Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ασφάλεια "Lightweight" Κρυπτογραφικών Αλγορίθμων

Νικόλαος Λαζαρίδης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ασφάλεια "Lightweight" Κρυπτογραφικών Αλγορίθμων

Νικόλαος Λαζαρίδης

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2020

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η ανάγκη, της σύγχρονης εποχής για χρήση ηλεκτρονικών συσκευών με μικρή επεξεργαστική ισχύ, χαμηλή ενεργειακή αυτονομία και μικρής επιφάνειας, λόγου χάριν σε δίκτυα αισθητήρων σε εφαρμογές του Διαδικτύου των Πραγμάτων, έχει οδηγήσει στην ανάγκη ανάπτυξης νέων αλγόριθμων κρυπτογραφίας, αφού τα υπάρχοντα πρότυπα κρυπτογράφησης δεν μπορούν να υλοποιηθούν αποτελεσματικά σε περιβάλλοντα με τέτοιους περιορισμούς. Οι νέοι αυτοί αλγόριθμοι χαρακτηρίζονται με τον όρο lightweight κρυπτογραφικοί αλγόριθμοι, με κύρια σχεδιαστική πρόκληση αυτών να μπορούν να υλοποιηθούν αποδοτικά σε συστήματα με τους ανωτέρω περιορισμούς, χωρίς όμως την υποβάθμιση της ασφάλειας. Για τους λόγους αυτούς, ο οργανισμός NIST έχει εκκινήσει διαγωνισμό για την επιλογή πρότυπων lightweight αλγορίθμων.

Η μεταπτυχιακή διατριβή πραγματεύεται την ασφάλεια των lightweight αλγορίθμων, επικεντρώνοντας κατ' αρχάς στους 32 υποψήφιους προς προτυποποίηση αλγορίθμους του εν εξελίξει διαγωνισμού του NIST. Η μεθοδολογική προσέγγιση έγκειται στη διερεύνηση των κρυπτογραφικών ιδιοτήτων των υποκείμενων λογικών συναρτήσεων που οι αλγόριθμοι αυτοί χρησιμοποιούν: στο πλαίσιο αυτό μελετώνται γνωστά κρυπτογραφικά κριτήρια συναρτήσεων, όπως ο αλγεβρικός βαθμός, η μη γραμμικότητα και η ανθεκτικότητα σε αλγεβρικές επιθέσεις, καθώς επίσης το βαθμό στον οποίο η συνάρτηση μπορεί να προσεγγιστεί ικανοποιητικά από άλλη συνάρτηση με μικρότερο πλήθος μεταβλητών αξιοποιώντας μία πρόσφατη τεχνική που έχει προταθεί.

Η παρούσα διατριβή εστίασε στον αλγόριθμο Skinny του προαναφερθέντος διαγωνισμού του NIST, ο οποίος χρησιμοποιεί στη λειτουργία του ένα S-Box κατά τη λογική του καθολικού πρότυπου κρυπτογράφησης AES (Advanced Encryption Standard). Τα αποτελέσματα της έρευνας καταδεικνύουν ότι σημαντικός αριθμός συναρτήσεων του εν λόγω S-box δεν έχουν καλές κρυπτογραφικές ιδιότητες, αναδεικνύοντας αφενός το γνωστό πρόβλημα κατασκευής λογικών συναρτήσεων οι οποίες να πληρούν το σύνολο των κρυπτογραφικών ιδιοτήτων και, αφετέρου την ανάγκη περαιτέρω διερεύνησης της ασφάλειας των lightweight (και όχι μόνο) αλγορίθμων και ως προς αυτήν την κατεύθυνση.

Summary

In the modern society the need to usage electronic devices with small demand of processing power, low energy consumption and small area of usage (for example network of sensors in applications in Internet of Things) necessitate the development of new cryptographic ciphers, since existing cryptographic standards cannot be used efficiency in such environments. These new ciphers are being called lightweight, because they can be used in restricted environments like those mentioned above, without degrading the security of the cipher. Due to the above, the organization NIST has initiated a competition for the choice of a standard for the lightweight cryptographic ciphers.

In this thesis the security of the lightweight ciphers is studied, focusing on specifically the 32 candidates for standardization ciphers in the ongoing contest of NIST. Our methodological approach is based on the investigation of the cryptographic properties of Boolean functions that are being used by the cryptographic ciphers: in this framework, specific known cryptographic properties such as algebraic degree, nonlinearity and algebraic immunity are being investigated, in conjunction with –based on a recent research result - the criterion that is related with the extent to which the function can be approximated satisfactorily from another function with fewer variables .

As a case study, the cipher Skinny has been chosen for our analysis, being a candidate in the ongoing NIST competition, which uses a S-Box with the same logic of the standard cryptographic cipher AES (Advanced Encryption Standard). The results of our research show that a significant number of functions of this S-Box does not have good cryptographic properties, thus further illustrating the known problem in construction of Boolean functions simultaneously satisfying all the main cryptographic properties, whereas it becomes evident that there is strong need for further research of the security that lightweight (and not only) ciphers, taking into account .

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1
Εισαγωγή

Στην σύγχρονη εποχή η τεχνολογική ανάπτυξη έχει προοδεύσει δραματικά. Η επιστημονική κοινότητα στην προσπάθειά της να εξελίξει τον τρόπο διαβίωσης των ανθρώπων κατάφερε να δημιουργήσει μία νέα τεχνολογία, η οποία προσπαθεί να εξυπηρετήσει τον άνθρωπο με τον καλύτερο δυνατό τρόπο. Αυτή η τεχνολογία βρίσκεται ακόμα υπό εξέλιξη, καθώς σε κάθε νέα τεχνολογία εγείρονται διάφορα τεχνικά και ηθικά διλλήματα. Η τεχνολογία αυτή ονομάστηκε Διαδίκτυο των Πραγμάτων (Internet of Things) και αποτελείται από διάφορα αντικείμενα και συσκευές τα οποία μετρούν παραμέτρους και με την βοήθεια του διαδικτύου αποστέλλουν τις πληροφορίες αυτές στην κεντρική πλατφόρμα, η οποία περιέχει ειδικές εφαρμογές που επιτρέπουν την παρακολούθηση των πληροφοριών αυτών και τον κατάλληλο έλεγχο εκ νέου των συσκευών προκειμένου να γίνει πιθανή διόρθωση των παραμέτρων αυτών.

1.1 Ασφάλεια Επικοινωνιών και Πληροφοριών

Στην σύγχρονη εποχή όλο και περισσότερα δεδομένα αποθηκεύονται στο διαδίκτυο μέσω των ιστοσελίδων κοινωνικής δικτύωσης, αλλά και λόγω της χρήσης διαδικτυακών εφαρμογών επικοινωνίας. Για αυτό το λόγο αυξήθηκαν και οι περιπτώσεις κατά τις οποίες υποκλάπηκαν (προσωπικά ή μη) δεδομένα από τρίτους. Η αυξανόμενη χρήση του διαδικτύου οδήγησε στην ανάγκη εύρεσης ασφαλών μεθόδων ανταλλαγής πληροφοριών μέσω διαδικτύου. Η επιστημονική κοινότητα υποστήριξε ότι η διαδρομή που ακολουθεί η πληροφορία πρέπει να θεωρείται μη ασφαλής και με σχετική ευκολία ένας τρίτος μπορεί να αντλήσει τις πληροφορίες της διαδρομής.

Η ευρωπαϊκή Ένωση υπό το πρίσμα της προστασίας των προσωπικών δεδομένων εξέδωσε μία πιο αυστηρή νομοθεσία για την επεξεργασία των δεδομένων από τεχνολογικές επιχειρήσεις και διαδικτυακούς τόπους, η οποία ονομάστηκε General Data Protection Regulation (GPDR) (European Union, 2018). Αντιστοίχως έχει εκδώσει και μία

Οδηγία για την ασφάλεια κρίσιμων υποδομών (Οδηγία EU 2016/1148 – Network and Information Security Directive). Παραδοσιακά, για την ενίσχυση της ασφάλειας των προσωπικών δεδομένων που ανταλλάσσονται μέσω διαδικτύου χρησιμοποιήθηκε η επιστήμη της Κρυπτογραφίας. Η κρυπτογραφία, στον πιο απλό της ορισμό, είναι η επιστήμη με την οποία ένα μήνυμα μετατρέπεται με την χρήση ενός γνωστού αλγορίθμου και ενός, τουλάχιστον, μυστικού κλειδιού σε ένα νέο κρυπτογραφημένο μήνυμα, το οποίο δεν μπορεί να αναγνωστεί από καμία άλλη οντότητα εκτός του νόμιμου παραλήπτη της, ο οποίος γνωρίζει και το μυστικό κλειδί.

Η απαίτηση της ασφάλειας της πληροφορίας γίνεται όλο και πιο απαιτητή, λόγω της αυξανόμενης παγκοσμίως χρήσης του διαδικτύου. Η ανάπτυξη νέων δομών Διαδικτύου των Πραγμάτων απαιτεί αυξημένη ασφάλεια, διότι οι δομές αυτές διαχειρίζονται προσωπικά δεδομένα του ατόμου. Η χρήση διαφόρων αισθητήρων και συσκευών στην παραπάνω δομή δημιουργεί νέες ανάγκες όσον αφορά τους ήδη υπάρχοντες κρυπτογραφικούς αλγορίθμους, επειδή διαφέρουν στις ελάχιστες απαιτήσεις που έχουν αυτοί οι αλγόριθμοι για την σωστή λειτουργία τους. Τα ήδη γνωστά και καθιερωμένα πρότυπα κρυπτογράφησης δεν είναι κατάλληλα για τις νέες αυτές προκλήσεις. Για παράδειγμα, δεν μπορούν να υλοποιηθούν σε μία συσκευή αισθητήρα με πολύ περιορισμένη υπολογιστική ισχύ, πολύ μικρή επιφάνεια και πολύ μικρή μνήμη. Αποτέλεσμα των διαφορετικών αναγκών οδήγησε στην δημιουργία ενός νέου, σχετικά, τύπου κρυπτογραφικών αλγορίθμων που ονομάστηκαν lightweight κρυπτογραφικοί αλγόριθμοι.

1.2 Τεχνικά ζητήματα του Διαδικτύου των Πραγμάτων

Όπως κάθε νέα τεχνολογία έτσι και στο IoT έχουν προκύψει αρκετά τεχνικά ζητήματα που πρέπει να αντιμετωπιστούν προκειμένου η τεχνολογία να γίνει πιο ασφαλής και έτοιμη για ευρέα χρήση. Η τεχνολογία αυτή υποφέρει από τις επιθέσεις που μπορεί να εκτελέσει ένας τρίτος ως προς τους server, workstation αλλά και κινητά τηλέφωνα με την ιδιομορφία ότι οι συσκευές που χρησιμοποιούνται έχουν μικρό μέγεθος σε RAM και ROM, μικρή αυτονομία (ή και καθόλου αυτονομία όντας παθητικές συσκευές) και χαμηλές ταχύτητες επεξεργασίας λόγω του μεγέθους τους.

Το αποτέλεσμα των κατασκευαστικών περιορισμών των συσκευών αυτών οδήγησε τον οργανισμό NIST (National Institute of Standards and Technology), ο οποίος θεσπίζει διεθνώς αναγνωρισμένα πρότυπα κρυπτογράφησης, να εκκινήσει διαγωνισμό προκειμένου να καθοριστεί νέο πρότυπο lightweight κρυπτογραφικών αλγορίθμων που επιτυγχάνουν εμπιστευτικότητα, πιστοποίηση ταυτότητας του αποστολέα και διασφάλιση του αδιάβλητου της πληροφορίας. Τα τρία παραπάνω χαρακτηριστικά αποτελούν την αναγκαία συνθήκη για την ασφάλεια της πληροφορίας.

Στην συγκεκριμένη διατριβή θα μελετήσουμε τους lightweight κρυπτογραφικούς αλγορίθμους, ακριβώς λόγω της σπουδαιότητάς τους και του έντονου ενδιαφέροντος της επιστημονικής κοινότητας σε αυτούς. Έμφαση θα δοθεί στους αλγορίθμους οι οποίοι αυτή τη στιγμή εξετάζονται από τον NIST ως υποψήφιοι προς προτυποποίηση. Στο πλαίσιο αυτό, θα γίνει μία περιγραφή και ταξινόμηση των υποψήφιων κρυπτογραφικών αλγορίθμων, που έχουν περάσει επιτυχώς στον δεύτερο γύρο του διαγωνισμού του NIST ο οποίος είναι σε εξέλιξη. Παρακάτω, θα επικεντρωθούμε στη μελέτη της ασφάλειάς τους, βάσει συγκεκριμένης μεθοδολογίας η οποία περιγράφεται στη συνέχεια.

1.3 Ερευνητικά Ερωτήματα

Η παρούσα διατριβή εστιάζει στην ασφάλεια των lightweight κρυπτογραφικών αλγορίθμων. Ειδικότερα, θα εστιάσει στον τρέχοντα διαγωνισμό του NIST για καθορισμό των νέων προτύπων κρυπτογράφησης σε αυτήν την κατηγορία. Αρχικά, θα γίνει μία κατηγοριοποίηση όλων αυτών των αλγορίθμων, βάσει συγκεκριμένων κριτηρίων ταξινόμησης (π.χ. αν πρόκειται για αλγόριθμος τμήματος ή για αλγόριθμο ροής). Περαιτέρω, ως προς την αποτίμηση της ασφάλειάς τους, η προσέγγιση που ακολουθείται στο πλαίσιο της διατριβής είναι η εξής: θα αναζητηθούν αλγόριθμοι στους οποίους ενυπάρχει, στη λειτουργία τους, κάποια δομή S-box (Substitution Box – Μονάδα Αντικατάστασης), προκειμένου να διερευνηθούν τα κρυπτογραφικά κριτήρια που οι υποκείμενες λογικές συναρτήσεις αυτού πληρούν. Ο λόγος που ακολουθείται αυτή η προσέγγιση έγκειται στο ότι, αν και είναι γνωστό ότι η μη εκπλήρωση κάποιων κρυπτογραφικών κριτηρίων ενός S-box ή των υποκείμενων αυτού λογικών συναρτήσεων μπορεί να αποτελεί σημείο ευπάθειας για τον αλγόριθμο, εν τούτοις στον εν εξελίξει διαγωνισμό του NIST – όπου όλοι οι αλγόριθμοι υποβάλλονται ήδη σε μελέτη από την ερευνητική κοινότητα – δεν έχουν ακόμα μελετηθεί, βάσει της βιβλιογραφίας, τα κρυπτογραφικά κριτήρια αυτών. Εξάλλου, στο πλαίσιο αυτό, θα μελετηθεί και ένα

κρυπτογραφικό κριτήριο, για το οποίο μία μεθοδολογία αποδοτικού υπολογισμού του προτάθηκε πολύ πρόσφατα και ως εκ τούτου δεν έχει τύχει ακόμα ευρείας χρήσης.

Ειδικότερα, τα κρυπτογραφικά κριτήρια που θα μελετηθούν είναι τα εξής:

i) Η «ισορροπία» (balancedness) ως προς τις τιμές '0' και '1' στην έξοδο του πίνακα αληθείας των υποκείμενων λογικών συναρτήσεων
ii) Ο αλγεβρικός βαθμός (algebraic degree) των υποκείμενων λογικών συναρτήσεων
iii) Η μη γραμμικότητα (nonlinearity) των υποκείμενων λογικών συναρτήσεων
iv) Η αλγεβρική ανθεκτικότητα (algebraic immunity) των υποκείμενων λογικών συναρτήσεων.

Θα μελετηθεί επίσης, αξιοποιώντας μία πρόσφατα αναπτυχθείσα τεχνική, ο βαθμός στον οποίο μία υποκείμενη λογική συνάρτηση μπορεί να προσεγγιστεί ικανοποιητικά από μία άλλη λογική συνάρτηση η οποία έχει μικρότερο πλήθος μεταβλητών. Τα εν λόγω κριτήρια θα αξιολογηθούν, βάσει γνωστών αποτελεσμάτων των βέλτιστων τιμών που – ιδανικά – θα έπρεπε να έχουν, προκειμένου να εξαχθεί συμπέρασμα ως προς το αν υπάρχει ευπαθές σημείο στον αλγόριθμο ή όχι.

Όπως κατέδειξε η μελέτη όλων των υπό εξέταση κρυπτογραφικών αλγορίθμων, ο αλγόριθμος εκείνος ο οποίος χρησιμοποιεί S-box στη λειτουργία του είναι ο Skinny, κατά συνέπεια, τα ανωτέρω ερευνητικά ερωτήματα επικεντρώθηκαν σε αυτόν. Χρήσιμα συμπεράσματα αναφύονται για αυτήν την περίπτωση, όπως παρουσιάζονται στην παρούσα διατριβή, δεδομένου ότι ο Skinny χρησιμοποιεί ένα S-box διαστάσεων 8 x 8 και συνεπώς μελετήθηκαν αναλυτικά 2^8=256 λογικές συναρτήσεις.

1.4 Μεθοδολογία της έρευνας

Για τον υπολογισμό των τιμών των ως άνω κρυπτογραφικών κριτηρίων, θα αξιοποιηθούνται κατάλληλα εργαλεία λογισμικού, ενώ επίσης αναπτύχθηκαν, στο πλαίσιο της διατριβής, κατάλληλοι υπο-βοηθητικοί αλγόριθμοι. Ειδικότερα, για τον υπολογισμό των τιμών της «ισορροπίας», του αλγεβρικού βαθμού, της μη γραμμικότητας και της αλγεβρικής ανθεκτικότητας, αξιοποιήθηκε το ελεύθερα διαθέσιμο εργαλείο λογισμικού Sage. Για την αρχική εξαγωγή του πίνακα αληθείας της εκάστοτε λογικής

συνάρτησης, αλλά και για τον προσδιορισμό του κατά πόσον η λογική συνάρτηση μπορεί να προσεγγιστεί από άλλη συνάρτηση με μικρότερο πλήθος μεταβλητών, χρησιμοποιήθηκαν ειδικά προς αυτόν το σκοπό προγράμματα λογισμικού.

1.5 Δομή Διατριβής

Η δομή της διατριβής είναι η εξής.

Αρχικά, στο Δεύτερο Κεφάλαιο της διατριβής παρατίθεται μία περιγραφή των λεγόμενων συμμετρικών κρυπτογραφικών αλγορίθμων, που χρησιμοποιούνται για την ασφάλεια επικοινωνιών. Οι κρυπτογραφικοί αλγόριθμοι αυτής της οικογένειας χωρίζονται σε δύο βασικές κατηγορίες, οι οποίες είναι αλγόριθμοι ροής (stream ciphers) και αλγόριθμοι δέσμης (block ciphers). Στις σύγχρονες εφαρμογές, και ειδικά στις εφαρμογές που απαιτούν lightweight αλγορίθμους παρατηρείται η χρήση και των δύο παραπάνω κατηγοριών αλγορίθμων.

Στο Τρίτο Κεφάλαιο της διατριβής αυτής, θα περιγραφεί το Διαδίκτυο των πραγμάτων (IoT), τεκμηριώνοντας τους λόγους που αυτό δημιουργεί νέες ανάγκες στους κρυπτογραφικούς αλγορίθμους, λόγω των συσκευών που το απαρτίζουν. Όπως θα αναλυθεί, οι συσκευές που απαρτίζουν το IoT είναι κατά κύριο λόγο μικρές σε μέγεθος (αισθητήρες, RFID), με αποτέλεσμα να έχουν μειωμένη επεξεργαστική ισχύ, χαμηλή αυτονομία και περιορισμό στην ενέργεια που διατίθεται για την λειτουργία του.

Λόγω του ότι πολλοί συμμετρικοί κρυπτογραφικοί αλγόριθμοι βασίζονται σε λογικές συναρτήσεις, για τις οποίες είναι γνωστό ότι πρέπει να πληρούν συγκεκριμένες κρυπτογραφικές ιδιότητες προκειμένου να διασφαλίζεται η ανθεκτικότητα έναντι συγκεκριμένου τύπου επιθέσεων, στο Τέταρτο Κεφάλαιο γίνεται μία γενική περιγραφή της έννοιας των λογικών συναρτήσεων και των συναφών κρυπτογραφικών ιδιοτήτων (όπως, για παράδειγμα, η μη γραμμικότητα). Ταυτόχρονα, γίνεται και μία περιγραφή των κρυπτογραφικών ιδιοτήτων ακολουθιών οι οποίες χρησιμοποιούνται σε κρυπτογραφικούς αλγορίθμους – με κύρια τη λεγόμενη γραμμική πολυπλοκότητα. Ο λόγος που μελετάται η γραμμική πολυπλοκότητα των ακολουθιών είναι ότι, βασιζόμενοι σε αλγορίθμους υπολογισμού γραμμικής πολυπλοκότητας, μπορούμε να εξάγουμε επίσης χρήσιμες πληροφορίες για λογικές συναρτήσεις, όπως περιγράφεται στο εν λόγω κεφάλαιο (στηριζόμενοι σε πρόσφατα ερευνητικά αποτελέσματα).

Στο πέμπτο Κεφάλαιο γίνεται μία περιγραφή των υποψηφίων του διαγωνισμού που εκτελεί ο οργανισμός NIST για την εύρεση ενός lightweight κρυπτογραφικού αλγορίθμου, που θα μπορεί να χρησιμοποιηθεί ως πρότυπο κρυπτογράφησης για εφαρμογές Διαδικτύου των Πραγμάτων. Θα παρατεθεί μία ταξινόμηση όλων των αλγορίθμων και, ακολούθως, θα επιλεχθεί ένας από τους διαγωνιζόμενους αλγορίθμους προκειμένου να μελετηθούν οι κρυπτογραφικές ιδιότητες των υποκείμενων λογικών συναρτήσεων. Ο αλγόριθμος που επιλέγεται είναι ο Skinny, ο οποίος βασίζει τη λειτουργία του στη χρήση ενός S-Box διαστάσεων 8 x 8, όπως ακριβώς και στην περίπτωση του σημερινού πρότυπου κρυπτογραφικού αλγορίθμου AES (Advanced Encryption Standard). Στο πλαίσιο αυτό θα περιγραφεί η μεθοδολογία που ακολουθήθηκε και θα αναλυθούν οι Boolean συναρτήσεις, αλλά και όλοι οι πιθανοί συνδυασμοί τους, αυτού του S-box για την μελέτη των κρυπτογραφικών ιδιοτήτων του.

Τέλος, τα συμπεράσματα της έρευνας, αλλά και πιθανές μελλοντικές ερευνητικές κατευθύνσεις, αποτελούν περιεχόμενα του Έκτου κεφαλαίου.

Κεφάλαιο 2
Κρυπτογραφικοί αλγόριθμοι

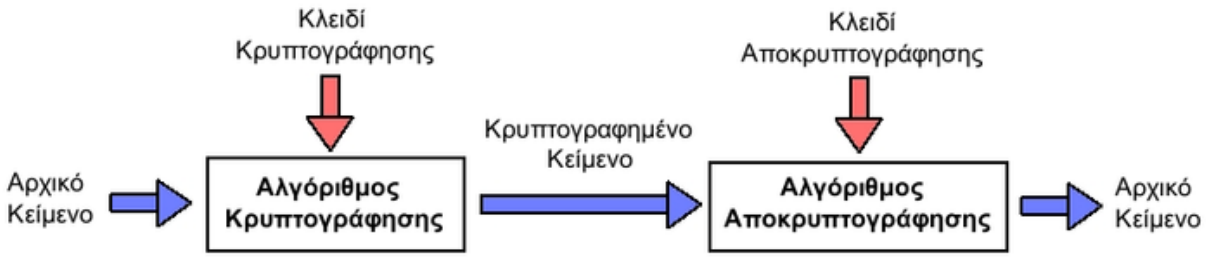
Η κρυπτογραφία είναι η επιστήμη η οποία χρησιμοποιεί διάφορες τεχνικές προκειμένου να μετατρέψει ένα μήνυμα προς αποστολή σε ένα μην κατανοητό μήνυμα από τρίτους. Βασικός στόχος της κρυπτογραφίας είναι η εμπιστευτικότητα ενός μηνύματος, ώστε ακόμα και αν υποκλαπεί από τρίτους να μην έχουν δυνατότητα ανάγνωσης αυτού. Ωστόσο, στο σύγχρονο κόσμο με τον όρο κρυπτογραφία αναφερόμαστε σε κάτι πολύ ευρύτερο: ουσιαστικά, αναφερόμαστε σε μαθηματικές τεχνικές με τις οποίες προσπαθούμε να διασφαλίσουμε τρία βασικά ζητήματα που αφορούν την ασφάλεια της πληροφορίας. Αυτά τα τρία ζητήματα είναι η εμπιστευτικότητα της πληροφορίας, η πιστοποίηση της ταυτότητας του αποστολέα και τέλος η εξασφάλιση της ακεραιότητας της πληροφορίας (M. Burmester, 2011).

