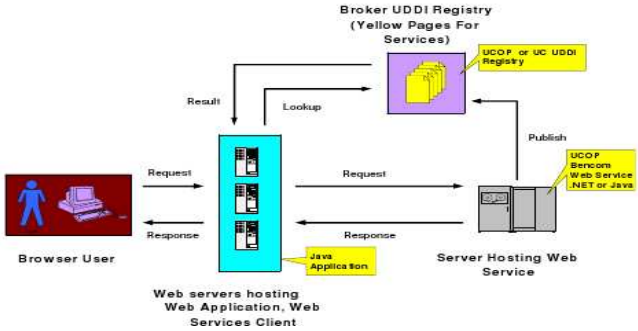
- Επιμέρους εξυπηρετητές οι οποίοι αναλαμβάνουν επιμέρους λειτουργίες, όπως π.χ. τοποικούς εξυπηρετητές τηλεσυνδιάσκεψης, διανεμημένους εξυπηρετητές βασικής λειτουργικότητας και backup servers, εξυπηρετητές γραμματείας κτλ.

Το δίκτυο εξυπηρετείται από ευρυζωνική διαδικτυακή υποδομή η οποία επιτρέπει τη διαμεταγωγή δεδομένων με μεγάλες ταχύτητες.

Η δομή ενός δικτύου όπως αυτό που περιγράψαμε απεικονίζεται στις δυο παρακάτω εικόνες :



Σχ.1 : Κατανεμημένο δίκτυο e-learning



Σχ.2 : Εξυπηρέτηση χρήστη

Τέτοιου τύπου συστήματα προτυποποιήθηκαν σύμφωνα με το πρότυπο ISO/IEC 24751:2008 [20]. Το πρότυπο αυτό, σε συνδυασμό με το πρότυπο ISO/IEC 15408-1 [19] το οποίο χρησιμοποιείται για την αξιολόγηση της ασφάλειας ενός δικτύου, μπορεί να μας δώσει μια ολοκληρωμένη προσέγγιση δόμησης ενός ασφαλούς συστήματος e-αξιολόγησης.

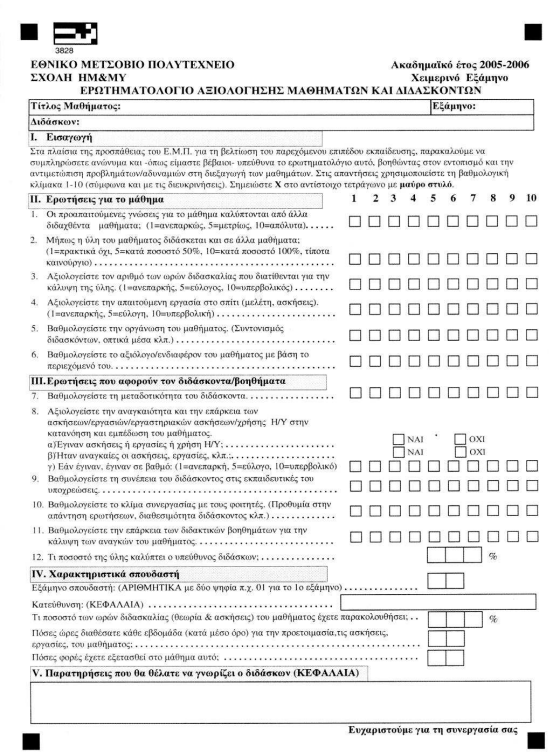
2.5 Τα υπάρχοντα πρότυπα και η ασφάλεια σε επίπεδο software

Αντίστοιχα με τη διαδικτυακή υποδομή του σύστήματος, τόσο το λογισμικό της πλατφόρμας όσο και το περιεχόμενο θα πρέπει να έχουν κάποια βασικά χαρακτηριστικά τα οποία θα επιτρέπουν ευκολία χρήσης, ασφάλεια, δυνατότητα πολλαπλών χρήσεων του περιεχομένου και συμβατότητα με αντίστοιχα προγράμματα.

Οι περισσότερες εφαρμογές e-αξιολόγησης τις οποίες έχουμε εντοπίσει στο διαδίκτυο αφορούν συστήματα τα χαρακτηριστικά ασφαλείας έχουν σα βάση συστήματα απλής ταυτοποίησης της ταυτότητας του χρήστη με χρήση κωδικού πρόσβασης (password-based systems). Τα συστήματα τα οποία θα εξετάσουμε στην εργασία αυτή ανήκουν στις εφαρμογές e-learning.

Ένας από τους πρώτους φορείς που ασχολήθηκε με την e-αξιολόγηση στην εκπαιδευτική διαδικασία είναι το πανεπιστήμιο της Γλασκώβης με το πρόγραμμα Teaching with Independent Learning Technologies-TILT [44]. Στο πρόγραμμα αυτό χρησιμοποιήθηκαν διάφορες μέθοδοι (ερωτηματολόγια, μικρά κουίζ, καταγραφή της εμπιστοσύνης των φοιτητών) για τη μέτρηση της αποτελεσματικότητας της εκπαιδευτικής διαδικασίας σε πολλά διαφορετικά περιβάλλοντα. Μετεξέλιξη του προγράμματος αυτού είναι το πρόγραμμα Evaluation of Learning with Information & Communication Technology-ELICT [45].

Το πιό διαδεδομένο πακέτο λογισμικού e-learning είναι το πακέτο ανοικτού κώδικα Moodle [2], το οποίο αποτελεί μια πλατφόρμα η οποία χρησιμοποιεί διάφορα υπάρχοντα πρότυπα για την κατασκευή εφαρμογών e-learning. Το σύστημα βασίζεται στη γλώσσα προγραμματισμού ιστοσελίδων PHP και σε σχεσιακές βάσεις δεδομένων που κάνουν χρήση της γλώσσας διαχείρισης SQL (π.χ. MySQL, Microsoft SQL, Oracle, PostGRE SQL). Στην Ελλάδα, το σύστημα αυτό έχει χρησιμοποιηθεί για την ανάπτυξη πλατφόρμας e-learning στο Εθνικό Μετσόβιο Πολυτεχνείο [39] σύμφωνα με την εργασία [42]. Στα πλαίσια της εσωτερικής αξιολόγησης της εκπαιδευτικής διαδικασίας στο ΕΜΠ γίνεται χρήση ερωτηματολογίων στα οποία οι φοιτητές καταγράφουν την άποψη τους για την εκπαιδευτική διαδικασία. Ένα τέτοιο ερωτηματολόγιο είναι το παρακάτω :



3828

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ **Ακαδημαϊκό έτος 2005-2006**
ΣΧΟΛΗ ΗΜ&ΜΥ **Χειμερινό Εξάμηνο**
ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΜΑΘΗΜΑΤΩΝ ΚΑΙ ΔΙΔΑΣΚΟΝΤΩΝ

Τίτλος Μαθήματος: **Εξάμηνο:**
Διδάσκων:

I. Εισαγωγή

Στα πλαίσια της προσπάθειας του Ε.Μ.Π. για τη βελτίωση του παρεχόμενου επιπέδου εκπαίδευσης, παρακαλούμε να συμπληρώσετε ανώνυμα και -όπως είμαστε βέβαιοι- υπεύθυνα το ερωτηματολόγιο αυτό, βοηθώντας στον εντοπισμό και την αντιμετώπιση προβλημάτων/αδυναμιών στη διεξαγωγή των μαθημάτων. Στις απαντήσεις χρησιμοποιείστε τη βαθμολογική κλίμακα 1-10 (σύμφωνα και με τις διευκρινήσεις). Σημειώστε **X** στο αντίστοιχο τετράγωνο με **μαύρο στυλό**.

II. Ερωτήσεις για το μάθημα	1	2	3	4	5	6	7	8	9	10
1. Οι προαπαιτούμενες γνώσεις για το μάθημα καλύπτονται από άλλα διδαχθέντα μαθήματα; (1=ανεπαρκώς, 5=μετρίως, 10=απόλυτα)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2. Μήπως η ύλη του μαθήματος διδάσκεται και σε άλλα μαθήματα; (1=εγκυκλία όχι, 5=κατά ποσοστό 50%, 10=κατά ποσοστό 100%, τίποτα καινούργιο)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3. Αξιολογείστε τον αριθμό των ωρών διδασκαλίας που διατίθενται για την κάλυψη της ύλης; (1=ανεπαρκής, 5=εύλογος, 10=υπερβολικός)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4. Αξιολογείστε την απαιτούμενη εργασία στο σπίτι (μελέτη, ασκήσεις). (1=ανεπαρκής, 5=εύλογη, 10=υπερβολική)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5. Βαθμολογείστε την οργάνωση του μαθήματος. (Συντονισμός διδασκόντων, οπτικά μέσα κλπ.)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6. Βαθμολογείστε το αξιολογο/ενδιαφέρον του μαθήματος με βάση το περιεχόμενό του.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
III. Ερωτήσεις που αφορούν τον διδάσκοντα/βοηθήματα										
7. Βαθμολογείστε τη μεταδοτικότητα του διδάσκοντα.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8. Αξιολογείστε την αναγκαιότητα και την επάρκεια των ασκήσεων/εργασιών/εργαστηριακών ασκήσεων/χρήσης Η/Υ στην κατανόηση και εμπέδωση του μαθήματος α)Έγιναν ασκήσεις ή εργασίες ή χρήση Η/Υ; ☐ ΝΑΙ ☐ ΟΧΙ β)Ήταν αναγκαίες οι ασκήσεις, εργασίες, κλπ.; ☐ ΝΑΙ ☐ ΟΧΙ γ) Εάν έγιναν, έγιναν σε βαθμό: (1=ανεπαρκή, 5=εύλογο, 10=υπερβολικό)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9. Βαθμολογείστε τη συνέπεια του διδάσκοντος στις εκπαιδευτικές του υποχρεώσεις.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10. Βαθμολογείστε το κλίμα συνεργασίας με τους φοιτητές. (Προθυμία στην απάντηση ερωτήσεων, διαθεσιμότητα διδάσκοντος κλπ.)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11. Βαθμολογείστε την επάρκεια των διδακτικών βοηθημάτων για την κάλυψη των αναγκών του μαθήματος.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12. Τι ποσοστό της ύλης καλύπτει ο υπεύθυνος διδάσκων;										%
IV. Χαρακτηριστικά σπουδαστή										
Εξάμηνο σπουδαστή: (ΑΡΙΘΜΗΤΙΚΑ με δύο ψηφία π.χ. 01 για το 1ο εξάμηνο)										
Κατεύθυνση: (ΚΕΦΑΛΑΙΑ)										
Τι ποσοστό των ωρών διδασκαλίας (θεωρία & ασκήσεις) του μαθήματος έχετε παρακολουθήσει;										%
Πόσες ώρες διαθέσατε κάθε εβδομάδα (κατά μέσο όρο) για την προετοιμασία.τις ασκήσεις, εργασίες, του μαθήματος;										
Πόσες φορές έχετε εξεταστεί στο μάθημα αυτό;										

V. Παρατηρήσεις που θα θέλατε να γνωρίζει ο διδάσκων (ΚΕΦΑΛΑΙΑ)

Ευχαριστούμε για τη συνεργασία σας

Σχ.3 : Ερωτηματολόγιο αξιολόγησης ΕΜΠ

Ένα άλλο τέτοιο σύστημα ηλεκτρονικής αξιολόγησης της εκπαιδευτικής διαδικασίας έχει υλοποιηθεί από το Ελληνικό Ανοικτό Πανεπιστήμιο [61].

Υπάρχουν διάφορα πρότυπα τα οποία μπορούν να ακολουθηθούν για τη δόμηση ενός συστήματος e-learning. Ένα τέτοιο πρότυπο είναι το Sharable Content Object Reference Model-SCORM [53] το οποίο προέρχεται από την υπηρεσία Προηγμένης Καταναμημένης Εκπαίδευσης του υπουργείου Άμυνας των Η.Π.Α. . Το πρότυπο αυτό έχει σα βάση τη γλώσσα XML και χρησιμοποιείται κατά τέτοιο τρόπο έτσι ώστε να καθορίζει το ρυθμό εκπαίδευσης του εκπαιδευόμενου αλλά και να τον συγχρονίζει με το υλικό και τον τρόπο αξιολόγησης του. Ένα τέτοιο παράδειγμα συστήματος εμφανίζεται στην εργασία [64]. Άλλα πρότυπα αυτού του τύπου είναι το πρότυπο ανοικτού κώδικα LAMS [37], το οποίο κάνει χρήση της γλώσσας προγραμματισμού Java καθώς και το πρωτόκολλο AICC [11].

Αξίζει να σημειωθεί ότι υπάρχει έντονη ερευνητική και επιχειρηματική δραστηριότητα γύρω από το αντικείμενο της e-αξιολόγησης στο e-learning. Παραδείγματα αποτελούν το ετήσιο συνέδριο Distance Learning Administration Conference [1], ο οργανισμός ascilite (Australasian Society for Computers in Learning in Tertiary Education) [17] και η εταιρία eLearnCAMPUS [16]

2.6 Η εφαρμογή της κρυπτογραφίας στην ασφάλεια

Με τον όρο κρυπτογραφία ονομάζουμε ¨τη μελέτη των μαθηματικών τεχνικών που σχετίζονται με διάφορες όψεις της ασφάλειας δεδομένων όπως είναι η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η ταυτοποίηση μιας οντότητας και η ταυτοποίηση της προέλευσης μιας πληροφορίας¨ [40]. Με βάση αυτό τον ορισμό, τεχνικές κρυπτογραφίας χρησιμοποιούνται με σκοπό η πληροφορία που διακινείται εντός του δικτύου που εξυπηρετεί το σύστημα e-αξιολόγησης να είναι μη αναγνώσι-

μη από κάποιο μη εξουσιοδοτημένο χρήστη ή επιτιθέμενο στο σύστημα ο οποίος την έχει υποκλέψει.

Ας θυμηθούμε τα κριτήρια ασφαλείας που πρέπει να πληρούνται για ένα ασφαλές περιβάλλον δικτύωσης :

- Εμπιστευτικότητα.
- Ακεραιότητα.
- Διαθεσιμότητα.
- Αναγνωρισιμότητα και εξακρίβωση ταυτότητας για τα διαπιστευμένα μέλη του δικτύου.
- Εξουσιοδότηση (έλεγχος τοπικής πρόσβασης).
- Μη δυνατότητα αποκύρηξης πράξης.

Σε ένα σύστημα e-αξιολόγησης, εκτός από τις παραπάνω απαιτήσεις, μπορούν να προστεθούν κατά περίπτωση και οι παρακάτω :

- Ιδιωτικότητα : Δεν πρέπει να υπάρχει κανένας έμμεσος ή άμεσος τρόπος με τον οποίο να μπορεί κανείς να συνάγει τις επιλογές ενός αξιολογητή.
- Επιλεξιμότητα : Δηλαδή κάθε αξιολογητής μπορεί να αξιολογήσει μόνο μία φορά.
- Ανεξάρτητη επιβεβαίωση : Κάθε αξιολογητής μπορεί να επιβεβαιώσει ότι καταμετρήθηκε τη επιλογή του.
- Καθολική Επιβεβαίωση : Κάθε μέλος ή τρίτος παρατηρητής μπορεί να ελέγξει αν η αξιολόγηση είναι δίκαια.
- Εντιμότητα : Κάθε συμμετέχων στην διαδικασία της αξιολόγησης δεν μπορεί να γνωρίζει έστω και μερικό αποτέλεσμα πριν την καταμέτρηση.
- Ευστάθεια : Να μπορεί να αυτοπροστατεύεται από κάθε λάθος ή σκόπιμη ενέργεια των συμμετεχόντων.
- Receipt-freeness: Κάθε συμμετέχων στην αξιολόγηση δεν μπορεί να πείσει κάποιον άλλο παρατηρητή για το τι αυτός επέλεξε και να τον επηρεάσει αντίστοιχα.
- Ανεξαρτησία σύγκρουσης : Δεν είναι δυνατό να παίρνουν δύο ή περισσότεροι χρήστες ίδια διακριτικά διαπίστευσης (αποτρέπει το ενδεχόμενο της διπλής ¨ψήφου¨)

Οι απαιτήσεις ασφαλείας, έτσι όπως βλέπουμε ότι προσαρμόζονται για ένα σύστημα e-αξιολόγησης, μοιάζουν πολύ με τις απαιτήσεις ασφαλείας για συστήματα ηλεκτρονικής ψηφοφορίας (e-voting systems) και, κατά συνέπεια, η προσέγγιση ασφάλειας ενός δικτύου που χρησιμοποιείται για ένα σύστημα e-αξιολόγησης θα μοιάζει σε μεγάλο βαθμό με την προσέγγιση που ακολουθείται σε συστήματα ηλεκτρονικής ψηφοφορίας. Αυτό σημαίνει ότι οι τεχνικές και η στρατηγική που θα

ακολουθήσουμε είναι εμπνευσμένες από αυτές που χρησιμοποιούνται σε συστήματα e-voting.

Ένα πρωτόκολλο e-voting προστατεύει τη διαδικασία της ηλεκτρονικής ψηφοφορίας κρυπτογραφόντας και υπογράφοντας ψηφιακά τις ψήφους και συγκεντρώνοντας τις ανώνυμα, αποτρέπωντας τόσο την ανάγνωση πληροφορίας από το σύστημα όσο και τη μεταβολή της ροής της πληροφορίας και άρα υλοποιεί τα κριτήρια ασφαλείας που θεσπίστηκαν παραπάνω. Αντίστοιχα, για ένα σύστημα e-αξιολόγησης, θα γίνει προσαρμογή των τεχνικών αυτών με τέτοιο τρόπο έτσι ώστε να διασφαλίζεται τόσο η ακεραιότητα των πληροφοριών όσο και το αδιάβλητο της διαδικασίας μέσω της ικανοποίησης των παραπάνω κριτηρίων.

Στο επόμενο κεφάλαιο θα κάνουμε μια παρουσίαση των βασικών τεχνικών κρυπτογραφίας που χρησιμοποιούνται σε συστήματα e-αξιολόγησης, δίνοντας ιδιαίτερη έμφαση σε πρωτόκολλα e-voting.

Μέρος ΙΙΙ

Εισαγωγή στην κρυπτογραφία

ΚΕΦΑΛΑΙΟ 3

Εισαγωγή στην κρυπτογραφία

3.1 Ιστορία της κρυπτογραφίας

Η κρυπτογραφία είναι 'μια αρχαία τέχνη και μια νεαρή επιστήμη' [38] και έχει μια μακρά και πολύ ενδιαφέρουσα ιστορία. Ιστορικά, η κρυπτογραφία πρωτοεμφανίζεται τόσο στον αρχαίο αιγυπτιακό πολιτισμό, όσο και στους αρχαίους Έλληνες (η σκυτάλη των αρχαίων σπαρτιατών). Οι αρχαίοι Ρωμαίοι χρησιμοποιούσαν κατά κόρον κρυπτοσυστήματα μονοαλφαβητικής αντικατάστασης, δηλαδή κρυπτοσυστήματα που βασίζονται στην αντικατάσταση ενός γράμματος με ένα άλλο, με πιό γνωστό το κρυπτόγραμμα του Καίσαρα, που αντικαθιστούσε κάθε γράμμα με το κατά τρεις θέσεις επόμενο του στο λατινικό αλφάβητο. Η πρώτη μεγάλη εξέλιξη στο αντικείμενο έγινε από τους Άραβες τον 9ο αι. μ.Χ. και πιό συγκεκριμένα από τον Άραβα πολυμαθή Αλ-Κιντί στο έργο του 'Ένα χειρόγραφο περί της αποκρυπτογράφησης κρυπτογραφημένων μηνυμάτων', και αφορούσε την τεχνική της ανάλυσης συχνοτήτων, όπου και παρατηρείται η πρώτη πρακτική μέθοδος κρυπτανάλυσης. Στη συνέχεια, εμφανίστηκε στην αναγεννησιακή Ευρώπη η τεχνική της πολυαλφαβητικής αντικατάστασης στα έργα των φιλόσοφων Alberti και Trithemius (σαν πολυαλφαβητική αντικατάσταση ορίζεται η κλάση κρυπτοσυστημάτων όπου κάθε χαρακτήρας από το αλφάβητο μπορεί να αντικατασταθεί με διαφορετικούς χαρακτήρες), η οποία και έφτασε στο απόγειο της με το κρυπτοσύστημα Vigenère, το οποίο και καλούταν le chiffre indéchiffrable, δηλαδή το άθραυστο κρυπτόγραμμα.

Οι πρώτες επιτυχείς επιθέσεις σε κρυπτοσυστήματα πολυαλφαβητικής αντικατάστασης πραγματοποιήθηκαν πρώτα από τον Charles Babbage και λίγο αργότερα από τον Friedrich Kasiski στα μέσα του 19ου αιώνα. Με την έλευση του 20ου αιώνα, για να ικανοποιηθούν οι αυξανόμενες ανάγκες για κρυπτογραφημένες επικοινωνίες που ήρθαν ως αποτέλεσμα του τηλέγραφου, του τηλεφώνου και του ασυρμάτου, συντελέστηκε η εκμηχάνιση της κρυπτογραφίας, με πιό διάσημο παράδειγμα τη μηχανή Enigma του γερμανικού στρατού κατά το δεύτερο παγκόσμιο πόλεμο. Οι μηχανές αυτές χρησιμοποιούσαν διατάξεις από ρότορες με τους οποίους αντιστοιχούσαν διαδοχικά κάθε στοιχείο του απλού μηνύματος σε κάποιο άλλο. Μέχρι και πριν από μερικές δεκαετίες, οι σχεδόν αποκλειστικοί χρήστες της κρυπτογραφίας ήταν ο στρατός και τα διπλωματικά σώματα που χρησιμοποιούσαν την κρυπτογραφία για να μεταδίδουν απόρρητες και ευαίσθητες πληροφορίες. Μια πολύ αναλυτική παρουσίαση της ιστορίας της κρυπτογραφίας στους αιώνες βρίσκεται στο βιβλίο του D. Kahn, The codebreakers: the story of secret writing [32].

Μετά το δεύτερο παγκόσμιο πόλεμο, η έλευση των ηλεκτρονικών υπολογιστών και, ιδιαίτερα μετά τη δεκαετία του 1970, των δικτύων ηλεκτρονικών υπολογιστών, μετέφερε το πεδίο εφαρμογών από το στρατό στις εμπορικές εφαρμογές. Την περίοδο

αυτή συντελέσθηκαν τρεις μεγάλες εξελίξεις οι οποίες έφεραν επανάσταση στο πεδίο της κρυπτογραφίας. Η πρώτη ήταν η θεμελίωση της μαθηματικής θεωρίας πληροφοριών με τις εργασίες σταθμό 'A mathematical theory of communication' [55] και τη συμπληρωματική της 'Communication theory of secrecy systems' [56] από τον Claude Shannon στα τέλη της δεκαετίας του 1940. Στην εργασία αυτή εισήχθησαν οι βασικές για την κρυπτογραφία έννοιες της εντροπίας της πληροφορίας ($H(X) = \mathbb{E}_X[I(x)] = -\sum_{x\in\mathbb{X}} p(x)\log p(x)$ για τυχαία μεταβλητή X και $\mathbb{X}$ το σύνολο όλων των δυνατών μηνυμάτων για την τυχαία μεταβλητή Q), της απόστασης μοναδιαιότητας (unicity distance - το μήκος του κρυποτκειμένουπου είναι αναγκαίο για να σπαστεί το κρυπτοσύστημα ελαττώνοντας τον αριθμό των πλαστών κλειδιών στο μηδέν) και της τέλειας μυστικότητας (perfect secrecy - η πιθανότητα απόκτησης του απλού κειμένου από το αντίστοιχο κρυπτοκείμενο να είναι ίδια με το να αποκτηθεί το απλό κείμενο χωρίς την ύπαρξη του κρυπτοκειμένου).

Η δεύτερη ήταν η δουλειά του Horst Feistel στην IBM όπου και ανέπτυξε την τεχνική των δικτύων Feistel κάνοντας χρήση της καινοτόμας τεχνικής των S-boxes για κρυπτογράφηση των μηνυμάτων. Οι τεχνικές αυτές αποτελούν πλέον τη βάση για το σχεδιασμό κρυπτοσυστημάτων που κάνουν χρήση ενός μυστικού κλειδιού.(τα οποία και καλούνται συμμετρικά κρυπτοσυστήματα ή κρυπτοσυστήματα μυστικού κλειδιού). Χαρακτηριστικά παραδείγματα είναι τα κρυπτοσυστήματα DES, AES και Blowfish.

Η τρίτη και πιο σημαντική εξέλιξη ήρθε το 1976 με την εργασία των Ralph Merkle και Whitfield Diffie : 'New directions in cryptography' [14], όπου και προτάθηκε η πρωτοποριακή ιδέα της κρυπτογραφίας δημοσίου κλειδιού και παρείχε μια νέα μέθοδο για ανταλλαγή κλειδιού, η ασφάλεια της οποίας βασίζεται στην μη υπολογιστική επιλυσιμότητα του προβλήματος του διακριτού λογαρίθμου, το οποίο και θα ορίσουμε στη συνέχεια. Η ιδεά της κρυπτογραφίας δημοσίου κλειδιού βασίζεται στην ιδέα ότι οποιοσδήποτε μπορεί να χρησιμοποιήσει το δημόσιο κλειδί ενός ατόμου για να κρυπτογραφήσει ένα μήνυμα αλλά το μήνυμα αυτό μπορεί να το αποκρυπτογραφήσει μόνο ο κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί. Η ιδέα αυτή προκάλεσε μια επανάσταση στο χώρο της κρυπτογραφίας αποτελώντας τη βάση για τεχνολογίες όπως η ψηφιακή υπογραφή ενός εγγράφου, τα συστήματα συμφωνίας κλειδιού με κρυφό κωδικό, τα συστήματα διαμοιρασμού μυστικού, τα συστήματα ηλεκτρονικής ψηφοφορίας και ηλεκτρονικών δημοπρασιών και πολλές άλλες. Επίσης, αποτέλεσε αφορμή και για πολλές θεωρητικές καινοτομίες σε διάφορους τομείς των μαθηματικών όπως η άλγεβρα, η θεωρία πολυπλοκότητας και πολλούς άλλους.

