ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ &
ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ**

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

**«ΣΧΕΔΙΑΣΜΟΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ ΜΕ ΥΛΙΚΟ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ»**

ΓΕΩΡΓΙΟΣ Ν. ΣΕΛΙΜΗΣ

**ΔΙΠΛΩΜΑΤΟΥΧΟΣ ΗΛΕΚΤΡΟΛΟΓΟΣ ΜΗΧΑΝΙΚΟΣ &
ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ**

ΑΡΙΘΜΟΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ: 204

ΠΑΤΡΑ ΙΟΥΛΙΟΣ 2008

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ &
ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ**

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

**«ΣΧΕΔΙΑΣΜΟΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ ΜΕ ΥΛΙΚΟ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ»**

ΓΕΩΡΓΙΟΣ Ν. ΣΕΛΙΜΗΣ

**ΔΙΠΛΩΜΑΤΟΥΧΟΣ ΗΛΕΚΤΡΟΛΟΓΟΣ ΜΗΧΑΝΙΚΟΣ &
ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ**

**ΑΡΙΘΜΟΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ: 204
ΠΑΤΡΑ ΙΟΥΛΙΟΣ 2008**

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους με στήριξαν κατά τη διάρκεια της εκπόνησης της διδακτορικής διατριβής.

Ευχαριστώ θερμά τον καθηγητή κ. Οδυσσέα Κουφοπαύλου για την καθοδήγησή του, τις χρήσιμες συμβουλές του και τη συνολική του υποστήριξη κατά τη διάρκεια της εκπόνησης της παρούσας διδακτορικής διατριβής.

Ευχαριστώ επίσης τα μέλη τις τριμελούς επιτροπής καθηγητές κ. Κωνσταντίνο Γκούτη και κ. Δημήτριο Σερπάνο για τις πολύτιμες παρατηρήσεις τους και συμβουλές τους, ώστε να γίνει η διδακτορική διατριβή καλύτερη, καθώς και όλα τα μέλη της επταμελούς επιτροπής.

Ευχαριστώ επίσης, για τις ωραίες στιγμές που περάσαμε μαζί αλλά και για τη βοήθειά τους, τα μέλη του εργαστηρίου Σχεδιασμού Ολοκληρωμένων Κυκλωμάτων του τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Απόστολο Φούρναρη, Νικόλαο Ευθυμιόπουλο, Σάκη Χρηστακίδη, Χρήστο Χρυσούλα, Γιώργο Κωστόπουλο, Αθανάσιο Μηλιδώνη, Βασίλη Πόρποδα, Γιάννη Κουρέτα, Σταύρο Γεωργιόπουλο, Χαράλαμπο Μιχαήλ, Ελένη Φωτοπούλου, Αθανάσιο Κακαρούντα, Παρασκευά Κίτσο και Νικόλαο Σκλάβο. Επίσης ευχαριστώ τη Νίκη Σαραντόγλου για την υποστήριξη που μου πρόσφερε όλη αυτήν την περίοδο.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου, Νίκο και Σταυρούλα, για τη συμπαράστασή τους και την κατανόησή τους όλα αυτά τα χρόνια, τον αδερφό μου και συγκάτοικο Στάθη, και τη φίλη μου Δήμητρα για την υπομονή της και την αμέριστη βοήθειά της. Η διδακτορική διατριβή τους είναι αφιερωμένη.

Γεώργιος Ν. Σελίμης
Πάτρα, Ιούνιος 2008

Περίληψη

Το αντικείμενο της διδακτορικής διατριβής του κ. Γεωργίου Σελίμη με τίτλο “**Σχεδιασμός Κρυπτογραφικών Συστημάτων με Υλικό Ειδικού Σκοπού**” είναι ο σχεδιασμός κρυπτογραφικών μηχανισμών για την ενσωμάτωσή τους σε συστήματα περιορισμένων πόρων (κόστος υλικού, καταναλισκόμενη ισχύς, ενέργεια). Πρωταρχικοί στόχοι είναι η περιορισμένη κατανάλωση ισχύος και η ελαχιστοποίηση του κόστους υλικού ενώ ο ρυθμός απόδοσης σε αυτά τα συστήματα αποτελεί δεύτερο στόχο.

Πολλές προσεγγίσεις έχουν προταθεί για συστήματα κρυπτογραφίας, οι οποίες προτείνουν αρχιτεκτονικές-συστήματα με υψηλή απόδοση. Οι υλοποιήσεις αυτές υποστηρίζονται από ειδικού σκοπού συστήματα υλικού. Η απόδοση πολλών από αυτών ξεπερνά το 1 Gbps και ακόμη και τα 10 Gbps αλλά καμία μελέτη δεν έχει γίνει με σκοπό την μείωση της κατανάλωσης ισχύος και κόστους υλικού. Η εξέλιξη όμως της επιστήμης της κρυπτογραφίας τα τελευταία χρόνια προήλθε από την δυνατότητα ολοκλήρωσης ηλεκτρονικών συστημάτων σε φορητές και περιορισμένων πόρων συσκευές οι οποίες επικοινωνούν ασύρματα. Σε καμία περίπτωση δεν θα μπορούσε να επιτευχθεί ασύρματη επικοινωνία σε τέτοιους ρυθμούς μετάδοσης αλλά, ούτε τα υψηλού κόστους κρυπτογραφικά συστήματα δεν θα μπορούσαν να ολοκληρωθούν σε φορητές συσκευές. Η χρήση λοιπόν των συστημάτων αυτών θα μπορούσε να γίνει στα ενσύρματα δίκτυα - στην περίπτωση βέβαια που οι υπάρχοντες υπολογιστές του δικτύου δεν θα μπορούσαν να υποστηρίξουν με το κατάλληλο λογισμικό τέτοιες ταχύτητες. Είναι λοιπόν σημαντικό να προταθούν καινούργιες προσεγγίσεις με σκοπό την μείωση της κατανάλωσης ισχύος και του συνολικού κόστους του υλικού. Η εποχή των φορητών ηλεκτρονικών υπολογιστών και των διαφόρων προσωπικών μικροσυσκευών δημιούργησε την ανάγκη για πολιτικές που στοχεύουν στην αποδοτικότερη κατανάλωση ισχύος στα ηλεκτρονικά κυκλώματα. Σύγχρονα συστήματα όπως έξυπνες κάρτες και RFID ετικέτες δεν έχουν την απαιτούμενη επιφάνεια για να ολοκληρώσουν-ενσωματώσουν μεγάλα συστήματα κρυπτογραφίας άλλα ούτε τους απαραίτητους πόρους σε ενέργεια. Δίκτυα αισθητήρων μπορεί να συμπεριλαμβάνουν σε κάθε κόμβο τους απλοϊκά συστήματα ασφάλειας αλλά σε συνεργασία μεταξύ τους μπορούν να δημιουργούν ισχυρά συστήματα ασφάλειας.

Οι κρυπτογραφικές πράξεις είναι από τη φύση τους δύσκολο να αναλυθούν, να απλοποιηθούν και να υλοποιηθούν. Παρόλα αυτά η διδακτορική διατριβή έδειξε ότι μπορεί να εφαρμοστούν σε αυτές τεχνικές χαμηλής κατανάλωσης ισχύος. Αν σε ένα κρυπτογραφικό σύστημα, οι μη αποδοτικές πράξεις από πλευράς κατανάλωσης ισχύος του συνολικού συστήματος μπορεί να αποκτήσουν χαρακτηριστικά χαμηλής κατανάλωσης ισχύος, τότε μειώνεται αισθητά η μέση κατανάλωση ισχύος. Μια προσέγγιση στην προσπάθεια μείωσης της μέσης κατανάλωσης ισχύος είναι ο εντοπισμός των λιγότερο αποδοτικών πράξεων των κρυπτογραφικών συστημάτων και η μελέτη-ανάλυση με σκοπό τη μείωση της κατανάλωσης ισχύος. Επειδή είναι προφανές πως η μεθοδολογία αυτή προορίζεται για συστήματα χαμηλών πόρων

πρέπει και το αντίστοιχο κόστος σε υλικό να είναι περιορισμένο. Έτσι ο ρυθμός απόδοσης του συνολικού συστήματος είναι ένας παράγοντας που μπορεί να μειωθεί.

Η δομή της παρούσας διδακτορικής διατριβής είναι η ακόλουθη:

Στο Κεφάλαιο 1 τονίζονται οι στόχοι της διδακτορικής διατριβής ενώ αναφέρονται περιληπτικά οι βασικές συνεισφορές της.

Ο βασικός στόχος του Κεφαλαίου 2 είναι να εισάγει τον αναγνώστη στις αρχές της επιστήμης της κρυπτογραφίας. Αναφέρονται όλα τα βασικά στοιχεία που είναι απαραίτητα στο να διασαφηνιστούν έννοιες και αρχές σχετικά με την κρυπτογραφία. Διευκρινίζονται θέματα όπως κρυπτογραφία και μαθηματικές συναρτήσεις, ασφάλεια πληροφορίας, κατηγοριοποίηση των αλγορίθμων, βασικές κρυπτογραφικές πράξεις, αλγόριθμοι και πρωτόκολλα, η γνώση των παραπάνω αποτελεί τη βάση για το σχεδιασμό ασφαλών συστημάτων.

Στο Κεφάλαιο 3 παρουσιάζονται κλασικές προσεγγίσεις ενσωμάτωσης κρυπτογραφικών αλγορίθμων σε συστήματα περιορισμένων πόρων, αναφέρονται οι κύριες πηγές κατανάλωσης ισχύος για τα κυκλώματα CMOS και παρουσιάζονται έπειτα μερικές μέθοδοι για το πώς μπορεί να περιοριστεί η κατανάλωση ισχύος στα διάφορα επίπεδα σχεδιασμού. Αρχικά δίνονται περιληπτικά κάποιες τυπικές προσεγγίσεις σε θέματα κρυπτογραφίας και χαμηλής κατανάλωσης ισχύος. Έπειτα γίνεται αναφορά στις παραμέτρους υλοποίησης του συστήματος και πώς αυτές επηρεάζουν το συνολικό σύστημα. Τέλος στο Κεφάλαιο 3 αναφέρονται λεπτομερώς οι κυριότερες τεχνικές μείωσης κατανάλωσης ισχύος.

Στο Κεφάλαιο 4 παρουσιάζεται μια προσέγγιση για ολοκληρωμένο σύστημα ασφάλειας σε συστήματα εξαιρετικά περιορισμένων πόρων. Τέτοια συστήματα μπορεί να είναι Έξυπνες Κάρτες και RFID ετικέτες. Η μελέτη για τη σχεδίαση του συστήματος αυτού ξεκινά από το επίπεδο πρωτοκόλλου. Έπειτα ακολουθεί η επιλογή των αλγορίθμων που θα υποστηρίξουν το πρωτόκολλο. Σε επίπεδο αρχιτεκτονικής συστήματος προτάσεις παρατίθενται για την καλύτερη σύγκλιση των αλγορίθμων κρυπτογραφίας με τις απαιτήσεις χαμηλών πόρων του συνολικού συστήματος.

Στο Κεφάλαιο 5 παρουσιάζεται λεπτομερώς η διαδικασία βελτιστοποίησης τριών δομικών κρυπτογραφικών πράξεων, στον πολλαπλασιασμό σε πεπερασμένα σώματα (Finite Fields) που χρησιμοποιείται κυρίως στα κρυπτογραφικά συστήματα δημοσίου κλειδιού και σε δύο δομικές μονάδες του αλγορίθμου συμμετρικής κρυπτογραφίας AES, το Subbytes/InvSubBytes μετασχηματισμό και το MixColumn/InvMixColumns μετασχηματισμό.

Στο Κεφάλαιο 6 προτείνεται αρχιτεκτονική 8-bit περιορισμένης κατανάλωσης ισχύος και επιφάνειας για τον αλγόριθμο AES. Η προτεινόμενη αρχιτεκτονική υποστηρίζει την κρυπτογράφηση και την αποκρυπτογράφηση καθώς και τις αντίστοιχες βασικές διαδικασίες δημιουργίας των κλειδιών για τρία διαφορετικά μεγέθη του κλειδιού (128, 192 και 256 bit), δίνοντας τη δυνατότητα στο σύστημα της υποστήριξης διαφορετικών επιπέδων ασφάλειας. Οι προτεινόμενες αρχιτεκτονικές χαμηλής κατανάλωσης ισχύος, του 5^{ου} Κεφαλαίου, για τους κρυπτογραφικούς μετασχηματισμούς SubBytes/InvSubBytes και MixColumns/InvMixColumns ενσωματώνονται στο σύστημά μας. Η προτεινόμενη υλοποίησή μας όχι μόνο μειώνει την κατανάλωση ισχύος σε μεγάλο βαθμό αλλά προσφέρει ικανοποιητικά

αποτελέσματα για τον παράγοντα «Απόδοση x Ισχύς» σε σχέση με άλλες εργασίες για τον AES αλγόριθμο.

Συμπεράσματα και μελλοντικές προεκτάσεις της εργασίας αυτής παρουσιάζονται στο Κεφάλαιο 7.

Abstract

The evolution of mobile-wireless computing systems have triggered the development of new cryptographic needs. Therefore, existing and new cryptographic algorithm architectures have to be designed in order to satisfy the mobile wireless system specifications. Wireless mobile standards limit a wireless system's throughput to less than a hundred Mbps. This is a quite satisfactory limit and it is capable to support real-time applications as voice, video and online streaming. Additionally, the nature of mobile systems highlights the needs for strict power and area constraints. However, many cryptographic designs focus on achieving high-throughput by unrolling the rounds of the algorithm and using extended pipelining techniques. These designs that can achieve high throughput rates, are appropriate for high-end applications that are not constrained in power consumption and chip covered area. Therefore, it is impossible to integrate these modules in mobile systems. In addition, high throughput values are useless in wireless systems since transmitting data in such a high rate is infeasible.

The main contributions of this phd thesis involve:

Lightweight secure mechanism: A top-down methodology

A complete design approach for cryptographic systems in limited resources (power, energy, area) systems is introduced. Such systems can be Smart Cards and RFID tags. The methodology is presented in three levels of design, protocol level, algorithmic level and architecture level. Firstly, the choice of the appropriate secure protocol is discussed. Then, the choice of algorithms that support the protocol and the appropriate applied hardware techniques are presented. Finally, hardware design techniques in architecture level are discussed. Power, area and energy optimization results are presented in the experimental results analysis.

There are three contributions in the domain of optimized cryptographic operations.

a) Versatile multiplier for $GF(2^8)$ Finite Fields

Bit serial multipliers are used in resources constrained systems. The throughput of a multiplier is dependent on the required number of clock cycles to reach a result and its critical path delay. However, most bit serial $GF(2^m)$ multipliers do not manage to reduce the required number of clock cycles below the threshold of m clock cycles without increasing dramatically their critical path delay. This increase is more evident if a multiplier is designed to be versatile. In this article, a new versatile bit serial MSB multiplier for $GF(2^m)$ fields is proposed that achieves a 50 % increase in throughput when compared to other designs, with a very small increase in its critical path delay. This is achieved by an average 33,4 % reduction in the required number of clock cycles below m . The proposed design can handle arbitrary bit-lengths upper bounded by m and is suitable for applications where the field order may vary, like Elliptic Curve Cryptography. By being versatile, the proposed multiplier can support any cryptographic standard using $GF(2^m)$ fields depending on the security, power, energy, throughput and area requirements of the system.

b) Optimized SubBytes transformation in terms of power and area

In this contribution low power architectures in limited area resources are proposed for Sbox, the basic cryptographic primitive of AES. Those architectures support encryption and decryption operation modes. In our proposed implementations, retaining a small chip covered area cost, hardware techniques for low power design, such as re-ordering of the components, introduction of redundant hardware (ideal delay line), reducing the driving strength – fan out, and insertion of registers in highly unbalanced points of the circuit are applied. Therefore, our implementations do not only reduce power consumption by a large degree, but they also have good area properties and offer an advantageous power-delay-area product in comparison with other known Sbox implementations. These properties give to our system the advantage to support low power mobile devices in low area system environments.

c) Optimized MixColumns transformation in terms of power and area

In this contribution the low power techniques of Resource Sharing and Power Management are applied in a 32-bit architecture for the MixColumn/InvMixColumn transformation of the Advanced Encryption Standard. The proposed architecture performs multiplication in $GF(2^8)$ field of a byte $s_{i,j}$ with specific constants, using a common data path. Low power consumption is also achieved by deactivating the unused parts of the data path when MixColumn Transformation is performed. The proposed architecture achieves low power consumption and low area resources compared to other designs.

An 8-bit Advanced Encryption Standard Design with low power-low area properties

In this contribution a low power 8-bit architecture in limited area resources is proposed for AES. The proposed architecture supports encryption, and decryption with their corresponding key expansion processes for three different sizes of key (128, 192 and 256 bit). Two proposed low power designs for SubBytes and MixColumns main cryptographic primitives of AES algorithm are presented. Our implementation does not only reduce power consumption by a large degree, but it also utilizes limited area resources and it offers an advantageous "power x area" product in comparison with other known AES implementations, achieving throughput rates that are satisfactory for wireless protocols. The proposed design achieves maximum throughput 42.9 Mbps using 0.18 μm CMOS technology with 180 MHz clock rate. The hardware implementation cost is 7545 gates with power consumption of 0.82 mW.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1. Εισαγωγή	23
ΚΕΦΑΛΑΙΟ 2. Βασικά στοιχεία κρυπτογραφίας	29
2.1. Εισαγωγή	29
2.2. Ασφάλεια πληροφορίας και κρυπτογραφία	29
2.3. Συναρτήσεις και κρυπτογραφία	33
2.3.1. Συναρτήσεις (1-1, ενός δρόμου (one-way), trapdoor one way)	33
2.3.2. Αναδιατάξεις (Permutations)	35
2.3.3. Involutions	35
2.4. Βασική ορολογία για την κρυπτογραφία	36
2.4.1. Κρυπτογράφηση: Domains και Co domains	36
2.4.2. Μετασχηματισμοί κρυπτογράφησης και αποκρυπτογράφησης	36
2.4.3. Επιτυχάνοντας εμπιστευτικότητα	36
2.4.4. Τα μέρη της επικοινωνίας	37
2.4.5. Τα Κανάλια Επικοινωνίας	38
2.4.6. Θεωρία Ασφάλειας	39
2.5. Κρυπτογραφία συμμετρικού κλειδιού	40
2.5.1. Γενικά για τους αλγόριθμους Block και Stream ciphers	40
2.5.2. Κρυπτογραφικοί αλγόριθμοι Ροής (Stream ciphers)	41
2.6. Ψηφιακές Υπογραφές	42
2.7. Συστήματα κρυπτογραφίας δημοσίου κλειδιού	43
2.7.1. Κρυπτογράφηση δημόσιου κλειδιού	43
ΚΕΦΑΛΑΙΟ 3. Σχεδιασμός κρυπτογραφικών συστημάτων σε υλικό	47
3.1 Τυπικές προσεγγίσεις σε θέματα χαμηλής κατανάλωσης ενέργειας στην κρυπτογραφία	47
3.1.1. ASIC Προσέγγιση	47
3.1.2. FPGA Προσέγγιση	48
3.1.3. Προσέγγιση λογισμικού	48

3.2	Γνωστά κρυπτογραφικά σχήματα για χαμηλή κατανάλωση ισχύος	48
3.3	Βασικές κρυπτογραφικές αρχιτεκτονικές και επιπτώσεις στο συνολικό σύστημα	49
3.4	Πηγές κατανάλωσης ισχύος	52
3.4.1.	Δυναμική Ισχύς	52
3.4.2.	Ισχύς διακοπτικής δραστηριότητας	52
3.4.3.	Ισχύς βραχυκυκλώματος	53
3.4.4.	Στατική ισχύς	54
3.4.5.	Μη αποδεκτές φορτίσεις-εκφορτίσεις (glitching)	54
3.5	Τεχνικές Μείωσης Μέσης Κατανάλωσης Ισχύος	55
3.5.1.	Βελτιστοποίηση σε Επίπεδο Τεχνολογίας (Technology Level)	56
3.5.2.	Βελτιστοποίηση σε επίπεδο συστήματος (System Level)	56
3.5.3.	Βελτιστοποίηση σε επίπεδο συμπεριφοράς/αλγορίθμου (Behavioral/ Algorithmic Level)	57
3.5.4.	Βελτιστοποίηση σε επίπεδο αρχιτεκτονικής (Architectural Level)	59
3.5.5.	Βελτιστοποίηση σε επίπεδο πύλης (Gate Level)	61
3.5.6.	Βελτιστοποίηση σε φυσικό Επίπεδο (Physical Layer)	65
ΚΕΦΑΛΑΙΟ 4. Σχεδιασμός συστήματος ασφάλειας για περιορισμένων πόρων εφαρμογές		69
4.1.	Εισαγωγή	69
4.2.	Υπηρεσίες ασφάλειας συστήματος	70
4.2.1.	Συμμετρική Μονομερής Πιστοποίηση	70
4.2.2.	Συμμετρική από Κοινού πιστοποίηση	72
4.3.	Οι αλγόριθμοι του συστήματος	73
4.3.1.	Ο αλγόριθμος κρυπτογράφησης DES	74
4.3.2.	Ο αλγόριθμος κρυπτογράφησης TDES	77
4.3.3.	Η γεννήτρια τυχαίων αριθμών PRNG ANSI X9.17	77
4.4.	Σχεδιασμός σε Υλικό Ολοκληρωμένου Συστήματος	78
4.5.	Συμπεράσματα	81

ΚΕΦΑΛΑΙΟ 5. Βελτιστοποίηση δομικών κρυπτογραφικών πράξεων για συστήματα περιορισμένων πόρων	83
5.1. Εισαγωγή	83
5.2. Προτεινόμενη αρχιτεκτονική σειριακού πολλαπλασιαστή σε πεπερασμένα σώματα $GF(2^m)$	83
5.3. Γενικά για τους πολλαπλασιαστές σε πεπερασμένα πεδία $GF(2^m)$	84
5.4. Πολλαπλασιασμός σε Πολυωνυμική Βάση	86
5.4.1. Μαθηματικό Υπόβαθρο	86
5.4.2. MSB σειριακός πολλαπλασιαστής πεπερασμένων σωμάτων $GF(2^m)$	86
5.5. Τυπική αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$	88
5.6. Προτεινόμενη αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$	90
5.7. Πολιτική Ελέγχου της Ροής Δεδομένων	94
5.8. Ανάλυση της απόδοσης του προτεινόμενου συστήματος	95
5.9. Συγκρίσεις με άλλες εργασίες	99
5.10. Συμπεράσματα σχετικά με την προτεινόμενη αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$	100
5.11. Σχεδιασμός του κρυπτογραφικού μετασχηματισμού SubBytes/InvSubBytes (Sbox) για συστήματα χαμηλών πόρων	102
5.12. Γενικά για το μετασχηματισμό SubBytes (Sbox)	102
5.13. Ο αλγόριθμος AES (Advanced Encryption Standard)	103
5.14. Ο Subbytes/InvSubBytes μετασχηματισμός	104
5.15. Προηγούμενες υλοποιήσεις στο Subbytes/InvSubBytes μετασχηματισμό	106
5.16. Προτεινόμενη υλοποίηση του Subbytes/InvSubBytes μετασχηματισμού	108
5.17. Πειραματικά αποτελέσματα και Συγκρίσεις με άλλες εργασίες για το στοιχείο SubBytes	114
5.18. Προτεινόμενη αρχιτεκτονική MixColumns / InvMixColumns για εφαρμογές περιορισμένων πόρων	117
5.19. Μαθηματικό υπόβαθρο	117
5.20. Οι Μετασχηματισμοί MixColumns και InvMixColumns	117

5.21. Προτεινόμενη αρχιτεκτονική MixColumns / InvMixColumns	119
5.21.1. Η αρχιτεκτονική του συστήματος MixColumns / InvMixColumns	119
5.21.2. Ο προτεινόμενος αλγόριθμος	120
5.21.3. Η τεχνική κοινής χρήσης των πόρων (Resource Sharing)	121
5.21.4. Διαχείριση καταναλισκόμενης ισχύος	123
5.22. Αποτελέσματα, συγκρίσεις και συμπεράσματα	124
ΚΕΦΑΛΑΙΟ 6. Υλοποίηση του αλγορίθμου AES για εφαρμογές περιορισμένων πόρων	127
6.1. Εισαγωγή	127
6.2. Ο αλγόριθμος AES (Advanced Encryption Standard)	128
6.3. Σχεδίαση του Συστήματος	128
6.4. Αρχιτεκτονική Χαμηλής Κατανάλωσης Ισχύος για το Μετασχηματισμό SubBytes	131
6.5. Αρχιτεκτονική Χαμηλής Κατανάλωσης Ισχύος για το Μετασχηματισμό MixColumns/InvMixColumns	132
6.6. Χαμηλής Κατανάλωσης Αρχιτεκτονική AES	133
6.7. Συμπεράσματα	138
ΚΕΦΑΛΑΙΟ 7. Τελικά συμπεράσματα και μελλοντική εργασία	141
ΒΙΒΛΙΟΓΡΑΦΙΑ	147
ΔΗΜΟΣΙΕΥΣΕΙΣ	153

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

Εικόνα 1: Η συσχέτιση των βασικών μηχανισμών ασφάλειας.....	32
Εικόνα 2: Η συνάρτηση f από το σύνολο X σε τρία στοιχεία του συνόλου Y	33
Εικόνα 3: Η αντίστροφη συνάρτηση f και η αντίστροφή της $g = f^{-1}$	34
Εικόνα 4: Σχηματικό απλού κρυπτογραφικού συστήματος.....	37
Εικόνα 5: Σχηματικό επικοινωνίας δύο συμβαλλόμενων μελών χρησιμοποιώντας κρυπτογράφηση.....	38
Εικόνα 6: Σχηματικό επικοινωνίας για κρυπτογράφηση συμμετρικού κλειδιού.....	41
Εικόνα 7: Η υπογραφή και επαλήθευση σε ένα σύστημα ψηφιακής υπογραφής.....	43
Εικόνα 8: Το σύστημα κρυπτογράφησης Δημοσίου Κλειδιού.....	44
Εικόνα 9: Το σύστημα ρυθμιζόμενης ασφάλειας/απόδοσης.....	49
Εικόνα 10: Η μέθοδος ανάδρασης.....	50
Εικόνα 11: Η μέθοδος Διοχέτευσης.....	51
Εικόνα 12: Παράλληλη Επεξεργασία Δεδομένων.....	51
Εικόνα 13: Οι χωρητικότητες εξόδου του αναστροφέα.....	53
Εικόνα 14: Οι ανεπιθύμητες φορτίσεις-εκφορτίσεις.....	54
Εικόνα 15: Η ιεραρχία για την υλοποίηση πρωτοκόλλων ασφαλείας.....	69
Εικόνα 16: Μονομερής πιστοποίηση με χρήση συμμετρικού αλγορίθμου.....	71
Εικόνα 17: Οι ερμηνείες των συμβόλων.....	71
Εικόνα 18: Συμμετρική Πιστοποίηση με χρήση συμμετρικού αλγορίθμου.....	73
Εικόνα 19: Οι 16 κύκλοι για τη δημιουργία του κρυπτογραφημένου μπλοκ στον αλγόριθμο DES.....	75
Εικόνα 20: Η συνάρτηση $f(R,K)$	76
Εικόνα 21: Η παραγωγή των κλειδιών (KS)για κάθε κύκλο του αλγορίθμου DES.....	76
Εικόνα 22: Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης TDES.....	77
Εικόνα 23: Η γεννήτρια τυχαίων αριθμών X9.17.....	78
Εικόνα 24: Οι βασικές είσοδοι και εξοδοι του συστήματος.....	78
Εικόνα 25: Η προτεινόμενη αρχιτεκτονική του συστήματος ασφαλείας.....	79
Εικόνα 26: Η προτεινόμενη αρχιτεκτονική της τεχνολογίας gated clock.....	80
Εικόνα 27: Η ροή των δεδομένων για τον MSB $GF(2^m)$ πολλαπλασιασμό.....	88
Εικόνα 28: Τυπική αρχιτεκτονική του MSB σειριακού πολλαπλασιαστή σε $GF(2^m)$	88
Εικόνα 29: Η εσωτερική δομή του κελιού.....	90
Εικόνα 30: Η προτεινόμενη αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$	92
Εικόνα 31: Η ροή των δεδομένων μεταξύ δύο γειτονικών κελιών για $mode=ORDINARY$	93
Εικόνα 32: Η ροή των δεδομένων μεταξύ δύο γειτονικών κελιών για $mode=OMISSION$	94
Εικόνα 33: Το δομικό στοιχείο PASS.....	94
Εικόνα 34: Shift Register κατάσταση (a) πριν και (b) μετά την παράλειψη κύκλου και οι δύο καταστάσεις (c) και (d) του PASS δομικού στοιχείου.....	95
Εικόνα 35: Το ποσοστό % των κύκλων που παραλείπονται κατά μέσο όρο.....	96
Εικόνα 36: Συγκρίσεις απόδοσης τυπικής και προτεινόμενης αρχιτεκτονικής για $m=100, 200, 400, 57098$	98
Εικόνα 37: Συγκρίσεις απόδοσης/επιφάνεια τυπικής και προτεινόμενης αρχιτεκτονικής για $m=100, 200, 400, 570$	98
Εικόνα 38: Οι διεργασίες κρυπτογράφησης και αποκρυπτογράφησης του AES αλγορίθμου.....	104
Εικόνα 39: Ο affine μετασχηματισμός σε μορφή μητρώου.....	105
Εικόνα 40: Γραφική αναπαράσταση του SubBytes μετασχηματισμού.....	105
Εικόνα 41: Ο πίνακας μετασχηματισμών για την κρυπτογράφηση (σε δεκαεξαδική μορφή).....	106
Εικόνα 42: Ο πίνακας μετασχηματισμών για την αποκρυπτογράφηση (σε δεκαεξαδική μορφή)......	106
Εικόνα 43: Η αριθμητική υλοποίηση της τυπικής SubBytes αρχιτεκτονικής.....	109
Εικόνα 44: Οι προτεινόμενες αρχιτεκτονικές Implem1 και Implem2.....	110
Εικόνα 45: Οι κόμβοι εσωτερικά του δομικού στοιχείου COMP.....	111
Εικόνα 46: Οι προτεινόμενες αρχιτεκτονικές Implem1R (a) και Implem2R (b).....	113
Εικόνα 47: Συγκρίσεις αρχιτεκτονικών ως προς την επιφάνεια.....	114
Εικόνα 48: Συγκρίσεις αρχιτεκτονικών ως προς την Ισχύ.....	115
Εικόνα 49: Συγκρίσεις αρχιτεκτονικών ως προς την καθυστέρηση.....	115
Εικόνα 50: Συγκρίσεις αρχιτεκτονικών ως προς την Ισχύ x Επιφάνεια x Καθυστέρηση.....	116
Εικόνα 51: Η γραφική απεικόνιση της MixColumns πράξης.....	119
Εικόνα 52: Η 32-bit αρχιτεκτονική του συστήματος MixColumns/InvMixColumns.....	120
Εικόνα 53: Η διαδικασία των MixColumns πολλαπλασιασμών σε μορφή δέντρου.....	122
Εικόνα 54: Type II διεργασία.....	123
Εικόνα 55: Type III διεργασία.....	123
Εικόνα 56: Το εσωτερικό κύκλωμα του δομικού στοιχείου Multiplier.....	124

<i>Εικόνα 57: Η αρχιτεκτονική του AES συστήματος.....</i>	<i>130</i>
<i>Εικόνα 58: Η προτεινόμενη αρχιτεκτονική του δομικού στοιχείου SubBytes</i>	<i>131</i>
<i>Εικόνα 59: 8-bit Αρχιτεκτονική της MixColumn/InvMixColumn</i>	<i>133</i>
<i>Εικόνα 60: Τα σενάρια λειτουργίας του αλγορίθμου.....</i>	<i>134</i>
<i>Εικόνα 61: 8-bit προτεινόμενη αρχιτεκτονική AES.....</i>	<i>135</i>
<i>Εικόνα 62: Η αρχιτεκτονική Key Expansion.....</i>	<i>136</i>
<i>Εικόνα 63: Η συνολική ενέργεια σε σχέση με τα διαφορετικά σενάρια λειτουργίας.....</i>	<i>137</i>
<i>Εικόνα 64: Η κατανομή της συνολικής επιφάνειας του συστήματος στα δομικά στοιχεία</i>	<i>138</i>

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

Πίνακας 1: Βασικές έννοιες στη θεωρία Ασφάλειας.....	30
Πίνακας 2: Παράδειγμα συνάρτησης one-way	34
Πίνακας 3: Προσπάθειες κρυπτανάλυσης RC5 κρυπτογραφικού συστήματος.....	49
Πίνακας 4: Αποτελέσματα Εξομοίωσης.....	80
Πίνακας 5: Σύγκριση των δύο τεχνικών	80
Πίνακας 6: Σύγκριση Τυπικής με Προτεινόμενης Αρχιτεκτονικής	97
Πίνακας 7: Σύγκριση με άλλες εργασίες	100
Πίνακας 8: Τα αποτελέσματα εξομοίωσης όλων των αρχιτεκτονικών.....	116
Πίνακας 9: Οι απαιτούμενοι κύκλοι για κάθε μεταβλητή.....	122
Πίνακας 10: Αποτελέσματα σύγκρισης αρχιτεκτονικών.....	125
Πίνακας 11: Οι απαιτούμενοι κύκλοι για διαφορετικά κλειδιά.....	136
Πίνακας 12: Συγκρίσεις αρχιτεκτονικών AES	137

ΚΕΦΑΛΑΙΟ 1. Εισαγωγή

Η συγκεκριμένη Διδακτορική Διατριβή ήρθε να συνεισφέρει στην ανάγκη για σχεδιασμό κρυπτογραφικών μηχανισμών ώστε να ενσωματωθούν σε συστήματα περιορισμένων πόρων (κόστος υλικού, καταναλισκόμενη ισχύς, ενέργεια). Ο ρυθμός απόδοσης σε αυτά τα συστήματα αποτελεί δεύτερο στόχο, ενώ πρωταρχικοί στόχοι είναι η περιορισμένη κατανάλωση ισχύος και η ελαχιστοποίηση του κόστους υλικού.

Η ενσωμάτωση και ολοκλήρωση κρυπτογραφικών αλγορίθμων σε ηλεκτρονικά συστήματα είναι άρρηκτα συνδεδεμένη με την εφαρμογή (προτυποποιήσεις) και τα περιθώρια σε πόρους (υλικού, καταναλισκόμενη ισχύς, ενέργεια) του ηλεκτρονικού συστήματος. Η προσφερόμενη ασφάλεια εξαρτάται κυρίως από το πρότυπο-πρωτόκολλο ασφάλειας και στην περίπτωση που το πρότυπο μας επιτρέπει να χρησιμοποιήσουμε διαφορετικά επίπεδα ασφάλειας έχουμε τη δυνατότητα να ενσωματώσουμε στη συσκευή μας όσο το δυνατό ασφαλέστερα χαρακτηριστικά (περισσότερα του ενός πρότυπα-πρωτόκολλα ή διαφορετικά σενάρια λειτουργίας του ιδίου προτύπου). Αν το σύστημά μας ικανοποιεί έστω και ένα αποδεκτό πρότυπο ασφάλειας τότε μπορεί να χρησιμοποιηθεί σε σενάριο επικοινωνίας και να μεταδώσει πληροφορία σε άλλα συμβαλλόμενα μέρη του συστήματος επικοινωνίας. Σε περίπτωση που έχει τη δυνατότητα να εμπεριέχει και πιο ασφαλή πρότυπα τότε το σύστημά μας γίνεται πιο αξιόπιστο αλλά και συμβατό με περισσότερα συμβαλλόμενα μέρη στην επικοινωνία (1).

Η ολοκλήρωση συστημάτων ασφαλείας σε υλικό είναι σχεδόν αναγκαία για τα ενσωματωμένα συστήματα κρυπτογράφησης. Τα πλεονεκτήματα που έχουμε είναι η υψηλή απόδοση, η μειωμένη κατανάλωση ισχύος με μειονέκτημα το κόστος της ολοκλήρωσης σε υλικό. Νέες τεχνολογίες όπως FPGAs (Field-Programmable Gate Array) (2), επιτρέπουν την πιο εύκολη ολοκλήρωση του αλγορίθμου και την ανανέωση - αντικατάστασή του από νεώτερους-βελτιωμένους. Ήδη τα τελευταίες γενιάς FPGAs τείνουν να έχουν τις ιδιότητες των ASICs (Application-Specific Integrated Circuit) (3)-μειωμένη κατανάλωση ισχύος, υψηλή απόδοση, και ρύθμιση της λειτουργικότητας ανάλογα την εφαρμογή. Ένα άλλο πλεονέκτημα των υλοποιήσεων σε υλικό είναι πως από τις φύση τους είναι λιγότερο ευαίσθητο σε επιθέσεις κρυπτανάλυσης (4), (5) ενώ μπορεί ευκολότερα να ενσωματώσει πολιτικές αντιμετώπισης κρυπταναλυτικών τεχνικών (6).

Πολλές προσεγγίσεις έχουν προταθεί για συστήματα κρυπτογραφίας οι οποίες εστιάζονται και προτείνουν αρχιτεκτονικές-συστήματα με υψηλή απόδοση. Οι υλοποιήσεις αυτές υποστηρίζονται από ειδικού σκοπού συστήματα υλικού. Πολλά εξ' αυτών ξεπερνούν το 1Gbps και ακόμη και τα 10 Gbps και καμία μελέτη δε γίνεται σε θέματα κατανάλωσης ισχύος και κόστους υλικού. Η εξέλιξη όμως της επιστήμης της κρυπτογραφίας τα τελευταία χρόνια προήλθε από την δυνατότητα ολοκλήρωσης ηλεκτρονικών συστημάτων σε φορητές και περιορισμένων πόρων συσκευές οι οποίες

επικοινωνούν ασύρματα. Σε καμία περίπτωση δεν θα μπορούσε να επιτευχθεί επικοινωνία μέσω αέρα σε τέτοιους ρυθμούς μετάδοσης, ούτε τα υψηλού κόστους κρυπτογραφικά συστήματα δε θα μπορούσαν να ολοκληρωθούν σε φορητές συσκευές. Η χρήση λοιπόν των συστημάτων αυτών θα μπορούσε να γίνει στα ενσύρματα δίκτυα- στην περίπτωση βέβαια που οι υπάρχοντες υπολογιστές του δικτύου δε θα μπορούσαν να υποστηρίξουν με το κατάλληλο λογισμικό τέτοιες ταχύτητες.

Σε αυτό το θέμα πρέπει να προτείνονται προσεγγίσεις με το ελάχιστο κόστος σε υλικό και με την μικρότερη κατανάλωση ισχύος. Η νέα γενιά των φορητών ηλεκτρονικών υπολογιστών και των διαφόρων προσωπικών μικροσυσκευών δημιούργησε την ανάγκη για πολιτικές που στοχεύουν στην αποδοτικότερη κατανάλωση ισχύος στα ηλεκτρονικά κυκλώματα. Σύγχρονα συστήματα όπως έξυπνες κάρτες (7) και RFID ετικέτες δεν έχουν την απαιτούμενη επιφάνεια για να ολοκληρώσουν-ενσωματώσουν μεγάλα συστήματα κρυπτογραφίας, άλλα ούτε τους απαραίτητους πόρους σε ενέργεια-μπορεί ακόμη να εξάγουν ενέργεια από το ηλεκτρομαγνητικό πεδίο. Δίκτυα αισθητήρων μπορεί να συμπεριλαμβάνουν σε κάθε κόμβο τους απλοϊκά συστήματα ασφάλειας αλλά σε συνεργασία μεταξύ τους (8) μπορούν να δημιουργούν ισχυρά συστήματα ασφάλειας.

Οι κρυπτογραφικές πράξεις είναι από τη φύση τους δύσκολο να αναλυθούν και να απλοποιηθούν. Παρόλα αυτά μπορούμε να εφαρμόσουμε σε αυτές τεχνικές χαμηλής κατανάλωσης ισχύος. Αν οι μη αποδοτικές πράξεις από πλευράς κατανάλωσης ισχύος του συνολικού συστήματος, μπορούν να αποκτήσουν χαρακτηριστικά χαμηλής κατανάλωσης ισχύος, τότε θα μειωθεί αισθητά η μέση κατανάλωση ισχύος του κρυπτογραφικού συστήματος. Μια προσέγγιση στην προσπάθεια μείωσης της μέσης κατανάλωσης ισχύος είναι ο εντοπισμός των λιγότερο αποδοτικών πράξεων των κρυπτογραφικών συστημάτων και η μελέτη-ανάλυση με σκοπό τη μείωση της κατανάλωσης ισχύος. (9). Επειδή είναι προφανές πως η μεθοδολογία αυτή προορίζεται για συστήματα χαμηλών πόρων πρέπει και το αντίστοιχο κόστος σε υλικό να είναι περιορισμένο. Από την άλλη πλευρά, ο ρυθμός απόδοσης του συνολικού συστήματος είναι ένας παράγοντας που μπορεί να θυσιαστεί.

Επιπλέον ένα σημαντικό χαρακτηριστικό των σύγχρονων συστημάτων ασφαλείας είναι το να μπορούν να υποστηρίζουν σενάρια βαθμωτής ασφαλείας (1). Το γεγονός αυτό μπορεί και προστατεύει τους εναπομείναντες πόρους του συστήματος (ενέργεια), ή επιτρέπει σε λιγότερο πολύπλοκα συστήματα να επικοινωνούν με λιγότερους σύνθετους μηχανισμούς ασφαλείας.

Σκοπός της διδακτορικής διατριβής είναι η ενσωμάτωση μηχανισμών ασφαλείας σε υλικό για περιβάλλοντα περιορισμένων πόρων (ενέργεια, ισχύς, κόστος υλικού). Στην παρούσα διδακτορική διατριβή δύο κεφάλαια μας εισάγουν στις βασικές αρχές της κρυπτογραφίας (Κεφάλαιο 2) και στις βασικές τεχνικές για συστήματα περιορισμένων πόρων (Κεφάλαιο 3) αντίστοιχα. Στο Κεφάλαιο 4, προτείνεται πρωτόκολλο ασφαλείας για συστήματα πολύ χαμηλών πόρων. Το πρωτόκολλο

ασφαλείας στηρίζεται στον αλγόριθμο κρυπτογραφίας DES (10). Επιλέγουμε τους κατάλληλους μηχανισμούς ώστε να υποστηρίξουμε το πρωτόκολλο ασφάλειας πάλι με κριτήριο τους μειωμένους πόρους της συσκευής. Έπειτα τεχνικές χαμηλής κατανάλωσης ισχύος και υλικού εφαρμόζονται ώστε το σύστημά μας να διαχειριστεί πιο αποδοτικά την καταναλισκόμενη ισχύς αλλά και να είναι περιορισμένο σε επιφάνεια.

Υπάρχουν τρεις συνεισφορές στο θέμα της βελτιστοποίησης βασικών κρυπτογραφικών δομικών στοιχείων και παρουσιάζονται στο Κεφάλαιο 5. Αρχικά παρουσιάζεται η υλοποίηση ενός επαναπροσδιορίσιμου σειριακού πολλαπλασιαστή σε αριθμητική πεπερασμένων σωμάτων (Finite Fields) για συστήματα περιορισμένων πόρων. Ο πολλαπλασιαστής αυτός έχει το πλεονέκτημα ότι διατηρώντας χαμηλούς τους πόρους σε υλικό και ισχύ, εκτελεί κάτω από m κύκλους αλγορίθμου (περίπου 34% πιο γρήγορα) τον πολλαπλασιασμό. Επίσης έχει τη δυνατότητα να υποστηρίξει οποιοδήποτε πολυώνυμο μέχρι m ψηφία μήκος αλλά και οποιοδήποτε ανάγωγο (irreducible) πολυώνυμο προσφέροντας διαφορετικών επιπέδων ασφάλεια. Η δυνατότητα αυτή το κάνει κατάλληλο συστατικό για συστήματα ελλειπτικών καμπυλών χαμηλών πόρων.

Η βασική κρυπτογραφική πράξη του αλγορίθμου AES (Advanced Encryption Standard), SuBBytes/InvSubBytes, με ιδιότητες χαμηλής κατανάλωσης ισχύος και σε μικρό κόστος επιφάνειας είναι το δεύτερο δομικό κρυπτογραφικό στοιχείο που βελτιστοποιήθηκε και παρουσιάζεται στο Κεφάλαιο 5. Αρχικά έγινε μια μελέτη διαφορετικών προσεγγίσεων-υλοποιήσεων του μετασχηματισμού SubBytes. Έπειτα παρουσιάστηκε η μεθοδολογία ώστε να καταλήξουμε στην προσέγγιση όπου είναι ιδανική για χαμηλών πόρων συστήματα.

Μια εξίσου σημαντική πράξη του αλγορίθμου AES βελτιστοποιήθηκε με σκοπό τη χαμηλή κατανάλωση ενέργειας και τους μειωμένους πόρους σε υλικό είναι η MixColumns που βελτιστοποιείται στο Κεφάλαιο 5. Βρίσκοντας λογικές συνθήκες στην είσοδο του συστήματος ώστε να κρατάμε ανενεργά δομικά στοιχεία του, κατορθώνουμε να εξοικονομούμε συνολική ενέργεια μειώνοντας το ρυθμό κατανάλωσης ισχύος. Επιπλέον τεχνικές εφαρμόζονται για τη μείωση του συνολικού κόστους σε υλικό.

Στο Κεφάλαιο 6 μια ολοκληρωμένη μεθοδολογία για σχεδιασμό χαμηλής κατανάλωσης ισχύος κρυπτογραφικά συστήματα προτείνεται. Παρουσιάζεται αναλυτικά όλη η διαδικασία μέχρι ο σχεδιαστής να καταλήξει στην υλοποίηση σε υλικό. Σαν εφαρμογή χρησιμοποιούμε τον αλγόριθμο AES. CAD εργαλεία και πακέτα λογισμικού υψηλού επιπέδου (Γλώσσα Προγραμματισμού C) αποτελούν χρήσιμα εργαλεία σε αυτήν την προσπάθεια. Οι ήδη προτεινόμενες αρχιτεκτονικές χαμηλών πόρων (Κεφάλαιο 5) για τους μετασχηματισμούς SubBytes και MixColumns βοηθούν ώστε τα τελικά μας αποτελέσματα να είναι ακόμη καλύτερα. Διαφορετικά σενάρια λειτουργίας του αλγορίθμου δίνουν τη δυνατότητα για

συσχέτιση επιπέδων ασφάλειας με επίπεδα καταναλισκόμενης ενέργειας του συστήματος χαμηλών πόρων.

Συμπεράσματα και μελλοντικές προεκτάσεις της εργασίας αυτής παρουσιάζονται στο Κεφάλαιο 7.

ΚΕΦΑΛΑΙΟ 2. Βασικά στοιχεία κρυπτογραφίας

Ο βασικός στόχος του Κεφαλαίου 2 είναι να εισάγει τον αναγνώστη στις βασικές αρχές της επιστήμης της κρυπτογραφίας. Αναφέρονται όλα τα βασικά στοιχεία που είναι απαραίτητα στο να διασαφηνιστούν έννοιες και αρχές σχετικά με την κρυπτογραφία. Διευκρινίζονται θέματα όπως κρυπτογραφία και μαθηματικές συναρτήσεις, ασφάλεια πληροφορίας, κατηγοριοποίηση των αλγορίθμων, βασικές κρυπτογραφικές πράξεις, αλγόριθμοι και πρωτόκολλα, η γνώση των παραπάνω αποτελεί τη βάση για το σχεδιασμό ασφαλών συστημάτων.

2.1.Εισαγωγή

Η κρυπτογραφία (11) (12), έχει μια μακρόχρονη ιστορία. Το πιο ολοκληρωμένο βιβλίο που παρουσιάζει μια ιστορική αναδρομή στην κρυπτογραφία, είναι το «*The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*» (13). Το βιβλίο αυτό αναφέρεται από την αρχή της ιστορίας της Κρυπτογραφίας, 4000 χρόνια πριν και τη χρήση της από του Αιγυπτίους, μέχρι τον 20^ο αιώνα, όπου έπαιξε σημαντικό ρόλο και στους δύο παγκόσμιους πολέμους. Παρουσιάζει τις ιστορικές στιγμές όπου η κρυπτογραφία έπαιξε πρωταρχικό ρόλο στις στρατιωτικές επιχειρήσεις, στη διπλωματία και γενικότερα στις κυβερνήσεις και αποτέλεσε εργαλείο στην προστασία εθνικών μυστικών και στρατηγικών.

Η καθιέρωση των υπολογιστών και των συστημάτων τηλεπικοινωνιών που έλαβε χώρα ειδικά στη δεκαετία του 60, έφερε την ανάγκη για προστασία της μετάδοσης δεδομένων με σκοπό να προστατεύεται η ψηφιακή πληροφορία και να παρέχονται ασφαλείς ψηφιακές υπηρεσίες. Ο Feistel (14) ξεκίνησε την έρευνα στην IBM στις αρχές του 1970 με σκοπό να φτιάξει έναν ασφαλή αλγόριθμο κρυπτογραφίας. Προϊόν της έρευνάς του ήταν ο αλγόριθμος DES (10) όπου έγινε πρότυπο το 1977 (U.S. Federal Information Processing Standard), και χρησιμοποιείται ακόμη και σήμερα αποτελώντας το πιο γνωστό κρυπτογραφικό μηχανισμό στη σύγχρονη ιστορία. Τα τελευταία χρόνια η χρήση του αλγορίθμου DES έχει περιοριστεί από τον αντικαταστάτη του AES (14).