2.1 Είδη Κρυπτογραφικών Αλγορίθμων

Οι κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δύο βασικά είδη. Ο ένας τύπος αποτελεί τα συμμετρικά κρυπτογραφικά συστήματα και ο άλλος τα ασύμμετρα κρυπτογραφικά συστήματα. Στην παρούσα μεταπτυχιακή διατριβή θα γίνει εκτενής αναφορά στους συμμετρικούς κρυπτογραφικούς αλγορίθμους.

2.1.1 Συμμετρικοί Κρυπτογραφικοί Αλγόριθμοι

Τα συμμετρικά κρυπτογραφικά συστήματα βασίζουν την ασφάλεια τους στην ύπαρξη ενός μυστικού κλειδιού, το οποίο γνωρίζουν ο πομπός και ο δέκτης του μηνύματος. Η ανταλλαγή του μυστικού κλειδιού πρέπει να εκτελεστεί σε ένα ασφαλές κανάλι επικοινωνίας ή με οποιοδήποτε άλλο τρόπο με τον οποίο αποδεικνύεται ότι δεν μπορεί οποιαδήποτε τρίτη οντότητα να αποκτήσει το μυστικό κλειδί. Η απαίτηση της ασφαλούς ανταλλαγής του μυστικού κλειδιού αποτελεί μία βασική πρόκληση της συμμετρικής κρυπτογραφίας (η οποία αντιμετωπίζεται με την ασύμμετρη κρυπτογραφία).



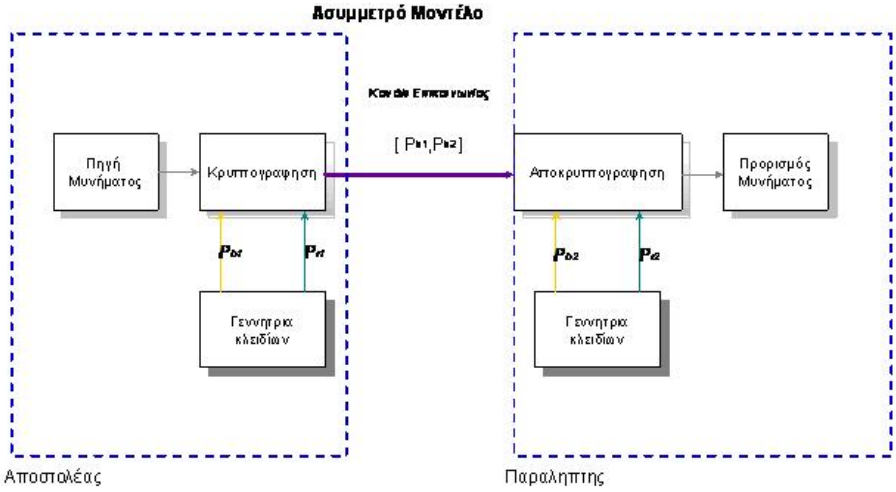
Εικόνα 1: Συμμετρικό κρυπτογραφικό σύστημα

Στο παραπάνω σχήμα περιγράφεται με απλοϊκό τρόπο η διαδικασία ενός συμμετρικού κρυπτογραφικού συστήματος. Αρχικά ο πομπός με την χρήση ενός συμμετρικού αλγορίθμου κρυπτογράφησης και ενός μυστικού κλειδιού δημιουργεί ένα κρυπτογραφημένο κείμενο. Το κρυπτογραφημένο κείμενο μεταφέρεται μέσα από ένα μη ασφαλές κανάλι επικοινωνίας στον δέκτη. Ο δέκτης χρησιμοποιεί το ίδιο μυστικό κλειδί με τον πομπό προκειμένου να αποκρυπτογραφήσει το μήνυμα και να ανακτήσει το αρχικό αναγνώσιμο μήνυμα.

Οι συμμετρικοί αλγόριθμοι χωρίζονται σε δύο επιμέρους κατηγορίες. Στους αλγόριθμους Ροής (Stream ciphers), οι οποίοι κρυπτογραφούν μία αλληλουχία μηνύματος, και στους αλγόριθμους Τμήματος (Block ciphers), οι οποίοι κρυπτογραφούν ανά τμήματα το μήνυμα. Αυτές οι κατηγορίες θα αναλυθούν εκτενώς στις επόμενες ενότητες του ίδιου Κεφαλαίου.

2.1.2 Ασύμμετροι Κρυπτογραφικοί Αλγόριθμοι

Τα ασύμμετρα κρυπτογραφικά συστήματα χρησιμοποιούνται για την κρυπτογράφηση μικρών μηνυμάτων με την χρήση δύο ειδών κλειδιών. Το ένα κλειδί λέγεται δημόσιο κλειδί και είναι γνωστό σε όλους τους χρήστες του καναλιού. Το δεύτερο κλειδί είναι το ιδιωτικό κλειδί το οποίο το γνωρίζει μόνο ένας χρήστης. Βασική σχέση μεταξύ των δύο κλειδιών είναι ότι η κρυπτογράφηση μπορεί να γίνει με οποιαδήποτε από τα δύο, αλλά η αποκρυπτογράφηση θα γίνει με την χρήση του μη χρησιμοποιηθέντος κλειδιού. Βασικές χρήσεις των ασύμμετρων κρυπτογραφικών συστημάτων γίνεται για την ανταλλαγή μυστικών κλειδιών συμμετρικού συστήματος και στην δημιουργία ψηφιακών υπογραφών, οπού αποδεικνύεται ο αυθεντικός αποστολέας του μηνύματος.



Εικόνα 2: Ασύμμετρο κρυπτογραφικό σύστημα

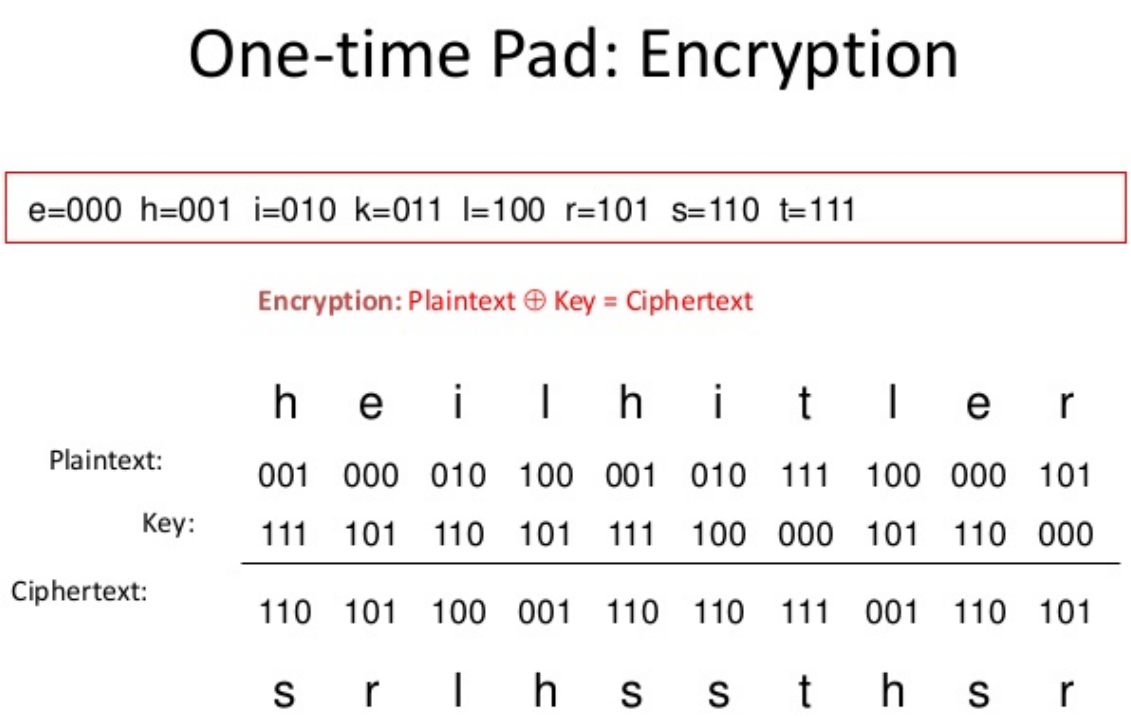
2.2 Κρυπτογραφικοί Αλγόριθμοι Ροής (Stream Ciphers)

Οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι ροής έχουν σχεδιαστεί ώστε να είναι με την χρήση της επιστήμης των Μαθηματικών υπολογιστικά (computationally) ασφαλείς και όχι απεριόριστα ασφαλείς (unconditionally). Αυτό συμβαίνει επειδή ένας απεριόριστα ασφαλής κρυπτογραφικός αλγόριθμος περιγράφεται ως εξής: ακόμα και εάν ένας τρίτος, ο οποίος προσπαθεί να «σπάσει» τον απόλυτα ασφαλή αλγόριθμο, διαθέτει άπειρους πόρους (σε υπολογιστική ισχύ και κατανάλωση ενέργειας) δεν θα το επιτύχει. Ο μόνος απόλυτα ασφαλής αλγόριθμος ροής, ο οποίος έδωσε και το έναυσμα στην επιστημονική κοινότητα να δημιουργήσει διάφορους αλγόριθμους ροής, είναι ο one-time pad (OTP) (C. Shannon, 1949).

2.2.1 Βασικές Αρχές

Αρχική υλοποίηση ενός αλγόριθμου ροής αποτελεί ο OTP. Ο OTP απαιτεί για την υλοποίηση του μία πραγματική μηχανή παραγωγής τυχαίων αριθμών (True Random Number Generator-TRNG) για την παραγωγή ενός κλειδιού κρυπτογράφηση ίσου ή μεγαλύτερου μεγέθους από το μέγεθος του μηνύματος. Το κλειδί αυτό θα πρέπει να μεταδοθεί ασφαλώς προς τον λήπτη προκειμένου να μπορεί να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα. Για την πραγματοποίηση του OTP επιβάλλεται η γεννήτρια να είναι πραγματικά τυχαία και όχι ψευδοτυχαία, επειδή στην περίπτωση της ψευδοτυχαίας γεννήτριας ο OTP παύει να είναι απεριόριστα ασφαλής αλγόριθμος. Μέχρι και τώρα δεν είναι τεχνολογικά επιτεύξιμο να τοποθετηθεί μία πραγματική τυχαία

γεννήτρια σε ευρέως χρησιμοποιούμενες ηλεκτρονικές συσκευές(όπως τα κινητά τηλέφωνα, οι ηλεκτρονικοί υπολογιστές κ.α.), δηλαδή από ντετερμινιστικά υπολογιστικά συστήματα. Ένα ακόμα πρόβλημα που δεν έχει επιλυθεί είναι η μετάδοση από ασφαλές κανάλι του κλειδιού, που θα χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος (το μέγεθος του κλειδιού είναι ίδιο ή μεγαλύτερο σε μέγεθος από το μήνυμα). Τα προβλήματα που προκύπτουν για την χρήση του OTP οδήγησε την επιστημονική κοινότητα στην έρευνα και στην δημιουργία αλγορίθμων ροής με την χρήση ψευδοτυχαίων γεννητριών, που θα χρησιμοποιήσουν ένα κλειδί ως συγχρονιστικό μέσο, για την επιτυχή υλοποίηση κρυπτογραφίας (C. Paar, 2010).



Εικόνα 3: One-Time Pad κρυπτογραφικός αλγόριθμος

Οι κρυπτογραφικοί αλγόριθμοι ροής είναι συμμετρικού κλειδιού αλγόριθμοι για την παροχή εμπιστευτικότητας ενός μηνύματος, οι οποίοι «προσπαθούν» να προσομοιάσουν τη λειτουργία του OTP. Με την εμπιστευτικότητα εννοείται ότι το μήνυμα μπορεί να το αναγνώσει μόνο το πρόσωπο που είναι ο πραγματικός λήπτης και κανένας άλλος. Ο αλγόριθμος παράγει με την χρήση ενός κλειδιού από τον αποστολέα ένα σύνολο από αριθμούς από το σύνολο GF (2) = {0,1} (δηλαδή από το πεπερασμένο σώμα 2 στοιχείων).

Κατά ουσία παράγεται η παραπάνω αριθμοσειρά (ακολουθία) από 0 και 1 χάρις στο κλειδί του αποστολέα και εκείνη συνδυάζεται κατάλληλα (πρόσθεση XOR) με την αριθμοσειρά από 0 και 1 του μηνύματος δημιουργώντας το κρυπτογραφημένο μήνυμα, το οποίο με την σειρά του θα διαδοθεί μέσα από κανάλια που δεν παρέχουν ασφάλεια. Ο λήπτης θα παραλάβει το κρυπτογραφημένο μήνυμα και με την χρήση του ίδιου κλειδιού θα αποκρυπτογραφήσει το μήνυμα. Το βασικό πλεονέκτημα των αλγόριθμων ροής είναι η ταχύτητά τους σε σχέση με τους αλγόριθμους τμήματος (block ciphers), καθώς και η μειωμένη πολυπλοκότητα σε υλικά κατασκευής. Ωστόσο, μέχρι τώρα δεν έχει επισήμως καθοριστεί πρότυπος αλγόριθμος κρυπτογράφησης ο οποίος να είναι αλγόριθμος ροής.

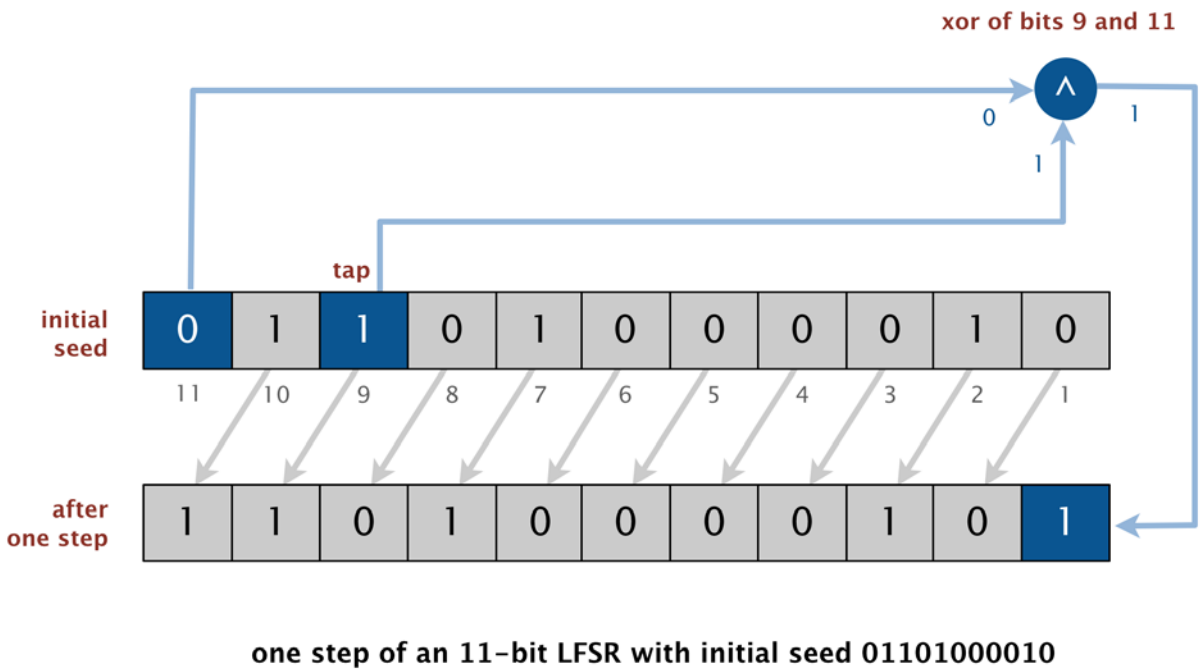
2.2.2 Γεννήτρια Παραγωγής Τυχαίων Αριθμών

Όπως αναφέρθηκε και παραπάνω η γεννήτρια παραγωγής τυχαίων αριθμών είναι υψίστης σημασίας στους αλγόριθμους ροής καθώς η ασφάλειά τους μπορεί να κριθεί από την γεννήτρια που χρησιμοποιήθηκε. Οι γεννήτριες παραγωγής τυχαίων αριθμών χωρίζονται σε δύο μεγάλες κατηγορίες: γεννήτριες πραγματικών τυχαίων αριθμών και γεννήτριες ψευδοτυχαίων αριθμών. Το επιθυμητό χαρακτηριστικό είναι η χρήση μιας γεννήτριας παραγωγής πραγματικά τυχαίων αριθμών καθώς τότε κάθε αλληλουχία θα ήταν πραγματικά μη προβλέψιμη δίνοντας έτσι στον αλγόριθμο χαρακτηριστικά απόλυτης ασφάλειας. Ωστόσο, όπως προαναφέρθηκε, υπάρχουν δυσκολίες στην παραγωγή πραγματικά τυχαίων ακολουθιών από ντετερμινιστική συσκευή. Περαιτέρω, ένα άλλο βασικό πρόβλημα στην παραγωγή μίας πραγματικά τυχαίας αριθμοσειράς είναι το ότι πρέπει ταυτόχρονα και δύο ενδιαφερόμενοι (αποστολέας και λήπτης) να παράγουν ακριβώς την ίδια, σε απόλυτο συγχρονισμό. Όσον αφορά τις γεννήτριες παραγωγής ψευδοτυχαίων αριθμών λειτουργούν με την αρχική τοποθέτηση μίας αρχικής τιμής. Η αρχική τιμή (η οποία, ουσιαστικά, έχει το ρόλο του μυστικού κλειδιού) χρησιμοποιείται ως το σημείο εκκίνησης της γεννήτριας και η γεννήτρια αρχίζει να παράγει τυχαίες αλληλουχίες αριθμών. Για να μπορεί μια τέτοια γεννήτρια να είναι αποδεκτή σε κρυπτογραφικούς αλγόριθμους θα πρέπει να συμμορφώνονται με καλά στατιστικές ιδιότητες με τις οποίες πλησιάζουν στις ιδιότητες μίας γεννήτριας παραγωγής πραγματικών τυχαίων αριθμών. Γεννήτριες που δεν πλησιάζουν στις στατιστικές ιδιότητες μιας γεννήτριας παραγωγής πραγματικά τυχαίων αριθμών δεν μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση κειμένου διότι το κρυπτογραφημένο κείμενο είναι ευπαθές σε απλές επιθέσεις ανάκτησης του μηνύματος, που βασίζονται σε δυνατότητα «πρόβλεψης» της άγνωστης ακολουθίας.

Στην κρυπτογραφία χρησιμοποιούνται οι γεννήτριες αυτές που παρουσιάζουν χαρακτηριστικά που δεν μπορούν να προβλεφθούν οι αλληλουχίες αριθμών που παράγουν. Το ότι δεν μπορούν να προβλεφθούν αυτά τα στοιχεία σημαίνει ότι για ένα τυχαίο αριθμό που αποτελεί μέρος της αλληλουχίας δεν είναι δυνατή η πρόβλεψη του προηγούμενου αλλά και του επόμενου στοιχείου με καλύτερη πιθανότητα από 50%. Για αυτό το λόγο αυτές οι γεννήτριες χρησιμοποιούνται στους αλγόριθμους ροής.

2.2.3 Καταχωρητές ολίσθησης με ανάδραση

Οι καταχωρητές ολίσθησης με ανάδραση είναι ένα βασικό στοιχείο στοιχείο προκειμένου να επιτευχθεί η δημιουργία μίας γεννήτριας με τα κατάλληλα τεχνικά χαρακτηριστικά, αφού συναντάται σε πολλές γεννήτριες. Οι καταχωρητές αυτοί χρησιμοποιούνται στην δημιουργία αλγορίθμων ροής καθώς προσφέρουν μεγάλες περιόδους, καλή απόδοση και καλές στατιστικές ιδιότητες.



Εικόνα 4: Καταχωρητής ολίσθησης με ανάδραση των 11 bits

Οι γραμμικοί καταχωρητές ολίσθησης με ανάδραση (Linear Feedback Shift Registers-LFSRs), που αποτελούν ειδική περίπτωση, έχουν μελετηθεί εκτενώς από την επιστημονική κοινότητα, επειδή προσφέρουν καλές στατιστικές ιδιότητες. Η κύρια ιδιότητά τους είναι ότι γνωρίζουμε με ποιον τρόπο μπορούμε να κατασκευάσουμε/επιλέξουμε κάποιον εξ αυτών ο οποίος να παράγει ακολουθία μέγιστης

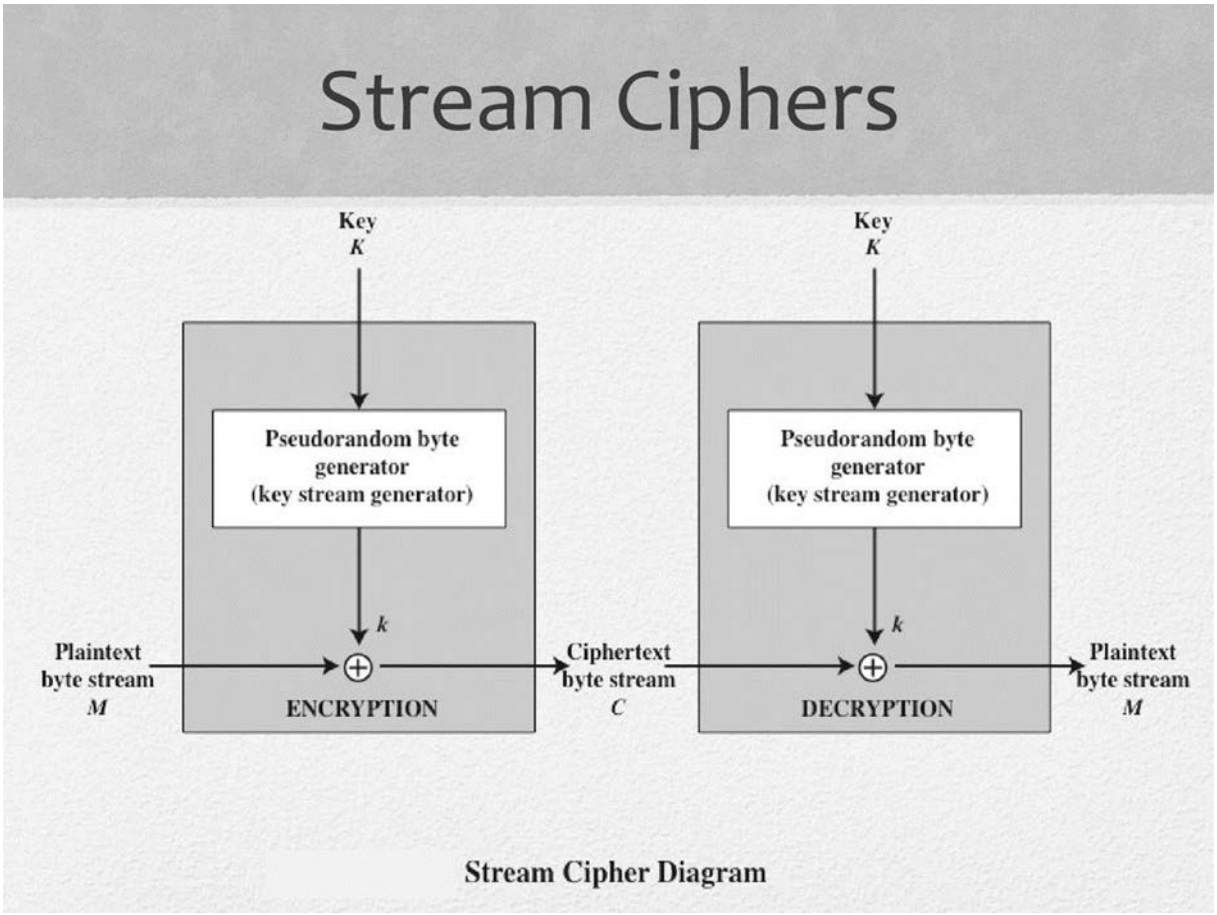
περιόδου 2^n-1 για οποιαδήποτε επιθυμητή τιμή του πλήθους n των βαθμίδων αυτού (S.W. Golomb, 1981). Παρόλο, όμως που εμφανίζουν πολύ καλές στατιστικές ιδιότητες οι LFSRs είναι κρυπτογραφικά αδύναμοι λόγω της γραμμικότητάς τους. Συγκεκριμένα, οι ακολουθίες που παράγονται από LFSRs έχουν, εξ ορισμού, χαμηλή γραμμική πολυπλοκότητα (linear complexity), η οποία ορίζεται, για δοθείσα ακολουθία, ως το μέγεθος του μικρότερου LFSR που μπορεί να την παράγει. Αν η γραμμική πολυπλοκότητα μιας ακολουθίας είναι c(s) τότε μόλις 2c(s) διαδοχικά bits από το κρυπτογραφημένο κείμενο είναι αρκετά ώστε να ανακαλύψει ένας υποκλοπέας τον LFSR που παράγει την κλειδοροή. Π.χ. στην περίπτωση ενός LFSR μεγέθους n ο οποίος παράγει ακολουθία με μέγιστη περίοδο 2^n-1, η γραμμική πολυπλοκότητα αυτή ισούται μόλις με n, οπότε γνώση 2n bits αυτής επιτρέπει τον υπολογισμό (πρόβλεψη) ολόκληρης. Αυτή η επίθεση μπορεί να εκτελεστεί με την χρήση του αλγορίθμου των Berlekamp-Massey. Για αυτό το λόγο οι αλγόριθμοι ροής πρέπει να χρησιμοποιούν ακολουθίες υψηλής γραμμικής πολυπλοκότητας προκειμένου να μην εμφανίζουν αδυναμίες (J. Massey, Jan. 1969).