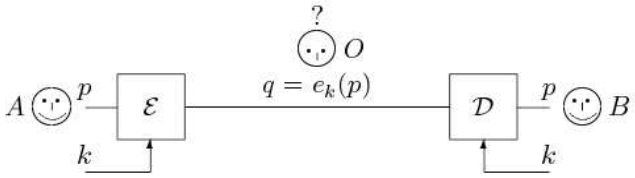
Από τα μέσα της δεκαετίας του '80, με τη δυναμική είσοδο τόσο της επιχειρηματικής όσο και της ακαδημαϊκής κοινότητας στην κρυπτογραφική έρευνα, το πεδίο της κρυπτογραφίας διευρύνθηκε θεαματικά και προς πολλές κατευθύνσεις, τόσο θεωρητικά όσο και σε επίπεδο εφαρμογών. Αυτό συνέβη για να καλυφθούν οι ολοένα και μεγαλύτερες ανάγκες για ασφάλεια των ψηφιακών δεδομένων καθώς τόσο η υιοθεσία ηλεκτρονικών συσκευών για συναλλαγές (π.χ. τραπεζικά ATM) όσο και η έλευση και εξάπλωση του διαδικτύου και του ψηφιακού ταχυδρομείου (e-mail) (που με τη σειρά τους αποτέλεσαν τη βάση για περισσότερες εφαρμογές όπως την ψηφιακή υπογραφή εγγράφων, το ηλεκτρονικό εμπόριο και πολλές άλλες) κατέστησαν προφανή την ανάγκη προστασίας ευαίσθητων δεδομένων και διασφάλισης των ηλεκτρονικών συναλλαγών.

3.1.1 Κρυπτοσυστήματα δημοσίου και μυστικού κλειδιού

Πρωτού ξεκινήσουμε την περιγραφή των δυο κύριων κατηγοριών κρυπτοσυστημάτων αξίζει να αναφέρουμε μια από τις κυρίαρχες συμβάσεις στην περιγραφή κρυπτοσυστημάτων. Σύμφωνα με τη σύμβαση αυτή, που πρωτοεμφανίστηκε στο [14], οι δύο οντότητες που ανταλλάσουν κρυπτογραφημένα μηνύματα καλούνται Αλίκη και Μπομπ (Alice και Bob) ενώ ο αντίπαλος ο οποίος υποκλέπτει το μήνυμα καλείται Εύα (Eve). Η σύμβαση αυτή εμπλουτίστηκε με τα χρόνια με διάφορα ονόματα ανάλογα με τα χαρακτηριστικά των πρωτοκόλλων και των κρυπτοσυστημάτων που εμφανίστηκαν κατά καιρούς. Έτσι, ακολουθώντας τη σύμβαση αυτή, θα χρησιμοποιούμε μεταφρασμένα στα Ελληνικά, τα αντίστοιχα ονόματα στις περιγραφές των διαφόρων κρυπτογραφικών εργαλείων τα οποία θα παρουσιάσουμε.

Το χαρακτηριστικό που καθορίζει τις δύο κύριες κατηγορίες κρυπτοσυστημάτων είναι ο τύπος κλειδιού τον οποίο χρησιμοποιούν, ο οποίος και καθορίζει τη λειτουργία τους. Υπάρχουν δύο κύριες κατηγορίες κρυπτοσυστημάτων. Ο πρώτος τύπος είναι τα λεγόμενα συμμετρικά κρυπτοσυστήματα ή κρυπτοσυστήματα μυστικού κλειδιού. Τα κρυπτοσυστήματα αυτά λειτουργούν ως εξής :

Η Αλίκη θέλει να στείλει στον Μπομπ ένα κρυπτογραφημένο μήνυμα. Έχοντας συμφωνήσει απο πριν με τον Μπομπ για το μυστικό κλειδί που θα χρησιμοποιήσουν, η Αλίκη κρυπτογραφεί το μήνυμα με το κλειδί αυτό και το στέλνει στον Μπομπ. Ο Μπομπ λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το προσυμφωνυμένο κλειδί. Εαν στο ενδιάμεσο της επικοινωνίας ένα τρίτο πρόσωπο, το οποίο καλούμε Εύα, υποκλέψει το μήνυμα δεν μπορεί να το διαβάσει εάν δεν έχει το κλειδί που έχουν η Αλίκη και ο Μπομπ. Να σημειώσουμε ότι τα ονόματα Αλίκη, Μπομπ και Εύα είναι ονόματα που χρησιμοποιούνται στην κρυπτογραφία ως εθιμοταξία.



Σχ.4 : $\mathcal{E}$ είναι ο αλγόριθμος κρυπτογράφησης, $\mathcal{D}$ είναι ο αλγόριθμος αποκρυπτογράφησης, k είναι το κλειδί, p είναι το μήνυμα και q το κρυπτοκείμενο.

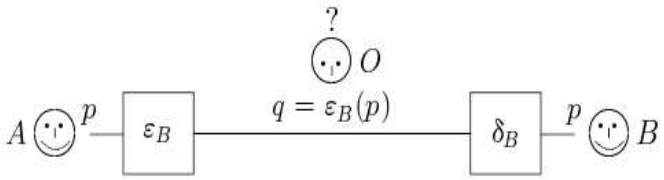
Υπάρχουν δύο υποκατηγορίες συμμετρικών κρυπτοσυστημάτων : τα block κρυπτοσυστήματα και τα stream κρυπτοσυστήματα.

Τα block κρυπτοσυστήματα κρυπτογραφούν τα δεδομένα ανά block δοθέντος μήκους. Τα κρυπτοσυστήματα αυτά χρησιμοποιούν δίκτυα Feistel, τα οποία αναφέραμε προηγουμένως, για την κρυπτογράφηση των δεδομένων. Τα πιο διαδεμένα κρυπτοσυστήματα αυτού του τύπου είναι τα DES (μαζί με τις πιό σύγχρονες παραλλαγές του όπως το 3DES), το AES και το Blowfish.

Τα stream κρυπτοσυστήματα συνδυάζουν τα bits του μηνύματος με ένα ψευδοτυχαίο ρεύμα από bits (το οποίο καλείται ρεύμα κλειδιού (keystream» για να κρυπτογραφήσουν τα δεδομένα. Τα πιό διαδεδομένα κρυπτοσυστήματα δημοσίου κλειδιού είναι τα RC4, A5/1, A5/2 και FISH.

Τα κρυπτοσυστήματα δημοσίου κλειδιού βασίζονται στη χρήση ενός ζεύγους κλειδιών τα οποία καλούνται ιδιωτικό και δημόσιο κλειδί. Ο Μπομπ συνδυάζει το δημόσιο κλειδί της με το κρυπτοσύστημα και κατασκευάζει ένα δημόσιο αλγόριθμο

κρυπτογράφησης, τον οποίο και αναρτά. Η Αλίκη κρυπτογραφεί το μήνυμα της με το δημόσιο αλγόριθμο και τον στέλνει στο Μπομπ. Ο Μπομπ χρησιμοποιεί τον ιδιωτικό αλγόριθμο αποκρυπτογράφησης (που είναι συνδυασμός του ιδιωτικού κλειδιού και του κρυπτοσυστήματος και των οποίων μοναδικός γνώστης είναι ο Μπομπ) για να αποκρυπτογραφήσει το μήνυμα. Εάν στο ενδιάμεσο της επικοινωνίας ένα τρίτο πρόσωπο, το οποίο καλούμε Εύα, υποκλέψει το μήνυμα δεν μπορεί να το διαβάσει εάν δεν έχει το ιδιωτικό κλειδί αποκρυπτογραφησης του Μπομπ.



Σχ.5 : ϵ_B είναι ο δημόσιος αλγόριθμος κρυπτογράφησης , δ_B είναι ο ιδιωτικός αλγόριθμος αποκρυπτογράφησης, B είναι το ζεύγος κλειδιών, p είναι το μήνυμα και q το κρυπτοκείμενο.

Υπάρχει μεγάλει ποικιλία κρυπτοσυστημάτων δημοσίου κλειδιού, όπως τα κρυπτοσυστήματα MQV, ECDSA, McEliece, NTRU, Pallier και Chor-Rivest. Τα δύο πιό διαδεδομένα, όμως, κρυπτοσυστήματα δημοσίου κλειδιού, τα οποία και θα παρουσιάσουμε στη συνέχεια είναι το κρυπτοσύστημα RSA και το κρυπτοσύστημα ElGamal.

3.1.2 Κρυπτοσυστήματα μυστικού κλειδιού

Το κρυπτοσύστημα DES

Το κρυπτοσύστημα DES (Data Encryption Standard) αποτελεί το πλέον γνωστό κρυπτοσύστημα μυστικού κλειδιού και ήταν το πρώτο κρυπτοσύστημα του οποίου, στα μέσα της δεκαετίας του '70, ο αλγόριθμος έγινε ανοικτός και με πλήρως διευκρινισμένες λεπτομέρειες υλοποίησης. Το κρυπτοσύστημα αυτό ορίζεται από το αμερικανικό standard FIPS 46-2 [62].

Το κρυπτοσύστημα DES (όπως και όλα τα κρυπτοσυστήματα αυτού του τύπου) βασίζει την ασφάλεια στην κατασκευή μίας ασφαλούς συνάρτησης κρυπτογράφησης από τη σύνθεση αρκετών απλών πραξεων οι οποίες μεμονωμένα προσφέρουν ανεπαρκή προστασία. Τέτοιου τύπου πράξεις αποτελούν οι γραμμικοί μετασχηματισμοί, οι αντιμεταθέσεις, οι μεταφράσεις (π.χ. το XOR), οι πολλαπλασιασμοί modulo, και οι απλές αντικαταστάσεις.

Αρχικά θα ορίσουμε κάποιες βασικές έννοιες για τα κρυπτοσυστήματα μυστικού κλειδιού. Σαν κρυπτοσύστημα παραγώγου, ορίζουμε ένα κρυπτοσύστημα το οποίο συνδυάζει δύο ή περισσότερους, μετασχηματισμούς με τέτοιο τρόπο έτσι ώστε το κρυπτοσύστημα που παράγεται σαν αποτέλεσμα είναι πιό ασφαλές από τα επιμέρους κομμάτια του. Πλέον, ένα δίκτυο αντιμετάθεσης-αντικατάστασης είναι ένα κρυπτοσύστημα παραγώγου το οποίο αποτελείται από ένα αριθμό από φάσεις ο καθένας από τις οποίες αποτελείται από αντικαταστάσεις και αντιμεταθέσεις.

Ένα επαναληπτικό block κρυπτοσύστημα είναι ένα κρυπτοσύστημα το οποίο κάνει χρήση διαδοχικών επαναλήψεων μίας εσωτερικής συνάρτησης η οποία καλείται συνάρτηση γύρου. Οι παράμετροι για ένα τέτοιο κρυπτοσύστημα περιλαμβάνουν

τον αριθμό γύρων r, το μέγεθος σε bit του block n, το μέγεθος σε bit του κλειδιού εισόδου K από το οποίο παράγονται r υποκλειδιά K_i για κάθε γύρο. Δίκην αντιστρεψιμότητας, για κάθε τιμή του K_i η συνάρτηση γύρου είναι μια αμφιμονοσήμαντη και επί συνάρτηση (αμφίρριψη) πάνω στην είσοδο του γύρου.

Ένα δίκτυο Feistel είναι ένα επαναληπτικό κρυπτόγραμμα το οποίο απεικονίζει ένα $2t$-bit απλό κείμενο (L_0, R_0) για t blocks L_0 και R_0 σε ένα κρυπτοκείμενο (L_r, R_r) μέσω μίας διαδικασίας r γύρων, όπου $r > 1$. Για $1 \leq i \leq r$, στο γύρο i έχουμε την απεικόνιση $(L_{i-1}, R_{i-1}) \rightarrow^{K_i} (L_i, R_i)$ ως εξής : $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, όπου κάθε υποκλειδί K_i παράγεται από το κλειδί K.

Το κρυπτοσύστημα DES είναι ένα δίκτυο Feistel το οποίο επεξεργάζεται blocks απλού κειμένου μήκους 64 bits παράγοντας blocks κρυπτοκείμενο μήκους 64 bits. Το μήκος κλειδιού είναι 56 bits (64 bits όπου 8 από αυτά τα bits χρησιμοποιούνται ως bits ελέγχου). Τα 2^{56} κλειδιά υλοποιούν 2^{56} από τις 2^{64} δυνατές αμφιρρίψεις για τα 64-μπιτα blocks. Το DES κάνει χρήση 16 γύρων και ενός αρχικού (IP) και ενός τελικού (IP^{-1}) πίνακα αντιμετάθεσης.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Σχ.6 : Οι πίνακες αντιμετάθεσης IP και IP^{-1}

Πριν από τον κύριο γύρο, το block σπάει σε δύο μισά μήκους 32 bit τα οποία και επεξεργάζεται εναλασσόμενα, διαδικασία η οποία καλείται σχήμα Feistel. Η διαδικασία αυτή διασφαλίζει ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι παρόμοιες διαδικασίες (αρκεί να χρησιμοποιηθούν τα υποκλειδιά στην ανάστροφη σειρά για να έχουμε αποκρυπτογράφηση). Με το σύμβολο $\oplus$ συμβολίζουμε το αποκλειστικό ή (XOR). Η συνάρτηση γύρου f ανακατεύει μισό block χρησιμοποιόντας το αντίστοιχο για το γύρο υποκλειδί και το αποτέλεσμα της συνδυάζεται με το άλλο μισό του block. Πλέον, τα μισά εναλλάσονται μεταξύ τους πριν τον επόμενο γύρο μέχρι και το πέρας της διαδικασίας.

Η συνάρτηση γύρου λειτουργεί πάνω σε μισό block σε κάθε γύρω και αποτελείται από τέσσερις φάσεις :

1. Εξάπλωση : Το block εξαπλώνεται από τα 32 στα 48 bit χρησιμοποιόντας την αντιμετάθεση εξάπλωσης όπου τα μισά από τα bit αντιγράφονται με βασή τον πίνακα επέκτασης E. το αποτέλεσμα είναι 8 κομμάτια των 6-bit, όπου καθένα περιέχει ένα αντίγραφο από 4 αντίστοιχα bits εισόδου συν ένα αντίγραφο από το αμέσως γειτονικό bit από καθένα τα κομμάτια εισόδου σε οποιαδήποτε από τις δύο πλευρές.

2. Ανάμιξη κλειδιών : Το αποτέλεσμα συνδυάζεται με το υποκλειδί χρησιμοποιώντας την πράξη XOR. 16 υποκλειδιά μεγέθους 48 bits (ένα για κάθε γύρο) παράγονται από το κύριο κλειδί χρησιμοποιώντας το πρόγραμμα υποκλειδών, το οποίο και θα περιγράψουμε παρακάτω.

3. Αντικατάσταση : έπειτα από την ανάμειξη με το υποκλειδί, το block χωρίζεται σε 8 κομμάτια των 6-bit πριν γίνει επεξεργασία τους από τα κουτιά αντικατάστασης (S-boxes) Κάθε ένα από αυτά τα οκτώ S-boxes αντικαθιστά τα έξι bit εισόδου με τέσσερα bit εξόδου σύμφωνα με ένα μη γραμμικό μετασχηματισμό ο οποίος παρέχεται με τη μορφή ενός πίνακα ανάθεσης (lookup table). Τα S-boxes αποτελούν τον πυρήνα της ασφάλειας του DES καθώς χωρίς αυτά το κρυπτοσύστημα θα ήταν ένας γραμμικός μετασχηματισμός και άρα θα ήταν πάρα πολύ ευκολο να σπάσει.

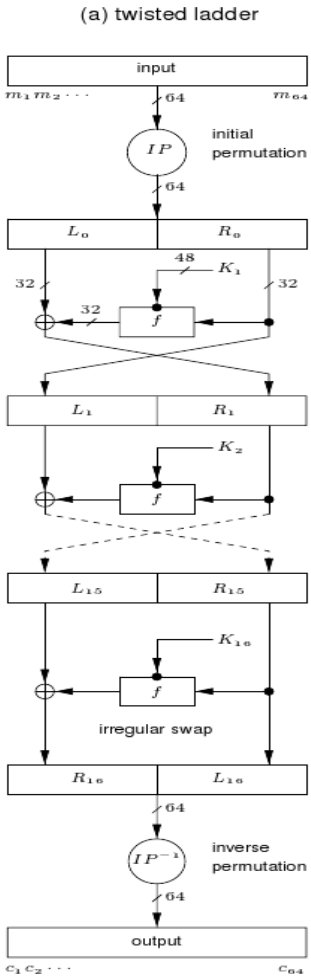
4. Αντιμετάθεση : Τέλος, οι 32 έξοδοι από τα S-boxes επαναταξινομούνται με χρήση του σταθερού πίνακα αντιμετάθεσης P. Ο σκοπός αυτής της αντιμετάθεσης είναι, έπειτα από την εξάπλωση, τα bit εξόδου να είναι εξαπλωμένα σε έξι διαφορετικά S-boxes στον επόμενο γύρο.

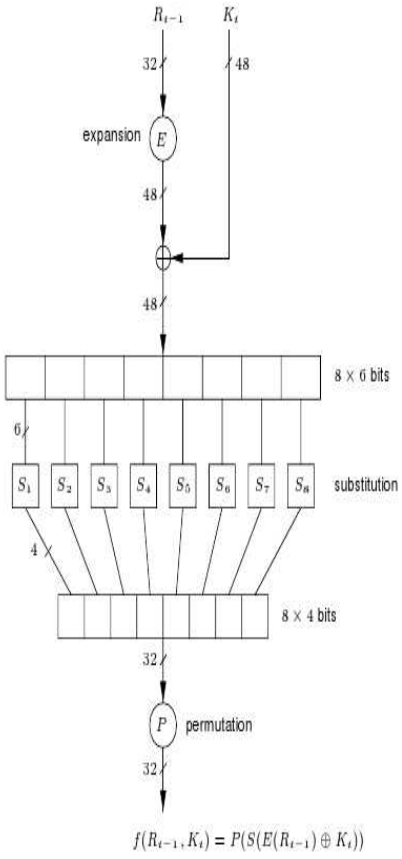
E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Σχ.7 : Οι πίνακες επέκτασης E και αντιμετάθεσης P

Για το πρόγραμμα κλειδιών αρχικά επιλέγονται 56 από τα 64 bits μέσω αντιμεταθετικής επιλογής (τα υπόλοιπα 8 χρησιμοποιούνται ως ελεγκτές σφάλματος). Έπειτα τα 56 αυτά bits χωρίζονται σε δύο μισά των 28 bits, καθένα από τα οποία τα μεταχειριζόμαστε διαφορετικά. Σε διαδοχικούς γύρους, καθένα από τα μισά ¨περιστρέφεται¨ αριστερά κατά 1 ή 2 bits (ανάλογα με το γύρο) και τα 48 bits του υποκλειδιού επιλέγονται από μια δεύτερη αντιμεταθετική επιλογή (24bits από το αριστερό μισό και 24 bits από το δεξιό μισό). Κάθε bit χρησιμοποιείται σε περίπου 14 από τα 16 υποκλειδιά. Η ίδια διαδικασία με ανάστροφη φορά χρησιμοποιείται για την κατασκευή των υποκλειδιών για την αποκρυπτογράφηση.





Καθώς το κρυπτοσύστημα αυτό ήταν το πρώτο εμπορικό κρυπτοσύστημα με ευρεία χρήση και ανοικτές στο ευρύ κοινό τις προδιαγραφές, τόσο του αλγορίθμου όσο και τις λεπτομέρειες της υλοποίησης, το DES υπήρξε, και συνεχίζει να αποτελεί, αντικείμενο πολλών κρυπταναλυτικών επιθέσεων. Πλέον, μετά από 30 χρόνια από την καθιέρωση του το DES θεωρείται μη ασφαλές και ξεπερασμένο λόγω του μικρού μεγέθους κλειδιού και των διαφόρων αδυναμιών που έχουν κατά καιρούς βρεθεί από τις κρυπταναλυτικές επιθέσεις εναντίων του. Τον αντικαταστάτη του, το κρυπτοσύστημα AES θα περιγράψουμε αμέσως μετά.

Το κρυπτοσύστημα AES

Το κρυπτοσύστημα AES είναι ένα κρυπτοσύστημα το οποίο επιλέχθηκε μέσα από μια πενταετή διαδικασία αξιολόγησης ανάμεσα από 15 διαφορετικά κρυπτοσυστήματα και έγινε το στάνταρ για τους συμμετρικούς αλγόριθμους κρυπτογράφησης του Αμερικανικού Ινστιτούτου Στάνταρ και Τεχνολογίας ως U.S. FIPS PUB 197 (FIPS 197) το Νοέμβριο του 2001 [43]. Το κρυπτοσύστημα αυτό σχεδιάστηκε από τους J. Daemen και V. Rijmen και το αρχικό του όνομα ήταν Rijndael, σα συνδυασμός των ονομάτων των δημιουργών του. Ακολουθεί μια σύντομη περιγραφή του κρυπτοσυστήματος.

Το κρυπτοσύστημα AES έχει σταθερό μέγεθος block 128 bits και μεταβλητό μέγεθος κλειδιού 128, 192 και 256 bits Σε αντίθεση με τον προκάτοχο του, το AES είναι ένα δίκτυο αντικατάστασης-αντιμετάθεσης και όχι ένα δίκτυο Feistel.

Το κρυπτοσύστημα κάνει χρήση 4 βασικών διαδικασίων και ενός προγράμματος κλειδιών με βάση την παρακάτω διαδικασία :

- Επέκταση Κλειδιών με χρήση του προγράμματος κλειδιών Rijndael
- Αρχικός γύρος
    1. Πρόσθεση Κλειδιού Γύρου βάση του προγράμματος κλειδιών Rijndael
- Γύροι
    1. SubBytes : ένα μη γραμμικό βήμα αντικατάστασης όπου κάθε byte αντικαθίσταται με κάποιο άλλο με βάση ένα πίνακα αντικατάστασης.
    2. ShiftRows : ένα βήμα αντιμετάθεσης όπου κάθε σειρά του στιγμιοτύπου του μετακινείται κυκλικά με ένα συγκεκριμένο αριθμό βημάτων
    3. MixColumns : μια πράξη ανάμειξης η οποία εκτελείται στις στήλες του στιγμιότυπου συνδυάζοντας 4 bytes ανά στήλη.
    4. AddRoundKey : Συνδυασμός κάθε byte του στιγμιότυπου με το κλειδί του γύρου βάση του προγράμματος κλειδιών Rijndael.
- Τελευταίος γύρος
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

Το κρυπτοσύστημα AES, όντας το στάνταρ για τα κρυπτοσυστήματα μυστικού κλειδιού σήμερα και ένα από τα πιό ευρέως χρησιμοποιούμενα κρυπτοσυστήματα σε πολλές εφαρμογές έχει δοκιμαστεί με επιτυχία εναντίον πολλών και διαφορετικών επιθέσεων. Η μόνη ένσταση που έχει εγερθεί από την κρυπτογραφική κοινότητα είναι το γεγονός ότι το κρυπτοσύστημα σαν αλγεβρική απεικόνιση είναι πολύ απλό και ενδέχεται αυτό να δώσει τη δυνατότητα εύρεσης μιας αποτελεσματικής επίθεσης εναντίον του κρυπτοσυστήματος.

3.1.3 Κρυπτοσυστήματα δημοσίου κλειδιού

Το κρυπτοσύστημα RSA

Το κρυπτοσύστημα RSA πρωτοπαρουσιάστηκε από τους Ronald Rivest, Adi Shamir και Leonard Adleman το 1978 με την εργασία τους 'A method for obtaining digital signatures and public-key cryptosystems' [50]. Το κρυπτοσύστημα αυτό βασίζει την υπόθεση ασφαλείας του στη μη υπολογιστική επιλύσημότητα του πρόβλήματος της παραγοντοποίησης μεγάλων ακεραίων. Ο αλγόριθμος του κρυπτοσυστήματος είναι ο παρακάτω :

Δημιουργία κλειδιών Η Αλίκη δημιουργεί το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί με τον εξής τρόπο :

1. Δημιουργεί δύο μεγάλους πρώτους αριθμούς p, q (και οι δύο να είναι περίπου ιδιού μεγέθους)

2. Υπολογίζει $n = pq\ ,\ \phi(n) = (p-1)(q-1)$

3. Επιλέγει έναν ακέραιο $e\ ,\ 1 < e < \phi(n)$ τέτοιο ώστε $\gcd(e, \phi) = 1$

4. Υπολογίζει μοναδικό ακέραιο $d\ ,\ 1 < d < \phi$ τέτοιο ώστε $ed \equiv 1 \mod \phi(n)$

5. Το δημόσιο κλειδί είναι το (n, e), το ιδιωτικό είναι το d.