Από τότε η επιστήμη της κρυπτογραφίας έχει κάνει μεγάλα βήματα με σημαντικά ερευνητικά γεγονότα όπως η εργασία των Diffie και Hellman (16) το 1976 όπου θεμελίωσε την κρυπτογραφία δημοσίου κλειδιού, όπου στηρίχτηκαν οι Rivest, Shamir και Adleman (17) ώστε να δημιουργηθεί το πρότυπο κρυπτογράφησης δημοσίου κλειδιού RSA. Τα τελευταία χρόνια η δυνατότητα ολοκλήρωσης των αλγορίθμων με την ανάπτυξη της επιστήμης της ηλεκτρονικής καθώς και η ανάπτυξη των ασύρματων επικοινωνιών έδωσε νέα πνοή στην εξέλιξη της κρυπτογραφίας και γενικότερα στην εξέλιξη της ασφάλειας των συστημάτων.

2.2.Ασφάλεια πληροφορίας και κρυπτογραφία

Με σκοπό την εισαγωγή στην κρυπτογραφία, η κατανόηση θεμάτων σχετικά με την ασφάλεια πληροφορίας είναι αναγκαία. Η ασφάλεια πληροφορίας σχετίζεται με το σενάριο επικοινωνίας, τις απαιτήσεις και τη διαθεσιμότητα των συμβαλλόμενων

μελών σε πόρους συστήματος. Μερικές από τις βασικές έννοιες οι οποίες σχετίζονται με τη θεωρία ασφάλεια της πληροφορίας βρίσκονται στον Πίνακα 1.

Ανά τους αιώνες, ένα σύνολο πρωτοκόλλων και μηχανισμών έχει δημιουργηθεί για να διασφαλίσει την ασφάλεια της πληροφορίας, όταν μεταβιβάζεται η πληροφορία μέσω φυσικών εγγράφων. Συχνά οι στόχοι της ασφάλειας πληροφορίας δεν μπορούν να επιτευχθούν μέσω των μαθηματικών αλγορίθμων και των πρωτοκόλλων, αλλά απαιτούνται φυσικές τεχνικές και κατάλληλο νομικό πλαίσιο ώστε να επιτευχθεί το επιθυμητό αποτέλεσμα. Για παράδειγμα, η μυστικότητα των επιστολών παρέχεται από τους σφραγισμένους φακέλους που παραδίδονται από μια αποδεκτή υπηρεσία ταχυδρομείου. Η φυσική ασφάλεια του φακέλου είναι περιορισμένη και έτσι νόμοι θεσπίζονται που μετατρέπουν σε ποινικό αδίκημα το άνοιγμα της αλληλογραφίας για το οποίο κάποιος δεν εξουσιοδοτείται. Επίσης μερικές φορές η ασφάλεια επιτυγχάνεται μέσω του τρόπου της καταγραφής της πληροφορίας. Για παράδειγμα, η τύπωση νομισμάτων απαιτεί επιπρόσθετα «έξυπνα» μελάνια και υλικό για να αποτραπεί η πλαστογράφηση.

Πίνακας 1: Βασικές έννοιες στη θεωρία Ασφάλειας

Μυστικότητα ή Εμπιστευτικότητα (Privacy or confidentiality)	Μόνο οι εγκεκριμένοι χρήστες μπορούν να δουν την πληροφορία
Ακεραιότητα δεδομένων (data integrity)	Διαβεβαίωση πως η πληροφορία δεν έχει αλλαχτεί από μη εγκεκριμένους χρήστες
Πιστοποίηση Οντότητας (entity authentication or identification)	Πιστοποίηση-έγκριση μιας οντότητας από μία άλλη
Επιβεβαίωση της πηγής πληροφορίας (Message authentication)	Πιστοποίηση-έγκριση της πηγής πληροφορίας
Υπογραφή (signature)	Ένα μέσο ώστε να δεσμευτούν πληροφορίες σε μια οντότητα
Έγκριση (authorization)	Μεταβίβαση σε μια άλλη οντότητα δικαιωμάτων, του επισήμου φορέα, για να είναι ή να κάνει κάτι
Επικύρωση (validation)	Μέσο ώστε να παρασχεθεί έγκριση ή να χειριστούν τις πληροφορίες ή τους πόρους.
Έλεγχος Πρόσβασης (access control)	Έλεγχος πρόσβασης σε οντότητες που έχουν τα απαραίτητα δικαιώματα
Πιστοποίηση (certification)	Επικύρωση των πληροφοριών από μια εγκεκριμένη οντότητα
Timestamping	Καταγραφή του χρόνου της δημιουργίας ή της ύπαρξης των πληροφοριών
Μαρτυρία (witnessing)	Επαλήθευση της δημιουργίας ή της ύπαρξης των πληροφοριών από μια οντότητα εκτός από το δημιουργό της πληροφορίας
Απόδειξη επιτυχημένης αποστολής (receipt)	Απόδειξη ότι η πληροφορία έχει αποσταλεί στον προορισμό της
Επικύρωση επιτυχημένων υπηρεσιών (confirmation)	Επικύρωση ότι οι υπηρεσίες έχουν παρασχεθεί επιτυχώς
Ιδιοκτησία (ownership)	Διεργασίες ώστε να παρασχεθεί σε μια οντότητα το νόμιμο δικαίωμα να χρησιμοποιεί ή να μεταφέρει δικαιώματα σε άλλες οντότητες
Ανωνυμία (anonymity)	Διεργασίες που αποκρύπτουν την ταυτότητα μιας οντότητας που περιλαμβάνεται σε κάποια διαδικασία
Μη άρνηση (non-repudiation)	Αποτροπή άρνησης προηγούμενων πράξεων
Ανάκληση (revocation)	Ανάκληση πιστοποίησης ή έγκρισης

Ο τρόπος που οι πληροφορίες καταγράφονται δεν έχει αλλάξει εντυπωσιακά με την πάροδο του χρόνου. Ενώ η πληροφορία αποθηκευόταν σε έγγραφα, πλέον υπάρχει η δυνατότητα αποθήκευσης της πληροφορίας σε ηλεκτρονικά μέσα και μεταδίδεται μέσω τηλεπικοινωνιακών συστημάτων εκ των οποίων κάποια από αυτά μεταδίδουν πληροφορία μέσω του αέρα. Αυτό που έχει αλλάξει εντυπωσιακά είναι η δυνατότητα να αντιγραφούν ή να αλλαχτούν οι πληροφορίες. Κάποιος μπορεί να κάνει χιλιάδες ίδια αντίγραφα ενός κομματιού των πληροφοριών που αποθηκεύονται ηλεκτρονικά όπου το καθένα να είναι όμοιο με το αρχικό, κάτι που με παραδοσιακές μεθόδους θα ήταν πολύ δυσκολότερο. Αυτό που απαιτείται λοιπόν για μια κοινωνία όπου οι πληροφορίες αποθηκεύονται συνήθως και διαβιβάζονται με ηλεκτρονική μορφή είναι ένας τρόπος να εξασφαλιστεί ασφάλεια πληροφορίας που είναι ανεξάρτητη από το φυσικό μέσο ή τη μεταβίβαση του και η ασφάλεια να στηρίζεται στην ψηφιακή πληροφορία μόνο.

Ένα από τα θεμελιώδη εργαλεία-έννοιες που χρησιμοποιούνται στην ασφάλεια πληροφοριών είναι η υπογραφή. Αποτελεί δομική μονάδα και για άλλες υπηρεσίες όπως η μη άρνηση, η επικύρωση της προέλευσης δεδομένων, πιστοποίηση οντότητας, και η μαρτυρία. Μαθαίνοντας κάποιος να γράφει, έπειτα διδάσκεται πώς να παραγάγει μια χειρόγραφη υπογραφή με σκοπό τον προσδιορισμό της ταυτότητάς του. Με τις ηλεκτρονικές πληροφορίες η έννοια μιας υπογραφής πρέπει να επαναπροσδιοριστεί και δεν μπορεί απλά να είναι κάτι μοναδικό για τον υπογράφοντα και ανεξάρτητο των υπογεγραμμένων πληροφοριών.

Επίσης ανάλογοι μηχανισμοί των «πρωτοκόλλων εγγράφου» απαιτούνται. Αυτά τα νέα ηλεκτρονικά πρωτόκολλα είναι τουλάχιστον το ίδιο καλά αυτών που αντικαθιστούν. Υπάρχει λοιπόν μια μοναδική ευκαιρία για την κοινωνία να εισαγάγει τους νέους και αποδοτικότερους τρόπους στην ασφάλεια πληροφοριών.

Η επίτευξη ασφάλειας πληροφοριών σε μια ηλεκτρονική κοινωνία απαιτεί μια σειρά τεχνικών και νομικών διεργασιών. Δεν υπάρχει, εντούτοις, καμία εγγύηση ότι όλοι οι στόχοι ασφάλειας πληροφοριών που κρίνονται απαραίτητοι μπορούν να επιτευχθούν επαρκώς. Όλα τα τεχνικά μέσα παρέχονται μέσω του συστήματος κρυπτογραφίας.

Ορισμός 2.1: Η κρυπτογραφία (Cryptography) είναι η επιστήμη των μαθηματικών τεχνικών που σχετίζονται με την ασφάλεια της πληροφορίας, όπως εμπιστευτικότητα, ακεραιότητα δεδομένων, επικύρωση οντότητας, και επικύρωση προέλευσης στοιχείων. Η κρυπτογραφία δεν είναι μόνο οι τρόποι που συντελούν στην ασφάλεια πληροφορίας, αλλά περισσότερο ένα σύνολο τεχνικών.

Οι πιο βασικές έννοιες στην επιστήμη της κρυπτογραφίας είναι οι παρακάτω:

1. **Εμπιστευτικότητα (Confidentiality)** είναι η υπηρεσία που χρησιμοποιείται για να προφυλάσσεται το περιεχόμενο της πληροφορίας από τους μη εξουσιοδοτημένους. Η Μυστικότητα (Secrecy) αποτελεί όρο συνώνυμο με την εμπιστευτικότητα.
2. Η **Ακεραιότητα δεδομένων (Data integrity)** είναι η υπηρεσία η οποία διευθετεί την μη εξουσιοδοτημένη αλλαγή των δεδομένων. Για να διασφαλιστεί η Ακεραιότητα δεδομένων, κάποιος πρέπει να έχει τη δυνατότητα να ανιχνεύει την αλλαγή δεδομένων από μη εξουσιοδοτημένα μέρη. Η αλλαγή των δεδομένων περιλαμβάνει ενέργειες όπως εισαγωγή, αφαίρεση-διαγραφή και αντικατάσταση.

3. **Η Πιστοποίηση (Authentication)** είναι η υπηρεσία που σχετίζεται με την αναγνώριση-ταυτοποίηση. Τα δύο μέρη που θέλουν να επικοινωνήσουν πρέπει να αναγνωρίσουν το ένα το άλλο. Αυτή η διεργασία εφαρμόζεται και στις δύο οντότητες που θέλουν να επικοινωνήσουν αλλά και στην πληροφορία. Για την πληροφορία η οποία μεταφέρεται μέσω ενός καναλιού πρέπει να επικυρώνεται η προέλευσή της, η ημερομηνία δημιουργίας, το περιεχόμενο κτλ.. Γι αυτούς τους λόγους η Πιστοποίηση χωρίζεται σε δύο βασικές κλάσεις: Πιστοποίηση οντότητας και Πιστοποίηση προέλευσης δεδομένων. Η Πιστοποίηση προέλευσης δεδομένων μπορεί να παρέχει την Ακεραιότητα δεδομένων .
4. **Μη Άρνηση (Non-repudiation)** είναι η υπηρεσία που αποτρέπει μία οντότητα από το να αρνηθεί ότι διέπραξε προηγούμενες συμφωνίες ή ενέργειες. Όταν διαφωνίες προκύπτουν λόγω της άρνησης μιας οντότητας ότι ορισμένες ενέργειες έχουν πραγματοποιηθεί, είναι απαραίτητοι μηχανισμοί ώστε να επιλύονται τέτοια προβλήματα. Για παράδειγμα, μια οντότητα μπορεί να εγκρίνει κάποια αγορά από μια άλλη οντότητα και να αρνηθεί αργότερα σχετικά με αυτήν την ενέργεια. Επομένως μια διαδικασία που περιλαμβάνει έναν εμπιστευμένο τρίτο (third party) απαιτείται για να επιλύσει τη διαφωνία.

Ένας θεμελιώδης στόχος της επιστήμης κρυπτογραφίας είναι να εξεταστούν επαρκώς αυτές οι τέσσερις περιοχές και στη θεωρία και στην πράξη. Στην Εικόνα 1 παρέχεται μια σχηματική λίστα των βασικών λειτουργιών-μηχανισμών της ασφάλειας πληροφορίας και πώς σχετίζονται. Πολλοί από αυτούς θα εισαχθούν εν συντομία σε αυτό το Κεφάλαιο.

Εικόνα 1: Η συσχέτιση των βασικών μηχανισμών ασφάλειας

2.3.Συναρτήσεις και κρυπτογραφία

Ένα από τα πιο βασικά θέματα στην κρυπτογραφία είναι η έννοια της συνάρτησης. Η συνάρτηση επίσης αναφέρεται και ως αντιστοίχιση (mapping) ή μετασχηματισμός (transformation).

2.3.1. Συναρτήσεις (1-1, ενός δρόμου (one-way), trapdoor one way)

Ένα σύνολο A (A set) αποτελείται από διαφορετικά αντικείμενα τα οποία καλούνται στοιχεία του συνόλου. Για παράδειγμα, ένα σύνολο X μπορεί να αποτελείται από τα στοιχεία a, b, c , και αυτό συμβολίζεται ως $X = \{a, b, c\}$.

Ορισμός 2.2: Μια συνάρτηση ορίζεται από δύο σύνολα X και Y και ένα κανόνα f ο οποίος αντιστοιχεί κάθε στοιχείο του X ακριβώς με ένα στοιχείο του Y . Το σύνολο X ονομάζεται ο χώρος που ορίζεται η συνάρτηση (domain) και το Y το πεδίο τιμών (codomain). Αν το x είναι ένα στοιχείο του X (δηλαδή $x \in X$) η εικόνα του x είναι το στοιχείο του Y όπου ο κανόνας f σχετίζει με το x . Η εικόνα y του x συμβολίζεται με $y = f(x)$. Ο επίσημος συμβολισμός μιας συνάρτησης από το σύνολο του X στο σύνολο Y είναι $f: X \rightarrow Y$. Αν $y \in Y$ τότε η εικόνα του (reimage) είναι ένα στοιχείο $x \in X$ για το οποίο ισχύει $f(x)=y$. Το σύνολο των στοιχείων στο Y για τα οποία τουλάχιστον υπάρχει μια εικόνα (reimage) καλούνται εικόνα του f και συμβολίζονται με $Im(f)$.

Παρατηρώντας το σχηματικό που φαίνεται στην Εικόνα 2 βλέπουμε πως για κάθε στοιχείο του domain X υπάρχει ακριβώς μια αντιστοίχιση (βέλος) που κατευθύνεται προς το Y . Κάθε στοιχείο του codomain Y μπορεί να έχει οποιοδήποτε αριθμό αντιστοιχίσεων από το σύνολο X περιλαμβάνοντας μηδενικές αντιστοιχίσεις. Συχνά μόνο το domain X και ο κανόνας f δίνονται και το codomain υποτίθεται πως είναι η εικόνα του f .

Εικόνα 2: Η συνάρτηση f από το σύνολο X σε τρία στοιχεία του συνόλου Y .

Παράδειγμα 2.1: Έστω τα σύνολα $X=\{a, b, c\}$, $Y=\{1, 2, 3, 4\}$ και ο κανόνας f από το X στο Y ορίζεται ως εξής: $f(a) = 2$, $f(b) = 4$, $f(c) = 1$. Η Εικόνα 2 δείχνει το σχηματικό των συνόλων και του κανόνα f . Η reimage του στοιχείου 2 είναι το a . Η image του f είναι $\{1, 2, 4\}$.

Ορισμός 2.3: Μια συνάρτηση (ή ένας μετασχηματισμός) είναι 1 – 1 (ένα προς ένα) αν κάθε στοιχείο του codomain Y είναι η εικόνα για το πολύ ένα στοιχείο του domain X .

Ορισμός 2.4: Μια συνάρτηση (ή ένας μετασχηματισμός) είναι *onto* αν κάθε στοιχείο του *codomain* Y είναι η εικόνα για τουλάχιστον ένα στοιχείο *domain*, $Im(f) = Y$.

Ορισμός 2.5: Αν μια συνάρτηση είναι ένα προς ένα και *onto*, τότε καλείται *αντίστροφη* (bijection).

Ορισμός 2.6: Αν f είναι αντίστροφη από X στο Y τότε ο απλούστερος τρόπος για να ορίσουμε μία αντιστροφή από το Y στο X είναι ο εξής: για κάθε $y \in Y$ ορίζουμε $g(y) = x$ όπου $x \in X$ και $f(x) = y$. Αυτή η συνάρτηση g η οποία προκύπτει από την f καλείται *αντίστροφη συνάρτηση της f* και συμβολίζεται ως εξής: $g = f^{-1}$

Παράδειγμα 2.2: Έστω $X = \{a, b, c, d\}$ και $Y = \{1, 2, 3, 4, 5\}$ τότε θεωρώντας την συνάρτηση f η οποία φαίνεται στην Εικόνα 3 βλέπουμε πως η f είναι αντίστροφη, και η αντιστροφή της g προκύπτει αντιστρέφοντας τις αντιστοιχίες.

Εικόνα 3: Η αντίστροφη συνάρτηση f και η αντιστροφή της $g = f^{-1}$.

Επιπλέον αν η f είναι αντίστροφη, τότε και η f^{-1} είναι. Στην κρυπτογραφία οι αντιστροφες συναρτήσεις χρησιμοποιούνται σαν εργαλεία για κρυπτογράφηση μηνυμάτων και οι αντιστροφικοί μετασχηματισμοί χρησιμοποιούνται για την αποκρυπτογράφηση. Με αυτό τον τρόπο επιτυγχάνεται η αποκρυπτογράφηση σε ένα μοναδικό μήνυμα.

Υπάρχουν αρκετοί τύποι συναρτήσεων οι οποίοι παίζουν σημαντικό ρόλο στην κρυπτογραφία. Ένας γνωστός τύπος συναρτήσεων είναι οι ενός δρόμου συναρτήσεις (one-way functions).

Ορισμός 2.7: Μια συνάρτηση f αντιστοιχεί τα στοιχεία από ένα σύνολο X σε ένα σύνολο Y , καλείται *ενός δρόμου* (one-way συνάρτηση) αν η $f(x)$ είναι εύκολο να υπολογιστεί για όλα τα $x \in X$, αλλά για όλα τα στοιχεία $y \in Im(f)$ είναι «υπολογιστικά αδύνατο» να βρεθεί ένα $x \in X$ έτσι ώστε $f(x) = y$.

Παράδειγμα 2.3: Έστω $X = \{1, 2, 3, \dots, 16\}$ και $f(x) = r_x$ για όλα τα $x \in X$ όπου r_x είναι το υπόλοιπο της διαίρεσης του 3^x με το 17.

Πίνακας 2: Παράδειγμα συνάρτησης one-way

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Δίνοντάς μας έναν αριθμό μεταξύ 1 και 16, είναι εύκολο να βρεθεί η εικόνα του αριθμού αυτού σύμφωνα με την συνάρτηση f . Όμως αν μας δώσουν τον αριθμό 7, χωρίς τη βοήθεια του Πίνακα 1, είναι δυσκολότερο να βρούμε το x ώστε $f(x) = 7$.

Ας προσέξουμε πως το παραπάνω παράδειγμα χρησιμοποιεί πολύ μικρούς αριθμούς και το σημαντικό σημείο εδώ είναι ότι υπάρχει διαφορά στην επεξεργασία που χρειάζεται ώστε να υπολογιστεί η $f(x)$ και στο να υπολογιστεί το x αν γνωρίζουμε την $f(x)$.

Παράδειγμα 2.4: Ένας πρώτος αριθμός είναι κάθε θετικός ακέραιος ο οποίος είναι μεγαλύτερος από 1 και οι μοναδικοί θετικοί και ακέραιοι διαιρέτες του είναι το 1 και ο εαυτός του. Επιλέγουμε τους πρώτους $p=48611$, $q=53933$ όπου $n = p \cdot q = 2624653723$, και έστω $X = \{1, 2, 3, \dots, n-1\}$. Έστω η συνάρτηση f με X και $f(x) = r_x$ για κάθε $x \in X$, όπου r_x είναι το υπόλοιπο όταν το x^3 διαιρείται με το n . Για παράδειγμα, $f(2489991) = 1981394214$, εφόσον $2489991^3 = 5881949859 \cdot n + 1981394214$. Υπολογίζοντας την $f(x)$ είναι σχετικά εύκολο, αλλά η αντίστροφη διαδικασία είναι πολύ πιο δύσκολη, δηλαδή με δεδομένο το υπόλοιπο να βρεθεί η αρχική τιμή του x .

Ορισμός 2.8: Μία trapdoor one-way συνάρτηση, είναι μία ενός δρόμου συνάρτηση, $f: X \rightarrow Y$, με μια επιπρόσθετη ιδιότητα, με ορισμένη πληροφορία (η οποία καλείται trapdoor πληροφορία) είναι εύκολο να βρεθεί για κάθε $y \in \text{Im}(f)$, το $x \in X$, έτσι ώστε $f(x) = y$.

2.3.2. Αναδιατάξεις (Permutations)

Ορισμός 2.9: Έστω S είναι ένα πεπερασμένο σύνολο στοιχείων. Η αναδιάταξη p στο σύνολο S είναι η αντιστροφή της και είναι από το σύνολο S στο S .

Παράδειγμα 2.5: Έστω $S = \{1, 2, 3, 4, 5\}$. Η αναδιάταξη $p: S \rightarrow S$ ορίζεται ως εξής: $p(1)=3$, $p(2)=5$, $p(3)=4$, $p(4)=2$, $p(5)=1$.

Εφόσον οι αναδιατάξεις είναι αντίστροφες, έχουν αντίστροφες συναρτήσεις οι οποίες μπορούν να βρεθούν εύκολα.

2.3.3. Involutions

Οι involutions συναρτήσεις έχουν την ιδιότητα ότι η αντίστροφή του είναι ίδια με την αρχική συνάρτηση. Δηλαδή $f = f^{-1}$.

Ορισμός 2.10: Έστω S ένα σύνολο πεπερασμένων στοιχείων και έστω f η συνάρτηση από S σε S . Η συνάρτηση f καλείται involution αν $f = f^{-1}$. Διαφορετικά $f(f(x)) = x$, για κάθε $x \in X$.

2.4. Βασική ορολογία για την κρυπτογραφία

2.4.1. Κρυπτογράφηση: Domains και Co domains

- Το $\mathcal{A}$ δηλώνει ένα σύνολο πεπερασμένων στοιχείων όπου είναι το αλφάβητο. Για παράδειγμα, $A = \{0,1\}$, είναι το δυαδικό αλφάβητο. Οποιοδήποτε βέβαια αλφάβητο όμως μπορεί να κωδικοποιηθεί σε δυαδικό αλφάβητο.
- Το $\mathcal{M}$ δηλώνει το διάστημα του μηνύματος (message space) και κάθε στοιχείο του $\mathcal{M}$ ονομάζεται αρχικό κείμενο (plaintext). Προκύπτει από όλους τους δυνατούς συνδυασμούς των στοιχείων της αλφαβήτου, για δεδομένο αριθμό συμβόλων.
- Το $\mathcal{C}$ δηλώνει το διάστημα του κρυπτογραφήματος (ciphertext space). Ένα στοιχείο του $\mathcal{C}$ ονομάζεται κρυπτογραφημένο μήνυμα (ciphertext).

2.4.2. Μετασχηματισμοί κρυπτογράφησης και αποκρυπτογράφησης

- Το $\mathcal{K}$ συμβολίζει ένα σύνολο αποκαλούμενο διάστημα κλειδιών (key space). Ένα στοιχείο του $\mathcal{K}$ καλείται κλειδί.
- Κάθε στοιχείο $e \in K$ ορίζει μοναδικά μια bijection από το $\mathcal{M}$ στο $\mathcal{C}$, η οποία συμβολίζεται E_e . Η E_e καλείται συνάρτηση ή μετασχηματισμός κρυπτογράφησης.
- Για κάθε στοιχείο $d \in K$, το D_d δηλώνει το μετασχηματισμό από το $\mathcal{C}$ στο $\mathcal{M}$ και ονομάζεται αποκρυπτογράφηση ή μετασχηματισμός αποκρυπτογράφησης.
- Η διαδικασία εφαρμογής του μετασχηματισμού E_e στο μήνυμα $m \in \mathcal{M}$, συνήθως αναφέρεται ως κρυπτογράφηση του m .
- Η διαδικασία εφαρμογής του μετασχηματισμού D_d στο κρυπτογραφημένο μήνυμα c , συνήθως αναφέρεται ως αποκρυπτογράφηση του c .
- Ένα σχήμα κρυπτογράφησης αποτελείται από ένα σύνολο $\{E_e : e \in K\}$ κρυπτογραφικών μετασχηματισμών και ένα αντίστοιχο σύνολο $\{D_d : d \in K\}$ μετασχηματισμών αποκρυπτογράφησης με την ιδιότητα ότι για κάθε $e \in K$ υπάρχει ένα μοναδικό κλειδί $d \in K$ έτσι ώστε $D_d = E_e^{-1}$, όπου $D_d(E_e(m)) = m$ για όλα τα $m \in \mathcal{M}$. Ένα σχήμα κρυπτογράφησης πολλές φορές καλείται και cipher.
- Τα κλειδιά e και d ορίζονται ως ζεύγος κλειδιών και μερικές φορές συμβολίζονται ως (e, d) . Τα e και d μπορεί να είναι ίδια.
- Η κατασκευή ενός σχήματος κρυπτογράφησης απαιτεί την επιλογή του διαστήματος μηνύματος $\mathcal{M}$, του διαστήματος κρυπτογραφήματος $\mathcal{C}$, του διαστήματος κλειδιών $\mathcal{K}$ και την επιλογή μετασχηματισμών E_e καθώς και αντίστροφων μετασχηματισμών D_d .

2.4.3. Επιτυγχάνοντας εμπιστευτικότητα

Για να επιτευχθεί εμπιστευτικότητα ένα σχήμα κρυπτογράφησης μπορεί να αναπτυχθεί ως εξής: Έστω δύο μέρη, η Alice και ο Bob, που πρέπει αρχικά να επιλέξουν μυστικά ένα ζεύγος κλειδιών (e, d) . Αμέσως μετά έστω πως η Alice επιθυμεί να στείλει ένα μήνυμα $m \in \mathcal{M}$ στο Bob, και υπολογίζει $c = E_e(m)$ και το στέλνει στο Bob. Από τη μεριά του ο Bob υπολογίζει $D_d(c) = m$ και επομένως μπορεί και διαβάζει το καθαρό μήνυμα m .

Γιατί όμως τα κλειδιά είναι απαραίτητα; (Γιατί δηλαδή να μη θεωρούσαμε μόνο μια συνάρτηση κρυπτογράφησης και την αντίστοιχη συνάρτηση αποκρυπτογράφησης;) Έχοντας μετασχηματισμούς που είναι πολύ παρόμοιοι αλλά χαρακτηρισμένοι από τα κλειδιά σημαίνει ότι εάν κάποιος ιδιαίτερος μετασχηματισμός αποκρυπτογράφησης αποκαλύπτεται, έπειτα κάποιος δεν είναι απαραίτητο να ξανασχεδιάσει όλο τον μετασχηματισμό αλλά απλά αλλάζει το κλειδί. Αποτελεί «υγιής» κρυπτογραφική πρακτική να αλλάγεται το κλειδί (κρυπτογράφηση/μετασχηματισμός αποκρυπτογράφησης) συχνά. Σαν φυσικό ανάλογο, ας εξετάσουμε μια επανατοποθετήσιμη κλειδαριά συνδυασμών. Η δομή της κλειδαριάς είναι διαθέσιμη σε καθέναν που επιθυμεί να αγοράσει αλλά ο συνδυασμός επιλέγεται και τίθεται από τον ιδιοκτήτη. Εάν ο ιδιοκτήτης υποψιάζεται ότι ο συνδυασμός έχει αποκαλυφθεί μπορεί εύκολα να το επαναριθμήσει χωρίς αντικατάσταση του φυσικού μηχανισμού.

Παράδειγμα 2.5: Έστω $\mathcal{M}=\{m1, m2, m3\}$ και $\mathcal{C}=\{c1, c2, c3\}$. Υπάρχουν $3!=6$ μετασχηματισμοί από το $\mathcal{M}$ στο $\mathcal{C}$. Το διάστημα των κλειδιών περιλαμβάνει $K=\{1, 2, 3, 4, 5, 6\}$ αποτελείται από 6 στοιχεία και κάθε στοιχείο ορίζει ένα διαφορετικό μετασχηματισμό. Η Εικόνα 4 παρουσιάζει 6 συναρτήσεις κρυπτογραφίας οι οποίες συμβολίζονται με $E_i, 1 \leq i \leq 6$. Έστω πως η Alice και ο Bob συμφωνούν στο μετασχηματισμό E_1 . Για να κωδικοποιηθεί το μήνυμα λοιπόν $m1$, η Alice υπολογίζει $E_1(m1) = c_3$ και στέλνει το c_3 στο Bob. Ο Bob αποκωδικοποιεί το c_3 βάσει του E_1 και παρατηρεί πως το αρχικό κείμενο ήταν το $m1$.

Εικόνα 4: Σχηματικό απλού κρυπτογραφικού συστήματος

Όταν το $\mathcal{M}$ είναι ένα μικρό σύνολο, το διάγραμμα είναι ένας απλός οπτικός τρόπος να περιγραφεί η αντιστοίχιση και οι μετασχηματισμοί. Σε αντίθετη περίπτωση όμως, και για τους ισχύοντες κρυπτογραφικούς αλγόριθμους, μόνο με χρήση μαθηματικών σχέσεων μπορεί να παρασταθούν οι μετασχηματισμοί.

2.4.4. Τα μέρη της επικοινωνίας

Παρατηρώντας την Εικόνα 5 μπορούμε να ορίσουμε την παρακάτω ορολογία.

Εικόνα 5: Σχηματικό επικοινωνίας δύο συμβαλλόμενων μελών χρησιμοποιώντας κρυπτογράφηση

- Μια οντότητα ή ένα συμβαλλόμενο μέρος (entity or party) είναι κάποιος που μεταδίδει, ή λαμβάνει, ή διαχειρίζεται τις πληροφορίες. Η Alice και ο Bob είναι οι οντότητες όπως αναφέρθηκε πριν. Μια οντότητα μπορεί να είναι ένα πρόσωπο, ένα τερματικό υπολογιστών, κ.λπ. .
- Ο αποστολέας (sender) είναι η οντότητα σε μια επικοινωνία δύο μερών και αποτελεί την επίσημη πηγή αποστολής πληροφορίας. Στην Εικόνα 5, ο αποστολέας είναι η Alice.
- Ο δέκτης (receiver) είναι η οντότητα σε μια επικοινωνία δύο μερών που αποτελεί τον επίσημο παραλήπτη πληροφορίας. Στην Εικόνα 5, ο δέκτης είναι ο Bob.
- Ο εισβολέας (adversary) είναι η οντότητα σε μια επικοινωνία δύο μερών (two-party) που δεν είναι ούτε ο αποστολέας ούτε δέκτης, και που προσπαθεί να παρακάμψει την υπηρεσία ασφάλειας πληροφοριών που παρέχεται μεταξύ του αποστολέα και του δέκτη. Διάφορα άλλα ονόματα που είναι συνώνυμα με τον εισβολέα όπως ο εχθρός, ο επιτιθέμενος, ο αντίπαλος, ο ωτακουστής και ο παρείσακτος χρησιμοποιούνται. Ο εισβολέας προσπαθεί συχνά να διαδραματίσει το ρόλο είτε του νόμιμου αποστολέα είτε του νόμιμου δέκτη.

2.4.5. Τα Κανάλια Επικοινωνίας

Η διαφορά μεταξύ ενός φυσικά ασφαλούς καναλιού και ενός ασφαλούς καναλιού είναι πως το ασφαλές κανάλι μπορεί να προστατευτεί από φυσικές ή κρυπτογραφικές τεχνικές εισβολής. Ορισμένα κανάλια υποτίθεται ότι είναι φυσικά ασφαλή και περιλαμβάνουν τους έμπιστους μεταφορείς πληροφορίας, προσωπική επαφή μεταξύ των επικοινωνούντων συμβαλλόμενων μερών, και μια αφιερωμένη σύνδεση επικοινωνίας. Αναλυτικότερα:

- Το κανάλι (channel) είναι το μέσο μετάδοσης πληροφορίας από μια οντότητα σε άλλη.

- Ένα φυσικά ασφαλές κανάλι (*physically secure channel*) ή το ασφαλές κανάλι (*secure channel*) είναι το κανάλι που δεν είναι φυσικά προσιτό στον εισβολέα.
- Ένα μη ασφαλές κανάλι (*unsecured channel*) είναι το κανάλι όπου εκτός από τα συμβαλλόμενα μέρη και εκτός από εκείνους για τους οποίους οι πληροφορίες προορίζονται, μπορούν και άλλοι να διαγράψουν, να παρεμβληθούν, ή να διαβάσουν.
- Ένα (*secured channel*) ασφαλές κανάλι είναι το κανάλι από το οποίο ο εισβολέας δεν έχει τη δυνατότητα να παραγγείλει, να διαγράψει, να παρεμβάλει, ή να διαβάσει.

2.4.6. Θεωρία Ασφάλειας

Μια θεμελιώδης προϋπόθεση στο σύστημα κρυπτογραφίας είναι ότι τα σύνολα $\mathcal{M}$, $\mathcal{C}$, $\mathcal{K} \{E_e: e \in K\}$, $\{D_d: d \in K\}$ είναι γνωστά σε όλους. Όταν δύο συμβαλλόμενα μέρη επιθυμούν να επικοινωνήσουν με ασφάλεια και να χρησιμοποιήσουν ένα σύστημα κρυπτογράφησης, το μόνο πράγμα που κρατούν μυστικό είναι το ζευγάρι μυστικών κλειδιών $\{e, d\}$. Θα μπορούσε κάποιος να κερδίσει πρόσθετη ασφάλεια με το να διαφυλάξει μυστικό το μετασχηματισμό-αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης αλλά σε καμία περίπτωση δεν πρέπει να βασίζεται την ασφάλεια του ολόκληρου συστήματος σε αυτήν την προσέγγιση.

Ορισμός 2.11: Ένα σχέδιο κρυπτογράφησης λέγεται ότι είναι εύθραυστο (*breakable*) εάν ένας τρίτος, χωρίς προγενέστερη γνώση του ζευγαριού κλειδιών $\{e, d\}$, μπορεί συστηματικά να ανακτήσει καθαρό κείμενο από το αντίστοιχο κρυπτογράφημα μέσα σε κάποιο κατάλληλο χρονικό διάστημα.

Ένα κατάλληλο χρονικό διάστημα είναι συνάρτηση της διάρκειας ζωής όπου τα στοιχεία πρέπει να είναι προστατευμένα. Για παράδειγμα, μια εντολή για να αγοραστεί μια συγκεκριμένη μετοχή, πρέπει να κρατηθεί μυστική για μερικά λεπτά ενώ τα κρατικά μυστικά μπορεί να πρέπει να παραμείνουν εμπιστευτικά για μεγάλο χρονικό διάστημα.

Ένα σχέδιο κρυπτογράφησης μπορεί να «σπάσει» με να δοκιμαστούν όλα τα πιθανά κλειδιά ώστε να βρεθεί ποιο ζεύγος κλειδιών τα επικοινωνούντα συμβαλλόμενα μέρη χρησιμοποιούν (ο αλγόριθμος κρυπτογράφησης είναι γνωστός). Αυτό καλείται εξαντλητική αναζήτηση (*exhaustive search*) του διαστήματος κλειδιών. Ακολουθεί έπειτα ότι ο αριθμός κλειδιών (δηλ., το μέγεθος του διαστήματος κλειδιών) πρέπει να είναι αρκετά μεγάλος ώστε να καταστήσει αυτή την προσέγγιση υπολογιστικά ανέφικτη. Ο στόχος λοιπόν του σχεδιαστή ενός συστήματος κρυπτογράφησης είναι η τεχνική αυτή να είναι η καλύτερη προσέγγιση για να σπάσει το σύστημα.

Συχνά αναφέρονται στη βιβλιογραφία οι αναγκαίες συνθήκες του Κίρκοφ (*Kerckhoffs' desiderata*), ένα σύνολο απαιτήσεων για τα συστήματα κρυπτογραφίας. Παρακάτω φαίνεται η λίστα με τις συνθήκες:

- ο αλγόριθμος κρυπτογράφησης πρέπει να είναι, εάν όχι θεωρητικά άθραυστος, άθραυστος πρακτικά
- Ο αλγόριθμος κρυπτογράφησης δεν πρέπει να απαιτηθεί να είναι μυστικός, και μπορεί να περιέλθει στα χέρια οποιουδήποτε, εφόσον είναι επίσημα δημοσιευμένος
- το κλειδί του πρέπει να είναι ανακοινώσιμο χωρίς τη βοήθεια των γραπτών σημειώσεων, και μεταβλητό ή τροποποιήσιμο.

- iv. το κρυπτογραφημένο κείμενο να μπορεί να στέλνεται με τηλεγράφο
- v. η διαδικασία πρέπει είναι φορητή στα διάφορα συστήματα
- vi. τελικά, είναι απαραίτητο, το σύστημα ασφάλειας να είναι εύχρηστο, απαιτώντας ούτε τη διανοητική πίεση ούτε τη γνώση μιας σειράς κανόνων

Ο κατάλογος απαιτήσεων αρθρώθηκε το 1883 και, για το μεγαλύτερο μέρος, παραμένει επίκαιρος σήμερα. Το σημείο ii) επιτρέπει ότι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται είναι γνωστοί σε όλους και ότι η ασφάλεια του συστήματος πρέπει να στηριχτεί μόνο στο κλειδί που επιλέγεται.

Η ασφάλεια πληροφοριών είναι πολύ ευρύτερη, καλύπτοντας έννοιες όπως την επικύρωση και ακεραιότητα των στοιχείων.

- Μια υπηρεσία ασφάλειας πληροφοριών είναι μια μέθοδος για να παρέχει κάποια συγκεκριμένη πτυχή της ασφάλειας.
- Σπάζοντας μια υπηρεσία ασφάλειας πληροφοριών υπονοείται η κατάργηση της προοριζόμενης υπηρεσίας.
- Ένας παθητικός εισβολέας είναι αυτός που επιτίθεται βάσει των πληροφοριών του καναλιού.
- Ένας ενεργός εισβολέας είναι αυτός που μπορεί επίσης να διαβιβάσει, να αλλάξει, ή να διαγράψει τις πληροφορίες που διαβιβάζονται μέσω του καναλιού.
- Η κρυπτανάλυση είναι η μελέτη των μαθηματικών τεχνικών οι οποίες αποσκοπούν στο να υπερνικήσουν τις κρυπτογραφικές τεχνικές
- Η κρυπτογραφία είναι η μελέτη της κρυπτογραφίας και της κρυπτανάλυσης
- Το κρυπτογραφικό σύστημα αποτελεί ένα γενικό όρο που αναφέρεται στο σύνολο των κρυπτογραφικών δομικών στοιχείων που χρησιμοποιούνται ώστε να συγκροτηθούν αξιόπιστες υπηρεσίες ασφάλειας.

2.5.Κρυπτογραφία συμμετρικού κλειδιού

2.5.1. Γενικά για τους αλγόριθμους Block και Stream ciphers

Ορισμός 2.12: Ένα σύστημα κρυπτογράφησης που αποτελείται από τα σύνολα μετασχηματισμών κρυπτογράφησης και αποκρυπτογράφησης $\{E_e: e \in K\}$ και $\{D_d: d \in K\}$, αντίστοιχα, όπου K είναι το διάστημα κλειδιών, ονομάζεται συμμετρικού κλειδιού εάν για κάθε ζευγάρι κλειδιών κρυπτογράφησης/αποκρυπτογράφησης $\{e, d\}$ είναι υπολογιστικά «εύκολο» να καθοριστεί το d γνωρίζοντας το e , και αντίστροφα να καθοριστεί το d από το e .

Επειδή, πρακτικά $e = d$ στα περισσότερα συστήματα συμμετρικού κλειδιού κρυπτογράφησης, ο όρος συμμετρικό κλειδί, κρίνεται καταλληλότερος.

Εικόνα 6: Σχηματικό επικοινωνίας για κρυπτογράφηση συμμετρικού κλειδιού

Μια επικοινωνία δύο μερών (two-party) που χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού μπορεί να περιγραφεί από την Εικόνα 6, η οποία είναι η Εικόνα 5 με την προσθήκη του ασφαλούς καναλιού. Ένα από τα σημαντικότερα ζητήματα στα συστήματα κρυπτογράφησης συμμετρικού κλειδιού είναι να βρεθεί μια αποδοτική και ασφαλή μέθοδος για την ανταλλαγή κλειδιών, ανάμεσα στα συμβαλλόμενα μέρη. Αυτό το πρόβλημα αναφέρεται ως πρόβλημα διανομής κλειδιών.

Υποτίθεται ότι όλα τα συμβαλλόμενα μέρη μπορούν να χρησιμοποιήσουν ένα σύνολο αλγορίθμων κρυπτογράφησης/αποκρυπτογράφησης (δηλ., όλα ξέρουν το σύστημα κρυπτογράφησης). Όπως τονίστηκε οι μόνες πληροφορίες που απαιτείται να κρατηθούν μυστικές είναι το κλειδί d . Εντούτοις, στη συμμετρικού κλειδιού κρυπτογράφηση, αυτό σημαίνει ότι το κλειδί e πρέπει να κρατηθεί μυστικό, δεδομένου ότι το d μπορεί να δημιουργηθεί από το e . Στην Εικόνα 6 το κλειδί κρυπτογράφησης e μεταφέρεται από μια οντότητα σε άλλη ενώ και οι δύο μπορούν να κατασκευάσουν το κλειδί αποκρυπτογράφησης d .

Υπάρχουν δύο κατηγορίες αλγορίθμων συμμετρικού κλειδιού κρυπτογράφησης: block και stream ciphers.

Ορισμός 2.12: Ο *block cipher* αποτελεί ένα σύστημα κρυπτογράφησης όπου κωδικοποιεί το καθαρό κείμενο σε κομμάτια κρυπτογραφικού κείμενου δεδομένου μήκους t βάσει ενός αλφαβήτου A , και κρυπτογραφεί ένα τμήμα κειμένου (*block*) κάθε φορά.

2.5.2. Κρυπτογραφικοί αλγόριθμοι Ροής (Stream ciphers)

Οι κρυπτογραφικοί αλγόριθμοι ροής αποτελούν μια σημαντική κατηγορία αλγορίθμων συμμετρικού κλειδιού. Είναι, υπό μια έννοια, block ciphers όπου το πακέτο που κωδικοποιούν έχει μήκος ίσο με ένα.

Ορισμός 2.13: Έστω το K είναι το διάστημα κλειδιών για ένα σύνολο κρυπτογραφικών μετασχηματισμών. Η ακολουθία των συμβόλων $e_1 e_2 e_3 \dots e_i \in K$ καλείται *Keystream*.

Ο κρυπτογραφικός αλγόριθμος ροής εφαρμόζει απλούς κρυπτογραφικούς μηχανισμούς σύμφωνα με το κλειδί (keystream) που χρησιμοποιείται. Το keystream μπορεί να παραχθεί τυχαία ή από ένα αλγόριθμο ο οποίος το παράγει βάσει ενός αρχικού μικρού μήκους keystream (*seed*), ή από ένα seed από προηγούμενα κρυπτογραφημένα σύμβολα. Ο αλγόριθμος αυτός ονομάζεται *keystream generator*.

2.6. Ψηφιακές Υπογραφές

Μία βασική κρυπτογραφική λειτουργία, η οποία είναι θεμελιώδης στην πιστοποίηση, έγκριση και μη άρνηση είναι η ψηφιακή υπογραφή. Ο σκοπός της ψηφιακής υπογραφής είναι να παρασχεθούν μέσα σε ένα συμβαλλόμενο μέρος επικοινωνίας ώστε να δηλωθεί η ταυτότητά του σε ένα κομμάτι πληροφοριών. Η διαδικασία ψηφιακής υπογραφής συνεπάγεται κρυπτογράφηση του μηνύματος μαζί με κάποια μυστική πληροφορία σχετική με τον αποστολέα και μεταφορά μέσω μηνύματος. Ακολουθεί γενική περιγραφή:

- Έστω M το σύνολο των μηνυμάτων τα οποία μπορούν να υπογραφούν.
- Το S είναι το σύνολο των στοιχείων που καλούνται υπογραφές, και είναι δυαδικού κώδικα ακολουθίες καθορισμένου μήκους.
- Το S_A είναι ο μετασχηματισμός από το σύνολο μηνυμάτων M σε υπογραφές S , και καλείται μετασχηματισμός υπογραφής για την οντότητα A . Ο μετασχηματισμός S_A είναι μυστικός από τον A , και θα χρησιμοποιηθεί ώστε να δημιουργηθούν υπογραφές για μηνύματα του M .
- Ο V_A είναι ο μετασχηματισμός από το σύνολο $M \times S$ στο σύνολο $\{\text{αληθές}, \text{ψευδές}\}$. Το V_A καλείται επαλήθευση του μετασχηματισμού για τις υπογραφές του A , και χρησιμοποιείται και από τις άλλες οντότητες για να επιβεβαιώσουν τη δημιουργία μηνυμάτων από το A .

Ορισμός 2.15: Οι μετασχηματισμοί S_A και V_A παρέχουν ένα σύστημα ψηφιακών υπογραφών για την οντότητα A .

Παράδειγμα 2.6: Έστω $M = \{m_1, m_2, m_3\}$ και $S = \{s_1, s_2, s_3\}$. Η αριστερή πλευρά της Εικόνας 7 παρουσιάζει την συνάρτηση υπογραφής S_A που εφαρμόζεται στο σύνολο M , ενώ η δεξιά πλευρά, την αντίστοιχη συνάρτηση επιβαβαίωσης V_A .

Εικόνα 7: Η υπογραφή και επαλήθευση σε ένα σύστημα ψηφιακής υπογραφής

Η διαδικασία υπογραφής είναι η εξής: Η οντότητα A δημιουργεί μια υπογραφή από το μήνυμα $m \in M$, κάνοντας τα εξής: Υπολογίζει το $s = S_A(m)$ και μεταδίδει το ζευγάρι (m, s) . Το s καλείται η υπογραφή του μηνύματος m .

Από την άλλη γίνεται πλευρά η διαδικασία επαλήθευσης, έτσι ώστε να διαπιστωθεί πως η υπογραφή s του μηνύματος m δημιουργήθηκε από τον A, και η οντότητα B (που κάνει την επαλήθευση) εκτελεί τα παρακάτω:

Παίρνει την επαλήθευση V_a από το A, υπολογίζει $u = V_A(m, s)$, αποδέχεται ή αρνείται την υπογραφή

2.7.Συστήματα κρυπτογραφίας δημοσίου κλειδιού

Το θέμα της κρυπτογράφησης δημοσίου κλειδιού αν και φαίνεται αρχικά απλό, αποτέλεσε και αποτελεί θέμα με μεγάλη ερευνητική δραστηριότητα. Παρακάτω αναφέρουμε κάποια σημαντικά σημεία και αρχές σχετικά με την κρυπτογράφηση δημοσίου κλειδιού.

2.7.1. Κρυπτογράφηση δημοσίου κλειδιού

Ας υποθέσουμε πως $E_e: e \in K$ είναι ένα σύνολο μετασχηματισμών κρυπτογράφησης και $D_d: d \in K$ αποτελεί το σύνολο των αντιστοίχων μετασχηματισμών αποκρυπτογράφησης με K να είναι το διάστημα κλειδιών. Ας θεωρήσουμε ένα ζεύγος συσχετισμένων μετασχηματισμών κρυπτογράφησης/αποκρυπτογράφησης (E_e, D_d) και ας θεωρήσουμε πως για κάθε ζεύγος ισχύει πως είναι υπολογιστικά αδύνατο, δεδομένου ενός τυχαίου (random) κωδικοποιημένου πλαισίου (ciphertext), $c \in C$, να βρεθεί το μήνυμα $m \in M$ έτσι ώστε $E_e(m) = c$. Αυτή η ιδιότητα υπογραμμίζει πως δεδομένου του e είναι αδύνατο να υπολογιστεί το αντίστοιχο κλειδί αποκρυπτογράφησης d .

Αν θεωρήσουμε δύο συμβαλλόμενα μέρη σε ένα σενάριο επικοινωνίας μεταξύ της Alice και του Bob, όπως παρουσιάζεται στην Εικόνα 8. Ο Bob επιλέγει το ζεύγος κλειδιών (e, d) . Ο Bob αποστέλλει το κλειδί κρυπτογράφησης e (το οποίο καλείται

Δημόσιο Κλειδί) στην Alice πάνω από μη ασφαλές κανάλι και κρατά μυστικό το κλειδί αποκρυπτογράφησης d (το οποίο καλείται μυστικό κλειδί). Η Alice μπορεί να αποστείλει ένα μήνυμα m στον Bob εφαρμόζοντας το μετασχηματισμό κρυπτογράφησης και εφαρμόζοντας το μετασχηματισμό κρυπτογράφησης που ορίζεται από το δημόσιο κλειδί του Bob και $c = E_e(m)$. Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο c εφαρμόζοντας τον αντίστροφο μετασχηματισμό κρυπτογράφησης D_d που ορίζεται μοναδικά από το κλειδί d .