Για αυτό τον λόγο που περιγράφεται στην παραπάνω παράγραφο έχουν γίνει πολλές προσπάθειες προκειμένου να αυξηθεί η μη γραμμικότητα ενός αλγορίθμου με τον συνδυασμό διαφόρων εξόδων από LFSRs (αφού η χαμηλή γραμμική πολυπλοκότητα της ακολουθίας είναι συνυφασμένη με την γραμμικότητα της γεννήτριας ακολουθίας) (A.J. Menezes, 1996). Αυτές οι προσπάθειες δεν έφεραν τα επιθυμητά επίπεδα ασφάλειας που αναμενόταν (A. Braeken and J. Lano, 2006). Η μη γραμμικότητα είναι μία ιδιότητα της συνάρτησης όπου δείχνει την ελάχιστη απόσταση της f από μία άλλη γραμμική συνάρτηση. Λόγω των προβλημάτων που εντοπίστηκαν στους LFSRs χρησιμοποιήθηκαν η μη γραμμική καταχωρητές ολίσθησης με ανάδραση (Nonlinear Feedback Shift Registers-NLFSRs). Οι NLFSRs μπορούν να υποστηρίξουν υψηλή μη γραμμικότητα σε σύγκριση με τους LFSRs. Ωστόσο, υπάρχουν ακόμη πολλά ερωτήματα ανοιχτά ως προς τη σχεδίαση NLFSR με αποδεδειγμένα καλές ιδιότητες.

2.2.4 Σύγχρονοι και Ασύγχρονοι Κρυπταλγόριθμοι Ροής

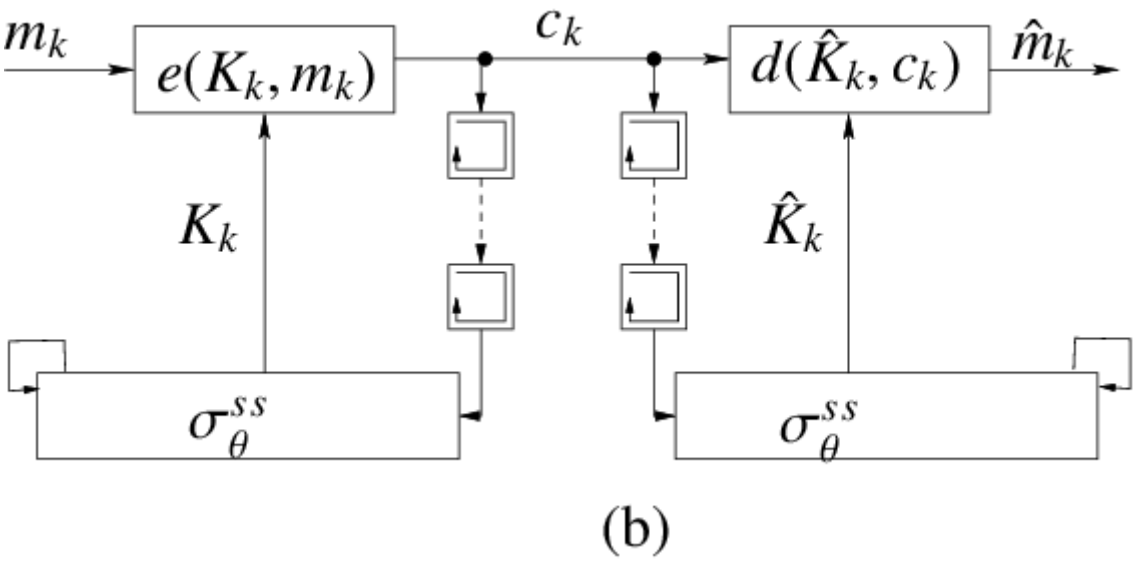
Ο σχεδιασμός των αλγόριθμων ροής περιέχει δύο σημαντικές διεργασίες. Η πρώτη σημαντική διεργασία είναι η αλληλεπίδραση του μηνύματος που πρόκειται να κρυπτογραφηθεί με την κλειδοροή. Η δεύτερη διεργασία είναι η κατάσταση του αλγόριθμου. Η πρώτη διεργασία πραγματοποιείται με την χρήση μίας XOR (exclusive-Or) μεταξύ των bit του μηνύματος και της κλειδοροής προκειμένου να προκύψει το

κρυπτογραφημένο μήνυμα. Η κατάσταση του αλγορίθμου κρυπτογράφησης χωρίζεται σε δύο κατηγορίες, οι οποίες είναι η σύγχρονη και η ασύγχρονη.



Εικόνα 5: Σύγχρονος αλγόριθμος ροής

Στους σύγχρονους αλγορίθμους ροής η κατάστασή τους ενημερώνεται αυτόνομα, χωρίς να υπάρχει η ανάγκη χρησιμοποίησης του αρχικού κειμένου ή του κρυπτογραφημένου κειμένου. Κατά αυτόν τον τρόπο η πιθανή μετάδοση ενός λανθασμένου Bit είτε λόγω θορύβου στο κανάλι διάδοσης είτε λόγω επεξεργαστικού λάθους δεν θα έχει καμία επίπτωση στα bit που ακολουθούν. Παρόλο που φαίνεται ότι είναι μία ιδιότητα που μπορούσε να είναι επιθυμητή έχει κάποια βασικά μειονεκτήματα. Ένα από αυτά είναι μία επίθεση, κατά την οποία ο υποκλοπέας θα εκτελέσει μερικές αλλαγές σε συγκεκριμένα bit του κρυπτογραφημένου κειμένου που θα οδηγήσουν σε ένα νέο μήνυμα, το οποίο θα περιέχει διαφορετικές πληροφορίες από αυτές που έστειλε ο νόμιμος αποστολέας. Για να γίνει η σωστή αποκρυπτογράφηση του μηνύματος, στους σύγχρονους αλγόριθμους ροής, θα πρέπει αποστολέας και λήπτης να είναι συγχρονισμένοι μεταξύ του ώστε κάθε φορά να προκύπτει η σωστή αλληλουχία κλειδοροής κάτι που επιτυγχάνεται με την χρήση σημειωμένων θέσεων επί του κρυπτογραφημένου κειμένου.



Εικόνα 6: Ασύγχρονος αλγόριθμος ροής

Σε αντίθεση με τους σύγχρονους αλγόριθμους, οι ασύγχρονοι υπολογίζουν την επόμενη κατάσταση της κλειδοροής (συνεπακόλουθα του κρυπτογραφημένου κειμένου) με την χρήση των bit που παράχθηκαν προηγουμένως. Στο συγκεκριμένο τύπο υπάρχει ένα όριο σχετικά με την διάδοση λάθος, επειδή αν ένα Bit της ακολουθίας είναι λανθασμένο τότε τα επόμενα παραγόμενα bits από αυτό θα είναι εσφαλμένα. Βέβαια ο Rueppel περιέγραψε δύο μειονεκτήματα των συγκεκριμένων αλγορίθμων (New Approaches to Stream Ciphers, 1984). Το ένα είναι ότι κάποιος επιτιθέμενος μπορεί να αναγνωρίσει κάποιες από τις μεταβλητές που χρησιμοποιεί η γεννήτρια και το δεύτερο είναι η αδυναμία περαιτέρω ανάλυσης αυτών των γεννητριών αφού εξαρτώνται από το κείμενο που πρόκειται να κρυπτογραφήσουν.

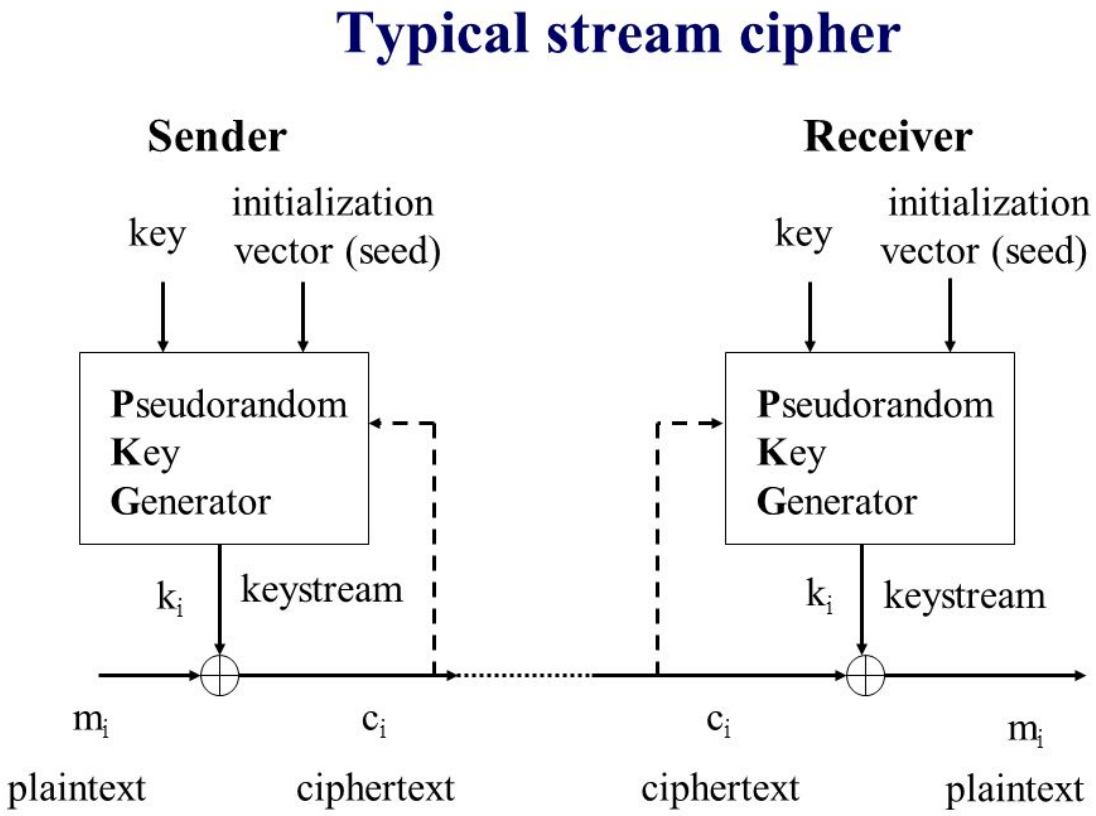
2.2.5 Σχεδίαση

Οι σχεδιαστές αλγορίθμων ροής λαμβάνουν υπόψιν του την περίοδο του αλγορίθμου, η οποία για να είναι αποδεκτή θα πρέπει να είναι αρκετά μεγάλη. Ο λόγος, που η μεγάλη περίοδος είναι μία επιθυμητή ιδιότητα, είναι ότι αλγόριθμοι με μικρή περίοδο μπορούν να δεχτούν επιθέσεις λόγω του ότι το κείμενο μπορεί να εμφανίσει ίδιες κρυπτογραφημένες λέξεις ή στοιχεία. Το ιδανικό θα ήταν ότι η αλληλουχία που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μέρους του κειμένου να μην επαναχρησιμοποιηθεί. Πρέπει, ακόμα, οι σχεδιαστές να ικανοποιούν τα κριτήρια τυχαιότητας που έθεσε ο Golomb προκειμένου μία γεννήτρια ψευδοτυχαίας ακολουθίας να θεωρείται ότι πλησιάζει τις ιδιότητες μιας πραγματικά τυχαίας γεννήτριας (S.W.

Golomb, 1981). Παρόλο που μία γεννήτρια μπορεί να ικανοποιεί τα κριτήρια τυχαιότητας του Golomb δεν αποδεικνύεται ότι προσφέρει καλή ψευδοτυχαία ακολουθία για αυτό πρέπει να εφαρμοστούν διάφορα στατιστικά τεστ προκειμένου να αποδειχθεί η τυχαιότητα των παραγόμενων στοιχείων (H. Piper, 1982).

2.2.6 Διάνυσμα Αρχικοποίησης (Initialization Vector-IV)

Στους μοντέρνους αλγόριθμους ροής εισάγονται δύο ακολουθίες. Η πρώτη είναι το κρυφό κλειδί k και το δεύτερο το διάνυσμα αρχικοποίησης (IV). Όπως είναι γνωστό το κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση (ουσιαστικά, «τροφοδοτεί» τη γεννήτρια κλειδοροής, η οποία χρησιμοποιείται και στην κρυπτογράφηση και στην αποκρυπτογράφηση). Το IV, όμως, χρησιμοποιείται για να εγγυηθεί για την ασφάλεια του συστήματος επικοινωνίας και να αποφευχθεί κάποιος επιτιθέμενος να χρησιμοποιήσει παλαιότερες επικοινωνίες μεταξύ των δύο μερών και να επιδοθεί σε μία επαναλαμβανόμενη επίθεση (replay attack).



Εικόνα 7: Αλγόριθμος ροής

2.3 Κρυπτογραφικοί Αλγόριθμοι Τμήματος (Block ciphers)

Οι κρυπτογραφικοί αλγόριθμοι τμήματος χρησιμοποιούν στην λειτουργία τους έναν αλγόριθμο, ο οποίος εφαρμόζεται σε ένα τμήμα του κειμένου για να του προσφέρει ασφάλεια. Οι συγκεκριμένοι αλγόριθμοι χρησιμοποιούνται για την τήρηση της εμπιστευτικότητας αλλά και της αυθεντικότητας ενός μηνύματος (NIST Computer Security Division's (CSD) Security Technology Group(STG), 2012). Έτσι ο αλγόριθμος τμήματος είναι απόλυτος υπεύθυνος για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση ενός συγκεκριμένου τμήματος της πληροφορίας. Οι πράξεις της κρυπτογράφησης, εφόσον επενεργούν σε ολόκληρο το τμήμα από bit, και όχι σε μεμονωμένα bit, είναι πιο σύνθετες από ό,τι μία πράξη XOR που συναντάται, όπως είδαμε παραπάνω, στους αλγόριθμους ροής.

2.3.1 Διάνυσμα Αρχικοποίησης (Initialization Vector-IV)

Το διάνυσμα αρχικοποίησης χρησιμοποιείται στον αλγόριθμο τμήματος προκειμένου να διασφαλιστεί ότι ένα τμήμα πληροφορίας κρυπτογραφηθεί ξανά με το ίδιο κλειδί το αποτέλεσμα του κρυπτογραφημένου κειμένου να είναι διαφορετικό από αυτό της πρώτης κρυπτογράφησης. Για τον παραπάνω λόγο το IV χρησιμοποιείται σχεδόν σε όλους τους σύγχρονούς αλγόριθμους τμήματος. Αξίζει να σημειωθεί ότι σε κάποιες περιπτώσεις θα πρέπει να είναι και το τυχαίο το IV που χρησιμοποιείται για να παράγεται ένα ασφαλή κρυπτογραφημένο κείμενο.

Η κύρια λειτουργία του IV είναι να κάνει τυχαίο τον τρόπο της κρυπτογράφησης της πληροφορίας. Παρόλο που ο ρόλος του IV είναι διαφορετικός από το κλειδί που χρησιμοποιείται για την κρυπτογράφηση έχει αποδειχτεί ότι σε αρκετά είδη αλγορίθμων δέσμης η επαναχρησιμοποίηση του IV καταστρέφει μερικώς ή και ολοσχερώς την ασφάλεια που παρέχει ο αλγόριθμος (B. Moeller, 2004).

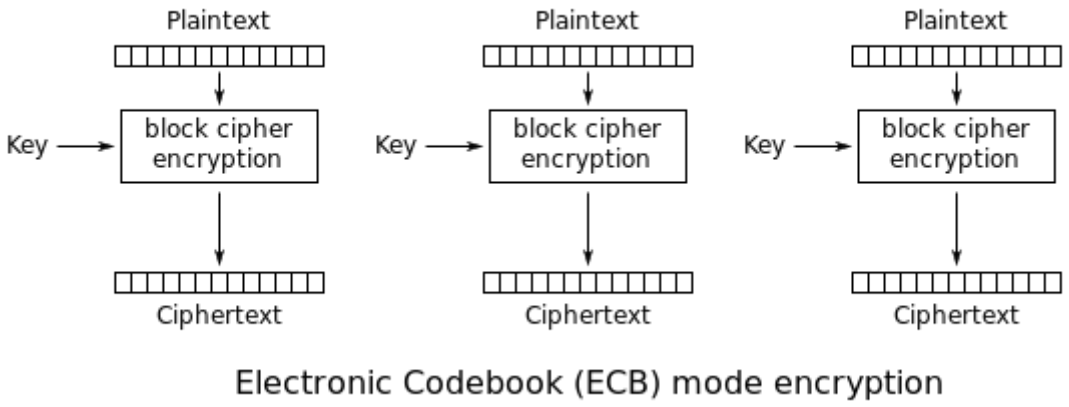
2.3.2 Padding

Η πληροφορία που θέλει ο αποστολέας να κρυπτογραφήσει μπορεί να ποικίλει σε μέγεθος με αποτέλεσμα ο αλγόριθμος τμήματος που να χρησιμοποιηθεί να έχει τμήματα (block) που να μην έχουν συμπληρωθεί με πληροφορία. Για αυτό το λόγο χρησιμοποιείται το padding το οποίο γεμίζει τα κενά σημεία του τελευταίου τμήματος έτσι ώστε ο

αλγόριθμος να μπορέσει να κρυπτογραφήσει σωστά το κείμενο. Βέβαια η αναγκαιότητα για το γέμισμα των κενών έγκειται σε ποιον τρόπο λειτουργίας επιθυμούμε να χρησιμοποιήσουμε.

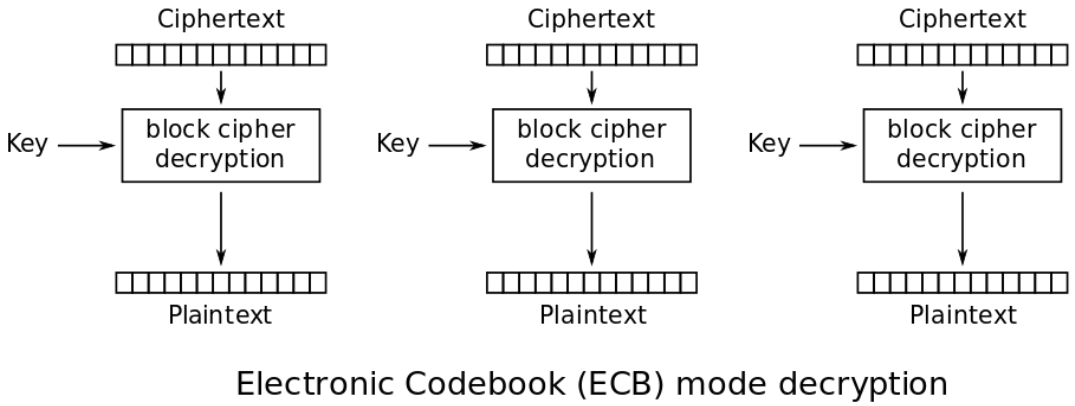
2.3.3 Γνωστοί Τρόποι Λειτουργίας Αλγορίθμων Τμήματος

Ο τρόπος λειτουργίας Electronic Codebook (ECB) αποτελεί έναν από τους πιο απλούς τρόπους σε αλγόριθμο τμήματος. Στην συγκεκριμένη έκδοση η πληροφορία χωρίζεται σε συγκεκριμένα τμήματα και έπειτα κάθε ένα από αυτά κρυπτογραφείται ξεχωριστά με την χρήση του κλειδιού.



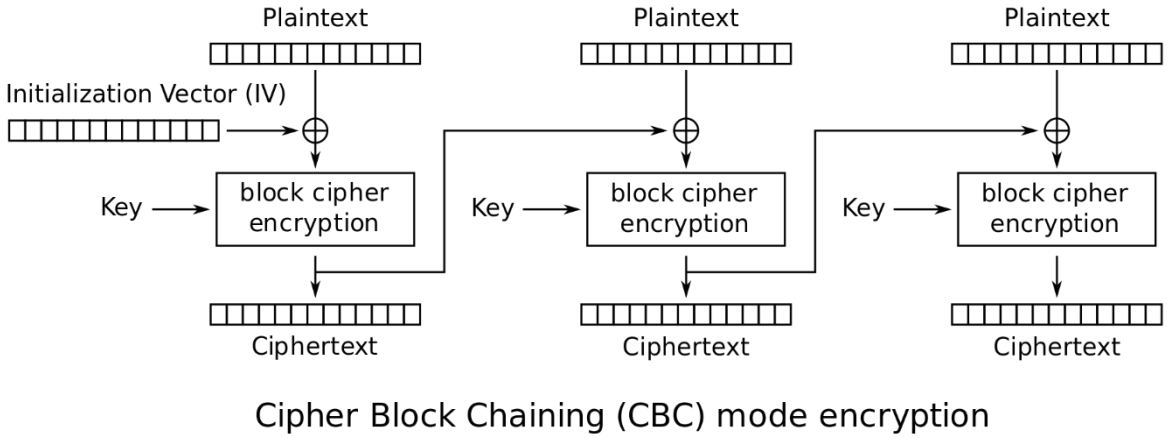
Εικόνα 8: ECB τρόπος λειτουργίας αλγορίθμου τμήματος (κρυπτογράφηση)

Το βασικό μειονέκτημα του συγκεκριμένου τρόπου λειτουργίας είναι ότι ίδια τμήματα κειμένου σε διαφορετικά σημεία της πληροφορίας κρυπτογραφούνται με ακριβώς τον ίδιο τρόπο. Αυτή η ιδιότητα οδηγεί τον αλγόριθμο σε ευπάθεια σε replay attacks. Σε κάθε περίπτωση, το κρυπτοκείμενο αποκαλύπτει κάποια πληροφορία για το μήνυμα (όπως το ότι το μήνυμα περιέχει κάποια επαναλαμβανόμενα μοτίβα). Για τον λόγο αυτό η έκδοση αυτή δεν χρησιμοποιείται καθόλου στην κρυπτογραφία ή σε πολύ περιορισμένες, ειδικού τύπου, περιπτώσεις (M. Dworkin, 2001).