Κρυπτογράφηση Για να κρυπτογραφήσει έναν ακέραιο $m\ ,\ 0 \leq m < n$ (το αρχικό κείμενο), ο Μπομπ πρέπει να υπολογίσει το $c = m^e \mod n$ (το κρυπτοκείμενο)

Απόκρυπτογράφηση Η Αλίκη ανακτά το αρχικό κείμενο m από το κρυπτοκείμενο c υπολογίζοντας $m = c^d \mod n$

Το κρυπτοσύστημα ElGamal

Το κρυπτοσύστημα ElGamal παρουσιάστηκε από τον Taher ElGamal το 1985 στην εργασία του 'A public key cryptosystem and a signature scheme based on discrete logarithms' [25] και βασίζει την υπόθεση ασφαλείας του στη μη υπολογιστική επιλυσιμότητα του πρόβλήματος του διακριτού λογαρίθμου. Το πρόβλημα του διακριτού λογαρίθμου ορίζεται ώς εξής :

Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n, a ένας γεννήτορας της G και $b \in G$. Ο διακριτός λογάριθμος του b στη βάση a, που συμβολίζεται $log_a b$ είναι ο μοναδικός ακέραιος x , $0 \leq x \leq n-1$, τέτοιος ώστε $b = a^x$

Πλέον, το πρόβλημα του διακριτού λογαρίθμου (Discrete Logarithm Problem-DLP)ορίζεται ως εξής :

- Δεδομένα : Ένας πρώτος αριθμός π, ένας γεννήτορας a του $\mathbb{Z}_p^*$ και ένα στοιχείο $b \in \mathbb{Z}_p^*$.
- Ζητούμενα : Να βρεθεί ακέραιος x, $0 \leq x \leq p-2$, τέτοιος ώστε $a^x \equiv b (mod\ p)$

Το κρυπτοσύστημα ElGamal μπορεί να βασιστεί σε οποιαδήποτε οικογένεια ομάδων για την οποία το πρόβλημα του διακριτού λογαρίθμου θεωρείται υπολογιστικά μη επιλύσιμο. Συνήθως, χρησιμοποιούμε μια υποομάδα G_q τάξης q της $\mathbb{Z}_p$, όπου p, q μεγάλοι πρώτοι αριθμοί που ικανοποιούν $q \mid p-1$. Σαν εναλλακτική, μπορούν να χρησιμοποιηθούν ελλειπτικές καμπύλες πάνω σε πεπερασμένα σώματα, περίπτωση για την οποία το πρόβλημα του διακριτού λογαρίθμου θεωρείται πιο δύσκολο. Ο αλγόριθμος του κρυπτοσυστήματος για την πρώτη περίπτωση είναι ο παρακάτω :

Δημιουργία κλειδιών Η Αλίκη δημιουργεί το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί με τον εξής τρόπο :

1. Δημιουργεί μεγάλο πρώτο αριθμό p και ένα γεννήτορα g για την πολλαπλασιαστική ομάδα $\mathbb{Z}_p$ των ακεραίων modulo p

2. Επιλέγει τυχαίο ακέραιο α, όπου $1 \leq \alpha \leq p-2$ και υπολογίζει $h = g^\alpha$

3. Το δημόσιο κλειδί είναι η τριπλέτα (p, g, h) και το ιδιωτικό είναι το α

Κρυπτογράφηση Ο Μπομπ λαμβάνει το δημόσιο κλειδί (p, g, h) της Αλίκης και θέλει με αυτό να κρυπτογραφήσει ένα μύνημα m, όπου $0 \leq m < p$. Θα πρέπει τότε να ακολουθήσει την ακόλουθη διαδικασία :

1. Επιλέγει τυχαίο ακέραιο k , $0 \leq k \leq p-2$
2. Υπολογίζει $x = g^k$, $y = mh^k$
3. Στέλνει το κρυπτοκείμενο $c = (x, y)$ στην Αλίκη.

Απόκρυπτογράφηση Για να ανακτήσει το αρχικό κείμενο m η Αλίκη από το $c = (x, y)$ η Αλίκη θα πρέπει να πράξει τα ακόλουθα :

1. Χρησιμοποιόντας το ιδιωτικό κλειδί α, υπολογίζει $r = x^{p-1-\alpha}$ ($r = x^{p-1-\alpha} = x^{-\alpha} = (g^k)^{-\alpha} = g^{-k\alpha}$)
2. Ανακτά το αρχικό κείμενο m υπολογίζοντας $m = yr \mod p$

ΚΕΦΑΛΑΙΟ 4

Βασικά Εργαλεία

Καθώς στο προηγούμενο κεφάλαιο κάναμε μια εισαγωγή στην κρυπτογραφία και τα κρυπτοσυστήματα δημόσιου και μυστικού κλειδιού, στο κεφάλαιο αυτό θα δούμε μια σειρά από εργαλεία τα οποία και χρησιμοποιούνται σαν δομικά κομμάτια ενός συστήματος ηλεκτρονικής ψηφοφορίας και αποτελούν προϊόν της εξέλιξης της κρυπτογραφικής έρευνας με σκοπό την προσομοίωση και μαθηματική μοντελοποίηση διεργασιών μυστικής ανταλλαγής πληροφορίας μεταξύ δύο ή περισσότερων πλευρών.

4.1 Κρυπτογραφικά Εργαλεία

4.1.1 Σχήματα διαμοιρασμού μυστικού

Με τον όρο σχήμα διαμοιρασμού μυστικού secret sharing scheme εννούμε μια μέθοδο για τη διανομή ενός μυστικού σε μια ομάδα συμμετεχόντων, σε καθέναν από τους οποίους δίνεται ένας κλήρος, δηλαδή ένα κομμάτι, του μυστικού. Μεμονωνμένα κομμάτια δεν έχουν κάποια χρησιμότητα από μόνα τους. Ο σκοπός ενός σχήματος διαμοιρασμού μυστικού είναι το να διαμοιραστεί μια πληροφορία σε N οντότητες με τέτοιο τρόπο έτσι ώστε μόνο κάποιες προαποφασισμένες ομάδες των οντοτήτων αυτών να μπορούν να ανακατασκευάσουν μετέπειτα την πληροφορία. Διαφορετικές ομάδες δε θα πρέπει να μπορούν να αποκτήσουν καθόλου γνώση του μυστικού.

Στην παρούσα εργασία θα δούμε το $(t+1, N)$ σχήμα μυστικού διαμοιρασμού του Shamir [54] το οποίο επιτρέπει σε μια ομάδα $t+1$ από N να μπορούν να ανακατασκευσουν την πληροφορία.

Έστω σύνολο μυστικών σχηματίζουν σώμα F (είτε σύνολο $X \subset \mathbb{R}$ είτε $\mathbb{Z}_p$). Τότε το F θα πρέπει τουλάχιστον $N+1$ διαφορετικά στοιχεία, $0, 1, \ldots, N$.

Διαμοιρασμός των κλήρων Ένα μυστικό $s \in F$ διανέμεται μεταξύ των N οντοτήτων και κάθε οντότητα παίρνει κλήρο $s_j \in F$. Επιλέγουμε ένα τυχαίο πολυώνυμο f βαθμού t στο σώμα F του οποίου το s είναι ρίζα, δηλ. $f(0) = s$. Δίνουμε στην οντότητα A_j τον κλήρο $s_j = f(j)$.

Επανακατασκευή του μυστικού Ένα σύνολο από $t+1$ οντότητες A αποκτά το μυστικό s ανακατασκευάζοντας το πολυώνυμο (με χρήση παρεμβολής Lagrange) και υπολογίζοντας $s = f(0)$:

$$s = f(0) = \sum_{j \in A} f(j)\lambda_{j,A} = \sum_{j \in A} s_j \lambda_{j,A}$$

με

$$\lambda_{j,A} = \prod_{l \in A - \{j\}} \frac{l}{l-j}$$

Η πληροφορία την οποία t ή λιγότερες οντότητες έχουν για το πολυώνυμο f δεν αποκαλύπτει τίποτα για την τιμή $f(0) = s$. Οποιαδήποτε τιμή επιλεχθεί για $f(0) = r$, οι οντότητες οι οποίες την επέλεξαν μπορούν να υπολογίσουν πολυώνυμο g το οποίο να ικανοποιεί $g(0) = r$.

4.1.2 Δημόσια επαληθεύσιμος διαμοιρασμός μυστικού

Ένα σχήμα δημόσια επαληθεύσιμου διαμοιρασμού μυστικού (Publicly verifiable secret sharing - PVSS) είναι ένα σχήμα διαμοιρασμού μυστικού που επιτρέπει να επαληθευθεί ότι ο διανομέας έχει διανείμει έγκυρους κλήρους του μυστικού (κάθε σύνολο από $t+1$ οντότητες θα αποκτήσει το ίδιο μυστικό) και επιτρέπει τη σύλληψη μιας μη έντιμης οντότητας η οποία πλαστογραφεί τον κλήρο της.

Το σχήμα που παρουσιάζουμε στην παρούσα εργασία είναι αυτό του B. Schoenmakers [52] και ειναι ένα από τα πιο διαδεδομένα σχήματα δημόσια επαληθεύσιμου διαμοιρασμού μυστικού.

Αρχικοποίηση Επιλέγουμε σώμα $\mathbb{Z}_p$ και γεννήτορες G, g. Η οντότητα A_j επιλέγει το ιδιωτικό κλειδί z_j και δημοσιεύει το δημόσιο κλειδί $h_j = g^{z_j}$. Ο διαμοιραστής θέλει να μοιράσει ένα μυστικό g^s στις οντότητες.

Διαμοιρασμός των κλήρων Ο διαμοιραστής επιλέγει τυχαίο πολυώνυμο βαθμού t στο $\mathbb{Z}_p$:

$$p(x) = \sum_{k=0}^{t} \alpha_k x^k$$

όπου $\alpha_0 = s$ και $\alpha_1, \ldots, \alpha_t \in \mathbb{Z}_p$. Το πολυώνυμο κρατιέται μυστικό και οι δεσμεύσεις $C_k = G^{\alpha_k}$, $0 \leq k \leq t$, όπως επίσης και οι κρυπτογραφημένοι κλήροι $H_j = h_j^{p(j)}$, $j = 1, 2, \ldots, N$ δημοσιεύονται. Επιπλέον, ο διαμοιραστής δείχνει ότι οι κρυπτογραφημένοι κλήροι είναι συνεπείς : Έστω $X_j = \prod_{k=0}^{t} C_k^{j^k} = G^{\sum_{k=0}^{t} \alpha_k j^k} = G^{p(j)}$. Τότε ο διαμοιραστής δείχνει ότι

$$\log_G X_j = \log_{h_j} = H_j$$

κάνοντας χρήση μη διαλογικής απόδειξης της ισότητας διακριτών λογαρίθμων (Κεφ. 4.2.2).

Επανακατασκευή του μυστικού Η αρχή A_j αποκρυπτογραφεί τον κλήρο της $S_j = g^{p(j)}$ υπολογίζοντας $S_j = H_j^{1/z_j}$. Η A_j αποδεκνύει, επίσης, ότι $\log_G h_j = -\log_{H_j} S_j$. Επιπλέον, ας υποθέσουμε ότι $t+1$ αρχές A_j , $j \in A$ παράγουν τις σωστές τιμές για τα S_j , $j \in A$. Το μυστικό ανακτάται με χρήση παρεμβολής Lagrange :

$$\prod_{j \in A} S_j^{\lambda_{j,A}} = \prod_{j \in A} g^{p(j)\lambda_{j,A}} = g^{\sum_{j \in A} p(j)\lambda_{j,A}} = g^{p(0)=g^s}$$

όπου $\lambda_{j,A} = \prod_{l \in A - \{j\}} \frac{l}{l-j}$ είναι ένας συντελεστής Lagrange.

Ένα άλλο σχήμα τέτοιου τύπου είναι αυτό του M. Stadler [57]

4.1.3 Ψηφιακές υπογραφές - Τυφλές υπογραφές

Με τον όρο ψηφιακή υπογραφή καλούμε ένα μαθηματικό σχήμα το οποίο επιτρέπει σε μία οντότητα να συνδέσει την ταυτότητα της με μια πληροφορία. Η διαδικασία της υπογραφής συνίσταται στην μετατροπή ενός μηνύματος και μίας μυστικής πληροφορίας που έχει στην κατοχή της μια οντότητα σε μια ετικέτα που καλείται υπογραφή.

Τυπικά, ένα σχήμα ψηφιακής υπογραφής για το χώρο μυνημάτων M είναι μια τριάδα (η, σ, Γ) όπου :

- η είναι ένας πολυωνυμικού χρόνου πιθανοτικός αλγόριθμος που κατασκευάζει το δημόσιο (pk) και το αντίστοιχο ιδιωτικό (sk) κλειδί του υπογράφοντα.
- σ είναι ένας πολυωνυμικού χρόνου αλγόριθμος υπογραφής όπου για μήνυμα $m \in M$ και ιδιωτικό κλειδί sk κατασκευάζει μια υπογραφή s
- Γ είναι ένας πολυωνυμικού χρόνου αλγόριθμος επαλήθευσης υπογραφής όπου για το ζεύγος μυνήματος-υπογραφής (m, s) και το δημόσιο κλειδί pk απαντάει είτε Ναι είτε Όχι.

Οι απαιτήσεις για να είναι επιτυχής η ψηφιακή υπογραφή μιας πληροφορίας είναι να είναι αυθεντική (μόνο ο αποστολέας να μπορεί να υπογράψει την υπογράψει) και δημόσια επαληθεύσιμη (να μπορεί οποιοσδήποτε τρίτος να επαληθεύσει κατά πόσον δοθείσα υπογραφή είναι ορθή).

Οι ψηφιακές υλοποιούνται με χρήση κρυπτοσυστημάτων δηκοσίου κλειδιού όπως το RSA, το DSA, το ECDSA κ.α.

Ο όρος 'τυφλή υπογραφή' εισήχθη από τον D. Chaum στην εργασία του [9]. Με τον όρο τυφλή υπογραφή εννοούμε μια μορφή ψηφιακής υπογραφής στην οποία το περιεχόμενο του μηνήματος αποκρύπτεται ('τυφλώνεται') προτού υπογραφεί. Η υπογραφή την οποία παίρνουμε μπορεί πλέον να επαληθευθεί δημόσια έναντι του αυθεντικού, μη τυφλωμένου μηνύματος με τη μορφή μιας κανονικής ψηφιακής υπογραφής.

Τυπικά, ένα σχήμα τυφλής υπογραφής για το χώρο μηνυμάτων M είναι μια πεντάδα $(\eta, \chi, \sigma, \delta, \Gamma)$ όπου :

- η είναι ένας πολυωνυμικού χρόνου πιθανοτικός αλγόριθμος που κατασκευάζει το δημόσιο (pk) και το αντίστοιχο ιδιωτικό (sk) κλειδί του υπογράφοντα.
- χ είναι ένας πολυωνυμικού χρόνου αλγόριθμος ¨τύφλωσης¨, οπου για μήνυμα $m \in M$ ένα δημόσιο κλειδί pk και μια τυχαία συμβολοσειρά r κατασκευάζουν ένα τυφλό μήνυμα m'
- σ είναι ένας πολυωνυμικού χρόνου αλγόριθμος υπογραφής όπου για τυφλό μήνυμα m' και ιδιωτικό κλειδί sk κατασκευάζει μια τυφλή υπογραφή s' για το μήνυμα m'
- δ είναι ένας πολυωνυμικού χρόνου αλγόριθμος ανάκτησης όπου για τυφλή υπογραφή s' και την τυχαία συμβολοσειρά r ανακτούν την υπογραφή r για το μήνυμα m.

- Γ είναι ένας πολυωνυμικού χρόνου αλγόριθμος επαλήθευσης υπογραφής όπου για το ζεύγος μηνύματος-υπογραφής (m, s) και το δημόσιο κλειδί pk απαντάει είτε Ναι είτε Όχι.

Με τον όρο πολυωνυμικού χρόνου αλγόριθμο εννοούμε έναν αλγόριθμο του οποίου ο αριθμός των βημάτων εκτέλεσης του είναι άνω φραγμένος από ένα πολυώνυμο $T(n)$ του μεγέθους n της εισόδου του αλγορίθμου.

Ένα παράδειγμα λειτουργίας της τυφλής υπογραφής είναι το παρακάτω.

Εαν ο υπογραφών έχει ένα δημόσιο κλειδί RSA (n, e) και το αντίστοιχο ιδιωτικό κλειδί d, μπορεί να υπογράψει ένα μήνυμα m , $m \in \mathbb{Z}_n$ ως $sm^d \mod n$. Δοθείσης της υπογραφής s του μηνύματος m, καθένας μπορεί να επαληθεύσει την εγκυρότητα της ελέγχοντας εάν $m \stackrel{?}{=} s^e \mod n$. Έτσι, η υπογραφή ενός μυνήματος και η επαλήθευση της πραγματοποιούνται μέσω της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης του κρυπτοσυστήματος RSA.

Ας υποθέσουμε, τώρα, ότι κάποιος αιτείται να λάβει την υπογραφή του υπογράφοντος για το μήνυμα m χωρίς να θέλει να του αποκαλύψει το περιεχόμενο του μηνύματος (π.χ. επικύρωση της ψήφου σε εκλογές από τον εκλογικό αντιπρόσωπο). Από τον υπογράφοντα ζητείται να υπογράψει τυφλά το μήνυμα χωρίς να ξέρει τι υπογράφει.

Εάν ο υπογράφων έχει δημόσιο κλειδί RSA (n, e) και το αντίστοιχο ιδιωτικό κλειδί d, ο αιτών την τυφλή υπογραφή τη λαμβάνει για μήνυμα m ως εξής :

1. Ο αιτών ¨τυφλώνει¨ το μήνυμα m του σε $m' = mr^e \mod n$ όπου $r \in_R \mathbb{Z}_n$ τυχαίο, και στέλνει το m' στον υπογράφοντα.

2. Ο υπογράφων υπογράφει το ¨τυφλό¨μήνυμα m' και στέλνει την υπογραφή $s' = m' \mod n$ στον αιτούντα.

3. Ο αιτών ανακτά την υπογραφή s για το μήνυμα m υπολογίζοντας :

$$s = \frac{s'}{r} = \frac{m'^d}{r} = \frac{m^d r^{ed}}{r} = \frac{m^d r}{r} = m^d(\pmod n)$$

Για σχήματα τυφλής υπογραφής κατωφλιού (threshold blind signatures), όπου το μυστικό κλειδί sk διαμοιράζεται μεταξύ N οντοτήτων δείτε [13] και [31].

4.1.4 Δέσμευση δυαδικού ψηφίου

Έστω ότι η Αλίκη θέλει να στείλει το δυαδικό ψηφίο (bit) b στο Μπομπ χωρίς να θέλει να του το αποκαλύψει άμεσα. Ο Μπομπ απαιτεί η Αλίκη να μην αλλάξει άποψη μετέπειτα και άρα το (bit) που θα του αποκαλύψει θα είναι ίδιο με αυτό που είχε σκεφτεί αρχικά. Η διαδικασία με την οποία αυτό επιτυγχάνεται καλείται δέσμευση δυαδικού ψηφίου (bit commitment)

Γενικά Η Αλίκη κρυπτογραφεί το (bit) b με κάποιο τρόπο και στέλνει το αποτέλεσμα στον Μπομπ. Ο Μπομπ δεν μπορεί να αποκρυπτογραφήσει το μήνυμα (και άρα να ανακτήσει το b) μέχρι η Αλίκη να του στείλει το κλειδί. Η κρυπτογράφηση του b καλείται blob. Γενικά, ένα σχήμα δέσμευσης δυαδικού ψηφίου είναι μια συνάρτηση $\xi : \{0, 1\} \times X \to Y$, όπου Q, U είναι πεπερασμένα σύνολα. Μια κρυπτογράφηση του b μπορεί να είναι μια οποιαδήποτε τιμή $\xi(b, k)$, $k \in X$. Ένα σχήμα δέσμευσης δυαδικού ψηφίου πρέπει να ικανοποιεί τις εξής ιδιότητες :

- Απόκρυψη - ο Μπομπ δεν μπορεί να καθορίσει την τιμή του b από το $\xi(b,k)$
- Δέσμευση - Η Αλίκη μπορεί να ανοίξει αργότερα το $\xi(b,k)$ αποκαλύπτοντας τα b,k που χρησιμοποιήσε κατά την κατασκευή του $\xi(b,k)$. Η Αλίκη δεν θα πρέπει να μπορεί να ανοίξει το blob ταυτόχρονα σαν 0 και σαν 1.

Εάν η Αλίκη θέλει να δεσμεύσει μια σειρά από bits θα πρέπει να δεσμεύσει το καθένα ξεχωριστά. Δέσμευση δυαδικού ψηφίου στο οποίο η Αλίκη μπορεί να ανοίξει το blob ταυτόχρονα σαν 0 και σαν 1 καλείται δέσμευση δυαδικού ψηφίου καταπακτής.

Ένα σχήμα δέσμευσης δυαδικού ψηφίου, το οποίο βρίσκεται στην εργασία [8] είναι το παρακάτω:

Έστω μεγάλος πρώτος αριθμός p, γεννήτορας g του $\mathbb{Z}_p$ και $G \in \mathbb{Z}_p$ γνωστά. Ο διακριτός λογάριθμος του G με βάση g δε θα πρέπει να είναι γνωστός ταυτόχρονα και στην Αλίκη και στο Μπομπ. Δέσμευση δυαδικού ψηφίου $\xi : \{0,1\} \times \mathbb{Z}_p \to \mathbb{Z}_p$ είναι

$$\xi(b,k) = g^k G^b$$

.

Έστω $\log_g G = a$. Το blob μπορεί να ανοιχτεί σαν b αποκαλύπτοντας το k και σαν $\neg b$ αποκαλύπτοντας $k-a$ εαν $b=0$ ή $k+a$ εάν $b=1$. Εάν η Αλίκη δεν γνωρίζει το a τότε δε μπορεί να ανοίξει το blob σαν $\neg b$. Ομοίως, εάν ο Μπομπ δε γνωρίζει το k, δε μπορεί να καθορίσει το b απλά γνωρίζοντας το $\xi(b,k) = g^k G^b$.

Ένα σχήμα δέσμευσης δυαδικού ψηφίου καταπακτής επιτυγχάνεται εάν η Αλίκη γνωρίζει το a. Εάν το το a είναι γνωστό στο Μπομπ και η Αλίκη ανοίξει το blob στο Μπομπ μέσω ενός μη υποκλέψιμου καναλιού, ο Μπομπ μπορεί να πει ψέμματα σε κάποιο τρίτο για το δεσμευμένο bit b με το να ισχυριστεί ότι έλαβε το $k+a$ ή το $k-a$ αντί του k. Τέτοιου τύπου σχήματα δέσμευσης δυαδικού ψηφίου καλούνται χαμαιλεοντικά.

Τέλος, αντί η Αλίκη να δεσμεύσει κάθε bit σε μια συμβολοσειρά s ανεξάρτητα, η Αλίκη μπορεί απλά να αναθέσει στο $0 \leq s < p$ το $\xi(s,k) = g^k G^s$, καθώς η γνώση του a δίνει στην Αλίκη τη δυνατότητα να ανοίξει το $\xi(s,k)$ ως οποιοδήποτε s', k' ικανοποιώντας τη σχέση $as + k = as' + k'$

4.1.5 Δίκτυα ανάμειξης

Η κύρια ιδέα πίσω από τα δίκτυα ανάμειξης είναι το να μετατίθεται κα να μεταβάλλεται μια ακολουθία αντικειμένων με σκοπό την απόκρυψη της αναλογίας μεταξύ στοιχείων της αρχικής και της τελικής ακολουθίας. Ο σκοπός της ιδέας αυτής ήταν να χρησιμοποιηθεί για την υλοποίηση ανώνυμου καναλιού [9].

Υπάρχουν n εξυπηρετητές ανάμειξης $M_1, \ldots, M_n$, καθένας με το αντίστοιχο ζεύγος δημοσίου και ιδιωτικού κλειδιού (E_j, D_j). Όταν κάποιος θέλει να στείλει ένα μήνυμα m μέσω ενός ανώνυμου καναλιού, το κρυπτογραφεί

$$E_1(E_2(\ldots E_n(m))\ldots)$$

και το στέλνει στο M_1.

Ο M_1 περιμένει μέχρι να φτάσουν περισσότερα κρυπτογραφημένα μηνύματα. Τότε, παίρνει τα μηνύματα που έχει λάβει, αφαιρεί ένα επίπεδο κρυπτογράφησης, τα αντιμεταθέτει με τυχαία σειρά και τα στέλνει στον M_2.

Πλέον, ο εξυπηρετητής ανάμειξης M_j λαμβάνει τα κρυπτογραφημένα μυνήματα, αφαιρεί ένα επίπεδο κρυπτογράφησης, τα αντιμεταθέτει με τυχαία σειρά και στέλνει $E_{j+1}(E_{j+2}(\ldots E_n(m))\ldots)$ στον M_{j+1}. Ο τελευταίος εξυπηρετητής ανάμειξης αποκρυπτογραφεί τα μηνύματα και τα στέλνει στους αποδέκτες.

Μπορούμε να απαιτήσουμε ένας εξυπηρετητής ανάμειξης να δώσει απόδειξη της ορθότητας της ορθής απόκρυψης και αντιμετάθεσης των μηνυμάτων [47]

4.1.6 Ομομορφική κρυπτογράφηση

Ας θεωρήσουμε ένα πιθανοτικό σχήμα κρυπτογράφησης. Έστω P ο χώρος των αρχικών κειμένων και C ο χώρος των κρυπτοκειμένων έτσι ώστε το P να είναι μία ομάδα υπό τη δυαδική πράξη $\oplus$ και C είναι μία ομάδα υπό τη δυαδική πράξη $\otimes$. Το στιγμιότυπο E του σχήματος πιθανοτικής κρυπτογράφησης δημιουργείται με την κατασκευή του ζεύγους δημοσίου και ιδιωτικού κλειδιού. Έστω $E_r(m)$ υποδηλώνει την κρυπτογράφηση του μηνύματος m χρησιμοποιώντας το σύνολο παραμέτρων r για το στιγμιότυπο E. Το r είναι ένας παράγοντας τυχαιότητας που χρησιμοποιείται στη διαδικασία κρυπτογράφησης.