Εικόνα 8: Το σύστημα κρυπτογράφησης Δημοσίου Κλειδιού

ΚΕΦΑΛΑΙΟ 3. Σχεδιασμός κρυπτογραφικών συστημάτων σε υλικό

Προκειμένου οι κρυπτογραφικοί αλγόριθμοι, να σχεδιαστούν και να ολοκληρωθούν σε υλικό, για συστήματα περιορισμένων πόρων, η κατανάλωση ισχύος και το κόστος επιφάνειας, πρέπει να γίνουν οι σημαντικότεροι παράμετροι σχεδιασμού. Αυτό το κεφάλαιο παρουσιάζει κλασικές προσεγγίσεις ενσωμάτωσης κρυπτογραφικών αλγορίθμων σε συστήματα περιορισμένων πόρων, αναφέρονται οι κύριες πηγές κατανάλωσης ισχύος για τα κυκλώματα CMOS και παρουσιάζονται έπειτα μερικές μέθοδοι για το πώς μπορεί να περιοριστεί η κατανάλωση ισχύος στα διάφορα επίπεδα σχεδιασμού. Μια λεπτομερής περιγραφή των μεθοδολογιών χαμηλής κατανάλωσης ισχύος μπορεί να βρεθεί στα βιβλία (18), (9) και στην εργασία (19). Επιπλέον, τεχνικές χαμηλής κατανάλωσης ισχύος και προσεγγίσεις για συστήματα κρυπτογραφίας μπορούν να βρεθούν στις εργασίες (20), (21). Αρχικά θα δοθούν περιληπτικά κάποιες τυπικές προσεγγίσεις σε θέματα κρυπτογραφίας και χαμηλής κατανάλωσης ισχύος. Έπειτα θα αναφερθούμε στις παραμέτρους υλοποίησης του συστήματος και πως αυτές επηρεάζουν το συνολικό σύστημα. Τέλος θα αναφερθούν λεπτομερώς οι κυριότερες τεχνικές μείωσης κατανάλωσης ισχύος.

3.1 Τυπικές προσεγγίσεις σε θέματα χαμηλής κατανάλωσης ενέργειας στην κρυπτογραφία

Οι κρυπτογραφικοί αλγόριθμοι συνήθως υλοποιούνται σε λογισμικό (CPU, μικροελεγκτές, DSP), σε ASIC ή σε FPGA. Ορισμένα χαρακτηριστικά αυτών των προσεγγίσεων εμφανίζονται παρακάτω:

3.1.1. ASIC Προσέγγιση

Ιδιαίτερη έμφαση έχει δοθεί στο σχεδιασμό ASIC με χαρακτηριστικά χαμηλής κατανάλωσης ενέργειας. Ορισμένες τυπικές μέθοδοι ελάττωσης της κατανάλωσης ισχύος είναι οι εξής:

Απομόνωση ρολογιού (Clock Gating): Επιτυγχάνεται σημαντική ελάττωση στην κατανάλωση ενέργειας. Κομμάτια λογικής, τα οποία δε λειτουργούν για έναν οι περισσότερους κύκλους ρολογιού, αποκόπτονται από το σήμα ρολογιού και αδρανοποιούνται.

Ασύγχρονος σχεδιασμός: Ο σχεδιασμός ασύγχρονων συστημάτων (με σήματα χειραψίας-handshaking) περιορίζει την κατανάλωση ενέργειας και αυξάνει την απόδοση του συστήματος. Το πρόβλημα στην περίπτωση αυτή είναι η έλλειψη εργαλείων για την υποστήριξη του σχεδιασμού αυτού.

Γεννήτρια μεταβλητής τάσης: Σε συστήματα που έχουν περιθώρια για μείωση της απόδοσης υπάρχει η δυνατότητα να μειώνουμε την εξωτερική τάση. Με μείωση της εξωτερικής τάσης η κατανάλωση ενέργειας υποτετραπλασιάζεται.

Μείωση των ανεπιθύμητων φορτίσεων-εκφορτίσεων (glitches): Η μείωση των glitch δηλαδή των μη επιθυμητών φορτίσεων και εκφορτίσεων των τρανζίστορ

μπορεί να γίνει με σωστό σχεδιασμό. Συνήθως γίνονται αναδιατάξεις σε επίπεδο πυλών και επιλέγονται κατάλληλες κωδικοποιήσεις δεδομένων.

Παραλληλισμός και Διοχέτευση: Και οι δύο μέθοδοι αυξάνουν την απόδοση του συστήματος. Πολλές φορές χρησιμοποιούνται ώστε να αντισταθμίσουν την ελάττωση της απόδοσης εξαιτίας της εφαρμογής της μεθόδου της μείωσης της εξωτερικής τάσης.

Βελτιστοποιήσεις Συναρτήσεων: Επανασχεδιασμός συναρτήσεων με περισσότερη απόδοση στο θέμα της κατανάλωσης ισχύος.

3.1.2. FPGA Προσέγγιση

Μια μικρή κατηγορία FPGAs είναι διαθέσιμη για εφαρμογές χαμηλής κατανάλωσης ενέργειας. Υπάρχουν FPGAs όπου χρησιμοποιούν ασύγχρονες μεθόδους σχεδιασμού και gated clock τεχνικές. Γενικότερα οι σχεδιαστές των FPGAs προσπαθούν να ενσωματώσουν τεχνικές κατανάλωσης ενέργειας που εφαρμόζονται στα ASICs.

3.1.3. Προσέγγιση λογισμικού

Υπάρχει προσπάθεια για βελτιστοποίηση κρυπτογραφικών υλοποιήσεων σε λογισμικό. Επομένως «χτίζονται» επεξεργαστές που ενσωματώνουν κρυπτογραφικές πράξεις, όπως rotate, permutation κ.α. Οι πράξεις αυτές βελτιστοποιούνται από πλευράς ενέργειας και ισχύος.

3.2 Γνωστά κρυπτογραφικά σχήματα για χαμηλή κατανάλωση ισχύος

Ασύγχρονες VLSI υλοποιήσεις των κρυπτογραφικών αλγορίθμων IDEA και DES παρουσιάζονται στις εργασίες (22) και (23) αντίστοιχα. Στην εργασία (22) παρουσιάζεται μια ασύγχρονη υλοποίηση VLSI του International Data Encryption Algorithm (IDEA). Για λόγους σύγκρισης υλοποιήθηκε και η σύγχρονη έκδοση του αλγορίθμου. Χρησιμοποιήθηκε η γλώσσα περιγραφής υλικού VHDL ώστε να περιγραφεί ο αλγόριθμος. Η σύνθεση έγινε με εργαλεία της Synopsys (24). Η ασύγχρονη έκδοση του αλγορίθμου υπερείχε συγκριτικά στα θέματα της κατανάλωσης ενέργειας και απόδοσης. Στην εργασία (23) οι συγγραφείς έχουν κατασκευάσει το γνωστό αλγόριθμο κρυπτογραφίας DES σε ασύγχρονη έκδοση. Από την υλοποίηση αυτή αποδεικνύεται και εδώ ότι ο ασύγχρονος σχεδιασμός προσδίδει στο σύστημα υψηλή απόδοση.

Σύστημα ρυθμιζόμενης ασφάλειας/απόδοσης προτείνεται στην εργασία (1). Αποτελείται από δύο βασικά μπλοκ: ένα μεταβλητό σύστημα κρυπτογραφίας και ένα μετατροπέα DC/DC. Το σύστημα κρυπτογραφίας χρησιμοποιεί τον αλγόριθμο quadratic residue generator ώστε να παράγεται μια κρυπτογραφικά ασφαλή ακολουθία ψηφίων, η οποία με πράξη Xor με τα δεδομένα, παράγει ένα κρυπτογραφημένο κείμενο. Με τη βοήθεια του DC/DC μετατροπέα καθορίζεται η εξωτερική τάση καθώς η ανάγκη για παράλληλη επεξεργασία αλλάζει. Υπάρχει επίσης και ένας εξωτερικός Lookup Table ο οποίος έχει ως εισόδους τις ανάγκες για ασφάλεια και απόδοση σε μια ψηφιακή λέξη που παριστάνει την τάση. Ο DC/DC μετατροπέας μεταφράζει την ψηφιακή λέξη σε σήμα PWM το οποίο φιλτράρεται μέσω ενός LC φίλτρου ώστε να παραχθεί η εξωτερική τάση. Η τάση αυτή

δειγματοληπτείται από τον μετατροπέα ώστε να κανονικοποιηθεί. Το προτεινόμενο σχήμα υλοποίησης της εργασίας αυτής φαίνεται στην Εικόνα 9.

Εικόνα 9: Το σύστημα ρυθμιζόμενης ασφάλειας/απόδοσης

Βελτιστοποιημένες αρχιτεκτονικές ως προς την ισχύ παρουσιάζονται στην εργασία (25). Έχει αναπτυχθεί αρχιτεκτονική χαμηλής κατανάλωσης για το SybBytes/InvSubBytes δομικό στοιχείο, του αλγορίθμου AES. Προσεχτικός σχεδιασμός σε επίπεδο πυλών έχει ακολουθηθεί ώστε να εξαλειφθούν όλες οι πιθανές αιτίες κατανάλωσης ισχύος.

3.3 Βασικές κρυπτογραφικές αρχιτεκτονικές και επιπτώσεις στο συνολικό σύστημα

Είναι γνωστό στο χώρο της κρυπτογραφίας πως αυξάνοντας τον αριθμό των γύρων ενός αλγορίθμου αυξάνεται και η δυσκολία κρυπτανάλυσης του. Η αύξηση όμως των γύρων ενός αλγορίθμου κάνει το σύστημα λιγότερο αποδοτικό στην καταλυπτόμενη επιφάνεια, στο ρυθμό απόδοσης και ενέργεια. Για να λυθεί αυτό το πρόβλημα εφευρέθηκαν νέοι αλγόριθμοι που προσφέρουν ασφάλεια με μικρό αριθμό γύρων (15). Ο Πίνακας 3 παρουσιάζει διαφορετικά επίπεδα ασφάλειας για τον αλγόριθμο RC5 (26) που καθορίζονται από τον αριθμό των γύρων λειτουργίας (27). Οι αριθμοί που παρουσιάζονται στον Πίνακα 3 είναι ο αριθμός προσπαθειών που απαιτείται για το «σπάσιμο» του RC5 με διάφορες τεχνικές κρυπτανάλυσης.

Πίνακας 3: Προσπάθειες κρυπτανάλυσης RC5 κρυπτογραφικού συστήματος

Rounds	4	6	8	10	12	14	16
DC-C	2^{19}	2^{42}	2^{58}	2^{83}	2^{106}	2^{123}	>
DC-K	2^{74}	2^{86}	2^{94}	2^{106}	2^{118}	>	>
LC	2^{47}	2^{95}	2^{119}	>	>	>	>

DC_C: Differential cryptanalysis (chosen plain-text)

DC-K: Differential cryptanalysis (known plain-text),

LC: Linear Cryptanalysis (known plain-text)

Η βασική αρχιτεκτονική που χρησιμοποιείται ώστε να υλοποιηθεί ένας συμμετρικός αλγόριθμος κρυπτογραφίας είναι η μέθοδος της ανάδρασης όπως φαίνεται στην Εικόνα 10. Ένας γύρος του αλγορίθμου υλοποιείται χρησιμοποιώντας συνδυαστική

λογική, έναν καταχωρητή και έναν πολυπλέκτη. Στον πρώτο κύκλο ρολογιού το μπλοκ των δεδομένων περνά στο κύκλωμα μέσω ενός πολυπλέκτη και αποθηκεύεται στον καταχωρητή. Για κάθε επόμενο κύκλο ρολογιού, εκτελείται ένας γύρος του αλγορίθμου και το αποτέλεσμα ανατροφοδοτεί το κύκλωμα μέσω ενός πολυπλέκτη.

Εικόνα 10: Η μέθοδος ανάδρασης

Για τα συστήματα αυτά ένας τρόπος να αυξηθεί το επίπεδο ασφαλείας είναι με την αύξηση των γύρων του αλγορίθμου. Αυτό έχει τις παρακάτω συνέπειες:

- Η ισχύς του συστήματος είναι η ίδια εξαιτίας του γεγονότος πως ένας μόνος γύρος του αλγορίθμου εκτελείται κάθε φορά. Όμως η ενέργεια του συστήματος είναι ανάλογη του αριθμού των γύρων και επομένως αυξάνεται.
- Η επιφάνεια του συστήματος παραμένει προφανώς η ίδια.
- Η απόδοση του συστήματος μειώνεται αφού η διαδικασία κρυπτογράφησης /αποκρυπτογράφησης αυξάνεται.

Στην Εικόνα 11 φαίνεται η αρχιτεκτονική διοχέτευσης. Σε κάθε γύρο ένα μπλοκ εισόδου περνάει στο σύστημα και ένα κρυπτογραφημένο μπλοκ εξάγεται.

Εικόνα 11: Η μέθοδος Διοχέτευσης

Ο αριθμός ασφάλειας του συστήματος μπορεί να αυξηθεί αν ο αριθμός των εσωτερικών μπλοκ ενός γύρου αυξηθεί. Αυτό το γεγονός έχει τις παρακάτω συνέπειες

- Η ισχύς και η κατανάλωση ενέργειας είναι ανάλογη του αριθμού των εισερχόμενων μπλοκ
- Η επιφάνεια του συστήματος είναι περίπου ίση με την επιφάνεια του ενός γύρου του κρυπτογραφικού συστήματος πολλαπλασιασμένη με τον αριθμό των μπλοκ
- Η απόδοση του συστήματος με αυτή την αρχιτεκτονική αυξάνεται σημαντικά. Είναι ίση με την απόδοση του ενός γύρου του κρυπτογραφικού αλγορίθμου.

Πολλές φορές τα εισερχόμενα μπλοκ είναι περισσότερα από τα μπλοκ όπου το σύστημα μπορεί να επεξεργαστεί. Σε αυτή την περίπτωση μπορεί να αυξηθεί το πλάτος παράλληλης επεξεργασίας των ψηφίων τοποθετώντας περισσότερων του ενός συστήματος παράλληλα όπως φαίνεται στην Εικόνα 12.

Εικόνα 12: Παράλληλη Επεξεργασία Δεδομένων

Το γεγονός αυτό έχει τις παρακάτω συνέπειες:

- Η ασφάλεια του συστήματος δεν μπορεί να αυξηθεί με αυτή την τεχνική. Αν αυτό επιθυμείται μπορούμε να συνδυάσουμε την τεχνική αυτή με μία από τις παραπάνω.
- Η κατανάλωση ενέργειας και ισχύος του συστήματος αυξάνονται αφού περισσότερα συστήματα λειτουργούν στη μονάδα του χρόνου.
- Η επιφάνεια του συστήματος είναι ανάλογη του αριθμού των συστημάτων.
- Η απόδοση του συστήματος αυξάνεται γραμμικά για κάθε παράλληλο σύστημα που προστίθεται.

3.4 Πηγές κατανάλωσης ισχύος

Είναι απαραίτητη η εξέταση και η κατανόηση των πηγών κατανάλωσης ισχύος στα CMOS κυκλώματα. Η παρακάτω εξίσωση χαρακτηρίζει την κατανάλωση ισχύος (28):

$$P = \left(\frac{1}{2} C_L \cdot V_{DD}^2 + Q_{sc} \cdot V_{DD} \right) f \cdot N + I_{leak} \cdot V_{DD} \quad [3.1]$$

Ο όρος V_{DD} είναι η πηγή τάσης. Ο όρος $P_{dynamic}$ παρουσιάζει τη δυναμική κατανάλωση ισχύος. Ο δεύτερος όρος $P_{Leakage}$ παρουσιάζει τη στατική κατανάλωση ισχύος η οποία καταναλώνεται όταν το κύκλωμα είναι σε λειτουργία. Η στατική κατανάλωση ισχύος είναι ανεξάρτητη της ισχύς διακοπτικής δραστηριότητας (switching activity) και της συχνότητας, επομένως υποθέτουμε το μέγεθος αυτό σταθερό για κάθε κύκλωμα. Παρακάτω θα εξετάσουμε τους δύο βασικούς παράγοντες κατανάλωσης ισχύος αναλυτικότερα.

3.4.1. Δυναμική Ισχύς

Η δυναμική κατανάλωση ισχύος αποτελείται από δύο βασικούς παράγοντες: ισχύς διακοπτικής δραστηριότητας και ισχύς βραχυκυκλώματος (short circuit power). Και δύο αυτοί βασικοί παράγοντες εξαρτώνται από τη διακοπτική δραστηριότητα (switching activity), το οποίο εκφράζει τον αριθμό των αλλαγών στην έξοδο ανά κύκλων ρολογιού και συχνότητας λειτουργίας f .

$$P_{dynamic} = P_{sw} + P_{sc} \quad [3.2]$$

Για την ανάλυση της δυναμικής κατανάλωσης ισχύος χρησιμοποιούμε το απλό μοντέλο CMOS αντιστροφέα (Εικόνα 13), ως γενικό μοντέλο κάθε CMOS πύλης.

3.4.2. Ισχύς διακοπτικής δραστηριότητας

Η κατανάλωση που οφείλεται στην ισχύ διακοπτικής δραστηριότητας περιγράφει την ισχύ που καταναλώνεται από τη φόρτιση και την εκφόρτιση των κόμβων χωρητικότητας C_L , επομένως αναφέρεται και ως χωρητική κατανάλωση ισχύος. Για απλοποίηση υποθέτουμε πως όλες οι χωρητικότητες βρίσκονται στον κόμβο εξόδου. Σε αυτό το μοντέλο η χωρητικότητα C_L αποτελείται από δύο μέρη: C_1 και C_2 , όπως φαίνεται στην Εικόνα 13 όπου C_1 είναι η χωρητικότητα στη γείωση ενώ C_2 στην V_{DD} . Όταν η είσοδος Α βρίσκεται στο λογικό 0, τότε το n-channel τρανζίστορ Q_1 είναι ανοικτό και το p-channel τρανζίστορ Q_2 είναι κλειστό, οδηγώντας σε λογικό 1 στην

έξοδο X. Την ίδια στιγμή, η χωρητικότητα C_2 εκφορτίζεται, με βραχυκυκλωμένο το Q_2 και η χωρητικότητα C_1 φορτίζεται. Η αλλαγή στην είσοδο A από λογικό 0 σε 1 προκαλεί το κλείσιμο του Q_1 , το οποίο θα εκφορτίσει την χωρητικότητα C_1 και το Q_2 θα ανοίξει, και με τη σειρά του θα φορτίσει την χωρητικότητα C_2 . Κατά τη διάρκεια αυτής της απλής μετάβασης, ένα φορτίο $C_2 V_{DD}$ εκλύεται από την πηγή V_{DD} . Στην επόμενη αλλαγή στην είσοδο το φορτίο $C_1 V_{DD}$ φεύγει από την πηγή V_{DD} . Υποθέτοντας ότι $C_L = C_1 + C_2$, μπορούμε να πούμε πως μετά τη μεταβίβαση της τιμής της εισόδου από 0 σε 1 και πάλι «πίσω» σε 0 ο αντιστροφέας έχει απορροφήσει το φορτίο $(C_1 + C_2) V_{DD}$ από την πηγή. Επομένως για μια απλή μετάβαση στην έξοδο του μοντέλου μας, κατά μέσο όρο η τιμή του φορτίου είναι $\frac{1}{2} (C_1 + C_2) V_{DD}$. Η αντίστοιχη ισχύς που καταναλώνεται είναι $\frac{1}{2} C_L V_{DD}^2$ η οποία μας οδηγεί στην ισχύς διακοπτικής δραστηριότητας P_{SW} της εξίσωσης 3.3.

$$P_{sw} = \frac{1}{2} \cdot C_L \cdot V_{DD}^2 \cdot f \cdot N \quad [3.3]$$

Εικόνα 13: Οι χωρητικότητες εξόδου του αναστροφέα

3.4.3. Ισχύς βραχυκυκλώματος

Κατά τη διάρκεια μιας μετάβασης στην είσοδο ενός CMOS κυκλώματος, υπάρχει ένα μικρό χρονικό διάστημα όπου τα τρανζίστορ είναι και τα δύο ανοικτά προκαλώντας ένα βραχυκύκλωμα από την πηγή V_{DD} προς το έδαφος. Το αντίστοιχο ρεύμα που προκαλείται I_{SC} , ρέει όταν η τάση εισόδου είναι μεταξύ των τιμών V_T και $V_{DD} - V_T$, όπου V_T είναι η τάση κατωφλίου. Η ποσότητα του ρεύματος εξαρτάται από το συντελεστή κέρδους β (amplification) του MOS τρανζίστορ και τους χρόνους ανόδου και πτώσης της τάσης εισόδου τ . Ο Veendrick (29) υπολόγισε το ρεύμα βραχυκύκλωσης (short circuit current):

$$I_{SCmean} = \frac{1}{12} \cdot \frac{\beta}{V_{DD}} \cdot (V_{DD} - 2V_T) \cdot \frac{t}{T} \quad [3.4]$$

Και χρησιμοποιώντας το γεγονός ότι $\frac{1}{T} = f$ εκφράζεται η P_{SC} ως

$$P_{sc} = \left(\frac{1}{12} \cdot \frac{\beta}{V_{DD}} \cdot (V_{DD} - 2V_T) \cdot \tau \right) V_{DD} \cdot f \cdot N \quad [3.5]$$

Αυτή η προσέγγιση έχει βελτιωθεί από τους Turgid et al. στο (30) με μια πιο αναλυτική παρουσίαση του όρου P_{SC} . Επίσης εισήγαγαν την ιδέα να εκφράσουν την ισχύς βραχυκυκλώματος μέσω ενός φορτίου Q_{SC} που αντιστοιχίζεται στο ρεύμα βραχυκύκλωσης και έτσι οδηγούμαστε στην εξίσωση 3.6.

$$P_{SC} = \frac{1}{2} \cdot Q_{SC} \cdot V_{DD} \cdot f \cdot N \quad [3.6]$$

3.4.4. Στατική ισχύς

Η στατική κατανάλωση ισχύος ενός CMOS κυκλώματος προκαλείται από το leakage ρεύμα των τρανζίστορ και pn-επαφές. Αν πάμε πίσω στην Εικόνα 13 και υποθέσουμε πως η είσοδος είναι στο λογικό 0, γνωρίζουμε πως το n-channel τρανζίστορ Q_1 είναι ανοικτό. Η leakage ισχύς δίνεται από το leakage ρεύμα I_{0n} του συγκεκριμένου τρανζίστορ. Όταν η είσοδος βρίσκεται στο λογικό 1 τότε η leakage ισχύς προκύπτει από το leakage ρεύμα I_{0p} του p-channel τρανζίστορ Q_2 . Τα παραπάνω φαίνονται από την εξίσωση που ακολουθεί.

$$P_{Leakage} = P_S = V_{DD} \cdot \frac{I_{0n} + I_{0p}}{2} = I_{leak} \cdot V_{DD} \quad [3.7]$$

Τα ρεύματα διαρροής (leakage) αυξάνονται με την εξέλιξη της τεχνολογίας CMOS εξαιτίας της μείωσης της τάσης κατωφλίου, του μήκους του καναλιού, και του πάχους του οξειδίου του πυριτίου της επαφής-πύλης (31). Στις μελλοντικές τεχνολογίες η leakage ισχύς αναμένεται να γίνει ένας από τους βασικότερους παράγοντες της συνολικής κατανάλωσης ισχύος (32).

3.4.5. Μη αποδεκτές φορτίσεις-εκφορτίσεις (glitching)

Οι μη αποδεκτές μεταβάσεις (Glitches) ενός σήματος συμβαίνουν ύστερα από αλλαγή της εισόδου μέχρι η έξοδος να φτάσει στην τελική της τιμή. Αυτή η συμπεριφορά προκαλείται από τους διαφορετικούς χρόνους άφιξης των σημάτων εισόδου σε μια πύλη και καλούνται logic hazards. Η Εικόνα 14 παριστάνει το κύκλωμα της λογικής εξίσωσης $Q = AB + BC$ όπου φαίνεται το static-1 hazard. Όταν οι είσοδοι A και C βρίσκονται στο λογικό 1 οποιαδήποτε αλλαγή στο B θα προκαλέσει μετάβαση στο Q. Το φαινόμενο αυτό προκαλεί καθυστέρηση, και δημιουργεί ανεπιθύμητες φορτίσεις και εκφορτίσεις στην έξοδο Q. Μεγαλύτερα και πιο πολύπλοκα κυκλώματα όπως ripple carry αθροιστές, ενισχύουν αυτό το πρόβλημα. Σε τυπικά συνδυαστικά κυκλώματα το glitching αποτελεί το 10% με 40% της συνολικής δυναμικής κατανάλωσης ισχύος. Τα Hazards και επομένως glitches μπορούν να αποφευχθούν με επιπλέον κόστος υλικού.

Εικόνα 14: Οι ανεπιθύμητες φορτίσεις-εκφορτίσεις

3.5 Τεχνικές Μείωσης Μέσης Κατανάλωσης Ισχύος

Στην προηγούμενη παράγραφο αναλύθηκαν οι πηγές στατικής και δυναμικής κατανάλωσης ισχύος σε ένα CMOS ψηφιακό ολοκληρωμένο. Σε αυτή την παράγραφο θα δοθούν συνοπτικά τεχνικές για το σχεδιασμό κυκλωμάτων χαμηλής κατανάλωσης ισχύος.

Ο σημαντικότερος όρος που συνεισφέρει στην δυναμική κατανάλωση ενός κυκλώματος είναι η τάση τροφοδοσίας του, V_{dd} , μιας και αυτή εμφανίζεται με τετραγωνική έκφραση. Είναι λοιπόν προφανές ότι μείωση της τάσης τροφοδοσίας θα είχε τα πλέον θετικά αποτελέσματα όσον αφορά το σχεδιασμό κυκλωμάτων χαμηλής κατανάλωσης ισχύος. Η στρατηγική που ακολουθείται συνήθως είναι η τροποποίηση του κυκλώματος έτσι ώστε αυτό να λειτουργεί με μεγαλύτερη συχνότητα λειτουργίας, από ότι απαιτείται στο αρχικό κύκλωμα. Είναι γνωστό ότι μείωση της τάσης τροφοδοσίας έχει ως αποτέλεσμα να αυξάνει η καθυστέρηση διάδοσης των τυποποιημένων κύτταρων μιας βιβλιοθήκης. Τροποποιώντας λοιπόν το κύκλωμα έτσι ώστε να αυξηθεί η συχνότητα λειτουργίας του, και δεδομένου ότι θέλουμε σταθερή απόδοση στο κύκλωμά μας (δηλαδή θέλουμε η συχνότητα λειτουργίας του να μένει αναλλοίωτη), μπορούμε να μειώσουμε την τάση τροφοδοσίας του μέχρις ότου να επιτευχθεί η αρχική συχνότητα λειτουργίας του κυκλώματος. Πρέπει να τονιστεί ότι η δημιουργία πιο γρήγορου κυκλώματος δεν οδηγεί πάντα στην βέλτιστη λύση όσον αφορά τη μέση κατανάλωση ισχύος, αφού για την επίτευξη αυτού του στόχου (συνήθως) χρησιμοποιείται επιπλέον επιφάνεια (δηλαδή επιπλέον κύκλωμα όπως Π.χ. στην περίπτωση της παραλληλίας). Έτσι, σαν τελικό αποτέλεσμα είναι η καταναλισκόμενη ισχύς λόγω της επιπλέον χωρητικότητας να είναι μεγαλύτερη από το κέρδος λόγω της πτώσης τάσεως.

Ένας άλλος τρόπος να μειωθεί η μέση κατανάλωση της ισχύος ενός κυκλώματος, είναι να μειωθεί η ενεργός χωρητικότητα (Effective ή Switched Capacitance) που ορίζεται ως το γινόμενο της χωρητικότητας επί την πιθανότητα δραστηριότητας ενός κόμβου, $E_i \cdot C_j$. Για παράδειγμα η επιλογή της κατάλληλης οικογένειας στην οποία θα υλοποιηθεί τελικά το κύκλωμα μπορεί να οδηγήσει σε μείωση και της χωρητικότητας αλλά και της μέσης δραστηριότητας μετάβασης των κόμβων του κυκλώματος. Έχει αποδειχθεί για παράδειγμα ότι η οικογένεια CPL (Complementary Pass Transistor Logic) παρουσιάζει κατά μέσο όρο τη μικρότερη φυσική χωρητικότητα από όλες τις υπάρχουσες. Άλλες επιλογές μπορούν να γίνουν μεταξύ στατικών και δυναμικών κυκλωμάτων. Εξαιτίας της περιοδικής προφόρτισης (Precharging) των κόμβων ενός δυναμικού κυκλώματος, παρουσιάζεται μια αυξημένη δραστηριότητα μετάβασης, σε σχέση με τα αντίστοιχα στατικά κυκλώματα, αν και αυτό εξαρτάται πάρα πολύ και από τη λειτουργία που επιτελούν. Αυτή η αύξηση στις μεταβάσεις οφείλεται στο ότι σε κάθε κύκλο ρολογιού ακόμα και αν δεν γίνει μετάβαση στην έξοδο ενός κόμβου, αυτός φορτίζεται στη λογική τιμή '1' ακόμα και πρέπει να παραμείνει στο λογικό '0'. Με κατάλληλο σχεδιασμό και διαχείριση των ρολογιών (Gated Clocks), αυτό το πρόβλημα των δυναμικών κυκλωμάτων μειώνεται.

Τεχνικές μείωσης της μέσης κατανάλωσης ισχύος ενός ολοκληρωμένου κυκλώματος μπορούν να εφαρμοστούν σε όλα τα επίπεδα σχεδίασης όπως για παράδειγμα σε επίπεδο τεχνολογίας, σε επίπεδο συστήματος, σε επίπεδο αρχιτεκτονικής, σε επίπεδο πύλης και σε επίπεδο κυκλώματος. Αλλαγές σε πιο υψηλό επίπεδο έχουν ως αποτέλεσμα μεγαλύτερες μειώσεις στη μέση κατανάλωση ισχύος.

3.5.1. Βελτιστοποίηση σε Επίπεδο Τεχνολογίας (Technology Level)

Μείωση κατωφλίου αγωγής των τρανζίστορ (Threshold Reduction): Η μείωση του κατωφλίου αγωγής των N-MOS και P-MOS τρανζίστορ οδηγεί σε μείωση της τάσης τροφοδοσίας που μπορούμε να επιλέξουμε για ένα κύκλωμα. Για να γίνει αυτό δεν πρέπει η νέα τάση τροφοδοσίας να είναι μικρότερη από $V_{noise\ margin} \leq V_{optimal} \leq V_{critical}$. Η καθυστέρηση διάδοσης ενός τρανζίστορ είναι ανάλογη του λόγου $1/(V_{dd} - V_{thr})$. Έτσι αν μειωθεί το κατώφλι αγωγής του τρανζίστορ, επιτρέπεται να μειωθεί και η τάση τροφοδοσίας μέχρις ότου η καθυστέρηση διάδοσης του τρανζίστορ να είναι όσο ήταν πριν την μείωση των δύο αυτών παραμέτρων. Ένα πρόβλημα που παρουσιάζεται με τη μείωση του κατωφλίου αγωγής των τρανζίστορ όμως είναι ότι αν μειωθεί αρκετά το κατώφλι αγωγής δημιουργούνται προβλήματα λόγω των αυξημένων ρευμάτων διαρροής υποστρώματος.

Μείωση του μεγέθους των τρανζίστορ (Transistor Sizing Reduction): Όσο η τεχνολογία κατασκευής ενός ολοκληρωμένου κυκλώματος «κλιμακώνεται» (Technology Scaling) η καθυστέρηση διάδοσης των τρανζίστορ μειώνεται με αποτέλεσμα να μειωθεί η τάση τροφοδοσίας του κυκλώματος, δεδομένου ότι θέλουμε να διατηρήσουμε την αρχική συχνότητα λειτουργίας του κυκλώματος σταθερή. Επειδή το μεγαλύτερο ποσοστό της φυσική χωρητικότητα (Physical Load Capacitance) οφείλεται στις χωρητικότητες των τρανζίστορ, σε ένα σχεδιασμό χαμηλής κατανάλωσης ισχύος επιβάλλεται τα τρανζίστορ να έχουν το ελάχιστο επιτρεπόμενο μέγεθος. Αν αυτό δεν είναι εφικτό να γίνει σε όλο το κύκλωμα, λόγω μεγάλου αριθμού τρανζίστορ, μπορεί να γίνει στους κόμβους εκείνους που έχουν είτε μεγάλη δραστηριότητα μετάβασης ή/και οδηγούν μεγάλη χωρητικότητα στην έξοδό τους. Αυτή η τεχνική δεν μπορεί να εφαρμοστεί σε σχεδιασμούς με βιβλιοθήκες από τυποποιημένα κύτταρα όπου τα μεγέθη των τρανζίστορ είναι προκαθορισμένα.

3.5.2. Βελτιστοποίηση σε επίπεδο συστήματος (System Level)

Σε αυτό το επίπεδο, καθορίζονται οι προδιαγραφές και οι απαιτήσεις σε επιφάνεια και συχνότητα λειτουργίας του συστήματος. Με το όρο σύστημα εννοούμε ένα πολύπλοκο οικοδόμημα από ένα σύνολο κυκλωμάτων τα οποία όλα μαζί υλοποιούν τη λειτουργία του συστήματος. Παράδειγμα τέτοιου συστήματος αποτελεί ένας προσωπικός υπολογιστής ο οποίος απαρτίζεται από ένα ή περισσότερους επεξεργαστές, μια κύρια μνήμη, ειδικά ολοκληρωμένα κυκλώματα εισόδου/εξόδου για τη διαχείριση π.χ. του σκληρού δίσκου, της οθόνης κ.λπ. περιφερειακών συσκευών.

Σε ένα τέτοιο πολύπλοκο σύστημα καταρχάς πρέπει να γίνει επιλογή προσχεδιασμένων κυκλωμάτων τα οποία είναι σχεδιασμένα για εφαρμογές χαμηλής κατανάλωσης ισχύος (και σε περίπτωση που δεν υπάρχουν τέτοια κυκλώματα απαιτείται η τροποποίηση ήδη υπαρχόντων κυκλωμάτων ώστε η συχνότητα λειτουργίας τους να μην μεταβληθεί αλλά η μέση κατανάλωση της ισχύος τους να είναι μικρότερη).

Ακόμα και αν χρησιμοποιούνται τέτοια κυκλώματα χαμηλής κατανάλωσης ισχύος, διάφορες τεχνικές μπορούν να εφαρμοστούν στο επίπεδο συστήματος για περαιτέρω μείωση της συνολική μέσης κατανάλωσης ισχύος. Τέτοιες τεχνικές βασίζονται στην ιδέα της διαχείρισης της ενέργειας (Power Management, Power Down Techniques) όταν ένα τμήμα ενός συστήματος είναι ανενεργό τότε μπορούμε είτε να κόψουμε την παροχή ρεύματος σε αυτό, σώζοντας πρώτα την τρέχουσα κατάσταση του τμήματος αυτού ώστε σε μελλοντική ενεργοποίηση του να ξεκινήσει από την κατάσταση στην οποία βρισκόταν όταν έγινε η αποκοπή του από το συνολικό σύστημα, είτε να σταματήσουμε να δίνουμε ρολόι και εισόδους στο τμήμα αυτό, είτε να μειώσουμε την τάση τροφοδοσίας του σε τέτοιο επίπεδο ώστε να διατηρείται η πληροφορία όλων των στοιχείων μνήμης του είτε με συνδυασμό των παραπάνω τεχνικών.

3.5.3. Βελτιστοποίηση σε επίπεδο συμπεριφοράς/αλγορίθμου (Behavioral/ Algorithmic Level)

Πριν από μια λεπτομερή περιγραφή ενός κυκλώματος σε επίπεδο αρχιτεκτονικής, βελτιώσεις μπορούν να γίνουν σε επίπεδο συμπεριφοράς / αλγορίθμου του προς σχεδίαση κυκλώματος. Αλλάζοντας τις αρχικές προδιαγραφές ή τροποποιώντας τον αλγόριθμο ώστε να είναι πιο αποδοτικός ο σχεδιασμός του κυκλώματος, όσον αφορά την κατανάλωση ισχύος, μπορούμε να επιτύχουμε μείωση της καταναλισκόμενης ισχύος του κυκλώματος. Οι αλλαγές που μπορούν να γίνουν σε αυτό το επίπεδο παίζουν σημαντικό ρόλο όσον αφορά την κατανάλωση ισχύος ενός ψηφιακού κυκλώματος. Η επιλογή του σωστού αλγορίθμου και η σωστή τεμαχιοποίηση του κυκλώματος, μπορούν να έχουν σημαντικές, θετικές επιδράσεις ως προς την κατανάλωση ισχύος.

Γενικά το πρόβλημα σχεδίασης κυκλωμάτων χαμηλής κατανάλωσης ισχύος σε επίπεδο συμπεριφοράς / αλγορίθμου είναι ένα θέμα για το οποίο ο σχεδιαστής πρέπει να λάβει υπόψη του πολλούς και συχνά αντιφατικούς παράγοντες, οι επιδράσεις των οποίων στην τελική μορφή του κυκλώματος δεν είναι γνωστές στα αρχικά βήματα του σχεδιασμού. Οι τεχνικές που μπορεί κανείς να εφαρμόσει σε αυτό το επίπεδο σχεδιασμού είναι οι παρακάτω:

Επιλογή υλοποίησης (Implementation Choice): Σημαντικό ρόλο στην μέση κατανάλωση ισχύος παίζει η επιλογή του κατάλληλου μοντέλου / μεθοδολογίας με βάση το οποίο θα σχεδιαστεί το ζητούμενο κύκλωμα. Επιλογές μπορούν να γίνουν μεταξύ: 1) Δυναμικού/ στατικού κυκλώματος, 2) Υλοποίησης με τυποποιημένα κύτταρα μιας βιβλιοθήκης η με CPL πύλες, 3) Σύγχρονο/ ασύγχρονο κύκλωμα.

Μείωση του αριθμού των πράξεων (Operation Reduction): Ένας τρόπος για τη μείωση της ενεργούς χωρητικότητας, που ορίζεται όπως ήδη έχει αναφερθεί σαν το γινόμενο της χωρητικότητας επί την δραστηριότητα μετάβασης, είναι η μείωση των πράξεων ενός αλγορίθμου, μέσω αλγεβρικών μετασχηματισμών ή οποιονδήποτε άλλων κατάλληλων μετασχηματισμών και συνεπώς η μείωση των συνολικών μεταβάσεων σε ένα κύκλωμα που υλοποιεί τον συγκεκριμένο αυτό αλγόριθμο. Πρέπει όμως να τονιστεί ότι η μείωση των πράξεων έχει ως αποτέλεσμα τη μείωση της ενεργούς χωρητικότητας αλλά πολλές φορές επιδρά στη μέγιστη καθυστέρηση διάδοσης του κυκλώματος, την οποία και αυξάνει με αποτέλεσμα την εμφάνιση ενός ανασταλτικού παράγοντα ως προς τη μείωση της τάσης.

Αντικατάσταση πράξεων (Operation Substitution): Η βασική ιδέα αυτής της τεχνικής συνίσταται στο ότι πολλές πράξεις ενός αλγορίθμου συχνά καταναλώνουν από τη φύση τους λιγότερη ενέργεια από κάποιες άλλες, (κυρίως λόγω μικρότερης χωρητικότητας). Κατά συνέπεια είναι επιθυμητή η αντικατάσταση κάποιων πράξεων από άλλες που καταναλώνουν λιγότερη ενέργεια. Κλασικό παράδειγμα είναι η αντικατάσταση της πράξης του πολλαπλασιασμού, όπου ο ένας από τους δύο τελεστές είναι σταθερός, από αυτή των διαδοχικών προσθέσεων μετατοπισμένων τελεστών (Add/Shifts). Είναι σημαντικό όμως να τονιστεί ότι για μια άλλη φορά το κέρδος από τη μείωση της χωρητικότητας έχει ως αντίβαρο την κατά κανόνα αύξηση της μέγιστης καθυστέρησης διάδοσης του κυκλώματος με αποτέλεσμα να δημιουργείται πρόβλημα όσον αφορά την υποβάθμιση της τάσης τροφοδοσίας.

Μείωση του εύρους λέξης των εσωτερικών διαύλων (Word/length reduction): Ο αριθμός των δυαδικών ψηφίων που χρησιμοποιούνται για την υλοποίηση ενός αλγορίθμου παίζει σημαντικό ρόλο στην μέση κατανάλωση του κυκλώματος που τον υλοποιεί. Είναι φανερό ότι λιγότερα δυαδικά ψηφία στους εσωτερικούς διαύλους (Busses) έχει ως αποτέλεσμα:

- Τη μείωση της κατανάλωσης λόγω των λιγότερων κόμβων που θα φορτίζονται και θα εκφορτίζονται.
- Τη πιο γρήγορη απόκριση του κυκλώματος μιας και με λιγότερα δυαδικά ψηφία οι πράξεις γίνονται γρηγορότερα πράγμα που οδηγεί σε εκμετάλλευση αυτής της ιδιότητας για να υποβαθμισθεί η τάση.
- Τη μικρότερη καλωδίωση και κατά συνέπεια τη μείωση του μεγέθους των διασυνδέσεων και τη μείωση της χωρητικότητάς τους.
- Το μειονέκτημα αυτής της μεθόδου είναι ότι πολλές φορές οδηγεί σε αύξηση του αριθμού των απαιτούμενων πράξεων για να ολοκληρωθεί επιτυχώς ο αλγόριθμος.

Τοπικότητα των αναφορών (Locality Of Reference): Ένα σημαντικό στοιχείο κάθε αλγορίθμου, το οποίο και πρέπει να επιδιώκεται για σχεδίαση χαμηλής κατανάλωσης ισχύος, είναι η λεγόμενη τοπικότητα των αναφορών. Πράξεις οι οποίες γίνονται τοπικά και δεν απαιτούν επικοινωνία για παράδειγμα με κάποια κεντρική κύρια

μνήμη, συνεπάγονται μικρότερη χωρητικότητα και δραστηριότητα μετάβασης και κατά συνέπεια μικρότερη κατανάλωση. Είναι φανερό ότι η τοπικότητα των αναφορών παίζει σημαντικό ρόλο και σε επίπεδο αρχιτεκτονικής. Έτσι πράξεις για μια συνάρτηση είναι δυνατόν να ανατίθενται στον ίδιο επεξεργαστή ή στο ίδιο συνδυαστικό κύκλωμα (Data Path Partition). Αυτό έχει ως αποτέλεσμα της μείωση της καταναλισκόμενη ισχύος λόγω της μη μεταφοράς των δεδομένων από διαύλους με υψηλή χωρητικότητα.

Επίσης μια σωστή διαχείριση της μνήμης έχει και αυτή θετικά αποτελέσματα μιας και οι προσπελάσεις στη μνήμη καταναλώνουν σημαντικό ποσό ενέργειας.

Προτείνεται πολλές φορές μια ιεραρχία κατανεμημένης μνήμης (Distributed Memory) αντί μίας κεντρικής μνήμης (Single Centralized Memory) μιας και έτσι εξασφαλίζεται μικρότερη χωρητικότητα λόγω καλωδίωσης.

Αναπαράσταση/ Κωδικοποίηση δεδομένων (Data Representation): Η σωστή επιλογή της αναπαράστασης των δεδομένων ενός αλγορίθμου είναι δυνατόν να ελαττώσει την δραστηριότητα μετάβασης ενός αλγορίθμου και κατά συνέπεια την δυναμική του κατανάλωση. Σαν παράδειγμα μπορεί να δοθεί η χρήση του κώδικα Gray σε για την διευθυνσιοδότηση μίας μνήμης σε αντιδιαστολή με την κλασική γραμμική προσπέλαση. Στη δεύτερη περίπτωση υπάρχουν περιπτώσεις όπου όλα τα δυαδικά ψηφία αλλάζουν ταυτόχρονα από '0' σε '1' πράγμα που δε συμβαίνει με τον κώδικα Gray. Άλλο παράδειγμα αποτελεί η προσημασμένη και η μη προσημασμένη (Unsigned και Signed) αναπαράσταση που χρησιμοποιείται για τα δεδομένα ενός αλγορίθμου. Για παράδειγμα ένας πολλαπλασιαστής στον οποίο τα δεδομένα έχουν αναπαράσταση Sign Magnitude, όπου το πιο υψηλής σημασίας δυαδικό ψηφίο χρησιμοποιείται σαν πρόσημο του αριθμού και τα υπόλοιπα δυαδικά ψηφία χρησιμοποιούνται για να δηλώσουν το μέγεθος του αριθμού, καταναλώνει σημαντικά λιγότερη ενέργεια σε σχέση με την 2's Complement αναπαράσταση των δεδομένων γιατί γίνονται λιγότερες μεταβάσεις στις εισόδους του.

3.5.4. Βελτιστοποίηση σε επίπεδο αρχιτεκτονικής (Architectural Level)

Το επίπεδο αυτό σχεδιασμού είναι εκείνο στο οποίο μπορεί κανείς να πετύχει σημαντικές βελτιώσεις όσον αφορά και την κατανάλωση ισχύος. Στο επίπεδο αυτό είναι απαραίτητο να φτιαχτούν τα απαραίτητα CAD εργαλεία που να εφαρμόζουν τις τεχνικές που θα αναφέρουμε παρακάτω. Ο βασικός στόχος των τεχνικών βελτιστοποίησης αφορά και τη μείωση της τάσης τροφοδοσίας, Vdd, και της ενεργούς χωρητικότητας, Ceff. Η βασική ιδέα είναι να χρησιμοποιείται η "αρχή της τοπικότητας των αναφορών" (Locality Of References): όπου είναι δυνατό πρέπει να αποφεύγεται η πρόσβαση/ προσπέλαση γενικών/ κεντρικών πόρων (όπως μνημών, διαύλων, αριθμητικών/ λογικών μονάδων ALU's κ.λπ.).

Επιλογή αρχιτεκτονικής και τμηματοποίηση (Architecture Selection And Partitioning):

- Παραλληλισμός (Parallelism): Ένας τρόπος για να διατηρηθεί σταθερή η απόδοση του κυκλώματος είναι να γίνει διπλασιασμός σε κάποιο μέρος του κυκλώματος στο οποίο ο παραλληλισμός αυτός οδηγεί σε μείωση της συχνότητας λειτουργίας. Ένα προφανές μειονέκτημα είναι η αύξηση της επιφανείας του κυκλώματος, που στην περίπτωση της πλήρους παραλληλίας είναι διπλάσια. Τυπικές μειώσεις της μέσης κατανάλωσης ισχύος μετά την εφαρμογή της τεχνικής της παραλληλίας είναι της τάξης 60-65 %.
- Διοχέτευση (Pipelining): Σε σύγχρονα κυρίως κυκλώματα μπορούμε να εισάγουμε την τεχνική της διοχέτευσης, εισάγοντας π.χ. καταχωρητές στις εισόδους ή τις εξόδους ενός συνδυαστικού τμήματος του κυκλώματος (αλλά όχι και στις δύο μαζί), καθυστερώντας την απόκριση του κυκλώματος κατά ένα κύκλο. Αυτό οδηγεί σε μείωση της συνολικής καθυστέρησης διάδοσης και έτσι επιτρέπει μείωση της τάσης τροφοδοσίας. Τυπικές μειώσεις της μέσης κατανάλωσης ισχύος μετά την εφαρμογή της τεχνικής διοχέτευσης είναι της τάξης 65-70 %.
- Παραλληλισμός και Διοχέτευση (Parallelism and pipelining): Προφανώς μία υλοποίηση που χρησιμοποιεί και τις δύο παραπάνω τεχνικές πετυχαίνει τη βέλτιστη μείωση της κατανάλωσης ισχύος. Τυπικές μειώσεις της μέσης κατανάλωσης ισχύος μετά την εφαρμογή της τεχνικής παραλληλισμού και διοχέτευσης είναι της τάξης 75-80 %.

Πρέπει να τονιστεί ότι οι τρεις παραπάνω τεχνικές έχουν πολύ καλύτερα αποτελέσματα στην μέση κατανάλωση ισχύος σε σχέση με τις κλασσικές πολύπλεξης χρόνου (Time Multiplexed) αρχιτεκτονικές που χρησιμοποιούνται στη σχεδίαση ολοκληρωμένων κυκλωμάτων όπως π.χ. μικροεπεξεργαστές, επεξεργαστές επεξεργασίας ψηφιακού σήματος (DSPs) κ.α. Αυτό συμβαίνει γιατί η πολύπλεξη αυξάνει τη συνολική καθυστέρηση διάδοσης και έτσι δεν επιτρέπει περαιτέρω μείωση της τάσης τροφοδοσίας. Από την άλλη μεριά όμως πρέπει να σημειώσουμε ότι δεν είναι πάντα δυνατή η εφαρμογή αυτών των μεθόδων και εξαρτάται από το εκάστοτε κύκλωμα και τις προδιαγραφές σε επιφάνεια και συχνότητας λειτουργίας. Πιθανόν σε κομμάτια του συνολικού κυκλώματος που μπορούν να υλοποιηθούν παράλληλα ή/και με διοχέτευση να μπορούν να εφαρμοστούν (αν δεν επηρεάζουν τη λειτουργία του κυκλώματος). Τέλος πρέπει να σημειωθεί ότι υπάρχει ένα πάνω όριο στη χρήση αυτών των τεχνικών πέρα από το οποίο δεν μπορεί να επιτευχθεί περαιτέρω μείωση της τάσης τροφοδοσίας, το οποίο εξαρτάται από τη σχέση τάσης τροφοδοσίας και καθυστέρησης διάδοσης των τυποποιημένων κυττάρων της χρησιμοποιούμενης τεχνολογίας.