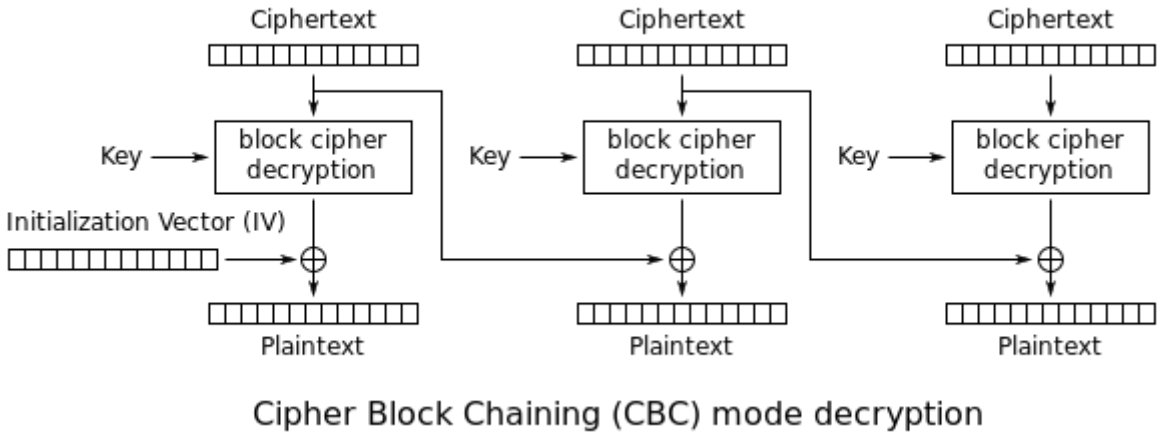
Εικόνα 9: ECB τρόπος λειτουργίας αλγορίθμου τμήματος (αποκρυπτογράφηση)

Ένας άλλος τρόπος λειτουργίας είναι ο Cipher Block Chaining (CBC), ο οποίος δημιουργήθηκε από τους Ehrsam, Meyer, Smith και Tuchman περί το 1976 και είναι μία πιο πολύπλοκη μορφή ενός αλγορίθμου τμήματος σε σχέση με τον ECB. Στον συγκεκριμένο τρόπο λειτουργίας κάθε τμήμα της πληροφορίας εκτελεί την δυαδική πράξη XOR με το κρυπτογραφημένο προηγούμενο τμήμα. Το πρώτο τμήμα του κειμένου εκτελεί την πράξη XOR με το IV.



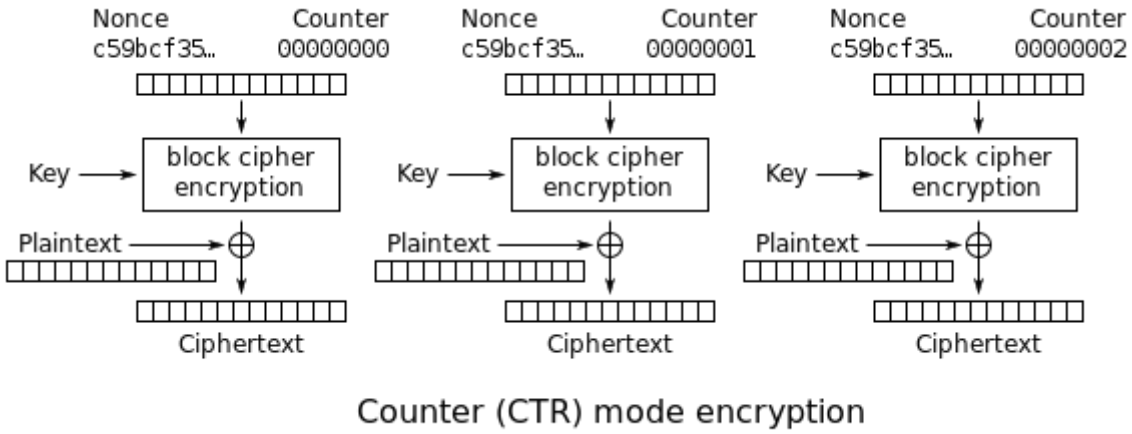
Εικόνα 10: CBC αλγόριθμος τμήματος (κρυπτογράφηση)

Ο συγκεκριμένος τρόπος λειτουργίας χρησιμοποιείται ευρέως αν και παρουσιάζει αρκετά μειονεκτήματα. Ένα από τα μειονεκτήματα που διαθέτει είναι, όπως ισχύει άλλωστε και στον ECB τρόπο, ότι πρέπει να εφαρμοστεί το padding για πληροφορίες που δεν είναι ακριβώς διαιρούμενες με το μέγεθος των block.



Εικόνα 11: CBC αλγόριθμος τμήματος (αποκρυπτογράφηση)

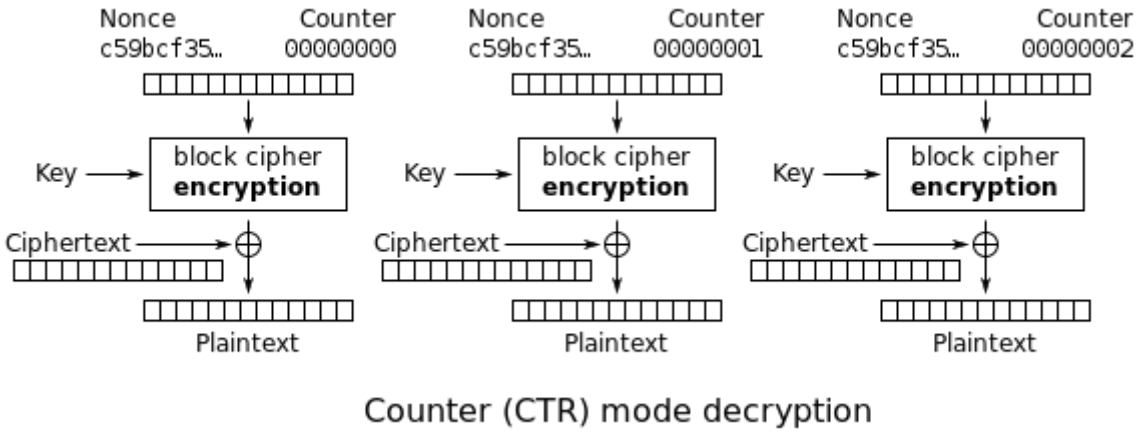
Ένας ακόμα γνωστός τρόπος λειτουργίας αλγορίθμου τμήματος είναι ο Counter (CTR). Με την χρήση του CTR ο κρυπτογραφικός αλγόριθμος μετατρέπεται, ουσιαστικά, από τμήματος σε ροής. Μία γεννήτρια παραγωγής αυξανόμενων αριθμών (μετρητής) παράγει μία ακολουθία, η οποία, εν συνεχεία, κρυπτογραφείται στον αλγόριθμο τμήματος με την χρήση του μυστικού κλειδιού και το αποτέλεσμά τους προστίθεται με πράξη XOR με το αρχικό κείμενο προκειμένου να προκύψει το κρυπτογραφημένο κείμενο. Η γεννήτρια αυτή παράγει ακολουθία η οποία αυξάνεται κατά ένα ανά κύκλο και έχει την βασική ιδιότητα ότι δεν επαναλαμβάνεται για μεγάλο χρονικό διάστημα.



Εικόνα 12: CTR αλγόριθμος τμήματος (κρυπτογράφηση)

Ο συγκεκριμένος αλγόριθμος τμήματος έχει μία αρχική ποσότητα, η οποία αναπαριστά το IV, η οποία είναι τυχαία και προστίθεται με XOR ή απλή πρόσθεση για να δημιουργηθεί ένα μοναδικό τμήμα του μετρητή, το οποίο θα εισαχθεί στον αλγόριθμο κρυπτογράφησης. Αυτή η τυχαία ποσότητα ονομάζεται nonce. Συνήθως η ποσότητα

nonce έχει τιμή ως 64 bits και ο μετρητής έχει μέγεθος από 64 έως 128 bits ανά τμήμα. Η απλή πρόσθεση των δύο ποσοτήτων ή και η πράξη XOR μεταξύ τους παρουσιάζει ευπάθεια ως προς τις επιθέσεις με την χρήση chosen-plaintext επίθεσης.



Εικόνα 13: CTR αλγόριθμος τμήματος (αποκρυπτογράφηση)

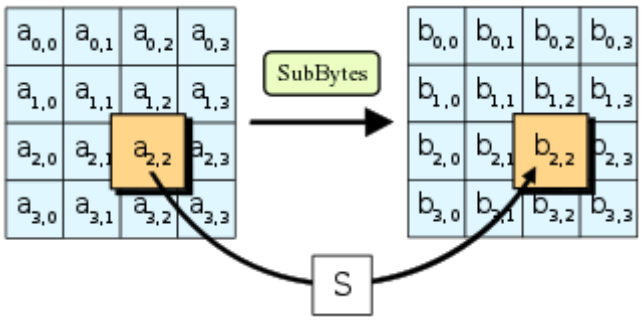
2.4 Advanced Encryption Standard (AES)

Ο AES είναι μία οικογένεια αλγορίθμων των Rijndael αλγορίθμων τμήματος με διαφορετικό μέγεθος μυστικού κλειδιού και μεγέθους τμήματος. Αποτέλεσε πρόταση των ερευνητών Vincent Rijmen και Joan Daemen κατά τον διαγωνισμό του NIST μεταξύ των ετών 1997 και 2000 για την εύρεση ενός πρότυπου αλγορίθμου προς αντικατάσταση του Data Encryption Standard (DES) (V. Rijmen, 2003). Ο διαγωνισμός έθετε ως βασικές προϋποθέσεις ελάχιστο μήκος κλειδιού 128 bits και δυνατότητα υλοποίησης σε επεξεργαστές 8 bit.

Ο αλγόριθμος Rijndael υποστηρίζει τρία μεγέθη κλειδιού, 128, 192 και 256 bits, και τρία μήκη τμήματος δεδομένων, 128, 192 και 256 bits. Στο πρότυπο του AES χρησιμοποιήθηκε μέγεθος τμήματος των 128 bits. Βασικό πλεονέκτημα του αλγορίθμου είναι η εύκολη υλοποίησή του από άποψη hardware (Federal Information Processing Standards Publication,, 2001). Αποτελείται από 10 έως 15 επαναλήψεις ανάλογα με το μέγεθος του κλειδιού. Κάθε επανάληψη αποτελείται από τις παρακάτω 4 βασικές πράξεις:

i) Αντικατάσταση Byte (=8 bits) με την χρήση s-boxes που διαθέτουν καλά χαρακτηριστίκα (Byte Substitution).
ii) Ολίσθηση (Shift Row).
iii) Συνδυασμός πολλών bit (Mix Column).

iv) Πρόσθεση (XOR) του κλειδιού.



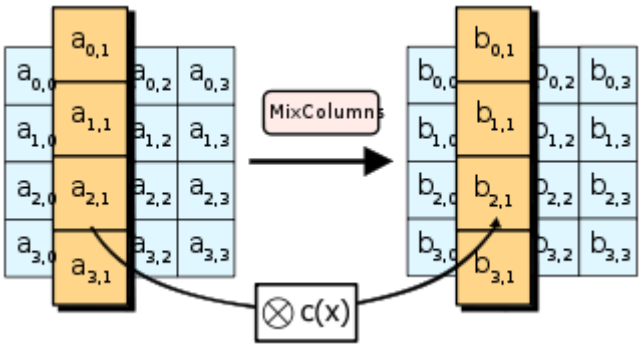
Εικόνα 14: Στάδιο αντικατάστασης Byte στον αλγόριθμο AES

Στον παρακάτω πίνακα φαίνεται το πλήθος των γύρων ανάλογα με το μέγεθος του κλειδιού καθώς και λοιπές παράμετροι:

Μέγεθος Κλειδιού	128	192	256
Μέγεθος Τμήματος	128	128	128
Πλήθος Γύρων	10	12	14
Μέγεθος υπο-Κλειδιού για κάθε γύρο	128	128	128
Μέγεθος Επεκταμένου Κλειδιού	176	208	240

Πίνακας 1: Παράμετροι λειτουργίας αλγορίθμου AES

Ο πρώτος γύρος είναι απλά μία πράξη XOR με το κλειδί. Οι υπόλοιποι γύροι είναι όμοιοι με τον πρώτο γύρο εκτός από τον τελευταίο γύρο, ο οποίος είναι διαφορετικός.



Εικόνα 15: Στάδιο συνδυασμού bit στον αλγόριθμο AES

Τα τελευταία έτη διάφοροι ερευνητές προσπαθούν να δημιουργήσουν κρυπτογραφικούς αλγόριθμους τμήματος που να μπορούν να υλοποιηθούν σε μικρής υπολογιστικής ισχύος και μνήμης συσκευές, λόγω των περιορισμένων πόρων. Ο AES παρέχει καλές τεχνικές

υλοποίησης αλλά σε ορισμένες συσκευές δεν μπορεί να υλοποιηθεί λόγω των υψηλών απαιτήσεων του αλγορίθμου σε υπολογιστικούς πόρους. Για αυτό τον λόγο δημιουργήθηκαν αλγόριθμοι τμήματος με χαμηλές απαιτήσεις σε υπολογιστικούς πόρους και ονομάστηκαν lightweight κρυπτογραφικοί αλγόριθμοι. Έτσι η πρόκληση που έθεσαν οι lightweight αλγόριθμοι είναι σχεδιαστική πρόκληση για τους ερευνητές, επειδή πρέπει να διασφαλίζεται η ασφάλεια αλλά και η απόδοση του αλγορίθμου.

Κεφάλαιο 3
Διαδίκτυο Των Πραγμάτων

Η ιδέα ενός δικτύου αποτελούμενο από πολλές έξυπνες συσκευές ξεκίνησε περί το 1982 με την χρήση ενός τροποποιημένου αυτόματου πωλητή γνωστής πολυεθνικής εταιρείας στο Carnegie Mellon University. Ο συγκεκριμένος αυτόματος πωλητής είχε τροποποιηθεί προκειμένου να αναφέρει τις ποσότητες που διαθέτει από αναψυκτικά και για το εάν τα νέα τοποθετημένα αναψυκτικά ήταν παγωμένα ή όχι (M. Weiser, 1991). Κατά αυτόν τον τρόπο ο παραπάνω πωλητής αποτέλεσε το αρχικό δημιούργημα για την ενσάρκωση της ιδέας ενός έξυπνου πωλητή και συνεπακόλουθα η αρχική υλοποίηση ενός δικτύου με «έξυπνες» συσκευές. Η συνέχεια της ιδέας του «Διαδικτύου των πραγμάτων»(Internet Of Things, πλέον θα αναφερόμαστε στον όρο με την συντομογραφία IoT).

3.1 Ιστορία

Ο όρος Internet Of Things (IoT) καθιερώθηκε από τον Kevin Ashton, καθώς ήταν εκείνος που θεώρησε αναγκαία την ύπαρξη των radio-frequency identification (RFID) στο Διαδίκτυο των Πραγμάτων, αφού με την βοήθεια των RFID γίνεται δυνατός ο έλεγχος της κάθε μίας ηλεκτρονικής συσκευής (P. Magrassi, 12 August 2002) (Commission of the European Communities, 2009). Σύμφωνα με την Cisco Systems η «γέννηση» του IoT εκτιμάται ότι έγινε μεταξύ του 2008 και του 2009, όπου έγινε αύξηση των ηλεκτρονικών συσκευών που ήταν συνδεδεμένες στο διαδίκτυο σε σύγκριση με τον αριθμό των ανθρώπων. Αυτή η αναλογία ηλεκτρονικών συσκευών/αριθμός ανθρώπων αυξήθηκε από 0.08 το 2003 σε 1.84 το 2010 (D. Evans, 2011).

Ο Mohamed M. Atalla και ο Dawon Kahng εφηύραν στα εργαστήρια της Bell το τρανζίστορ MOSFET(metal-oxide-semiconductor field-effect transistor) το 1959 το οποίο θεωρείται απαραίτητο για την επίτευξη του IoT. Το συγκεκριμένο τρανζίστορ είναι το αναπόσπαστο κομμάτι όλων των σύγχρονων ηλεκτρονικών συσκευών, όπως ηλεκτρονικών υπολογιστών, κινητών τηλεφώνων και των υπηρεσιών του διαδικτύου. Στην σύγχρονη εποχή οι επιστήμονες προσπαθούν την μείωση του μεγέθους τον εν λόγω

τρανζίστορ για την μείωση της κατανάλωσης ενέργειας, χρήση της silicon on insulator (SOI) τεχνολογίας και την χρήση πολλών πυρήνων επεξεργασίας, τεχνολογίες που είναι κύριες στο IoT (D. Khang, 1963).

3.2 Λειτουργίες του IoT

Η λειτουργία του IoT στηρίζεται σε μία πλατφόρμα, η οποία συγκεντρώνει δεδομένα από συσκευές και αντικείμενα με αισθητήρες. Αυτή η πλατφόρμα συγκεντρώνει τα δεδομένα από τους αισθητήρες και τις διαμοιράζεται με συγκεκριμένες εφαρμογές, που έχουν αναπτυχθεί για την ανάλυση των δεδομένων αυτών και αντιμετώπιση των αναγκών. Χάρις σε αυτές τις συσκευές που αποτελούν το IoT αυτοματοποιεί διάφορες εργασίες που μπορεί να είναι επαναλαμβανόμενες ή επικίνδυνες (IBM, 2016).

Η διαχείριση των δεδομένων αυτών αποτελεί μία μεγάλη πρόκληση για τους κατασκευαστές τεχνολογικών συστημάτων, καθώς απαιτείται η διαχείριση και η ανάλυση μεγάλου όγκου πληροφοριών. Ο τεράστιος όγκος των πληροφοριών αυτών προκύπτει λόγω της συνεχούς επικοινωνίας των συσκευών του συστήματος IoT με το δίκτυο δημιουργώντας έτσι την ανάγκη του συστήματος για μεγάλη αποθηκευτική μνήμη (J. Gubbi).

3.3 Εφαρμογές του IoT

Η χρήση συσκευών που αποτελούν μέρη ενός IoT συστήματος έχουν εφαρμογή σε διάφορους τομείς της σύγχρονής κοινωνίας. Αυτές μπορεί να είναι σε καταναλωτές, βιομηχανικούς, εμπορικούς και στρατιωτικούς σκοπούς.

Οι κύριες χρήσεις που αφορούν το καταναλωτικό κοινό μπορούν να συνοψιστούν στα αυτόνομα οχήματα, στο «έξυπνο» σπίτι, στην απομακρυσμένη παρακολούθηση υγείας και εφαρμογές για την παρακολούθηση ασθενών (Indian Business of Tech, 2016).

Οι κύριες εφαρμογές για βιομηχανικούς σκοπούς είναι η εφαρμογή του συστήματος IoT στην αυτοματοποίηση της διαδικασίας παραγωγής των αγαθών κάθε βιομηχανίας μειώνοντας τον χρόνο παραγωγής και αυξάνοντας την παραγωγή τους. Ακόμα η τεχνολογία του IoT μπορεί να εφαρμοστεί σε φάρμες ή οποιοδήποτε επάγγελμα το οποίο σχετίζεται άμεσα με την μέτρηση διαφόρων περιμέτρων του εδάφους ή και του ίδιου του

περιβάλλοντος για την λήψη μέτρων αποτροπής παραγόντων που μπορούν να απομειώσουν την σοδειά ή την παραγωγή (J. Lee).

Στον τομέα το εμπορίου το σύστημα του IoT μπορεί να εφαρμοστεί στο τομέα της υγείας και περίθαλψης των ασθενών χρησιμοποιώντας αισθητήρες RFID οι οποίοι θα μετρούν τις παραμέτρους στην υγεία των ασθενών απομειώνοντας έτσι τον χρόνο αντίδρασης σε περίπτωση που δημιουργηθεί κάποιο ιατρικό περιστατικό με τον ασθενή (N. Dey, 2018). Ακόμα μπορεί να χρησιμοποιηθεί για την αύξηση της ασφάλειας των οδικών μεταφορών των πολιτών μίας πόλης με την συνεχόμενο έλεγχο διαφόρων παραμέτρων όσων αφορά το ίδιο το όχημα αλλά και του οδοστρώματος (M. Ersue, 2014).

Τέλος η τεχνολογία IoT μπορείς να εφαρμοστεί στον τομέα των στρατιωτικών εφαρμογών συμπεριλαμβάνοντας την χρήση αισθητήρων, ρομπότ, οχημάτων, βιομετρικών προσθετικών για τον άνθρωπο και άλλα τεχνολογικά προϊόντα που μπορούν να βελτιώσουν τις συνθήκες σε ένα εμπόλεμο περιβάλλον (L. Cameron). Για αυτό το λόγο σχεδιάστηκαν δύο μεγάλα project για την βελτιστοποίηση των στρατιωτικών επιχειρήσεων που ονομάζονται Internet of Battlefield Things (IoBT) (K. Gudeman) και Ocean of Things (OoT) (A. Nordum, 2020).

3.4 Τεχνικά Ζητήματα

Λόγω των δεδομένων που αποστέλλονται από τις συσκευές που αποτελούν το σύστημα IoT δημιουργούνται προκλήσεις που αφορούν τον τρόπο που πρέπει να αποστέλλονται στην κεντρική πλατφόρμα. Κατά αυτόν τον τρόπο εγείρονται διάφορα ερωτήματα για την ασφάλεια που μπορούν να επιδείξουν τέτοια συστήματα. Βέβαια είναι μία τεχνολογία που βρίσκεται ακόμα σε στάδιο εξέλιξης και συνεπώς επιδέχεται συνεχώς βελτιώσεις προκειμένου στο μέλλον να αποτελέσει μία πολύ ασφαλής τεχνολογία. Το 2008 ερευνητές είχαν επιτύχει την εξ' αποστάσεως ικανότητα ελέγχου βηματοδοτών, ενώ σε μεταγενέστερες προσπάθειες διάφοροι επιστήμονες κατάφεραν να επιτύχουν τον εξ' αποστάσεως έλεγχο των αντλιών ινσουλίνης (Scientific American, April 2015).