Λέμε ότι ένα πιθανοτικό σχήμα κρυπτογράφησης είναι $(\oplus, \otimes)-$ομομορφικό εάν για κάθε στιγμιότυπο E του σχήματος κρυπτογράφησης, δοθέντων $c_1 = E_{r1}(m_1)$ και $c_2 = E_{r2}(m_2)$, υπάρχει r τέτοιο ώστε :

$$c_1 \otimes c_2 = E_r(m_1 \oplus m_2)$$

.

Για παράδειγμα, το κρυπτοσύστημα ElGamal είναι ομομορφικό. Εδώ, P είναι ένα σύνολο ακεραίων modulo p ($P = \mathbb{Z}_p$) και C είναι ένα σύνολο ζευγών $C = \{(a, b) \mid a, b \in \mathbb{Z}_p\}$. Η πράξη $\oplus$ είναι ένας πολλαπλασιασμός modulo p. Για τη δυαδική πράξη $\otimes$ ορισμένη σε κρυπτοκείμενα, ας πάρουμε τον πολλαπλασιασμό modulo p ανά συνιστώσα. Δυο αρχικά κείμενα m_0 , m_1 κρυπτογραφούνται σε

$$E_{k_0}(m_0) = (g^{k_0}, h^{k_0} m_0)$$

$$E_{k_1}(m_1) = (g^{k_1}, h^{k_1} m_1)$$

όπου k_0 , k_1 είναι τυχαία.

Ισχύει ότι

$$E_{k_0}(m_0)E_{k_1}(m_1) = (g^{k_0}g^{k_1}, h^{k_0}m_0h^{k_1}m_1) = (g^k, h^k m_0 m_1) = E_k(m_0 m_1)$$

για $k = k_0 + k_1$

Άρα, στο κρυπτοσύστημα ElGamal με πολλαπλασιασμό των κρυπτοκειμένων επιτυγχάνουμε την πρόσθεση των αντίστοιχων απλών κειμένων.

Αξίζει επίσης να σημειωθεί ότι και το κρυπτοσύστημα RSA είναι ένα κρυπτοσύστημα για το οποίο ισχύει η ιδιότητα της ομομορφικής κρυπτογράφησης.

Η έννοια της ομομοφικής κρυπτογράφησης πρωτοεμφανίστηκε στην εργασία [49]

4.2 Διαλογικές αποδείξεις γνώσης

Ένα σύστημα διαλογικής απόδειξης είναι ένα πρωτόκολλο που περιγράφει τον τρόπο με τον οποίο μπορεί κανείς να μεταβιβάσει μια (συνήθως πιθανοτική) απόδειξη ορθότητας μιας πρότασης. Στα πλαίσια μιας διαλογικής απόδειξης, μια μηχανή απόδειξης (Prover) επικοινωνεί με την μηχανή επαλήθευσης (Verifier) η οποία επιβεβαιώνει την ορθότητα της απόδειξης. Αποδείξεις που δεν αποκαλύπτουν καμία επιπρόσθετη γνώση για την πρόταση παρά μόνο την ορθότητα (με πολύ μεγάλη πιθανότητα) της, καλούνται αποδείξεις μηδενικής γνώσης.

Σε αυτό το κομμάτι θα παρουσιάσουμε διαλογικές αποδείξεις που χρησιμοποιούνται σε συστήματα ψηφοφορίας και, κατα συνέπεια, θα χρησιμοποιηθούν και σε συστήματα e-αξιολόγησης. Οι αποδείξεις αυτές βασίζονται στο πρόβλημα του διακριτού λογαρίθμου (δηλαδή στην υπόθεση ότι είναι μη υπολογιστικά επιλύσιμο) και το κρυπτοσύστημα ElGamal. Παρόμοιες αποδείξεις μπορούν να σχεδιαστούν και για άλλα κρυπτοσυστήματα (όπως, για παράδειγμα, το κρυπτοσύστημα του Pailler [δτζ01]). Όλες αυτές οι διαλογικές αποδείξεις μπορούν μετατραπούν σε μη διαλογικές χρησιμοποιόντας την τεχνική των Fiat-Shamir, όπως θα περιγράψουμε παρακάτω.

4.2.1 Κάνοντας μία διαλογική απόδειξη μη διαλογική

Όλα τα πρωτόκολλα διαλογικών αποδείξεων έχουν παρόμοια δομή : ο αποδείκτης (prover) θέλει να αποδείξει το P. Στέλνει κάποιο A στον επαληθευτή, ο οποίος δίνει μια πρόκληση C (αλληλουχία τυχαίων bits) και τελικά ο αποδείκτης υπολογίζει μία απάντηση $R = respond(P, A, C)$. Η επικοινωνία $(P; A, C, R)$ και το γεγονός ότι ο αποδείκτης δεν ήξερε τίποτα για το C τη στιγμή που είχε υπολογίσει το A πείθει τον επαληθευτή ότι το P ισχύει.

Το όλο πρωτόκολλο γίνεται μη διαλογικό εάν δώσουμε εντολή στον αποδείκτη να κατασκευάσει ο ίδιος τυχαία μη αναμενόμενα bits C. Ο επαληθευτής δε θα πρέπει να μπορεί να κατασκευάσει το C πριν να δημιουργείσει τα P και A. Οι Fiat και Shamir πρότειναν μία τεχνική όπου το C είναι το αποτέλεσμα μιας συνάρτησης κατακερματισμού : $C = H(P, A)$.

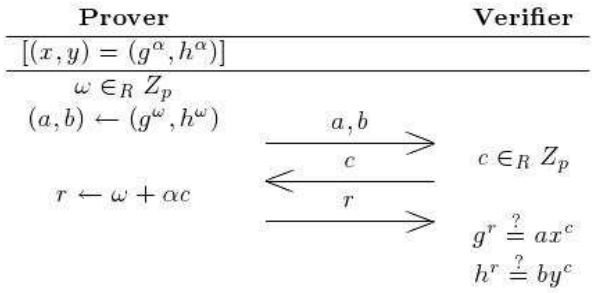
Η μη διαλογική απόδειξη κατασκευάζεται ως

$$(P; A, H(P, A), R)$$

όπου $R = respond(P, A, H(P, A))$.

4.2.2 Ισότητα διακριτών λογαρίθμων

Σε αυτό το κομμάτι θα παρουσιάσουμε το πρωτόκολλο το οποίο χρησιμοποιείται για να δειχθεί η ισότητα διακριτών λογαρίθμων. Ο αποδείκτης έχει μια τετράδα (g, x, h, y) , $g, x, h, y \in \mathbb{Z}_p$ και επιδεικνύει κατοχή ενός $\alpha \in \mathbb{Z}_p$ το οποίο ικανοποιεί $x = g^\alpha$ και $u = h^\alpha$. Ιδιότητες ασφαλείας του πρωτοκόλλου μπορούν να βρεθούν σε διάφορες εργασίες, όπως η [12]. Το πρωτόκολλο απεικονίζεται παρακάτω :



Σχ.8 : Διαδραστική απόδειξη γνώσης για $\log_g x = \log_h y$

Για τυχαία c, r οποιοσδήποτε μπορεί να κατασκευάσει $(g^r x^{-c}, h^r y^{-c}, c, r)$ τα οποία είναι η αποδεκτή συνδιαλλαγή με τη σωστή κατανομή. Παρολαυτά, ο αποδείκτης στέλνει a, b πριν να λάβει την πρόκληση c. Έτσι, χωρίς γνώση του α δε μπορεί να υπολογίσει την απάντηση r έτσι ώστε να ικανοποιεί τις απαιτήσεις του επαληθευτή.

Μη διαλογική εκδοχή

- Οι υπολογισμοί του αποδείκτη είναι ίδιοι όπως και στη διαλογική απόδειξη, αλλά αυτός κατασκευάζει την πρόκληση c για τον εαυτό του ως

$$c = H(a \parallel b \parallel c \parallel x \parallel y)$$

  όπου H είναι μια ασφαλής συνάρτηση κατακερματισμού. Ο αποδείκτης αποθηκεύει τα c, r σαν απόδειξη.

- Η επαλήθευση μπορεί να πραγματοποιηθεί ελέγχοντας εάν

$$c \stackrel{?}{=} H(g^r x^{-c} \parallel h^r y^{-c} \parallel x \parallel y)$$

Παρατηρείστε ότι εάν, αντί για τέσσερα στοιχεία ομάδας τα οποία συμμετέχουν στη διαλογική απόδειξη, η μη διαλογική εκδοχή χρειάζεται να αποθηκεύσει μόνο δυο τέτοια στοιχεία.

4.2.3 1-από-L Απόδειξη Επανακρυπτογράφησης

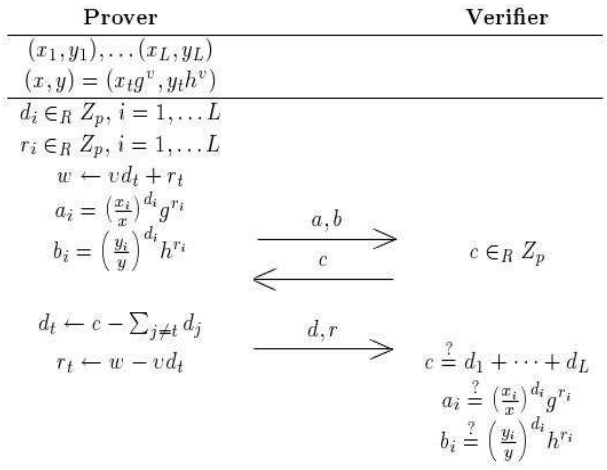
Ο αποδείκτης θέλει να αποδείξει ότι για το κρυπτογραφημένο μήνυμα (x, y) υπάρχει μια επανακρυπτογράφηση στα L κρυπτογραφημένα μηνύματα $(x_1, y_1), (x_2, y_2), \ldots, (x_L, Y_L)$. Τα μηνύματα κρυπτογραφούνται με χρήση του κρυπτοσυστήματος ElGamal.

Ας υποθέσουμε ότι η επανακρυπτογράφηση του (x, y) είναι (x_t, y_t) και ότι η τυχαιότητα της επανακρυπτογράφησης (ο μάρτυρας) είναι u, δηλαδή $(x_t, y_t) = (xg^u, yh^u)$. Σημειώστε ότι τα a, b, d, r από το πρωτόκολλο είναι διανύσματα : $a = (a_1, \ldots, a_L)$, $b = (b_1, \ldots, b_L)$, $d = (d_1, \ldots, d_L)$ και $r = (r_1, \ldots, r_L)$.

Οι τιμές a_i, b_i που έχουν σταλεί δεσμεύουν τον αποδείκτη στα d_i και r_i για όλα τα $i = 1, 2, \ldots, L$ εκτός από $i = t$. Οι τιμές a_t και b_t δεσμεύουν τον αποδείκτη μόνο σε μία τιμή $w = ud_t + r_t$ καθώς $a_t = g^{ud_t + r_t}$ και $b_t = h^{ud_t + r_t}$. Καθώς ο αποδείκτης γνωρίζει το u, μπορεί ακόμα να αλλάξει τα d_t και r_t μετά από αυτό το γύρο.

Ο επαληθευτής προκαλεί τον αποδείκτη να μετατρέψει τα d και r του κατά τέτοιο τρόπο ώστε το d να αθροίζεται σε τυχαίο αριθμό c. Ο αποδείκτης, πλέον, μετατρέπει τις τιμές d_t και r_t για να ικανοποιήσει τις προϋποθέσεις ($c = d_1 + d_2 + \ldots + d_l$

και $w = ud_t + r_t$) και στέλνει τα τροποποιημένα $d_1, d_2, \ldots, d_L$ και $r_1, r_2, \ldots, r_L$ στον επαληθευτή. Με αυτή τη διαδικασία ο επαληθευτής πείθεται ότι ανάμεσα σε L κρυπτογραφημένα ζεύγη πράγματι υπάρχει ένα επανακρυπτογραφημένο ζεύγος του (x, y) και ο αποδείκτης γνωρίζει την τυχαιότητα της επανακρυπτογράφησης διαφορετικά δε θα μπορούσε να προσαρμόσει τις τιμές του για το δοσμένο άθροισμα. Για τις ιδιότητες ασφαλείας του πρωτοκόλλου δείτε την εργασία [12].



Σχ.9 : Απόδειξη γνώσης για 1-από-L επανακρυπτογράφηση

Μη διαλογική εκδοχή

- Οι υπολογισμοί του αποδείκτη είναι ίδιοι όπως και στη διαλογική απόδειξη αλλά ο αποδείκτης κατασκευάζει ο ίδιος την πρόκληση c ως εξής :

$$c = H(a_1 \parallel \ldots \parallel a_L \parallel b_1 \parallel \ldots \parallel b_L \parallel x \parallel y \parallel x_1 \parallel \ldots \parallel x_L \parallel y_1 \parallel \ldots y_L)$$

  όπου H είναι μια ασφαλής συνάρτηση κατακερματισμού. Ο αποδείκτης αποθηκέυει τα $c, d_1, \ldots, d_L, r_1, \ldots, r_L$ ως απόδειξη.

- Η επαλήθευση μπορεί να πραγματοποιηθέι ελέγχοντας εάν :

$$c \stackrel{?}{=} H(a_1 \parallel \ldots \parallel a_L \parallel b_1 \parallel \ldots \parallel b_L \parallel x \parallel y \parallel x_1 \parallel \ldots \parallel x_L \parallel y_1 \parallel \ldots \parallel y_L)$$

  όπου

$$a_i = \left(\frac{x_i}{x}\right)^{d_i} g^{r_i}$$

$$b_i = \left(\frac{y_i}{y}\right)^{d_i} h^{r_i}$$

Πλεόν παρατηρούμε ότι αντί για $4L + 1$ στοιχεία ομάδας τα οποία συμμετέχουν στη διαλογική απόδειξη, η μη διαλογική εκδοχή χρειάζεται να αποθηκεύσει μόνο $2L + 1$ τέτοια στοιχεία.

L Πιθανότητες για το διακριτό λογάριθμο

Για το κρυπτογραφημένο μήνυμα $(x, y) = E(m)$ (στο κρυπτοσύστημα ElGamal) θέλουμε να δώσουμε μια απόδειξη ότι το m είναι ένα από L πιθανά μηνύματα

$G_1, \ldots, G_L$ και τίποτα άλλο. Αποκαλύπτοντας κάποια πληροφορία για το μήνυμα m πέραν του ότι ανήκει στο σύνολο αυτό δεν είναι επιθυμητό. Ας υποθέσουμε ότι ο διακριτοί λογάριθμοι (με βάσεις g, h) των στοιχείων $G_1, \ldots, G_L$ δεν είναι γνωστοί.

Ο σκοπός είναι να αποδείξουμε ότι

$$\log_g x = \log_h(y/G_1) \vee \log_g x = \log_h(y/G_2) \vee \ldots \vee \log_g x = \log_h(y/G_L)$$

όπου $\vee$ είναι η πράξη της διάζευξης (or).

Αρκεί να δείξουμε ότι μεταξύ των στοιχείων

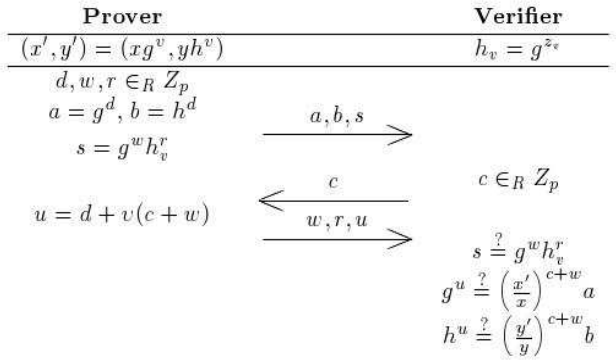
$$(x_1, y_1) = (x, y/G_1)\ (x_2, y_2) = (x, y/G_2) \vdots (x_L, y_L) = (x, y/G_L)$$

βρίσκεται η επανακρυπτογράφηση του κρυπτογραφημένου μηνύματος $(1, 1)$. Για το σκοπό αυτό χρησιμοποιούμε το πρωτόκολλο διαλογικής απόδειξης 1-από-L επανακρυπτογράφησης.

4.2.4 Επανακρυπτογράφηση καθορισμένου επαληθευτή

Ο αποδείκτης θέλει να αποδείξει μυστικά ότι (x', y') είναι μια επανακρυπτογράφηση του $(x, y) = (g^k, h^k m)$ δηλαδή ότι $(x', y') = (xg^u, h^k u)$ όπου u είναι ένας παράγοντας τυχαιότητας για την επανακρυπτογράφηση. Η απόδειξη κατασκευάζεται για το συγκεκριμένο αποδείκτη ο οποίος κατέχει ένα μυστικό z_u (το διακριτό λογάριθμο του h_u στη βάση g_u : $h_u = g^{z_u}$). Η γνώση του z_u του επιτρέπει να κατασκευάσει μια απόδειξη τέτοιου είδους για καθένα από τα ζεύγη $(x', y'), (x, y)$. Το πρωτόκολλο βασίζεται στη γνώση του z_u από τον επαληθευτή. Εάν αυτή η ιδιότητα δεν διασφαλιστεί από την υποδομή δημοσίου κλειδιού που υποστηρίζει το πρωτόκολλο, τότε χρησιμοποιείται πρωτόκολλο που διασφαλίζει τη γνώση του δημοσίου κλειδιού, και το οποίο θα δούμε παρακάτω.

Οι τιμές a, b, s σταλμένες στον επαληθευτή δεσμεύουν το χρήστη στα d, w, r. Ο αποδείκτης δεν μπορεί να αλλάξει τις τιμές w, r. Ο επαληθευτής μπορεί, ωστόσο, να χρησιμοποιήσει τη γνώση του z_u για να ανοίξει το s για αυθείρετες τιμές w' , r' ικανοποιώντας τη σχέση $w + rz_u = w'r'z_u$.



Σχ.10 : Απόδειξη γνώσης για 1-από-L επανακρυπτογράφηση καθορισμένου επαληθευτή

Μη διαλογική εκδοχή

1. Οι υπολογισμοί του αποδείκτη είναι οι ίδιοι με αυτούς που είναι στη διαλογική απόδειξη αλλά ο αποδείκτης κατασκευάζει ο ίδιος την πρόκληση c ως εξής :

$$c = H(x \parallel y \parallel\parallel x' \parallel y' \parallel a \parallel b \parallel s)$$

όπου H είναι μια συνάρτηση κατακερματισμού. Ο αποδείκτης αποθηκέυει τα c, w, r, u ως απόδειξη.

2. Η επαλήθευση μπορεί να πραγματοποιηθεί ελέγχοντας εάν

$$c \stackrel{?}{=} H(x \parallel y \parallel x' \parallel y' \parallel \frac{g^u}{\left(\frac{x'}{x}\right)^{c+w}} \parallel \frac{h^u}{\left(\frac{y'}{y}\right)^{c+w}} \parallel g^w h_u^r)$$

Πλεόν παρατηρούμε ότι αντί για 7 στοιχεία ομάδας τα οποία συμμετέχουν στη διαλογική απόδειξη, η μη διαλογική εκδοχή χρειάζεται να αποθηκεύσει μόνο 4 τέτοια στοιχεία.

Πως μπορεί ο επαληθευτής να πλαστογραφήσει την απόδειξη

Ο επαληθευτής που γνωρίζει το μυστικό z_u έτσι ώστε $h_u = g^{z_u}$ μπορεί να κατασκευάσει τη μη διαλογική απόδειξη για οποιοδήποτε (x, y) και (x^*, y^*). Το σημείο κλειδί είναι ότι η τιμή s δε δεσμεύει τον επαληθευτή στα w και r. Ο επαληθευτής επιλέγει α, β, u^* τυχαία, θέτει $E = x \parallel y \parallel x^* \parallel y^*$ και υπολογίζει

$$c^* = H\left(E \parallel \frac{g^{u^*}}{\left(\frac{x^*}{x}\right)^{\alpha}} \parallel \frac{h^{u^*}}{\left(\frac{y^*}{y}\right)^{\alpha}} \parallel g^{\beta}\right)$$

$$w^* = a - c^*$$
$$r^* = \frac{\beta - w^*}{z_u}$$

και θέτει τα (c^*, w^*, r^*, u^*)

4.2.5 Διασφαλίζοντας τη γνώση του ιδιωτικού κλειδιού

Το ακόλουθο πρωτόκολλο χρησιμοποιείται για να επαληθευτεί εάν ο χρήστης (ψηφοφόρος, αξιολογητής) πραγματικά γνωρίζει το ιδιωτικό του κλειδί που ανταποκρίνεται στο αντίστοιχο δημόσιο κλειδί $h_u = g^{z_u}$. Ακόμα και αν ο χρήστης δε γνωρίζει το ιδιωτικό του κλειδί και συμπεριφέρεται σύμφωνα με τις υποδείξεις εκβιαστή (ο οποίος γνωρίζει το ιδιωτικό κλειδί), εν τέλει μαθαίνει το ιδιωτικό του κλειδί.

Η γνώση του χρήστη για το z_u επαληθεύεται από N οντότητες (αρχές). Υποθέτουμε ότι τουλάχιστον t από αυτές είναι τίμιες. Το μη υποκλέψιμο κανάλι μεταξύ του χρήστη και των οντοτήτων είναι αναγκαίο.

1. Ο χρήστης διαμοιράζει το ιδιωτικό του κλειδί z_u μετακύ των οντοτήτων χρησιμοποιώντας ένα $(t + 1, N)$ σχήμα διαμοιρασμού μυστικού (όπως αυτό που περιγράψαμε σε προηγούμενο κομμάτι της εργασίας) :

   - Επιλέγει τυχαίο πολυώνυμο βαθμού t : $f_u(x) = z_u + a_1 x + \ldots + a_t x^t$

- Στέλνει $s_j = f_u(j)$ μέσω του μη υποκλέψιμου καναλιού στην αρχή A_j , $j = 1, \ldots, N$
- Δεσμεύεται από τις συνιστώσες του πολυωνύμου στέλνωντας $C_j = g^{a_j}$ στον πίνακα ανακοινώσεων (bulletin board)

2. Κάθε οντότητα A_j επαληθεύει εάν ο κλήρος που έλαβε ανταποκρίνεται στο πολυώνυμο στο οποίο δεσμεύεται ο χρήστης :

$$g^{s_j} \stackrel{?}{=} h_u C_1^j C_2^{j^2} \ldots C_t^{j^t} (= g^{z_u} g^{a_1 j} g^{a_2 j^2} \ldots g^{a_t j^t} = g^{f_u(j)})$$

3. Εάν η οντότητα A_j εντοπίσει ένα σφάλμα, τότε υποβάλλει διαμαρτυρία και ζητείται από το χρήστη να δημοσιεύσει τον κλήρο του στον πίνακα ανακοινώσεων. Εάν ο υποβληθείς κλήρος δεν ανταποκρίνεται στις δεσμεύσεις, ο χρήστης αποπέμπεται.

4. Τέλος, εάν κάθε οντότητα δεν έχει υποβάλει διαμαρτυρία στο προηγούμενο στάδιο, στέλνει στο χρήστη τον κλήρο της μέσω μη υποκλέψιμου καναλιού.

Τουλάχιστον t τίμιες οντότητες είτε υποβάλουν διαμαρτυρία (και τα κομμάτια τους υποβάλλονται στον πίνακα ανακοινώσεων) είτε στέλνουν τους κλήρους τους μυστικά στο χρήστη. Ο χρήστης, πλέον μπορεί να να ανακτήσει το ιδιωτικό του κλειδί z_u χρησιμοποιώντας πολυωνυμική παρεμβολή στα ληφθέντα κομμάτια (όπως είδαμε και προηγουμένως, ο πιό διαδεδομένος τύπος παρεμβολής είναι η παρεμβολή Λαγρανγε).

ΚΕΦΑΛΑΙΟ 5

Ηλεκτρονική ψηφοφορία

5.1 Εισαγωγικά

Με τον όρο ηλεκτρονική ψηφοφορία (e-voting) ορίζουμε το σύνολο των τεχνικών που αφορούν ηλεκτρονικά μέσα και που χρησιμοποιούνται τόσο για την κατάθεση ψήφων σε μια ψηφοφορία όσο και για την καταμέτρηση ψήφων. Καθώς οι σύγχρονες εφαρμογές ηλεκτρονικής ψηφοφορίας αφορούν υπολογιστικά συστήματα, οι τεχνικές που χρησιμοποιούνται για να ικανοποιήσουν τις απαιτήσεις ασφάλειας, ιδιωτικότητας και μη διαβλητότητας της εκλογικής διαδικασίας προέρχονται από την επιστήμη της κρυπτογραφίας. Ένας κρυπτογραφικός αλγόριθμος ο οποίος καθορίζει τον τρόπο διενέργειας μιας εκλογικής διαδικασίας καλείται πρωτόκολλο ηλεκτρονικής ψηφοφορίας. Όπως αναφέραμε και στο πρώτο κεφάλαιο, ένα πρωτόκολλο e-voting προστατεύει τη διαδικασία της ηλεκτρονικής ψηφοφορίας κρυπτογραφόντας και υπογράφοντας ψηφιακά τις ψήφους και συγκεντρώνοντας τις ανώνυμα, αποτρέπωντας τόσο την ανάγνωση πληροφορίας από το σύστημα όσο και τη μεταβολή της ροής της πληροφορίας, διασφαλίζοντας έτσι τη διαδικασία. Συστήματα ηλεκτρονικής ψηφοφορίας, τα οποία αποτελούν υλοποίηση σε ολοκληρωμένα συστήματα κρυπτογραφικών πρωτοκόλλων, χρησιμοποιούνται από αρκετές χώρες (π.χ. Η.Π.Α., Ινδία, Ελβετία, Βενεζουέλα, Βραζιλία, Καναδά κ.α.) για τη διενέργεια τόσο εθνικών και δημοτικών εκλογών όσο και για δημοψηφίσματα και διαδικασίες απογραφής (e-census).