- Τμηματοποίηση (Partition): Για παράδειγμα η χρησιμοποίηση μιας αρχιτεκτονικής με μια ιεραρχία κρυφών μνημών αντί μιας κεντρικής μνήμης, "βαριάς" από άποψη κατανάλωσης ισχύος λόγω προσπέλασης, βοηθάει στην αποσυμφόρηση του όλου συστήματος και στη μείωση της κατανάλωσης ισχύος.

Καλό θα είναι, όπου είναι δυνατό, να αποφεύγεται η χρήση κοινών πόρων του κυκλώματος. Κλασσική περίπτωση τέτοιων πόρων αποτελούν οι δίαυλοι προσπέλασης (διευθύνσεων, δεδομένων, εντολών). Από άποψη ισχύος είναι καλό να χρησιμοποιούμε ειδικούς τοπικούς δίαυλους (σε σύνδεση σημείου με σημείο) αντί για ένα κοινό δίαυλο, γιατί αυτό οδηγεί σε αύξηση της χωρητικότητας του διαύλου εξαιτίας του μεγάλου αριθμού των κόμβων που είναι συνδεδεμένοι στον κοινό αυτό δίαυλο. Καλό τέλος θα είναι τέλος να αποφεύγεται η χρήση πολλών πολυπλεκτών μέσα στο προς σχεδίαση κύκλωμα (εκτός και αν το επιβάλλει η σχεδίαση σε ορισμένα σημεία).

Επιλογή συνόλου εντολών και υλικού (Instruction Set And Hardware Selection):

Αν στη σχεδίαση π.χ. ενός μικροεπεξεργαστή λάβουμε υπόψη μας τις πιο χρησιμοποιούμενες εντολές και κωδικοποιήσουμε κατάλληλα το σύνολο εντολών του ώστε να μειώσουμε την ενεργό χωρητικότητα των πιο συχνά χρησιμοποιούμενων εντολών, τότε πετυχαίνουμε σημαντική μείωση της μέσης κατανάλωσης ισχύος τους. Αυτή η προσέγγιση είναι πιο δημοφιλής στη σχεδίαση επεξεργαστών ειδικών εφαρμογών (Application Specific Processors) όπως modem και επεξεργαστές κωδικοποίησης/αποκωδικοποίησης και επεξεργασίας φωνής (Voice Codec Processors).

Σύνθεση επιπέδου αρχιτεκτονικής (Architecture Synthesis): Η σύνθεση σε επίπεδο αρχιτεκτονικής περιλαμβάνει τρεις φάσεις: Ανάθεση (Allocation) , Διανομή (Assignment) και Προγραμματισμό εκτέλεσης των επιμέρους διεργασιών (Scheduling). Με λίγα λόγια οι τρεις αυτές φάσεις καθορίζουν πόσα κομμάτια από κάθε υποκύκλωμα χρειάζονται κατά τη διάρκεια της σύνθεσης (Allocation) , πάνω σε πιο υποκύκλωμα θα γίνει μια συγκεκριμένη ενέργεια/ πράξη (Assignment) και πότε αυτή η πράξη θα εκτελεστεί (Scheduling). Συνήθως η σύνθεση σε αυτό το επίπεδο προσπαθεί να ελαχιστοποιήσει τον αριθμό των απαιτούμενων υποκυκλωμάτων για ένα συγκεκριμένο τμήμα του κυκλώματος ή προσπαθεί να μειώσει τον συνολικό χρόνο που απαιτείται για να ολοκληρωθεί μια διεργασία. Χρησιμοποιώντας τις υπάρχουσες τεχνικές μείωσης της επιφανείας ή/ και μείωσης της συνολικής καθυστέρησης του κυκλώματος, φτάνουμε σε μια λύση η οποία συνήθως δεν είναι και η βέλτιστη από άποψη κατανάλωσης ισχύος.

3.5.5. Βελτιστοποίηση σε επίπεδο πύλης (Gate Level)

Επανασυνχρονισμός και αξιοποίηση πόρων (Retiming/Resource Utilization): Με βάση αυτή την τεχνική, χρησιμοποιώντας μια ευριστική μέθοδο, επιλέγουμε ένα σύνολο από κόμβους του κυκλώματος με την προϋπόθεση ότι αν βάλουμε ένα I στοιχείο μνήμης (Flip-Flop) στις εξόδους των κόμβων αυτών, θα μειωθεί η συνολική δραστηριότητα μετάβασης τους. Οι κόμβοι επιλέγονται με κριτήριο την πιθανότητα εμφάνισης ανεπιθύμητων μεταβάσεων στις εξόδους τους καθώς και την πιθανότητα διάδοσης αυτών των ανεπιθύμητων μεταβάσεων στο υπόλοιπο κύκλωμα. Η μείωση που μπορούμε να πετύχουμε φτάνει το 8 %. Συνήθως είναι δυνατό αν μειώσουμε το

απαιτούμενο υλικό που απαιτείται για την υλοποίηση ενός κυκλώματος χρησιμοποιώντας επανασυγχρονισμό να πετύχουμε μείωση της κατανάλωσης ισχύος.

Προϋπολογιζόμενη λογική (Pre-Computation Logic): Με βάση αυτή την τεχνική, επιλέγουμε, με κριτήριο τη δραστηριότητα μετάβασης, κάποιους κόμβους, των οποίων προϋπολογίζουμε την τιμή των εξόδων τους, ένα κύκλο προτού αυτή εμφανιστεί. Χρησιμοποιώντας αυτή την λογική τιμή που υπολογίσαμε μειώνουμε την εσωτερική δραστηριότητα μετάβασης των κόμβων αυτών στον επόμενο κύκλο ρολογιού. Η μείωση της κατανάλωσης ισχύος που μπορούμε να πετύχουμε φτάνει το 62 % με μικρή σχετικά αύξηση της επιφανείας και της συνολικής καθυστέρησης διάδοσης του κυκλώματος.

Κωδικοποίηση κατάστασης (State Assignment): Σε ένα ακολουθιακό κύκλωμα που αναπαρίσταται με μια μηχανή πεπερασμένων καταστάσεων (FSM), τότε προσοχή πρέπει να δοθεί στην κωδικοποίηση των καταστάσεων της έτσι ώστε κατά τις μεταβάσεις από τη μία κατάσταση στην άλλη να γίνονται όσο το δυνατόν λιγότερες αλλαγές στους κόμβους του κυκλώματος (από 1 ~ 0 και από 0 ~ 1). Επειδή είναι πολύ δύσκολο να βρεθεί ο ακριβής αριθμός των μεταβάσεων ενός κόμβου (και ιδίως αν το κύκλωμα είναι μεγάλο!) με τις κλασσικές μεθόδους, χρησιμοποιούνται στατικές πιθανοτικές τεχνικές για την πρόβλεψη του αριθμού αυτών των μεταβάσεων. Τέτοια εργαλεία κωδικοποίησης των καταστάσεων μιας μηχανής πεπερασμένων καταστάσεων έχουν αναπτυχθεί και βοηθούν και στην βέλτιστη κωδικοποίηση των καταστάσεων της FSM και στην καλή εκτίμηση του αριθμού των μεταβάσεων στις γραμμές κατάστασης.

Βελτιστοποίηση κυκλωμάτων πολλών επιπέδων (Multi Level Network Optimization): Αν χρησιμοποιήσουμε τις αδιάφορες καταστάσεις (Don't Care Values) των εσωτερικών κόμβων του κυκλώματος μπορούμε να πετύχουμε μείωση της μέσης κατανάλωσης ισχύος. Δύο είδη αδιάφορων καταστάσεων μπορούμε να εκμεταλλευτούμε: Μη εμφανιζόμενες καταστάσεις (Function Preserving Don't Care): αποτελούν καταστάσεις των κόμβων του κυκλώματος οι οποίες δεν πρόκειται ποτέ να συμβούν. Μη παρατηρήσιμοι κόμβοι (Function Modifying Don't Care): αποτελούν κόμβους του κυκλώματος οι οποίοι δεν είναι άμεσα παρατηρήσιμοι στο κύκλωμα.

Εξαγωγή κοινών εκφράσεων (Common Sub Expression Extraction): Συνήθως μια πολύπλοκη λογική έκφραση/ συνάρτηση μπορεί να υλοποιηθεί με την εισαγωγή ενός ή περισσότερων επιπέδων μεταξύ των εισόδων και των εξόδων της συνάρτησης αυτής. Βελτιστοποίηση τέτοιου είδους συναρτήσεων απαιτεί την προσθήκη ή/ και την αφαίρεση ενδιάμεσων κόμβων/ σημάτων έτσι ώστε να επιτευχθεί μείωση της επιφανείας που καταλαμβάνει το κύκλωμα χωρίς να παραβιάζονται οι χρονικοί περιορισμοί του κυκλώματος. Η τεχνική που χρησιμοποιείται σε αυτή την περίπτωση είναι η παραγοντοποίηση για μείωση της κατανάλωσης ενέργειας (Factoring For Power Saving). Η γενική ιδέα είναι ότι αν έχω ένα σύνολο συναρτήσεων $F_1, F_2, \dots, F_L$ οι οποίες περιέχουν κοινά τμήματα $C = \{g, f, h, \dots\}$ τότε βρες εκείνο(α) από αυτά τα

κοινά τμήματα τα οποία ανήκουν στο σύνολο C, ώστε το μετασχηματισμένο ολικό κύκλωμα, στο οποίο τα κοινά αυτά τμήματα εμφανίζονται μόνο μία και όχι L φορές, τελικά να έχει μικρότερη κατανάλωση ισχύος από το αρχικό. Η μείωση της ισχύος που μπορούμε να επιτύχουμε φτάνει το 12 %.

Διαχείριση ρολογιού (Clock Management): Η ύπαρξη ρολογιού σε ένα κύκλωμα είναι ένας ακόμη σημαντικός παράγοντας όσον αφορά την κατανάλωση ισχύος. Καλή διαχείριση του ρολογιού σε επίπεδο αρχιτεκτονικής θα έχει προφανώς θετικά αποτελέσματα. Το ρολόι είναι το σήμα εκείνο που έχει μια από τις μεγαλύτερες δραστηριότητες μετάβασης (αφού αλλάζει κατάσταση σε κάθε κύκλο) και ταυτόχρονα παρουσιάζει μία από τις μεγαλύτερες χωρητικότητες (αφού συνήθως οδηγεί εκατοντάδες ή χιλιάδες κόμβους) μέσα σε ένα κύκλωμα. Η ιδέα είναι να χρησιμοποιήσουμε ένα κεντρικό ρολόι το οποίο θα διαδίδεται ομοιόμορφα σε όλο το κύκλωμα και ο σκοπός είναι να ελαχιστοποιήσουμε τη χωρητικότητα στους απομονωτές (Buffers) του ρολογιού, ώστε να είμαστε μέσα στα ανεκτά όρια απόκλισης της συχνότητας του ρολογιού (Clock Skew). Η μείωση της κατανάλωσης που μπορούμε να πετύχουμε στην κατανάλωση που προκαλεί το ρολόι σε ένα κύκλωμα (που μπορεί να είναι και το 30-40 % της συνολικής κατανάλωσης ισχύος) μπορεί να φτάσει το 70 % με αποτέλεσμα να παρουσιάζεται μια μείωση στη συνολική κατανάλωση ισχύος ενός κυκλώματος της τάξης του 20-25%.

Ένας άλλος βασικός παράγοντας που πρέπει να ληφθεί υπόψη για το σωστό και αποδοτικό σχεδιασμό ενός σύγχρονου κυκλώματος είναι η διαχείριση των ρολογιών του. Σημαντικό μέρος της καταναλισκόμενης ισχύος οφείλεται στη μη σωστή διαχείριση τους. Οι τεχνικές που ακολουθούνται σε αυτή την περίπτωση είναι: 1) Απομόνωση ρολογιού (Gated Clocks) και 2) Ασύγχρονα ρολόγια (Self Timing Clocks).

- Απομόνωση ρολογιού (Gated Clocks): Η βασική ιδέα σε αυτή την τεχνική είναι ότι πολλές φορές κατά τη διάρκεια λειτουργίας ενός κυκλώματος υπάρχουν καταστάσεις οι οποίες παραμένουν οι ίδιες λόγω των εισόδων τους. Σε αυτή λοιπόν την περίπτωση η παρουσία ρολογιού δε χρησιμεύει σε τίποτε, αφού δε πρόκειται να έχουμε μετάβαση σε μία άλλη κατάσταση και κατά συνέπεια το ρολόι μπορεί να απομονωθεί/αποκοπεί. Η όλη προσπάθεια συνίσταται στην πρόβλεψη των καταστάσεων οι οποίες δεν αλλάζουν για αρκετά μεγάλο χρονικό διάστημα (Self Loop) και στην εκμετάλλευση αυτής της γνώσης έτσι ώστε να απαγορεύεται η γένεση σημάτων ρολογιού σε αυτές τις περιπτώσεις.
- Ασύγχρονα ρολόγια (Self Timing Clock): Είναι γνωστό ότι η ύπαρξη ρολογιού στα σύγχρονα κυκλώματα χρησιμεύει για το συγχρονισμό των αποκρίσεων των στοιχείων μνήμης τα οποία απαρτίζουν τις βαθμίδες αυτών των κυκλωμάτων. Η ύπαρξη ρολογιού σε συνδυασμό με την αλλαγή εισόδων και εσωτερικών κόμβων οδηγούν στην απόκριση των στοιχείων μνήμης. Πολλές φορές είναι προτιμότερος ο σχεδιασμός με τη λογική των σημάτων

χειραγίας (Handshake Signals) έτσι ώστε οι βαθμίδες να αποκρίνονται όταν υπάρχει λόγος (Request) και να παραμένουν αδρανείς στις άλλες περιπτώσεις. Αυτή η τεχνική μειώνει την κατανάλωση που οφείλεται στην ύπαρξη σημάτων ρολογιού σε σημαντικό βαθμό και εκμεταλλεύεται τις ιδιότητες της τοπικότητας των αναφορών, αλλά έχει επιπτώσεις ως προς τη πολυπλοκότητα της σχεδίασης και την αύξηση της επιφάνειας λόγω της εμφάνισης του επιπλέον υλικού για τη χειραγία (Handshake Hardware).

Ισοστάθμιση μονοπατιών (Path Balancing): Για να ελαχιστοποιήσουμε την επίδραση των ανεπιθύμητων δυναμικών μεταβάσεων (glitches) στην συνολική μέση κατανάλωση ισχύος ενός στατικού CMOS ψηφιακού κυκλώματος, είναι σημαντικό να εξισώσουμε, όσο μπορούμε, το χρόνο άφιξης των σημάτων στις εισόδους κάθε πύλης. Αυτό μπορεί να επιτευχθεί πριν την απεικόνιση σε κάποια τεχνολογία τυποποιημένων κυττάρων (Technology Mapping) με την εισαγωγή καθυστέρησης ώστε να πετύχουμε ισοσταθμισμένες καθυστερήσεις (Balance Path Delays). Το βασικό θέμα που πρέπει να μας απασχολεί είναι να βάλουμε όσο το δυνατό λιγότερα στοιχεία καθυστέρησης (Delay Elements), όπως απομονωτές ή/και αντιστροφείς, για να περιορίσουμε την ασυμβατότητα στους χρόνους άφιξης των σημάτων στις εισόδους μιας πύλης. Η αλλαγή που γίνεται αφορά την οδήγηση των εξόδων των πυλών με τη διάσπαση του κυκλώματος και τη χρησιμοποίηση περισσοτέρων επιπέδων. Καλό θα ήταν επίσης να μειωθεί, όσο αυτό είναι δυνατό, ο αριθμός των επιπέδων κατά την υλοποίηση μιας λογικής συνάρτησης.

Διάσπαση σε τεχνολογία (Technology Decomposition): Δοθείσας της δραστηριότητας μετάβασης κάθε ενός σήματος του κυκλώματος μπορούμε να κάνουμε π.χ. AND διάσπαση κάποιου κόμβου, η οποία οδηγεί σε ένα δύο-εισόδων AND δέντρο το οποίο ελαχιστοποιεί τη δραστηριότητα μεταβάσεων του κόμβου αυτού. Αυτή η μέθοδος είναι παρόμοια με τον αλγόριθμο του Huffman για την κατασκευή ενός δυαδικού δέντρου με ισοκατανεμημένα μονοπάτια και έχει άριστα αποτελέσματα για δυναμικά CMOS κυκλώματα και πολύ καλά αποτελέσματα για στατικά. Η μείωση που μπορούμε να πετύχουμε φτάνει το 3 % μετά από την εφαρμογή της διάσπασης αυτής.

Απεικόνιση σε τεχνολογία (Technology Mapping): Το πρόβλημα της ελαχιστοποίησης της κατανάλωσης ισχύος κατά τη διάρκεια της απεικόνισης σε μία τεχνολογία λύνεται σε δύο φάσεις. Στην πρώτη φάση οι καμπύλες κατανάλωσης/καθυστερήσης υπολογίζονται για κάθε κόμβο του κυκλώματος. Στο δεύτερο βήμα γίνεται η απεικόνιση με βάση αυτές τις καμπύλες και το συνολικό χρόνο καθυστέρησης στις εξόδους του κυκλώματος. Συγκρινόμενη με μία μέθοδο απεικόνισης η οποία ελαχιστοποιεί την καθυστέρηση διάδοσης, η μείωση που μπορούμε να πετύχουμε φτάνει το 18 % με περίπου 16 % αύξηση της συνολικής επιφάνειας του ολοκληρωμένου κυκλώματος.

Αντιστοίχιση σήματος-ακίδας (Signal to pin Assignment): Γενικά οι πύλες των βιβλιοθηκών από τυποποιημένα κύτταρα έχουν διάφορες ακίδες από τα οποία μπορεί κανείς να πάρει την έξοδό τους ή να συνδέσει μια είσοδό τους (π.χ. σε μία AND 3 εισόδων όλες οι εισοδοί της είναι ισοδύναμες). Αυτές οι ακίδες είναι ισοδύναμες, ως προς την συνάρτηση που υλοποιούν και μπορεί να έχουν διαφορετικά φορτία συνδεδεμένα επάνω τους. Προφανώς θέλουμε εισόδους με μεγάλη δραστηριότητα να τις συνδέσουμε σε ακίδες με μικρή χωρητικότητα. Για να βρούμε τη βέλτιστη αντιστοίχιση σήματος-ακίδας πρέπει να λύσουμε ένα αρκετά δύσκολο πρόβλημα βελτιστοποίησης. Εναλλακτικά μπορεί κάποιος να χρησιμοποιήσει ευριστικές μεθόδους για να λύσει το πρόβλημα.

3.5.6. Βελτιστοποίηση σε φυσικό Επίπεδο (Physical Layer)

Τμηματοποίηση κυκλώματος (Circuit Partitioning): Η τμηματοποίηση ενός κυκλώματος είναι η τεχνική εκείνη κατά την οποία μπορούμε να χωρίσουμε ένα πολύπλοκο κύκλωμα σε απλούστερα τμήματα, τα οποία έχουν βελτιστοποιηθεί ως προς την κατανάλωση ισχύος τους και τα οποία χρησιμοποιούνται ως χωριστά και ανεξάρτητα τμήματα μέσα σε ένα κύκλωμα, με σκοπό την μείωση της καταναλισκόμενης ισχύος.

Οργάνωση φυσικού χώρου (Floorplaning): Η οργάνωση του φυσικού χώρου παίζει ένα σημαντικό ρόλο κατά τη φάση της φυσικής σχεδίασης (Layout) , καθώς είναι αυτή που καθορίζει τα χαρακτηριστικά της επικοινωνίας (Interface) του κυκλώματος με εξωτερικά κυκλώματα (π.χ. σχήμα, μέγεθος και θέση των ακίδων εισόδου/εξόδου) καθώς και τη θέση των υποκυκλωμάτων σε μια ιεραρχική σχεδίαση. Χρησιμοποιώντας τους κατάλληλους αλγορίθμους μπορούμε να κάνουμε μια εκτίμηση της συνολικής επιφάνειας του κυκλώματος έτσι ώστε να την ελαχιστοποιήσουμε και ταυτόχρονα να ελαχιστοποιήσουμε και τη μέση κατανάλωση της ισχύος του κυκλώματος.

Τοποθέτηση τυποποιημένων κυττάρων (Placement): Η ύπαρξη ενός κατάλληλου αλγορίθμου για την τοποθέτηση των τυποποιημένων κυττάρων του κυκλώματος, γίνεται επιτακτική όσον αφορά το σχεδιασμό κυκλωμάτων χαμηλής κατανάλωσης ισχύος. Το όλο πρόβλημα διατυπώνεται, οριοθετείται, σαν ένα υπολογιστικό πρόβλημα περιορισμών (Constrained Programming Problem) και λύνεται σε δύο φάσεις: 1) Γενική Βελτιστοποίηση (Global Optimization) και 2) Διανομή σχισμών (Slot Assignment). Η συνάρτηση κόστους (Objective Function) που χρησιμοποιείται και στις δύο φάσεις είναι το συνολικό μήκος καλωδίου (Total Weighted Net Length) όπου το κόστος αυτό υπολογίζονται σαν την αναμενόμενη ενεργή χωρητικότητα του κάθε κυττάρου του κυκλώματος. Ουσιαστικά γίνεται μια εκτίμηση της συνολικής επιφάνειας που απαιτείται και προσπαθείς να βρεις την βέλτιστη τοποθέτηση των τυποποιημένων κυττάρων έτσι ώστε η συνάρτηση κόστους με τις παραμέτρους που από πριν έχεις οριοθετήσει, χωρητικότητα, καθυστέρηση, κατανάλωση ισχύος να είναι ικανοποιητική. Γενικά αυτή η διεργασία μειώνει την κατανάλωση ισχύος

αυξάνοντας σε πολύ μικρό βαθμό τη συνολική καθυστέρηση διάδοσης του κυκλώματος συγκρινόμενη με ένα αλγόριθμο τοποθέτησης ο οποίος κάνει μόνο ελαχιστοποίηση του μήκους των διασυνδέσεων. Η μείωση της κατανάλωσης ισχύος που μπορούμε να επιτύχουμε φτάνει το 10 %.

Καλωδίωση (Routing): Η όλη φιλοσοφία βασίζεται στην κατάλληλη διαχείριση των διασυνδέσεων των τυποποιημένων κυττάρων του κυκλώματος, λαμβάνοντας υπόψη το ρυθμό εναλλαγής των λογικών καταστάσεων με σκοπό τη μείωση της ολικής χωρητικότητας και τελικά τη μείωση της ισχύος. Σε σήματα με μεγάλη δραστηριότητα μετάβασης ή/και με μεγάλη χωρητικότητα πρέπει να δίνεται προτεραιότητα κατά τη διάρκεια της καλωδίωσης (όπως Π.χ. στα ρολόγια, στο γενικό σήμα αρχικοποίησης του κυκλώματος).

Μέγεθος πυλών και καλωδίων (Gate And Wire Sizing): Το μέγεθος των καλωδίων που χρησιμοποιούμε κατά την καλωδίωση καθώς και το μέγεθος των διαφόρων απομονωτών που χρησιμοποιούμε στο κύκλωμά μας, είναι βασικός παράγοντας σε κυκλώματα ευαίσθητα σε καθυστερήσεις. Επίσης σημαντική είναι η επίδρασή τους και στην μέση κατανάλωση της ισχύος, μιας και η μείωση που μπορούμε να πετύχουμε φτάνει το 10 % για κυκλώματα στα οποία διατηρούμε τη μέγιστη καθυστέρηση διάδοσης σταθερή.

ΚΕΦΑΛΑΙΟ 4. Σχεδιασμός συστήματος ασφάλειας για περιορισμένων πόρων εφαρμογές

Στο Κεφάλαιο 4 παρουσιάζεται μια προσέγγιση για ολοκληρωμένο σύστημα ασφάλειας σε συστήματα εξαιρετικά περιορισμένων πόρων. Τέτοια συστήματα μπορεί να είναι Έξυπνες Κάρτες και RFID ετικέτες. Η μελέτη για τη σχεδίαση του συστήματος αυτού ξεκινά από το επίπεδο πρωτοκόλλου και τη λειτουργικότητα-μηχανισμοί που σχετίζονται με αυτό. Έπειτα ακολουθεί η επιλογή των αλγορίθμων που θα υποστηρίξουν το πρωτόκολλο. Σε επίπεδο αρχιτεκτονικής συστήματος, προτάσεις παρατίθενται για την καλύτερη σύγκλιση των αλγορίθμων κρυπτογραφίας με τις απαιτήσεις του συνολικού συστήματος.

4.1.Εισαγωγή

Ο σκοπός του κεφαλαίου αυτού είναι να αναδείξει τα βασικά χαρακτηριστικά που πρέπει να έχουν τα συστήματα ασφαλείας σε περιβάλλοντα περιορισμένων πόρων καθώς και τις τεχνικές σε επίπεδο συστήματος υλικού που πρέπει να εφαρμοστούν. Οι γενικότερες αρχές που πρέπει να ακολουθηθούν είναι:

Πρωτόκολλα κρυπτογράφησης με ελάχιστο κόστος (Έξυπνες κάρτες, RFID ετικέτες): Η επιλογή του πρωτοκόλλου ασφαλείας αποτελεί την πιο καθοριστική απόφαση για τη μετέπειτα σχεδίαση του συστήματος, αλλά και για τις προσφερόμενες υπηρεσίες ασφαλείας. Το επιλεγμένο πρωτόκολλο ασφαλείας συνδέεται άμεσα με τους αλγόριθμους κρυπτογράφησης που το υποστηρίζουν και αυτοί με τη σειρά τους συνδέονται με τις βασικές κρυπτογραφικές πράξεις των αλγορίθμων αυτών. Στην παρακάτω Εικόνα 15 παρουσιάζεται η ιεραρχία για την υλοποίηση πρωτοκόλλων ασφαλείας.

Εικόνα 15. Η ιεραρχία για την υλοποίηση πρωτοκόλλων ασφαλείας

Η προσπάθεια να στηριχτούν πρωτόκολλα κρυπτογράφησης πάνω σε όσο το δυνατό λιγότερο κόστος (επιφάνεια) είναι απαραίτητη για χαμηλών πόρων εφαρμογές. Το σενάριο αυτό επιτυγχάνεται με υποστήριξη πολλών κρυπτογραφικών λειτουργιών

από το ίδιο αλγόριθμο. Το γεγονός αυτό προϋποθέτει κατάλληλη μονάδα ελέγχου και λογική ώστε να αλλάζει το σενάριο λειτουργίας του αλγορίθμου.

Υποστήριξη Πολλαπλών Σεναρίων Ασφάλειας: Το χαρακτηριστικό αυτό επιτρέπει στο σύστημα να λειτουργεί σε περισσότερη της μιας κατάσταση για μια συγκεκριμένη λειτουργία (π.χ. κρυπτογράφηση) με αποτέλεσμα να ρυθμίζεται η παρεχόμενη ασφάλεια ανάλογα με τις απαιτήσεις σε απόδοση ή τους πόρους του συστήματος. Επιπλέον μπορεί να συνεργαστεί με περισσότερες οντότητες που τα συστήματα ασφαλείας τους ανήκουν στο σύνολο συστημάτων ασφαλείας που διαθέτει.

Εκμετάλλευση του Συνολικού Δικτύου: Εκμεταλλευόμαστε τη συνολική δομή του δικτύου και ολοκληρώνουμε στις συσκευές περιορισμένων πόρων μόνο τις απαραίτητες κρυπτογραφικές πράξεις. Μπορούμε να αφήνουμε σύνθετους μηχανισμούς κρυπτογράφησης σε πολύπλοκα συστήματα του δικτύου.

Επιπλέον κίνητρα που προωθούν την κατεύθυνση αυτή στα συστήματα κρυπτογραφίας περιορισμένων πόρων είναι τα ακόλουθα:

Η εξέλιξη της τεχνολογίας των ολοκλήρωσης των αλγορίθμων σε υλικό: Η εξέλιξη της τεχνολογίας των FPGAs επέτρεψε τη ανάπτυξη ιδανικών συσκευών για συστήματα σε περιορισμένα περιβάλλοντα πόρων. Ήδη υπάρχουν στην αγορά τέτοια συστήματα για περιορισμένων πόρων εφαρμογές. Μελλοντικές προεκτάσεις της τεχνολογίας αυτής αφήνουν περιθώρια για στιγμιαίο (on-the-fly) επαναπροσδιορισμό της λογικής τους. Επομένως σε ένα τέτοιο σενάριο θα ήταν θεμιτή η ολοκλήρωση-ρύθμιση του αλγορίθμου ανάλογα με τις τρέχουσες συνθήκες.

4.2. Υπηρεσίες ασφάλειας συστήματος

Βασικό θέμα για συσκευές περιορισμένων πόρων όπως Έξυπνες Κάρτες, RFID ετικέτες και δίκτυα αισθητήρων είναι η πιστοποίηση της ταυτότητας. Όπως εξηγήσαμε, υπάρχουν βασικά σημεία που υποδεικνύουν την ανάγκη για περιορισμένης πολυπλοκότητας σχήματα στο μηχανισμό πιστοποίησης και κρυπτογράφησης.

Δύο βασικές υπηρεσίες ασφάλειας λοιπόν πρέπει να «ενσωματώνονται» στον πελάτη (client- σύστημα περιορισμένων πόρων) είναι η πιστοποίηση και η μυστικότητα. Θα αναφερθούμε πρώτα στο σχήμα της πιστοποίησης της ταυτότητας του client.

Παρακάτω παρουσιάζουμε το προτεινόμενο πρωτόκολλο πιστοποίησης το οποίο είναι αυτό της αμοιβαίας συμμετρικής πιστοποίησης. Το πρωτόκολλο αυτό βασίζεται στη συμμετρική μονομερή πιστοποίηση όπου και την παρουσιάζουμε για την καλύτερη κατανόηση της τεχνικής που τελικά επιλέξαμε.

4.2.1. Συμμετρική Μονομερής Πιστοποίηση

Η αρχή της μονομερούς πιστοποίησης με χρήση ενός συμμετρικού αλγορίθμου απεικονίζεται στην Εικόνα 16.

Εικόνα 16. Μονομερής πιστοποίηση με χρήση συμμετρικού αλγορίθμου

Η συμμετρική μονομερής πιστοποίηση εξυπηρετεί στο να βεβαιώσει η μία συμβαλλόμενη οντότητα την αξιοπιστία της άλλης. Για να επιτευχθεί αυτό, οι δύο οντότητες πρέπει να μοιράζονται ένα μυστικό, η γνώση του οποίου πιστοποιείται από τη διαδικασία πιστοποίησης. Για λόγους σαφήνειας, υποθέτουμε πως το τερματικό επικυρώνει τον client. Αυτό σημαίνει πως το τερματικό ελέγχει αν ο client είναι αξιόπιστος. Οι ερμηνείες των συμβόλων δίνονται στην παρακάτω Εικόνα 17.

Εικόνα 17. Οι ερμηνείες των συμβόλων

Το τερματικό παράγει έναν τυχαίο αριθμό και τον στέλνει στον client. Αυτή είναι η πρόκληση. Ο client κρυπτογραφεί τον τυχαίο αριθμό που λαμβάνει, χρησιμοποιώντας ένα κλειδί που είναι γνωστό και στο τερματικό. Η ασφάλεια της διαδικασίας εξαρτάται από αυτό το κλειδί, εφόσον μόνο ο ιδιοκτήτης του μυστικού κλειδιού μπορεί να παράγει τη σωστή απάντηση. Ο client τότε επιστρέφει το αποτέλεσμα της κρυπτογράφησης στο τερματικό. Αυτή είναι η απάντηση στην πρόκληση. Το τερματικό χρησιμοποιεί το μυστικό κλειδί για να αποκρυπτογραφήσει την απάντηση και συγκρίνει το αποτέλεσμα με τον τυχαίο αριθμό που είχα αρχικά στείλει. Αν οι δύο αριθμοί είναι ίδιοι, τότε το τερματικό γνωρίζει ότι ο client είναι έγκυρος.

Αυτή η διαδικασία δεν είναι ευάλωτη σε επιθέσεις που επαναλαμβάνουν την πρόκληση ή την απάντηση που είχε αποκοπεί από κάποια προηγούμενη σύνοδο γιατί σε κάθε σύνοδο παράγεται διαφορετικός τυχαίος αριθμός. Το μοναδικό είδος επίθεσης που έχει σχετικά καλό ποσοστό επιτυχίας, είναι η συστηματική αναζήτηση του μυστικού κλειδιού. Εφόσον το ζεύγος πρόκληση-απάντηση είναι απλά ένα ζεύγος καθαρού κειμένου-κρυπτογραφήματος (plaintext-ciphertext), το μυστικό κλειδί μπορεί να βρεθεί με εξαντλητική αναζήτηση (brute-force επίθεση), που βασίζεται στον υπολογισμό όλων των πιθανών τιμών του κλειδιού.

Αν όλοι οι clients για μια δοσμένη εφαρμογή είχαν το ίδιο κλειδί και αυτό το κλειδί είχε γνωστοποιηθεί τότε το σύστημα θα ήταν μη αξιόπιστο. Προκειμένου να αποφευχθεί αυτή η πιθανότητα, κάθε client έχει το δικό του κλειδί το οποίο προκύπτει από ένα μη μυστικό χαρακτηριστικό γνώρισμά του. Αυτό το χαρακτηριστικό μπορεί να είναι ο σειριακός αριθμός του client, ο οποίος τυπώνεται στο τσιπ κατά την κατασκευή του, ή κάποιος άλλος αριθμός που είναι χαρακτηριστικός για κάθε client.

Σε αυτή την περίπτωση, το τερματικό ζητάει τον αριθμό του τσιπ από τον client προκειμένου να υπολογίσει το χαρακτηριστικό για τον client αριθμό. Ο αριθμός του τσιπ είναι ξεχωριστός για κάθε client και για το σύστημα, συνεπώς δεν υπάρχει άλλος client με τον ίδιο αριθμό. Η τιμή του χαρακτηριστικού για τον client αριθμού είναι μια συνάρτηση του αριθμού του client και του κύριου κλειδιού που είναι γνωστό στο τερματικό. Στην πραγματικότητα ένα τμήμα του αριθμού του client κρυπτογραφείται χρησιμοποιώντας το κύριο κλειδί, και το αποτέλεσμα χρησιμοποιείται ως χαρακτηριστικός αριθμός του client.

Είναι σαφές ότι αν το κύριο κλειδί υποκλαπεί, τότε ολόκληρο το σύστημα καταρρέει, εφόσον μπορούν να υποκλαπούν όλοι οι χαρακτηριστικοί αριθμοί των client μέσω του κύριου κλειδιού. Επομένως, το κύριο κλειδί πρέπει να είναι αποθηκευμένο με ασφάλεια στο τερματικό και αν είναι δυνατό να ανανεώνεται ή να διαγράφεται δυναμικά σε περίπτωση επίθεσης.

Όταν το τερματικό υπολογίσει το απαραίτητο κλειδί επικύρωσης του client, λαμβάνει χώρα η διαδικασία πρόκληση-απάντηση (challenge – response). Ο client λαμβάνει ένα τυχαίο αριθμό, τον κωδικοποιεί χρησιμοποιώντας το χαρακτηριστικό κλειδί και επιστρέφει το αποτέλεσμα στο τερματικό. Το τερματικό εκτελεί την αντίστροφη διαδικασία και συγκρίνει τα δύο αποτελέσματα. Αν ταιριάζουν, το τερματικό και ο client έχουν ένα κοινό μυστικό, το οποίο είναι το μυστικό μοναδικό κλειδί του client.

4.2.2. Συμμετρική από Κοινού πιστοποίηση

Η αρχή της από κοινού πιστοποίησης μπορεί να θεωρηθεί σαν μια διπλή μονόπλευρη πιστοποίηση. Κατά βάση, μπορούν να χρησιμοποιηθούν και δύο επιτυχείς μονομερείς διαδικασίες πιστοποίησης, μία για κάθε μέλος της επικοινωνίας ώστε από κοινού (και για τα δύο μέρη) να επιτευχθεί πιστοποίηση. Εντούτοις, ο αριθμός των υπολογισμών πρέπει να διατηρηθεί όσο το δυνατόν μικρότερος για να ελαχιστοποιηθεί ο συνολικός χρόνος που απαιτείται. Η διαδικασία αυτή αυξάνει την ασφάλεια της επικοινωνίας και είναι δυσκολότερο για έναν τρίτο να αναμιχθεί στην επικοινωνία.

Το τερματικό, προκειμένου να μπορεί να υπολογίσει το χαρακτηριστικό μυστικό κλειδί επικύρωσης του client από τον αριθμό του client, χρειάζεται τον αριθμό του client. Εφόσον λάβει τον αριθμό αυτό, υπολογίζει το χαρακτηριστικό κλειδί

επικύρωσης του client. Στη συνέχεια ζητάει έναν τυχαίο αριθμό από τον client και παράγει και αυτό έναν τυχαίο αριθμό. Το τερματικό αντιμετωπίζει τους δύο αυτούς αριθμούς, τους συνδέει και έπειτα κρυπτογραφεί τον προκύπτον αριθμό με το μοναδικό κλειδί πιστοποίησης του client. Το κρυπτογραφημένο block το αποστέλλει στον client. Στόχος της αντιμετάθεσης των δύο τυχαίων αριθμών είναι να διακριθεί η πρόκληση από την απάντηση.

Ο client μπορεί από την πλευρά της να αποκρυπτογραφήσει το λαμβανόμενο block και να ελέγξει αν ο τυχαίος αριθμός που είχε αρχικά στείλει ταυτίζεται με αυτό που πήρε ως απάντηση. Αν ταιριάζει τότε το τερματικό έχει πιστοποιηθεί για τον client. Στη συνέχεια ο client αντιμετωπίζει τους δύο τυχαίους αριθμούς και του αποστέλλει κρυπτογραφημένους πίσω στο τερματικό. Ανάλογη διαδικασία ακολουθεί το τερματικό ώστε να πιστοποιήσει τον client. Έτσι ολοκληρώνεται η αμοιβαία πιστοποίηση. Υπάρχει η δυνατότητα ο client να αποστείλει τον τυχαίο αριθμό μαζί με τον χαρακτηριστικό αριθμό προκειμένου η διαδικασία να ολοκληρωθεί πιο σύντομα.

Στην Εικόνα 17 παρουσιάζεται η από κοινού πιστοποίηση με χρήση συμμετρικού αλγορίθμου.

Εικόνα 18. Συμμετρική Πιστοποίηση με χρήση συμμετρικού αλγορίθμου

Εφόσον το σύστημα πιστοποιηθεί από το τερματικό μπορεί να αποστείλει κρυπτογραφημένα μηνύματα με το ίδιο μυστικό κλειδί ή το τερματικό να τροφοδοτήσει με νέο για περισσότερη ασφάλεια. Κατά το τέλος της επικοινωνίας το τερματικό μπορεί επίσης να ανανεώσει και το μυστικό κλειδί της κάρτας ώστε στη νέα σύνοδο να χρησιμοποιηθεί νέο-διαφορετικό μυστικό κλειδί.

4.3.Οι αλγόριθμοι του συστήματος

Όπως διαπιστώθηκε στην Παράγραφο 4.2 οι βασικές διαδικασίες ασφάλειας του client είναι η Πιστοποίηση (authentication) και η Μυστικότητα (Privacy). Οι βασικές –πολύπλοκες λειτουργίες που πρέπει να ολοκληρωθούν στο σύστημα αυτό είναι ο αλγόριθμος κρυπτογράφησης και η γεννήτρια τυχαίων αριθμών. Εκμεταλλευόμενοι

τα πλεονεκτήματα του σχεδιασμού σε υλικό μπορούμε να ενσωματώσουμε αποδοτικά συστήματα ασφαλείας σε περιορισμένων πόρων συστήματα.

Ως βασικό αλγόριθμο κρυπτογράφησης επιλέξαμε τον αλγόριθμο DES (10). Οι λόγοι που μας οδήγησαν στην παρακάτω επιλογή είναι οι περιορισμένοι απαιτούμενοι πόροι σε επιφάνεια και ισχύς, η υποστήριξη σεναρίων διαβαθμιζόμενης ασφάλειας (σενάριο λειτουργίας DES, σενάριο λειτουργίας Triple DES), υποστήριξη λειτουργίας παραγωγής τυχαίων αριθμών, ικανοποιητικά επίπεδα ασφάλειας για χαμηλού κόστους εφαρμογή. Παρακάτω παρουσιάζουμε τα βασικά στοιχεία του αλγόριθμου DES.

4.3.1. Ο αλγόριθμος κρυπτογράφησης DES

Ο αλγόριθμος κρυπτογράφησης DES κρυπτογραφεί-αποκρυπτογραφεί μπλοκ δεδομένων 64 ψηφίων και χρησιμοποιεί κλειδί 64 ψηφίων για την κρυπτογράφηση των δεδομένων. Η αντίστοιχη αποκρυπτογράφηση πρέπει να χρησιμοποιεί το ίδιο κλειδί ώστε να εξαχθεί το αρχικό καθαρό κείμενο. Ένα μπλοκ δεδομένων που πρόκειται να κρυπτογραφηθεί, αρχικά υποβάλλεται σε μια αναδιάταξη της σειράς των ψηφίων του IP, και κατόπιν σε ένα σύνθετο υπολογισμό ο οποίος εξαρτάται από το κλειδί και τελικά σε μια αναδιάταξη των ψηφίων αντίστροφης της αρχικής, IP^{-1} . Ο σύνθετος υπολογισμός, ο οποίος εξαρτάται από το κλειδί βασίζεται στην συνάρτηση κρυπτογραφίας f και στη συνάρτηση KS, η οποία είναι υπεύθυνη για τη δημιουργία του κλειδιού σε κάθε κύκλο. Ο αλγόριθμος DES ολοκληρώνεται σε 16 κύκλους. Παρακάτω στην Εικόνα 19 φαίνεται το σχηματικό διάγραμμα του βασικού τμήματος του αλγορίθμου.

Εικόνα 19. Οι 16 κύκλοι για τη δημιουργία του κρυπτογραφημένου μπλοκ στον αλγόριθμο DES

Οι μετασχηματισμοί IP και IP^{-1} οι οποίοι βρίσκονται στην αρχή και στο τέλος του αλγορίθμου έχουν αντίστοιχα εισόδους των 64 και 56 ψηφίων και εξόδους των 56 και 64 ψηφίων. Η IP αποτελεί αναδιάταξη των ψηφίων στην είσοδο ενώ η IP^{-1} είναι ο αντίστοιχος αντίστροφος μετασχηματισμός. Σε κάθε κύκλο του αλγορίθμου εφαρμόζεται το κλειδί του κύκλου K_i το οποίο δίνεται από τη σχέση $K_n = KS(n, KEY)$. Όπου το K_n καθορίζεται από 48 διαφορετικές θέσεις των ψηφίων του μπλοκ KEY . Παρακάτω θα δούμε τη συνάρτηση KS η οποία παράγει τα 48 ψηφίων μπλοκ K_n .

Το μπλοκ της εισόδου μετά από την αρχική αναδιάταξη είναι LR σε κάθε κύκλο του αλγορίθμου έχουμε τις παρακάτω σχέσεις:

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

Η συνάρτηση $f(R, K)$ δίνεται στην παρακάτω Εικόνα 20. Η E είναι μια συνάρτηση η οποία λαμβάνει μπλοκ των 32 ψηφίων και στην έξοδο αποδίδει μπλοκ των 48 ψηφίων. Οι συναρτήσεις $S1$ έως $S8$ είναι τα λεγόμενα Sbox του αλγορίθμου DES. Κάθε ένα έχει είσοδο 6 ψηφίων και αποδίδει στην έξοδο 4 ψηφία σύμφωνα με τους πίνακες που υπάρχουν στο πρότυπο του DES. Η συνάρτηση P αποτελεί μετασχηματισμό αναδιάταξης με είσοδο και έξοδο 32 ψηφίων.

Εικόνα 20. Η συνάρτηση $f(R, K)$

Το K_n με $1 \leq n \leq 16$ αποτελεί ένα μπλοκ 48 ψηφίων το οποίο παίρνει διαφορετική τιμή ανά κύκλο του αλγορίθμου. Η συνάρτηση που συνδέεται με το K_n είναι η KS.

Εικόνα 21. Η παραγωγή των κλειδιών (KS) για κάθε κύκλο του αλγορίθμου DES

Οι συναρτήσεις PC 1 και PC 2 ονομάζονται πίνακες Permutation Choice. Οι C_n , D_n καθορίζονται από ένα πίνακα όπου κάθε κύκλο ορίζει τις κυκλικές αριστερές ολισθήσεις σε σχέση με την προηγούμενη κατάσταση.

4.3.2. Ο αλγόριθμος κρυπτογράφησης TDES

Ο αλγόριθμος κρυπτογράφησης TDES έλαβε το όνομά του από τα αρχικά των λέξεων Triple Data Encryption Standard. Ορισμένες φορές συναντάται και ως ο αλγόριθμος TDEA (33). Ο TDEA είναι συμμετρικός αλγόριθμος κρυπτογραφίας εγκεκριμένος από τη NIST. Ο απλός αλγόριθμος DES χρησιμοποιείται για την υλοποίηση του TDES και ο τελευταίος αποτελεί μια σύνθετη διαδικασία της DES κρυπτογράφησης. Για το λόγο αυτό παρέχει περισσότερη ασφάλεια από τον DES.

Ας θεωρηθεί ότι τα $E_K(I)$ και $D_K(I)$ αναπαριστούν αντίστοιχα την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων I χρησιμοποιώντας το κλειδί K . Η διαδικασία κρυπτογράφησης αποκρυπτογράφησης TDES είναι μια σύνθετη διαδικασία κρυπτογράφησης αποκρυπτογράφησης DES.

1. Διαδικασία Κρυπτογράφησης TDES: Ο μετασχηματισμός ενός μπλοκ I 64 ψηφίων, σε ένα μπλοκ O 64 ψηφίων, καθορίζεται ως εξής:

$$O = E_{K3}(D_{K2}(E_{K1}(I)))$$

2. Διαδικασία Αποκρυπτογράφησης TDES: Ο μετασχηματισμός ενός μπλοκ I 64 ψηφίων, σε ένα μπλοκ O 64 ψηφίων, καθορίζεται ως εξής:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

Το πρότυπο καθορίζει τους ακόλουθους τρόπους διαμόρφωσης για τα κλειδιά (K_1 , K_2 , K_3). Τα K_1 , K_2 , K_3 μπορεί να είναι ανεξάρτητα κλειδιά, μπορεί $K_3 = K_1$ και $K_1 = K_2 = K_3$.

Εικόνα 22. Η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης TDES

4.3.3. Η γεννήτρια τυχαίων αριθμών PRNG ANSI X9.17

Το πρότυπο ANSI X9.17 (34) ενσωματώνει τη λειτουργία TDES για την παραγωγή τυχαίων αριθμών. Ως εισόδους χρησιμοποιεί το seed T_i το οποίο εξαρτάται από το χρόνο και προέρχεται από πραγματικό ρολόι ή διέγερση του χρήστη. V_o αποτελεί μυστικό 64-bit seed. Το T είναι timestamp.

$$R_i = E_K(E_K(T_i) \oplus V_i),$$

$$V_{i+1} = E_K(E_K(T_i) \oplus R_i)$$

Στην παρακάτω Εικόνα 23 παρουσιάζεται η γεννήτρια τυχαίων αριθμών X.9.17

Εικόνα 23. Η γεννήτρια τυχαίων αριθμών X9.17

4.4.Σχεδιασμός σε Υλικό Ολοκληρωμένου Συστήματος

Στην Εικόνα 24 παρουσιάζονται οι βασικές εισοδοι και έξοδοι του συστήματος. Το σήμα Operation Mode καθορίζει το σενάριο λειτουργίας του συνολικού συστήματος. Τα βασικά σενάρια λειτουργίας είναι 3. Mode-1, όπου το σύστημα κρυπτογραφεί-αποκρυπτογραφεί δεδομένα υποστηρίζοντας τη λειτουργία DES, Mode-2, όπου το σύστημα υποστηρίζει τη λειτουργία TDES, και Mode-3 όπου το σύστημα παράγει τυχαίους αριθμούς. Τα Plaintext/Ciphertext και Ciphertext/Plaintext είναι η είσοδος και έξοδος του συστήματος για τα μπλοκ δεδομένων, καθαρό κείμενο ή κρυπτογραφημένο. Οι εισοδοι T_i και V_i χρησιμοποιούνται ως εισοδοι για τη δημιουργία του τυχαίου αριθμού R_i .

Εικόνα 24. Οι βασικές εισοδοι και έξοδοι του συστήματος

Σύμφωνα με τις παραγράφους 4.2 και 4.3 όλο το σύστημα ασφάλειας, Πιστοποίηση και Μυστικότητα μπορεί να στηριχτεί πάνω στον αλγόριθμο κρυπτογράφησης DES. Το γεγονός αυτό περιορίζει την καταλυπτόμενη επιφάνεια του συστήματος σημαντικά. Επιπλέον εξαιτίας των υψηλών ρυθμών μετάδοσης που επιτυγχάνουμε με

την ολοκλήρωση των αλγορίθμων σε υλικό μπορούμε να χρησιμοποιήσουμε τη μέθοδο της ανάδρασης για το σχεδιασμό του DES αλγορίθμου, ολοκληρώνοντας μόνο έναν από του δεκάξι κύκλους του αλγορίθμου σε συνεργασία με μια μονάδα ελέγχου. Στην Εικόνα 25 φαίνεται η προτεινόμενη αρχιτεκτονική για το σύστημα Πιστοποίησης και Μυστικότητας.