Τα κύρια τεχνικά ζητήματα που προκύπτουν για τις συσκευές του IoT είναι ίδια με τα τεχνικά ζητήματα που προκύπτουν σε εξυπηρετητές (server), σταθμούς εργασίας (workstations) και κινητά τηλέφωνα. Σε αυτά συμπεριλαμβάνονται αδυναμία αυθεντικοποίησης, μη κρυπτογραφημένα μηνύματα που μεταφέρονται σε ανασφαλή

δίκτυα ανάμεσα στις συσκευές, SQL injections και αδυναμία σωστού τρόπου εγκατάστασης ενημερώσεων ασφαλείας (S. Li, 2017). Βέβαια οι συσκευές της τεχνολογίας IoT έχουν αρκετούς περιορισμούς σχετικά με την ικανότητα που προσφέρουν λόγω υλικού κατασκευής προσθέτοντας επιπλέον περιορισμούς στον τρόπο ασφάλισης των συσκευών αυτών. Σε αυτούς τους περιορισμούς είναι η κατανάλωση ενέργειας καθώς αρκετές συσκευές είναι παθητικές και όχι ενεργητικές. Κατά αυτόν τον τρόπο οι περιορισμοί αυτοί οδηγούν στην ανικανότητα χρήσης βασικών μέτρων στην ασφάλεια όπως της χρήσης τοίχους προστασίας ή και την χρήση δυνατών κρυπτογραφικών αλγορίθμων για την κρυπτογράφηση των μηνυμάτων (X. Liu, 2018).

Από τα πολλά τεχνικά ζητήματα που προκύπτουν σε νέες τεχνολογίες κάποια από αυτά αναφέρονται παραπάνω. Σε αυτή την διατριβή θα επικεντρωθούμε στην χρήση κρυπτογραφικών αλγορίθμων σε συσκευές της τεχνολογίας IoT. Οι αλγόριθμοι που θα αναλυθούν θα έχουν επιλεχθεί από το National Institute of Standards and Technology (NIST).

Κεφάλαιο 4
Κρυπτογραφικές Ιδιότητες Ακολουθιών και Συναρτήσεων

Είδαμε νωρίτερα ότι για τους αλγόριθμους ροής είναι απαραίτητο να χρησιμοποιούνται ακολουθίες με καλά χαρακτηριστικά τυχαιότητας, όπως υψηλή γραμμική πολυπλοκότητα. Ταυτόχρονα όμως, τόσο στους αλγόριθμους ροής όσο και στους αλγορίθμους τμήματος είναι σημαντικό, κατά την κατασκευή τους, να επιλέγονται συναρτήσεις με κάποιες επιθυμητές ιδιότητες. Συγκεκριμένα, σε μεγάλο πλήθος συμμετρικών κρυπτογραφικών αλγορίθμων χρησιμοποιούνται λογικές συναρτήσεις (Boolean functions) οι οποίες, αναλόγως και του τρόπου με τον οποίο χρησιμοποιούνται στον αλγόριθμο, πρέπει να ικανοποιούν σύνολο συγκεκριμένων κρυπτογραφικών κριτηρίων. Αντίστοιχα, πέραν των λογικών συναρτήσεων, χρησιμοποιούνται και διανυσματικές (vectorial) συναρτήσεις, οι οποίες δεν είναι κάτι άλλο από λογικές συναρτήσεις με περισσότερες από μία εξόδους (τέτοιες συναρτήσεις, όταν χρησιμοποιούνται σε κρυπτογραφικού αλγορίθμους, ονομάζονται μονάδες αντικατάστασης (Substitution Box ή S-box), όταν ουσιαστικά χρησιμοποιούνται κατά τρόπο τέτοιο ώστε να αντικαθιστούν τα bit της εισόδου με κάποια άλλα bit – αυτά της αντίστοιχης εξόδου).

Σε αυτό το κεφάλαιο θα γίνει ανάλυση αρχικώς ενός κρυπτογραφικού κριτηρίου ακολουθιών που είναι επέκταση της γραμμικής πολυπλοκότητας, το λεγόμενο προφίλ ή φάσμα γραμμικής πολυπλοκότητας σφάλματος (Error Linear Complexity Spectrum (ELCS)), για το οποίο υπάρχουν γνωστά ερευνητικά αποτελέσματα στην περίπτωση ακολουθίας με περίοδο 2^n για κάποιον ακέραιο αριθμό n. Στην συνέχεια θα μελετηθούν οι Boolean συναρτήσεις, καθώς και τα αντίστοιχα σημαντικά κρυπτογραφικά τους

κριτήρια. Θα δοθεί ιδιαίτερη έμφαση σε ένα πρόσφατο ερευνητικό αποτέλεσμα (K. Limniotis, 2019), το οποίο συνδέει τις ακολουθίες με τις λογικές συναρτήσεις και, κατ' αυτόν τον τρόπο, αλγόριθμοι γνωστοί στον τομέα των ακολουθιών μπορούν να δώσουν χρήσιμη πληροφορία σε ένα συγκεκριμένο κρυπτογραφικό κριτήριο λογικών συναρτήσεων – συγκεκριμένα, στο κατά πόσον μία λογική συνάρτηση μπορεί να προσεγγιστεί από άλλη η οποία έχει μικρότερο πλήθος μεταβλητών.

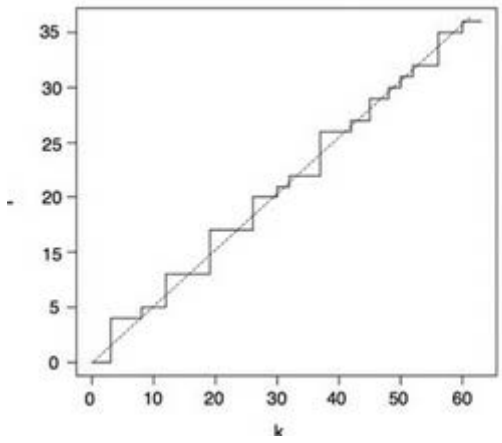
4.1 Error Linear Complexity Spectrum (ELCS)

Οι κλειδοροές που χρησιμοποιούνται από τους αλγόριθμους ροής προκειμένου να συνδυαστούν με την πληροφορία και να προκύψει το κρυπτογραφημένο μήνυμα είναι δυαδικές αλληλουχίες με καλές ψευδοτυχαίες ιδιότητες όπως η γραμμική πολυπλοκότητα (A. Rueppel, 1986). Η γραμμική πολυπλοκότητα περιγράφει τον μικρότερο δυνατό LFSR που μπορεί να αναπαράγει την αλληλουχία s. Για τον λόγο αυτό οι συναρτήσεις που χρησιμοποιούνται στην κρυπτογραφία θα πρέπει να έχουν υψηλή γραμμική πολυπλοκότητα προκειμένου να αποφεύγεται η αναπαράστασή της με μικρού μεγέθους LFSR. Βέβαια η γραμμική πολυπλοκότητα δεν είναι η μόνη ιδιότητα που ελέγχεται προκειμένου η συνάρτηση να έχει καλές κρυπτογραφικές ιδιότητες.

Άλλες ιδιότητες που πρέπει να τηρούνται ώστε η συνάρτηση να παρουσιάζει καλά κρυπτογραφικά κριτήρια είναι οι υποθέσεις του Golomb. Οι υποθέσεις αυτές αποδεικνύουν ότι η δυαδική ακολουθία που προκύπτει από μια συνάρτηση έχει ψευδοτυχαία χαρακτηριστικά (S.W. Golomb, 1981). Παρόλα αυτά, τα κριτήρια του Golomb πρέπει να τηρούνται αλλά από μόνα τους δεν παράγουν μία αλληλουχία η οποία είναι κατάλληλη για την κρυπτογραφία. Αυτό αποδεικνύεται από τον αλγόριθμο των Berlekamp-Massey με τον οποίο ο επιτιθέμενος χρησιμοποιώντας 2l συνεχόμενα bits της αλληλουχίας του κρυπτογραφημένου μηνύματος, όπου l είναι η γραμμική πολυπλοκότητα της κλειδοροής, μπορεί να βρει όλη την αλληλουχία και την συνάρτηση που την παράγει. Για την εύρεση της συνάρτησης ο αλγόριθμος απαιτεί μέχρι και $O(N^2)$ κύκλους, έχοντας ως γνωστό αριθμό το N (όπου, στην περίπτωση που περιεγράφηκε, το N ισούται με 2l). Με την χρήση του συγκεκριμένου αλγορίθμου υπολογίζεται η γραμμική πολυπλοκότητα αλλά και η συνάρτηση ανάδρασης του μικρότερου σε μέγεθος LFSR που παράγει την συγκεκριμένη αλληλουχία s (J. Massey, Jan. 1969).

Εκτός από τον αλγόριθμο των Belekamp-Massey, ο αλγόριθμος Games-Chan (GCA) είναι ικανός να υπολογίσει την γραμμική πολυπλοκότητα l με πολύ λιγότερους κύκλους (R. Games, 1983). Σε αυτόν τον αλγόριθμο η εύρεση της γραμμικής πολυπλοκότητας εκτελείται σε O(N) κύκλους, που σημαίνει ότι εκτελείται πολύ πιο γρήγορα από τον αλγόριθμο Berlekamp-Massey. Σε αντίθεση με τον χρόνο εύρεσης του επιθυμητού αποτελέσματος ο GCA απαιτεί ολόκληρη την περίοδο της αλληλουχίας προκειμένου να βγάλει το ορθό αποτέλεσμα, με αποτέλεσμα να μην ικανός να χρησιμοποιηθεί σε μοντέρνους αλγορίθμους με μεγάλες περιόδους (K. G. Paterson, 1994). Επίσης, ο αλγόριθμος CGA μπορεί να λειτουργήσει αποκλειστικά σε ακολουθίες περιοδικές με περίοδο 2^n (όπου n κάποιος ακέραιος αριθμός).

Η γραμμική πολυπλοκότητα αποτελεί ένα πολύ καλό κριτήριο όσων αφορά των ιδιοτήτων τυχαιότητας που παρουσιάζουν πεπερασμένες ακολουθίες. Οι τιμές της γραμμικής πολυπλοκότητας, για κάθε υπο-τμήμα της ακολουθίας, ονομάζεται προφίλ γραμμικής πολυπλοκότητας. Ο ορισμό αυτός δόθηκε από τον Rueppel. Αυτή η ανακάλυψη του Rueppel χρησιμοποιείται ως ένα χρήσιμο εργαλείο για την αξιολόγηση των κλειδοροών των αλγορίθμων ροής όσων αφορά τα κριτήρια τυχαιότητας (A. Rueppel, 1986). Μία τυχαία ακολουθία μήκος N αναμένεται να έχει τιμή γραμμικής πολυπλοκότητας πλησίον της τιμής N/2 και αυτό πρέπει να ισχύει για κάθε τμήμα της ακολουθίας (με σημείο αφετηρίας το πρώτο της bit) μήκους N'<N, όπως φαίνεται στο ακόλουθο σχήμα.



Σχήμα 1: Το προφίλ γραμμικής πολυπλοκότητας μίας τυχαίας ακολουθίας

Μία δυαδική αλληλουχία πρέπει να έχει υψηλή γραμμική πολυπλοκότητα προκειμένου να παρέχει ασφάλεια. Βέβαια δεν αρκεί μόνο να έχει την υψηλή γραμμική

πολυπλοκότητα, αλλά να διατηρεί υψηλή γραμμική πολυπλοκότητα ακόμα και εάν κάποια bits της αλληλουχίας αλλαχθούν. Σε αντίθετη περίπτωση που δεν διατηρείται η γραμμική πολυπλοκότητα τότε μπορεί η νέα κλειδοροή να μπορεί να παραχθεί από κάποιο μικρό LFSR που θα πλησιάζει την αρχική συνάρτηση. Η παραπάνω παρατήρηση έχει κρυπταναλυτική σημασία και περιγράφεται ως το κρυπτογραφικό κριτήριο της γραμμικής πολυπλοκότητας k σφαλμάτων (k-error linear complexity) μίας ακολουθίας. Από τον ορισμό καταλαβαίνουμε ότι το k-error linear complexity ασχολείται με τις τιμές που πρόκειται να λάβει η γραμμική πολυπλοκότητα της συνάρτησης άμα τροποποιηθούν το πολύ k bits της ακολουθίας (M. Stamp, 1993). Πιο συγκεκριμένα, η γραμμική πολυπλοκότητα k σφάλματος (που συμβολίζεται ως $c_k(s)=l_k$) μίας ακολουθίας δυαδικών δεδομένων που έχουν περίοδο N και γραμμική πολυπλοκότητα l [=c(s)] είναι η μικρότερη δυνατή γραμμική πολυπλοκότητα μίας τροποποιημένης ακολουθίας η οποία μπορεί να προκύψει από την αρχική εάν τροποποιηθούν k bits (ή, ισοδύναμα, συμβούν k σφάλματα) σε μια περίοδο της ακολουθίας αυτής.

Ο συνδυασμός του ELCS και της k-error linear complexity δείχνουν πως η γραμμική πολυπλοκότητα k σφαλμάτων της ακολουθίας μειώνεται όσο ο αριθμός k των bits που αλλάζουν αυξάνονται, δηλαδή $c_{k'}(s) \leq c_k(s)$ για κάθε k'>k. Προφανώς η γραμμική πολυπλοκότητα k σφαλμάτων είναι μέγιστη με l (c(s)) όσο δεν έχουμε κάποιο σφάλμα (δηλαδή k=0) και είναι ελάχιστη, ίση με τιμή 0, όταν το πλήθος k των σφαλμάτων είναι ίσο με το wt(s), όπου wt υποδηλώνει το βάρος Hamming της ακολουθίας – το οποίο ορίζεται ως το πλήθος των «1» της ακολουθίας. Οποιαδήποτε άλλο ζευγάρι με $(k, l' = c_k(s))$ ανήκει ανάμεσα στο προαναφερθέν διάστημα. Σύμφωνα με τους Martin και Stamp, αλλά και σε έρευνα που εκτέλεσε ο Niederreiter το ELCS επηρεάζεται από το k λάθος γραμμικής πολυπλοκότητας για το πως μειώνεται η γραμμική πολυπλοκότητα της αλληλουχίας s (M. Stamp, 1993) (H. Niederreiter, 1999).

Ο Martin και Stamp χρησιμοποίησαν τον αλγόριθμο Games – Chan και δημιούργησαν έναν αλγόριθμο με τον οποίο μπόρεσαν να μετρήσουν την γραμμική πολυπλοκότητα για μία δυαδική περιοδική ακολουθία με περίοδο $N = 2^n$ έχοντας συγκεκριμένο αριθμό σφαλμάτων k (M. Stamp, 1993). Σύμφωνα με τους ερευνητές ο αλγόριθμος υπολογίζει το αποτέλεσμα σε $O(N^2 \log N)$ κύκλους. Στην συνέχεια οι Lauder και Paterson κατάφεραν να δημιουργήσουν ένα πιο γενικό αλγόριθμο βασιζόμενοι στον παραπάνω αλγόριθμο (B. Lauder, 2003) (J. L. Massey, 1973).

Ο αλγόριθμος που δημιούργησαν οι Lauder και Paterson (LPA) απαιτεί για εισαγωγικά στοιχεία μία αλληλουχία s με περίοδο $N = 2^n$ και στην έξοδο του αλγορίθμου θα επιδεικνύονται τα σημεία στα οποία παρουσιάζεται μείωση της γραμμικής πολυπλοκότητας της αλληλουχίας καθώς και ο αριθμός των bits που πρέπει να αλλαχθούν για να προκύψει αυτή η μείωση. Τα σημεία που προκύπτουν ονομάζονται κρίσιμα σημεία του φάσματος γραμμικής πολυπλοκότητας k σφαλμάτων. Τα κρίσιμα σημεία έχουν την μορφή $(k, c_k(s))$ και όπως αναφέραμε παραπάνω όλες οι αλληλουχίες θα εμφανίζουν τουλάχιστον δύο κρίσιμα σημεία τα οποία θα είναι $(0, c(s))$ και $(wt(s), 0)$. Τα ενδιάμεσα στοιχεία εξαρτώνται από την ακολουθία αυτή καθαυτή. Για κάθε δοθέν k, μία κρίσιμη λανθασμένη ακολουθία, η οποία δημιουργείται από έναν παράγοντα e, η οποία έχει περίοδο N και weight (βάρος) k για την οποία ισχύει ότι η γραμμική πολυπλοκότητα προκύπτει είναι $c(s \oplus e) = c_k(s)$.

Για παράδειγμα, αν για μία ακολουθία s περιόδου 8 και βάρους 4 έχουμε τα εξής κρίσιμα σημεία: (0,8), (2,5), (4,0), αυτό συνεπάγεται ότι: i) $c(s)=c_0(s)=8$, ii) $c_1(s)=8$, iii) $c_2(s)=5$, iv) $c_3(s)=5$, v) $c_4(s)=0$ (η τελευταία είναι η περίπτωση όπου αλλάζουμε και τα τέσσερα bit της ακολουθίας που έχουν τιμή «1», οπότε προκύπτει η μηδενική ακολουθία, της οποίας η γραμμική πολυπλοκότητα θεωρείται κατά σύμβαση ίση με 0).

4.2 Λογικές Συναρτήσεις

Οι Λογικές (Boolean) συναρτήσεις είναι ένα αναπόσπαστο κομμάτι και πιο σημαντικό εργαλείο στην κρυπτογραφία. Η κύρια χρήση τους είναι στη δημιουργία δομών εντός των κρυπτογραφικών συστημάτων κατά τρόπο τέτοιο ώστε να επιτυγχάνονται καλές ιδιότητες. Αξίζει να σημειωθεί ότι τέτοιου είδους συναρτήσεις έχουν χρησιμοποιηθεί για την δημιουργία των S-boxes που χρησιμοποιούνται στους αλγόριθμους τμήματος (συμπεριλαμβανομένου του πρότυπου αλγορίθμου AES) αλλά και σαν κατασκευαστές φίλτρων ή συνδυαστική συνάρτηση στους αλγόριθμους ροής (A.J. Menezes, 1996). Η ευρεία χρήση τους οφείλεται κατά κύριο λόγο στην εύκολη δημιουργία τους από φθηνά εξαρτήματα αλλά και τον εύκολο προγραμματισμό τους. Εκτός από τα παραπάνω πλεονεκτήματα οι Boolean συναρτήσεις έχουν ανθεκτικότητα ενάντια σε πολλές κρυπταναλυτικές επιθέσεις, όταν χρησιμοποιούνται σωστά στα κρυπτογραφικά συστήματα.

Μία Boolean συνάρτηση είναι μία συνάρτηση στην επιστήμη των Μαθηματικών, η οποία είναι της μορφής $f: B^n \to B$, οπού $B = \{0,1\}$ και η μεταβλητή n είναι ένας θετικός ακέραιος αριθμός που δείχνει το πλήθος των μεταβλητών της συνάρτησης. Στην περίπτωση που η μεταβλητή n είναι 0 τότε η συνάρτηση είναι απλά ένας σταθερός αριθμός (δεν έχει καμία μεταβλητή). Πιο συγκεκριμένα όταν χρησιμοποιείται μία n-ιοστή Boolean συνάρτηση τότε η συνάρτηση αποτελείται από n μεταβλητές $x_1, \dots, x_n$. Η πιο συνήθης για κρυπτογραφικές εφαρμογές μορφή παρουσίασης είναι η Αλγεβρική Κανονική Μορφή (Algebraic Normal Form). Στη συγκεκριμένη μορφή παρουσιάζονται με XOR άθροισμα των γινομένων των μεταβλητών για παράδειγμα:

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$$

Στην συνέχεια του κειμένου της μεταπτυχιακής διατριβής το άθροισμα XOR θα παρουσιάζεται με το σύμβολο της απλής πρόσθεσης. Κάθε συνάρτηση έχει μόνο μία Αλγεβρική Κανονική Μορφή και, αντίστροφα, κάθε Αλγεβρική Κανονική Μορφή αντιστοιχεί ακριβώς σε μία λογική συνάρτηση.

Ένας διαφορετικός τρόπος παρουσίασης της Boolean συνάρτησης είναι μέσω του πίνακα αληθείας της με την οποία παρουσιάζονται όλες οι τιμές της F_2^n και η τιμή της f. Για να κατανοηθεί η μορφή ας θεωρήσουμε την Boolean συνάρτηση $f = x_1 + x_2 x_3$. Σύμφωνα με τους ερευνητές McWilliams και Sloane μία Boolean συνάρτηση που αναπαρίσταται με τον πίνακα αληθείας της μπορεί να γραφτεί και με την αλγεβρική κανονική μορφή της (F. J. MacWilliams, 1977).

x_1	x_2	x_3	$x_1 + x_2 x_3$
0	0	0	0
1	0	0	1
0	1	0	0
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	1

Πίνακας 2: Πίνακάς αληθείας της $f = x_1 + x_2x_3$.

Έστω μία Boolean συνάρτηση f που εξαρτάται από n μεταβλητές. Ένας άλλος τρόπος με τον οποίο μπορούμε να αναπαραστήσουμε την συνάρτηση αυτή, ο οποίος ονομάζεται Shannon's αναπαράσταση, για κάθε εισαγόμενη μεταβλητή x_i όπου $i = 1, \cdots, n$ ως ακολούθως:

$$f(x_1, \cdots, x_n) = (1 + x_i)f_0(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots x_n) + x_i f_1(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots x_n)$$

Όπου και οι δύο συναρτήσεις f_0, f_1 εξαρτώνται από $n - 1$ μεταβλητές.

Για να περιγράψουμε γενικά τις ιδιότητες και τη μορφή της Αλγεβρικής Κανονικής Μορφής οποιασδήποτε συνάρτησης, αρκεί να θεωρήσουμε το σύνολο $F_2 = \{0,1\}$ και η B_n να αποτελεί το σύνολο των Boolean συναρτήσεων με n μεταβλητές. Θεωρείται ότι $f \in B_n$ και ότι ισχύει $f : F_2^n \to F_2$. Για να εκφράσουμε την f θα χρησιμοποιήσουμε την αλγεβρική κανονική μορφή η οποία μπορεί να γραφεί, στη γενική της μορφή, ως εξής:

$$f(x_1, \cdots, x_n) = \sum_{i \in F_2^n} a_i \, x_1^{i_1} \cdots x_n^{i_n} \quad a_i \in F_2 \ (1)$$

Όπου στο άθροισμα (Σ) ουσιαστικά περιγράφει την XOR πρόσθεση. Κάθε όρος του πολυωνύμου διαθέτει έναν αριθμό από μεταβλητές. Η συνάρτηση αυτή θα πρέπει να ικανοποιεί τις ιδιότητες των LFSR και να έχει τις παρακάτω καλές κρυπτογραφικές ιδιότητες.

4.2.1 Αλγεβρικός Βαθμός (Algebraic degree)

Ο αλγεβρικός βαθμός της f (συμβολίζεται $\deg(f)$) είναι ο μέγιστος αριθμός από μεταβλητές που θα υπάρχει σε ένα όρο του πολυωνύμου με συντελεστή που δεν είναι μηδενικός (βλ. τη σχέση (1)). Όταν $\deg(f) = 1$ τότε η συνάρτηση είναι αφφινική (affine) και εάν η σταθερά της αλγεβρικής κανονικής μορφής της συνάρτησης είναι 0 τότε η f είναι γραμμική (linear). Ο βαθμός της λογικής συνάρτησης πρέπει να είναι μεγάλος στις κρυπτογραφικές λογικές συναρτήσεις. Για παράδειγμα, αν η λογική συνάρτηση χρησιμοποιείται για την παραγωγή κλειδοροής σε κρυπταλγόριθμο ροής, τότε ο υψηλός βαθμός είναι αναγκαίος για να επιτυγχάνεται υψηλή γραμμική πολυπλοκότητα. Σε

περίπτωση που αλγεβρικός βαθμός της συνάρτησης είναι χαμηλός, τότε η συνάρτηση διαφέρει από μία γραμμική συνάρτηση g σε πολύ λίγες θέσεις στον πίνακα αληθείας. Συνεπώς, στην περίπτωση – για παράδειγμα – των κρυπταλγορίθμων ροής, η κλειδοροή που θα προέκυπτε από τη λογική συνάρτηση g, η οποία έχει χαμηλότερη γραμμική πολυπλοκότητα από την f, διαφέρει σε λίγες θέσεις μόνο από την κλειδοροή της αρχικής συνάρτησης. Αυτού του είδους επιθέσεις ονομάζονται επιθέσεις προσεγγίσεων (approximation attacks). Αντίστοιχες επιθέσεις μπορούν να εφαρμοστούν και σε κρυπταλγορίθμους τμήματος.