Τα σχήματα ηλεκτρονικής ψηφοφορίας (e-voting schemes) είναι ένας από τους τομείς της κρυπτογραφίας στους οποίους έχει συντελεστεί πολύ μεγάλο ερευνητικό έργο. Παρολαυτά, μέχρι στιγμής δεν έχει βρεθεί λύση που να ικανοποιεί συνολικά τις απαιτήσεις ταυτόχρονα τόσο σε ασφάλεια όσο και σε αποδοτικότητα είτε σε πρακτικό είτε σε θεωρήτικό επίπεδο. Ως εκ τούτου, έχει προταθεί ένας αρκετά μεγάλος αριθμός σχημάτων ηλεκτρονικής ψηφοφορίας, με αρκετά μεγάλη ποικιλία ως προς τις ιδιότητες ασφαλείας που αυτά ικανοποιούν. Ένας κατάλογος με τις ιδιότητες που μπορεί να ικανοποιεί ένα πρωτόκολλο ηλεκτρονικής ψηφοφορίας έχει ως εξής :

- Εμπιστευτικότητα : τα δεδομένα που είναι αποθηκευμένα στις βάσεις δεδομένων και διακινούνται στο δίκτυο δεν είναι αναγνώσιμα από τρίτους.
- Ακεραιότητα : τα δεδομένα που είναι αποθηκευμένα στις βάσεις δεδομένων και διακινούνται στο δίκτυο δεν είναι δυνατό να μεταβληθούν από τρίτους
- Διαθεσιμότητα : τα δεδομένα είναι πάντα διαθέσιμα σε διαπίστευμένα μέλη του δικτύου.

- Αναγνωρισιμότητα και εξακρίβωση ταυτότητας για τα διαπιστευμένα μέλη του δικτύου.
- Εξουσιοδότηση (έλεγχος τοπικής πρόσβασης): τα διαπιστευμένα μέλη έχουν πρόσβαση μόνο στα σχετικά με αυτά δεδομένα και όχι σε άλλα.
- Μη δυνατότητα αποκύρηξης πράξης : κάθε χρήστης του δικτύου μπορεί να καταστεί υπεύθυνος για κάθε πράξη την οποία έχει τελέσει χρησιμοποιώντας το δίκτυο.
- Ιδιωτικότητα: Δεν πρέπει να υπάρχει κανένας έμμεσος ή άμεσος τρόπος με τον οποίο μπορεί να μπορεί κανείς να συνάγει τις επιλογές ενός αξιολογητή.
- Επιλεξιμότητα: Κάθε αξιολογητής μπορεί να αξιολογήσει μόνο μία φορά.
- Ανεξάρτητη και καθολική επιβεβαίωση: Κάθε αξιολογητής μπορεί να επιβεβαιώσει ότι καταμετρήθηκε τη επιλογή του.
- Καθολική Επιβεβαίωση: Κάθε μέλος ή τρίτος παρατηρητής μπορεί να ελέγξει αν η αξιολόγηση είναι δίκαια.
- Δικαιοσύνη: Κάθε συμμετέχων στην διαδικασία της αξιολόγησης δεν μπορεί να γνωρίζει έστω και μερικό αποτέλεσμα πριν την καταμέτρηση.
- Ευστάθεια: Να μπορεί να αυτοπροστατεύεται από κάθε λάθος ή σκόπιμη ενέργεια των συμμετεχόντων.
- Receipt-freeness: Κάθε συμμετέχων στην αξιολόγηση δεν μπορεί να πείσει κάποιον άλλο παρατηρητή για το τι αυτός επέλεξε και να τον επηρεάσει αντίστοιχα.
- Ανεξαρτησία σύγκρουσης : Δεν είναι δυνατό να παίρνουν δύο ή περισσότεροι χρήστες ίδια διακριτικά διαπίστευσης (αποτρέπει το ενδεχόμενο της διπλής ψήφου).

Υπάρχουν τρεις κύριες κατηγορίες σχημάτων ηλεκτρονικής ψηφοφορίας : τα σχήματα που χρησιμοποιούν ανώνυμο κανάλι, τα σχήματα που χρησιμοποιούν συνδυασμό ανώνυμου καναλιού και τυφλών υπογραφών, και τα σχήματα ομομορφικής κρυπτογράφησης. Οι πρώτες δύο είναι αρκετά δημοφιλείς σε συστήματα τα οποία δεν παρουσιάζουν μεγάλες απαιτήσεις ασφάλειας, είναι αρκετά αποδοτικά και υποστηρίζουν όλους τους δυνατούς τύπους ψηφοφορίας. Στα μειονεκτήματα τους καταλογίζονται το ότι επιβάλλουν στο χρήστη να δρα σε πολλούς γύρους (αρχικοποίηση, ψήφο, αρίθμηση, επαλήθευση, τυχόν διαμαρτυρία) και συνήθως δεν περιλαμβάνουν το χαρακτηριστικό της καθολικής επιβεβαίωσης. Όσο για τα σχήματα ομομορφικής κρυπτογράφησης, ικανοποιούν σε αρκετα μεγαλύτερο βαθμό τις απαιτήσεις ασφαλείας του συστήματος, καθώς η πληροφορία μέσα σε αυτά διέρχεται κρυπτογραφημένη, αλλά αυτό προκαλεί μεγάλο κόστος επικοινωνίας στο δίκτυο. Τα σχήματα αυτά υποστηρίζουν μόνο συγκεκριμένο τύπο ψηφοδελτίων. Κάθε σχήμα ικανοποιεί σε διαφορετικό βαθμό κάποιες από τις παραπάνω απαιτήσεις ασφαλείας που δώσαμε παραπάνω. Συνήθως, όσο περισσότερες απαιτήσεις ασφαλείας ικανοποιεί ένα πρωτόκολλο τόσο πιο μεγάλη είναι η πολυπλοκότητα χώρου ή/και χρόνου που απαιτείται για τη λειτουργία του.

Θα προχωρήσουμε στην παρουσίαση ενός χαρακτηριστικού σχήματος ηλεκτρονικής ψηφοφορίας από κάθε κατηγορία και μέσα από αυτά θα δίνουμε και κάποια σύντομη περιγραφή για τα υπόλοιπα σχήματα που απαρτίζουν την κατηγορία.

5.1.1 Σχήματα ανώνυμου καναλιού : το σχήμα του Chaum

Το σχήμα του Chaum ήταν το πρώτο σχήμα ηλεκτρονικής ψηφοφορίας που παρουσιάστηκε το 1981 [9].

Οι αρχές της ηλελτρονικής ψηφοφορίας είναι N εξυπηρετητές ανάμειξης με δημόσια κλειδιά $E_1, \ldots, E_N$. Ένας ψηφοφόρος V_i δημιουργεί το δημόσιο κλειδί του K_i και γράφει στο κομμάτι που έχει στον πίνακα ανακοινώσεων $E_1(E_2(\ldots E_N(K_i))\ldots)$. Οι εξυπηρετητές ανάμειξης ανακατεύουν τα μηνύματα αυτά, όπως είδαμε κατά την περιγραφή των δικτύων ανάμειξης, και παράγουν μια λίστα κλειδιών K_i. Εδώ, πλέον, ο χρήστης μπορεί να ισχυριστεί κατά πόσο το κλειδί του K_i είναι ή όχι στη λίστα. Στην περίπτωση αυτή, η διαδικασία της ψηφοφορίας επανεκκινείται. Εάν δεν εγερθεί καμμία διαμαρτυρία, τότε ο ψηφοφόρος γράφει $E_1(E_2(\ldots E_N(K_i \parallel K_i^{-1}(u_i)))\ldots)$ στον πίνακα ανακοινώσεων. Πάλι, οι εξυπηρετητές ανάμειξης ανακατεύουν αυτά τα μηνύματα και η λίστα $K_i \parallel K_i^{-1}(u_i)$ συνδυάζεται με την προηγούμενη λίστα για να παρθούν οι ψήφοι u_i.

Το σχήμα αυτό έχει αρκετά μειονεκτήματα. Για παράδειγμα, αποτυχία ενός και μόνο χρήστη θα διαταράξει τη διαδικασία ψηφοφορίας και θα προκαλέσει την επανέναρξη της. Επιπλέον, εάν η εκλογική διαδικασία πρέπει να ξαναρχίσει μετά τη δεύτερη φάση, οπότε και κάποιες ψήφοι θα έχουν ήδη δημοσιευτεί, αυτό μπορει να επηρεάσει τη διαδικασία καθώς έχουμε εμφάνιση μερικού αποτελέσματος. Επίσης, το σχήμα αυτό δεν εκπληρώνει το χαρακτηριστικό της ανεξαρτησίας σύγκρουσης και έχει αρκετά μεγάλη πολυπλοκότητα κατά τη φάση της αρχικοποίησης. Το σχήμα αυτό βελτιώνεται σε αποδοτικότητα και από άποψη δικαίου στην εργασία [47].

5.1.2 Σχήματα ανώνυμου καναλιού με χρήση ψηφιακής υπογραφής

Σχήματα τέτοιου τύπου περιγράφονται στις εργασίες [10] [7] [22] [48] [30] [31]. Σε γενικές γραμμές, σχήματα αυτού του τύπου δουλεύουν με τον εξής τρόπο : ο ψηφοφόρος λαμβάνει ένα κουπόνι, το οποίο είναι ένα τυφλά υπογεγραμμένο μήνυμα από την αρχή. Ο ψηφοφόρος μπορεί να λάβει μόνο ένα κουπόνι, καθώς για κάθε ψηφοφόρο η αρχή μπορεί να υπογράψει τυφλά μόνο ένα μήνυμα. Έπειτα, ο ψηφοφόρος αποστέλλει την ψήφο του διαμέσου του ανώνυμου καναλιού πίσω στην αρχή. Η αρχή συλλέγει τις ψήφους και τις δημοσιεύει μαζί με τα κουπόνια.

Η αρχή η οποία εκδίδει τα κουπόνια καλείται διαχειριστής και η αρχή η οποία τα μεζεύει καλείται συλλέκτης. Οι όροι αυτοί μπορεί να αναφέρονται σε δυο διαφορετικές αρχές με διαχωρισμένες αρμοδιότητες ή μόνο σε μία η οποία εκπληρώνει και τους δύο ρόλους, ανάλογα με το σχήμα.

Η προσέγγιση αυτή έχει μερικά συγκεκριμένα προβλήματα ασφαλείας τα οποία τα διάφορα σχήματα καλούνται να λύσουν. Τα πιό σημαντικά από αυτά είναι τα εξής :

- Το χαρακτηριστικό της δικαιοσύνης μπορεί να μην εκπληρώνεται καθώς ο συλλέκτης γνωρίζει από πριν το μερικό αποτέλεσμα πριν από τη φάση της μέτρησης.

- Το χαρακτηριστικό της ανεξαρτησίας σύγκρουσης μπορεί να μην εκπληρωθεί καθώς υπάρχει περίπτωση δύο χρήστες να πάρουν ίδιο κουπόνι και έτσι η ψήφος του ενός από τους δύο να αποπεμφθεί σα διπλή ψήφος.

- Μια ανέντιμη αρχή (διαχειριστής) μπορεί να υποδυθεί ψηφοφόρους απέχωντας από τις εκλογές και προσθέτωντας δικούς της ψήφους, ή παρέχοντας μυστικά περισσότερα από ένα κουπόνια σε μερικούς ψηφοφόρους.

- Σε περίπτωση που η ψήφος ενός ψηφοφόρου δεν έχει καταμετρηθεί, ο ψηφοφόρος αυτός δε μπορεί να υποβάλλει διαμαρτυρία χωρίς να αποκαλύψει την ψήφο του.

Για να διορθωθεί το χαρακτηριστικό της δικαιοσύνης, μπορούμε να αποτρέψουμε από το συλλέκτη να μπορεί να δει τις πραγματικές ψήφους με το να κρυπτογραφούμε τις ψήφους τις οποίες συγκεντρώνει ο συλλέκτης και αποκρυπτογραφώντας τις σε σημείο της διαδικάσιας μεταγενέστερο της φάσης της μέτρησης. Το κλειδί αποκρυπτογράφησης μπορεί είτε να αποστέλλεται ανώνυμα (όπως θα δούμε παρακάτω στο σχήμα FOO- (από τα ονόματα των συγγραφέων της εργασίας Fujioka, Ohta και Okamoto» είτε να ανακατασκευάζεται από ένα σύνολο αρχών (σχήμα [30]).

Το χαρακτηριστικό ανεξαρτησίας σύγκρουσης μπορεί να επιτευχθεί εισάγοντας την ταυτοποίηση του χρήστη μέσα στο κουπόνι με τρόπο που είναι μη υπολογιστικά εφικτό να εξαχθεί από εκεί.

Για να αποφύγουμε το ενδεχόμενο της ανέντιμης συμπεριφοράς από μία αρχή μπορούμε να διανείμουμε τις αρμοδιότητες της περισσότερες από μια αρχές. Στην παρούσα εργασία θα παρουσιάσουμε το σχήμα FOO [22], το οποίο είναι και το πιο αντιπροσωπευτικό της κατηγορίας.

Το σχήμα FOO

Το σχήμα αυτό περιλαμβάνει δύο αρχές, ένα διαχειριστή και ένα συλλέκτη, οι οποίες δεν είναι αναγκαστικά έμπιστες. Ο διαχειριστής είναι υπέυθυνος για την έκδοση κουπονιών και ο συλλέκτης είναι υπεύθυνος για τη συλλογή και καταμέτρηση των ψήφων και την έκδοση τελικού αποτελέσματος. Το κουπόνι είναι μια τυφλά υπογεγραμμένη ψήφος από το διαχειριστή. Ο συλλέκτης συλλέγει τα κουπόνια, τα αριθμεί και δημοσιεύει τη λίστα με το πέρας των εκλογών. Ο ψηφοφόρος βρίσκει το κουπόνι του στη λίστα, και στέλνει ανώνυμα τον αριθμό του κουπονιού του μαζί με το κλειδί στο συλλέκτη. Ο συλλέκτης δημοσιεύει τα κλειδιά, αποκρυπτογραφεί τις ψήφους και δημοσιεύει το αποτέλεσμα των εκλογών.

Έστω ID_i είναι η ταυτότητα του ψηφοφόρου V_i, σ_i είναι το σχήμα υπογραφής του V_i κι σ_A είναι το σχήμα υπογραφής του διαχειριστή. Επιπλέον, έστω χ είναι η τεχνική ¨τύφλωσης¨ και δ είναι η τεχνική επανάκτησης που χρησιμοποιείται στις τυφλές υπογραφές.

Στάδιο αρχικοποίησης

Ο διαχειριστής κατασκευάζει το σχήμα υπογραφής του και δημοσιεύει το δημόσιο κλειδί του.

Στάδιο εγγραφής Ο ψηφοφόρος προετοιμάζει το ψηφοδέλτιο του ως εξής :

- Ο V_i επιλέγει την ψήφο u_i και κατασκευάζει το ψηφοδέλτιο του $x_i = \chi(u_i, k_i)$, όπου χ είναι ένα ασφαλές σχήμα δέσμευσης δυαδικού ψηφίου, όπως αυτό που είδαμε στο κεφάλαιο 4.1.4, χρησιμοποιώντας τυχαίο κλειδί k_i.

- Ο V_i υπολογίζει το μήνυμα e_i χρησιμοποιώντας την τεχνική τύφλωσης $e_i = \chi(x_i, r_i)$
- Ο V_i υπογράφει το $s_i = \sigma(e_i)$ και στέλνει την τριπλέτα (ID_i, e_i, s_i) στο διαχειριστή.

Η δέσμευση δυαδικού ψηφίου γίνεται για να δωθεί η δυνατότητα στο διαχειριστή να ελέγξει το γνήσιο της υπογραφής του ψηφοφόρου. Σκοπός είναι η αποτροπή πλαστοπροσωπίας από κάποιον τρίτο.

Ο διαχειριστής A λαμβάνει την τριπλέτα (ID_i, e_i, s_i) και ελέγχει εάν :

- Ο ψηφοφόρος V_i έχει δικαίωμα ψήφου
- Ο ψηφοφόρος V_i δεν έχει κάνει αίτηση για υπογραφή
- Η υπογραφή s_i του μηνύματος e_i είναι έγκυρη

Εάν όλες αυτές οι συνθήκες ικανοποιούνται τότε ο διαχειριστής A υπογράφει $d_i = \sigma_A(e_i)$ και στέλνει το d_i στον ψηφοφόρο. Εάν κάποια από αυτές τις προϋποθέσεις δεν ισχύει τότε ο διαχειριστής απορρίπτει την υπογραφή.

Με το πέρας του σταδίου εγγραφής ο διαχειριστής ανακοινώνει τον αριθμό των ψήφοφόρων που έλαβαν την υπογραφή του και δημοσιεύει τη λίστα (ID_i, e_i, s_i).

Στάδιο ψηφοφορίας

- Ο ψηφοφόρος V_i ανακτά την υπογραφή y_i του ψηφοδελτίου x_i χρησιμοποιώντας την τεχνική ανάκτησης δ : $y_i = \delta(d_i, r_i)$, αφαιρώντας έτσι τον παράγοντα τύφλωσης r_i.
- Ο V_i ελέγχει ότι η y_i είναι πράγματι η υπογραφή του διαχειριστή από το x_i. Εάν ο έλεγχος αποτύχει τότε ο V_i ισχυρίζεται ότι έχει γίνει διατάραξη της διαδικασίας δείχνοντας ότι το ζεύγος (x_i, y_i) είναι μη έγκυρο.
- Ο V_i στέλνει το κουπόνι (x_i, y_i) ανώνυμα στο συλλέκτη.
- Ο συλλέκτης C ελέγχει την υπογραφή του διαχειριστή y_i για το ψηφοδέλτιο x_i. Εάν ο έλεγχος είναι επιτυχής τότε ο C εισάγει την τριπλέτα (l, x_i, y_i) σε μία λίστα ως το l-οστό αντικείμενο της.

Στάδιο καταμέτρησης Το στάδιο καταμέτρησης αποτελείται από δύο ξεχωριστές φάσεις : άνοιγμα και καταμέτρηση.

Φάση ανοίγματος

Όταν όλοι οι ψηφοφόροι έχουν ψηφίσει τότε ο συλλέκτης C δημοσιεύει τη λίστα (l, x_i, y_i). Ο ψηφοφόρος V_i, τότε, κάνει τα ακόλουθα :

- Ο V_i ελέγχει ότι ο αριθμός των ψηφοδελτίων στη λίστα είναι ίσος με τον αριθμό των ψηφοφόρων. Εάν αυτός ο έλεγχος αποτύχει τότε ο ψηφοφόρος το ισχυρίζεται αποκαλύπτοντας το κουπόνι x_i, y_i και τον παράγοντα τύφλωσης r_i
- Ο V_i ελέγχει ότι η ψήφος του περιλαμβάνεται στη λίστα. Εάν αυτός ο έλεγχος αποτύχει τότε ο ψηφοφόρος το ισχυρίζεται αποκαλύπτοντας το (x_i, y_i) το έγκυρο ψηφοδέλτιο και την υπογραφή του.

- Ο V_i στέλνει το κλειδί k_i μαζί με τον αριθμό l, δηλαδή το (l, k_i) στο συλλέκτη C μέσω ανωνύμου καναλιού.

Φάση μέτρησης

- Ο συλλέκτης C ανοίγει τη δέσμευση του ψηφοδελτίου x_i και ανακτά την ψήφο u_i και την προσθέτει μαζί με το κλειδί k_i στη λίστα και ελέγχει εάν το u_i είναι έγκυρη ψήφος.

- Ο C μετράει τις ψήφους και δημοσιεύει το αποτέλεσμα της ψηφοφορίας.

Ιδιότητες ασφάλειας

- Αναγνωρισιμότητα και εξακρίβωση ταυτότητας για τα διαπιστευμένα μέλη του δικτύου: μόνο διαπιστευμένα μέλη της ψηφοφορίας μπορούν να παρουν κουπόνι. Μη έγκυρα κουπόνια και ψήφοι θα διαγράφονται. Το κουπόνι δε μπορεί να χρησιμοποιείται παραπάνω από μία φορά.

- Ιδιωτικότητα: Η ιδιωτικότητα του χρήστη επιτυγχάνεται ακόμα και αν ο διαχειριστής και ο συλλέκτης συνωμοτήσουν εναντίον του ψηφοφόρου : η σχέση μεταξύ του ID του ψηφοφόρου και του ψηφοδελτίου του είναι κρυμμένη από το σχήμα τυφλής υπογραφής. Ο ψηφοφόρος στέλνει το ψηφοδέλτιο του x_i όπως επίσης και το κλειδί k_i μέσω ανώνυμου καναλιού οπότε δεν είναι δυνατή η ανίχνευση της προέλευσης τους.

- Ανεξάρτητη επιβεβαίωση: Ο ψηφοφόρος μπορεί να ελέγξει εάν το ψηφοδέλτιο του (x_i, y_i) είναι εντός της λίστας που δημοσιεύεται από το συλλέκτη και κατά πόσον τα k_i και u_i του έχουν προστεθεί στη λίστα. Όταν ο ψηφοφόρος ισχυρίζεται ότι έχει υπάρξει ανωμαλία στη διαδικασία, δε χρειάζεται να αποκαλύψει την ψήφο του u_i αλλά μόνο τα x_i, y_i του. Με αυτό τον τρόπο μπορεί, εφόσον τα x_i, y_i είναι έγκυρα, να πάρει καινούριο κουπόνι. Με αυτό τον τρόπο, όμως, κατά τη φάση της μέτρησης οποιοσδήποτε συμμετέχων μπορεί να μάθει ποιοί είναι οι ψήφοι που προήλθαν από ψηφοφόρους που διαμαρτυρήθηκαν. Εκτός κι αν έχουμε επανεκκίνηση της διαδικασίας ψηφοφορίας, δεν επιτυγχάνεται η ιδιωτικότητα των διαμαρτυρόμενων χρηστών.

- Καθολική επιβεβαίωση : Δεν επιτυγχάνεται καθώς εάν λοίπουν κάποιοι ψηφοφόροι μπορεί η ανεξάρτητη αρχή να ψηφίσει στη θέση τους.

- Δικαιοσύνη: Το σχήμα είναι δίκαιο καθώς η μέτρηση των ψήφων δεν επηρρεάζει τη διαδικασία της ψηφοφορίας.

- Receipt-freeness: Δεν επιτυγχάνεται καθώς κάθε συμμετέχων μπορεί να βρει την ψήφο του στο τέλος κάθε εκλογής.

Άλλα σχήματα αυτού του τύπου

Άλλα σχήματα αυτού του τύπου περιλαμβάνουν :

- Το σχήμα [46] το οποίο και αποτελεί μαι μετατροπή του σχήματος FOO για να αποτρέπει τη δυνατότητα του χρήστη να μπορεί να αποδείξει το περιεχόμενο της ψήφου του. Αυτό επιτυγχάνεται με τη χρήση μιας τυχαίας αντιμετάθεσης από το συλλέκτη κατά τη μέτρηση των ψήφων.

- Το σχήμα Radwin [48], το οποίο δανείζεται την τεχνική του ανώνυμου καναλιού με δυνατότητα απάντησης από τα σχήματα ηλεκετρονικού χρήματος, προσφέρει τη δυνατότητα εντοπισμού διπλής ψήφου. Αυτό το επιτυγχάνει με το να μην ενσωματώνει την ψήφο στο κουπόνι, αλλά με το να την κρυπτογραφεί με ένα κρυπτοσύστημα δημοσίου κλειδιού (στην προκειμένη περίπτωση το κρυπτοσύστημα RSA) και να τη χρησιμοποιεί εν είδη ψευδωνύμου. Με αυτό τον τρόπο, κατά τη φάση της καταμέτρησης μπορεί να βρεθεί διπλοψηφίσας ψηφοφόρος με το να εντοπιστεί το ψευδώνυμο του στη λίστα.

- Το σχήμα JL [30], το οποίο ενσωματώνει το συλλέκτη με το διαχειριστή και χρησιμοποιεί N ελεγκτικές οντότητες για να ελέγξει τη διαδικασία ψηφοφορίας. Αυτό επιτυγχάνεται με το διαμοιρασμό του κλειδιού (μέσω ενός σχήματος $(t+1, N)$ διαμοιρασμού μυστικού) που χρησιμοποιείται για την κρυπτογράφηση των ψήφων με το κρυπτοσύστημα ElGamal στις ελεγκτικές οντότητες, οι οποίες το ανακτούν με το πέρας της φάσης της μέτρησης των ψήφων.

5.1.3 Σχήματα ομομορφικής κρυπτογράφησης

Τα σχήματα ομομορφικής κρυπτογράφησης εκμεταλλέυονται την ιδιότητα της ομομορφικής κρυπτογράφησης να πολλαπλασιάζει δυο κρυπτοκείμενα με σκοπό να προσθέσει τα αντίστοιχα απλά κείμενα από τα οποία προήλθαν τα κρυπτοκείμενα. Με τον τρόπο αυτό επιτυγχάνουν να μαζέψουν κρυπτογραφημένο το σύνολο των ψήφων και έπειτα να τις αποκρυπτογραφήσουν σα σύνολο, αποσυνδέοντας έτσι το περιεχόμενο της ψήφου από την ταυτότητα του ψηφοφόρου.