Εικόνα 25. Η προτεινόμενη αρχιτεκτονική του συστήματος ασφαλείας

Στην Εικόνα 25 βλέπουμε το εσωτερικό του συστήματος που παρουσιάζεται στην Εικόνα 24. Η Control Unit σε συνδυασμό με τους πολυπλέκτες του συστήματος παίρνουν αποφάσεις για την πορεία που θα έχουν τα δεδομένα μέσα στο κύκλωμα. Στα Mux1 και Mux2 είναι ολοκληρωμένες και οι IP , IP^{-1} συναρτήσεις οι οποίες εφαρμόζονται στην αρχή και στο τέλος του αλγορίθμου DES και TDES.

Κατά τη λειτουργία του αλγορίθμου DES το κύκλωμα εξάγει το αποτέλεσμα μετά από 16 κύκλους του αλγορίθμου, ενώ κατά τη διάρκεια του TDES, εξάγει το αποτέλεσμα μετά από $3 \cdot 16 = 48$ κύκλους του αλγορίθμου. Όταν το σύστημα λειτουργεί για την παραγωγή τυχαίου αριθμού απαιτούνται $48 \cdot 3 + 3 = 147$ κύκλοι.

Προκειμένου να μειωθεί η κατανάλωση ισχύος του αλγορίθμου εισάγουμε εσωτερικά στο βασικό του κύκλο καταχωρητές. Και ενεργοποιούμε όλους τους καταχωρητές του συστήματος μόνο όταν απαιτείται να αποκτήσουν ή να μεταφέρουν δεδομένα. Η

τεχνική αυτή έχει ως αποτέλεσμα ο κάθε κύκλος να απαιτεί 6 κύκλους ρολογιού και να αυξηθεί η επιφάνεια του συνολικού συστήματος.

Το αποτέλεσμα είναι αισθητή μείωση της κατανάλωσης ισχύος του συστήματος και ο αλγόριθμος DES να απαιτεί 96 κύκλους, ο TDES 288 κύκλους ενώ η RNG 867 κύκλους ρολογιού. Η καταναλισκόμενη ισχύς υπολογίζεται χρησιμοποιώντας τους εκτιμητές κατανάλωσης ισχύος «XILINX power tools estimators» (33) για FPGA τεχνολογία και το Xpower εργαλείο. Στην Εικόνα 26 παρουσιάζεται η λογική για την απομόνωση των μη λειτουργικών μονάδων του συστήματος.

Εικόνα 26. Η προτεινόμενη αρχιτεκτονική της τεχνολογίας gated clock

Τα αποτελέσματα εξομοίωσης του προτεινόμενου συστήματος παρουσιάζονται στον παρακάτω Πίνακα 4. Παρουσιάζονται και τυπικές τιμές απόδοσης του συστήματος για συχνότητα λειτουργίας 5MHz.

Πίνακας 4: Αποτελέσματα Εξομοίωσης

FPGA DEVICE	XILINX (v100epq240)
Fun. Generat.	411
CLB Slices	418
Dffs	311
Frequency	80 MHz
Throughput f=5MHz	$F \cdot 64 / 96 = 3.3 \text{ Mbps}$
	$F \cdot 64 / 288 = 1.11 \text{ Mbps}$
	$F \cdot 64 / 867 = 0.36 \text{ Mbps}$

Στον Πίνακα 5 παρουσιάζεται η σύγκριση από πλευράς κατανάλωσης ισχύος των δύο διαφορετικών προσεγγίσεων. Η συχνότητα της τυπικής προσέγγισης είναι τέσσερεις φορές μικρότερη από την προτεινόμενη εξαιτίας των ενδιάμεσων καταχωρητών. Αν και έχουμε βάλει περισσότερα επίπεδα καταχωρητών η μείωση της καθυστέρησης δεν είναι η αντίστοιχη εξαιτίας του χρόνου που απαιτείται ώστε να ενεργοποιηθεί ο καταχωρητής (setup time). Παρατηρούμε μείωση στην κατανάλωση ισχύος σε σχέση με την τυπική αρχιτεκτονική.

Πίνακας 5: Σύγκριση των δύο τεχνικών

Proposed	Clbs activated	D flip flops activated	Est. Power	Frequency
Cycle1	42	83	22 mW	F1
Cycle2	124	124	26 mW	
Cycle3	54	76	21 mW	
Cycle4	17	33	16 mW	
Cycle5	33	65	20 mW	
Cycle6	33	65	20 mw	
Conventional	310	88	76 mW	F1/4

4.5.Συμπεράσματα

Ο σκοπός τους σχεδιασμού του συστήματος ασφάλειας του client ήταν η δημιουργία ενός συστήματος αποδοτικού ώστε οι επικοινωνία να διεξάγεται γρήγορα με μειωμένη κατανάλωση ισχύος και περιορισμένους πόρους. Επομένως ο σχεδιασμός ακολούθησε και υιοθέτησε τους παρακάτω κανόνες:

- Το συνολικό σύστημα πρέπει να καταναλώνει μικρή περιοχή. Οπότε υπάρχει ανάγκη προσεχτικής διαχείρισης των συστατικών μερών του. Σχεδιαστικές μέθοδοι όπως η ανατροφοδότηση και η κοινή χρήση υλικού πρέπει να υιοθετηθούν
- Εξαιτίας της περιορισμένης επιφάνειας του συστήματος η συνολική χωρητικότητά του είναι περιορισμένη.
- Το σύστημα πρέπει να κάνει προσεχτική διαχείριση της ισχύος του-ενέργειας. Για συστήματα όπως οι έξυπνες κάρτες όπου δεν ενσωματώνεται μπαταρία, αλλά αποσπούν ενέργεια από το ηλεκτρομαγνητικό πεδίο, η απαίτηση αυτή είναι επιτακτική.
- Ο ρυθμός απόδοσης του client είναι μια παράμετρος που μπορεί να «θυσιαστεί» εξαιτίας των μικρών απαιτήσεων σε μεταφορά δεδομένων/δευτερόλεπτο.
- Οι απαιτήσεις σε ασφάλεια βασίζονται στην πιστοποίηση – ταυτοποίηση του client από ένα τερματικό και στην κρυπτογράφηση δεδομένων.

Για τους λόγους αυτούς, οι ακόλουθες σχεδιαστικές τεχνικές χρησιμοποιήθηκαν κατά το σχεδιασμό του συστήματος του client.

- Οι αλγόριθμοι κρυπτογραφίας DES, TDES και η γεννήτρια τυχαίων αριθμών βασίζεται στον αλγόριθμο κρυπτογραφίας DES.
- Πιο συγκεκριμένα όλο το πρωτόκολλο κρυπτογράφησης βασίζεται σε ένα γύρο του αλγορίθμου DES με αποτέλεσμα και οι τρεις ρουτίνες να μοιράζονται το περιορισμένης επιφάνειας κύκλο του DES.

Με τις δύο παραπάνω τεχνικές η επιφάνεια του κυκλώματος μειώνεται αισθητά.

Επιπλέον χρησιμοποιήθηκαν οι τεχνικές:

- Gated clock τεχνική ώστε να απενεργοποιούνται τα μέρη του συστήματος στα οποία δεν υπάρχει δραστηριότητα. Μειώνεται η κατανάλωση ισχύος αποτελεσματικά.
- Παράλληλα μείωση ανεπιθύμητων φορτίσεων εκφορτίσεων (glitch reduction) τεχνική ώστε να φιλτράρονται οι ανεπιθύμητες μεταδόσεις των σημάτων εσωτερικά του συστήματος.

ΚΕΦΑΛΑΙΟ 5. Βελτιστοποίηση δομικών κρυπτογραφικών πράξεων για συστήματα περιορισμένων πόρων

Στο κεφάλαιο αυτό θα αναφερθούμε στη διαδικασία βελτιστοποίησης τριών δομικών κρυπτογραφικών πράξεων, του πολλαπλασιασμού σε πεπερασμένα σώματα (Finite Fields) που χρησιμοποιείται κυρίως στα κρυπτογραφικά συστήματα δημοσίου κλειδιού και σε δύο δομικές μονάδες του αλγορίθμου συμμετρικής κρυπτογραφίας AES, το Subbytes/InvSubBytes μετασχηματισμό και το MixColumn/InvMixColumns μετασχηματισμό.

5.1.Εισαγωγή

Όπως έχουμε αναφέρει, κάθε αλγόριθμος κρυπτογραφίας εμπεριέχει υπολογιστικά μη αποδοτικές πράξεις-μετασχηματισμούς. Το κόστος σε επιφάνεια, καθυστέρηση και κατανάλωση ισχύος είναι βασικά χαρακτηριστικά που πρέπει να λάβει υπόψη ο σχεδιαστής πριν ολοκληρώσει και ενσωματώσει τις αριθμητικές πράξεις αυτές στο σύστημα. Η διαδικασία αυτή ονομάζεται profiling και έχει σκοπό την αναγνώριση των δύσκολων τμημάτων του αλγορίθμου. Τα εργαλεία profiling εντοπίζουν τις υπολογιστικά δύσκολες πράξεις του αλγορίθμου, τις πιο συνηθισμένες ακολουθίες πράξεων που εμφανίζονται στον αλγόριθμο και δίνουν μια πρώτη εκτίμηση των τμημάτων που πρέπει να υλοποιηθούν σε υλικό- βελτιστοποιηθούν.

Οι χαρακτηρισμένες πολύπλοκες κρυπτογραφικές πράξεις πρέπει έπειτα να περάσουν στο στάδιο της βελτιστοποίησης επιφάνειας, ισχύος, απόδοσης ή κατάλληλο συνδυασμό αυτών των παραμέτρων ανάλογα με την τρέχουσα εφαρμογή. Η βελτιστοποίηση αυτή θα αποφέρει μεγάλο κέρδος στην συνολική αποδοτικότητα του αλγορίθμου. Η διαδικασία αυτή ακολουθείται στο σχεδιασμό ειδικού σκοπού συνόλων εντολών (Application Specific Instruction Set Processors - ASIPs) (9), (36). Παρακάτω αναφέρουμε τρεις προτεινόμενες αρχιτεκτονικές οι οποίες είναι βελτιστοποιημένες για κρυπτογραφικά συστήματα χαμηλών πόρων.

5.2.Προτεινόμενη αρχιτεκτονική σειριακού πολλαπλασιαστή σε πεπερασμένα σώματα $GF(2^m)$

Ο υψηλός ρυθμός απόδοσης του πολλαπλασιασμού σε πεπερασμένα σώματα $GF(2^m)$ αποτελεί σημαντικό θέμα στα αριθμητικά συστήματα εξαιτίας της ποικιλίας εφαρμογών όπου εμπεριέχεται, όπως η κρυπτογραφία, η ανίχνευση σφαλμάτων και γενικότερα στα αριθμητικά προβλήματα της επιστήμης των υπολογιστών. Η απόδοση του πολλαπλασιαστή εξαρτάται άμεσα από τον αριθμό των απαιτούμενων κύκλων ρολογιού για να εξαχθεί το αποτέλεσμα και την καθυστέρηση (critical path) - συχνότητα του κυκλώματος. Στους περισσότερους σειριακούς πολλαπλασιαστές $GF(2^m)$ δεν επιτυγχάνεται να μειωθεί ο αριθμός των απαιτούμενων κύκλων (κάτω από τον αριθμό m) για να εξαχθεί το αποτέλεσμα, χωρίς παράλληλα να αυξηθεί δραματικά η καθυστέρηση του κυκλώματος. Η αύξηση αυτή είναι ιδιαίτερα σημαντική όταν ο πολλαπλασιαστής σχεδιάζεται ώστε να είναι ευέλικτος (versatile),

δηλαδή να υποστηρίζει πολλαπλασιασμό μέχρι m ψηφίων (όπου m ο μέγιστος αριθμός των ψηφίων που μπορεί να επεξεργαστεί ο πολλαπλασιαστής). Στο Κεφάλαιο αυτό, προτείνεται ένας νέος versatile σειριακός MSB (Most Significant Bit) πολλαπλασιαστής για πεπερασμένα σώματα $GF(2^m)$ ο οποίος επιτυγχάνει 50 % αύξηση κατά μέσο όρο στο ρυθμό απόδοσης όταν συγκρίνεται με τυπικές αρχιτεκτονικές σειριακών πολλαπλασιαστών, με κόστος μικρή αύξηση της καθυστέρησης του κυκλώματος και της επιφάνειας. Η βελτίωση αυτή επιτυγχάνεται με κατά 33.4 % μείωση των απαιτούμενων κύκλων ρολογιού ώστε να εξαχθεί το αποτέλεσμα. Η προτεινόμενη αρχιτεκτονική μπορεί να διαχειριστεί δεδομένα μέχρι και μήκους m ψηφίων και είναι κατάλληλη για εφαρμογές όπου το πεδίο δεν είναι σταθερό. Η ελάττωση των απαιτούμενων κύκλων του αλγορίθμου προκαλεί ταυτόχρονη μείωση της καταναλισκόμενης ενέργειας του συστήματος, της ενέργειας δηλαδή που απαιτείται για να ολοκληρωθεί ο πολλαπλασιασμός.

5.3.Γενικά για τους πολλαπλασιαστές σε πεπερασμένα πεδία $GF(2^m)$

Η αριθμητική σε πεπερασμένα σώματα $GF(2^m)$ είναι ένα πολύ χρήσιμο εργαλείο για μαθηματικές εφαρμογές υπολογιστών όπως οι κώδικες διόρθωσης λάθους και τα συστήματα κρυπτογράφησης δημοσίου κλειδιού (37), (38), (39). Σε αυτές τις εφαρμογές, ο πολλαπλασιασμός $GF(2^m)$ διαδραματίζει βασικό ρόλο στον τελικό υπολογισμό. Εντούτοις, αυτή η λειτουργία είναι υψηλού κόστους από πλευράς καλυπτόμενης επιφάνειας, χρονικής πολυπλοκότητας, ισχύος και συνολικής ενέργειας και εκτεταμένη έρευνα έχει γίνει στο σχεδιασμό μικρής επιφάνειας, χαμηλής κατανάλωσης ισχύος και υψηλής ταχύτητας πολλαπλασιαστών (40), (41).

Τα στοιχεία ενός $GF(2^m)$ πεδίου μπορούν να αναπαρασταθούν χρησιμοποιώντας διάφορους τύπους βάσεων. Κυρίως, υπάρχουν τρεις κοινοί τύποι βάσης, Πολυωνυμική Βάση, (Polynomial Basis SB/PB), Normal Basis (NB) και Dual Basis (DB). Για τον αποδοτικό υπολογισμό του αριθμητικού πεδίου χρησιμοποιούμε γενικά Normal Basis ή Polynomial Basis (42) (43).

Η Πολυωνυμική βάση αναπαράστασης των στοιχείων του πεδίου $GF(2^k)$ είναι της μορφής $\{1, x, x^2, \dots, x^{m-1}\}$ όπου το x είναι ρίζα ενός ανάγωγου (irreducible) πολυωνύμου $F(x)$, βαθμού m με συντελεστές που ανήκουν στο πεπερασμένο σώμα $GF(2)$. Όταν χρησιμοποιείται αναπαράσταση πολυωνυμικής βάσης, κάθε στοιχείο του πεπερασμένου σώματος $GF(2^m)$ μπορεί να εκφραστεί ως ένα δυαδικό πολυώνυμο βαθμού $m-1$, και ο πολλαπλασιασμός των στοιχείων συντελείται με modulo το ανάγωγο πολυώνυμο $F(x)$ (44). Διαφορετικοί τύποι αρχιτεκτονικών για τον πολυωνυμικό πολλαπλασιασμό βάσης πεπερασμένων σωμάτων $GF(2^m)$ έχουν προταθεί όπως σειριακοί (bit-serial), digit-serial, παράλληλοι.

Οι παράλληλοι πολλαπλασιαστές εκτελούν το $GF(2^m)$ πολλαπλασιασμό σε σταθερό αριθμό κύκλων (ανεξάρτητου και μικρότερου του m), έχουν όμως πολύ υψηλή πολυπλοκότητα επιφάνειας (43), (45), (46), (47). Ο λόγος αυτός κάνει τη χρήση των παράλληλων πολλαπλασιαστών σε χαμηλά συστήματα πόρων, όπως στις κρυπτογραφικές εφαρμογές, μη ρεαλιστική λόγω των μεγάλων απαιτήσεων σε υλικό (44). Οι αρχιτεκτονικές σειριακού πολλαπλασιαστή προσφέρουν ένα δίκαιο λόγο απόδοσης/επιφάνειας και είναι περιορισμένοι σε απαιτήσεις επιφάνειας και ισχύος

(48), (49), (50), (51). Εντούτοις, απαιτούν τουλάχιστον m τους κύκλους ρολογιού για να υπολογίσουν ένα αποτέλεσμα πολλαπλασιασμού. Οι Digital-Serial/parallel αρχιτεκτονικές ωφελούνται και από τη διαβάθμιση στην απόδοση και από μια λογική αύξηση στους καλυπτόμενους πόρους του υλικού έναντι της σειριακής προσέγγισης (44), (52), (53), (54), (55), (56). Ταιριάζουν καλύτερα στις εφαρμογές όπου απαιτείται ένα σταθερό μέγεθος λέξης για την αναπαράσταση στοιχείων.

Η επιλογή του ανάγωγου πολυωνύμου $F(x)$ μπορεί να επηρεάσει την απόδοση ενός πολλαπλασιαστή πεπερασμένων σωμάτων $GF(2^m)$. Για παράδειγμα, η χρησιμοποίηση των ανάγωγων πολυωνύμων με πολύ λίγους διαφορετικούς από το μηδέν συντελεστές (π.χ., τριώνυμα ή πεντώνυμα) μπορεί να προσφέρει σημαντικές βελτιστοποιήσεις από άποψη επιφάνειας, ισχύος, ταχύτητας και ενέργειας (43), ειδικά για τις παράλληλες αρχιτεκτονικές πολλαπλασιαστών. Εντούτοις, αυτή η λύση σχεδιασμού οδηγεί σε $GF(2^m)$ πολλαπλασιαστές που πραγματοποιούνται για συγκεκριμένα ανάγωγα τριώνυμα ή πεντώνυμα για σταθερή τάξη m . Αυτοί οι πολλαπλασιαστές δεν μπορούν να επαναχρησιμοποιηθούν για $GF(2^m)$ πράξεις διαφορετικής τάξης και διαφορετικού ανάγωγου πολυώνυμου.

Ένα πρόσθετο ζήτημα στο σχεδιασμό των κλασικών αρχιτεκτονικών πολλαπλασιαστών πεπερασμένων σωμάτων $GF(2^m)$ είναι η μη ικανότητά τους να υποστηρίζουν τα μεγέθη πεδίων μικρότερα από αυτά που σχεδιάστηκαν αρχικά (50). Ορίζουμε ως versatile (ευέλικτους) (44) τους πολλαπλασιαστές που σχεδιάζονται για έναν συγκεκριμένο $GF(2^m)$ πεδίο με δεδομένη τάξη m , και μπορούν επίσης να εκτελέσουν τους πολλαπλασιασμούς για όλα τα $GF(2^n)$ πεπερασμένα σώματα, όπου $1 < n \leq m$. Οι ευέλικτοι $GF(2^m)$ πολλαπλασιαστές έχουν πλεονέκτημα ότι μπορούν να επαναχρησιμοποιηθούν σε συστήματα υποστηρίζοντας περισσότερα από ένα $GF(2^m)$ πεπερασμένα σώματα, εξοικονομώντας επιπρόσθετο υλικό και προσφέροντας ευελιξία. Πιο συγκεκριμένα, αντί της χρήσης ενός $GF(2^n)$ πολλαπλασιαστή για κάθε $GF(2^n)$ πεπερασμένο σώμα που χρησιμοποιείται σε ένα σύστημα, ένας ευέλικτος (2^m) πολλαπλασιαστής GF , όπου το m είναι η μέγιστη τάξη των διαφορετικών τιμών n του πεπερασμένου σώματος, μπορεί να επαναχρησιμοποιηθεί για όλο το εύρος πεπερασμένων σωμάτων. Οι ευέλικτοι $GF(2^m)$ πολλαπλασιαστές μπορούν να χρησιμοποιηθούν εκτεταμένα σε κρυπτογραφικά συστήματα όπου το πεπερασμένο σώμα σχετίζεται με το επίπεδο ασφάλειας το οποίο προσφέρεται, τη χρονική πολυπλοκότητα και την κατανάλωση ισχύος του κρυπτογραφικού συστήματος (57).

Προτείνουμε μια νέα αρχιτεκτονική για σειριακούς MSB πολλαπλασιαστές πεπερασμένων σωμάτων χρησιμοποιώντας γενικά ανάγωγα πολυώνυμα, η οποία βελτιώνει την απόδοση του συστήματος σε σχέση με τον τυπικό πεπερασμένου σώματος $GF(2^m)$ πολλαπλασιαστή κατά 50%. Η προτεινόμενη αρχιτεκτονική είναι ευέλικτη και μπορεί να επεξεργαστεί οποιοδήποτε αριθμό ψηφίων μέχρι την τιμή m . Εκμεταλλευόμαστε τους κύκλους του αλγορίθμου πολλαπλασιασμού χωρίς εσωτερική δραστηριότητα και επιτυγχάνουμε αποδοτικά να μειώσουμε τον αριθμό των κύκλων. Δημιουργώντας το κατάλληλο και ρεαλιστικό σενάριο εξομοίωσης αποδεικνύουμε την πιο πιθανή μείωση στην τιμή των κύκλων λειτουργίας του αλγορίθμου. Το αποτέλεσμα είναι ο αριθμός των κύκλων να μειωθεί κατά 33.4% αυξάνοντας την απόδοση κατά 50%. Η προτεινόμενη αρχιτεκτονική μαζί με την τυπική αρχιτεκτονική σειριακού πολλαπλασιαστή $GF(2^m)$ πεπερασμένων πεδίων υλοποιήθηκε σε υλικό και σε τεχνολογία FPFA και η απόδοσή τους μετρήθηκε για διάφορα σενάρια κύκλων λειτουργίας του αλγορίθμου. Το κόστος μας σε επιφάνεια σε σχέση με την τυπική αρχιτεκτονική μετρήθηκε με μέτρο το απόδοση/επιφάνεια. Αποδεικνύεται πειραματικά πως το κόστος της επιπρόσθετης επιφάνειας είναι πολύ

μικρότερο σε σχέση με το κέρδος μας σε απόδοση, ενώ η συνολική ενέργεια για να ολοκληρωθεί ο κάθε πολλαπλασιασμός είναι αντίστοιχα μειωμένη.

5.4. Πολλαπλασιασμός σε Πολυωνυμική Βάση

5.4.1. Μαθηματικό Υπόβαθρο

Ένα πεδίο με πεπερασμένο αριθμό στοιχείων καλείται πεπερασμένων σωμάτων (Finite Fields) και συμβολίζεται με F_q ή $GF(q)$, όπου το q αντιπροσωπεύει τον αριθμό στοιχείων στο πεδίο. Όταν το q είναι πρώτη δύναμη, δηλ. $q = p^m$, το πεπερασμένο σώμα $GF(p^m)$ καλείται σώμα επέκτασης (extension field). Το σώμα επέκτασης $GF(p^m)$ παράγεται χρησιμοποιώντας το m βαθμό του ανάγωγου πολυωνύμου στο $GF(p)$. Επομένως, σε πολυωνυμική αναπαράσταση τα στοιχεία στο $GF(p^m)$ αναπαριστώνται από τα πολυώνυμα βαθμού $m-1$ με συντελεστές στο $GF(p)$.

Επομένως, ένα στοιχείο a στο $GF(2^m)$ ορίζεται ως εξής:

$$A(x) = \sum_{i=0}^{m-1} a_i x^i = a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \dots + a_1 x + a_0, \text{ όπου οι συντελεστές } a_i \in GF(2)$$

ορίζονται πάνω από το ανάγωγο πολυώνυμο της μορφής

$$F(x) = x^m + \sum_{i=0}^{m-1} f_i x^i = x^m + f_{m-1} x^{m-1} + f_{m-2} x^{m-2} + \dots + f_1 x + f_0.$$

Οι συντελεστές ενός στοιχείου a του $GF(2^m)$ πεδίου μπορούν να αναπαρασταθούν με ένα διάνυσμα της μορφής $A = (a_{m-1} a_{m-2} \dots a_1 a_0)$.

Η πρόσθεση των στοιχείων A και B σε $GF(2^m)$ εκτελείται προσθέτοντας τα πολυώνυμα $A(x)$ και $B(x)$, όπου οι συντελεστές προστίθενται στο πεπερασμένο σώμα $GF(2^m)$. Η πράξη αυτή είναι ισοδύναμη με την XOR πράξη για τα διανύσματα A και B .

Ο πολλαπλασιασμός σε πεπερασμένα σώματα $GF(2^m)$ εκτελείται χρησιμοποιώντας αναπαράσταση πολυωνυμικής βάσης, για τα στοιχεία a και b και προκύπτει από τον παρακάτω υπολογισμό:

$$C(x) = A(x) \cdot B(x) \bmod F(x)$$

όπου $C(x)$ είναι το πολυώνυμο βαθμού $m-1$, συμβολίζει ένα στοιχείο $C \in GF(2^m)$. Έτσι, ο πολλαπλασιασμός πάνω σε $GF(2^m)$ πεδία συντελείται από τον πολλαπλασιασμό των αντιστοίχων πολυωνύμων modulo το ανάγωγο πολυώνυμο $F(x)$.

5.4.2. MSB σειριακός πολλαπλασιαστής πεπερασμένων σωμάτων $GF(2^m)$

Έστω ότι θέλουμε να πολλαπλασιάσουμε τα παρακάτω πολυώνυμα στα πεπερασμένα σώματα $GF(2^m)$:

$$A(x) = a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \dots + a_1 x + a_0 \text{ με } a_i \in GF(2) \text{ και } 0 \leq i \leq m-1$$

και $B(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots + b_1x + b_0$ με $b_i \in GF(2)$ και $0 \leq i \leq m-1$

Το reduction πολυώνυμο ορίζεται ως το ανάγωγο πολυώνυμο χωρίς το x^m να συνεισφέρει και έχει την παρακάτω μορφή:

$$R(x) = r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \dots + r_1x + r_0 \text{ με } r_i = f_i \in GF(2) \text{ και } 0 \leq i \leq m-1.$$

Ο πολλαπλασιασμός μπορεί να βασιστεί σε μια επαναληπτική διεργασία ακολουθώντας τον παρακάτω επαναληπτικό αλγόριθμο (39), όπου η συνάρτηση $leftshift(C)$ αναπαριστά μια αριστερή ολίσθηση ενός bit:

INPUT: $A = (a_{m-1}, \dots, a_1, a_0), B = (b_{m-1}, \dots, b_1, b_0)$ και reduction πολυώνυμο $R = (r_{m-1}, \dots, r_1, r_0)$ όπου $a_i, b_i, r_i \in GF(2), 0 \leq i \leq m-1$

OUTPUT: $C = A \cdot B$, with $C = (c_{m-1}, \dots, c_1, c_0)$ με συντελεστές, $c_i \in GF(2)$.

1. Set $C \leftarrow 0$.
2. For i from $m-1$ down to 0 do:
 - a. $C \leftarrow leftshift(C) + c_{m-1}R$
 - b. $C \leftarrow C + b_iA$

Return (C)

Στην Εικόνα 27, παρουσιάζεται η ροή των δεδομένων κατά την πράξη του σειριακού MSB πολλαπλασιασμού $GF(2^m)$. Κάθε μονάδα λειτουργεί πάνω σε m ψηφία εύρος. Η αρχική τιμή του **Intermediate Result** στοιχείου είναι μηδέν. Το τελευταίο (αριστερό) ψηφίο του Intermediate Result καθορίζει αν το ανάγωγο πολυώνυμο θα δεχτεί την πράξη XOR με το Intermediate Result ώστε να παραχθεί το αποτέλεσμα Result A. Η XOR πράξη του Multiplicand με το Result A καθορίζεται από την τιμή του πιο σημαντικού ψηφίου bit του Multiplier. Το αποτέλεσμα στην έξοδο αποτελεί το νέο Intermediate Result. Το Intermediate Result αποθηκεύεται στο Shift Register και εκτελεί ενός ψηφίου αριστερή ολίσθηση των δεδομένων σε κάθε κύκλο ρολογιού. Το αποτέλεσμα προκύπτει σε m κύκλους ρολογιού.

Εικόνα 27: Η ροή των δεδομένων για τον MSB $GF(2^m)$ πολλαπλασιασμό

5.5.Τυπική αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$

Σε αυτό το σημείο παρουσιάζεται, η τυπική αρχιτεκτονική MSB σειριακού πολλαπλασιαστή πεπερασμένων σωμάτων $GF(2^m)$. Μια σύντομη ανάλυση του πολλαπλασιαστή δίνεται με σκοπό να παρουσιαστούν οι βασικές καινοτομίες της προτεινόμενης δουλειάς. Η τυπική αρχιτεκτονική δίνεται ως ευέλικτη (versatile) σε $GF(2^m)$ πεπερασμένα σώματα. Με άλλα λόγια, το σύστημα μπορεί να υποστηρίξει οποιονδήποτε πολλαπλασιασμό μεταξύ πολυωνύμων σε οποιοδήποτε από τα $GF(2^n)$ πεπερασμένα σώματα για $1 < n \leq m$. Στην Εικόνα 28 παρουσιάζεται η τυπική αρχιτεκτονική MSB σειριακού πολλαπλασιαστή:

Εικόνα 28: Τυπική αρχιτεκτονική του MSB σειριακού πολλαπλασιαστή σε $GF(2^m)$

Το σύστημα αυτό αποτελείται από δύο καταχωρητές m ψηφίων, Register A και Register R. Ο καταχωρητής Register A αποθηκεύει τους συντελεστές του πολυωνύμου $A(x)$ και ο καταχωρητής Register R αποθηκεύει τους συντελεστές του ανάγωγου πολυωνύμου $R(x)$. Οι συντελεστές του πολυωνύμου $B(x)$ αποθηκεύονται στον m -ψηφίων καταχωρητή ολίσθησης Shift Register B. Η τιμή των δεδομένων για κάθε θέση i σε κάθε καταχωρητή συμβολίζεται ως $A(i)$, $B(i)$, $C(i)$ ή $R(i)$ αντιστοίχως. Το κύριο υπολογιστικό τμήμα του συστήματος έχει ολοκληρωθεί εσωτερικά των m κελιών (Cells). Σε κάθε κύκλο ρολογιού, οι τιμές του Intermediate Result καταχωρητή (Εικόνα 27) τα οποία αποθηκεύονται στα m κελιά, ολισθαίνουν κατά 1 ψηφίο αριστερά. Η επόμενη τιμή του κάθε εσωτερικού καταχωρητή του κελιού "Internal Register of Cell_(i)" καθορίζεται από τις εισόδους του $A(i)$ πολλαπλασιαστέου, $B(m-1)$ πολλαπλασιαστή, $R(i)$ ανάγωγου πολυωνύμου και τη $C'(m-1)$ τιμή. Η τιμή του $C'(m-1)$ σήματος καθυστερεί ένα γύρο ρολογιού (Reg1) πριν μεταδοθεί εσωτερικά στα m κελιά του συστήματος σύμφωνα με τις προδιαγραφές του αλγορίθμου. Η διεργασία απαιτεί m κύκλους ρολογιού για να ολοκληρωθεί.

Το σύστημα μπορεί να γίνει ευέλικτο εισάγοντας μονάδα ελέγχου. Αν τα πολυώνυμα $A(x)$, $B(x)$ και $R(x)$ ορίζονται στο $GF(2^n)$ πεδίο όπου $1 < n \leq m$ τότε μόνο τα κελιά του συστήματος $C_{(m-1)}$ έως $C_{(m-n)}$ θα χρησιμοποιηθούν για την $GF(2^n)$ πράξη πολλαπλασιασμού. Η μονάδα ελέγχου θέτει σε τιμή ίση με το μηδέν τα υπόλοιπα $(m-n)$ ψηφία του καταχωρητή A (Register A) (bits $A(m-n-1)$ to $A(0)$), του καταχωρητή R (Register R) (bits $R(m-n-1)$ to $R(0)$) και του καταχωρητή ολίσθησης B (Shift Register B ($\leftarrow$)) (bits $B(m-n-1)$ to $B(0)$). Τα $(m-n)$ σήματα του καταχωρητή A (Register A) και του καταχωρητή R (Register R) δεν προκαλούν καμιά δραστηριότητα στα εσωτερικά κελιά. Επομένως τα n κελιά (cells) ($C_{(m-1)}$ to $C_{(m-n)}$) τα οποία συνεισφέρουν στην πράξη καλούνται ενεργά (active) κελιά. Τα $(m-n)$ κελιά ($C_{(m-n-1)}$ έως $C_{(0)}$) τα οποία δεν λαμβάνουν χώρα στις πράξεις καλούνται μη ενεργά (inactive). Μετά από n κύκλους ρολογιού, η μονάδα ελέγχου θέτει το σήμα control_2 signal στη τιμή 1, με σκοπό να μαρκάρει το τέλος της πράξης πολλαπλασιασμού και το αποτέλεσμα βρίσκεται στα out(i) ψηφία.

Σε κάθε κελί, τρεις βασικές λειτουργίες μπορούν να σημειωθούν. Η πρώτη (Cell mode=0) χαρακτηρίζει ένα κελί, το οποίο είναι το πρώτο ενεργό κατά την λειτουργία. Επιπροσθέτως, τα μη ενεργά κελιά τα οποία έχουν είσοδο 0, βρίσκονται σε mode=0. Η κατάσταση Cell mode = 1 χαρακτηρίζει ένα ενεργό κελί, όπου αναγωγή εφαρμόζεται και δεν είναι το πρώτο ενεργό κελί. Η κατάσταση Cell mode=2 χαρακτηρίζει ένα ενεργό κελί όπου η αναγωγή δεν εφαρμόζεται ($R(i)=0$).

Αν το κελί Cell_(i) λειτουργεί σε mode = 0 (η input(i) του Cell_(i) γίνεται μηδέν) ή σε κατάσταση mode = 1, 2 ορίζεται από το σήμα control_1 signal. Οι καταστάσεις Mode 1 και 2 έχουν τις ίδιες ρυθμίσεις (όπου control_1 signal = '1') και η έξοδος του κελιού Cell_(i-1) μεταδίδεται στο Cell_(i). Οι καταστάσεις Mode 1, 2 ξεχωρίζουν από την είσοδο $R(i)$. Αν $R(i) = '1'$, το Cell_(i) λειτουργεί σε mode='1' και αν $R(i) = '0'$, το κελί Cell_(i) λειτουργεί σε mode='2'. Όταν ένα κελί λειτουργεί σε mode = '2' η αρχιτεκτονική του μπορεί να απλοποιηθεί παραβλέποντας μία AND πύλη και μία XOR πύλη. Αν γίνουν όμως αυτές οι απλοποιήσεις το σύστημα παύει να υποστηρίζει ευέλικτες πράξεις. Τα κελιά τα οποία δεν χρησιμοποιούνται δεν συνεισφέρουν ούτε στην καθυστέρηση του συστήματος ούτε στην κατανάλωση ισχύος (mode = 0).

Εικόνα 29: Η εσωτερική δομή του κελιού

Στην Εικόνα 29, η εσωτερική δομή του κελιού $Cell_{(i)}$ παρουσιάζεται. Οι βασικές είσοδοι του κελιού $Cell_{(i)}$ είναι τα σήματα εισόδων $A(i)$, $B(m-1)$, $R(i)$, το $C(m-1)$ το οποίο καθυστερεί κατά ένα κύκλο ρολογιού ($C'(m-1)$) και η έξοδος $output(i)$. Υπάρχουν επίσης οι rst και clk είσοδοι για το 1-bit εσωτερικό καταχωρητή (Register) του $Cell_{(i)}$.

Η αρχιτεκτονική του τυπικού ευέλικτου MSB σειριακού πολλαπλασιαστή $GF(2^m)$ έχει καθυστέρηση $T = 2 \cdot T_{XOR} + T_{AND}$, όπου T_{AND} είναι η καθυστέρηση της AND πύλης και T_{XOR} είναι η καθυστέρηση της XOR πύλης, και χρησιμοποιεί $3m$ AND πύλες, $2m$ XOR πύλες και $4m + 1$ bit καταχωρητή. Το σύστημα απαιτεί m κύκλους ρολογιού μέχρι να εξάγει το αποτέλεσμα.

5.6. Προτεινόμενη αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$

Η προτεινόμενη αρχιτεκτονική σειριακού πολλαπλασιασμού MSB $GF(2^m)$ αποτελεί βελτιστοποιημένη έκδοση της τυπικής αρχιτεκτονικής η οποία παρουσιάστηκε στο στην παράγραφο 5.5 και βασίζεται στην εκμετάλλευση των κύκλων μη δραστηριότητας κατά την διεργασία του πολλαπλασιασμού. Στην προτεινόμενη αρχιτεκτονική προβλέπουμε ενδιάμεσες πράξεις οι οποίες δε θα γίνουν. Σαν αποτέλεσμα οι πράξεις αυτές μπορούν να παραληφθούν χωρίς να εκτελεστούν (omitted rounds). Επομένως, ο απαιτούμενος χρόνος – κύκλοι αλγορίθμου ώστε να βγει το αποτέλεσμα μειώνεται.

Παράδειγμα 1: Υποθέτουμε ότι θέλουμε να πολλαπλασιάσουμε τα πολυώνυμα $A(x)$ και $B(x)$ στο πεπερασμένο σώμα $GF(2^4)$:

Τα $A(x) = x^3 + 1$ και $B(x) = x$ είναι τα πολυώνυμα στο $GF(2^4)$ τα οποία ορίζονται στο ανάγωγο πολυώνυμο $R(x) = x^4 + x^3 + x^2 + x + 1$. Θέλουμε να βρούμε το Γινόμενο

μεταξύ των πολωνύμων $A(x)$ και $B(x)$ που δηλώνεται ως $C(x)$.

Το πολώνυμο A σε μορφή διανύσματος αναπαριστάνεται ως **1001** και το πολώνυμο B σε **0010**, ενώ η τιμή αποθηκεύεται στον καταχωρητή R , που προκύπτει από το $R(x)$, είναι **1111**. Σύμφωνα με τον αλγόριθμο που παρουσιάστηκε για την τυπική αρχιτεκτονική πολλαπλασιαστή, χρειαζόμαστε $m = 4$ κύκλους ώστε να υπολογιστεί το αποτέλεσμα. Η διεργασία του πολλαπλασιασμού παρουσιάζεται με λεπτομέρεια παρακάτω:

Κύκλος 1: (IR: Intermediate Result)

$i=3$

a. $IR = \text{leftshift}(IR) + IR(3) \cdot r(x) \Rightarrow \text{"0000"} \text{ XOR } (\text{"0"} \text{ AND } \text{"1111"}) \Rightarrow IR = \text{"0000"}.$

b. $IR = IR + B(i) \cdot A \Rightarrow \text{"0000"} \text{ XOR } (B(3) \text{ AND } A) \Rightarrow IR = \text{"0000"}.$

Κύκλος 2:

$i=2$

a. $IR = \text{leftshift}(IR) + IR(3) \cdot r(x) \Rightarrow \text{"0000"} \text{ XOR } (\text{"0"} \text{ AND } \text{"1111"}) \Rightarrow IR = \text{"0000"}.$

b. $IR = IR + B(i) \cdot A \Rightarrow \text{"0000"} \text{ XOR } (B(2) \text{ AND } A) \Rightarrow IR = \text{"0000"}.$

Κύκλος 3:

$i=1$

a. $IR = \text{leftshift}(IR) + IR(3) \cdot r(x) \Rightarrow \text{"0000"} \text{ XOR } (\text{"0"} \text{ AND } \text{"1111"}) \Rightarrow IR = \text{"0000"}.$

b. $IR = IR + B(i) \cdot A \Rightarrow \text{"0000"} \text{ XOR } (B(1) \text{ AND } A) \Rightarrow IR = \text{"1001"}.$

Κύκλος 4:

$i=0$

a. $IR = \text{leftshift}(IR) + IR(3) \cdot r(x) \Rightarrow \text{"0010"} \text{ XOR } (\text{"1"} \text{ AND } \text{"1111"}) \Rightarrow IR = \text{"0010"} \text{ XOR } \text{"1111"} \Rightarrow IR = \text{"1101"}.$

b. $IR = IR + B(i) \cdot A \Rightarrow \text{"1101"} \text{ XOR } (B(0) \text{ AND } A) \Rightarrow IR = \text{"0111"}, \text{ the final result.}$

Στην τυπική αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$ μπορούν να εφαρμοστούν οι παραπάνω διαπιστώσεις. Επομένως ένας διαφορετικός ευέλικτος σειριακός πολλαπλασιαστής μπορεί να προταθεί στην Εικόνα 30. Η πρόβλεψη των παραλειπόμενων κύκλων γίνεται με τη χρήση μιας NOR πύλης. Η πύλη αυτή συνδέεται μέσω ενός καταχωρητή (reg2) στα PASS συστατικά μέρη. Τα PASS συστατικά μέρη ελέγχουν την εσωτερική δομή των δεδομένων του κυκλώματος.

Μπορούμε να ορίσουμε δύο καταστάσεις λειτουργίας του κυκλώματος. Την κατάσταση λειτουργίας όπου συμβαίνουν παραλείψεις κύκλων και την κατάσταση που δε συμβαίνουν παραλείψεις. Η κατάσταση όπου δε συμβαίνουν παραλείψεις καλείται «mode = ORDINARY» και η κατάσταση όπου συμβαίνουν καλείται «mode = OMISSION».

Τα σήματα $Cell_{(m-1)}$ και $B(m-2)$ του καταχωρητή ολίσθησης Register B ($\leftarrow$) είναι είσοδοι της NOR πύλης και ελέγχονται. Αν η έξοδος της NOR πύλης (con) είναι 1 τότε στον επόμενο κύκλο το σύστημα θα λειτουργήσει στην κατάσταση mode = OMISSION. Κατά τη διάρκεια της mode = OMISSION, συμβαίνει μία παραπάνω ολίσθηση αριστερά στο κύκλο ρολογιού στα δεδομένα του $Cell_{(i)}$ και τα δεδομένα από το κελί $Cell_{(i-1)}$ περνάνε στο $Cell_{(i+1)}$, παραβλέποντας οποιαδήποτε πράξη μπορούσε να συμβεί στο κελί $Cell_{(i)}$. Ο κύκλος όπου $B(m-1) = 0$ και $C(m-1) = 0$ αντιπροσωπεύεται από την 1 bit αριστερά ολίσθηση. Όταν βρίσκεται το σύστημα στην κατάσταση mode = OMISSION, τα δεδομένα του καταχωρητή ολίσθησης B ολισθαίνουν δύο θέσεις αριστερά, με αποτέλεσμα να παραβλέπεται το $B(i-1)$ μηδενικό ψηφίο.

Στην Εικόνα 31, τα δεδομένα μεταξύ δύο γειτονικών κελιών παρουσιάζονται. Το σύστημα λειτουργεί στην κατάσταση mode = ORDINARY χωρίς να συμβαίνει παράλειψη στους κύκλους. Τα δεδομένα τα οποία έρχονται από το κελί $Cell_{(i-2)}$ χρησιμοποιούνται ως είσοδο στο κελί $Cell_{(i-1)}$ και η τιμή του εσωτερικού καταχωρητή $R(i-1)$ Register ανανεώνεται. Η πορεία των δεδομένων, όταν το σύστημα βρίσκεται στην κατάσταση mode = ORDINARY, παρουσιάζεται στην Εικόνα 31 με έντονη μαύρη γραμμή. Στον ίδιο κύκλο ρολογιού, οι τιμές οι οποίες αποθηκεύονται στο $R(i-1)$ είναι η είσοδος του κελιού $Cell_{(i)}$. Οι διακεκομμένες γραμμές (wire) είναι μη ενεργές και δεν περνάει πάνω από αυτές πληροφορία. Σε κάθε $Cell_{(i)}$ μια διεργασία process(i) λαμβάνει χώρα. Οι διακεκομμένες γραμμές δεν περιλαμβάνονται στην διεργασία.

Εικόνα 31: Η ροή των δεδομένων μεταξύ δύο γειτονικών κελιών για mode=ORDINARY

Η ροή των δεδομένων μεταξύ δύο γειτονικών κελιών του συστήματος, όταν βρίσκεται το σύστημα σε κατάσταση mode = OMISSION φαίνεται στην Εικόνα 32. Σε αυτήν την περίπτωση, για κάθε καταχωρητή Register $R(i-1)$ του κελιού $Cell_{(i-1)}$, τα δεδομένα διαπερνούν μέσω του κελιού $Cell_{(i)}$ και αποθηκεύονται στο καταχωρητή $R(i+1)$. Κάθε κελί $Cell_{(i)}$ υποστηρίζει δύο παράλληλες διεργασίες. Τα δεδομένα, περνούν μέσω του κελιού $Cell_{(i)}$ (FIRST PART OF PROCESS (i)), που αντιστοιχεί στην ολίσθηση κατά ένα ψηφίο του παραλειπόμενου κύκλου και η διεργασία στο κελί $Cell_{(i+1)}$ (SECOND PART OF PROCESS(i)) αντιστοιχεί στον επόμενο κύκλο που ακολουθεί. Αυτές οι δύο διεργασίες απαιτούν ένα κύκλο λειτουργίας.

Εικόνα 32: Η ροή των δεδομένων μεταξύ δύο γειτονικών κελιών για mode=OMISSION

5.7. Πολιτική Ελέγχου της Ροής Δεδομένων

Στην Εικόνα 33, ο σχεδιασμός του PASS δομικού στοιχείου παρουσιάζεται.

Εικόνα 33: Το δομικό στοιχείο PASS

Το PASS συστατικό στοιχείο χρησιμοποιείται για την μετάδοση και έλεγχο των δεδομένων μεταξύ των κελιών του συστήματος και μεταξύ των καταχωρητών ενός ψηφίου του καταχωρητή ολίσθησης B. Το con σήμα μέσω ενός ψηφίου καταχωρητή είναι συνδεδεμένο με τα συστατικά στοιχεία PASS. Εάν con = '1' (Εικόνα 34 d), στον επόμενο κύκλο το σήμα a με την έξοδο out1 και η έξοδος out2 παίρνει τιμή ίση με το '0'. Εάν con = '0' (Εικόνα 34 c), στον επόμενο κύκλο το σήμα a συνδέεται με την έξοδο out2 και το σήμα b περνάει στην έξοδο out1. Τα Pass δομικά στοιχεία ελέγχονται απευθείας από την έξοδο της NOR πύλης. Η ολίσθηση κατά δύο κύκλους παρουσιάζεται στην Εικόνα 34a, b. Στην Εικόνα 33, ο Shift Register B παρουσιάζεται.

Εικόνα 34: Shift Register κατάσταση (a) πριν και (b) μετά την παράλειψη κύκλου και οι δύο καταστάσεις (c) και (d) του PASS δομικού στοιχείου

Η έξοδος της NOR πύλης (con) είναι επίσης συνδεδεμένη με το εξωτερικό περιβάλλον (control unit). Όταν $con = 0$, τότε ένα εξωτερικό σύστημα αυξάνει την εσωτερική του τιμή κατά 1. Όταν $con = 1$, τότε το εξωτερικό σύστημα αυξάνει την εσωτερική του τιμή κατά 2. Για κάθε $GF(2^n)$ πολλαπλασιασμό, όταν η εσωτερική τιμή του συστήματος φτάνει την n τιμή, τότε το εξωτερικό σύστημα διαβάζει την έξοδο του συστήματος.

5.8.Ανάλυση της απόδοσης του προτεινόμενου συστήματος

Με σκοπό να βρεθεί μία μέση τιμή των κύκλων που παραλείπονται κατά μέσο όρο, το προτεινόμενο σύστημα μοντελοποιήθηκε σε περιβάλλον Mathematica (58). Η διαδικασία εξομοίωσης έχει τα παρακάτω χαρακτηριστικά:

- Πολλαπλασιαστές A: Τυχαίο Πολυώνυμο
- Πολλαπλασιαστής B: Τυχαίο Πολυώνυμο
- Irreducible Πολυώνυμο R: Τυχαίο ανάγωγο πολυώνυμο

Κατά το σενάριο εξομοίωσης, το σύστημα δοκιμάστηκε σε τιμές από 100-bit στα 250-bit για πεπερασμένα σώματα $GF(2^m)$ με βήμα 1 (101, 102,...250) χρησιμοποιώντας τυχαία πολυώνυμα A και B και τυχαίο ανάγωγο πολυώνυμο για το R. Σε κάθε περίπτωση του σεναρίου (π.χ. $m=140$) το σύστημα ελέγχτηκε 100 φορές με διαφορετικές τιμές για τα A, B, R πολυώνυμα και η μέση τιμή των παραλήψεων για κάθε τάξη βρέθηκε. Εξαιτίας της υπολογιστικής πολυπλοκότητας ο αλγόριθμος εξομοιώθηκε για τις τιμές 100-250. Το χαρακτηριστικό της ευελιξίας (versatility) του συστήματος δεν επηρεάζει την παραπάνω μεθοδολογία μετρήσεων. Η τυχειότητα των $B(m-2)$ και $Cell(m-1)$ τιμών bit, τα οποία είναι υπεύθυνα για την εκτίμηση της κατάστασης του συστήματος, δεν επηρεάζονται από την n τιμή του πεπερασμένου

σώματος $GF(2^n)$, όπου $0 < n \leq m$ εφόσον $B(m-1)$ έως $B(m-n)$ και $Cell(m-1)$ έως $Cell(m-n)$ κρατούν τις απαραίτητες πληροφορίες για κάθε $GF(2^n)$ πεδίο.