Στην έρευνα (A. Canteaut, 2016) αποδεικνύεται ότι ο βαθμός της συνάρτησης επηρεάζει το βάρος (weight) αυτής. Αν υπάρχουν μόνο όροι με τον ίδιο αριθμό μεταβλητών τότε η συνάρτηση ονομάζεται ομοιογενής. Η συμπληρωματική συνάρτηση της f είναι η f' και προκύπτει από την εξίσωση $f' = f \oplus 1$. Η συμπληρωματική συνάρτηση έχει πάντα τον ίδιο βαθμό με την αρχική συνάρτηση.

Ακόμα μία καλή ιδιότητα, που επιθυμούν οι επιστημονικές ομάδες να έχουν οι Boolean συναρτήσεις που χρησιμοποιούνται στους κρυπτογραφικούς αλγορίθμους, είναι να μην μπορεί η συνάρτηση f να προσεγγιστεί από άλλη συνάρτηση με λιγότερες μεταβλητές. Για την συγκεκριμένη ιδιότητα δεν έχει εκτελεστεί εκτενής έρευνα. Έστω η g συνάρτηση, τότε μπορεί να υπολογιστεί η ελάχιστη απόσταση από μία συνάρτηση με λιγότερες μεταβλητές που προσεγγίζει την συνάρτηση f. Τότε η απόσταση $d_h(f, B_n(k))$ της f από το σύνολο $B_n(k)$ που περιέχει όλες τις συναρτήσεις που περιέχουν την k μεταβλητή ικανοποιεί την ακόλουθη σχέση:

$$d_h(f, B_n(k)) \geq 2^{n-1} \frac{\mathcal{L}(f)}{2} \left(\sum_{i=t+1}^{k} \binom{k}{i}^{\frac{1}{2}} \right)$$

4.2.2 Βάρος Συνάρτησης (Balancedness)

Το βάρος της συνάρτησης f (συμβολίζεται $wt(f)$) είναι ο αριθμός των μονάδων (“1”) που συναντάμε στον πίνακα αληθείας της. Για μία συνάρτηση να ονομάζεται ισορροπημένη (balanced) θα πρέπει $wt(f) = 2^{n-1}$. Οι ισορροπημένες συναρτήσεις είναι αυτές που χρησιμοποιούνται στα κρυπτογραφικά συστήματα καθώς παρέχουν καλές ιδιότητες τυχαιότητας σε σχέση με τις μη-ισορροπημένες(unbalanced) συναρτήσεις. Σύμφωνα με την έρευνα που έχει εκτελεστεί οι μη-ισορροπημένες συναρτήσεις δεν παρέχουν

ανθεκτικότητα στις επιθέσεις συσχετίσεων (correlation attack), με αποτέλεσμα να μην ικανοποιούν τα κριτήρια ασφάλειας ενός κρυπτογραφικού συστήματος. Στις επιθέσεις συσχετίσεων, ο επιτιθέμενος βασίζεται στην εξάρτηση της εξόδου (δηλαδή της κλειδοροής) της συνάρτησης από κάποιες συγκεκριμένες εισόδους της. Έτσι αν η έξοδος ταυτίζεται με πιθανότητα μεγαλύτερη του 50% με στοιχεία της εισόδου, τότε ο επιτιθέμενος αν βρει ένα ικανοποιητικά μεγάλο τμήμα της εξόδου μπορεί να βρει τμήμα του κλειδιού.

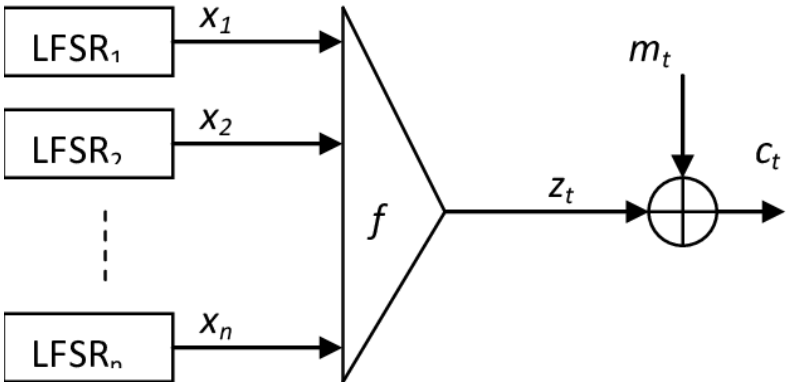
Σε σχέση με τις προαναφερθείσες επιθέσεις συσχετίσεων, υπάρχει ένα πιο αυστηρό κρυπτογραφικό κριτήριο. Συγκεκριμένα, η ανθεκτικότητα στην συσχέτιση (correlation immunity) είναι άλλη μία βασική ιδιότητα που πρέπει να διαθέτει η Boolean συνάρτηση προκειμένου να χρησιμοποιηθεί για κρυπτογραφικούς σκοπούς. Συγκεκριμένα, αν η συνάρτηση $f \in B_n$ είναι στατιστικά ανεξάρτητη από ένα υποσύνολο από k μεταβλητές $(1 \leq k \leq n)$, τότε η συνάρτηση είναι k τάξης ανθεκτική σε συσχετίσεις. Είναι ωστόσο γνωστό ότι όσο πιο πολύ υψηλή τιμή έχει το k σε μία k τάξης ανθεκτική σε συσχετίσεις συνάρτηση, τόσο μικρότερος είναι ο βαθμός της συνάρτησης: αυτό αποτελεί ένα χαρακτηριστικό παράδειγμα αντικρουόμενων κρυπτογραφικών κριτηρίων, καταδεικνύοντας τη δυσκολία του να ικανοποιούνται πλήρως όλα ταυτοχρόνως.

4.2.3 Μη γραμμικότητα (Non-linearity)

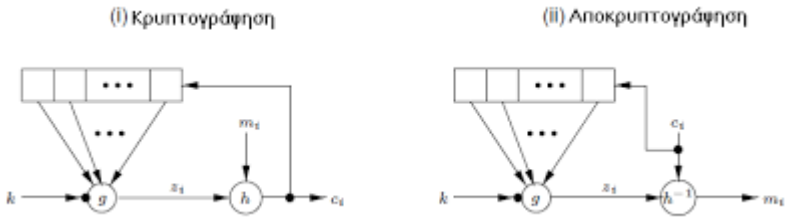
Οι LFSR, ενώ παρέχουν πολύ καλές στατιστικές ιδιότητες, είναι αδύναμοι όσων αφορά την ασφάλεια λόγω των αλγορίθμων Berlekamp-Massey και του Games – Chan. Για αυτό τον λόγο στην θέση τους μπορεί να χρησιμοποιηθεί μία μη γραμμική Boolean συνάρτηση για την παραγωγή της τυχαίας ακολουθίας. Η μη γραμμικότητα των Boolean συναρτήσεων επιτρέπουν στο κρυπτογραφικό σύστημα να είναι ανθεκτικό ως προς γραμμικές κρυπταναλυτικές επιθέσεις (M. Matsui, 1994) και τις καλύτερες γραμμικές προσεγγίσεις. (C. Ding, 1991) Για αυτό τον λόγο στα κρυπτογραφικά συστήματα (όχι μόνο σε κρυπταλγορίθμους ροής αλλά και σε κρυπταλγορίθμους τμήματος) χρησιμοποιούνται Boolean συναρτήσεις με υψηλή μη γραμμικότητα για την παραγωγή τυχαίων ακολουθιών ή για την αύξηση της μη γραμμικότητας του συστήματος σε επίπεδο που να το καθιστά ανθεκτικό στις κρυπταναλυτικές επιθέσεις.

Στην περίπτωση κρυπταλγορίθμων ροής, οι μη γραμμικές συνδυαστικές γεννήτριες και τα μη γραμμικά φίλτρα γεννητριών είναι τέτοια συστήματα που μπορούν να

χρησιμοποιηθούν οι Boolean συναρτήσεις. Στις μη γραμμικές συνδυαστικές γεννήτριες είναι n-LFSRs οι οποίες παράγουν τυχαίες ακολουθίες. Οι ακολουθίες εισέρχονται σε μία μη γραμμική Boolean συνάρτηση βαθμού n, της οποίας το αποτέλεσμα παράγει την κλειδοροή που θα χρησιμοποιηθεί για την κρυπτογράφηση. Στα μη γραμμικά φίλτρα γεννητριών ένας LFSR μεγέθους N και i σταδίων παράγει μία ακολουθία η οποία φιλτράρεται από την μη γραμμική συνάρτηση για να παραχθεί η κλειδοροή (T. W. Cusick, 2017).



Εικόνα 16: Μη γραμμική συνδυαστική γεννήτρια



Εικόνα 17: Μη γραμμικό φίλτρο γεννήτριας

Η απόσταση μεταξύ δύο συναρτήσεων είναι ο αριθμός των διαφόρων που έχουν στον πίνακα αληθείας του και συμβολίζονται ως εξής:

$$d(f, g) = wt(f \oplus g)$$

Η μη γραμμικότητα (nonlinearity) μίας συνάρτησης ισούται με τη μικρότερη απόσταση αυτής από κάποια γραμμική (ή αφφινική) συνάρτηση.

Για παράδειγμα, ας δούμε πάλι το Σχήμα 16. Η γεννήτρια f είναι μη γραμμική, προκειμένου να επιτυγχάνεται υψηλή γραμμική πολυπλοκότητα στην παραγόμενη

κλειδοροή. Αν όμως η f, αν και μη γραμμική, έχει χαμηλή μη γραμμικότητα (δηλαδή με λίγες τροποποιήσεις στον πίνακα αληθείας της μπορεί να γίνει γραμμική), τότε η κλειδοροή που παράγεται «μοιάζει πολύ» με μία ακολουθία χαμηλής γραμμικής πολυπλοκότητας και, άρα, καθίσταται προβλέψιμη!

4.2.4 Ανθεκτικότητα σε Αλγεβρικές Επιθέσεις(Algebraic immunity)

Πολλοί κρυπτογραφικοί αλγόριθμοι που έφεραν καλές κρυπτογραφικές ιδιότητες, όπως αυτές που περιεγράφηκαν στις παραπάνω ενότητες, ανακαλύφθηκε από τον Courtois το 2003 ότι μπορεί να είναι αδύναμες σε αλγεβρικές επιθέσεις. Αυτές εφαρμόστηκαν αρχικά σε κρυπτογραφικά συστήματα όπου στις γεννήτριες κλειδοροής υπεισέρχονται LFSRS. Κατά αυτόν τον τρόπο μία συνδυαστική μη γραμμική συνάρτηση που έχει υψηλό βαθμό, υψηλή μη γραμμικότητα και είναι ανθεκτική σε επιθέσεις συσχετίσεων δεν είναι απαραίτητα καλή για χρήση σε κρυπτογραφικά συστήματα, αν δεν έχει ελεγχθεί η ανθεκτικότητά της σε αλγεβρικές επιθέσεις.

Αποδεικνύεται ότι η λογική συνάρτηση f είναι ανθεκτική σε αλγεβρικές επιθέσεις αν δεν υπάρχει μία συνάρτηση g χαμηλού βαθμού τέτοια ώστε:

$$f * g = 0 \text{ ή } f' * g = 0$$

Όπου * δηλώνεται ο πολλαπλασιασμός μεταξύ των συναρτήσεων. Ο βαθμός της g (εκτός της μηδενικής συνάρτησης) που επαληθεύει την παραπάνω εξίσωση καθορίζει και την αλγεβρική ανθεκτικότητα της συνάρτησης f. Ο στόχος των μοντέρνων κρυπτογραφικών συστημάτων που χρησιμοποιούν λογικές συναρτήσεις είναι η σχεδίαση αυτών των συναρτήσεων με υψηλό βαθμό συνάρτησης, υψηλή μη γραμμικότητα, υψηλή ανθεκτικότητα σε επιθέσεις συσχετίσεων και υψηλή ανθεκτικότητα σε αλγεβρικές επιθέσεις.

4.2.5 Ειδικοί τύποι Λογικών Συναρτήσεων

Για μία Boolean συνάρτηση να ονομασθεί συμμετρική θα πρέπει η έξοδος της να εξαρτάται μόνο από το βάρος της εισόδου της. Αυτό σημαίνει ότι οποιαδήποτε αλλαγή στα bits της εισόδου δεν θα οδηγήσει στην αλλαγή της αξίας της συνάρτησης. Οι κρυπτογραφικές ιδιότητες των συμμετρικών συναρτήσεων περιγράφονται από τους Canteaut και τον Videau στην (A. Canteaut, 2005).

Άλλη μία ειδική κατηγορία Boolean συναρτήσεων είναι η bent συνάρτηση (O. S. Rothaus, 1976). Το ιδιαίτερο χαρακτηριστικό της συγκεκριμένης κατηγορίας συναρτήσεων είναι ότι έχουν την μέγιστη διαφορά από όλες τις γραμμικές συναρτήσεις, οπότε επιτυγχάνουν την μέγιστη μη γραμμικότητα. Αυτή η ιδιότητα είναι ιδιαίτερα σημαντική στην κρυπτογραφία για αυτό τον λόγο μελετιούνται εκτενώς και χρησιμοποιούνται αρκετά συχνά στους σύγχρονους αλγόριθμους (N. Tokareva, 2015). Βέβαια έχουν και κάποια βασικά μειονεκτήματα, όπως ότι η συνάρτηση για να είναι αυτής της κατηγορίας πρέπει να έχει άρτιο αριθμό μεταβλητών και δεν είναι ισορροπημένες συναρτήσεις(non-balanced).

4.2.6 Διανυσματικές Λογικές Συναρτήσεις

Οι διανυσματικές (vectorial) λογικές συναρτήσεις έχουν τεράστια σημασία για την επιστήμη της κρυπτογραφίας, επειδή τέτοιες συναρτήσεις ουσιαστικά υλοποιούν τις μονάδες αντικατάστασης (S-Box) των αλγορίθμων τμήματος. Για τον λόγο αυτό εκτελούνται εκτενείς μελέτες για τις ιδιότητες των συγκεκριμένων συναρτήσεων αλλά και του πόσου αυτές οι ιδιότητες μπορεί να είναι καλές για κρυπτογραφική χρήση. Στην ουσία μία συνάρτηση $f: F_2^n \to F_2^m$ ονομάζεται vectorial Boolean συνάρτηση, δηλαδή πρόκειται για λογικές συναρτήσεις με περισσότερες από μία εξόδους.

Οι κρυπτογραφικές ιδιότητες που θα πρέπει να πληρούν οι διανυσματικές συναρτήσεις είναι στενά συνυφασμένες με αυτές των λογικών συναρτήσεων. Ουσιαστικά, μία διανυσματική συνάρτηση m εξόδων περιγράφει μονοσήμαντα 2^m λογικές συναρτήσεις και, κατ' ουσίαν, είναι επιθυμητό – αν και σχεδιαστικά δύσκολο – κάθε μία εξ αυτών να έχει καλές κρυπτογραφικές ιδιότητες, όπως αυτές που περιγράφηκαν ανωτέρω. Παρόλο που, ακόμα και αν η μη εκπλήρωση κάποιων εκ των κριτηρίων για κάποιες εξ αυτών των 2^m συναρτήσεων δεν συνεπάγεται αυτόματα τη δυνατότητα πραγματοποίησης επιτυχούς κρυπταναλυτικής επίθεσης, μία τέτοια περίπτωση θεωρείται, κατ' αρχάς, από την ερευνητική σκοπιά, δυνητική ευπάθεια.

4.2.6.1 Άλλες ιδιότητες των Διανυσματικών Λογικών Συναρτήσεων

Υπάρχουν και συγκεκριμένα κρυπτογραφικά κριτήρια τα οποία χαρακτηρίζουν αποκλειστικά τις διανυσματικές συναρτήσεις. Ένα εξ αυτών είναι το κριτήριο της αυστηρής χιονοστιβάδας (Strict Avalanche Criterion-SAC).. Χρησιμοποιήθηκε πρώτη

φορά από τους ερευνητές Webster και Tavares σε μία έρευνα που είχαν κάνει για τον σχεδιασμό των S-boxes στους αλγορίθμους τμήματος (F. Webster, 1986). Συγκεκριμένα έστω μία διανυσματική Boolean συνάρτηση $f(x)$ με n μεταβλητές εισόδου και m μεταβλητές εξόδου, η οποία ικανοποιεί την ιδιότητα του SAC (συνήθως ισχύει n=m, αλλά δεν είναι απαραίτητο). Αυτό σημαίνει ότι με την αλλαγή ενός οποιουδήποτε bit οποιασδήποτε εισόδου, στην έξοδο της συνάρτησης θα έχει σε αποτέλεσμα την αλλαγή των ακριβώς μισών 2^{m-1} από τις εξόδων της συνάρτησης. Όπως έχει μελετηθεί στην (Babbage, 1990) ότι η ιδιότητα αυτή χρησιμοποιείται σε πολλά κρυπτογραφικά συστήματα. Χρησιμοποιείται ευρέως, καθώς η είσοδος σε μια διανυσματική Boolean συνάρτηση δεν μπορεί να συσχετισθεί από την έξοδο της συνάρτησης αυτής.

4.3 Σχέση Μεταξύ Δυαδικών Ακολουθιών και Boolean Συναρτήσεων

Όπως αποδεικνύεται από διάφορες μελέτες (A. M. Youssef, 2001) ότι υπάρχει μία «ένα-προς-ένα» συσχέτιση μίας δυαδικής ακολουθίας με περίοδο 2^n και μίας Boolean συνάρτησης με n μεταβλητές. Όμως υπάρχει μία διαφορετική προσέγγιση σε μία πρόσφατη μελέτη, που μπορεί να οδηγήσει σε κάποια επιθυμητά αποτελέσματα (K. Limniotis, 2019).

Κατά την εφαρμογή της παραπάνω ιδιότητας, αν θεωρήσουμε την ακολουθία $s = (s_1, \cdots, s_{2^n})$ με περίοδο 2^n , τότε αυτή μπορεί να αντιστοιχηθεί μονοσήμαντα σε μία Boolean συνάρτηση f με n μεταβλητές, της οποίας ο πίνακας αληθείας είναι $s_f = (s_1, \cdots, s_{2^n})$. Έτσι για κάθε $f \in B_n$ με n μεταβλητές υπάρχει μία περιοδική ακολουθία s με περίοδο 2^n τέτοια ώστε $s \leftrightarrow f_s$ και αντίστροφα (το σύμβολο $\leftrightarrow$. εκφράζει ακριβώς αυτήν την αντιστοίχιση, και για αυτό συμβολίζουμε με f_s τη συνάρτηση f η οποία σχετίζεται με την s με τον τρόπο που περιγράψαμε). Σύμφωνα με αυτό τον ορισμό, ο αλγόριθμος των Lauder-Paterson (LPA) για τον υπολογισμό του CELCS της ακολουθίας s μας δίνει πληροφορίες για μία συγκεκριμένη κρυπτογραφική ιδιότητα της αντίστοιχης λογικής συνάρτησης f_s.

4.3.1 Υπολογισμός της Προσεγγιστικής Συνάρτησης

Σύμφωνα με την μελέτη (K. Limniotis, 2019) για μία δυαδική ακολουθία s με γραμμική πολυπλοκότητα $c(s)$, όπου $2^{n-l-1} < c(s) \leq 2^{n-l}$ με το l να ανήκει $1 \leq l < n-1$, η

αντίστοιχηBoolean συνάρτηση με n μεταβλητές, σύμφωνα με τον ορισμό της αντιστοίχισης που περιγράφηκε ανωτέρω, εξαρτάται μόνο από τις $n-l$ μεταβλητές. Κατά αυτόν τον τρόπο δημιουργείται μία συσχέτιση μεταξύ της γραμμικής πολυπλοκότητας της δυαδικής ακολουθίας με τον αριθμό των μεταβλητών της αντίστοιχης Boolean συνάρτησης. Για αυτό τον λόγο αν η γραμμική πολυπλοκότητα της δυαδικής ακολουθίας μειωθεί αρκετά, τότε ο αριθμός των μεταβλητών της Boolean συνάρτησης θα μειωθεί και αυτός αντίστοιχα. Συμπερασματικά η μείωση της γραμμικής πολυπλοκότητας μας οδηγεί στον υπολογισμό προσεγγιστικών συναρτήσεων της αρχικής συνάρτησης, οι οποίες προσεγγιστικές συναρτήσεις έχουν λιγότερες μεταβλητές. Αυτό αποτελεί ένα σημαντικό κρυπτογραφικό κριτήριο αφού δεν είναι επιθυμητό, για μία κρυπτογραφική λογική συνάρτηση, να μπορεί να προσεγγιστεί ικανοποιητικά από άλλη συνάρτηση με μικρότερο πλήθος μεταβλητών.

Ο υπολογισμός της παραπάνω συνάρτησης που προσεγγίζει την Boolean συνάρτηση με λιγότερες μεταβλητές σχετίζεται με τις λεγόμενες επιθέσεις συσχέτισης (correlation attacks).. Η Canteaut κατέδειξε με ποιον τρόπο μπορούν να χρησιμοποιηθούν οι προσεγγιστικές συναρτήσεις στην κρυπτανάλυση (A. Canteaut, 2002).

Συνεπώς, σύμφωνα με το πρόσφατο ερευνητικό αποτέλεσμα στο (K. Limniotis, 2019), ο LPA αλγόριθμος είναι ακόμη ένας αλγόριθμος, ο οποίος μπορεί να οδηγήσει στην εύρεση προσεγγιστικής συνάρτησης με λιγότερες μεταβλητές, καθώς βρίσκει το ELCS της ακολουθίας και τα σημεία εκείνα που η γραμμική πολυπλοκότητα της ακολουθίας μειώνεται. Πιο συγκεκριμένα αν θεωρήσουμε την δυαδική ακολουθία s με περίοδο 2^n, η οποία διαθέτει τα κρίσιμα σημεία $(k, c(s))$. Ακόμα ικανοποιείται η σχέση $2^{n-l-1} < c(s) \leq 2^{n-l}$ όπου $l \geq 1$ και υπάρχει μία Boolean συνάρτηση για την οποία $s_f \leftrightarrow s$. Τότε σύμφωνα με την (K. Limniotis, 2019) υπάρχει συνάρτηση h η οποία μπορεί έχει παραχθεί από την ακολουθία $s_f \oplus \mathcal{E}$ που εξαρτάται από τις πρώτες $n-l$ μεταβλητές και δεν υπάρχει κάποια άλλη ακολουθία για την οποία να ισχύει $wt < k$, που θα μπορούσε να παραχθεί από αυτή την ιδιότητα κάποια συνάρτηση που να εξαρτάται από λιγότερες μεταβλητές (όπου $\mathcal{E}$ η ακολουθία σφάλματος – δηλαδή η ακολουθία που «περιγράφει» σε ποιες θέσεις θα πρέπει να μεταβληθεί η s_f).

Τέλος, πρέπει να επισημανθεί το εξής. Όπως περιγράφεται και στο (K. Limniotis, 2019), αν μετασχηματίσουμε μία λογική συνάρτηση σε μία «ισοδύναμή» της μέσω

αντιμετάθεσης των μεταβλητών της, ενδεχομένως ο LPA να δώσει ακόμα καλύτερα αποτελέσματα σε κάποια ισοδύναμη εκδοχή της αρχικής συνάρτησης. Αυτό καθιστά, για μεγάλες τιμές του n, μη αποδοτικό τον πλήρη έλεγχο, για όλες τις ισοδύναμες συναρτήσεις, του αποτελέσματος της εφαρμογής του LPA αφού, το σύνολο όλων των πιθανών αντιμεταθέσεων των μεταβλητών, είναι n!.