Το πρώτο σχήμα αυτού του τύπου το οποίο προτάθηκε είναι το σχήμα των Benaloh και Yung [4], [6]. Το σχήμα του Iversen [29] είναι εμπνευσμένο από αυτό. Οι Sako και Killian στην εργασία [51] βελτίωσαν την πολυπλοκότητα του σχήματος του Benaloh.

Ένα σχήμα το οποίο επηρέασε την περαιτέρω έρευνα στα σχήματα ψηφοφορίας ομομορφικής κρυπτογράφησης είναι αυτό των Cramer, Gennaro και Schoenmakers (CGS] [12]), το οποίο και είναι το σχήμα το οποίο θα παρουσιάσουμε στην εργασία αυτή.

Το σχήμα που περιγράφεται στην εργασία [52] είναι λιγότερο αποδοτικό από το σχήμα CGS αλλά ταιριάζει άριστα σε εκλογές μικρής κλίμακας, καθώς δε λαμβάνει χώρα καμία επικοινωνία μεταξύ των αρχών παρά μόνο κατά τη φάση αρχικοποίσης της διαδικασίας.

Το χαρακτηριστικό Receipt-freeness εισήχθει από τους Benaloh και Tuinstra [5] το οποίο προσωμοιώνει τη λειτουργία που έχει το παραβάν στις κανονικές εκλογές. Οι Hirt και Sako στην εργασία [27], όμως, έδειξαν ότι το σχήμα αυτό δεν είναι receipt-free. Στην εργασία αυτή προτείνουν, με τη σειρά τους ένα αποδοτικό receipt-free σχήμα το οποίο είναι βασισμένο στο σχήμα

Το χαρακτηριστικό αυτό επετεύχθη και από τους Lee και Kim [35] μέσω της συνεργασίας του ψηφοφόρου με έναν έντιμο επαληθευτή. Ενδεχόμενη κακόβουλη συνεργασία των δύο πλευρών, όμως, τους επιτρέπει να ρίξουν άκυρες ή διπλές ψήφους.

Το σχήμα CGS

Το σχήμα CGS είναι ένα αποδοτικό σχήμα το οποίο ικανοποιεί όλες τις απαιτήσεις ασφαλείας για ένα σύστημα ηλεκτρονικής ψηφοφορίας που περιγράψαμε στο προηγούμενο κεφάλαιο πλην του χαρακτηριστικού της receipt freeness. Το σχήμα έχει σα βάση της ασφάλειας του πρόβλημα του διακριτού λογαρίθμου, ενώ μπορεί να μετατραπεί κατά τέτοιο τρόπο έτσι ώστε να έχει σα βάση της ασφάλειας του το πρόβλημα των q-αδικών υπολοίπων.

Σχήμα για ψηφοδέλτιο μορφής ΝΑΙ/ΟΧΙ

Οι ψηφοφόροι στέλνουν δημοσίως τις ψήφους τους κρυπτογραφημένες με το κρυπτοσύστημα ElGamal. Το κλειδί αποκρυπτογράφησης μοιράζεται μεταξύ των αρχών με το πέρας των εκλογών, οι ψήφοι πολλαπλασιονται και οι αρχές αποκρυπτογραφούν το άθροισμα των ψήφων σαν αποτέλεσμα της εκλογικής διαδικασίας.

Φάση αρχικοποίησης

Οι αρχές χρησιμοποιούν το κρυπτοσύστημα ElGamal ως εξής : μοιράζονται το κλειδί αποκρυπτογράφησης s και δημοσιεύουν το δημόσιο κλειδί (p, g, h), τις δεσμεύσεις στους κλήρους $h_j = g^{s_j}$ και μια σταθερή τιμή G γεννήτρια του G_q.

Φάση Ψηφοφορίας

Ο ψηφοφόρος V_i επιλέγει την ψήφο του : $m_0 = G$ για ψήφο ΝΑΙ, $m_1 = 1/G$ για ψήφο όχι. Η κρυπτογραφημένη ψήφος είναι της μορφής $(x, y) = (g^k, h^k m_b)$, όπου k είναι τυχαίο και $b \in \{0, 1\}$. Ο ψήφοφόρος προσθέτει μια απόδειξη ότι η ψήφος του έχει τη σωστή μορφή. Για το σκοπό αυτό χρησιμοποιείται η μη διαλογική μορφή της απόδειξης $\log_g x = \log_h(y/G) \vee \log_g x = \log_h(y/G)$, όπως περιγράψαμε προηγουμένως στην εργασία (Κεφ. 4.2.2). Η κρυπτογραφημένη ψήφος μαζί με την απόδειξη εγκυρότητας στέλνονται στον πίνακα ανακοινώσεων.

Φάση καταμέτρησης

Γίνεται έλεγχος των αποδείξεων εγκυρότητας από τις αρχές γιά όλες τις έγκυρες κρυπτογραφημένες ψήφους, και δημιουργείται το γινόμενο $(X, Y) = (\prod_i x_i, \prod_i y_i)$. Τελικά, οι αρχές εκτελούν ταυτοχρόνως το πρωτόκολλο αποκρυπτογράφησης για το (X, Y) για να πάρουν την τιμή $W = Y/X^s$. Κάθε αρχή επίσης δημοσιεύει μια μη διαλογική απόδειξη από το πρωτόκολλο αποκρυπτογράφησης για να αποδείξει ότι έχει χρησιμοποιήσει το κομμάτι της από το μοιρασμένο κλειδί.

Έτσι, έχουμε $W = G^T$, όπου T είναι η διαφορά μεταξύ του αριθμού των ψήφων ΝΑΙ και των ψήφων ΟΧΙ.: $-M \leq T \leq M$, όπου M είναι ο αριθμός των διαπιστευμένων χρηστών. Με αυτό τον τρόπο παίρνουμε $T = \log_G W$ που είναι γενικά δύσκολο να υπολογιστεί. Η τιμή του T μπορεί να καθοριστεί χρησιμοποιώντας $O(M)$ modulo πολλαπλασιασμούς υπολογίζοντας επαναληπτικά $G^{-M}, G^{-M+1}, \ldots$ μέχρι να βρεθεί το W.

Σχήμα για ψηφοδέλτιο μορφής 1-από-L

Ένας από τους διάφορους τρόπους επέκτασης του ψηφοδελτίου ΝΑΙ/ΟΧΙ σε ψηφοδέλτιο 1-από-L είναι ο εξής :

Παίρνουμε L γεννήτορες $G_1, \ldots G_L$ και συγκεντρώνουμε τις ψήφους για κάθε επιλογή ξεχωριστά. Πλέον, η απόδειξη εγκυρότητας ανάγεται στην απόδειξη γνώσης του

$$\log_g x = \log_h(y/G_1) \vee \ldots \vee \log_g x = \log_h(y/G_L)$$

η οποία είναι η απόδειξη γνώσης που παρουσιάσαμε στο Κεφ. 4.2.3 .

Ο ψηφοφόρος μπορεί να κατασκευάσει την ψήφο του μόνο για ένα γεννήτορα G_j. Άρα έχουμε αυτόματα εγγύηση ότι θα ψηφίσει μόνο για μία επιλογή.

Τέλος, η τελική καταμέτρηση των ψήφων γίνεται υπολογίζοντας το γινόμενο όλων των έγκυρων ψήφων $W = G_1^{T_1} G_2^{T_2} \dots G_L^{T_L}$. Οι τιμές $T_1, , \dots, T_L$ μπορούν να υπολογιστούν χρησιμοποιώντας $O(M^{L-1})$ πολλαπλασιασμούς.

Σχήμα για ψηφοδέλτιο μορφής K-από-L

Σε αυτό τον τύπο ψηφοδελτίου ο ψηφοφοφόρος επιλέγει K-από-L επιλογές οι οποίες πρέπει να είναι διαφορετικές μεταξύ τους.

Όπως και στον προηγούμενο τύπο ψηφοδελτίου, οι L πιθανότητες αντιπροσωπεύονται από τις γεννήτριες $G_1, G_2 \dots G_L$. Το τελικό αποτέλεσμα υπολογίζεται από το $W = G_1^{T_1} G_2^{T_2} \dots G_L^{T_L}$, όπου $T_i \leq KM$.

Ο ψηφοφόρος στέλνει K κρυπτογραφημένες ψήφους $(x_1, y_1), \dots, (x_K, y_K)$. Πρέπει να αποδείξει ότι αυτά τα ψηφοδέλτια περιέχουν έγκυρες πιθανότητες και ότι οι πιθανότητες αυτές είναι διαφορετικές μεταξύ τους.

Ας πάρουμε ένα ζεύγος ψηφοδελτίων $[(x_i, y_i), (x_j, y_j)] \ , \ i < j]$. Εάν

$$(x_i, y_i) = (g^{k_i}, h^{k_i} G_r)$$

είναι η κρυπτογράφηση του G_r και

$$(x_j, y_j) = (g^{k_j}, h^{k_j} G_s)$$

τότε λέμε ότι το ζεύγος $[(x_i, y_i), (x_j, y_j)]$ είναι η κρυπτογράφηση του $[G_r, G_s]$.

Είναι αρκετό να αποδείξουμε ότι για όλα τα ζεύγη ψηφοδελτίων $[(x_i, y_i), (x_j, y_j)] \ , \ i < j]$ ότι το ζεύγος $[G_r, G_s]$.είναι η κρυπτογράφηση ενός στοιχείου από το συνολο

$$\{[G_r, G_s]\} \ r, s = 1 \dots L_i \ , \ r \neq s$$

Αυτό επιτυγχάνεται ως ακολούθως :

Το γινόμενο του ζεύγους των ψηφοδελτίων

$$(x_i x_j, y_i y_j) = (G^{ki+k_j}, h^{k_i+k_j} G_r G_s)$$

είναι η κρυπτογράφηση του $G_r G_s$. Έτσι, αρκεί να αποδείξουμε ότι $(x_i x_j, y_i y_j)$ είναι η κρυπτογράφηση ενός στοιχείου του συνόλου $\{[G_r, G_s]\} \ r, s = 1 \dots L_i \ , \ r \neq s$. Το σύνολο αυτό περιέχει $\frac{L(L-1)}{2}$ στοιχεία. Άρα, θα χρησιμοποιήσουμε την απόδειξη επανακρυπτογράφησης 1-από-$\frac{L(L-1)}{2}$, όπως τη περιγράψαμε στο αντίστοιχο κομμάτι της εργασίας μας.

Πλέον, κάθε χρήστης στέλνει K κρυπτογραφημένες ψήφους στον πίνακα ανακοινώσεων, δηλαδή $2K$ στοιχεία ομάδας. Επιπλέον, πρέπει να στείλει $\frac{K(K-1)}{2}$-από-$\frac{L(L-1)}{2}$ αποδείξεις επανακρυπτογράφησης. Συνολικά , στέλνει

$$2K + \frac{K(K-1)}{2} + \left(2\frac{L(L-1)}{2} + 1\right) = O(K^2 L^2)$$

στοιχεία ομάδας στον πίνακα ανακοινώσεων.

Ιδιότητες ασφάλειας

- Εξακρίβωση ταυτότητας : Οι ψήφοι κακόβουλων ή μη διαπιστευμένων χρηστών δε θα περάσουν από την απόδειξη εγκυρότητας. Το σχήμα είναι ανθέκτικό για

μέχρι και t αρχές.

- Ιδιωτικότητα: Η ιδιωτικότητα κάθε ψήφου διαφυλάσσεται από το κρυπτοσύστημα ElGamal. Κάθε ψήφος είναι κρυφή για κάθε σύνολο από το πολύ t αρχές.

- Καθολική επιβεβαίωση : Κάθε παρατηρητής μπορεί να ελέγξει τις αποδείξεις ορθότητας των ψηφοδελτίων, κάθε παρατηρητής μπορεί να φτιάξει το γινόμενο των έγκυρων ψήφων και κάθε παρατηρητής μπορεί να επαληθεύσει την ορθότητα της αποκρυπτογράφησης ελέγχοντας το ότι χρησιμοποιούν σωστούς κλήρους χρησιμοποιώντας τις αποδείξεις των αρχών.

- Receipt-freeness: Δεν επιτυγχάνεται καθώς κάθε ψηφοφόρος μπορεί να αποδείξει το πως ψήφισε απλά επιδεικνύοντας τον παράγοντα τυχαιότητας k που χρησιμοποιείται για την κρυπτογράφηση με το κρυπτούστημα ElGamal.

Άλλα σχήματα αυτού του τύπου

Άλλα σχήματα αυτού του τύπου περιλαμβάνουν :

- Το πρώτο σχήμα αυτού του τύπου, το σχήμα του Benaloh, το οποίο χρησιμοποιεί την τεχνική της ομομορφικής κρυπτογράφησης και το $(t+1, N)$ σχήμα μυστικού διαμοιρασμού του Shamir σε συνδυασμό με ένα πιθανοτικό κρυπτοσύστημα δημοσίου κλειδιού για να ικανοποιήσει τις απαιτήσεις ασφαλείας ενός συστήματος ηλεκτρονικής ψηφοφορίας για τύπους ψηφοδελτίων όπως αυτοί του σχήματος CGS. Το σχήμα αυτό δεν επιτυγχάνει receipt-freeness.

- Το σχήμα του Schoenmakers αποτελεί μια επέκταση του παραπάνω σχήματος με τη διαφορά ότι χρησιμοποιείται ένα σχήμα δημόσια επαληθεύσιμου διαμοιρασμού μυστικού.

- Στις εργασίες [21] και [13] προτείνεται η αντικατάσταση του κρυπτοσυστήματος ElGamal με την έκδοση κατωφλιού του κρυπτοσυστήματος του Pailler με σκοπό την επίτευξη receipt-freeness.

- Το σημα HS [27] χρησιμοποιεί κρυπτογράφηση και αντιμετάθεση των ψήφων από τις αρχές με σκοπό να αφαιρέσει από το χρήστη τη δυνατότητα να αποδείξει τι ψήφισε, αφαιρώντας έτσι τη δυνατότητα σε κάποιο τρίτο να εξαναγκάσει τον ψηφοφόρο να αποκαλύψει το περιεχόμενο της ψήφου του.

ΚΕΦΑΛΑΙΟ 6

Συλλογή και επεξεργασία δεδομένων που διατηρούν την ιδιωτικότητα

6.1 Συλλογή δεδομένων που διατηρεί την ιδιωτικότητα

Στο προηγούμενο κεφάλαιο κάναμε μια παρουσίαση σχημάτων ηλεκτρονικής ψηφοφορίας όπου και είδαμε τους τρόπους με τους οποίους προστατεύεται η ανωνυμία του χρήστη και αποσυνδέεται η ταυτότητα του από το περιεχόμενο της ψήφου του. Με δεδομένο ότι ένα ψηφοδέλτιο είναι μια φόρμα δεδομένων η οποία μπορεί να πάρει ποικίλες μορφές, μας δίνεται η δυνατότητα να γενικεύσουμε τη χρησιμότητα των σχημάτων ηλεκτρονικής ψηφοφορίας σε σχήματα συλλογής δεδομένων που διατηρούν την ιδιωτικότητα, αξιοποιώντας το γεγονός ότι μπορούμε να υποκαταστήσουμε τα ψηφοδέλτια με φόρμες δεδομένων τις οποίες θα μεταχειριζόμαστε σα βάσεις δεδομένων. Πλέον, κάνοντας χρήση των πρωτόκολλων ηλεκτρονικής ψηφοφορίας μπορούμε να συνενώσουμε τις φόρμες αυτές λαμβάνοντας τα δεδομένα που αυτές περιέχουν χωρίς να είναι δυνατός ο εντοπισμός της προέλευσης κάθε φόρμας ξεχωριστά. Η ιδέα αυτή πρωτοπαρουσιάστηκε στην εργασία [34].

Για να καταστεί δυνατή η αποτελεσματική συλλογή δεδομένων θα πρέπει αφενώς το σύστημα ηλεκτρονικής ψηφοφορίας να πληροί κάποιες συγκεκριμένες προϋποθέσεις και αφετέρου να προστεθούν σε αυτό κάποια συγκεκριμένα χαρακτηριστικά έτσι ώστε να μπορεί να εκπληρώνει τις απαιτήσεις ενός συστήματος συλλογής δεδομένων, τόσο σε όγκο όσο και στη δυνατότητα αποσύνδεσης των επιμέρους δεδομένων από την πηγή της προέλευσης τους.

Τα σχήματα ηλεκτρονικής ψηφοφορίας τα οποία προσφέρουν τις περισσότερες δυνατότητες είναι τα σχήματα ανώνυμου καναλιού με χρήση ψηφιακής υπογραφής και, πιο συγκεκριμένα, το σχήμα FOO το οποίο παρουσιάσαμε στο κεφάλαιο 5.1.2, καθώς παρέχει ορισμένες δυνατότητες που το καθιστούν κατάλληλο για συλλογή δεδομένων. Τα χαρακτηριστικά αυτά είναι :

- Η διαδικασία ψηφοφορίας είναι ανεξάρτητη της μορφής του ψηφοδελτίου, και άρα έχουμε ευελιξία στη μορφή των δεδομένων που συλλέγονται στα πλαίσια της διαδικασίας ανταλλαγής δεδομένων.

- Το σύστημα χρησιμοποιεί δύο ξεχωριστές αρχές, διευκολύνοντας με αυτό τον τρόπο τη λειτουργικότητα του συστήματος για μεγάλο όγκο δεδομένων.

- Η χρήση ανώνυμων δικτύων είναι εύκολα υλοποιήσιμη με τη χρήση τεχνικών δρομολόγησης κρεμμυδιού (onion routing) [26].

Τα χαρακτηριστικά που θα πρέπει να προστεθούν στο σύστημα για να το κάνουν κατάλληλο για συλλογή δεδομένων είναι τα εξής :

- Η αρχή του διαχειριστή υποκαθίσταται από ένα σύνολο έντιμων ανεξάρτητων αρχών πιστοποίησης των δεδομένων για κάθε ψηφοφόρο/χρήστη οι οποίοι καλούνται Ένωση Ειδικών. Ο σκοπός τους είναι να υπογράφουν τα δεδομένα με σκοπό την πιστοποίηση τόσο της εγκυρότητας τους όσο και της καταλληλότητας τους.

- Η αρχή του συλλέκτη αναλαμβάνει τις αρμοδιότητες του διαχειριστή που έχουν να κάνουν με την επιβεβαίωση της αυθεντικότητας των τυφλών υπογραφών για κάθε φόρμα δεδομένων.

- Το σύστημα θα πρέπει να παρέχει και υποδομές καθαρισμού των δεδομένων με το πέρας της διαδικασίας.

Ενσωματώνοντας τα παραπάνω χαρακτηριστικά, η λειτουργία και τα χαρακτηριστικά ασφαλείας του συστήματος αυτού είναι παρόμοια με αυτά του συστήματος ηλεκτρονικής ψηφοφορίας FOO με τη σημαντική διαφορά ότι αναιρείται η ανάγκη μιας μόνο παροχής ψηφοδελτίου ανά διαδικασία συλλογής δεδομένων. Αυτό σημαίνει ότι κάθε συμμετέχων στο σύστημα ξεχωριστά μπορεί να στείλει περισσότερες από μια επιμέρους βάσεις δεδομένων (¨ψηφοδέλτια¨) ανά διαδικασία χωρίς να παραβιάζονται οι υπόλοιπες απαιτήσεις ασφαλείας του συστήματος.

Ακολουθεί περιγραφή του συστήματος όπως παρουσιάζεται στην εργασία [34] :

Το σύστημα λειτουργεί κάνοντας χρήση μιας αρχής, την οποία και καλούμε Συλλέκτη. Στη διαδικασία συμμετέχουν ειδικοί επιφορτισμένοι με την επικύρωση της εγκυρότητας των δεδομένων οι οποίοι συστήνουν Ενώσεις Ειδικών.

Αρχικοποίηση και επικύρωση δεδομένων

(α) Ο Συλλέκτης ανακοινώνει την προθεσμία για τη λήψη όλων των δεδομένων και ένα δημόσιο κλειδί E_0

(β) Κάθε ειδικός υπογράφει με την υπογραφή της Ένωσης Ειδικών κάθε έγκυρο μητρώο δεδομένων και το αποστέλει στην αντίστοιχη Αλίκη. Η Αλίκη επαληθεύει την υπογραφή της Ένωσης Ειδικών σε κάθε μητρώο και υπογράφει το συνολικό αριθμό nor τους για τον Ειδικό. Οι Ειδικοί επαληθεύουν τις υπογραφές της Αλίκης στο nor.

(γ) Οι Ειδικοί αποστέλλουν στο Συλλέκτη τον ακριβή αριθμό μητρώων δεδομένων nor μαζί με την υπογραφή της Αλίκης και τη δική τους για αυτό. Ο Συλλέκτης επαληθεύει την υπογραφή της Ένωσης Ειδικών στα nor και τα αποδέχεται.

(δ) Κάθε Αλίκη κρυπτογραφεί το ζεύγος των μητρώων και των αντίστοιχων υπογραφών χρησιμοποιώντας το δημόσιο κλειδί E_0.

Τυφλή Υπογραφή και συλλογή δεδομένων από κάθε Αλίκη

(ε) Κάθε Αλίκη τυφλώνει τα κρυπτογραφημένα δεδομένα, τα υπογράφει με το ιδιωτικό κλειδί της και τα στέλνει μαζί με την ταυτότητα της στο Συλλέκτη.

(στ) Ο Συλλέκτης επαληθεύει την υπογραφή και την ταυτότητα της Αλίκης, και αποδέχεταιτο πακέτο.

(ζ) Ο Συλλέκτης υπογράφει τα δεδομένα και τα στέλνει πίσω στην Αλίκη.

(η) Η Αλίκη επαληθεύει την υπογραφή του Συλλέκτη, αφαιρεί την τύφλωση από τα δεδομένα και τα στέλνει πίσω στο Συλλέκτη με τη μορφή ξεχωριστών μητρώων μέσω ανώνυμου καναλιού.

(θ) Ο Συλλέκτης αναγνωρίζει την υπογραφή του στα κρυπτογραφημένα δεδομένα και τα αποδέχεται

Διανομή και επαλήθευση Δεδομένων

(ι) Με το πέρας της προθεσμίας και τη συλλογή όλων των δεδομένων, ο Συλλέκτης καταχωρεί όλα τα κρυπτογραφημένα δεδομένα με την υπογραφή του σε αυτά σε μια λίστα και τα αποστέλλει σε όλες τις Αλίκες.

(ια) Κάθε Αλίκη επαληθεύει ότι τα δεδομένα της έχουν συμπεριληφθεί στη λίστα.

Γνωστοποίηση κλειδιών και καθαρισμός δεδομένων

(ιβ) Ο Συλλέκτης διαθέτει το ιδιωτικό κλειδί D_0 σε όλες τις Αλίκες.

(ιγ) Κάθε Αλίκη αποκρυπτογραφεί τα δεδομένα και προχωρά σε καθαρισμό όσων μητρώων δεν είναι επαληθευμένα. Πλέον, όλα τα έγκυρα δεδομένα είναι στη διάθεση κάθε Αλίκης που συμμετέχει στο σύστημα.

Το παραπάνω σύστημα αποτελεί τη βάση για συστήματα συλλογής δεδομένων που διατηρεί την ιδιωτικότητα και μπορεί να δεχθεί πολλές προσαρμογές για μια σειρά διαφορετικών εφαρμογών. Για περισσότερες πληροφορίες σχετικά με την ανάλυση ασφάλειας και την πολυπλοκότητα του σχήματος δείτε την εργασία [34].

6.2 Εξορυξη δεδομένων που διατηρεί την ιδιωτικότητα

Το πρόβλημα της εξόρυξης δεδομένων που να διατηρεί την ιδιωτικότητα (privacy preserving data mining) έχει σα βάση του το γεγονός ότι καθώς κάθε δραστηριότητα αφήνει πίσω της ένα μονοπάτι δεδομένων από το οποίο μπορούμε να εξάγουμε χρήσιμη πληροφορία θα πρέπει να βρεθούν τρόποι εξόρυξης δεδομένων οι οποίοι θα μεταχειρίζονται τα δεδομένα με τέτοιο τρόπο έτσι ώστε τα ¨ευαίσθητο¨ μέρος των δεδομένων να φιλτράρεται και να μην αποτελεί μέρος των προς εξόρυξη δεδομένων.

Με βάση την παραπάνω περιγραφή του προβλήματος, το πρόβλημα μπορεί να οριστεί μαθηματικά ως εξής :

Έστω δυο οντότητες P_1 και P_2 κατέχουν βάσεις δεδομένων D_1 και D_2 αντίστοιχα και f ένας αλγόριθμος εξόρυξης δεδομένων. Υπολογίστε το $f(D_1 \cup D_2)$ χωρίς να αποκαλύπτεται μη επιθυμητή πληροφορία.

Το πρόβλημα αυτό έχει τύχει έντονης ερευνητικής δραστηριότητας καθώς αποτελεί τη βάση για μια σειρά εφαρμογών οι οποίες βασίζονται στην εξόρυξη δεδομένων για παροχή πληροφόρίας (π.χ. ενοποίηση νοσοκομειακών βάσεων δεδομένων) και, ως εκ τούτου, υπάρχει μεγάλη ποικιλία αλγορίθμων οι οποίοι επιχειρούν να το επιλύσουν. Οι δύο πιο βασικές εργασίες πάνω στο θέμα είναι οι [36], η οποία προσεγγίζει το πρόβλημα από κρυπτογραφική σκοπιά χρησιμοποιώντας τον αλγόριθμο ID3 ([65]) και η [3] που προτείνει την πρόσθεση στα δεδομένα από το χρήστη ενός παράγοντα τυχαιότητας με τη μορφή θορύβου (στη συγκεκριμένη εργασία προτείνονται δύο μέθοδοι για το σκοπό αυτό, οι value-class membership και value distortion).