Στην Εικόνα 35, η μέση τιμή των % παραλήψεων για κάθε τάξη πεπερασμένου σώματος παρουσιάζεται. Ο άξονας των X παρουσιάζει τον αριθμό των ψηφίων και ο Y άξονας παρουσιάζει την μέση τιμή των % παραλήψεων. Παρατηρείται πως το σύστημα λειτουργεί περίπου σε 33,4 % στην κατάσταση $mode = OMISSION$ και επομένως περίπου 66,4 % σε κατάσταση $mode = ORDINARY$. Για κάθε παράληψη, το σύστημα παραβλέπει ένα κύκλο, επομένως το προτεινόμενο σύστημα παρουσιάζει περίπου 33,4 % λιγότερους κύκλους λειτουργίας (μέση τιμή). Αυτή η κατάσταση εμφανίζεται με τη μεγαλύτερη πιθανότητα όταν ο αριθμός των παραλήψεων κυμαίνεται από 0 % έως 50 % των συνολικών κύκλων ρολογιού.

Εικόνα 35: Το ποσοστό % των κύκλων που παραλείπονται κατά μέσο όρο

Η καθυστέρηση (critical path) της τυπικής αρχιτεκτονικής είναι $l_1 = 2T_{XOR} + T_{AND}$ ενώ η καθυστέρηση για την προτεινόμενη είναι $l_2 = 2T_{XOR} + T_{MUX}$. Επομένως, η απόδοση των δύο αρχιτεκτονικών εκφράζεται αντιστοίχως από τις παρακάτω σχέσεις:

$$P_1 = \frac{N_{bits} \cdot \frac{1}{l_1}}{m_{clock_cycles}} \text{ and } P_2 = \frac{N_{bits} \cdot \frac{1}{l_2}}{m'_{clock_cycles}}, \text{ όπου } m'_{clock_cycles} = m_{clock_cycles} - n_{omitted_rounds} \text{ και}$$

$n_{omitted_rounds}$ είναι οι κύκλοι σε $mode=omission$. Όπως φαίνεται στην Εικόνα 34, $m'_{clock_cycles} = 0.664m_{clock_cycles}$ κατά μέσο όρο, γεγονός που δηλώνει ότι η προτεινόμενη αρχιτεκτονική απαιτεί 33.4 % λιγότερους κύκλους από αυτούς της τυπικής αρχιτεκτονικής. Η καθυστέρηση που εισάγει ο 2 προς ένα πολυπλέκτης T_{MUX} είναι μικρή αφού αυτό το συστατικό στοιχείο μπορεί να υλοποιηθεί σε υλικό σαν απλό lookup table σε FPGAs ή σαν pass transistor - transmission gate σε ASICs. Επομένως η καθυστέρηση των δύο αρχιτεκτονικών είναι περίπου η ίδια η ίδια.

Για περαιτέρω απόδειξη των παραπάνω, και οι δύο αρχιτεκτονικές περιγράφηκαν από τη γλώσσα περιγραφής VHDL και συνθέθηκαν σε 2V1000bg575 Virtex 2 XILINX FPGA τεχνολογία για πεπερασμένα σώματα $GF(2^m)$ ($m=100$, $m=200$, $m=400$, $m=570$). Τα αποτελέσματα παρουσιάζονται αναλυτικά στον Πίνακα 6. Η

καθυστέρηση της τυπικής αρχιτεκτονικής σε όλες τις περιπτώσεις του m που μετρήθηκε είναι πολύ κοντά στην καθυστέρηση της προτεινόμενης αρχιτεκτονικής. Για την ακρίβεια, στην περίπτωση $m = 100$ η καθυστέρηση της προτεινόμενης αρχιτεκτονικής ήταν 1,48 % περισσότερη από αυτή της τυπικής, για $m = 200$ αυτό το ποσοστό είναι 1,48 %, για $m = 400$ είναι 1,36 % και για $m = 570$ είναι 1,11%. Γενικότερα συμπεραίνουμε ότι εφόσον η διαφορά στο critical path l_1 και l_2 είναι λιγότερη από 1,5 % μπορεί να θεωρηθεί ότι $l_1 \approx l_2$. Σε αυτήν την περίπτωση, έχουμε

$$P_2 = \frac{1}{0.664} P_1 = 1.5 P_1. \text{ Η απόδοση της προτεινόμενης αρχιτεκτονικής είναι περίπου}$$

50% υψηλότερη κατά μέσο όρο. Ο λόγος $1/(CLB*Latency)$ φαίνεται στον Πίνακα 6. Με αυτό τον τρόπο γίνεται εκτίμηση της βελτιστοποίησης που συντελείται. Ο λόγος αυτός είναι για την περίπτωση της προτεινόμενης αρχιτεκτονικής 36% υψηλότερος.

Πίνακας 6: Σύγκριση Τυπικής με Προτεινόμενης Αρχιτεκτονικής

Τυπικός MSB-σειριακός πολλαπλασιαστής							
Μήκος Πράξης	Συχνότητα (MHz)	Critical path (ns)	Latency(ns) (average case)	Επιφάνεια (Clb)	D flip flops	$1/(CLB*Latency)$	Απόδοση (Mbps) (average case)
m=100	204 MHz	4,901	490,1	188	102	$1,0853*10^{-5}$	204
m=200	201 MHz	4,975	995	380	204	$2,644*10^{-6}$	201
m=400	198 MHz	5,05	2020	752	407	$6,58 *10^{-7}$	198
m=570	188 MHz	5,31	3026,7	1058	579	$3,12 *10^{-7}$	188
Προτεινόμενος MSB σειριακός πολλαπλασιαστής							
Μήκος Πράξης	Συχνότητα (MHz)	Critical path (ns)	Latency(ns) (average case)	Επιφάνεια (Clb)	D flip flops	$1/(CLB*Latency)$	Απόδοση (Mbps) (average case)
m=100	201MHz	4,975	331,335	204	104	$1,48*10^{-5}$	300
m=200	199 MHz	5,05	672,66	407	206	$3.65* 10^{-6}$	297
m=400	195 MHz	5,12	1364	813	409	$9.01 *10^{-7}$	291
m=570	186 MHz	5,37	2032,43	1158	581	$4.24*10^{-7}$	277.5

Η διαφοροποίηση στην απόδοση της προτεινόμενης αρχιτεκτονικής εξαρτάται από τον αριθμό των παραλειπόμενων κύκλων και παρουσιάζεται στην Εικόνα 36. Οι τιμές της απόδοσης υπολογίζονται χρησιμοποιώντας τις P_1 και P_2 εξισώσεις για τις περιπτώσεις όπου δεν υπάρχουν παραλειπόμενοι κύκλοι (proposed worst case), μέση τιμή (33,4% of total rounds) παραλειπόμενων κύκλων (proposed-mean values) και μέγιστη τιμή παραλειπόμενων (50% of total rounds) (proposed-best case). Ενώ η απόδοση του συστήματος για την χειρότερη περίπτωση είναι περίπου η ίδια με την τυπική αρχιτεκτονική, και είναι πολύ χειρότερη σε σχέση με την καλύτερη περίπτωση. Όμως η προτεινόμενη καλύτερη περίπτωση και η χειρότερη είναι σχεδόν απίθανο να συμβούν. Όπως φαίνεται από τα αποτελέσματα εξομοίωσης το πιο συχνό σενάριο παραλείψεων είναι 33,4%. Σε αυτήν την περίπτωση, η απόδοση είναι ακόμη υψηλότερη σε σχέση με την τυπική αρχιτεκτονική όπως φαίνεται στην Εικόνα 36.

Εικόνα 36: Συγκρίσεις απόδοσης τυπικής και προτεινόμενης αρχιτεκτονικής για $m=100, 200, 400, 570$

Προκειμένου να υπογραμμιστούν τα οφέλη της προτεινόμενης αρχιτεκτονικής και να αξιολογηθεί η αύξηση της επιφάνειας δε σχέση με την απόδοση καθορίζουμε το μέτρο απόδοση/καταλειπτομενη επιφάνεια. Στην Εικόνα 37, παρουσιάζεται η αναλογία ρυθμού απόδοσης/επιφάνεια για τα διάφορα m . Διαπιστώνεται ότι η προτεινόμενη αρχιτεκτονική επιτυγχάνει καλύτερο ρυθμό απόδοσης για την ίδια περιοχή κατά μέσο όρο 36%.

Εικόνα 37: Συγκρίσεις απόδοσης/επιφάνεια τυπικής και προτεινόμενης αρχιτεκτονικής για $m=100, 200, 400, 570$

5.9. Συγκρίσεις με άλλες εργασίες

Τα βασικά πλεονεκτήματα της προτεινόμενης αρχιτεκτονικής είναι:

- Versatile Σχεδιασμός
- Εκτέλεση του πολλαπλασιασμού σε 0.334 m κύκλους cycles λιγότερο σε σχέση με τις τυπικές σειριακές προσεγγίσεις.
- Μικρή καθυστέρηση, χαμηλοί πόροι

Τα παραπάνω χαρακτηριστικά καθιστούν το κύκλωμα κατάλληλο για χαμηλών πόρων εφαρμογές. Σε αυτά τα συστήματα η απόδοση εξαρτάται από τον αριθμό των κύκλων που απαιτούνται. Η απόδοση δεν απαιτείται από την συχνότητα (critical path) γιατί η συχνότητα καθορίζεται από την εφαρμογή (π.χ. μια τυπική συχνότητα λειτουργίας για τα συστήματα έξυπνων καρτών είναι μόνο 5 MHz).

Η επιφάνεια, η καθυστέρηση, ο απαιτούμενος χρόνος για να εξαχθεί το αποτέλεσμα παρουσιάζονται στον Πίνακα 7 μαζί με αποτελέσματα από παρόμοιες εργασίες ώστε να γίνουν συγκρίσεις.

Στην εργασία (50), προτείνεται ένας ευέλικτος επαναπροσδιορίσιμος σειριακός MSB πολλαπλασιαστής για $GF(2^m)$ πεπερασμένα σώματα επιτυγχάνοντας υψηλή ευελιξία και χαμηλή πολυπλοκότητα υλικού. Σε αυτόν τον πολλαπλασιαστή, πολλοί αποπολυπλέκτες ενσωματώνονται μαζί με τα περιορισμένα σήματα ρολογιών προκειμένου να επιλεγεί ποια βασικά κύτταρα του πολλαπλασιαστή θα είναι ενεργά ή όχι. Τα ανωτέρω συστατικά ρυθμίζονται από μια χωριστή μονάδα ελέγχου που δεν εμπεριέχεται στο προτεινόμενο σύστημα. Το ανάγωγο πολυώνυμο R και ο πολλαπλασιαστής A εισάγονται στα n λιγότερα σημαντικά ψηφία των καταχωρητών. Αυτή η προσέγγιση είναι διαφορετική από αυτήν που προτείνεται στην εργασία μας, όπου όλοι οι τελεστές εισάγονται στα n περισσότερα σημαντικά ψηφία των καταχωρητών. Κατά συνέπεια στην (50) η επικοινωνία του πολλαπλασιαστή με το εξωτερικό περιβάλλον είναι άμεση ενώ μια επιπλέον ολίσθηση ίσως χρειάζεται (ανάλογα με το σύστημα που χρησιμοποιεί τον πολλαπλασιαστή). Και στους δύο πολλαπλασιαστές υποτίθεται ότι γνωρίζουμε τον αριθμό του πεδίου n (n τιμή) και στο μεταξύ αυτή η επιπλέον ολίσθηση θα έχει πολύ μικρό κόστος σε σχέση με τον επιπλέον έλεγχο που απαιτείται από την εργασία (50). Ο προτεινόμενος πολλαπλασιαστής της εργασίας (50) καταλαμβάνει επιπλέον επιφάνεια εξαιτίας της εξωτερικής μονάδας ελέγχου και επιπλέον ο συνολικός χρόνος για να υπολογίσει τα δεδομένα (latency) καθώς και η καθυστέρηση (critical path) είναι μεγάλοι. Η αρχιτεκτονική μας είναι καλύτερη σε σχέση με τη (50), στο συνολικό χρόνο που απαιτείται για τον υπολογισμό και το κόστος σε επιφάνεια είναι περίπου το ίδιο.

Στην εργασία (59), ένας ευέλικτος σειριακός πολλαπλασιαστής ο οποίος μπορεί να υποστηρίξει οποιοδήποτε bit-serial ανάγωγο πολυώνυμο παρουσιάζεται. Αυτό το σχήμα προτάθηκε επίσης για το σχεδιασμό παράλληλων πολλαπλασιαστών και συστήματα πολλαπλασιασμού-διαίρεσης. Ο πολύπλοκος τρόπος υποστήριξης του ευέλικτου πολλαπλασιασμού έχει ως αποτέλεσμα ο πολλαπλασιαστής να έχει μικρή συχνότητα και να απαιτείται χρόνος ώστε να εξαχθεί το αποτέλεσμα. Η αρχιτεκτονική μας πλεονεκτεί στον αριθμό των flip flops που απαιτούνται ενώ σε

σύγκριση με τα άλλα στοιχεία επιφάνειας τα αποτελέσματα είναι παρόμοια.

Η εργασία Kim et al (60) προτείνει αρχιτεκτονική πολλαπλασιαστή/ύψωση στο τετράγωνο για πεπερασμένα σώματα $GF(2^m)$ που εκτελεί πολλαπλασιασμό και ύψωση στο τετράγωνο με κοινή λογική, ταυτόχρονα. Η αρχιτεκτονική αυτή δεν είναι ευέλικτη. Το προτεινόμενο μας σύστημα επιτυγχάνει πολύ καλύτερα αποτελέσματα σε επίπεδο κόστους επιφάνειας. Η καθυστέρηση της προτεινόμενης αρχιτεκτονικής μας είναι ελαφρώς μεγαλύτερη όμως η συνολική καθυστέρηση (latency) είναι μικρότερη.

Πίνακας 7: Σύγκριση με άλλες εργασίες

Πολλαπλασιαστές	Hasan (59)	Kitsos (50)	Kim (60)	Προτεινόμενη
2-input AND	$3m$	$2m$	$3m$	$3m$
2-input XOR	$2m$	m	$3m$	$2m$
3-input XOR	0	0	0	0
2-input OR	0	$m - 1$	0	0
1-bit latch	m^2	$3m$	$14m$	$4m + 2$
mux	m	0	$3m$	$2m$
demux	0	m	0	0
Καθυστέρηση (Critical Path)	$XOR + \lceil \log_2 m \rceil (AND + NOT + OR)$	$2AND + XOR + NOT + (m + 1)OR$	$AND + XOR + MUX$	$2XOR + MUX$
Συνολική καθυστέρηση (Latency)	$3m$	m	$3m$	$(0.664)m$
Versatile (yes/no)	Yes	yes	no	yes

5.10. Συμπεράσματα σχετικά με την προτεινόμενη αρχιτεκτονική MSB σειριακού πολλαπλασιαστή $GF(2^m)$

Σε αυτήν την εργασία ο σχεδιασμός μιας νέας ευέλικτης αρχιτεκτονικής σειριακού MSB πολλαπλασιαστή $GF(2^m)$ πεδία προτείνεται. Η προτεινόμενη αρχιτεκτονική έχει βελτιωμένη απόδοση σε σχέση με την τυπική αρχιτεκτονική κατά 50 %. Επιπλέον αντίστοιχη μείωση της απαιτούμενης συνολικής ενέργειας ώστε να εξαχθούν τα αποτελέσματα επιτυγχάνεται. Ο προτεινόμενος σχεδιασμός μπορεί να λειτουργήσει για οποιοδήποτε πράξη μήκους μέχρι m (όπου m ο μέγιστος αριθμός των bits που μπορεί να επεξεργαστεί) και βρίσκει εφαρμογή κυρίως σε κρυπτογραφικές εφαρμογές. Στις κρυπτογραφικές εφαρμογές, side channel attacks (SCA) μπορούν να εφαρμοστούν αν χρησιμοποιηθεί το στοιχείο της μεταβλητής συνολικής καθυστέρησης που εισάγεται για να ολοκληρωθεί η πράξη. Αν η πληροφορία εισαχθεί στον πολλαπλασιαστέο A και όχι στον πολλαπλασιαστή B , εφόσον το A δεν επηρεάζει τους κύκλους ρολογιού που απαιτούνται για την εκτέλεση. Στις κρυπτογραφικές εφαρμογές όπου ο προτεινόμενος πολλαπλασιαστής χρησιμοποιείται ως μέρος ενός μεγαλύτερου συστήματος όπως οι Ελλειπτικές Καμπύλες, η διαφοροποίηση στους κύκλους μπορεί να θεωρηθεί πολύ μικρή. Ο SCA επιτιθέμενος μπορεί να μετρήσει μόνο την είσοδο και την έξοδο του συστήματος ενώ τα μέτρα κατά των επιθέσεων SCA (61), (5), (62) λαμβάνονται σε υψηλότερο επίπεδο.

5.11. Σχεδιασμός του κρυπτογραφικού μετασχηματισμού SubBytes/InvSubBytes (Sbox) για συστήματα χαμηλών πόρων

Οι πιο γνωστές υλοποιήσεις της πράξης SubBytes/InvSubBytes του Advanced Encryption Standard (15) έχουν σκοπό στο να περιοριστούν οι πόροι σε επιφάνεια του κυκλώματος ή στο να επιτευχθεί υψηλή απόδοση, χωρίς να υπάρχουν προσεγγίσεις πάνω στο θέμα της μείωσης της κατανάλωσης ισχύος. Από την άλλη πλευρά, είναι εμφανής η ανάγκη για εφαρμογές χαμηλής κατανάλωσης ισχύος σε περιορισμένης επιφάνειας κυκλώματα, ειδικά για φορητά (ασύρματα)-χαμηλών πόρων συστήματα. Σε αυτό το κεφάλαιο προτείνονται χαμηλής κατανάλωσης ισχύος αρχιτεκτονικές σε περιορισμένους πόρους επιφάνειας για το δομικό κρυπτογραφικό στοιχείο του Advanced Encryption Standard Subbytes/InvSubBytes (Sbox). Οι προτεινόμενες αρχιτεκτονικές υποστηρίζουν την πράξη της κρυπτογράφησης και της αποκρυπτογράφησης. Στις προτεινόμενες αρχιτεκτονικές διατηρώντας μικρή την επιφάνεια, τεχνικές για χαμηλή κατανάλωση ισχύος εφαρμόζονται, όπως αναδιάταξη των επιμέρους στοιχείων του κυκλώματος, εισαγωγή επιπλέον υλικού για ισοστάθμιση των μονοπατιών μετάδοσης του σήματος, μείωση δυνατότητας οδήγησης των δομικών στοιχείων με την αντικατάστασή τους, εισαγωγή καταχωρητών για αποφυγή ανεπιθύμητων φορτίσεων/εκφορτίσεων (glitches). Επομένως, οι προτεινόμενες υλοποιήσεις μειώνουν την κατανάλωση ισχύος σε μεγάλο βαθμό, αλλά επιπλέον έχουν περιορισμένη επιφάνεια και προσφέρουν υψηλό γινόμενο «Ισχύος x Επιφάνειας» με αποδεκτούς ρυθμούς απόδοσης σε σχέση με άλλες γνωστές αρχιτεκτονικές SubBytes. Αυτές οι ιδιότητες δίνουν στο σύστημά μας το πλεονέκτημα να μπορεί να χρησιμοποιηθεί σε χαμηλής ισχύος και περιορισμένης επιφάνειας συστήματα όπως είναι οι φορητές-ασύρματες δικτυακές συσκευές (Laptops, PDAs, κινητά τηλέφωνα).

5.12. Γενικά για το μετασχηματισμό SubBytes (Sbox)

Τον Ιανουάριο του 1997, το Ινστιτούτο Προτύπων και Τεχνολογίας της Αμερικής (National Institute of Standards and Technology - NIST) ζήτησε από την ερευνητική κοινότητα προτάσεις για την αντικατάσταση του παλιού αλγορίθμου συμμετρικής κρυπτογράφησης Data Encryption Standard (DES) (10) από έναν νέο ο οποίος θα ονομαζόταν Advanced Encryption Standard (AES). Μετά από δύο κύκλους αξιολογήσεων των 15 υποψηφίων αλγορίθμων, η NIST επέλεξε τον Rijndael ως τον AES αλγόριθμο τον Οκτώβριο του 2000 (15). Η NIST υιοθέτησε τον Rijndael AES αλγόριθμο ως το βασικό αλγόριθμο για συστήματα συμμετρικής κρυπτογράφησης, και ο AES έγινε βασικός αλγόριθμος κρυπτογράφησης σε πολλά πρωτόκολλα επικοινωνίας και εφαρμογές. Ο AES αλγόριθμος μπορεί να εφαρμοστεί σε εφαρμογές όπως κινητή τηλεφωνία, έξυπνες κάρτες, RFID ετικέτες, εξυπηρετητές και γενικότερα σε όλα τα δικτυακά συστήματα.

Τα περισσότερα χρησιμοποιημένα ασύρματα πρωτόκολλα (63), (64) υιοθέτησαν τον AES αλγόριθμο ως το βασικό μηχανισμό ασφάλειας (65) για παροχή πιστοποίησης, έγκρισης και ακεραιότητας δεδομένων. Σε αυτά τα συστήματα οι περιορισμοί σε ισχύ και επιφάνεια του συστήματος είναι πολύ μεγάλοι. Οι νέες φορητές συσκευές (laptops, PDAs, κτλ.) μπορούν και δουλεύουν για λίγες ώρες μέχρι η μπαταρία τους να εξαντληθεί. Ακόμη χειρότερα, οι απαιτήσεις σε ενέργεια αυξάνουν με μεγαλύτερο ρυθμό από ότι η εξέλιξη της τεχνολογίας των μπαταριών (9), (66). Συστήματα όπως

οι έξυπνες κάρτες και οι RFID ετικέτες (67) τα οποία εξάγουν ενέργεια από το ηλεκτρομαγνητικό πεδίο κάνουν το πρόβλημα πιο σύνθετο-δύσκολο. Ο σχεδιασμός σε υλικό (Hardware design) επιταχύνει τις πράξεις και μειώνει αισθητά τις ανάγκες σε ισχύ με ένα επιπλέον κόστος σε υλικό. Επομένως η ύπαρξη επιπρόσθετου υλικού που θα υποστηρίζει τις κρυπτογραφικές πράξεις είναι αναγκαία (20) αν ο σκοπός του σχεδιαστή είναι να κατασκευάσει αποδοτικά από πλευράς ισχύος συστήματα.

Οι υπάρχουσες υλοποιήσεις του AES αλγορίθμου δεν επικεντρώνονται στο πρόβλημα της κατανάλωσης ισχύος, αλλά προτείνουν υψηλής απόδοσης αρχιτεκτονικές (68), (69). Αυτές οι αρχιτεκτονικές δεν καλύπτουν την ανάγκη των χαμηλών πόρων συστημάτων για χαμηλή κατανάλωση ισχύος. Στην εργασία αυτή προτείνουμε αρχιτεκτονικές για την AES SubBytes κρυπτογραφική πράξη, η οποία αποτελεί την βασική κρυπτογραφική πράξη του AES και το σημαντικότερο παράγοντα κατανάλωσης ισχύος (70), (71). Έχει αποδειχτεί ότι η κατανάλωση ισχύος του δομικού στοιχείου SubBytes είναι περίπου το 75% της συνολικής κατανάλωσης ισχύος του AES. Επομένως βελτιώνοντας τα χαρακτηριστικά κατανάλωσης ισχύος της SubBytes κρυπτογραφικής πράξης, βελτιώνουμε σημαντικά την αποδοτικότητα από πλευράς ισχύος του αλγορίθμου. Υπάρχουν αρκετές εργασίες (72), (73), (74), (75) οι οποίες δίνουν μια πιο αποδοτική από πλευράς πόρων επιφάνεια αρχιτεκτονική της AES SubBytes κρυπτογραφικής πράξης, αγνοώντας ότι η μείωση στην επιφάνεια δεν έχει ανάλογα αποτελέσματα στην κατανάλωση ισχύος-πολλές φορές μπορεί να έχει και αντίθετα. Σε αυτό το κεφάλαιο παρουσιάζουμε υλοποιήσεις της SubBytes κρυπτογραφικής πράξης και εφαρμόζοντας VLSI τεχνικές επιτυγχάνουμε χαμηλή κατανάλωση ισχύος σε περιορισμένους πόρους επιφάνειας.

5.13. Ο αλγόριθμος AES (Advanced Encryption Standard)

Ο AES αλγόριθμος ανήκει στην οικογένεια των συμμετρικών αλγορίθμων κρυπτογραφίας, όπου και ο αποστολέας και ο παραλήπτης συμφωνούν σε ένα κοινό μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο AES αλγόριθμος επεξεργάζεται 128 ψηφίων, ενώ το μήκος του κλειδιού μπορεί να είναι 128, 192, ή 256 ψηφία. Επιπρόσθετα, ο AES αλγόριθμος είναι επαναληπτικός αλγόριθμος. Κάθε επανάληψη καλείται κύκλος (round), και ο συνολικός αριθμός των κύκλων N_r είναι 10, 12, ή 14, όταν το μήκος του κλειδιού είναι 128, 192, ή 256 ψηφία, αντίστοιχα. Το block δεδομένων 128-bit χωρίζεται σε 16 bytes. Αυτά τα bytes αντιστοιχίζονται σε ένα 4×4 πίνακα ο οποίος καλείται State, και όλες οι εσωτερικές πράξεις του AES αλγορίθμου εκτελούνται στο State. Κάθε byte του State συμβολίζεται ως $S_{i,j}$ ($0 \leq i, j < 4$), και αποτελεί στοιχείο του πεπερασμένου σώματος $GF(2^8)$. Μολονότι διαφορετικά ανάγωγα (irreducible) πολυώνυμα χρησιμοποιούνται για να δημιουργηθεί το $GF(2^8)$ πεπερασμένο σώμα, το ανάγωγο πολυώνυμο που χρησιμοποιείται στον AES αλγόριθμο είναι το $p(x) = x^8 + x^4 + x^3 + x + 1$. Η Εικόνα 38 παρουσιάζει το διάγραμμα δομικών στοιχείων του AES αλγορίθμου για την κρυπτογράφηση και την αποκρυπτογράφηση, την σειρά που είναι συνδεδεμένα και τον αριθμό των κύκλων που απαιτούνται ανάλογα με το μέγεθος του κλειδιού.

Εικόνα 38: Οι διεργασίες κρυπτογράφησης και αποκρυπτογράφησης του AES αλγορίθμου.

Κατά τη διαδικασία της κρυπτογράφησης στον AES αλγόριθμο, κάθε κύκλος εκτός από τον τελικό αποτελείται από τέσσερις μετασχηματισμούς: SubBytes, ShiftRows, MixColumns, και AddRoundKey, ενώ στον τελικό κύκλο δεν υπάρχει ο MixColumns μετασχηματισμός. Παρακάτω παρουσιάζονται οι βασικές κρυπτογραφικές πράξεις και οι ιδιότητές εν συντομία.

- **SubBytes** – αποτελεί έναν μη γραμμικό μετασχηματισμό όπου κάθε byte αντικαθίσταται σύμφωνα με έναν πίνακα αντικατάστασης.
- **ShiftRows** – αποτελεί βήμα αλληλομετάθεσης όπου κάθε γραμμή από το State ολισθαίνει κυκλικά για ένα συγκεκριμένο αριθμό θέσεων.
- **MixColumns** – η πράξη αυτή εφαρμόζεται σε κάθε στήλη του State και αναπαριστά ένα γραμμικό μετασχηματισμό βασισμένο στα 4 bytes της στήλης.
- **AddRoundKey** – κάθε byte του state συνδυάζεται με ένα byte από το κλειδί του τρέχοντος κύκλου. Κάθε κλειδί του κύκλου προέρχεται από το κλειδί κρυπτογράφησης χρησιμοποιώντας το σύστημα παραγωγής κλειδιών του AES (key schedule).

Οι προηγούμενοι μετασχηματισμοί εφαρμόζονται και στην αποκρυπτογράφηση αλλά με παρόμοια λογική. Οι μετασχηματισμοί που προκύπτουν και χρησιμοποιούνται στην αποκρυπτογράφηση είναι οι InvShiftRows, InvSubBytes, InvMixColumns, και AddRoundKey.

5.14. Ο Subbytes/InvSubBytes μετασχηματισμός

Ο SubBytes/InvSubBytes (15) μετασχηματισμός είναι ένας μη-γραμμικός μετασχηματισμός που εφαρμόζεται ανεξάρτητα σε κάθε byte του State χρησιμοποιώντας έναν πίνακα αντικατάστασης (Sbox). Το Sbox (Εικόνα 40), το οποίο είναι αναστρέψιμο, βασίζεται σε δύο επιμέρους μετασχηματισμούς :

1. Εφαρμογή της αντιστροφής στο πεπερασμένο σώμα $GF(2^8)$, το στοιχείο $\{00\}$ αντιστοιχεί στον εαυτό του.
2. Εφαρμογή του ακόλουθου μετασχηματισμού στο $GF(2)$:

$$b'_i = b_i \oplus b_{(i+4)} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i, \text{ for } 0 \leq i \leq 7$$

όπου b_i είναι το i bit του byte b , και c_i το i bit του byte c με τιμή $\{63\}$ or $\{01100011\}$. Σε μορφή μητρώου ο δεύτερος μετασχηματισμός του Sbox μπορεί να παρουσιαστεί ως εξής:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Εικόνα 39: Ο affine μετασχηματισμός σε μορφή μητρώου

Εικόνα 40: Γραφική αναπαράσταση του SubBytes μετασχηματισμού

Το Sbox χρησιμοποιεί το **SubBytes** μετασχηματισμό και εκφράζεται από τον πίνακα ο οποίος απαρτίζεται από στοιχεία σε δεκαεξαδική μορφή όπως παρουσιάζεται στην Εικόνα 40. Για παράδειγμα, αν $S_{i,j} = \{53\}$, τότε η τιμή αντικατάστασης θα καθοριστεί από την τομή της γραμμής '5' και της στήλης '3' της Εικόνας. 40. Ως αποτέλεσμα το $S_{i,j}$ θα αντικατασταθεί από την τιμή $\{ed\}$.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Εικόνα 41: Ο πίνακας μετασχηματισμών για την κρυπτογράφηση (σε δεκαεξαδική μορφή).

Το **InvSubBytes** είναι ο πίνακας μετασχηματισμών κατά την αποκρυπτογράφηση και αποτελεί την αντίστροφη διεργασία του Sbox. Βασίζεται στην εφαρμογή του affine μετασχηματισμού και αντίστροφου μετασχηματισμού $GF(2^8)$ που τον ακολουθεί.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Εικόνα 42: Ο πίνακας μετασχηματισμών για την αποκρυπτογράφηση (σε δεκαεξαδική μορφή).

5.15. Προηγούμενες υλοποιήσεις στο Subbytes/InvSubBytes μετασχηματισμό

Ο πιο απλός τρόπος για να ολοκληρωθούν οι SBox πίνακες σε υλικό σύμφωνα με τις Εικόνες 41 και 42 είναι να ακολουθηθούν πιστά οι μετασχηματισμοί όπως ορίζονται από τους πίνακες. Σε αυτή την προσέγγιση, δεν γίνεται χρήση του μαθηματικού υπόβαθρου που διέπει τους πίνακες SBox. Η διαδικασία βελτιστοποίησης βασίζεται αποκλειστικά στα χαρακτηριστικά του εργαλείου σύνθεσης και στις βιβλιοθήκες που σχετίζονται σε αυτό. Επομένως, η κατανάλωση ισχύος εξαρτάται από τις βιβλιοθήκες του εργαλείου σύνθεσης και τις οικογένειες των πυλών. Αν το εργαλείο σύνθεσης

τρέχει μια διαδικασία βελτιστοποίησης που συνδυάζει χαμηλούς πόρους σε επιφάνεια και χαμηλή κατανάλωση ισχύος, το προκύπτον κύκλωμα είναι μικρής επιφάνειας και με χαμηλή κατανάλωση ισχύος. Ένα σημαντικό μειονέκτημα αυτής της προσέγγισης είναι η μεγάλη επιφάνεια εφόσον δύο κυκλώματα υπάρχουν, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση και το SubBytes κύκλωμα μπορεί να είναι περίπου τρεις φορές μεγαλύτερο σε σχέση με άλλες προσεγγίσεις (70), (73), (75), (72) .

Μια παρόμοια προσέγγιση είναι αυτή της αντικατάστασης του Sbox με ROM. Σε αυτή την περίπτωση, η καθυστέρηση του κυκλώματος είναι ίση με την πρώτη προσέγγιση αλλά η κατανάλωση μπορεί να είναι τάξεις μεγέθους μεγαλύτερη.

Η τρίτη προσέγγιση για την υλοποίηση του AES Sbox έχει προταθεί από τους Bertoni et al. Στην εργασία (74) χρησιμοποιώντας ενδιάμεση one-hot κωδικοποίηση της εισόδου, οποιαδήποτε λογική πράξη συμπεριλαμβανομένων των κρυπτογραφικών Sboxes μπορεί να υλοποιηθεί με χαρακτηριστικό τη χαμηλή κατανάλωση ισχύος. Σχεδιάζοντας το SubBytes μετασχηματισμό βασιζόμενοι σε αυτήν την προσέγγιση το σύστημα θα αποτελείται από έναν 8 σε 2^8 κωδικοποιητή, έναν 2^8 σε 8 αποκωδικοποιητή και την κατάλληλη αντιστοίχιση μεταξύ της εξόδου του κωδικοποιητή και της εισόδου του αποκωδικοποιητή. Το βασικό μειονέκτημα αυτής της προσέγγισης είναι ότι η προκύπτουσα υλοποίηση καταλαμβάνει μεγάλη επιφάνεια υλοποίησης. Επιπλέον η προσέγγιση αυτή καλύπτει την περίπτωση της κρυπτογράφησης. Για την αποκρυπτογράφηση, ένα παρόμοιο σύστημα πρέπει να σχεδιαστεί . Η προσέγγιση αυτή καταλαμβάνει πολύ περισσότερη επιφάνεια από την προσέγγιση των πινάκων και από τις αριθμητικές προσεγγίσεις που θα παρουσιαστούν στη συνέχεια. Ένα επιπλέον μειονέκτημα της προσέγγισης (74) είναι ότι η αρχιτεκτονική δεν μπορεί εύκολα να αλλαχτεί και δεν είναι ευέλικτη ώστε να επιταχυνθεί με στάδια από καταχωρητές. Τα παραπάνω καθιστούν την υλοποίηση για χαμηλών πόρων συστήματα ανέφικτη.

Υπάρχουν πιο προχωρημένες προσεγγίσεις στο σχεδιασμό SubBytes μετασχηματισμών. Οι προσεγγίσεις αυτές χρησιμοποιούν το μαθηματικό υπόβαθρο του πεπερασμένου σώματος $GF(2^8)$ (αριθμητικές προσεγγίσεις Sbox). Το βασικό θέμα σε αυτές τις προσεγγίσεις είναι η αποδοτική πραγματοποίηση της αντιστροφής $GF(2^8)$ η οποία μπορεί να στηριχτεί στην ανάλυση του $GF(2^8)$ σε πεπερασμένα σώματα $GF(2^4)$ και $GF(2^2)$. Η αντιστροφή ενός πεπερασμένου σώματος μπορεί να πραγματοποιηθεί με διάφορους τρόπους σύμφωνα με αυτήν την προσέγγιση. Το βασικό στοιχείο αυτών των προσεγγίσεων είναι η μικρή επιφάνεια εξαιτίας του γεγονότος ότι η κωδικοποίηση και η αποκωδικοποίηση βασίζονται στο ίδιο κύκλωμα. Η μείωση όμως στην επιφάνεια δεν οδηγεί σε αντίστοιχη μείωση στην κατανάλωση ισχύος. Επιπλέον στις προσεγγίσεις αυτές η κατανάλωση ισχύος δεν λαμβάνεται υπόψη. Εξαιτίας των ανεπιθύμητων φορτίσεων-εκφορτίσεων εσωτερικά του κυκλώματος και γενικότερα στην τοπολογία του κυκλώματος (topology network), η κατανάλωση ισχύος μπορεί να είναι 10-30 φορές υψηλότερη από την προσέγγιση των πινάκων (76).

Σε αυτό το σημείο προτείνουμε μια μεθοδολογία η οποία μπορεί να χρησιμοποιηθεί ώστε να συνθέσουμε κρυπτογραφικά Sbox σε ASIC με μείωση της κατανάλωσης ισχύος σαν πρωταρχικό στόχο. Για λόγους σύγκρισης υλοποιήσαμε την προσέγγιση look up table S-Box και την προσέγγιση όπως παρουσιάζεται στην εργασία (72) μαζί με τις τέσσερις δικές μας αρχιτεκτονικές.

5.16. Προτεινόμενη υλοποίηση του Subbytes/InvSubBytes μετασχηματισμού

Όπως περιγράφηκε στην προηγούμενη παράγραφο το βασικό πλεονέκτημα των αριθμητικών υλοποιήσεων SubBytes είναι οι περιορισμένες απαιτήσεις σε επιφάνεια. Το γεγονός αυτό είναι βασισμένο στην ικανότητα αυτών των υλοποιήσεων να υποστηρίζουν σε ένα κύκλωμα και κρυπτογράφηση και αποκρυπτογράφηση. Όπως ήδη αναλύσαμε, το βασικό πρόβλημα των αριθμητικών υλοποιήσεων είναι η αυξημένη κατανάλωση ισχύος αν και επιτυγχάνουν περιορισμένης επιφάνειας προσεγγίσεις. Προτείνουμε μια νέα προσέγγιση η οποία συνδυάζει χαμηλή κατανάλωση ισχύος και χαμηλούς πόρους σε επιφάνεια. Ο σκοπός αυτής της εργασίας είναι να επιτευχθεί μια λύση για το SubBytes μετασχηματισμό και γενικότερα για τον AES αλγόριθμο ώστε να το διέπουν χαμηλής κατανάλωσης ισχύος ιδιότητες. Η υλοποίηση αυτή είναι από τις πρώτες εργασίες για το SubBytes η οποία συνδυάζει χαμηλό κόστος επιφάνειας και χαμηλή κατανάλωση ισχύος. Τέσσερις εναλλακτικές υλοποιήσεις περιγράφονται και ονομάζονται Implem1, Implem2, Implem1R, and Implem2R. Όλα τα βήματα των βελτιστοποιήσεων παρουσιάζονται με λεπτομέρεια για τις προσεγγίσεις Implem1 και Implem2 καθώς και για τις εκδόσεις τους με στάδια καταχωρητών Implem1R και Implem2R.

Η προτεινόμενη SubBytes αριθμητική υλοποίηση μπορεί να διέπεται από χαμηλής κατανάλωσης ισχύος ιδιότητες τόσο σε ASIC όσο και σε FPGA τεχνολογίες. Η διαφοροποίηση αυτή μπορεί να επιτευχθεί κάνοντας χρήση τεχνικές, όπως αναδιάταξη των δομικών στοιχείων του συνολικού κυκλώματος, κάνοντας χρήση επιπλέον υλικού (ideal delay line), μειώνοντας το fan out του κυκλώματος, και εισαγωγή των καταχωρητών σε σημεία που δημιουργούν ανεπιθύμητες φορτίσεις εκφορτίσεις εξαιτίας της μη άφιξης των σημάτων εισόδου την ίδια χρονική στιγμή στις πύλες. Μία από τις μεγαλύτερες πηγές δημιουργίας επιπλέον ενέργειας είναι η δυναμική ενέργεια που δημιουργείται από την κατανάλωση στις πύλες και στο δίκτυο (wiring).

Τεχνικές ώστε να διευθετηθεί το πρόβλημα της κατανάλωσης ισχύος είναι η χρήση τρανζίστορ ειδικής τεχνολογίας (συγκεκριμένου μεγέθους) ή μετασχηματισμός του κυκλώματος λογικών πράξεων. Το πλεονέκτημα της δεύτερης μεθόδου είναι ότι μπορεί να εφαρμοστεί σε κυκλώματα με οποιαδήποτε τεχνολογία αφού βασίζεται κυρίως στην λειτουργία (εσωτερική συνάρτηση) που εμπεριέχεται στο κύκλωμα και όχι στη φυσική υλοποίηση. Επιπλέον οι μετασχηματισμοί σε αυτό το επίπεδο μπορούν να έχουν πολύ καλύτερα αποτελέσματα από πλευράς κατανάλωσης ισχύος

αν οι προκύπτοντες μετασχηματισμοί βελτιώνουν σε μεγάλο βαθμό την κατανάλωση ισχύος.

Εικόνα 44: Οι προτεινόμενες αρχιτεκτονικές Implem1 και Implem2

Οι καθυστερήσεις στο δίκτυο (τονισμένο δίκτυο στη Εικόνα 43) μπορούν να εξισορροπηθούν σχετίζοντας τις εξόδους απευθείας με τις εισόδους. Έπειτα εισάγουμε επιπλέον υλικό (XOR) ώστε να μεταδίδονται στους ίδιους χρόνους τα εσωτερικά σήματα στις εισόδους των πυλών. Στην Εικόνα 44(a) (Implem1 αρχιτεκτονική), το αποτέλεσμα είναι η δημιουργία του COMP δομικού στοιχείου. Η προσέγγιση αυτή συνεισφέρει σημαντικά στην μείωση των δημιουργημένων μεταβιβάσεων στο κύκλωμα εξαιτίας του συγχρονισμού στη διάδοση των σημάτων στο τονισμένο δίκτυο. Το αποτέλεσμα είναι το μέρος αυτό του SubBytes να είναι στο πιο ισορροπημένο.

Η απλοποίηση του COMP κυκλώματος στηρίζεται στο γεγονός ότι μόνο XOR πύλες το απαρτίζουν, και επομένως είναι ευκολότερο να δημιουργηθεί ένα εξισορροπημένο XOR δέντρο (Εικόνα 44 (a) - Implem1). Αναλύοντας λοιπόν τις βασικές πράξεις που απαρτίζουν το COMP δομικό στοιχείο μπορούμε να συσχετίσουμε τις εξόδους του απευθείας από τις εισόδους χωρίς να εμπεριέχονται οι ενδιάμεσες τιμές στην έξοδο. Η βελτιστοποίηση απαρτίζεται από δύο επιμέρους διεργασίες. Αρχικά η λογική απλοποιείται χρησιμοποιώντας βασικές αρχές ψηφιακής λογικής. Το αποτέλεσμα είναι αρκετά ενδιαφέρον γιατί παρατηρούμε πως το κύκλωμα απλοποιείται σε μέγιστο βαθμό ώστε να κατασκευαστεί ένα μικρό XOR δέντρο. Επιπλέον XOR πύλες προστίθενται ώστε να ισορροπηθούν οι διαδόσεις σημάτων εσωτερικά του XOR δέντρου.

Έπειτα από αυτή τη διεργασία γίνεται προσπάθεια ώστε να βελτιωθεί ακόμη η αποδοτικότητα του κυκλώματος από πλευράς κατανάλωσης ισχύος. Η βελτιστοποίηση αυτή έχει ως αποτέλεσμα το κύκλωμα Implem2 (Εικόνα 44 (b)). Ένα βασικό χαρακτηριστικό που προσπαθήσαμε να βελτιστοποιήσουμε ήταν το υψηλό

fan-out του δομικού στοιχείου MAP. Η διεργασία αυτή βασίστηκε στην μείωση του fan-out του δομικού στοιχείου MAP. Για το λόγο αυτό ακολουθήθηκαν δύο στάδια, έγινε εισαγωγή στο κύκλωμα ενός ταυτόσημου δομικού στοιχείου με το MAP ώστε να διαμοιραστεί το fan-out σε δύο ταυτόσημα δομικά στοιχεία και μετασχηματίστηκε το δομικό στοιχείο COMP ώστε να συμπεριλάβει και το δομικό στοιχείο MAP.

Το αποτέλεσμα παρουσιάζεται στην Εικόνα 44 (b) (Implem2). Παρακάτω οι πράξεις σε ψηφιακή λογική παρουσιάζονται που ακολουθήθηκαν ώστε να προκύψει το κύκλωμα COMP (βάσει της ιδιότητας $a(i) \oplus a(i) = 0$). Στην Εικόνα 45, παρουσιάζονται αναλυτικά οι αντίστοιχοι κόμβοι του κυκλώματος.

Εικόνα 45: Οι κόμβοι εσωτερικά του δομικού στοιχείου COMP

Node2

$$ah(0) = a(5) \oplus a(4) \oplus a(6)$$

$$ah(1) = a(1) \oplus a(7) \oplus a(4) \oplus a(6)$$

$$ah(2) = a(5) \oplus a(7) \oplus a(2) \oplus a(3)$$

$$ah(3) = a(5) \oplus a(7)$$

Node3

$$sq(0) = ah(0) \oplus ah(2) = a(5) \oplus a(4) \oplus a(6) \oplus a(5) \oplus a(7) \oplus a(2) \oplus a(3) = a(4) \oplus a(6) \oplus a(7) \oplus a(2) \oplus a(3)$$

$$sq(1) = ah(2) = a(5) \oplus a(7) \oplus a(2) \oplus a(3)$$

$$sq(2) = ah(1) \oplus ah(3) = a(1) \oplus a(7) \oplus a(4) \oplus a(6) \oplus a(5) \oplus a(7) = a(1) \oplus a(4) \oplus a(5) \oplus a(6)$$

$$sq(3) = ah(3) = a(5) \oplus a(7)$$

Node4

$$\begin{aligned}
e(0) &= sq(1) \oplus sq(2) \oplus sq(3) = a(5) \oplus a(7) \oplus a(2) \oplus a(3) \oplus a(1) \oplus a(4) \oplus a(5) \oplus a(6) \oplus \\
&a(5) \oplus a(7) = \\
&a(2) \oplus a(3) \oplus a(4) \oplus a(5) \oplus a(6) \oplus a(1) \\
e(1) &= sq(0) \oplus sq(1) = a(4) \oplus a(6) \oplus a(7) \oplus a(2) \oplus a(3) \oplus a(5) \oplus a(7) \oplus a(2) \oplus a(3) = \\
&a(4) \oplus a(5) \oplus a(6) \\
e(2) &= sq(0) \oplus sq(1) \oplus sq(2) = a(4) \oplus a(6) \oplus a(7) \oplus a(2) \oplus a(3) \oplus a(5) \oplus a(7) \oplus a(2) \\
&a(1) \oplus a(4) \oplus a(5) \oplus a(6) = a(1) \\
e(3) &= sq(0) \oplus sq(1) \oplus sq(2) \oplus sq(3) = a(4) \oplus a(6) \oplus a(7) \oplus a(2) \oplus a(3) \oplus a(5) \oplus a(7) \oplus \\
&\oplus a(3) \oplus a(1) \oplus a(4) \oplus a(5) \oplus a(6) \oplus a(5) \oplus a(7) = \\
&a(1) \oplus a(5) \oplus a(7)
\end{aligned}$$

Node5

$$\begin{aligned}
al(0) &= a(4) \oplus a(6) \oplus a(0) \oplus a(5) \\
al(1) &= a(1) \oplus a(2) \\
al(2) &= a(1) \oplus a(7) \\
al(3) &= a(2) \oplus a(4)
\end{aligned}$$

Node6

$$\begin{aligned}
sq'(0) &= al(0) \oplus al(2) = a(4) \oplus a(6) \oplus a(0) \oplus a(5) \oplus a(1) \oplus a(7) = \\
&a(0) \oplus a(1) \oplus a(4) \oplus a(5) \oplus a(6) \oplus a(7) \\
sq'(1) &= al(2) = a(1) \oplus a(7) \\
sq'(2) &= al(1) \oplus al(3) = a(1) \oplus a(2) \oplus a(2) \oplus a(4) = \\
&a(1) \oplus a(4) \\
sq'(3) &= al(3) = a(2) \oplus a(4)
\end{aligned}$$

Node7

$$\begin{aligned}
x(0) &= e(0) \oplus sq'(0) = a(0) \oplus a(2) \oplus a(3) \oplus a(7) \\
x(1) &= e(1) \oplus sq'(1) = a(1) \oplus a(7) \oplus a(4) \oplus a(5) \oplus a(6) \\
x(2) &= e(2) \oplus sq'(2) = a(4) \\
x(3) &= e(3) \oplus sq'(3) = a(2) \oplus a(4) \oplus a(1) \oplus a(5) \oplus a(7)
\end{aligned}$$

Το τελικό στάδιο της βελτιστοποίησης προσδίδει χαμηλής κατανάλωσης ισχύος ιδιότητες στο κύκλωμα. Αρχικά υπήρχε το fun-out πρόβλημα στο δομικό στοιχείο MAP. Ξεκινώντας τις βελτιστοποιήσεις από το COMP δομικό στοιχείο προέκυψε το δομικό στοιχείο COMP2, το οποίο έχει όμοιες εισόδους με το δομικό στοιχείο MAP. Με αυτό τον τρόπο εκτονώθηκε το υψηλό fan-out του δομικού στοιχείου MAP. Το αποτέλεσμα είναι η μεγιστοποίηση του κέρδους σε ισχύ για την τελευταία υλοποίηση σε σύγκριση με άλλες υλοποιήσεις SubBytes χωρίς ενδιάμεσους καταχωρητές.