Για την περιγραφή της Hamming απόστασης μεταξύ δύο Λογικών συναρτήσεων f,g χρησιμοποιείται μία ποσότητα ϵ, που ονομάζεται bias, και δίνεται από τον τύπο:

$$\epsilon = \left| p\big(f(x) = g(x)\big) - \frac{1}{2} \right|$$

Κεφάλαιο 5
Ασφάλεια Lightweight Αλγορίθμων-Μελέτη Περίπτωσης

Η αναγκαιότητα για την δημιουργία ενός νέου προτύπου lightweight κρυπτογραφικού αλγορίθμου προέκυψε λόγω της φύσης των συσκευών που χρησιμοποιούνται ιδίως στο δίκτυο του IoT. Ο AES, το σημερινό πρότυπο συμμετρικής κρυπτογράφησης, παρόλο που θεωρείται αποδοτικός αλγόριθμος και ικανός να υλοποιηθεί σε διάφορα περιβάλλοντα που έχουν περιορισμούς, δεν είναι lightweight αλγόριθμος και δεν ανταποκρίνεται στις σχετικές απαιτήσεις. Ένας πρότυπος lightweight αλγόριθμος θα πρέπει να έχει μειωμένο μέγεθος, άρα και απαιτήσεις επεξεργαστικής ισχύος και μνήμης (μικρότερη RAM/ROM). Να έχει μειωμένες απαιτήσεις σε ενέργεια , καθώς οι συσκευές αυτές έχουν περιορισμό σε ενεργειακή αυτονομία λόγω του μεγέθους και των λειτουργιών που έχουν. Για παράδειγμα τα RFID έχουν αρκετές ενεργειακές ανάγκες προκειμένου να ολοκληρώσουν σωστά την λειτουργία τους. Για αυτό τον λόγο η lightweight κρυπτογραφία απαιτεί την υιοθετήσει μία μέθοδος, που μπορεί να έχει υψηλή ασφάλεια, ακόμα και εάν έχουν μειωμένο μέγεθος κλειδιού από την κρυπτογραφία (T. Suzaki, 2012).

Ο NIST, όπως είχε πράξει και με την επιλογή του AES, έχει εκκινήσει διαγωνισμός για την εύρεση ενός προτύπου κρυπτογραφικού lightweight αλγορίθμου. Ο διαγωνισμός ξεκίνησε τον Αύγουστο του 2016 με τον προσδιορισμό από τον NIST των χαρακτηριστικών, που θα πρέπει να έχουν οι αλγόριθμοι που θα συμμετάσχουν σε αυτόν. Η έναρξη των συμμετοχών ξεκίνησε το 2017, όπου 56 συμμετέχοντες συμμετείχαν στον πρώτο γύρο. Από αυτούς στον δεύτερο γύρο πέρασαν 32 υποψήφιοι τον Αύγουστο του 2019.

5.1 Επισκόπηση Υποψήφιων “Lightweight” Κρυπτογραφικών αλγορίθμων

Στο συγκεκριμένο κεφάλαιο θα παρουσιαστούν συνοπτικά οι “lightweight” κρυπτογραφικοί αλγόριθμοι, οι οποίοι έχουν επιτύχει να είναι στο δεύτερο γύρο του διαγωνισμού του οργανισμού National Institute of Standards and Technology (NIST). Στο πλαίσιο της διατριβής πραγματοποιείται μία ταξινόμηση αυτών όπως φαίνεται στον παρακάτω πίνακα 2, αναδεικνύοντας στοιχεία όπως τα προτεινόμενα από τους ερευνητές μεγέθη του μυστικού κλειδιού K, την ποσότητα nonce (ποσότητα IV με την οποία αποφεύγεται η μείωση της ανθεκτικότητας του αλγορίθμου όταν χρησιμοποιηθεί το ίδιο μυστικό κλειδί για το ίδιο κείμενο), τα μεταδεδομένα AD (σχετικά δεδομένα που συνοδεύουν το μήνυμα), το μήνυμα το ίδιο M, το κρυπτογραφημένο μήνυμα C και την ετικέτα αυθεντικοποίησης T (NIST). Η ετικέτα αυθεντικοποίησης είναι ουσιαστικά πληροφορία που παράγεται προκειμένου, πέραν της εμπιστευτικότητας, να διασφαλίζεται και η ακεραιότητα (αυθεντικοποίηση) του μηνύματος. Τέτοιοι αλγόριθμοι ονομάζονται αυθεντικοποιημένοι αλγόριθμοι κρυπτογράφησης (Authenticated Encryption with Associated Data – AEAD).

Αλγόριθμος	είδος	K	Nonce	AD	T	AEAD	Hash	Hash size
ACE	hybrid	128	128	128	128	√	√	256
ASCON	block	128	128	ND	128	√	√	256
COMET	block	128	128	ND	128	√	-	-
DryGASCON	block	128	128	128	128	√	√	128
ELEPHANT	linear	128	160	ND	64	√	-	-
ESTATE	block	128	128	ND	128	√	-	-
ForkAE	block	128	104	ND	128	√	-	-
GIFT	block	128	128	ND	128	√	-	-
GIMLI	block	256	128	ND	128	√	√	256
GRAIN	block	128	96	ND	-	√	-	-
Hyena	hybrid	128	96	ND	128	√	-	-
ISAP	block	128	128	144	128	√	-	-
KNOT	block	128	64	ND	192	√	√	256

Lotus-Locus	block	128	128	ND	64	√	-	-
MixFeed	block	128	120	ND	128	√	-	-
Orange	block	128	128	ND	128	√	√	256
Oribatida	block	128	128	ND	128	√	-	-
Photon	block	128	128	ND	128	√	√	256
Pyjamask	block	128	128	96	128	√	-	-
Romulus	block	128	96	256	64	√	-	-
SAEAES	block	128	120	64	64	√	-	-
Saturnin	block	256	Up to 160	ND	Up to 256	√	√	256
SKINNY	block	128	128	ND	128	√	√	128
Sparkle	block	128	256	ND	128	√	√	128
Spix	block	128	128	60	128	√	-	-
Spoc	block	128	128	ND	64	√	-	-
Spook	block	128	256	ND	128	√	-	-
Subterranean	block	128	128	ND	128	√	√	256
SUNDAE-GIFT	block	128	96	ND	128	√	-	-
TinyJAMBU	block	128	96	ND	64	√	-	-
Wage	block	128	128	64	128	√	-	-
Xoodyak	block	128	128	ND	128	√	√	128

Πίνακας 3: Επισκόπηση αλγορίθμων του δεύτερου γύρου του διαγωνισμού του NIST (μεγέθη σε bits)

**ND=No-Defined δεν γίνεται ακριβής ορισμός της ποσότητας των σχετικών δεδομένων, καθώς σχετίζονται με το μέγεθος του κειμένου που είναι αποδεκτό από τον αλγόριθμο*

5.2 Έλεγχος ασφάλειας - Επιλογή αλγορίθμου

Η παρούσα διατριβή αποσκοπεί στη μελέτη ασφάλειας lightweight αλγορίθμων, εξετάζοντας τις κρυπτογραφικές ιδιότητες των υποκείμενων λογικών συναρτήσεων. Κατόπιν της εξέτασης όλων των αλγορίθμων του ανωτέρω Πίνακα 2, ο αλγόριθμος που επιλέχθηκε για τον έλεγχο ασφαλείας της παρούσας διατριβής είναι ο SKINNY-AEAD. Επισημαίνεται ότι είναι πολλοί λίγοι οι αλγόριθμοι οι οποίοι, στις προδιαγραφές τους, χρησιμοποιούν μία λογική συνάρτηση, ενώ εξ αυτών μόνο ο SKINNY χρησιμοποιεί S-box (δηλαδή διανυσματική συνάρτηση) – οπότε και η επιλογή μας κατευθύνθηκε από αυτά

τα δεδομένα. Ο αλγόριθμος SKINNY είναι ένας ασφαλής tweakable αλγόριθμος τμήματος επιτυγχάνοντας την ασφάλειά του προστατεύοντας την nonce ποσότητα. Η βασική έκδοση του αλγορίθμου έχει 128 bits κλειδιού, 128 bits nonce και μία ποσότητα σχετιζόμενων δεδομένων μαζί με το μήνυμα να έχει μέγεθος έως $2^{64} * 16$ bytes. Στην έξοδο του αλγορίθμου παράγεται το κρυπτογραφημένο κείμενο C με μέγεθος όσο αυτό του αρχικού μηνύματος και μία ετικέτα αυθεντικοποίησης T με μέγεθος 128 bits.

Ο αλγόριθμος έχει σχεδιαστεί σαν ένα Substitution-Permutation δίκτυο (δίκτυο αντικατάστασης-αντιμετάθεσης ή SPN), το οποίο έχει καλές ιδιότητες ασφαλείας έναντι των περισσότερων κρυπταναλυτικών προσεγγίσεων. Ο αλγόριθμος μπορεί να προσομοιαστεί ως ένας τροποποιημένος AES, ο οποίος όμως απλοποιεί πολλές διαδικασίες που εκτελούνται στον AES χωρίς ωστόσο να θυσιάζονται ιδιότητες για την ασφάλεια του αλγορίθμου. Για αυτό τον λόγο θεωρείται ότι ο αλγόριθμος έχει ελεγχθεί για πολλές κρυπταναλυτικές προσεγγίσεις (καθιστώντας έτσι ιδιαίτερα σημαντική την εκ νέου εξέταση της ασφάλειάς του, υπό διαφορετική οπτική, που πραγματοποιείται στο πλαίσιο της παρούσας διατριβής). Ο SKINNY-128-384 εκτελεί 29 γύρους και ο SKINNY-128-256 εκτελεί 25 γύρους.

Ο αλγόριθμος μπορεί να χρησιμοποιηθεί με την χρήση διαφόρων παραμέτρων διατηρώντας τα καλά του χαρακτηριστικά, αλλά και τις ελάχιστες απαιτήσεις ενός λίγο παλαιότερου διαγωνισμού, με το όνομα CAESAR [1], για την εύρεση ισχυρών αυθεντικοποιημένων κρυπτογραφικών αλγορίθων. Οι πιθανές εκδόσεις φαίνονται στον παρακάτω πίνακα 3, όπου είναι ιεραρχικά τοποθετημένες (η προτιμότερη έκδοση πρώτη, η αμέσως επόμενη προτιμότερη δεύτερη και ούτω καθεξής).

Έκδοση	Όνομα	Nonce	Tag	Key	Hash	Rate	Capacity
M1	SKINNY-128-384	128	128	128	384-bit sponge	128	256
M2	SKINNY-128-384	96	128	128			
M3	SKINNY-128-384	128	64	128			
M4	SKINNY-128-384	96	64	128			

Πίνακας 4: Εκδόσεις σε bits για τον αλγόριθμο SKINNY

[1] Βλ. σχετικώς το σύνδεσμο https://competitions.cr.yp.to/caesar.html (τελευταία πρόσβαση: 12 Απριλίου 2020)

Αντικείμενο του ελέγχου ως προς την ασφάλεια, στο πλαίσιο της παρούσας διατριβής, θα τεθεί το S-box S_8. Είναι S-box των 8 bits που εφαρμόζεται σε όλα τα κελιά του κρυπταλγορίθμου. Το κατασκευαστικό του σχέδιο έχει εμπνευστεί από τα PICCOLO S-box (Piccolo: An ultralightweight ultralightweight, 2011). Αν οι μεταβλητές $x_0, \cdots, x_7$ αναπαριστούν τις 8 εισόδους του S-box (με το x_0 να είναι η μικρότερης σημασίας μεταβλητή) εφαρμόζεται η εξής αλλαγές:

$$(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) \rightarrow \left(x_7, x_6, x_5, x_4 \oplus (\overline{x_7 \vee x_6}), x_3, x_2, x_1, x_0 \oplus (\overline{x_3 \vee x_2})\right)$$

Ακολουθούμενη με την παρακάτω ανακατάταξη:

$$(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) \rightarrow (x_2, x_1, x_7, x_6, x_4, x_0, x_3, x_5)$$

Οι παραπάνω διαδικασίες ακολουθούνται τέσσερις φορές, εκτός από την τελευταία φορά που γίνεται μία αλλαγή μεταξύ του x_1 και του x_2. Τα πιθανά αποτελέσματα από τις 256 πιθανές εισόδου (2^8) προκύπτουν όπως φαίνεται στον πίνακα του παραρτήματος Α σε δεκαεξαδική μορφή (C. Beierle, 2019). Οι ερευνητές αναφέρουν ότι ο μέγιστος παραγόμενος βαθμός είναι 6 (κάτι που επιβεβαιώθηκε και στο πειραματικό σκέλος της παρούσας διατριβής στη συνέχεια), οπότε έκριναν ότι δεν είναι ευάλωτος από αλγεβρικές επιθέσεις. Δεν γίνεται ωστόσο αναφορά σε άλλες κρυπτογραφικές ιδιότητες.

5.3 Ανάλυση κρυπτογραφικών ιδιοτήτων του S-box του SKINNY

Με την χρήση του παραρτήματος που παρουσιάζεται στην (C. Beierle, 2019) έχουμε τα πιθανά αποτελέσματα για κάθε συνδυασμό των μεταβλητών εισόδου του S-Box. Τα αποτελέσματα αυτά είναι σε δεκαεξαδική μορφή από τους ερευνητές. Η θεώρηση που γίνεται είναι ότι η κύρια μεταβλητή είναι αυτή που μεταβάλλεται ανά γραμμή. Το παραπάνω παράρτημα φαίνεται στο Παράρτημα Α.1. Κάθε δεκαεξαδικό ψηφίο αναπαρίσταται από 4 bits δυαδικής ακολουθίας. Με την χρήση του Παραρτήματος Α.2 εκτελέστηκε η αναπαράσταση της εξόδου του S-Box σε δυαδική ακολουθία. Για τον έλεγχο των κρυπτογραφικών ιδιοτήτων ελέγχθηκαν η κάθε δυαδική ακολουθία αλλά και κάθε δυνατός συνδυασμός μεταξύ των συναρτήσεων ($2^8 = 256$ συνδυασμοί). Αυτό επετεύχθη κατόπιν ειδικής προς τούτο αλγοριθμικής υλοποίησης που αναπτύχθηκε στο

πλαίσιο της διατριβής. Οι αρχικές συναρτήσεις που προκύπτουν στην έξοδο του S-Box είναι:

Α/Α	**Ονομασία Συνάρτησης**	**Αλγεβρική Κανονική Μορφή**
1	b1	$x0 * x4 + x0 * x6 * x7 + x0 * x6 + x0 * x7 + x2 * x3 * x4 + x2 * x3 * x6 * x7 + x2 * x3 * x6 + x2 * x3 * x7 + x2 * x4 + x2 * x6 * x7 + x2 * x6 + x2 * x7 + x3 * x4 + x3 * x6 * x7 + x3 * x6 + x3 * x7 + x5$
2	b2	$x4 + x6 * x7 + x6 + x7 + 1$
3	b3	$x0 + x2 * x3 + x2 + x3 + 1$
4	b4	$x0 * x4 + x0 * x6 * x7 + x0 * x6 + x0 * x7 + x2 * x3 * x4 + x2 * x3 * x6 * x7 + x2 * x3 * x6 + x2 * x3 * x7 + x2 * x4 + x2 * x6 * x7 + x2 * x6 + x2 * x7 + x3 * x4 + x3 * x6 * x7 + x3 * x6 + x3 * x7 + x3 + x4 * x5 + x4 + x5 * x6 * x7 + x5 * x6 + x5 * x7 + x6 * x7 + x6 + x7$
5	b5	$x0 * x3 + x0 + x1 + x2 * x3 + x2$
6	b6	$x1 * x2 + x1 + x2 + x6 + 1$
7	b7	$x0 * x1 * x2 * x4 + x0 * x1 * x2 * x6 * x7 + x0 * x1 * x2 * x6 + x0 * x1 * x2 * x7 + x0 * x1 * x4 + x0 * x1 * x6 * x7 + x0 * x1 * x6 + x0 * x1 * x7 + x0 * x2 * x4 + x0 * x2 * x6 * x7 + x0 * x2 * x6 + x0 * x2 * x7 + x0 * x4 * x6 + x0 * x6 + x1 * x2 * x3 * x4 + x1 * x2 * x3 * x6 * x7 + x1 * x2 * x3 * x6 + x1 * x2 * x3 * x7 + x1 * x2 * x5 + x1 * x2 + x1 * x3 * x4 + x1 * x3 * x6 * x7 + x1 * x3 * x6 + x1 * x3 * x7 + x1 * x5 + x1 + x2 * x3 * x4 * x6 + x2 * x3 * x6 + x2 * x4 * x6 + x2 * x4 + x2 * x5 + x2 * x6 * x7 + x2 * x7 + x2 + x3 * x4 * x6 + x3 * x6 + x5 * x6 + x6 + x7$

8	b8	$x0 * x1 * x2 * x3 * x4 + x0 * x1 * x2 * x3 * x5 + x0 * x1 * x2 * x3 * x6 * x7 + x0 * x1 * x2 * x3 * x6 + x0 * x1 * x2 * x3 * x7 + x0 * x1 * x2 * x3 + x0 * x1 * x2 * x5 + x0 * x1 * x2 + x0 * x1 * x3 * x4 + x0 * x1 * x3 * x5 + x0 * x1 * x3 * x6 * x7 + x0 * x1 * x3 * x6 + x0 * x1 * x3 * x7 + x0 * x1 * x3 + x0 * x1 * x4 * x6 + x0 * x1 * x4 + x0 * x1 * x5 + x0 * x1 * x6 * x7 + x0 * x1 * x7 + x0 * x1 + x0 * x2 * x3 * x4 + x0 * x2 * x3 * x5 + x0 * x2 * x3 * x6 * x7 + x0 * x2 * x3 * x6 + x0 * x2 * x3 * x7 + x0 * x2 * x3 + x0 * x2 * x5 + x0 * x2 + x0 * x3 * x4 * x6 + x0 * x3 * x5 * x6 + x0 * x3 * x7 + x0 * x3 + x0 * x5 * x6 + x0 * x6 + x0 * x7 + x0 + x1 * x2 * x3 * x4 * x6 + x1 * x2 * x3 * x6 + x1 * x2 * x4 * x6 + x1 * x2 * x4 + x1 * x2 * x5 + x1 * x2 * x6 * x7 + x1 * x2 * x7 + x1 * x2 + x1 * x3 * x4 * x6 + x1 * x3 * x6 + x1 * x5 * x6 + x1 * x6 + x1 * x7 + x1 + x2 * x3 * x4 + x2 * x3 * x5 * x6 + x2 * x3 * x5 + x2 * x3 * x6 * x7 + x2 * x5 * x6 + x2 * x6 + x2 * x7 + x3 * x4 * x6 + x3 * x6 + x5 * x6 + x6 + x7 + 1$

Πίνακας 5: Πίνακας βασικών συναρτήσεων στην έξοδο του S-Box

Οι κρυπτογραφικές ιδιότητες που λαμβάνονται υπόψη είναι ο βαθμός της κάθε συνάρτησης, η αλγεβρική ανθεκτικότητα και η μη γραμμικότητα όπως αυτά περιγράφονται στο Κεφάλαιο 4. Στο παράρτημα Α.3 αναδεικνύονται οι πιθανές συναρτήσεις που προκύπτουν από τους συνδυασμούς και η ονομασία τους.

5.3.1 Εργαλείο Ανάλυσης Λογικών Συναρτήσεων

Το εργαλείο που χρησιμοποιήθηκε για την ανάλυση των ιδιοτήτων που παρουσιάζουν οι παραπάνω συναρτήσεις, όπως και η παραγωγή των πιθανών συνδυασμών είναι το Sagemath. Το εργαλείο αυτό είναι ανοιχτού κώδικα και βασίζεται στην γλώσσα

προγραμματισμού Python και αποτελεί μία δωρεάν εναλλακτικών εφαρμογών, όπως το MATLAB και το Mathematica. Στην μεταπτυχιακή διατριβή χρησιμοποιήθηκε η online μορφή του εργαλείου μέσα από ηλεκτρονικό υπολογιστή με λειτουργικό σύστημα Windows 10 με όλα τις τρέχουσες ενημερώσεις κατά την εκπόνηση της μεταπτυχιακής διατριβής (https://www.cocalc.com/).

Ο William Stein είναι ο προγραμματιστής που δημιούργησε το Sage. Το Sage είναι μία γλώσσα προγραμματισμού που περιλαμβάνει διάφορα πακέτα από μαθηματικές εκφράσεις. Η αρχική κυκλοφορία του εργαλείου πραγματοποιήθηκε το 2005 και η ανάπτυξή του, καθώς και η διόρθωση των διαφόρων σφαλμάτων γίνεται από τους ίδιους τους χρήστες του (Sagemath, 2020).

Το συγκεκριμένο εργαλείο περιέχει βιβλιοθήκη για τις λογικές συναρτήσεις προκειμένου να βρεθούν οι ιδιότητες που περιεγράφηκαν στο Κεφάλαιο 4. Η εντολή με την οποία γίνεται η χρήση της συγκεκριμένης βιβλιοθήκης είναι:

Sage:from sage.crypto.boolean_function import *BooleanFunction*

Στην συνέχεια ο χρήστης μπορεί να εισάγει την λογική συνάρτηση που επιθυμεί θέτοντας αρχικά την ονομασία της συνάρτησης και, έπειτα, μέσω του αριθμού των μεταβλητών της, την αλγεβρική κανονική μορφή της ή και τον πίνακα αληθείας της. Για την εύρεση της εκάστοτε ιδιότητας αρκεί η χρήση εντολών που είναι προκαθορισμένες από την βιβλιοθήκη του εργαλείου όπως αυτά περιγράφονται παρακάτω:

sage: *f=BooleanFunction([1,0,0,1])*
sage: *f.algebraic_degree()*
sage: *f.algebraic_degree()*
sage: *f.algebraic_immunity()*
sage: *f.correlation_immunity()*
sage: *f.is_balanced()*
sage: *f.is_bent()*

Οι παραπάνω εντολές, αρχικά δημιουργούν μία f λογική συνάρτηση βάση του πίνακα αληθείας της. Έπειτα με στην σειρά το εργαλείο δείχνει τον αλγεβρικό βαθμό της

συνάρτησης, την ανθεκτικότητα σε αλγεβρικές επιθέσεις, την ανθεκτικότητα σε επιθέσεις προσεγγίσεις, αν η συνάρτηση είναι ισοβαρής και τέλος αν είναι bent.