Τέλος, αξίζει να αναφέρουμε την προσέγγιση που λαμβάνεται στην εργασία [59], όπου κάνοντας χρήση του αλγόριθμου ομαδοποίησης k-windows ([63]) πάνω σε κάθετα διαμερισμένα δεδομένα επιτυγχάνεται τόσο η μη ανταλλαγή δεδομένων των χρηστών με τρίτους αλλά και μεταξύ τους όσο και το να μην είναι δυνατή η εξαγωγή εμπιστευτικής πληροφορίας από αποτελέσματα.

Μέρος IV

e-αξιολόγηση και εφαρμογές

ΚΕΦΑΛΑΙΟ 7

Εφαρμογές

7.1 Πεδία εφαρμογών της e-αξιολόγησης

Όπως αναφέραμε και στην εισαγωγή, με τον όρο e-αξιολόγηση εννοούμε τη διαδικασία εξ αποστάσεως αξιολόγησης με τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών. Ως εκ τούτου, τα πεδία εφαρμογών της τλε-αξιολόγησης αφορούν κάθε διαδικασία η οποία κάνει χρήση των τεχνολογιών αυτών και για την οποία υπάρχει ανάγκη αξιολόγησης των αποτελεσμάτων που παράγει η διαδικασία αυτή, αλλά και της ίδιας της διαδικασίας και των επιμέρους κομματιών απο τα οποία αποτελείται.

Το πρώτο τέτοιο παράδειγμα εφαρμογής, το οποίο είναι και αυτό με το οποίο θα ασχοληθούμε σε αυτή την εργασία, είναι αυτό της ηλεκτρονικής εξ αποστάσεως εκπαίδευσης ή e-learning. Όπως θα εξετάσουμε και παρακάτω, η εκπαιδευτική διαδικασία, όταν αυτή διεξάγεται σε ένα διαδικτυακό διαδραστικό περιβάλλον, είναι ένα πεδίο εφαρμογής της e-αξιολόγησης το οποίο .

7.2 Η e-αξιολόγηση στην ανοικτή και εξ αποστάσεως εκπαίδευση

Με τον όρο εκπαιδευτική αξιολόγηση εννοούμε, τη μέτρηση της απόδοσης του εκπαιδευτικού έργου στα διάφορα επιμέρους κομμάτια του με σκοπό την ανάλυση και αποτίμηση της αποτελεσματικότητας του τόσο συνολικά όσο και για κάθε κομμάτι του ξεχωριστά.

Η εκπαιδευτική αξιολόγηση αφορά τους φορείς που λαμβάνουν μέρος στην εκπαιδευτική διαδικασία, δηλαδή το διδακτικό προσωπικό, τα τμήματα και το ίδρυμα στο σύνολο του. Για κάθε καθηγητή, η μεταδοτικότητα του, η ενημέρωση του σε σχέση με τις εξελίξεις του γνωστικού του αντικειμένου, οι σχέσεις του με τους εκπαιδευόμενους και η εν γένει απόδοση του στη διδασκαλία αποτελούν αντικείμενα προς αξιολόγηση. Το ίδιο ισχύει και το τμήμα σαν εκπαιδευτική μονάδα τόσο στην οργάνωση και την παροχή υποδομών, όσο και στην ποιότητα του εκπαιδευτικού υλικού που αυτό παρέχει. Η παρουσία του τμήματος στον εκπαιδευτικό χώρο, η εκπαιδευτική της δραστηριότητα, το πρόγραμμα σπουδών, η αρτιότητα και το επίπεδο εξοπλισμού της εκπαιδευτικής μονάδας, τα εγχειρίδια, οι σημειώσεις και το εναλλακτικό υλικό όπως λογισμικό και πολυμεσικό υλικό, αποτελούν αντικείμενα προς αξιολόγηση.

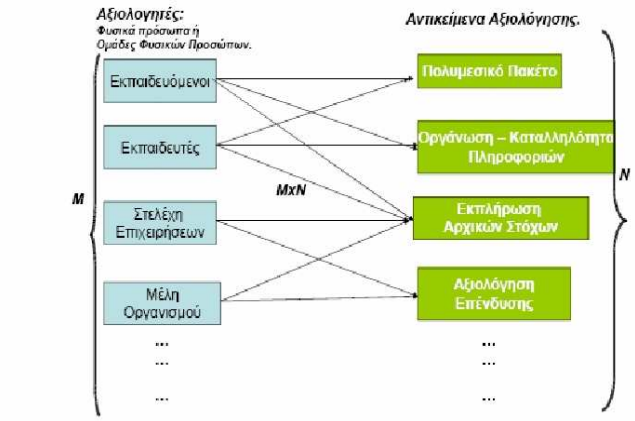
Αξιολογητής μπορεί να είναι οποιοσδήποτε συμμετέχει άμεσα ή και έμμεσα στην εκπαιδευτική διαδικασία. Πιο συγκεκριμένα το ρόλο του αξιολογητή μπορεί να έχει :

- οι εκπαιδευόμενοι
- οι εκπρόσωποι της εκπαιδευτικής κοινότητας
- παράγοντες και φορείς του παραγωγικού τομέα που άπτεται του εκπαιδευτικού αντικειμένου του εκάστοτε τμήματος.

Στη δια ζώσης εκπαίδευση, ο εκπαιδευτικός έχει τη δυνατότητα της συνεχούς διαπροσωπικής επικοινωνίας τόσο με τους εκπαιδευόμενους όσο και με τους υπόλοιπους καθηγητές που συμμετέχουν στην εκπαιδευτική διαδικασία. Αυτό δίνει τη δυνατότητα στον εκπαιδευτικό να κατανοεί άμεσα τις ανάγκες των εκπαιδευόμενων και να προσαρμόζεται κατάλληλα σε αυτές. Καθώς στο e-learning, αυτή η δυνατότητα δεν υπάρχει, καθίσταται αναγκαία η ανάπτυξη μεθόδων που θα υποκαθιστούν αυτό το ρόλο της διαπροσωπικής επαφής με την παροχή αντίστοιχων δεικτών απόδοσης για την εξ αποστάσεως διαδικασία.

7.2.1 Το βασικό μοντέλο

Με βάση τον ορισμό του ρόλου του αξιολογητή, βλέπουμε κατάρχήν ότι το θέμα της ηλεκτρονικής αξιολόγησης είναι πολυεπίπεδο. Οι αξιολογητές, μπορούν να είναι φυσικά πρόσωπα ή ομάδες φυσικών προσώπων. Για παράδειγμα, οι εκπαιδευόμενοι, οι εκπαιδευτικοί, οι λοιποί εμπλεκόμενοι κλπ., είναι αυτοτελείς ομάδες. Από την άλλη πλευρά, τα αντικείμενα της ηλεκτρονικής αξιολόγησης επίσης μπορούν να είναι διάφορα. Οι συσχετίσεις αξιολογητών και αξιολογούμενων αντικειμένων είναι γενικώς πολυσήμαντες $(M \times N)$, όπως για παράδειγμα φαίνεται στην παρακάτω εικόνα :



Σχ.11 : Το μοντέλο συσχετισμού των αξιολογητών

Επομένως κατά την ανάλυση του προβλήματος, η προσέγγιση θα πρέπει να γίνει με την εφαρμογή κάποιας ιεραρχίας. Για παράδειγμα μια εκπαιδευτική ομάδα μπορεί να αξιολογήσει έναν εκπαιδευτή αλλά ίσως να μην επιτρέπεται σε αυτή να δει τα συνολικά αποτελέσματα που τον αφορούν. Όπως επίσης, να μην επιτρέπεται σε έναν τρίτο εκπαιδευτικό η πρόσβαση στα αποτελέσματα που αφορούν ένα συνάδελφό του. Με βάση τα παραπάνω, ένα τυποποιημένο λογισμικό αξιολόγησης θα πρέπει να διαμορφώνεται κάθε φορά κατάλληλα με βάση την ιεραρχία κατά την έναρξη της λειτουργίας του. Σύμφωνα με τα παραπάνω, η αξιολόγηση μπορεί να επιτευχθεί άμεσα με την χρήση μεθόδων e-voting ως εξής:

- Τον ρόλο των ψηφοφόρων τον έχουν οι αξιολογητές (για παράδειγμα οι εκπαιδευόμενοι),
- Ψηφοδέλτια θεωρούνται τα δελτία αξιολόγησης,
- Ως κάλπη θεωρείται η υπηρεσία αξιολόγησης του ιδρύματος, και
- Ως εκλογικός κατάλογος θεωρείται η λίστα που καθορίζεται από την υπηρεσία αξιολόγησης του ιδρύματος και η οποία περιλαμβάνει μόνο τους πιστοποιημένους χρήστες (αξιολογητές) που έχουν δικαίωμα αξιολόγησης

Αντικείμενα Ηλεκτρονικής Αξιολόγησης

Ως αντικείμενα της ηλεκτρονικής αξιολόγησης στο e-λεαρνινγ μπορεί να είναι φυσικά πρόσωπα ή εκπαιδευτικό υλικό. Συγκεκριμένα μπορεί να έχουμε τα ακόλουθα :

Αξιολόγηση του εκπαιδευτικού υλικού : Το εκπαιδευτικό υλικό κυρίως αποτελείται από βιβλία, ιστοσελίδες και πακέτα μάθησης με χρήση πολυμέσων. Συνεπώς, μπορεί να γίνει αξιολόγηση στην μορφή της παρουσίασης των αντικειμένων του εκπαιδευτικού υλικού, κατά πόσον δηλαδή είναι κατάλληλη η μορφή και η παρουσίαση του υλικού που παρέχεται, η ικανότητα επαναχρησιμοποίησής του κλπ.

Αξιολόγηση φυσικών προσώπων : Φυσικά πρόσωπα είναι όσοι συμμετέχουν άμεσα ή έμμεσα στην εκπαιδευτική διαδικασία Τα φυσικά πρόσωπα μπορεί να είναι οι εκπαιδευόμενοι, οι εκπαιδευτικοί, διάφορα στελέχη παραγωγής τα οποία ενδιαφέρονται για την απόδοση του εκπαιδευτικού έργου στο προσωπικό τους, στελέχη άλλων οργανισμών ή εκπαιδευτικών ιδρυμάτων τα οποία μπορεί να είναι επιφορτισμένα με την πιστοποίηση του εκπαιδευτικού υλικού ή έργου κλπ. Η αξιολόγηση του εκπαιδευτή μπορεί να εστιαστεί χωριστά σε κάθε διάλεξη ή ενότητα, ακόμα και σε κάθε άσκηση ή και σε κάθε ομαδική συνεδρία κλπ.

Αξιολόγηση της ποιότητας μάθησης : Αφορά στην ποιότητα του μαθήματος και των αντικειμένων τα οποία χρησιμοποιούνται. Το ενδιαφέρον συνήθως παρουσιάζεται για τα αποτελέσματα που προκύπτουν από τον συνδυασμό δράσης εκπαιδευτικού υλικού και φυσικών προσώπων, αναφορικά πάντα με τους στόχους οι οποίοι έχουν τεθεί στην αρχή της εκπαιδευτικής διαδικασίας.

Αξιολόγηση της ικανοποίησης των συμμετεχόντων : Ως συμμετέχοντες μπορούν να θεωρηθούν φυσικά πρόσωπα ή ομάδες, όπως οι εκπαιδευόμενοι, οι εκπαιδευτικοί, αλλά και άλλα άτομα όπως στελέχη, διευθυντές, κυβέρνηση, επαγγελματίες, προμηθευτές, χρηματοδότες κλπ. Μπορεί να μετρηθεί, για παράδειγμα, η ανταπόκριση που είχε η εκπαιδευτική διαδικασία. Με μια τέτοια διαδικασία μπορούν να εντοπιστούν προβλήματα καθοδήγησης, ή η παροχή ευκαιριών, η ικανοποίηση των στόχων εκμάθησης, η σωστή αξιοποίηση του χρόνου κλπ.

Αξιολόγηση της επένδυσης : Είναι σημαντικό να υπάρξει μια αποτίμηση του συνόλου της παρεχόμενης εκπαιδευτικής υπηρεσίας (ιδιαίτερα στην ανοικτή και εξ αποστάσεως εκπαίδευση) σε σχέση με την επένδυση που γίνεται προς αυτή. Συγκεκριμένα, μπορεί να γίνει αποτίμηση του κόστους σε σύγκριση με το παραγόμενο αποτέλεσμα, καθώς επίσης και εκτίμηση της διάρκειας ζωής των αποτελεσμάτων του εκπαιδευτικού έργου. Οι αποτιμήσεις αυτές μπορεί να γίνουν από κατάλληλες επιστημονικές ομάδες από απόσταση.

Αξιολόγηση ανταπόκρισης και ευελιξίας στις τεχνολογικές αλλαγές : Πρόκειται για μια αξιολόγηση με βάση την οποία εκτιμάται ένας εκπαιδευτικός οργανισμός, αναφορικά με το πόσο μπορεί να ανταποκριθεί στις σημερινές μεταβαλλόμενες τεχνολογικές συνθήκες. Αξιολογείται η ευελιξία του και κατά συνέπεια η ικανότητα επιβίωσης του ίδιου του εκπαιδευτικού οργανισμού. Οι εκτιμήσεις αυτές μπορούν να γίνονται επίσης από κατάλληλες έγκυρες επιστημονικές ομάδες ή οργανισμούς και ενδιαφέρουν άμεσα τον ίδιο τον εκπαιδευτικό οργανισμό.

Με βάση τα παραπάνω, το βασικό μοντέλο διαμορφώνεται ως εξής :

Οι οντότητες που συναντάμε σε ένα οποιοδήποτε μοντέλο ηλεκτρονικής αξιολόγησης είναι:

1. Οι αξιολογητές. Οι ενέργειες των αξιολογητών θα πρέπει να είναι σαφείς, ξεκάθαρες και σύντομες. Οι αξιολογητές θα πρέπει να έχουν την δυνατότητα διακοπής ή ακόμη και ανάκλησης της επιλογής τους μέχρι και τον τερματισμό της αξιολόγησης.

2. Οι αρχές. Οι αρχές διαχειρίζονται τις αξιολογήσεις. Πρόκειται για υπολογιστικά συστήματα με μεγάλη ικανότητα υπολογισμών και δυνατότητα αποθήκευσης δεδομένων με ασφαλή τρόπο.

3. Οι επιλογές αξιολόγησης. Η δομή των επιλογών εξαρτάται από τον τύπο των εκλογών. Πιο συγκεκριμένα, εξαρτάται από τον τύπο των ερωτήσεων οι οποίες προσφέρονται στα μέλη μιας αξιολόγησης και τις πιθανές απαντήσεις. Οι τύποι των αξιολογήσεων διακρίνονται στις ακόλουθες κατηγορίες:

   - Αξιολογήσεις τύπου ΝΑΙ/ΟΧΙ. Σε αυτήν την περίπτωση η επιλογή είναι ένα απλό bit (0 ή 1).
   - Επιλογή 1 μεταξύ L περιπτώσεων.
   - Επιλογή K μεταξύ L περιπτώσεων.
   - Ταξινομημένη επιλογή K μεταξύ L περιπτώσεων. Δηλαδή οι αξιολογητές επιλέγουν K περιπτώσεις μεταξύ L περιπτώσεων και εν συνεχεία θέτουν τις K περιπτώσεις σε σειρά.
   - Επιλογή $1 - L - K$. Οι αξιολογητές επιλέγουν ένα σύνολο από L περιπτώσεις και στη συνέχεια από αυτό το σύνολο επιλέγουν K περιπτώσεις.
   - Δομημένη επιλογή. Υπάρχουν n πιθανά επίπεδα και οι αξιολογητές μετακινούνται από το πρώτο επίπεδο προς το τελευταίο χρησιμοποιώντας ενά επίπεδο μια από τις προηγούμενες περιπτώσεις.
   - Επιλογή με καταγραφή. Ο κάθε αξιολογητής απλώς καταγράφει μια άποψη.

   Επίσης σε ότι αφορά την ισοτιμία μεταξύ των αξιολογητών ορίζονται δύο τύποι αξιολόγησης.

   - Ισοδύναμη αξιολόγηση, σύμφωνα με την οποία κάθε αξιολογητής έχει ισοδύναμη ¨ψήφο¨, δηλαδή όλες οι αξιολογήσεις είναι ισοδύναμες.
   - Αξιολόγηση με βάρη, σύμφωνα με την οποία κάθε αξιολογητής έχει ένα συγκεκριμένο συντελεστή βαρύτητας.

4. Επικοινωνία. Στην ηλεκτρονική αξιολόγηση μπορούν να χρησιμοποιηθούν διάφοροι τύποι επικοινωνιακών καναλιών. Για παράδειγμα, ο πίνακας ανακοινώσεων μπορεί κατά κάποιο τρόπο να θεωρηθεί ως ένας κοινόχρηστος πίνακας. Κάθε συμμετέχων στην αξιολόγηση μπορεί να γράψει στην δική του περιοχή του πίνακα αλλά κανένας δεν μπορεί να σβήσει ή να αλλάξει οτιδήποτε είναι έξω από την δική του περιοχή. Ο πίνακας αυτός μπορεί να θεωρηθεί σαν ένα κοινόχρηστο κανάλι με μνήμη.

Τα σχήματα e-voting που μπορούμε να χρησιμοποιήσουμε χωρίζονται σε τρεις κατηγορίες, και κάθε σχήμα εκπληρώνει συγκεκριμένες ιδιότητες ασφαλείας, όπως τις περιγράψαμε στο προηγούμενο κεφάλαιο. Έτσι, ανάλογα με το σχήμα e-voting που επιλέξαμε για να υλοποιήσουμε το σύστημα e-αξιολόγησης μας, έχουμε γιάυτό τα ίδια χαρακτηριστικά ασφαλείας με το σχήμα e-voting στο οποίο βασίστηκε. Την εφαρμογή την οποία περιγράψαμε μπορεί κανείς να βρεί στις εργασίες [33], [23].

Στη συνέχεια θα δούμε μια θεωρητική υλοποίηση ενός συστήματος e-αξιολόγησης με βάση το σχήμα ανώνυμου καναλιού με χρήση ψηφιακής υπογραφής FOO :

Παράδειγμα υλοποίησης συστήματος e-αξιολόγησης με χρήση του πρωτοκόλλου ηλεκτρονικής ψηφοφορίας FOO

Το σύστημα αυτό περιλαμβάνει δύο αρχές, ένα διαχειριστή και ένα συλλέκτη σύμφωνα με το σχήμα e-voting FOO πάνω στο οποίο και βασίζεται. Ο διαχειριστής είναι υπεύθυνος για την έκδοση κουπονιών και ο συλλέκτης είναι υπεύθυνος για τη συλλογή και καταμέτρηση των ερωτηματολογίων και την έκδοση τελικού αποτελέσματος. Το κουπόνι είναι μια τυφλά υπογεγραμμένη ψήφος από το διαχειριστή. Ο συλλέκτης συλλέγει τα κουπόνια, τα αριθμεί και δημοσιεύει τη λίστα με το πέρας της διαδικασίας αξιολόγησης. Ο αξιολογητής βρίσκει το κουπόνι του στη λίστα, και στέλνει ανώνυμα τον αριθμό του κουπονιού του μαζί με το κλειδί στο συλλέκτη. Ο συλλέκτης δημοσιεύει τα κλειδιά, αποκρυπτογραφεί τα ερωτηματολόγια και δημοσιεύει το αποτέλεσμα της διαδικασίας αξιολόγησης.

Έστω ID_i είναι η ταυτότητα του αξιολογητή V_i, σ_i είναι το σχήμα υπογραφής του V_i κι σ_A είναι το σχήμα υπογραφής του διαχειριστή. Επιπλέον, έστω χ είναι η τεχνική ¨τύφλωσης¨ και δ είναι η τεχνική επανάκτησης που χρησιμοποιείται στις τυφλές υπογραφές.

Στάδιο αρχικοποίησης

Ο διαχειριστής κατασκευάζει το σχήμα υπογραφής του και δημοσιεύει το δημόσιο κλειδί του.

Στάδιο εγγραφής Ο αξιολογητής προετοιμάζει το προσωπικό του ερωτηματολόγιο ως εξής :

- Ο V_i κάνει τις επιλογές αξιολογησης του u_i και κατασκευάζει το προσωπικό του (απαντημένο) ερωτηματολόγιο του $x_i = \chi(u_i, k_i)$, όπου χ είναι ένα ασφαλές σχήμα δέσμευσης δυαδικού ψηφίου χρησιμοποιώντας τυχαίο κλειδί k_i.

- Ο V_i υπολογίζει το μήνυμα e_i χρησιμοποιώντας την τεχνική τύφλωσης $e_i = \chi(x_i, r_i)$

- Ο V_i υπογράφει το $s_i = \sigma(e_i)$ και στέλνει την τριπλέτα (ID_i, e_i, s_i) στο διαχειριστή.

Η δέσμευση δυαδικού ψηφίου γίνεται για να δωθεί η δυνατότητα στο διαχειριστή να ελέγξει το γνήσιο της υπογραφής του αξιολογητή. Σκοπός είναι η αποτροπή πλαστοπροσωπίας από κάποιον τρίτο.

Ο διαχειριστής A λαμβάνει την τριπλέτα (ID_i, e_i, s_i) και ελέγχει εάν :

- Ο αξιολογητής V_i έχει δικαίωμα ¨ψήφου¨
- Ο αξιολογητής V_i δεν έχει κάνει αίτηση για υπογραφή
- Η υπογραφή s_i του μηνύματος e_i είναι έγκυρη

Εάν όλες αυτές οι συνθήκες ικανοποιούνται τότε ο διαχειριστής A υπογράφει $d_i = \sigma_A(e_i)$ και στέλνει το d_i στον αξιολογητής. Εάν κάποια από αυτές τις προϋποθέσεις δεν ισχύει τότε ο διαχειριστής απορρίπτει την υπογραφή.

Με το πέρας του σταδίου εγγραφής ο διαχειριστής ανακοινώνει τον αριθμό των αξιολογητών που έλαβαν την υπογραφή του και δημοσιεύει τη λίστα (ID_i, e_i, s_i).

Στάδιο υποβολής ερωτηματολογίων

- Ο αξιολογητής V_i ανακτά την υπογραφή y_i του ερωτηματολογίου x_i χρησιμοποιώντας την τεχνική ανάκτησης δ : $y_i = \delta(d_i, r_i)$, αφαιρώντας έτσι τον παράγοντα τύφλωσης r_i .
- Ο V_i ελέγχει ότι η y_i είναι πράγματι η υπογραφή του διαχειριστή από το x_i. Εάν ο έλεγχος αποτύχει τότε ο V_i ισχυρίζεται ότι έχει γίνει διατάραξη της διαδικασίας δείχνοντας ότι το ζεύγος (x_i, y_i) είναι μη έγκυρο.
- Ο V_i στέλνει το κουπόνι (x_i, y_i) ανώνυμα στο συλλέκτη.
- Ο συλλέκτης C ελέγχει την υπογραφή του διαχειριστή y_i για το ερωτηματολόγιο x_i. Εάν ο έλεγχος είναι επιτυχής τότε ο C εισάγει την τριπλέτα (l, x_i, y_i) σε μία λίστα ως το l-οστό αντικείμενο της.

Στάδιο καταμέτρησης Το στάδιο καταμέτρησης αποτελείται από δύο ξεχωριστές φάσεις : άνοιγμα και καταμέτρηση

Φάση ανοίγματος

Όταν όλοι οι αξιολογητές έχουν καταθέσει τα ερωτηματολόγια τους τότε ο συλλέκτης C δημοσιεύει τη λίστα (l, x_i, y_i). Ο αξιολογητής V_i, τότε, κάνει τα ακόλουθα :

- Ο V_i ελέγχει ότι ο αριθμός των αξιολογητών στη λίστα είναι ίσος με τον αριθμό των αξιολογητών. Εάν αυτός ο έλεγχος αποτύχει τότε ο αξιολογητής το ισχυρίζεται αποκαλύπτοντας το κουπόνι x_i, y_i και τον παράγοντα τύφλωσης r_i
- Ο V_i ελέγχει ότι το ερωτηματολόγιο του περιλαμβάνεται στη λίστα. Εάν αυτός ο έλεγχος αποτύχει τότε ο αξιολογητής το ισχυρίζεται αποκαλύπτοντας το (x_i, y_i) το έγκυρο ερωτηματολόγιο του και την υπογραφή του.
- Ο V_i στέλνει το κλειδί k_i μαζί με τον αριθμό l, δηλαδή το (l, k_i) στο συλλέκτη C μέσω ανωνύμου καναλιού.

Φάση μέτρησης

- Ο συλλέκτης C ανοίγει τη δέσμευση του ερωτηματολογίου x_i και ανακτά την ψήφο u_i και την προσθέτει μαζί με το κλειδί k_i στη λίστα και ελέγχει εάν το u_i είναι έγκυρο ερωτηματολόγιο.

- Ο C μετράει τα ερωτηματολόγια και δημοσιεύει το αποτέλεσμα της διαδικασίας αξιολόγησης.