Σε αυτό το σημείο πήραμε πειραματικά αποτελέσματα και για τις προκύπτουσες αρχιτεκτονικές με ενδιάμεσα στάδια καταχωρητών οι οποίες ονομάστηκαν implem1R και implem2R με αποτέλεσμα τα μεγαλύτερο κέρδος από πλευράς κατανάλωσης ισχύος. Η εισαγωγή των επιπέδων καταχωρητών έγινε με στόχο την μη μετάδοση των ανεπιθύμητων φορτίσεων και εκφορτίσεων. Με αυτό τον τρόπο ελέγχουμε αποτελεσματικά την κατανάλωση ισχύος και τη διατηρούμε σε ακόμη πιο χαμηλά επίπεδα. Φυσικά η μέθοδος αυτή έχει ως αρνητικό αποτέλεσμα την μεγαλύτερη επιφάνεια ολοκλήρωσης. Στην περίπτωση αυτή οι αρχιτεκτονικές αυτές μπορούν να εφαρμοστούν σε περιβάλλοντα πολύ υψηλών απαιτήσεων για χαμηλή κατανάλωση ισχύος. Το κέρδος μείωσης της κατανάλωσης ισχύος εισάγοντας επίπεδα καταχωρητών είναι τουλάχιστον 2 φορές υψηλότερο από της αρχιτεκτονικές χωρίς ενδιάμεσα στάδια καταχωρητών. Περιορίζουμε εντελώς τις ανεπιθύμητες φορτίσεις και εκφορτίσεις οι οποίες δημιουργούνται εξαιτίας της έλλειψης συγχρονισμού των σημάτων μετάδοσης.

Εικόνα 46: Οι προτεινόμενες αρχιτεκτονικές Implem1R (a) και Implem2R (b)

5.17. Πειραματικά αποτελέσματα και Συγκρίσεις με άλλες εργασίες για το στοιχείο SubBytes

Όλες οι υλοποιήσεις συνθέθηκαν με εργαλεία Synopsys (24) (Design Compiler) σε λειτουργικό σύστημα Linux και σε τεχνολογία 0.18 μm με 1.8V core τάση. Οι εξομείωση και η δημιουργία πληροφορίας δραστηριότητας στο κύκλωμα (switching activity information) έγινε σε επίπεδο πύλης και σε ανάλυση 1 ps, χρησιμοποιώντας το VHDL εξομειωτή Modelsim (77). Η συνολική κατανάλωση ισχύος υπολογίστηκε με το PrimePower της Synopsys.

Υλοποιήσαμε έξι διαφορετικές προσεγγίσεις του μετασχηματισμού SubBytes σε VHDL. Η προσέγγιση lookup και η αριθμητική (J. Wolkerstorfer) υλοποιήθηκαν για τις συγκρίσεις. Οι άλλες τέσσερις υλοποιήσεις αποτελούν τα ενδιάμεσα βήματα βελτιστοποίησης και το τελικό που μπορούμε να ακολουθήσουμε για να πάρουμε την προτεινόμενη αρχιτεκτονική. Στις Εικόνες 47, 48, 49 και 50 τα βασικά προβλήματα της υλοποίησης (72) τονίζονται. Τα προβλήματα αυτά είναι η υψηλή κατανάλωση ισχύος και η καθυστέρηση και η βελτιστοποίηση από πλευράς επιφάνειας δεν είναι αρκετή ώστε να υπερτερεί στο γινόμενο «Επιφάνεια $\times$ Καθυστέρηση $\times$ Ισχύς». Επιπλέον όπως φαίνεται στις Εικόνες 47, 48, αν και η κατανάλωση ισχύος στην προσέγγιση look up είναι μειωμένη, η επιφάνεια είναι μεγάλη συγκριτικά με τις άλλες υλοποιήσεις. Οι Εικόνες 47, 48, 49 και 50 επιπλέον παρουσιάζουν τα αποτελέσματα από τις τέσσερις υλοποιήσεις που προτείνουμε. Χωρίς χρήση καταχωρητών βλέπουμε τα πολύ ικανοποιητικά αποτελέσματα της προσέγγισης Implem2. Το γινόμενο Ισχύς $\times$ Επιφάνεια $\times$ Καθυστέρηση, προσφέρει ένα αντικειμενικό μέτρο σύγκρισης των αρχιτεκτονικών και είναι περίπου το ίδιο με την τυπική lookup table προσέγγιση έχοντας λίγο μικρότερη επιφάνεια και λίγο περισσότερη κατανάλωση ισχύος. Με τη τοποθέτηση καταχωρητών, υλοποιήσεις Implem1R, implem2R, έχουμε τα καλύτερα αποτελέσματα σε σχέση με τις άλλες προσεγγίσεις. Όλα τα αποτελέσματα φαίνονται αναλυτικά στον Πίνακα 8. Συμπεραίνουμε πως η καλύτερη αρχιτεκτονική (για τις περιπτώσεις χωρίς καταχωρητές) από πλευράς κατανάλωσης ισχύος και πόρων επιφάνειας είναι η Implem2 και είναι η ιδανικότερη για χαμηλών πόρων εφαρμογές.

Εικόνα 47: Συγκρίσεις αρχιτεκτονικών ως προς την επιφάνεια

Εικόνα 48: Συγκρίσεις αρχιτεκτονικών ως προς την Ισχύ

Εικόνα 49: Συγκρίσεις αρχιτεκτονικών ως προς την καθυστέρηση

Εικόνα 50: Συγκρίσεις αρχιτεκτονικών ως προς την Ισχύς x Επιφάνεια x Καθυστέρηση

Πίνακας 8: Τα αποτελέσματα εξομοίωσης όλων των αρχιτεκτονικών

	Ισχύς (W)	Επιφάνεια (g.eq)	Καθυστέρηση (ns)	Ισχύς·xΕπιφάνεια	Ισχύς x Επιφάνεια x Καθυστέρηση
Look Up Tables	0,00056	1009,2384	2,93ns	0.56504	1,655958366
Wolk.[13]	0,0023	362,2191	7,33	0.8331	6,106651807
Implem1	0,00215	343,84275	6,69ns	0.7392	4,94556622
Implem2	0,001007	344,5444	6,17ns	0.3469	2,140719821
Implem1R	0,0003	708,977	2,15	0.2126	0,45729017
Implem2R	0,0001	712,6414	1,93ns	0.0712	0,1375398

5.18. Προτεινόμενη αρχιτεκτονική MixColumns / InvMixColumns για εφαρμογές περιορισμένων πόρων

Εκτός από το μετασχηματισμό SubBytes/InvSubBytes, μία σημαντική πράξη που συναντούμε στον αλγόριθμο AES είναι ο μετασχηματισμός MixColumns/InvMixColumns. Παρακάτω θα παρουσιάσουμε την προτεινόμενη αρχιτεκτονική για εφαρμογές περιορισμένων πόρων. Συγκρίσεις με άλλες εργασίες θα συζητηθούν και πειραματικά αποτελέσματα θα παρουσιαστούν.

5.19. Μαθηματικό υπόβαθρο

Πριν αναφερθούμε στις πράξεις MixColumns/InvMixColumns θα περιγράψουμε για διευκόλυνση του αναγνώστη κάποια εισαγωγικά στοιχεία σχετικά με τις πράξεις στα πεπερασμένα σώματα και κάποιους βασικούς ορισμούς που σχετίζονται με τον αλγόριθμο AES.

Bytes: Αποτελούν τη βασική μονάδα δεδομένων του αλγορίθμου AES. Όπου κάθε byte συμβολίζεται ως $a = \{a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0\}$. Το byte μπορεί να αναπαρασταθεί ως το βασικό στοιχείο των πεπερασμένων σωμάτων σε πολυωνυμική αναπαράσταση:

$$a(x) = \sum_{i=0}^7 a_i x^i = a_7 x^7 + a_6 x^6 + a_5 x^5 + \dots + a_1 x + a_0 \text{ που ορίζεται από το ανάγωγο}$$

πολυνώνυμο $p(x) = x^8 + x^4 + x^3 + x + 1$. Για παράδειγμα, η δυαδική τιμή $\{01100011\}$ είναι η τιμή $\{63\}$ σε δεκαεξαδική μορφή και παριστάνει το πολυνώνυμο $x^6 + x^5 + x + 1$.

Πρόσθεση: Η πρόσθεση δύο bytes που αναπαρίστανται από τα πολυνώνυμα $a(x), b(x) \in GF(2^8)$ επιτυγχάνεται προσθέτοντας τους αντίστοιχους συντελεστές των δύο πολυνύμων modulo 2, και στην πραγματικότητα είναι μια XOR πράξη η οποία συνήθως συμβολίζεται με $\oplus$. $a(x) \oplus b(x) = \sum_{i=0}^7 (a_i \oplus b_i) x^i$.

Η αντίθετη τιμή ενός byte είναι το ίδιο το byte: $-b(x) = b(x)$ και εξαιτίας της προηγούμενης σχέσης ισχύει: $a(x) - b(x) = a(x) + b(x)$

Πολλαπλασιασμός: Ο πολλαπλασιασμός δύο πολυνύμων $a(x), b(x) \in GF(2^8)$, συμβολίζεται με $a(x) \bullet b(x)$ και χρησιμοποιεί το ανάγωγο πολυνώνυμο $p(x)$ βαθμού ορίζοντας το πεπερασμένο σώμα. Η πράξη του πολλαπλασιασμού $c(x) = a(x) * b(x)$ στο $GF(2^8)$ εκτελείται πολλαπλασιάζοντας τα πολυνώνυμα $a(x), b(x)$ το οποίο οδηγεί στη δημιουργία ενός πολυνύμου βαθμού μικρότερου του 15, $t(x)$. Έπειτα ακολουθεί η modulo αναγωγή $c(x) = t(x) \bmod p(x)$ ώστε να διασφαλιστεί ότι το αποτέλεσμα είναι στοιχείο του πεπερασμένου σώματος $GF(2^8)$.

5.20. Οι Μετασχηματισμοί MixColumns και InvMixColumns

Ο μετασχηματισμός MixColumns λειτουργεί χωριστά σε κάθε στήλη του State του αλγορίθμου AES και αντιμετωπίζει κάθε στήλη σαν ένα πολυνώνυμο τεσσάρων όρων.

Μπορούμε να θεωρήσουμε τις στήλες σαν πολυώνυμα $GF(2^8)$ τα οποία πολλαπλασιάζονται modulo το ανάγωγο πολυώνυμο για τοβ AES με το πολυώνυμο $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + 02$.

Αρχικά, για την περίπτωση της κρυπτογράφησης έχουμε την παρακάτω σχέση για κάθε στήλη του State, $S'(x) = a(x) * S(x)$

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}, c \in (0 \leq c < 4)$$

Ως αποτέλεσμα της παραπάνω σχέσης έχουμε τις παρακάτω εξισώσεις:

$$S'_{0,c} = (\{02\} \bullet S_{0,c}) \oplus (\{03\} \bullet S_{1,c}) \oplus S_{2,c} \oplus S_{3,c},$$

$$S'_{1,c} = (\{02\} \bullet S_{1,c}) \oplus (\{03\} \bullet S_{2,c}) \oplus S_{0,c} \oplus S_{3,c},$$

$$S'_{2,c} = (\{02\} \bullet S_{2,c}) \oplus (\{03\} \bullet S_{3,c}) \oplus S_{0,c} \oplus S_{1,c},$$

$$S'_{3,c} = (\{02\} \bullet S_{3,c}) \oplus (\{03\} \bullet S_{0,c}) \oplus S_{1,c} \oplus S_{2,c},$$

Ο μετασχηματισμός InvMixColumns (για την αποκρυπτογράφηση) λειτουργεί ομοίως χωριστά σε κάθε στήλη του State του αλγορίθμου AES και αντιμετωπίζει κάθε στήλη σαν ένα πολυώνυμο τεσσάρων όρων. Μπορούμε να θεωρήσουμε τις στήλες σαν πολυώνυμα $GF(2^8)$ τα οποία πολλαπλασιάζονται modulo το ανάγωγο πολυώνυμο του AES με το πολυώνυμο $a(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + 0e$. Προκύπτει επομένως η παρακάτω σχέση:

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}, c \in (0 \leq c < 4)$$

Και βάσει του παρακάτω πίνακα προκύπτουν οι σχέσεις:

$$S'_{0,c} = (\{0e\} \bullet S_{0,c}) \oplus (\{0b\} \bullet S_{1,c}) \oplus (\{0d\} \bullet S_{2,c}) \oplus (\{09\} \bullet S_{3,c}),$$

$$S'_{1,c} = (\{09\} \bullet S_{1,c}) \oplus (\{0e\} \bullet S_{2,c}) \oplus (\{0b\} \bullet S_{0,c}) \oplus (\{0d\} \bullet S_{3,c}),$$

$$S'_{2,c} = (\{0d\} \bullet S_{2,c}) \oplus (\{09\} \bullet S_{3,c}) \oplus (\{0e\} \bullet S_{0,c}) \oplus (\{0b\} \bullet S_{1,c}),$$

$$S'_{3,c} = (\{0b\} \bullet S_{3,c}) \oplus (\{0d\} \bullet S_{0,c}) \oplus (\{09\} \bullet S_{1,c}) \oplus (\{0e\} \bullet S_{2,c}),$$

Στην Εικόνα 51 η γραφική απεικόνιση της MixColumns/InvMixColumns πράξης παρουσιάζεται:

Εικόνα 51: Η γραφική απεικόνιση της MixColumns πράξης

5.21. Προτεινόμενη αρχιτεκτονική MixColumns / InvMixColumns

5.21.1. Η αρχιτεκτονική του συστήματος MixColumns / InvMixColumns

Το προτεινόμενο σύστημα έχει είσοδο-έξοδο 32-bit. Κάθε είσοδος του συστήματος είναι η στήλη του AES State. Το ενός bit σήμα en/dec καθορίζει αν το σύστημα βρίσκεται σε λειτουργία κρυπτογράφηση ή αποκρυπτογράφηση. Το σύστημα εμπεριέχει τέσσερα δομικά στοιχεία Multiplier. Τα τέσσερα Multiplier δομικά στοιχεία εκτελούν πολλαπλασιασμούς σε $GF(2^8)$ πεπερασμένα σώματα, μεταξύ της 32-bit εισόδου και των σταθερών $\{01\}$, $\{01\}$, $\{02\}$ και $\{03\}$ για την κρυπτογράφηση και $\{09\}$, $\{0B\}$, $\{0D\}$ και $\{0E\}$ για την αποκρυπτογράφηση. Η έξοδος του συστήματος είναι 32-bit. Με τη κατάλληλη συσχέτιση των εξόδων τα 8-bit γινόμενα των πολλαπλασιαστών ακολουθούν το κατάλληλο XOR δέντρο όπως ορίστηκε από τους πολλαπλασιασμούς μητρώων παραπάνω. Στο τέλος της διεργασίας, η 32-bit έξοδος είναι η i στήλη του AES State όπου $0 \leq i < 4$. Στην Εικόνα 52, η προτεινόμενη αρχιτεκτονική 32-bit MixColumns / InvMixColumns παρουσιάζεται.

Εικόνα 52: Η 32-bit αρχιτεκτονική του συστήματος MixColumns/InvMixColumns

5.21.2. Ο προτεινόμενος αλγόριθμος

Σε αυτό το σημείο, παρουσιάζεται ο σχεδιασμός σε υλικό της μονάδας που εκτελεί πολλαπλασιασμό σε πεπερασμένα σώματα $GF(2^8)$, το οποίο καλείται Multiplier δομικό στοιχείο. Στον Αλγόριθμο 1 παρουσιάζεται η γενική μορφή του πολλαπλασιασμού για τα πολυώνυμα $a, b \in GF(2^m)$. Σύμφωνα με τον αλγόριθμο τα ψηφία-συντελεστές του b επεξεργάζονται από αριστερά (πιο σημαντικό ψηφίο) στα δεξιά (λιγότερο σημαντικό ψηφίο). Η λογική του πολλαπλασιαστή αυτού καλείται MSB (Most Significant Bit first) πολλαπλασιαστής.

Ο μετασχηματισμός του αλγορίθμου AES MixColumn είναι μια ειδική περίπτωση του πολλαπλασιασμού $GF(2^8)$ όπου τα στοιχεία του ορίζονται στο ανάγωγο πολυώνυμο $p(x) = x^8 + x^4 + x^3 + x + 1$. Λαμβάνοντας υπόψη το μετασχηματισμό MixColumn/InvMixColumn, ο Αλγόριθμος 1 παίρνει τη μορφή που παρουσιάζεται στον Αλγόριθμο 2. Η είσοδος είναι ένα 8-bit σήμα S και πολλαπλασιάζεται με μία από τις τιμές Constant (signal Con). Ο πολλαπλασιασμός ολοκληρώνεται μετά από 8 κύκλους του αλγορίθμου.

Αλγόριθμος 1.

Most significant bit first (MSB) multiplier for $GF(2^m)$

INPUT: $a = (a_{m-1}, \dots, a_1, a_0) \in GF(2^m)$,

$b = (b_{m-1}, \dots, b_1, b_0) \in GF(2^m)$ and reduction polynomial $p(x) = x^m + r(x)$.

OUTPUT: $c = a \bullet b$

1. Set $c \leftarrow 0$
2. For i from $m - 1$ downto 0 do
 - 2.1 $c \leftarrow \text{leftshift}(c) + c_{m-1}r$
 - 2.2 $c \leftarrow c + b_i a$
3. Return(c)

Αλγόριθμος 2.

MixColumn/InvMixColumn MSB multiplication in $GF(2^m)$

INPUT: $S = (s_7, \dots, s_1, s_0) \in GF(2^m)$

$Con = (con_7, \dots, con_1, con_0) \in GF(2^m)$, and reduction

polynomial $p(x) = x^8 + x^4 + x^3 + x + 1 = x^8 + r(x)$

OUTPUT: $c = S \bullet Con$

1. Set $c \leftarrow 0$
2. For i from 7 downto 0 do
 - 2.1 $c \leftarrow \text{leftshift}(c) + c_7 r$
 - 2.2 $c \leftarrow c + con_i S$
3. Return(c)

5.21.3. Η τεχνική κοινής χρήσης των πόρων (Resource Sharing)

Η τεχνική κοινής χρήσης των πόρων (Resource sharing) μπορεί να εφαρμοστεί με σκοπό να μειώσει την συνολική επιφάνεια του συστήματος και την κατανάλωση ισχύος. Παρατηρώντας τον Αλγόριθμο 2, μπορεί να σημειωθεί ότι μέχρι να εμφανιστεί και χρησιμοποιηθεί ο πρώτος μη μηδενικός όρος con_i , στον κύκλο του αλγορίθμου i , καμία αλλαγή δε συμβαίνει στην τιμή του c . Η τιμή του c παραμένει μηδενική. Επομένως, αν ο αριθμός i είναι ο πρώτος μη μηδενικός συντελεστής con_i και είναι γνωστός τότε $(7 - i)$ κύκλοι του Αλγορίθμου 2 μπορούν να παραληφθούν. Όπως παρουσιάζεται στον Πίνακα 9, όλες τις τιμές των σταθερών (Con value) οι οποίες χρησιμοποιούνται στον μετασχηματισμό MixColumn/InvMixColumn, con_7 μέχρι con_4 είναι μηδενικές. Συμπεραίνουμε πως $(7 - 3) = 4$ κύκλοι μπορούν να παραληφθούν σε κάθε πολλαπλασιασμό. Υπολογίζοντας τους κύκλους που απαιτούνται για να εξαχθεί το κάθε γινόμενο καταλήγουμε πως απαιτούνται το πολύ

τέσσερεις κύκλοι. Ο απαιτούμενος αριθμός των κύκλων για να εξαχθεί το κάθε γινόμενο πολλαπλασιάζοντας την είσοδο S με κάθε τη σταθερά Con παρουσιάζεται στον Πίνακα 9.

Πίνακας 9: Οι απαιτούμενοι κύκλοι για κάθε μεταβλητή

Τιμή Σταθεράς	Κύκλοι	Τιμή Σταθεράς	Κύκλοι
{01}: 00000001	1	{0B}: 00001011	4
{02}: 00000010	2	{0D}: 00001101	4
{03}: 00000011	2	{0E}: 00001111	4
		{0D}: 00001101	4

Κάθε κύκλος του Αλγορίθμου 2 μπορεί να αναπαρασταθεί σαν μια διεργασία, η οποία διαφοροποιείται σύμφωνα με τις εισόδους con_i και r . Οι τιμές Con και r είναι γνωστές για κάθε πιθανή είσοδο. Υπάρχουν τρεις τύποι διεργασιών. Ο Τύπος I (Type I) διεργασία η οποία σκοπό έχει στο να ανακαλύψει το πρώτο μη μηδενικό con_i και έχει την παρακάτω μορφή $c \leftarrow c + con_i S$ και εφόσον $c=0$ και $con_i=1$ προκύπτει $c \leftarrow S$. Η διεργασία Τύπος II (Type II) αντιστοιχεί στην περίπτωση όπου $con_i=0$ εφόσον έχει βρεθεί το πρώτο μη μηδενικό Con . Η διεργασία Type II έχει την παρακάτω μορφή $c \leftarrow leftshift(c) + c_7 r$. Η διεργασία Type III αντιστοιχεί στην περίπτωση όπου $con_i=1$ εφόσον έχει βρεθεί το πρώτο μη μηδενικό και έχει τη μορφή $c \leftarrow leftshift(c) + c_7 r + S$.

Εικόνα 53: Η διαδικασία των MixColumns πολλαπλασιασμών σε μορφή δέντρου

Οι τιμές των σταθερών όπως και ο αριθμός των κύκλων κατά το πολλαπλασιασμό της στήλης S με κάθε σταθερά είναι γνωστοί. Χρησιμοποιώντας την παραπάνω διαπίστωση ολόκληρη η διαδικασία του πολλαπλασιασμού παρουσιάζεται στην Εικόνα 53 σε μορφή δέντρου. Κάθε επίπεδο του δέντρου αντιστοιχεί σε ένα κύκλο του Αλγορίθμου 2. Κάθε κόμβος του δέντρου αντιστοιχεί στην διεργασία Type I, II, ή III η οποία εξαρτάται από την τρέχουσα τιμή con_i . Η αρχή (root) του δέντρου

(Level 1) αναφέρεται στην τιμή con_3 και ένα γύρο πολλαπλασιασμού, το Level 2 αναφέρεται στο con_2 και δύο γύροι πολλαπλασιασμού, το Level 3 αναφέρεται στο con_1 και τρεις γύροι πολλαπλασιασμού. το Level 4 αναφέρεται στο con_0 και τέσσερις γύρους πολλαπλασιασμού.

Εικόνα 54: Type II διεργασία

Εικόνα 55: Type III διεργασία

Κάθε γινόμενο προκύπτει στο κατάλληλο επίπεδο (Level) σύμφωνα με τον αριθμό των απαιτούμενων κύκλων για κάθε πολλαπλασιασμό όπως παρουσιάστηκε στον Πίνακα 9. Χρησιμοποιώντας το δέντρο όλα τα απαραίτητα αποτελέσματα μπορούν να υπολογιστούν. Για παράδειγμα, για να υπολογιστεί το αποτέλεσμα $S_{i,j} * \{09\}$ απαιτείται να ακολουθήσουμε στο δέντρο το μονοπάτι 1-0-0-1 ενώ για να υπολογίσουμε το αποτέλεσμα $S_{i,j} * \{0D\}$ απαιτείται να ακολουθήσουμε το μονοπάτι 1-1-0-1.

Κάθε διεργασία μπορεί να μοντελοποιηθεί με μεμονωμένα 8-bit υποσυστήματα. Τα υποσυστήματα αυτά παρουσιάζονται στις Εικόνες 54 και 55 για τις διεργασίες Type II, III αντίστοιχα. Το Type I υποσύστημα είναι μία αναδιάταξη των καλωδίων και δεν απαιτείται καμία πύλη. Το Type II υποσύστημα, υλοποιεί την εξίσωση $c \leftarrow leftshift(c) + c_7r$, και χρησιμοποιεί τρεις XOR πύλες, η τιμή του r είναι γνωστή σταθερά ($r=\{11011\}$) και το λιγότερο σημαντικό bit του c ύστερα από μία αριστερή ολίσθηση είναι μηδενικό. Το υποσύστημα, υλοποιεί τη σχέση $c \leftarrow leftshift(c) + c_7r + S$ χρησιμοποιώντας 11 XOR πύλες όπως φαίνεται στην Εικόνα 55.

5.21.4. Διαχείριση καταναλισκόμενης ισχύος

Η κατανάλωση ισχύος που προέρχεται από τη φόρτιση και εκφόρτιση των κόμβων του κυκλώματος (Ισχύς διακοπτικής δραστηριότητας - Switching Activity) αποτελεί βασικό παράγοντα της κατανάλωσης ισχύος για τα ψηφιακά κυκλώματα τεχνολογίας CMOS. Η ισχύς διακοπτικής δραστηριότητας της επιφάνειας του κυκλώματος η οποία δε συνεισφέρει στο αποτέλεσμα για μια δεδομένη χρονική μπορεί να

περιοριστεί. Η βασική αρχή στην ανάπτυξη τέτοιων πολιτικών είναι η εύρεση λογικών συνθηκών στις εισόδους, οι οποίες δε θα επηρεάσουν τα αποτελέσματα στην έξοδο. Όταν το σύστημα λειτουργεί στην κρυπτογράφηση (encryption mode) κάποια δομικά στοιχεία του πολλαπλασιαστή δε συνεισφέρουν στο αποτέλεσμα. Μπορούμε να «κλείσουμε» τα επίπεδα Level 3 και 4 του προτεινόμενου δέντρου (Multiplier) (Εικόνα 56) εισάγοντας AND πύλες με σκοπό τη διακοπή της μετάδοσης των σημάτων $S(i)$, $C(i)$. Εφαρμόζοντας την προτεινόμενη μέθοδο, μόνο τα απαραίτητα δομικά στοιχεία (Level 1 και Level 2) λειτουργούν κατά τη διάρκεια της κρυπτογράφησης. Στην Εικόνα 56 τα ενεργά (active) και μη ενεργά (inactive parts) δομικά στοιχεία του πολλαπλασιαστή παρουσιάζονται.

Εικόνα 56: Το εσωτερικό κύκλωμα του δομικού στοιχείου Multiplier

5.22. Αποτελέσματα, συγκρίσεις και συμπεράσματα

Το σύστημα μας συνδέθηκε σε VHDL και μετρήθηκε σε Synopsys (24) περιβάλλον. Για λόγους σύγκρισης υλοποιήσαμε και την τυπική αρχιτεκτονική όπου υλοποιούμε χωριστά το κύκλωμα που απαιτείται για τον πολλαπλασιασμό με κάθε μεταβλητή. Τα αποτελέσματα και η σύγκριση μεταξύ των δύο αρχιτεκτονικών φαίνονται στον παρακάτω Πίνακα 10. Η κατανάλωση ισχύος είναι οριακά μεγαλύτερη στην δική μας περίπτωση ενώ η προτεινόμενη αρχιτεκτονική μας είναι πολύ μικρότερη σε επιφάνεια. Το γεγονός αυτό συμβαίνει στην τεχνική διαμοίρασης πόρων που χρησιμοποιούμε για να υπολογίσουμε τα επιθυμητά αποτελέσματα. Στο γινόμενο $Ισχύς \times Επιφάνεια$ η αρχιτεκτονική μας είναι σαφώς καλύτερη.

Πίνακας 10: Αποτελέσματα σύγκρισης αρχιτεκτονικών

Υλοποιήσεις	Τυπική	Προτεινόμενη
Επιφάνεια	592 XOR	432 XOR+ 104 AND+32 OR
Κοινή Χρήση Πόρων	όχι	ναι
MixColumn oper.	152 XOR	152
InvMixColumn oper.	440 XOR	432
Καθυστέρηση	2,5ns	2,8
Κατανάλωση Ισχύος	0.3 mW	0.33 mW
Επιφάνεια(g.eq)	3207	2510
Επιφάνεια x Ισχύς	963,15	828

ΚΕΦΑΛΑΙΟ 6. Υλοποίηση του αλγορίθμου AES για εφαρμογές περιορισμένων πόρων

Οι περισσότερες υλοποιήσεις σε υλικό του αλγορίθμου κρυπτογράφησης AES (Advanced Encryption Standard) έχουν σκοπό την επίτευξη υψηλής απόδοσης του συστήματος κρυπτογράφησης ή την ελαχιστοποίηση της συνολικής επιφάνειας και συνήθως η κατανάλωση ισχύος είναι μια παράμετρος η οποία δεν εξετάζεται. Εντούτοις, η ανάγκη για εφαρμογές χαμηλής κατανάλωσης ισχύος σε περιορισμένη επιφάνεια υλικού είναι μεγάλη, ειδικά για ασύρματα συστήματα περιορισμένων πόρων. Σε αυτό το κεφάλαιο προτείνεται αρχιτεκτονική 8-bit περιορισμένης κατανάλωσης ισχύος και επιφάνειας για τον αλγόριθμο AES. Η προτεινόμενη αρχιτεκτονική υποστηρίζει την κρυπτογράφηση και την αποκρυπτογράφηση καθώς και τις αντίστοιχες βασικές διαδικασίες δημιουργίας των κλειδιών για τρία διαφορετικά μεγέθη του κλειδιού (128, 192 και 256 bit), δίνοντας τη δυνατότητα στο σύστημα υποστήριξης διαφορετικών επιπέδων ασφάλειας. Οι προτεινόμενες αρχιτεκτονικές χαμηλής κατανάλωσης ισχύος, του 5^{ου} Κεφαλαίου, για τους κρυπτογραφικούς μετασχηματισμούς SubBytes/InvSubBytes και MixColumns/InvMixColumns ενσωματώνονται στο σύστημά μας. Η προτεινόμενη υλοποίησή μας όχι μόνο μειώνει την κατανάλωση ισχύος σε μεγάλο βαθμό αλλά προσφέρει ικανοποιητικά αποτελέσματα για τον παράγοντα «Απόδοση x Ισχύς» σε σχέση με άλλες εργασίες για τον AES αλγόριθμο.

6.1.Εισαγωγή

Τα περισσότερα χρησιμοποιημένα ασύρματα πρωτόκολλα (63), (64) υιοθέτησαν τον AES αλγόριθμο ως το βασικό μηχανισμό ασφάλειας (65) για παροχή πιστοποίησης, έγκρισης και ακεραιότητας δεδομένων. Σε αυτά τα συστήματα οι περιορισμοί σε ισχύ και επιφάνεια του συστήματος είναι μεγάλοι. Οι νέες φορητές συσκευές (laptops, PDAs, κτλ.) μπορούν και δουλεύουν για λίγες ώρες μέχρι η μπαταρία τους να εξαντληθεί. Ακόμη χειρότερα, οι απαιτήσεις σε ενέργεια αυξάνουν με μεγαλύτερο ρυθμό από ότι η εξέλιξη της τεχνολογίας των μπαταριών (9), (66). Συστήματα όπως οι έξυπνες κάρτες και οι RFID ετικέτες (67) τα οποία εξάγουν ενέργεια από το ηλεκτρομαγνητικό πεδίο κάνουν το πρόβλημα πιο σύνθετο και δύσκολο. Ο σχεδιασμός σε υλικό (Hardware design) επιταχύνει τις πράξεις και μειώνει αισθητά τις ανάγκες σε ισχύ με ένα επιπλέον κόστος σε υλικό. Επομένως η ύπαρξη επιπρόσθετου υλικού που θα υποστηρίζει τις κρυπτογραφικές πράξεις είναι αναγκαία (20) αν ο σκοπός του σχεδιαστή είναι να κατασκευάσει αποδοτικά από πλευράς ισχύος συστήματα.

Η εξέλιξη των συστημάτων ασύρματης δικτύωσης έχει φέρει την ανάπτυξη νέων κρυπτογραφικών αναγκών. Επομένως, οι υπάρχουσες και νέες αρχιτεκτονικές κρυπτογραφίας πρέπει να προσαρμοστούν στις συνθήκες που επιβάλλουν τα περιορισμένα σε πόρους συστήματα. Τα πρότυπα ασύρματων - κινητών επικοινωνιών περιορίζουν την απόδοση των συστημάτων σε ρυθμούς κάτω των 100 Mbps. Αυτό είναι ένα αρκετά ικανοποιητικό όριο και είναι ικανό για να υποστηρίξει εφαρμογές σε πραγματικό χρόνο όπως φωνή, βίντεο και online streaming. Επιπλέον, ο περιορισμός των πόρων των συστημάτων αυτών ενεργοποιεί τις ανάγκες για περιορισμένη κατανάλωση ισχύος και επιφάνεια. Εντούτοις, πολλές υλοποιήσεις του αλγορίθμου

AES (69), (68), (78), (79) εστιάζονται στην επίτευξη υψηλού ρυθμού απόδοσης με τεχνικές όπως loop unrolling καθώς και εκτεταμένη χρήση καταχωρητών με την τεχνική pipelining για την αρχιτεκτονική του AES των 128-bit. Οι αρχιτεκτονικές αυτές επιτυγχάνουν ρυθμό απόδοσης ακόμη και πάνω από 10 Gbps, και είναι κατάλληλες για δικτυακές (high-end) εφαρμογές που δεν περιορίζονται από την κατανάλωση ισχύος και την επιφάνεια. Είναι αδύνατο να ενσωματωθούν αυτές οι υλοποιήσεις σε συστήματα περιορισμένων πόρων. Επιπλέον, οι υψηλές τιμές του ρυθμού απόδοσης είναι μη εφαρμόσιμες για συστήματα ασύρματων επικοινωνιών εφόσον δεν υπάρχει ακόμη η δυνατότητα μετάδοσης σε τέτοιους ρυθμούς μέσω αέρα.

Πρόσφατα, έχουν προταθεί πιο περιορισμένες από πλευράς κόστους επιφάνειας αρχιτεκτονικές για το πρότυπο AES. Κάποιες εργασίες (70), (72), (75), (74) προτείνουν αρχιτεκτονικές με χαμηλές απαιτήσεις σε επιφάνεια ή ισχύς για το μετασχηματισμό AES SubBytes, την κύρια κρυπτογραφική συνάρτηση, αλλά δεν κατορθώνουν να επιτύχουν σχήματα που να συνδυάζουν χαμηλής κατανάλωσης ισχύος και περιορισμένης επιφάνειας αρχιτεκτονικές. Το πρόβλημα αυτό αναφέρεται στο Κεφάλαιο 5 αλλά και στις εργασίες (80) και (25). Υπάρχουν επίσης εργασίες που παρουσιάζουν αποτελέσματα σε κατανάλωση ισχύος για τον AES αλγόριθμο όπως στις (81), (82) και (83). Οι εργασίες αυτές έχουν ικανοποιητικούς ρυθμούς απόδοσης αλλά απαιτούν μεγάλη επιφάνεια. Εργασίες όπως οι (84), (85) αποτελούν πιο ρεαλιστικές υλοποιήσεις για ασύρματες εφαρμογές περιορισμένων πόρων. Στην εργασία (84) προτείνεται μια περιορισμένων πόρων υλοποίηση με χαμηλή κατανάλωση ισχύος η οποία όμως υποστηρίζει μόνο 128-bits κρυπτογράφηση και επιτυγχάνει ρυθμό απόδοσης λιγότερο από 10 Mbps. Στην εργασία (85) προτείνεται μια περιορισμένων πόρων επιφάνειας υλοποίηση, η οποία έχει ρυθμό απόδοσης 2 Mbps, υποστηρίζει μόνο 128-bit κρυπτογράφηση και δεν υπάρχουν αποτελέσματα για την κατανάλωση ισχύος.

Στο κεφάλαιο αυτό προτείνεται αρχιτεκτονική για τον AES αλγόριθμο χαμηλής κατανάλωσης ισχύος και περιορισμένων πόρων σε επιφάνεια. Η αρχιτεκτονική αυτή υποστηρίζει 128, 192 και 256-bit λειτουργία-παραγωγή κλειδιών. Με στόχο την ικανοποίηση όλων των περιορισμών που θέτουν τα ασύρματα συστήματα, το σύστημά μας βελτιστοποιήθηκε σε όλα τα επίπεδα του σχεδιασμού. Επιπρόσθετα, οι βελτιστοποιημένες πράξεις SubBytes-MixColumns του Κεφαλαίου 5 ενσωματώθηκαν προσφέροντας σημαντική βελτίωση τόσο στους καταλυπτόμενους πόρους όσο και στην κατανάλωση ισχύος.

6.2.Ο αλγόριθμος AES (Advanced Encryption Standard)

Ο αλγόριθμος AES περιγράφεται περιληπτικά στην παράγραφο 5.13

6.3.Σχεδίαση του Συστήματος

Η σχεδίαση του συστήματος αποτελείται από διαφορετικά επίπεδα, όπως το επίπεδο τεχνολογίας, το επίπεδο συστήματος, το επίπεδο αλγορίθμου, το επίπεδο αρχιτεκτονικής, το επίπεδο καταχωρητή-πύλης και το φυσικό επίπεδο. Η βελτιστοποίηση σε τεχνολογικό και φυσικό επίπεδο είναι εφικτή μόνο σε επίπεδο βιομηχανίας. Εργαλεία όπως CAD-software και δημοσιευμένες σε διεθνές επίπεδο εργασίες μας δίνουν τη δυνατότητα να πάρουμε αποφάσεις για τα υπόλοιπα σχεδιαστικά επίπεδα σύμφωνα με τους περιορισμούς του συστήματός μας. Τεχνικές

χαμηλής κατανάλωσης ισχύος μπορούν να χρησιμοποιηθούν σε όλα τα επίπεδα του σχεδιασμού. Σε κάθε επίπεδο σχεδιασμού πρέπει να είμαστε εξίσου προσεκτικοί, γιατί οι αποφάσεις μας επηρεάζουν δραστικά τις βελτιστοποιήσεις μας στα παρακάτω επίπεδα.

Στην παρούσα εργασία εφαρμόζουμε σχεδιασμό και ανάλυση top-down κατευθυνόμενοι από τα υψηλά σχεδιαστικά επίπεδα στα χαμηλότερα με σκοπό να επιτύχουμε τους σχεδιαστικούς μας στόχους. Στην κατηγορία του συστήματος παίρνουμε τις παρακάτω αποφάσεις:

- Στο επίπεδο αυτό ορίζουμε τις βασικές προδιαγραφές του τελικού συστήματος. Ο βασικός στόχος μας είναι να μειώσουμε την κατανάλωση ισχύος καθώς και τους πόρους σε επιφάνεια. Ο ρυθμός απόδοσης ώστε να υποστηρίξουμε τα υπάρχοντα πρότυπα ασύρματων επικοινωνιών είναι κάτω των 100 Mbps. Οι παραπάνω απαιτήσεις κάνουν υποχρεωτική την ανάγκη του αλγορίθμου AES να υλοποιηθεί σε υλικό. Μία άλλη αιτία για την υλοποίηση σε υλικό είναι η αντίσταση των αλγορίθμων κρυπτογραφίας σε κρυπταναλυτικές επιθέσεις. (86).
- Οι πρόσβαση σε καταχωρητές απαιτεί λιγότερη κατανάλωση ισχύος (και τυπικά είναι πιο γρήγορη) από την πρόσβαση σε μεγάλα μπλοκ μνήμης. Η καταναλισκόμενη ισχύς αυξάνεται με το μέγεθος της μνήμης. Επίσης για λόγους ασφάλειας είναι προτιμότερη η χρήση καταχωρητών.
- Πολιτικές πρέπει να εφαρμοστούν σε όλα τα επίπεδα σχεδιασμού ώστε ο ρυθμός απόδοσης του τελικού συστήματος να μην πέσει κάτω από συγκεκριμένα όρια στην προσπάθεια να κατασκευαστεί σύστημα ασφάλειας χαμηλών πόρων.

Το επόμενο επίπεδο σχεδιασμού είναι το αλγοριθμικό. Σε αυτό το επίπεδο επιδιώκεται σύγκλιση μεταξύ του αλγόριθμου και τα φυσικά χαρακτηριστικά του συστήματος. Τα βασικά βήματα σε αυτήν την προσπάθεια είναι:

- Τα σενάρια λειτουργίας του συστήματος πρέπει να καθοριστούν. Οι δύο βασικές λειτουργίες του συστήματος είναι η κρυπτογράφηση και η αποκρυπτογράφηση. Επιπλέον υπάρχουν δύο αντίστοιχες διεργασίες δημιουργίας κλειδιών η forward και η reverse key. Όπως περιγράφεται στο πρότυπο του AES αλγορίθμου υπάρχουν επίσης τρεις διαφορετικές εκδοχές ασφάλειας – τρεις διαφορετικές εκδοχές μήκους κλειδιού 128, 192 ή 256 bit. Με σκοπό να διατηρήσουμε τα χαμηλά επίπεδα πόρων του συστήματος, μπορούμε να υλοποιήσουμε μόνο τις βασικές πράξεις-μετασχηματισμούς. Όπως θα δούμε και παρακάτω χρησιμοποιήσαμε εκτεταμένα την τεχνική resource sharing σε συνδυασμό με κατάλληλη λογική ελέγχου.
- Ένα βασικό θέμα σε αυτό το σημείο είναι ο χαρακτηρισμός των βασικών πράξεων του αλγορίθμου από πλευράς πολυπλοκότητας. Για αυτό το λόγο ο αλγόριθμος υλοποιήθηκε σε C. Οι βασικές πράξεις του αλγορίθμου υλοποιήθηκαν σε ξεχωριστές συναρτήσεις σε C. Ο πιο διάσημος Profiler στον κόσμο του ελεύθερου λογισμικού, οποίος δουλεύει σε συνδυασμό με το GCC compiler είναι το GNU Profiler ή Gprof (87). Κάθε συνάρτηση του αλγορίθμου AES χαρακτηρίστηκε βάσει του συνολικού χρόνου εκτέλεσης και βρέθηκε για τις SubBytes και MixColumns ότι καταναλώνουν αντίστοιχα 49 και 21 τοις εκατό, του συνολικού χρόνου εκτέλεσης. Αυτός ο χαρακτηρισμός

(profiling) μας δίνει μια πρώτη ανάλυση των πιο πολύπλοκων πράξεων του αλγορίθμου.

- Μια βασική απόφαση στο επίπεδο αλγορίθμου του σχεδιασμού είναι η επιλογή του datapath που θα ακολουθήσει η αρχιτεκτονική μας. Οι περισσότερες υλοποιήσεις του αλγορίθμου AES ακολουθούν αρχιτεκτονική 128-bit και 32-bit. Στην προτεινόμενη αρχιτεκτονική χρησιμοποιήσαμε 8-bit λογική με κύριο λόγο την περιορισμένη κατανάλωση ισχύος στους διαύλους επικοινωνίας (buses), και την περιορισμένη επιφάνεια των αριθμητικών μονάδων που χρησιμοποιούν λογική 8-bit. Κατά τη διάρκεια του χαρακτηρισμού των βασικών μετασχηματισμών του αλγορίθμου καταλήξαμε πως ο SubBytes μετασχηματισμός είναι πιθανό να συνεισφέρει περισσότερο στην επιφάνεια και στην κατανάλωση ισχύος. Ο μετασχηματισμός αυτός ακολουθεί 8-bit λογική. Χρησιμοποιώντας πάνω του ενός SubBytes δομικά στοιχεία, θα είχαμε αντίστοιχη αύξηση στην κατανάλωση ισχύος και επιφάνεια. Πρόχειρες εκτιμήσεις της απόδοσης του αλγορίθμου με ένα μόνο Subbytes μετασχηματισμό μας επιτρέπουν να προχωρήσουμε στην υλοποίηση του συστήματος. Επιπλέον, καθώς ο αλγόριθμος AES βασίζεται στο μαθηματικό υπόβαθρο των Finite Fields $GF(2^8)$, είναι πιο εύκολο για το σύστημα να ακολουθήσει την 8-bit λογική.

Λαμβάνοντας υπόψη τις προηγούμενες παρατηρήσεις μπορεί να προταθεί μια πρώτη εικόνα για την αρχιτεκτονική του αλγορίθμου AES, όπως φαίνεται στην Εικόνα 57. Τα βασικά δομικά στοιχεία της αρχιτεκτονικής είναι η AES logic Unit όπου βρίσκονται οι βασικές κρυπτογραφικές πράξεις, το Register file για την αποθήκευση και ενδιάμεση αποθήκευση των δεδομένων, η μονάδα ελέγχου (Control Unit) και οι πολυπλέκτες που οδηγούν τα δεδομένα με τη βοήθεια της μονάδας ελέγχου ανάλογα με το σενάριο λειτουργίας. Οι πράξεις ShiftRows και InvShiftRows όπως θα εξηγήσουμε αργότερα υποστηρίζονται από το register file σε συνδυασμό με τους πολυπλέκτες.

Εικόνα 57: Η αρχιτεκτονική του AES συστήματος

Για να αναλύσουμε την αρχιτεκτονική του συστήματος περισσότερο πρέπει να περιγράψουμε την πολιτική που ακολουθήσαμε για να εντάξουμε τις βασικές κρυπτογραφικές πράξεις (SubBytes και MixColumns) στο συνολικό σύστημα. Θα βασιστούμε στις αρχιτεκτονικές που προτάθηκαν στο Κεφάλαιο 5. Λεπτομέρειες για τις αρχιτεκτονικές αυτές υπάρχουν στο Κεφάλαιο 5, ενώ αναφέρονται πάλι στο παρόν Κεφάλαιο κάποια στοιχεία για διευκόλυνση του αναγνώστη. Οι υλοποιήσεις σε επίπεδο πύλης-καταχωρητή έχουν ως αποτέλεσμα σημαντικό κέρδος στην συνολική απόδοση του συστήματος, σε θέματα ισχύος και επιφάνειας.

6.4. Αρχιτεκτονική Χαμηλής Κατανάλωσης Ισχύος για το Μετασχηματισμό SubBytes

Περισσότερες λεπτομέρειες για την αρχιτεκτονική αυτή υπάρχουν στο Κεφάλαιο 5 όπου παρουσιάζεται αναλυτικά η μεθοδολογία για την προτεινόμενη αρχιτεκτονική για την πράξη SubBytes.

Όπως παρουσιάστηκε επιλέξαμε αρχικά για λόγους χαμηλού κόστους σε επιφάνεια την αριθμητική προσέγγιση για την αρχιτεκτονική των SubBytes/InvSubBytes. εκμεταλλευόμενοι το γεγονός ότι στο ίδιο κύκλωμα γίνεται και κρυπτογράφηση και αποκρυπτογράφηση. Έπειτα εφαρμόσαμε τεχνικές χαμηλής κατανάλωσης ισχύος. Το αποτέλεσμα ήταν η κατανάλωση ισχύος να μειωθεί αλλά παράλληλα μειώθηκε αισθητά ο παράγοντας «Ισχύς * Επιφάνεια», ο οποίος είναι καθοριστικός για χαμηλών πόρων συστήματα.

Εικόνα 58: Η προτεινόμενη αρχιτεκτονική του δομικού στοιχείου SubBytes

Από τις τέσσερις προτεινόμενες αρχιτεκτονικές του Κεφαλαίου 5 επιλέξαμε την τέταρτη (Implem2R) η οποία έχει τα καλύτερα αποτελέσματα σε κατανάλωση ισχύος εξαιτίας των τεχνικών που εφαρμόσαμε αλλά και εξαιτίας των καταχωρητών που τοποθετήσαμε. Επίσης το critical path είναι πολύ μικρό, και μας αφήνει περιθώρια ώστε να επιτύχουμε πολύ ικανοποιητικό ρυθμό απόδοσης.

Η προτεινόμενη αρχιτεκτονική SubBytes ελέγχεται μόνο από ένα εξωτερικό σήμα το οποίο καθορίζει αν βρισκόμαστε σε κρυπτογράφηση ή σε αποκρυπτογράφηση και απαιτούνται πέντε κύκλοι ρολογιού ώστε να εξαχθεί το αποτέλεσμα. Η μονάδα ελέγχου καθώς και οι πολυπλέκτες ελέγχουν τη ροή των δεδομένων τόσο κατά τη κρυπτογράφηση-αποκρυπτογράφηση, όσο και κατά την παραγωγή κλειδιών.

6.5. Αρχιτεκτονική Χαμηλής Κατανάλωσης Ισχύος για το Μετασχηματισμό MixColumns/InvMixColumns

Περισσότερες λεπτομέρειες για την αρχιτεκτονική αυτή υπάρχουν στο Κεφάλαιο 5 όπου παρουσιάζεται αναλυτικά η μεθοδολογία για την προτεινόμενη πράξη MixColumns/InvMixColumns.

Σε σχέση με την παράγραφο 6.4 όπου χρησιμοποιήσαμε αυτούσια την πράξη SubBytes/InvSubBytes από το 5^ο Κεφάλαιο, για την πράξη MixColumns/InvMixColumns πρέπει να γίνουν ορισμένες τροποποιήσεις ώστε η πράξη να λειτουργήσει στην 8-bit λογική. Θα χρησιμοποιήσουμε το δομικό στοιχείο Multiplier Εικόνα 54, μαζί με κατάλληλη λογική και καταχωρητές ώστε το σύστημά μας να μπορεί να λειτουργεί πάνω σε 8-bit δεδομένα. Όπως είδαμε, κάθε εξαγόμενο byte, της State του αλγορίθμου AES, στο οποίο έχει εφαρμοστεί ο μετασχηματισμός MixColumns/InvMixColumns προκύπτει από πολλαπλασιασμό μητρώων με bytes του προηγούμενου State. Επομένως οι βασικές πράξεις που χρησιμοποιούμε για να πάρουμε τα αποτελέσματα είναι ο πολλαπλασιασμός σε $GF(2^8)$ (Εικόνα 56), και η πρόσθεση μεταξύ των κατάλληλων γινομένων.

Εισάγουμε επιπλέον λογική, δηλαδή ένα σύνολο 8-bit καταχωρητών, 8-bit Xors και Muxes, για να υποστηρίξουμε την 8-bit MixColumns/InvMixColumns. Η λογική αυτή αποτελείται από δύο επιμέρους τμήματα τα Part1 και Part2, όπως φαίνεται στην Εικόνα 59. Κάθε τμήμα αποτελεί συνδυασμό Xor λογικής και κυκλικού καταχωρητή ολίσθησης. Με το σχεδιασμό αυτό, σύμφωνα με τη σχέση που εκφράζει MixColumns, τέσσερις κύκλοι ρολογιού απαιτούνται ώστε να ληφθεί το αποτέλεσμα. Ας περιγράψουμε το σενάριο λειτουργίας της πράξης MixColumns. Ένα byte εισάγεται στην είσοδο του κυκλώματος (Εικόνα 59), σε κάθε κύκλο ρολογιού. Στο τέλος του πρώτου κύκλου ρολογιού, το πρώτο αποτέλεσμα έχει αποθηκευτεί στους καταχωρητές του Part1. Κατά τη διάρκεια του δεύτερου κύκλου ρολογιού, τα πρώτα αποτελέσματα υφίστανται xor πράξη με τα επόμενα αποτελέσματα που προκύπτουν από το δεύτερο byte. Μετά από τέσσερις κύκλους ρολογιού το 32-bit αποτέλεσμα εμπεριέχεται στους τέσσερις καταχωρητές του Part1. Στο πέμπτο κύκλο ρολογιού, οι πολυπλέκτες (στην Εικόνα 59 είναι οριζόντια) μεταφέρουν τα δεδομένα στο Part2. Οι Mux1 ρυθμίζουν την έξοδο που είναι ενωμένη με τις XOR πύλες στην τιμή «00000000», ώστε να μην επηρεάζονται τα δεδομένα μεταξύ των καταχωρητών. Με αυτό τον τρόπο, τα δεδομένα τα οποία είναι αποθηκευμένα στο Part1 γράφονται στον κεντρικό καταχωρητή του συστήματος AES. Και τα 16 byte με αυτό τον τρόπο μπορούν και εξάγονται σε 20 κύκλους ρολογιού.

Εικόνα 59: 8-bit Αρχιτεκτονική της MixColumn/InvMixColumn

6.6. Χαμηλής Κατανάλωσης Αρχιτεκτονική AES

Στην Εικόνα 60 παρουσιάζονται τα σενάρια λειτουργίας του AES αλγορίθμου, οι αντίστοιχοι απαιτούμενοι κύκλοι και η σειρά των βασικών πράξεων. Τα βασικά σενάρια λειτουργίας του συστήματος είναι το σενάριο λειτουργίας κρυπτογράφησης με τις αντίστοιχες επιλογές κλειδιού (128, 192, 256) και το σενάριο αποκρυπτογράφησης με τις ίδιες επιλογές κλειδιού. Κάποιες βασικές διαφορές μεταξύ των σεναρίων λειτουργίας είναι οι εξής: Η κρυπτογράφηση υποστηρίζεται από τις πράξεις SubBytes, MixColumns, ShiftRows, Add Round Key (xor) και Key Expansion operations ενώ η αποκρυπτογράφηση υποστηρίζεται από τις πράξεις InvSubBytes, InvMixColumns, InvShiftRows, Add Round Key, Key Expansion και Reverse Key Expansion. Βασικές διαφορές μεταξύ κρυπτογράφησης και αποκρυπτογράφησης είναι η σειρά των πράξεων στους ενδιάμεσους κύκλους του αλγορίθμου καθώς και μια επιπρόσθετη αρχική Key Expansion λειτουργία που συμβαίνει κατά την αποκρυπτογράφηση. Επιπρόσθετα ο αριθμός των

κρυπτογραφικών κύκλων αλλάζει μεταξύ των τιμών 10, 12 και 14 σύμφωνα με τον αριθμό των ψηφίων του κλειδιού. Τα σενάρια λειτουργίας ορίζονται από την μονάδα ελέγχου και τους πολυπλέκτες.

N=10 or 12 or 14	κρυπτογράφηση	αποκρυπτογράφηση
αρχικοποίηση		Key Expansion
Πρώτος κύκλος	Add Round key	Add Round key
Ενδιάμεσοι κύκλοι	<i>Loop N-1 times</i> Key Expansion Subbytes ShiftRows MixColumns Add Round key <i>End Loop</i>	<i>Loop N-1 times</i> Rev Key Expansion InvSubbytes InvShiftRows Add Round key InvMixColumns <i>End Loop</i>
Τελευταίος κύκλος	Key Expansion Subbytes Shiftows Add Round key	Rev Key Expansion InvSubbytes InvShiftows Add Round key

Εικόνα 60: Τα σενάρια λειτουργίας του αλγορίθμου

Για καλύτερη κατανόηση του τελικού συστήματος, θα παρουσιάσουμε το σύστημα κρυπτογράφησης και το σύστημα υπολογισμού κλειδιού χωριστά. Μια σημαντική σημείωση είναι πως τα δύο συστήματα μοιράζονται το ίδιο SuBBytes δομικό στοιχείο. Στο τέλος θα παρουσιάσουμε από κοινού το σύστημα. Όπως έχουμε αναφέρει η αρχιτεκτονική μας είναι 8-bit. Επομένως με τη βοήθεια μονάδας ελέγχου υποστηρίζεται ο AES 128-bit αλγόριθμος.

Στην Εικόνα 61, η αρχιτεκτονική του κυρίου συστήματος (AES datapath) παρουσιάζεται. Τα βασικά αριθμητικά-δομικά στοιχεία της αρχιτεκτονικής είναι το SubBytes, MixColumns, Xor, ένα σύνολο πολυπλεκτών Muxes και ένας 128-bit καταχωρητής ολίσθησης. Το μήκος των διαύλων των δεδομένων είναι 8-bit. Τα βασικά αριθμητικά στοιχεία SubBytes και MixColumns υποστηρίζουν κρυπτογράφηση και αποκρυπτογράφηση μειώνοντας τη συνολική επιφάνεια του συστήματος αλλά και την πολυπλοκότητα στον έλεγχο του συστήματος.

Ένα σημαντικό πρόβλημα που αντιμετωπίσαμε κατά το σχεδιασμό του 8-bit συστήματος ήταν ότι οι πράξεις ShiftRows και MixColumns δεν απαιτούν τα δεδομένα σειριακά, όπως η πράξη SubBytes. Αν προσπαθούσαμε να επιλύσουμε το πρόβλημα αυτό με χρήση πολύπλοκων σχηματισμών πολυπλεκτών και καταχωρητών ώστε να εισάγουμε καθυστέρηση στα δεδομένα τότε ουσιαστικά δε θα κερδίζαμε σε καταλυπτόμενη επιφάνεια. Αντίθετα το πρόβλημα θα μεταφερόταν στους

πολυπλέκτες. Για να υπερνικήσουμε το πρόβλημα αυτό, συνδέσαμε τα τέσσερα αριστερά bytes του καταχωρητή ολίσθησης του AES συστήματος (Εικόνα 59) με ένα πολυπλέκτη. Με αυτόν τον τρόπο έχουμε τη δυνατότητα να επιλέγουμε οποιοδήποτε των τεσσάρων αυτών bytes και έτσι να υποστηρίζεται η πράξη ShiftRows (και InvShiftRows για την αποκρυπτογράφηση). Όπως είδαμε στην περιγραφή του αλγορίθμου AES, το State είναι ένα 4 x 4 μητρώο όπου κάθε στοιχείο του είναι ένα byte. Η πράξη MixColumns εφαρμόζεται σε κάθε στήλη χωριστά του μητρώου. Επομένως στην περίπτωση της κρυπτογράφησης μπορούμε να συνδυάσουμε τις πράξεις ShiftRows και MixColumns και να διαβάζουμε τα δεδομένα από τον καταχωρητή ολίσθησης του AES με την εξής σειρά 1, 6, 11, 16, 2, 7, 12, 13, 3, 8, 9, 14, 4, 5, 10, 15. Ένα παρόμοιο σενάριο εφαρμόζεται και για την αποκρυπτογράφηση. Οι πράξεις εκτελούνται παράλληλα και καμία από τη μονάδα δεν περιμένει την άλλη να τελειώσει. Η δυνατότητα αυτή αυξάνει το ρυθμό απόδοσης του συστήματος.

Στην Εικόνα 62, παρουσιάζεται το σύστημα που υποστηρίζει τη δημιουργία κλειδιών (Key Expansion Scheme) του AES αλγορίθμου. Σε αυτήν την περίπτωση χρησιμοποιείται ένας άλλος κυκλικός καταχωρητής ολίσθησης (Shift Register) ο οποίος είναι 256-bit. Οι αριθμητικές μονάδες του αλγορίθμου AES Subbytes και Rcon χρησιμοποιούνται. Τα bits του καταχωρητή χωρίζονται σε σύνολα των τεσσάρων bytes. Κάθε σύνολο (4 bytes) αποθηκεύει λέξεις 32-bit. Όταν η μονάδα δημιουργίας κλειδιών λειτουργεί σε 128-bit σενάριο λειτουργίας τότε τα τέσσερα αριστερά σύνολα απενεργοποιούνται, σε 192-bit σενάριο λειτουργίας τα δύο αριστερά σύνολα, ενώ στην περίπτωση των 256-bits κανένα. Το σύστημά μας υποστηρίζει τόσο τη λειτουργία Key Expansion για την κρυπτογράφηση τόσο τη λειτουργία Reverse Key Expansion για την αποκρυπτογράφηση. Όταν η δημιουργία του κλειδιού ολοκληρώνεται τότε το κλειδί περνάει στο σύστημα (AES datapath).

Εικόνα 61: 8-bit προτεινόμενη αρχιτεκτονική AES

Εικόνα 62: Η αρχιτεκτονική Key Expansion

Στον επόμενο πίνακα παρουσιάζονται οι συνολικοί κύκλοι ρολογιού που απαιτούνται για κάθε σενάριο λειτουργίας. Οι απαιτούμενοι κύκλοι για την ολοκλήρωση της κρυπτογράφησης ή της αποκρυπτογράφησης έχουν άμεσο αποτέλεσμα στον τελικό ρυθμό απόδοσης του συνολικού συστήματος ανάλογα με το σενάριο λειτουργίας στο οποίο βρισκόμαστε, όπως παρουσιάζεται στον Πίνακα 12.

Πίνακας 11: Οι απαιτούμενοι κύκλοι για διαφορετικά κλειδιά

Μήκος Κλειδιού	128-bit	192-bit	256-bit
Κρυπτογράφηση	537	805	983
Αποκρυπτογράφηση	553	831	1005

Στον παρακάτω Πίνακα παρουσιάζονται συγκρίσεις σχετικά πάνω στην αρχιτεκτονική του AES. Οι εργασίες (81), (88), (82), και (83) βασίζονται στο 128-bit datapath και προορίζονται για πολύ υψηλής απόδοσης εφαρμογές. Οι εργασίες (84), (85) λειτουργούν πάνω σε λογική 8-bit παρόμοια με τη δική μας. Βασικά μειονεκτήματα των υλοποιήσεων αυτών είναι ότι λειτουργούν μόνο σε 128-bit κλειδιά. Η εργασία (85) χρησιμοποιεί ROM για να αποθηκεύσει το πρόγραμμα και δεν αναφέρει αποτελέσματα σε κατανάλωση ισχύος, ενώ η εργασία (84) δεν παρέχει λεπτομέρειες για τη δημιουργία των κλειδιών και αποθηκεύει τα ενδιάμεσα δεδομένα σε RAM.

Πίνακας 12: Συγκρίσεις αρχιτεκτονικών AES

	Verbauwheide (81)	Su (88)	Hodjat (82)	Feldhofer (84)	Lin (83)	Good (85)	Προτεινόμενη
Τεχνολογία	0.18μm	0.35 μm	0.18 μm	0.35 μm	0.13 μm	FPGA	0.18 μm
Συχνότητα	154 MHz	200 MHz	295 MHz	80 MHz	333 MHz	72.3 MHz	180 MHz
Επιφάνεια (g.eq)	173K	58.4K	73.2K	3.4K	86.2K	262 Eq.SI	7.545K
Ισχύς	56mW	230.6mW	86mW	0.45mW	40.9mW	N/A	0.82-0.88mW 0.95 -1.01mW 1.05-1.11mW
Ρυθμός Απόδοσης	1.6 Gbps 1.33 Gbps 1.14 Gbps	2.3 Gbps 2 Gbps 1.74 Gbps	46.9 Gbps	9 Mbps	49.54 Gbps 41.30 Gbps 35.38 Gbps	2.18 Mbps	42.9 -Mbps 28.6 -Mbps 23.4 -Mbps
Ισχύς*Επιφάνεια	9688 K.mW	13467 K.mW	6395.2 K.mW	1.53 K.mW	3525.58 K.mW	N/A	6.187K.mW
Υποστηριζόμενα Κλειδιά	all	all	all	128	all	128	all

Στην Εικόνα 63 κάνουμε μια εκτίμηση για τη συνολική ενέργεια που απαιτείται, σε κάθε σενάριο λειτουργίας, ώστε να κωδικοποιηθεί ένα μπλοκ 128-bit. Στον άξονα των X αναφέρονται οι μονάδες ενέργειας, ενώ στον άξονα των Y υπάρχουν τα διαφορετικά σενάρια λειτουργίας.

Εικόνα 63: Η συνολική ενέργεια σε σχέση με τα διαφορετικά σενάρια λειτουργίας

Στην παρακάτω Εικόνα 64 παρουσιάζεται η κατανομή της επιφάνειας του συστήματος στα βασικά δομικά στοιχεία του συστήματος. Ο μετασχηματισμός SubBytes/InvSubBytes καταλαμβάνει 9.4%, ο μετασχηματισμός MixColumns το 9%, οι πολυπλέκτες και όλοι η υπόλοιπη λογική καταλαμβάνει το 33.4%, οι καταχωρητές καταλαμβάνουν το 33.4% ενώ η μονάδα ελέγχου το 20.5 % της συνολικής επιφάνειας.

Εικόνα 64: Η κατανομή της συνολικής επιφάνειας του συστήματος στα δομικά στοιχεία

6.7.Συμπεράσματα

Στο κεφάλαιο αυτό υλοποιήθηκε η αρχιτεκτονική 8-bit για τον AES αλγόριθμο κρυπτογράφησης. Ειδικό βάρος δόθηκε το ώστε το σύστημα να έχει χαμηλό κόστος επιφάνειας και περιορισμένη κατανάλωση ισχύος ώστε να είναι ιδανικό για χαμηλής κατανάλωσης εφαρμογές. Ο ρυθμός απόδοσης του συστήματος είναι αρκετά ικανοποιητικός και καλύπτει πρωτόκολλα ασύρματων επικοινωνιών. Το προτεινόμενο σύστημα υποστηρίζει και τις τρεις δυνατότητες κρυπτογράφησης με κλειδιά 128, 192 και 256-bit. Οι βασικές πράξεις του AES αλγορίθμου βελτιστοποιήθηκαν από πλευράς κατανάλωσης ισχύος και απόδοσης. Ακολουθήθηκε σχεδιασμός top-down και εφαρμόστηκαν τεχνικές σχεδιασμού σε υλικό σε όλα τα επίπεδα.

ΚΕΦΑΛΑΙΟ 7. Τελικά συμπεράσματα και μελλοντική εργασία

Σκοπός της διδακτορικής διατριβής είναι η ενσωμάτωση μηχανισμών ασφαλείας σε υλικό για περιβάλλοντα περιορισμένων πόρων (ενέργεια, ισχύς, κόστος υλικού). Στο Κεφάλαιο 4, προτείνεται πρωτόκολλο ασφάλειας για συστήματα πολύ χαμηλών πόρων. Το πρωτόκολλο ασφαλείας στηρίζεται στον αλγόριθμο κρυπτογραφίας DES (9). Επιλέγουμε τους κατάλληλους μηχανισμούς ώστε να υποστηρίξουμε το πρωτόκολλο ασφάλειας πάλι με κριτήριο τους μειωμένους πόρους της συσκευής. Έπειτα τεχνικές χαμηλής κατανάλωσης ισχύος και υλικού εφαρμόζονται ώστε το σύστημά μας να διαχειριστεί πιο αποδοτικά την καταναλισκόμενη ισχύς αλλά και να είναι περιορισμένο σε επιφάνεια.

Υπάρχουν τρεις συνεισφορές στο θέμα της βελτιστοποίησης βασικών κρυπτογραφικών δομικών στοιχείων και παρουσιάζονται στο Κεφάλαιο 5. Αρχικά παρουσιάζεται η υλοποίηση ενός επαναπροσδιορίσιμου σειριακού πολλαπλασιαστή σε αριθμητική πεπερασμένων σωμάτων (Finite Fields) για συστήματα περιορισμένων πόρων. Ο πολλαπλασιαστής αυτός έχει το πλεονέκτημα ότι διατηρώντας χαμηλούς τους πόρους σε υλικό και ισχύ, εκτελεί κάτω από m κύκλους αλγορίθμου (περίπου 34% πιο γρήγορα) τον πολλαπλασιασμό. Επίσης έχει τη δυνατότητα να υποστηρίζει οποιοδήποτε πολυώνυμο μέχρι m ψηφία μήκος αλλά και οποιοδήποτε ανάγωγο (irreducible) πολυώνυμο προσφέροντας διαφορετικών επιπέδων ασφάλεια. Η δυνατότητα αυτή το κάνει κατάλληλο συστατικό για συστήματα ελλειπτικών καμπυλών χαμηλών πόρων.

Η βασική κρυπτογραφική πράξη του αλγορίθμου AES (Advanced Encryption Standard), SuBBytes/InvSubBytes, με ιδιότητες χαμηλής κατανάλωσης ισχύος και σε μικρό κόστος επιφάνειας είναι το δεύτερο δομικό κρυπτογραφικό στοιχείο που βελτιστοποιήθηκε και παρουσιάζεται στο Κεφάλαιο 5. Αρχικά έγινε μια μελέτη διαφορετικών προσεγγίσεων-υλοποιήσεων του μετασχηματισμού SubBytes. Έπειτα παρουσιάστηκε η μεθοδολογία ώστε να καταλήξουμε στην προσέγγιση όπου είναι ιδανική για χαμηλών πόρων συστήματα.

Μια εξίσου σημαντική πράξη του αλγορίθμου AES βελτιστοποιήθηκε με σκοπό τη χαμηλή κατανάλωση ενέργειας και τους μειωμένους πόρους σε υλικό είναι η MixColumns που βελτιστοποιείται στο Κεφάλαιο 5. Βρίσκοντας λογικές συνθήκες στην είσοδο του συστήματος ώστε να κρατάμε ανενεργά δομικά στοιχεία του, κατορθώνουμε να εξοικονομούμε συνολική ενέργεια μειώνοντας το ρυθμό κατανάλωσης ισχύος. Επιπλέον τεχνικές εφαρμόζονται για τη μείωση του συνολικού κόστους σε υλικό.

Στο Κεφάλαιο 6 μια ολοκληρωμένη μεθοδολογία για σχεδιασμό χαμηλής κατανάλωσης ισχύος κρυπτογραφικά συστήματα προτείνεται. Παρουσιάζεται αναλυτικά όλη η διαδικασία μέχρι ο σχεδιαστής να καταλήξει στην υλοποίηση σε

υλικό. Σαν εφαρμογή χρησιμοποιούμε τον αλγόριθμο AES. CAD εργαλεία και πακέτα λογισμικού υψηλού επιπέδου (Γλώσσα Προγραμματισμού C) αποτελούν χρήσιμα εργαλεία σε αυτήν την προσπάθεια. Οι ήδη προτεινόμενες αρχιτεκτονικές χαμηλών πόρων (Κεφάλαιο 5) για τους μετασχηματισμούς SubBytes και MixColumns βοηθούν ώστε τα τελικά μας αποτελέσματα να είναι ακόμη καλύτερα. Διαφορετικά σενάρια λειτουργίας του αλγορίθμου δίνουν τη δυνατότητα για συσχέτιση επιπέδων ασφάλειας με επίπεδα καταναλισκόμενης ενέργειας του συστήματος χαμηλών πόρων.

Τα συμπεράσματα που εξάγονται κατά την εκπόνηση της παρούσας διδακτορικής διατριβής είναι τα ακόλουθα:

Η επιλογή πρωτοκόλλων ασφαλείας με τους ελάχιστους δυνατούς πόρους είναι αναγκαία για χαμηλών πόρων εφαρμογές. Προσεχτική μελέτη απαιτείται στο πρωτόκολλο το οποίο θα επιλέξουμε, τους αλγορίθμους που θα υποστηρίζουν το πρωτόκολλο καθώς και το σχεδιασμό του αλγορίθμου σε επίπεδο αρχιτεκτονικής και πύλης-καταχωρητή. Κατά το σχεδιασμό των συστημάτων υπάρχει ανάγκη για μελέτη σε όλα τα επίπεδα σχεδιασμού, όπως επίπεδο συστήματος, αλγορίθμου, αρχιτεκτονικής και πύλης-καταχωρητή.

Εργαλεία τα οποία χαρακτηρίζουν τις βασικές κρυπτογραφικές πράξεις από πλευράς πολυπλοκότητας και κόστους σε υλικό μας βοηθούν στην επιλογή των μετασχηματισμών, όπου πρέπει να δώσουμε ιδιαίτερο βάρος κατά την ολοκλήρωσή τους σε υλικό.

Υπάρχει ανάγκη ώστε τα κρυπτογραφικά συστήματα περιορισμένων πόρων να χαρακτηρίζονται με μέτρο τον παράγοντα «Επιφάνεια x Ισχύς», ενώ ο ρυθμός απόδοσης καθορίζεται από το πρότυπο - πρωτότυπο. Η προσπάθεια των σχεδιαστών στην κρυπτογραφία να μειώσουν την επιφάνεια των κυκλωμάτων βασικών κρυπτογραφικών πράξεων δεν οδηγεί σε αντίστοιχα αποτελέσματα σχετικά με την κατανάλωση ισχύος. Παραδείγματα είναι οι πράξεις MixColumns και SubBytes του αλγορίθμου AES, όπου προτάθηκαν στο παρελθόν εργασίες για συστήματα περιορισμένων πόρων, με μικρή επιφάνεια, χωρίς να λάμβαναν υπόψη την κατανάλωση ισχύος η οποία αυξανόταν.

Τεχνικές σε όλα τα επίπεδα με σκοπό τους περιορισμένους πόρους του συστήματος εφαρμόζονται. Η εφαρμογή του gated clock σε συνδυασμό με διοχέτευση προσδίδει στο κύκλωμα καλύτερες ιδιότητες από πλευράς κατανάλωσης ισχύος και συνολικής κατανάλωσης ενέργειας.

Η υποστήριξη πολλαπλών σεναρίων ασφάλειας επιτρέπει στο σύστημα να λειτουργεί σε περισσότερη της μιας κατάσταση για μια συγκεκριμένη λειτουργία (π.χ. κρυπτογράφηση) με αποτέλεσμα να ρυθμίζεται η παρεχόμενη ασφάλεια ανάλογα με τις απαιτήσεις σε απόδοση ή τους πόρους του συστήματος. Μπορεί να συνεργαστεί με περισσότερες οντότητες που τα συστήματα ασφαλείας τους ανήκουν στο σύνολο συστημάτων ασφαλείας που διαθέτει. Επιπλέον, είναι απαραίτητο πολλές φορές να επιδιώκεται κατά το σχεδιασμό των κρυπτογραφικών πράξεων το χαρακτηριστικό της

ευελιξίας (versatility), ώστε να υποστηρίζονται πολλαπλά σενάρια του ίδιου αλγορίθμου.

Ειδική σημασία πρέπει να δοθεί στους βασικούς κρυπτογραφικούς μηχανισμούς-μετασχηματισμούς που υποστηρίζουν τους αλγόριθμους κρυπτογραφίας. Οι αλγόριθμοι κρυπτογραφίας στηρίζουν την ασφάλειά τους σε τέτοιους πολύπλοκους μηχανισμούς οι οποίοι είναι βασικές πηγές κατανάλωσης ισχύος και καταλαμβάνουν σημαντικό ποσοστό της επιφάνειας. Η προσπάθεια βελτιστοποίησης των αλγορίθμων αυτών από πλευράς κατανάλωσης ισχύος και συνολικής επιφάνειας επιφέρει δραστική βελτίωση στις συνολικές ιδιότητες του αλγορίθμου.

Μελλοντική εργασία αποτελεί η μελέτη προβλημάτων σχετικά με κατανάλωση ισχύος και ασφάλεια – όχι όμως σε επίπεδο υλικού αλλά σε επίπεδο δικτύου. Η κατανάλωση ισχύος και η ασφάλεια αποτελούν από τα σημαντικότερα θέματα και στα ασύρματα δίκτυα αισθητήρων.

Ένα ασύρματο δίκτυο αισθητήρων (**wireless sensor network WSN**) (89) είναι ένα ασύρματο δίκτυο που αποτελείται από διανεμημένες στο χώρο αυτόνομες συσκευές που χρησιμοποιούν αισθητήρες για να ελέγχουν συνεταιριστικά τις φυσικές ή περιβαλλοντικές συνθήκες, όπως θερμοκρασία, ήχος, πίεση, κίνηση ή ρύποι, σε διαφορετικές θέσεις. Η ανάπτυξη των ασύρματων δικτύων αισθητήρων παρακινήθηκε αρχικά από τις στρατιωτικές εφαρμογές για την επιτήρηση πεδίων μαχών. Εντούτοις, τα ασύρματα δίκτυα αισθητήρων χρησιμοποιούνται τώρα σε πολλούς τομείς, συμπεριλαμβανομένου του περιβάλλοντος και της παρακολούθησης βιότοπων, των εφαρμογών υγειονομικής περίθαλψης, της αυτοματοποίησης, και του ελέγχου της κυκλοφορίας.

Επιπλέον, κάθε κόμβος σε ένα δίκτυο αισθητήρων είναι εξοπλισμένος με ράδιο-πομποδέκτη ή άλλη ασύρματη συσκευή επικοινωνιών, μικροελεγκτή, και μια πηγή ενέργειας, συνήθως μια μπαταρία. Το προβλεπόμενο μέγεθος ενός ενιαίου κόμβου αισθητήρων ποικίλει, ενώ είναι αξιόπιστοι ακόμη και σε μέγεθος νομίσματος. Το κόστος των κόμβων αισθητήρων είναι ομοίως μεταβλητό, κυμαινόμενο από εκατοντάδες των δολαρίων ως μερικά σεντ, ανάλογα με το μέγεθος του δικτύου αισθητήρων και της πολυπλοκότητας που απαιτείται από τους μεμονωμένους κόμβους αισθητήρων. Οι περιορισμοί μεγέθους και δαπανών στους κόμβους αισθητήρων οδηγούν στους αντίστοιχους περιορισμούς στους πόρους όπως η ενέργεια, η μνήμη, η ταχύτητα και το εύρος ζώνης

Ένα σημαντικό πρόβλημα στα ασύρματα δίκτυα αισθητήρων (Sensor networks) είναι η μεγιστοποίηση της διάρκειας ζωής των κόμβων. Αυτό μπορεί να οριστεί ως η μεγιστοποίηση του συνολικού αριθμού ροών (flows) που ένα δίκτυο αισθητήρων μπορεί να εξυπηρετήσει και αναλύεται ως η ικανότητα του δικτύου να δρομολογήσει οποιαδήποτε ροή από έναν κόμβο i σε οποιοδήποτε κόμβο k , σύμφωνα με την τοπολογία του δικτύου και την τεχνολογία των κόμβων. Το θέμα αυτό περιλαμβάνει την μοντελοποίηση πινάκων δρομολόγησης καθώς και τις διαφορετικές πολιτικές δρομολόγησης σε ένα περιβάλλον συνεργασίας με σκοπό τη βέλτιστη δρομολόγηση από πλευράς κατανάλωσης ισχύος της πληροφορίας. Προκειμένου να λυθεί και να μοντελοποιηθεί το πρόβλημα αυτό μελετούνται θέματα γραμμικής βελτιστοποίησης (90).

Ένα άλλο θέμα που μελετάται είναι ο επαναπροσδιορισμός θεμάτων ασφάλειας σε επίπεδο δικτύου. Η ασφάλεια δικτύου να αποτρέπει την επιβλαβή δραστηριότητα όχι μόνο επιτιθέμενων στο δίκτυο αλλά και οντοτήτων που έχουν εγωιστική συμπεριφορά (8). Ένα παράδειγμα στην περίπτωση των ασύρματων δικτύων, είναι η επιβλαβής δραστηριότητα μιας οντότητας με το να μεταδίδει συνεχώς πληροφορία σε ένα ασύρματο κανάλι και να προκαλεί συγκρούσεις πακέτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. **James Goodman, Abram P. Dancy, Anantha P. Chandrakasan.** An Energy/Security Scalable Encryption Processor Using an Embedded Variable Voltage DC/DC Converter. IEEE Journal of Solid-State Circuits. 1998.
2. **Kilts, Steve.** Advanced FPGA Design: Architecture, Implementation, and Optimization. s.l. : Wiley-IEEE Press, 2007.
3. **David Chinnery, Kurt Keutzer.** Closing the Power Gap between ASIC & Custom: Tools and Techniques for Low Power Design . s.l. : Springer, 2007.
4. **Anderson, Ross J.** Security Engineering: A Guide to Building Dependable Distributed Systems. s.l. : Wiley, 2008.
5. **Kocher, Paul C.** Differential Power Analysis. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology . 1999.
6. **A.G. Voyiatzis, A.G. Fragopoulos, D.N. Serpanos.** Chapter in R. Zurawski (editor), The Embedded Systems Handbook. CRC Press, 2006.
7. **W. Rankl, W. Effing.** Smart Card Handbook, 2nd Edition. s.l. : John Wiley & Sons, 2000.
8. **Levente Buttyan, Jean-Pierre Hubaux.** Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. s.l. : Cambridge University Press, 2008.
9. **Tilman Glökler, Heinrich Meyr.** Design of Energy-Efficient Application-Specific Instruction Set Processors. s.l. : Springer, 2004.
10. **DES.** 46-3, NIST FIPS. 1999. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.
11. **Alfred Menezes, Paul van Oorschot and Scott Vanstone.** Handbook of Applied Cryptography. s.l. : CRC-Press, 1996.
12. **Schneier, Bruce.** Applied Cryptography: Protocols, Algorithms, and Source Code in C. s.l. : Wiley, 1995.
13. **Kahn, David.** The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. s.l. : Scribner; Rev Sub edition, 1996.
14. **Feistel, H.** Cryptography and computer privacy. s.l. : Scientific American, 1973.
15. **AES.** Advanced Encryption Standard. Federal Information Processing Standards Publication 197 (FIPS PUB 197). 2001.
16. **Diffie, W. and Hellman, M.** New directions in cryptography. IEEE Transactions on Information Theory. 1976.
17. **R. L. Rivest, A. Shamir and L. Adleman.** A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978.
18. **J. M. Rabaey, A. Chandrakasan, B. Nikolic.** Digital Integrated Circuits: A Design Perspective, 2nd edition. 2nd edition. s.l. : Prentice-Hall, 2003.

19. **A.P. Chandrakasan, S. Sheng and R.W. Brodersen.** Low-power CMOS digital design. IEEE Journal of Solid-State Circuits. 1992.
20. **O. Koufopavlou, G. Selimis, N. Sklavos and P. Kitsos.** Cryptography: Circuits and Systems Approach. 5th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT05), Greece. 2005.
21. **P.Kitsos, O. Koufopavlou, G. Selimis and N. Sklavos.** Low Power Cryptography. Institute of Physics publishing, Journal of Physics: Conference Series (10) 2005.
22. **N. Sklavos, A. Papakonstantinou, Sp. Theoharis and O. Koufopavlou.** Low Power Implementation of an Encryption/Decryption System with Asynchronous Techniques. VLSI Design, An International Journal of Custom-Chip Design, Simulation, and Testing, Taylor and Francis Journal, Vol. 15, Issue 1, pp. 455-468. 2002.
23. **Pui-Lam Siu, Chiu-Sing Choy, Butas, J. and Chan, C.F.** A low power asynchronous DES. ISCAS . 2001.
24. **<http://www.synopsys.com>.**
25. **G. Selimis, A. Kakarountas, A. Fournaris, A. Milidonis, O. Koufopavlou.** A Low Power Design for SBOX Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users. Journal of Low Power Electronics. 2007, Vol. 3, 3.
26. **Rivest, Ronald L.** The RC5 encryption algorithm. Workshop on Fast Software. 1995.
27. **N.R. Potlapally, S. Ravi, A. Raghunathan and N.K. Jha.** Analyzing the energy Consumption of Security Protocols. Low Power Electronics and Design, 2003. ISLPED '03. 2003.
28. **Malik, S. Devadas and S.** A survey of optimization techniques targeting low power VLSI circuits. In Proceedings of the 32nd ACM/IEEE Conference on Design Automation. 1995.
29. **Veendrick, H.J.M.** Short-circuit dissipation of static CMOS circuitry and its impact on the design of buffer circuits. IEEE Journal of Solid-State Circuits. 1984.
30. **S. Turgis, N. Azemard and D Auvergne.** Explicit evaluation of short circuit power dissipation for CMOS logic structures. International Symposium on Low Power Design. 1995.
31. **K. Roy, S. Mukhopadhyay and H. Mahmoodi-Meimand.** Leakage current mechanisms and leakage reduction techniques in deep-submicrometer CMOS circuits. Proceedings of the IEEE, 91(2):305–327. 2003.
32. **Vivek De, Shekhar Borkar.** Technology and design challenges for low power and high performance. In International Symposium on Low Power Electronics and Design (ISLPED). 1999.
33. **46-3, FIPS.** Federal Information National Institute of Standards and Technology (1999, October 25). National Institute of Standards and Technology (1999, October 25).
34. **X9.17, ANSI.** Federal Information Processing Standards 171 1992 Key Management Using .
35. **Tools, Power.** http://www.xilinx.com/products/design_resources/power_central/index.htm. XILINX.
36. **Paolo Ienne, Rainer Leupers.** Customizable Embedded Processors: Design Technologies and Applications. Morgan Kaufmann. 2006.
37. **Berlekamp, E. R.** Algebraic Coding Theory. s.l. : McGraw-Hill, 1968.

38. **Koblitz, N.** Elliptic Curve Cryptography. s.l. : Math. Computation, vol. 48, no. 177, pp. 203-209, 1987.
39. **D. Harkelson, A. Menezes and S. Vanstone.** Guide to Elliptic Curve Cryptography. s.l. : Springer Verlag New York, 2004.
40. **Sunar, C. K. Koc and B.** Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields. IEEE Trans. Comput. 1998.
41. **C. Paar, N. Lange.** A comparative VLSI synthesis of finite field multipliers. proceedings of the third International Symposium of Communication Theory and its Applications, Lake District, UK. 1995.
42. **R. C Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson.** Optimal Normal Bases $GF(p^m)$. Discrete Applied Mathematics, 22(2):149-161. 1989.
43. **Mastrovito, E. D.** VLSI Architectures for Computation in Galois Fields. Ph. D. Thesis, Linkopings Universitet, Lingoping, Sweden. 1991.
44. **M. Hutter, J. Großschald, G.A. Kamenje.** A Versatile and Scalable Digit-Serial/Parallel Multiplier Architecture for $GF(2^m)$ Finite Fields. proceedings of the 4th International Conference on Information Technology: Coding and Computing. 2003.
45. **Paar, C.** Efficient VLSI Architectures for Bit Parallel Computation in Galois Fields. Ph. D. Thesis, Universitat GH Essen, Essen, Germany. 1994.
46. **T. Zhang, K. K. Parhi.** Systematic design of original and modified Mastrovito multipliers for general irreducible polynomials. IEEE Transactions on Computers, 50(7):734-749. 2001.
47. **Wu, H.** Bit-parallel finite field multiplier and squarer using polynomial basis. IEEE Transactions on Computers, 51:750-758. 2002.
48. **M. A. Hasan, V. K. Bhargava.** Division and bit-serial multiplication over $GF(q^m)$. IEE Proceedings-E, 139(3):230-236. 1992.
49. **P.A. Scott, S.E.Tavares, L.E. Peppard.** A fast VLSI Multiplier for $GF(2^m)$. IEEE JSAC. 1986.
50. **P. Kitsos, G. Theodoridis, O. Koufopavlou.** An efficient reconfigurable multiplier architecture for Galois field $GF(2^m)$. Elsevier Science Microelectronics Journal. 2003.
51. **C. Paar, P. Fleischmann, P. Soria-Rodriguez.** Fast arithmetic for public-key algorithms in Galois field with composite exponents. IEEE Transactions on Computers, 48(10) 1025-1034. 1999.
52. **J. H. Guo, C. L. Wang.** Digit-serial systolic multiplier for finite fields $GF(2^m)$. IEEE Proceedings-Computers and Digital Techniques, 145(2):143-148. 1998.
53. **Gustafson, O.** A digit-serial polynomial basis $GF(2^m)$ multiplier. in Proceedings of the 3rd IEEE Nordic Signal Processing Symposium (NORSIG '98), pp. 173-176, Aalborg, Denmark. 1998.
54. **L. Song, K.K. Parhi.** Efficient Finite Field Serial/Parallel Multiplication. IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'96). 1996.
55. **M. K. Ibrahim, A. S. Almulhem.** Bit-level pipelined digit serial $GF(2^m)$ multiplier. in Proceedings of the 34th IEEE Int. Symposium on Circuits and Systems (ISCAS 2001), vol. IV, pp. 586-589, Sydney Australia. 2001.

56. **C. H. Kim, C. P. Hong, S. Kwon.** A Digit-Serial Multiplier for Finite Field $GF(2^m)$. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no 4. 2005.
57. **James Goodman, Anantha P. Chandrakasan.** An Energy-Efficient Reconfigurable public-key Cryptography Processor. IEEE Journal of solid-state circuits, vol.36, NO.11. 2001.
58. **Mathematica.** <http://www.wolfram.com/>.
59. **M. A. Hasan, M. Ebtetaei.** Efficient architectures for computations over variable dimensional Galois field. IEEE Trans. Circuits Systems I Fundam. Theory Appl. vol. 45, no. 11. 1995.
60. **H. S. Kim, K.Y. Yoo.** Area efficient exponentiation using modular multiplier/squared in $GF(2^m)$. Lecture Notes in Computer Science, 2108, pp 262-267, Springer. 2001.
61. **Coron, J. S.** Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. Workshop on Cryptographic Hardware and Embedded Systems (CHES). 1999.
62. **M. Joye, C. Tymen.** Protections Against Differential Analysis for Elliptic Curve Cryptography. In Proc. of 2001 Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001). 2001.
63. **Standard, IEEE.** Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). 1999.
64. **802.16-2001,** IEEE Standard for Local and Metropolitan Area Networks, part 16, Air Interface for Fixed Broadband Wireless Access Systems, IEEE Press. 2001.
65. **802.11i-2004:** Standard for Information technology - Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements. 2004.
66. **Boukerche, A.** Handbook of Algorithms for Wireless Networking and Mobile Computing. s.l. : Chapman & Hall/CRC, 2005.
67. **Finkenzeller, K.** RFID Handbook - Fundamentals and Applications in Contactless Smart Cards & Identification. s.l. : John Wiley and Sons Ltd, 2003.
68. **X. Zhang, K. K. Parhi,.** High-speed VLSI architectures for the AES algorithm. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2004.
69. **A. Hodjat, I. Verbauwhede.** Area-Throughput Trade-offs for Fully Pipelined 30 to 70Gbits/s AES Processors. IEEE Transactions on Computers Volume 55, Issue 4. 2006.
70. **S. Morioka, A. Satoh.** An Optimized S-Box Circuit Architecture for Low Power AES Design. CHES (2002). 2002.
71. **A. Satoh, S. Morioka, K. Takano, S. Munetoh.** A Compact Rijndael Hardware Architecture with S-Box Optimization. ASIACRYPT (2001). 2001.
72. **J. Wolkerstorfer, E. Oswald, M. Lamberger.** An ASIC implementation of the AES SBoxes. In Topics in Cryptology CT-RSA , vol. 2271 of Lecture Notes in Computer Science, Springer Verlag. 2002.
73. **P. Chodowiec, K. Gaj.** Very compact FPGA implementation of the AES algorithm. in Cryptographic Hardware and Embedded Systems - CHES 2003, vol. 2779 of Lecture Notes in Computer Science, pp. 319–333. Springer Verlag. 2003.
74. **G. Bertoni, M. Macchetti, L. Negri, P. Fragneto.** Power-efficient ASIC Synthesis of Cryptographic Sboxes. in Proceedings of the 14th ACM Great Lakes Symposium on VLSI (GLSVLSI 2004), pp. 277–281. ACM Press. 2004.

75. **Canright, D.** A very compact S-Box for AES. in Cryptographic Hardware and Embedded Systems CHES 2005, vol. 3659 of Lecture Notes in Computer Science, pp. 441–455. Springer Verlag. 2005.
76. **S. Tillich, M. Feldhofer, J. Großschädl.** Area, Delay, and Power Characteristics of Standard-Cell Implementations of the AES S-Box. Embedded Computer Systems: Architectures, Modeling, and Simulation — SAMOS 2006, vol.4017 of Lecture Notes in Computer Science, pp. 457–466. Springer Verlag. 2006.
77. <http://www.model.com/>. Modelsim.
78. **N. Sklavos, O. Koufopavlou.** Architectures and VLSI Implementations of the AES-Proposal Rijndael. IEEE Transactions on Computers, Vol. 51, Issue 12, pp. 1454-1459. 2002.
79. **S. Morioka, A. Satoh.** 10-Gbps full-AES crypto design with a twisted BDD S-Box architecture. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. Vol.12, No. 7. 2004.
80. **Stefan Tillich, Martin Feldhofer, and Johann Großschädl.** Area, Delay, and Power Characteristics of Standard-Cell Implementations of the AES S-Box. SAMOS 2006, vol. 4017 of Lecture Notes in Computer Science, pp. 457–466. Springer Verlag. 2006.
81. **I. Verbauwhede, P. Schaumont, H. Kuo.** Design and Performance Testing of a 2.29 Gb/s Rijndael processor. IEEE Journal of Solid-State Circuits, pp. 569-572. 2003.
82. **Alireza Hodjat, Patrick Schaumont, Ingrid Verbauwhede.** Architectural Design Features of a Programmable High Throughput AES Coprocessor. Proceedings of the International Conference on Information Technology Coding and Computing (ITCC'04). 2004.
83. **Shin-Yi Lin, Chih-Tsun Huang.** A High-Throughput Low-Power AES Cipher for Network Applications. Design Automation Conference, ASP-DAC. 2007.
84. **Martin Feldhofer, Johannes Wolkerstorfer, Vincent Rijmen.** AES Implementation on a Grain of Sand. IEE Proceedings on Information Security, Volume 152, Issue 1, pp. 13-20. 2005.
85. **T. Good, M. Benaissa.** Very Small FPGA Application-Specific Instruction Processor for AES. IEEE Transactions on Circuit and Systems-I: Regular Papers, Vol. 53, No. 7. 2006.
86. **Kris Tiri, Ingrid Verbauwhede.** A Digital Design Flow for Secure Integrated Circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol. 25, no. 7, pp. 1197-1208. 2006.
87. **J. Fenlason, R. Stallman.** The gnu profiler . <http://www.gnu.org/software/binutils/manual/gprof-2.9.1/>. 1998.
88. **Chih-Pin Su, Tsung-Fu Lin, Chih-Tsiun Huang, Cheng-Wen Wu.** A high-throughput low-cost AES processor, Communications Magazine, IEEE, vol. 41, no. 12, pp.86-91. 2003.
89. **Krishnamachari, Bhaskar.** Networking Wireless Sensors. s.l. : Cambridge University Press, 2006.
90. **Bertsekas, Dimitri P.** Network Optimization: Continuous and Discrete Models (Optimization, Computation, and Control). s.l. : Athena Scientific, 1998.
91. **D. Harkelson, A. Menezes and, S. Vanstone.** Guide to Elliptic Curve Cryptography. s.l. : Springer Verlag New York, 2004.
92. **C. K. Koc, B. Sunar.** Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields. IEEE Trans. Comput. 47 (3). 1998.

93. **R. Lidl, H. Niederreiter.** Introduction to Finite Fields and their Applications. Cambridge University Press. 1994.
94. **Avanzi, R.** Side Channel Attacks on Implementations of Curve-Based Cryptographic Primitives. Cryptology ePrint Archive, report 2005/017. 2005.
95. **A. F. Tenca, C . K. Koc.** A scalable architecture for Montgomery multiplication. Proceedings of Cryptographic Hardware and Embedded Systems (CHES 1999), LNCS 1717, pages 94-108. Springer-Verlag . 1999.
96. **P. Noo-Intara, S. Chantarawong, S. Choomchuay.** Architectures for MixColumn Transform for the AES. proc. of ICEP2004. 2004.
97. **Wolkerstorfer, J.** An ASIC implementation of the AES MixColumn operation. in Proc. Austrochip 2001, Vienna, Austria, Oct. 12, 2001, pp. 129-132. 2001.

Περιοδικά

1. G. Selimis, A. Kakarountas, A. Fournaris, A. Milidonis and O. Koufopavlou, " **A Low Power Design for SBOX Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users**", in Vol. 3 N°3 of JOLPE - ASP Journal of Low Power Electronics, 2007.
2. G. Selimis, A. Fournaris, G. Kostopoulos, O. Koufopavlou, "**Hardware and Software Issues in Smart Card Technology**", accepted for publication in IEEE Communications Tutorial and Surveys.
3. G. Selimis, A. Fournaris, H. Michael, O. Koufopavlou, "**Improved Throughput Bit-Serial Multiplier for GF (2^m) fields**", accepted for publication in Elsevier VLSI Integration Journal.

Συνέδρια

1. P.Kitsos, G.Selimis, A. Skodras, O. Koufopavlou, "**A Hardware Implementation of CURUPIRA Block Cipher for Wireless Sensors**", 11th Euromicro Conference on Digital System Design, DSD 2008.
2. H. E. Michail, A. P. Kakarountas, G. Selimis and C. E. Goutis, " **Throughput Optimization of the Cipher Message Authentication Code**", 15th International Conference on Digital Signal Processing, Cardiff, Wales, UK, July 2007
3. G. Selimis, P. Fournaris, and O. Koufopavlou, " **Applying Low Power Techniques in AES MixColumn/InvMixColumn Transformations**", proceedings of 13th IEEE International Conference on Electronics, Circuits and Systems (ICECS'06), Nice, France, December 10-13, 2006.
4. O. Koufopavlou, G. Selimis, N. Sklavos, and P. Kitsos, "**Cryptography: Circuits and Systems Approach**", 5th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT05), Greece, December 18-21, 2005.
5. George N. Selimis, N. Lazarou, H. E. Michail, and O. Koufopavlou, "**VLSI Design and implementation of reconfigurable cryptographic systems for symmetric encryption**", proceedings of 12th IEEE International Conference on Electronics, Circuits and Systems (ICECS'05), Gammarth, Tunisia, December 11-14, 2005.
6. Odysseas G. Koufopavlou, George N. Selimis, Nicolas Sklavos, Paris Kitsos: "**Cryptography: Circuits and Systems Approach**", tutorial in PATMOS 2005, Leuven, Belgium.
7. H.E.Michail, A.P.Kakarountas, G.N.Selimis, C.E.Goutis, "**Optimizing SHA-1 Hash Function for High Throughput with a Partial Unrolling Study**", in The international workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), September 20-23, 2005 Leuven, Belgium.
8. P.Kitsos, O. Koufopavlou, G. Selimis and N. Sklavos, "**Low Power Cryptography**", Institute of Physics publishing, Journal of Physics: Conference Series (10) 2005.
9. N. Sklavos, G. Selimis and O. Koufopavlou, "**FPGA Implementation Cost and Performance Evaluation of IEEE 802.11 Protocol Encryption Schemes**", Institute of Physics publishing, Journal of Physics: Conference Series (10) 2005.
10. G. Selimis and O. Koufopavlou, "**Multi -Operation Cryptographic Engine: VLSI Design and Implementation**", Institute of Physics publishing, Journal of Physics: Conference Series (10) 2005.
11. P. Kitsos, O. Koufopavlou, G. Selimis, and N. Sklavos, "**Low Power Cryptography**", tutorial in 4th Marlow Workshop, September 14th 2004, Santorini, Greece.
12. G. Selimis, P. Kitsos and O. Koufopavlou, "**High Performance Cryptographic Engine PANAMA: Hardware Implementation**" in 11th IEEE International Conference on Electronics, Circuits and Systems, (ICECS 2004), December 13-15, Tel Aviv.

13. N. Sklavos, G. Selimis and O. Koufopavlou, **"Bulk Encryption Crypto-Processor for Smart Cards: Design and Implementation"** , in 11th IEEE International Conference on Electronics, Circuits and Systems, (ICECS 2004), December 13-15, Tel-Aviv, Israel.
14. G. Selimis, N. Sklavos, and O. Koufopavlou, **"Crypto Processor for Contactless Smart Cards"** proceedings of 12 IEEE Mediterranean Electrotechnical Conference - MELECON 2004 May 12-15, Dubrovnik, Croatia, 2004.
15. G. Selimis, N. Sklavos, and O. Koufopavlou, **"Area-Optimized Architecture and VLSI Implementation of a Multi-Coder Processor for the WTLS"**, proceedings of 46th IEEE Midwest Symposium on Circuits & Systems '03, December 27-30, Cairo, Egypt, 2003.
16. G. Selimis, N. Sklavos, and O. Koufopavlou **"VLSI Implementation of the Keyed-Hash Message Authentication Code for the Wireless Application Protocol"** proceedings of 10th IEEE International Conference on Electronics, Circuits and Systems (ICECS'03), United Arab Emirates, December 14-17, 2003.