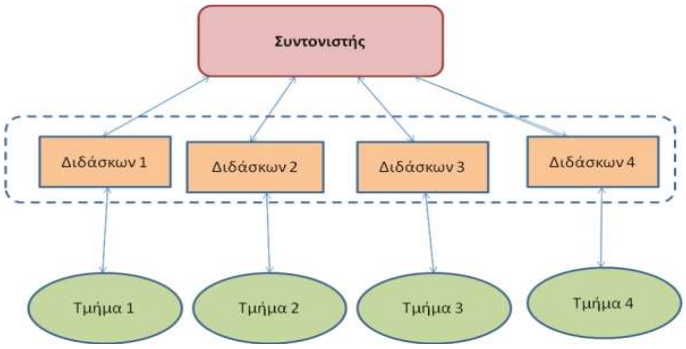
7.2.2 Δυναμική e-αξιολόγηση στο e-learning

Όπως περιγράψαμε και παραπάνω, η διαδικασία ηλεκτρονικής αξιολόγησης εξομοιώνει την αντίστοιχη διαδικασία που λαμβάνει μέρος μέσα στην κλασική εκπαιδευτική διαδικασία. Σημαντικό συστατικό στοιχείο της διαδικασίας αξιολόγησης στην κλασική εκπαίδευση είναι η καθημερινή επαφή εκπαιδευόμενου-εκπαιδευτή, γεγονός που επιτρέπει την απέυθείας προσαρμογή τόσο του εκπαιδευόμενου όσο και του εκπαιδευτή στις ανάγκες του μαθήματος και άρα στη βελτίωση της εκπαιδευτικής διαδικασίας. Για να επιτύχουμε κάτι αντίστοιχο για τη διαδικασία της ηλεκτρονικής αξιολόγησης θα πρέπει να εισάγουμε το στοιχείο της δυναμικότητας της εκπαιδευτικής αξιολόγησης, πράγμα το οποίο προσδίδει δυνατότητες προσαρμοστικότητας στους συμμετέχοντες. Να θυμίσουμε ότι μια διαδικασία αξιολόγησης στην οποία λαμβάνονται δεδομένα αξιολόγησης σε βάθος χρόνου με τέτοιο τρόπο έτσι ώστε να απεικονίζεται η πρόοδος των αντικειμένων αξιολόγησης μέσα στο διάστημα αυτό και να είναι δυνατή η προσαρμογή της διαδικασίας σε καινούριες συνθήκες μέσα στο χρονικό σιάστημα αυτό καλείται δυναμική αξιολόγηση. Η έννοια της δυναμικής e-αξιολόγησης περιγράφεται εκτενώς στην εργασία [24]

Για να επιτύχουμε κάτι τέτοιο, θα πρέπει να χρησιμοποιήσουμε ένα σχήμα το οποίο θα έχει σα βάση του σχήματα συλλογής δεδομένων που διατηρούν την ιδιωτικότητα, όπως αυτό που παρουσιάσαμε στο κεφάλαιο 6.1 . Ο Συλλέκτης συλλέγει τα δεδομένα που παράγονται κατά τη διαδικασία της ηλεκτρονικής αξιολόγησης λαμβάνοντας τα δεδομένα κρυπτογραφημένα και ψηφιακά υπογεγραμμένα κατά τέτοιο τρόπο έτσι ώστε η ταυτότητα του αποστολέα να διαχωρίζεται πλήρως από το δεδομένα που έστειλε, διατηρώντας την ανωνυμία του. Στη συνέχεια, η επεξεργασία των δεδομένων γίνεται με αυτοματοποιημένο τρόπο κάνοντας χρήση αλγορίθμων εξόρυξης δεδομένων που διατηρούν την ανωνυμία όπως αυτοί που παρουσιάσαμε στο κεφάλαιο 6.2 και δημοσιεύει τα αποτελέσματα με το πέρας της διαδικασίας.

Χρησιμοποιώντας σαν παράδειγμα τη δομή του Ελληνικού Ανοιχτού Πανεπιστημίου, κάθε θεματική ενότητα έχει αρκετούς διαφορετικούς διδάσκοντες και ένα συντονιστή που επιβλέπει την ενότητα αυτή. Για να εκμεταλλευτούμε τα χαρακτηριστικά της δομής αυτής μπορούμε να ορίσουμε να γίνεται η διαδικασία της αξιολόγησης, χρησιμοποιώντας ένα σύστημα όπως το παραπάνω, πρέπει πρώτα να αυξήσουμε τη συχνότητα διεξαγωγής αξιολόγησης από τους αξιολογητές (στην προκειμένη περίπτωση τους εκπαιδευόμενους) ανά τακτά χρονικά διαστήματα (π.χ. μια φορά το μήνα ή μαζί με την παράδοση κάθε εργασίας της ενότητας). Τα ερωτηματολόγια πρέπει να είναι φτιαγμένα κατά τέτοιο τρόπο έτσι ώστε να δίνουν έμφαση στις ανάγκες του μαθήματος από τη σκοπιά του εκπαιδευόμενου έτσι ώστε να αντικατοπτρίζουν τόσο τις μεμονωμένες ανάγκες κάθε τμήματος όσο και στη βελτιστοποίηση της συνεργασίας μεταξύ εκπαιδευτικού και εκπαιδευόμενου. Τα αποτελέσματα της αξιολόγησης παράγονται με αυτοματοποιημένο τρόπο από το σύστημα κάνοντας χρήση αλγορίθμων εξόρυξης δεδομένων. Όταν το σύστημα τελειώσει με τη διαδικασία αυτή για κά-

θε υπεύθυνο τμήματος, τότε στέλνει τα αποτελέσματα τόσο στους υπεύθυνους κάθε τμήματος όσο και στο συντονιστή της εκπαιδευτικής ενότητας.



Σχ.12 : Συντονισμός των αξιολογητών

Με βάση την πρώτη αξιολόγηση, και σε συνεργασία τόσο με το συντονιστή όσο και με τους υπόλοιπους διδάσκοντες, δημιουργείται για κάθε τμήμα μια πρώτη αξιολόγηση-σημείο αναφοράς η οποία αποτελεί ένδειξη του επιπέδου του εκάστοτε τμήματος, δίνει τα σημεία της εκπαιδευτικής διαδικασίας στα οποία θα πρέπει να δοθεί τυχόν μεγαλύτερη έμφαση στη συνέχεια του μαθήματος καθώς και παρουσιάζει τις επιμέρους ανάγκες κάθε τμήματος. Έτσι, θα υπάρχει καλύτερος συντονισμός και συνεργασία μεταξύ των συμμετεχόντων, αφού, χρησιμοποιώντας τις πληροφορίες από την αξιολόγηση σε συνδυασμό με την εκπαιδευτική πολιτική του τμήματος, θα καθορίζονται με σαφήνεια οι εκπαιδευτικοί στόχοι για κάθε τμήμα ξεχωριστά. Με την παροχή νέων αποτελεσμάτων από τις επόμενες αξιολογήσεις, μπορούμε να φτιάξουμε ένα ιστορικό αξιολόγησης το οποίο να αποτελεί ενδεικτικό της πορείας της διδασκαλίας για κάθε τμήμα και άρα και το βαθμό της προσαρμογής στις ανάγκες του κάθε τμήματος από την πλευρά του εκπαιδευτή. Έτσι, κάθε εκπαιδευτικός είναι σε θέση να μπορεί να διαπιστώσει καλύτερα τις μαθησιακές ανάγκες του τμήματος του και να ανταποκριθεί πιο αποτελεσματικά σε αυτές, αλλά, καθίσταται έτσι και πιο εύκολος ο συντονισμός και η συνεργασία μεταξύ των τμημάτων, καθώς για κάθε τμήμα υπάρχει ένα μετρήσιμο σημείο αναφοράς. Με αυτό τον τρόπο, μπορούμε να πούμε ότι φτιάχνουμε μια προσαρμοστική δυναμική διαδικασία αξιολόγησης η οποία να προσεγγίζει στον τρόπο λειτουργίας της την παραδοσιακή εκπαιδευτική διαδικασία. Το σύστημα το οποίο περιγράψαμε αποτελεί πρόταση για βελτίωση του ήδη υπάρχοντος συστήματος e-αξιολόγησης που χρησιμοποιείται ήδη με επιτυχία από το ΕΑΠ.

7.2.3 Πλεονεκτήματα της διαδικασίας e-αξιολόγησης

Σε αντίθεση με την παραδοσιακή αξιολόγηση, η ηλεκτρονική αξιολόγηση είναι μια προγραμματισμένη, συστηματική και ακριβής διαδικασία. Πιο συγκεκριμένα, η διαδικασία της ηλεκτρονικής αξιολόγησης μπορεί να είναι αυτόματη αλλά και η επεξεργασία των αποτελεσμάτων να διενεργείται αυτόματα ή μετά από σχετικά απλή εντολή. Επιπλέον, στην όλη διαδικασία της αξιολόγησης δεν υπάρχει η δυνατότητα επέμβασης της υπηρεσίας αξιολόγησης στα αποτελέσματα της αξιολόγησης. Καθώς η διαδικασία της αξιολόγησης είναι πολυεπίπεδη, όλες οι οντότητες της εκπαιδευτικής διαδικασίας δυνητικά είναι αξιολογήσιμες (εκπαιδευτικό υλικό, εκπαιδευτική μεθοδολογία, πρόοδος εκπαιδευομένων, ποσότητα και ποιότητα προσφερόμενης ύλης ανά θεματική ενότητα, ικανότητα εκπαιδευτών κλπ). Συνεπώς, η αυτοματοποίηση

της αξιολόγησης και η κατά συνέπεια μεγάλη οικονομία χρόνου είναι ένα σημαντικό πλεονέκτημα της ηλεκτρονικής αξιολόγησης σε σχέση με την παραδοσιακή.

Ένα δεύτερο σημαντικό πλεονέκτημα της ηλεκτρονικής αξιολόγησης είναι η δυνατότητα αποθήκευσης και ανάκλησης των αποτελεσμάτων. Η αποθήκευση με ανάλογο ευρετήριο δίνει τη δυνατότητα άμεσης ανάκλησης αξιολογήσεων και την συγκριτική παρουσίαση τους στο χρόνο. Τα αποθηκευμένα αυτά αποτελέσματα μπορούν να αποτελέσουν καλό υλικό μελέτης και εξαγωγής συμπερασμάτων για βελτίωση, για έλεγχο πειραματικών τεχνικών και στατιστικών αναλύσεων.

Πλεονέκτημα επίσης της ηλεκτρονικής αξιολόγησης αποτελεί ο ασύγχρονος χαρακτήρας της σε σχέση με την παραδοσιακή αξιολόγηση καθώς δεν είναι αναγκαία η ταυτόχρονη παρουσία των αξιολογητών για τη διενέργεια αξιολόγησης. Επίσης, ηηλεκτρονική αξιολόγηση μπορεί να βοηθήσει αρκετά και στην αρχή της εκπαιδευτικής διαδικασίας. Για παράδειγμα, μπορεί να συνδράμει στην κατανομή των εκπαιδευομένων σύμφωνα με το υπόβαθρο το οποίο έχουν (αρχάριοι, μέσου επιπέδου, προχωρημένοι κλπ). Η διαδικασία αυτή μπορεί να γίνει αξιόπιστα και γρήγορα.

Ακόμη, με την ηλεκτρονική αξιολόγηση μπορεί να έχουμε μια εύκολη εκμαίευση φυσικών και ψυχολογικών συμπερασμάτων για μια εκπαιδευτική ομάδα, ανά φύλλο, ηλικία αλλά και για κάθε πρόσωπο ξεχωριστά. Αυτή η διαδικασία απαιτεί αυστηρή τήρηση της ανωνυμίας του αξιολογητή αλλά και της εχεμύθειας των αποτελεσμάτων. Για την ικανοποίηση του σκοπού αυτού χρησιμοποιείται η έννοια της ιεραρχίας στην διαδικασία της ηλεκτρονικής αξιολόγησης, όπως προαναφέρθηκε. Οι δαπάνες για την ανάπτυξη της ηλεκτρονικής αξιολόγησης θα συμβάλλουν στην πραγματική και αντικειμενική καταγραφή των αποτελεσμάτων (και όχι σε συμπεράσματα από αντιπροσωπευτικά δείγματα ή απόψεις ειδικών κλπ), και θα προάγουν με σχέση πειράματος-αποτελέσματος την αναδιοργάνωση ή αναθεώρηση του εκπαιδευτικού έργου. Επίσης, με την ηλεκτρονική αξιολόγηση οι αξιολογητές αισθάνονται πιο ελεύθεροι όταν αξιολογούν από απόσταση. Στην παραδοσιακή αξιολόγηση δεν είναι πάντα εφικτό να παρευρίσκεται μεγάλο ποσοστό αξιολογητών προκειμένου να αξιολογήσει τον εκπαιδευτικό. Έτσι, αξιολογεί ενδεχομένως κάποιο όχι αντιπροσωπευτικό δείγμα αξιολογητών.

Κάνοντας χρήση του πρωτοκόλλου δυναμικής e-αξιολόγησης που περιγράψαμε παραπάνω, στα πλεονεκτήματα προστίθεται ένας δυναμικός και προσαρμοστικός χαρακτήρας στη διαδικασία της αξιολόγησης, με τα χαρακτηριστικά τα οποία ανφέραμε, έχοντας σα συνέπεια, όμως, και σχετικά αυξημένη πολυπλοκότητα και κόστος λειτουργίας για το σύστημα.

Μέρος V

Επίλογος

ΚΕΦΑΛΑΙΟ 8

Επίλογος

Η έννοια της ιδιωτικότητας είναι πλέον, στην εποχή της πληροφορίας, ένα πολύ σημαντικό πρόβλημα. Σα συνέπεια, τα εργαλεία που απαιτούνται για την προστασία της αποτελούν αντικείμενο έρευνας, κυρίως από το χώρο της ασφάλειας συστημάτων και την κρυπτογραφία. Στην παρούσα εργασία, έχοντας περιγράψει πλήρως τη μορφή που μπορεί να έχει ένα σύστημα ηλεκτρονικής αξιολόγησης σε επίπεδο λογισμικού και hardware και τις πιθανές απειλές σε αυτό, χρησιμοποιήσαμε τεχνικές προερχόμενες από το χώρο της κρυπτογραφίας, και δη από τα συστήματα ηλεκτρονικής ψηφοφορίας, έτσι ώστε να μπορέσουμε να δομήσουμε ένα θεωρητικό πλαίσιο για συστήματα αξιολόγησης μέσω του διαδικτύου, διαδικασία την οποία καλούμε e-αξιολόγηση. Έπειτα εξετάζουμε συστήματα αυτού του τύπου σε διάφορες εφαρμογές με κύρια έμφαση στο πεδίο της ανοικτής και εξ αποστάσεως εκπαίδευσης, όπου και ένα συστήμα αυτού του τύπου ήδη λειτουργεί με επιτυχία στα πλαίσια της λειτουργίας του Ελληνικού Ανοικτού Πανεπιστημίου. Τα συστήματα αυτά, εχοντας διασφαλίσει την αξιοπιστία της διαδικασίας αξιολόγησης και κάνοντας χρήση των αυξημένων δυνατοτήτων συλλογής και επεξεργασίας πληροφορίας την οποία μας δίνουν τα σύγχρονα υπολογιστικά συστήματα και το διαδίκτυο, μπορούν να εξομοιώνουν με επιτυχία τόσο τη διαδικασία αξιολόγησης στην κλασική εκπαίδευση, αλλά και να χρησιμοποιηθούν σε μια ευρεία γκάμα εφαρμογών.

Η εργασία αυτή αποτελεί βάση για περαιτέρω έρευνα πάνω στο αντικείμενο της ηλεκτρονικής αξιολόγησης, τόσο σε επίπεδο εφαρμογών όσο και σε επίπεδο των κρυπτογραφικών εργαλείων. Στο μέλλον ελπίζουμε να διευρύνουμε τόσο το πεδίο εφαρμογών της e-αξιολόγησης σε διάφορους άλλους τομείς όσο και να προσαρμόσουμε τη λειτουργικότητα της σε νέα υπολογιστικά περιβάλλοντα, που γίνονται σε συνεχώς αυξανόμενο βαθμό παράλληλα και κατανεμημένα, χρησιμοποιώντας καινοτόμες κρυπτογραφικές τεχνικές.

Βιβλιογραφία

[1] "Distance learning administration conference 2009", *http://www.westga.edu/ distance/dla/*, 2009.

[2] "Moodle e-learning package", *http://moodle.org/*, 2009.

[3] R. Agrawal and R. Srikant, "Privacy-preserving data mining", In the proceedings of the *Proc. of the ACM SIGMOD Conference on Management of Data*, ACM Press, 439–450, 2000.

[4] J. C. Benaloh, *Verifiable secret-ballot elections*, Ph.D. thesis, New Haven, CT, USA, 1987.

[5] J. C. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections (extended abstract)", In the proceedings of the *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, ACM, New York, NY, USA, 544–553, 1994.

[6] J. C. Benaloh and M. Yung, "Distributing the power of a government to enhance the privacy of voters", In the proceedings of the *PODC '86: Proceedings of the fifth annual ACM symposium on Principles of distributed computing*, ACM, New York, NY, USA, 52–62, 1986.

[7] C. Boyd, "A new multiple key cipher and an improved voting scheme", In the proceedings of the *EUROCRYPT '89: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, Springer-Verlag New York, Inc., New York, NY, USA, 617–625, 1990.

[8] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge", *J. Comput. Syst. Sci.*, vol. 37, No. 2, 156–189, 1988.

[9] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", *Commun. ACM*, vol. 24, No. 2, 84–90, 1981.

[10] D. L. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking rsa", In the proceedings of the *Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88*, Springer-Verlag New York, Inc., New York, NY, USA, 177–182, 1988.

[11] Aviation Industry CBT (Computer Based Training) Committee, "Aicc", *http://www.aicc.org/*.

[12] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme", Springer-Verlag, 103–118, 1997.

[13] I. Damgård and M. Koprowski, "Practical threshold rsa signatures without a trusted dealer", In the proceedings of the *EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, Springer-Verlag, London, UK, 152–165, 2001.

[14] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, No. 6, 644–654, 1976.

[15] C. J. Eibl, B. S.H.von Solms, and S. Schubert, "A framework for evaluating the information security of e-learning systems", 1996.

[16] eLearnCAMPUS, *http://www.elearncampus.com/*.

[17] Australasian Societyfor Computers in Learning in Tertiary Education, *http://www.ascilite.org.au/index.php?p=home*.

[18] International Organizationfor Standardization (ISO), "Iso 7498-2: Information processing systems - open systems interconnection - basic reference model - part 2: Security architecture", , 1989.

[19] International Organizationfor Standardization (ISO), "Iso/iec 15408-1 : Information technology - security techniques - evaluation criteria for it security", *http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html*, 2005.

[20] International Organizationfor Standardization (ISO), "Information technology - individualized adaptability and accessibility in e-learning, education and training", *http://www.iso.org/iso/pressrelease.htm?refid=Ref1217*, 2008.

[21] P. A. Fouque, G. Poupard, and J. Stern, "Sharing decryption in the context of voting or lotteries", In the proceedings of the *FC '00: Proceedings of the 4th International Conference on Financial Cryptography*, Springer-Verlag, London, UK, 90–104, 2001.

[22] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections", In the proceedings of the *ASIACRYPT '92: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, Springer-Verlag, London, UK, 244–251, 1993.

[23] V. I. Galanis, E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis, "e-evaluation in open and distance learning enviroments", *Proceedings of Infotech'09, International Conference on INFORMATION TECHNOLOGIES, Varna, Bulgaria*, 2009.

[24] V. I. Galanis, G. C. Meletiou, and M. N. Vrahatis, "Optimization of open and distance learning through electronic evaluation", *In Proc. of the Fifth International Conference on Open and Distance Learning (ICODL09), Part B, Hellenic Open University*, 144–150, in Greek.

[25] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", In the proceedings of the *Proceedings of CRYPTO 84 on Advances in cryptology*, Springer-Verlag New York, Inc., New York, NY, USA, 10–18, 1985.

[26] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information", In the proceedings of the *Proceedings of the First International Workshop on Information Hiding*, Springer-Verlag, London, UK, 137–150, 1996.

[27] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption", In the proceedings of the *Proceedings of EuroCrypt 2000, LNCS series*, Springer-Verlag, 539–556, 2000.

[28] E. R. House, "Assumptions underlying evaluation models", *Educational Researcher*, vol. 7(3), 4–12, 1978.

[29] Kenneth R. Iversen, "A cryptographic scheme for computerized elections", In the proceedings of the *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, London, UK, 405–419, 1992.

[30] W. S. Juang and C. L. Lei, "Blind threshold signatures based on discrete logarithm", In the proceedings of the *Computer Communications*, Springer, 172–181, 1996.

[31] W. S. Juang, C. L. Lei, and P. L. Yu, "A verifiable multi-authorities secret election allowing abstaining from voting", *International Computer Symposium*, vol. 45, 672–682, 1998.

[32] D. Kahn, *The codebreakers: the story of secret writing*, Scribner, rev. ed. 1996, 1967.

[33] E. C. Laskari, G. C. Meletiou, E. Stergiou, and M. N. Vrahatis, "Electronic evaluation in open and distance education", *In Proc. of the Third International Conference on Open and Distance Learning (ICODL'05), Hellenic Open University*, vol. 1, 497–507, in Greek.

[34] E. C. Laskari, G. C. Meletiou, D. K. Tasoulis, and M. N. Vrahatis, "Privacy preserving electronic data gathering", *Mathematical and Computer Modelling*, vol. 42, 739–746, 2005.

[35] B. Lee and K. Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier", In the proceedings of the *Proceeding of JW-ISC2000*, 101–108, 2000.

[36] Y. Lindell and B. Pinkas, "Privacy preserving data mining", In the proceedings of the *Journal of Cryptology*, Springer-Verlag, 36–54, 2000.

[37] LAMS Foundation Ltd, "Learning activity management system", *http://lamsfoundation.org/*, 2009.

[38] U. Maurer, "Cryptography 2000 ± 10", vol. 2000, 63–85, 2001.

[39] National Technical University of Athens MediaLab, "elearning portal", *http://elearn.medialab.ntua.gr/*.

[40] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, *Handbook of Applied Cryptography*, CRC Press, Inc., Boca Raton, FL, USA, 1996.

[41] M.Nickolova and E. Nickolov, "Threat model for user security in e-learning systems", *International Journal Information Technologies and Knowledge*, vol. 1, 2007.

[42] V. Nikolopoulos, I. Likourentzou, G. Mpardis, V. Loumos, and E. Kayafas, "A web-based statistical evvaluation method for e-learning courses using student logs analysis", *In Proceedings of 2nd International Conference on Interdisciplinarity in Education ICIE 2006, May 11-13 2006, Athens, Greece*, 2006.

[43] U.S. Departmentof Commerce/ National Bureau of Standards National Technical Information Service Springfield Virginia, "Fips 197 'advanced encryption standard'", , 2001.

[44] Universityof Glasgow, "Teaching with independent learning technologies", *http://www.elec.gla.ac.uk/TILT/TILT.html*, 1993.

[45] Universityof Glasgow, "Evaluation of learning with information and communication technology", *http://www.gla.ac.uk/rcc/projects/elict/index.html*, 2000.

[46] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections", In the proceedings of the *Proceedings of the 5th International Workshop on Security Protocols*, Springer-Verlag, London, UK, 25–35, 1998.

[47] C. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme", In the proceedings of the *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 248–259, 1994.

[48] M. J. Radwin, "Efficient anonymous channel and all/nothing election scheme", In the proceedings of the *Seminar in Cryptography by Professor Philip Klein*, 1995.

[49] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms", Academic, New York, 169–179, 1978.

[50] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Commun. ACM*, vol. 21, No. 2, 120–126, 1978.

[51] K. Sako and J. Kilian, "Secure voting using partially compatible homomorphisms", In the proceedings of the *CRYPTO '94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, London, UK, 411–424, 1994.

[52] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", In the proceedings of the *In CRYPTO*, Springer-Verlag, 148–164, 1999.

[53] US DoD Advanced Distributed Learning SCORM, "Sharable content object reference model", *http://www.adlnet.gov/Technologies/scorm/default.aspx*.

[54] A. Shamir, "How to share a secret." *Communications of the ACM*, vol. 22, No. 11, 612–613, 1979.

[55] C. E. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, 379–423, 623–656, 1948.

[56] C. E. Shannon, "Communication theory of secrecy systems", *Bell Systems Technical Journal*, vol. 28, 656–715, 1949.

[57] M. Stadler, "Publicly verifiable secret sharing", *Lecture Notes in Computer Science - Advances in Cryptology - EUROCRYPT •1•7*, vol. 1070/1996, 190–199, 1996.

[58] D. L. Stufflebeam and W. J. Webster, "An analysis of alternative approaches to evaluation", *Educational Evaluation and Policy Analysis.*, vol. 2(3), 5–19, 1980.

[59] D. K. Tasoulis, E. C. Laskari, G. C. Meletiou, and M. N. Vrahatis, "Privacy preserving unsupervised clustering over vertically partitioned data", In the proceedings of the *Computational Science and Its Applications - ICCSA 2006*, vol. 3984/2006, Springer-Verlag, Heidelberg, 635–643, 2006.

[60] UNESCO, "Open and distance learning: trends, policy and strategy", *http://unesdoc.unesco.org/images/0012/001284/128463e.pd*, 2002.

[61] Hellenic Open University, "Electronic evaluation portal", *http://193.108.160.56/EAP/*, 2009.

[62] VirginiaU.S. Department of Commerce/ National Bureau of Standards National Technical Information Service Springfield, "Fips 46-2 'data encryption standard'", , 1993.

[63] M. N. Vrahatis, B. Boutsinas, P. Alevizos, and G. Pavlides, "The new k-windows algorithm for improving the k-means clustering algorithm", *J. Complex.*, vol. 18, No. 1, 375–391, 2002.

[64] J. Wu and S. Zhang, "Broadband multimedia e-learning system using web service", *APAN Network Research Workshop*, 2004.

[65] A. D. Yao, "How to generate and exchange secrets", In the proceedings of the *SFCS '86: Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, Washington, DC, USA, 162–167, 1986.

[66] S. Zachos, *Notes on Number Theory and Cryptography (in Greek)*, NTUA publishing, 2004.