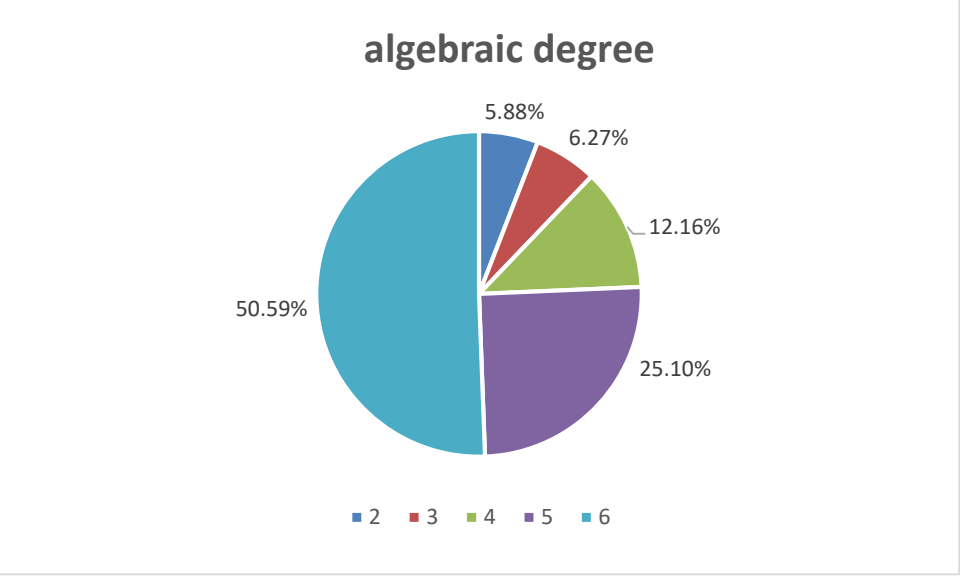
5.3.2 Βασικές ιδιότητες

Ο βαθμός των συναρτήσεων (algebraic degree) είναι στο 50% των περιπτώσεων στον μέγιστο εμφανιζόμενο βαθμό, ο οποίος είναι 6. Σε αλγεβρικό βαθμό συνάρτησης 5 παρουσιάστηκαν στο 25% των περιπτώσεων. Ο μέγιστος αλγεβρικός βαθμός που μπορεί να επιτευχθεί είναι $n-1=8-1=7$, όπου n=8 μεταβλητές (δηλαδή καμία συνάρτηση στη συγκεκριμένη περίπτωση δεν επιτυγχάνει το μέγιστο δυνατό βαθμό). Τα υπόλοιπα αποτελέσματα παρουσιάζονται στον παρακάτω πίνακα 6:

Βαθμός Συνάρτησης	Αριθμός συναρτήσεων	Ποσοστό
2	15	5,88%
3	16	6,27%
4	31	12,16%
5	64	25,10%
6	129	50,59%

Πίνακας 6: Ποσοστά συναρτήσεων που έχουν αλγεβρικούς βαθμούς (2,3,4,5,6)

Για να γίνουν πιο κατανοητά τα αποτελέσματα του πίνακα 6 χρησιμοποιήθηκε και το σχεδιάγραμμα τύπου πίτας προκειμένου να είναι πιο κατανοητά τα αποτελέσματα.



Διάγραμμα 1: Ποσοστό των συναρτήσεων με τους αλγεβρικούς βαθμούς τους

Το ποσοστό των συναρτήσεων που εμφανίζουν βαθμό συνάρτησης 2 είναι 6%. Αν και είναι πολύ μικρό ποσοστό, πρέπει να σημειωθεί ότι ο βαθμός 2 είναι πολύ χαμηλός βαθμός και συνιστά, κατ' αρχάς, μία κακή κρυπτογραφική ιδιότητα.

Α/Α	Συναρτήσεις	Αλγεβρικός Βαθμός	Μη Γραμμικότητα	Αλγεβρική ανθεκτικότητα
1	b2	2	64	2
2	b3	2	64	2
3	b5	2	64	2
4	b6	2	64	2
5	q8=b2+b3	2	96	2
6	q10=b2+b5	2	96	2
7	q11=b2+b6	2	96	2
8	q15=b3+b5	2	64	2
9	q16=b3+b6	2	64	2
10	q23=b5+b6	2	96	2
11	q51=b2+b3+b5	2	96	2
12	q52=b2+b3+b6	2	96	2
13	q59=b2+b5+b6	2	112	2
14	q69=b3+b5+b6	2	96	2
15	q124=b2+b3+b5+b6	2	112	2

Πίνακας 7: Πίνακας ιδιοτήτων συναρτήσεων με χαμηλό αλγεβρικό βαθμό

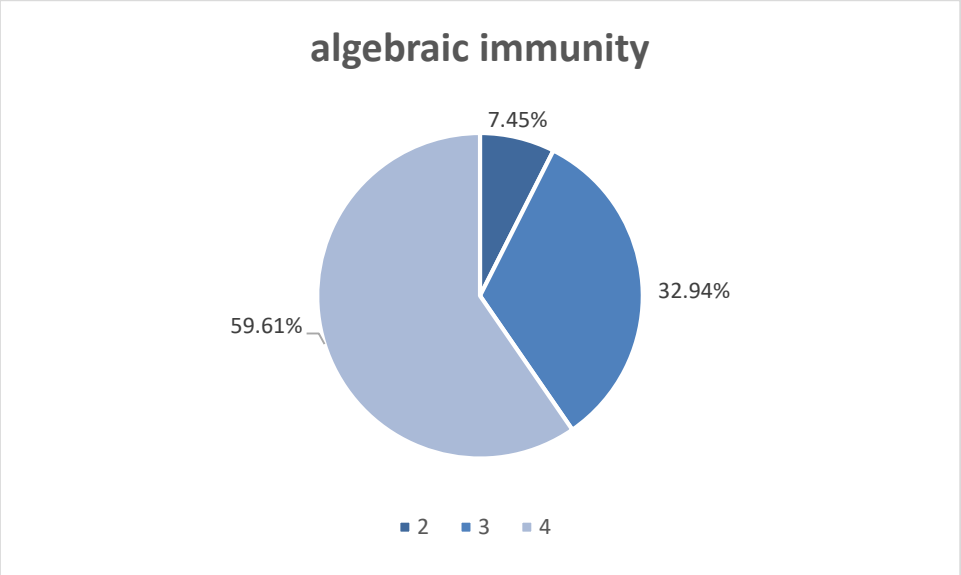
Αξιοσημείωτο πρέπει να θεωρηθεί ότι, όπως προαναφέρθηκε, καμία από τους συνδυασμούς των συναρτήσεων δεν επιτυγχάνει το μέγιστο δυνατό αλγεβρικό βαθμό 7.

Η αλγεβρική ανθεκτικότητα που παρουσιάζουν όλοι οι δυνατοί συνδυασμοί των Boolean συναρτήσεων είναι 4 για το 60% των συνδυασμών και 3 στο 33% των συνδυασμών. Στον πίνακα 8, όπως και στο διάγραμμα 2, εμφανίζονται τα αποτελέσματα για την αλγεβρική ανθεκτικότητα των συναρτήσεων.

Αλγεβρική Ανθεκτικότητα	Αριθμός Συναρτήσεων	Ποσοστό
2	19	7,45%
3	84	32,94%

4	152	59,61%

Πίνακας 8:Αριθμός-ποσοστό των συναρτήσεων που εμφανίζουν αλγεβρική ανθεκτικότητα (2,3,4)



Διάγραμμα 2: Ποσοστό των συναρτήσεων με την αλγεβρική ανθεκτικότητας τους

Κατά συνέπεια, περισσότερες από τις μισές συναρτήσεις επιτυγχάνουν τη βέλτιστη δυνατή τιμή της αλγεβρικής ανθεκτικότητας, ίση με 4. Υπάρχουν ωστόσο συναρτήσεις με τιμή 3 και, ακόμα χειρότερα, με τιμή 2. Ενδιαφέρον είναι ότι οι συναρτήσεις με τις χαμηλότερες τιμές αλγεβρικής ανθεκτικότητας δεν περιορίζονται μόνο σε αυτές που έχουν χαμηλό βαθμό (οπότε και για αυτές, εξ ορισμού, η αλγεβρική ανθεκτικότητα δεν θα μπορούσε να είναι μεγαλύτερη του βαθμού τους). Πιο συγκεκριμένα, αν και είναι 15 οι συναρτήσεις με βαθμό 2, οι συναρτήσεις με αλγεβρική ανθεκτικότητα 3 είναι 19 (δηλαδή οι 15 με βαθμό 2 συν 4 ακόμα). Αντίστοιχη παρατήρηση ισχύει και για τις συναρτήσεις με αλγεβρική ανθεκτικότητα 3.

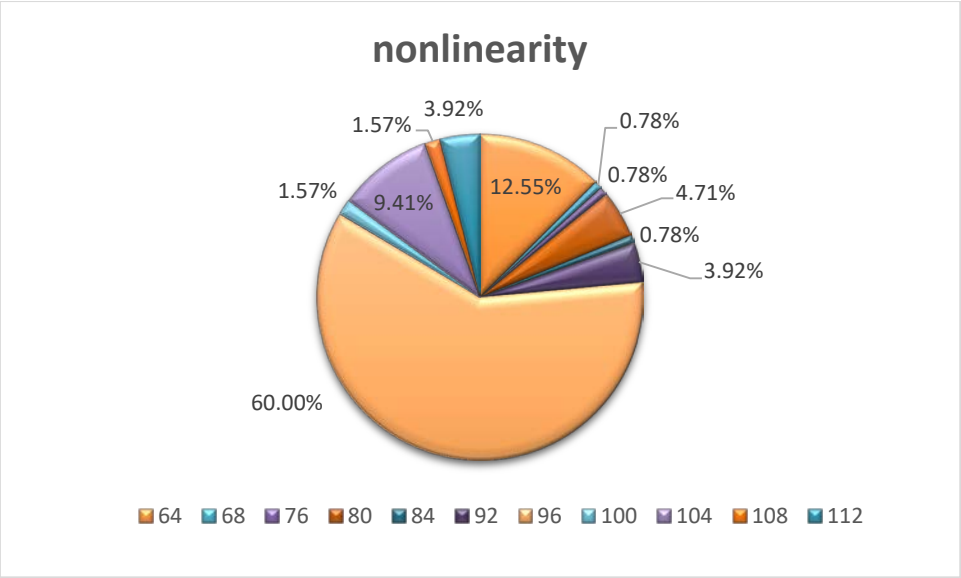
Συγκεντρωτικά, σε ποσοστό 7,45% εμφανίζεται αριθμός συναρτήσεων εξόδου, οι οποίες έχουν πολύ χαμηλή αλγεβρική ανθεκτικότητα (ίση με 2).

Όσον αφορά την μη γραμμικότητα των συναρτήσεων εξόδου του S-Box, οι τιμές που συναντώνται περιγράφονται στον Πίνακα 6. Κατ' αρχάς η μέγιστη δυνατή τιμή της μη γραμμικότητας για n=8 δίνεται από τις λεγόμενες συναρτήσεις bent (βλ. προηγούμενο κεφάλαιο) και ισούται με $2^{n-1} - 2^{\frac{n}{2}-1} = 2^7 - 2^3 = 120$. Οι συναρτήσεις μας δεν είναι

bent, οπότε αναμένουμε τιμή μη γραμμικότητας μικρότερη από 120. Μπορεί να θεωρηθεί ότι τιμές άνω του 100 θα μπορούσαν να θεωρηθούν ως υψηλές (για παράδειγμα, μία κρυπτογραφικά καλή συνάρτηση, η λεγόμενη συνάρτηση Carlet-Feng, έχει μη γραμμικότητα, για n=8, τιμή ίση με 112 (K. Limniotis, 2019)). Συνεπώς, η τιμή αυτή μπορεί να αποτελέσει μία βάση αναφοράς για την αποτίμηση των συναρτήσεων του S-box του Skinny. Παρατηρούμε ότι μόνο 10 συναρτήσεις (ποσοστό 3,92%) έχουν τιμή μη γραμμικότητας 112. Συνολικά, μόλις 42 από τις συνολικά 256 συναρτήσεις έχουν τιμή μη γραμμικότητας μεγαλύτερη από 100. Τιμή μη γραμμικότητας ίση με 96 εμφανίζεται στα $\frac{3}{5}$ του συνόλου των συναρτήσεων. Η χαμηλότερη τιμή είναι η 64, η οποία εμφανίζεται σε 32 συναρτήσεις, δηλαδή , στο 13% του συνόλου των συνδυασμών των συναρτήσεων. Το σύνολο των εμφανιζόμενων τιμών εμφανίζονται στον παρακάτω πίνακα 6, όπως και στο διάγραμμα 3.

Μη Γραμμικότητα	Αριθμός Συναρτήσεων	Ποσοστό
64	32	12,55%
68	2	0,78%
76	2	0,78%
80	12	4,71%
84	2	0,78%
92	10	3,92%
96	153	60,00%
100	4	1,57%
104	24	9,41%
108	4	1,57%
112	10	3,92%

Πίνακας 9: Μη γραμμικότητα με εμφανιζόμενο ποσοστό των συναρτήσεων εξόδων



Διάγραμμα 3: Μη γραμμικότητα με εμφανιζόμενο ποσοστό των συναρτήσεων εξόδων

Όπως φαίνεται παραπάνω καμία από τις συναρτήσεις δεν παρουσιάζει την μέγιστη μη γραμμικότητα. Αντίθετα σε ποσοστό περίπου 13% παρουσιάζουν ιδιαίτερα χαμηλή μη γραμμικότητα της τάξεως του 64.

5.3.3 Εφαρμογή Αλγορίθμου LPA

Ακολούθως θα ελέγξουμε το κρυπτογραφικό κριτήριο ως προς το κατά πόσον μία λογική συνάρτηση μπορεί να προσεγγιστεί ικανοποιητικά από άλλη με λιγότερο πλήθος μεταβλητών, αξιοποιώντας τον αλγόριθμο LPA όπως περιγράφηκε ανωτέρω. Χρησιμοποιήθηκε ο αλγόριθμος που έχουν δημοσιεύσει οι ερευνητές ελαφρά τροποποιημένος. Ο αλγόριθμος αυτός υπολογίζει τις τιμές των «κρίσιμων σημείων» του προφίλ γραμμικής πολυπλοκότητας σφαλμάτων για μία ακολουθία και, όπως περιγράφηκε, παρέχει χρήσιμη πληροφορία για τις αντίστοιχες λογικές συναρτήσεις, Οι συναρτήσεις που δόθηκε βαρύτητα είναι αυτές οι συναρτήσεις που τα bits που απαιτούνται να αλλαχθούν στην έξοδο του πίνακα αληθείας της προκειμένου για να απαλειφθεί μία μεταβλητή μία μεταβλητή είναι ίση ή μικρότερη από την χαμηλότερη μη γραμμικότητα των συναρτήσεων, που είναι 64 όπως αναφέρθηκε παραπάνω. Παρόλα αυτά παρατηρήθηκε ότι με το παραπάνω κριτήριο 72 από το σύνολο των συναρτήσεων μπορεί να προσεγγισθεί από συνάρτηση με μία λιγότερη μεταβλητή (δηλαδή 7 μεταβλητές), ήτοι το 28,24 %. Οι συναρτήσεις που διαθέτουν σημαντικό κρίσιμο σημείο, που μπορεί να οδηγήσει σε περαιτέρω απομείωση μεταβλητής (δηλαδή σε 6 μεταβλητές), είναι 71 από το σύνολο των συναρτήσεων, ήτοι 27,84 %, μείωση 3 μεταβλητών μπορούν να υποστούν 11 συναρτήσεις, ήτοι το 4,31 %. Περαιτέρω μείωση 4 μεταβλητών μπορεί

να εφαρμοστεί σε 17 συναρτήσεις, ήτοι 6,67%, μείωση 5 μεταβλητών μπορούν να υποστούν 5 συναρτήσεις, ήτοι 1,96% και τέλος μείωσης 6 μεταβλητών μπορεί να εφαρμοστεί σε 3 συναρτήσεις, δηλαδή 1,18 %. Στο παράρτημα Α.4 παρουσιάζονται οι συναρτήσεις που μπορούν να προσεγγισθούν από συναρτήσεις λιγότερων κατά 5 ή 6 μεταβλητών από τις αρχικές συναρτήσεις (δηλαδή με 3 ή 2 μεταβλητές/η αντίστοιχα).

Για την συνάρτηση b3 παρατηρήθηκε ότι παρουσιάζει 1 σημαντικό κρίσιμο σημείο, το οποίο είναι (62,2), από τα τρία κρίσιμα σημεία (0,13), (62,2) και (128,0). Όπως περιγράφηκε στην θεωρία στο κεφάλαιο 4 για να αποδειχθεί ότι υπάρχει συνάρτηση που προσεγγίζει την συνάρτηση θα πρέπει η γραμμική πολυπλοκότητα που προκύπτει στο κρίσιμο σημείο να είναι ίση ή μικρότερη από την υποδιπλάσια τιμή της μέγιστης γραμμικής πολυπλοκότητας (στην συγκεκριμένη περίπτωση $\frac{2^8}{2} = 128$). Στον πίνακα 10 συνοψίζεται η ύπαρξη συναρτήσεων με το πλήθος των μεταβλητών που διαθέτουν και το ποσοστό προσέγγισης της αρχικής συνάρτησης:

Μεταβλητές	Απόσταση	Bias(%)
2	62	25,8

Πίνακας 10: Significant Critical Points της b3

Άλλη μία συνάρτηση άξια αναφοράς είναι η b4, η οποία παρουσιάζει τα εξής CPs (0,225), (32,49), (64,9) και (128,0). Τα σημαντικά στην περίπτωσή μας CPs είναι τα (32,49) και (64,9). Παρατηρήθηκε ότι με την εναλλαγή 64 μόλις bits από το σύνολο των 256 bits προκύπτει μία συνάρτηση (που δεν υπολογίζεται στην συγκεκριμένη μεταπτυχιακή διατριβή) με 3 μεταβλητές, της οποίας η αντίστοιχη ακολουθία έχει γραμμική πολυπλοκότητα 9. Στον πίνακα 11 συνοψίζονται τα κρίσιμα CPs.

Μεταβλητές	Απόσταση	Bias(%)
6	32	37,5
3	64	25

Πίνακας 11: Significant Critical Points της b4

Η b5 είναι άλλη μία συνάρτηση που εμφανίζει κρίσιμα σημεία με τα οποία ενδεχομένως θα μπορούσε να προσεγγιστεί με μία συνάρτηση 2 μεταβλητών! Τα CPs είναι (0,13),

(64,3) και (128,0). Το σημαντικό στην περίπτωσή μας CPs είναι το (64,3). Στον πίνακα 12 παρουσιάζονται το πλήθος μεταβλητών των προσεγγιστικών συναρτήσεων:

Μεταβλητές	Απόσταση	Bias(%)
2	64	25

Πίνακας 12: Significant Critical Points της b5

Η επόμενη συνάρτηση είναι η b8. Τα CPs είναι (0,208), (4,205), (12,141), (20,135), (28,131), (52,45), (60,43), (64,5), (96,3) και (128,0). Τα σημαντικά στην περίπτωσή μας CPs είναι τα (52,45) και (64,5). Στον πίνακα 13 παρουσιάζονται το πλήθος μεταβλητών των προσεγγιστικών συναρτήσεων:

Μεταβλητές	Απόσταση	Bias(%)
6	52	29,7
3	64	25

Πίνακας 13: Significant Critical Points της b8

Επόμενη ενδιαφέρουσα συνάρτηση για πιθανό περαιτέρω έλεγχο είναι η q3 (=b1+b4), που παρουσιάζει τα CPs (0,225), (32,49), (64,9) και (128,0). Τα σημεία ενδιαφέροντος είναι (32,49) και (64,9). Ο πίνακας 14 παρουσιάζει τις πιθανές συναρτήσεις:

Μεταβλητές	Απόσταση	Bias(%)
6	32	37,5
3	64	25

Πίνακας 14: Significant Critical Points της q3

Η επόμενη συνάρτηση είναι η q15 (=b3+b5). Τα CPs είναι (0,10), (64,3) και (128,0). Το κρίσιμο CPs είναι το (64,3). Στον πίνακα 15 παρουσιάζονται το πλήθος μεταβλητών των προσεγγιστικών συναρτήσεων:

Μεταβλητές	Απόσταση	Bias(%)
2	64	25

Πίνακας 15: Significant Critical Points της q15

Η q28 (=b7+b8) είναι άλλη μία συνάρτηση που εμφανίζει κρίσιμα σημεία με τα οποία ενδεχομένως θα μπορούσε να προσεγγιστεί με μία συνάρτηση 3 μεταβλητών. Τα CPs είναι (0,208), (4,202), (12,141), (28,135), (36,131), (52,45), (56,43), (60,39), (64,5), (96,3) και (128,0). Τα σημαντικά στην περίπτωσή μας CPs είναι τα (52,45) και (64,5). Στον πίνακα 16 παρουσιάζονται το πλήθος μεταβλητών των προσεγγιστικών συναρτήσεων:

Μεταβλητές	Απόσταση	Bias(%)
5	52	29,7
3	64	25

Πίνακας 16: Significant Critical Points της q28

Τέλος η q83 (=b5+b7+b8) είναι άλλη μία συνάρτηση που θα μπορούσε ενδεχομένως να προσεγγιστεί από συνάρτηση με λιγότερες κατά 3 μεταβλητές από την αρχική συνάρτηση. Αρχικά παρουσιάζει τα εξής CPs (0,208), (4,202), (12,141), (28,135), (36,131), (52,45), (56,43), (60,39), (64,5), (96,3) και (128,0) με τα σημαντικά κρίσιμα σημεία να είναι (52,45) και (64,5) όπως Φαίνεται και στον πίνακα 17:

Μεταβλητές	Απόσταση	Bias(%)
5	52	29,7
3	64	25

Πίνακας 16: Significant Critical Points της q83

Αξιοσημείωτο είναι ότι αρκετές από τις συναρτήσεις παρουσίασαν σημαντικά κρίσιμα σημεία με τα οποία με μόλις εναλλαγή 64 bits προκύπτει μείωση 6 μεταβλητών! Κατά αυτόν τον τρόπο αυτές οι λογικές συναρτήσεις μπορούν να προσεγγιστούν από λογική συνάρτηση μόλις 2 μεταβλητών. Αυτές οι συναρτήσεις παρουσιάζουν κακή κρυπτογραφική ιδιότητα και θεωρείται ο περαιτέρω έλεγχος τους επιβεβλημένος.

Κεφάλαιο 6
Συμπεράσματα

Ο AES είναι το πρότυπο όλων των μοντέρνων κρυπτογραφικών αλγορίθμων. Αυτός προέκυψε σαν πρότυπο, έπειτα, από τον διαγωνισμό που διενήργησε το NIST προκειμένου να δημιουργήσει ένα πρότυπο για τα μοντέρνα κρυπτογραφικά συστήματα. Την τελευταία δεκαετία, όμως, αναπτύχθηκε μία τεχνολογία που ονομάστηκε Διαδίκτυο των Πραγμάτων. Ο AES, ενώ σαν πρότυπο σε εξυπηρετητές, σταθμούς εργασίας και κινητά τηλέφωνα αποδίδει και είναι ασφαλής δεν μπορεί να εκτελεστεί με την ίδια απόδοση σε συσκευές με μικρότερη επεξεργαστική ισχύ. Για τον λόγο αυτό το NIST εκκίνησε έναν νέο διαγωνισμό με τον οποίο αναζητά ένα κρυπτογραφικό αλγόριθμο, που θα ήταν ασφαλής και θα απέδιδε σε συσκευές με χαμηλότερη υπολογιστική ισχύ αλλά και χαμηλότερη αυτονομία. Ο διαγωνισμός αυτός βρίσκεται ακόμη εν εξελίξει με 32 υποψήφιους να βρίσκονται στον δεύτερο γύρο του διαγωνισμού. Αυτοί οι αλγόριθμοι λόγω της μειωμένης υπολογιστικής ισχύς που απαιτούν, αλλά και λόγω της χαμηλής ενεργειακής κατανάλωσης ονομάζονται Lightweight κρυπτογραφικοί αλγόριθμοι.

Η παρούσα διατριβή εστίασε στους lightweight κρυπτογραφικούς αλγορίθμους, λόγω του έντονου ερευνητικού ενδιαφέροντος που παρουσιάζουν. Αφού έγινε μία συνοπτική περιγραφή και κατηγοριοποίηση των αλγορίθμων που είναι αυτή τη στιγμή υποψήφιοι προς προτυποποίηση (δεύτερος γύρος του εν εξελίξει διαγωνισμού), ακολούθως μελετήθηκε η ασφάλεια υπό το πρίσμα της εξέτασης των κρυπτογραφικών ιδιοτήτων που ικανοποιούν οι υποκείμενες λογικές συναρτήσεις. Οι λογικές συναρτήσεις είναι ένα δομικό στοιχείο για τους αλγορίθμους ροής αλλά και για κρυπταλγορίθμους τμήματος - στη δεύτερη περίπτωση, κάποια είδη τους απαντώνται ιδίως σε S-Box.. Τα είδη των λογικών συναρτήσεων που συναντώνται σε S-Boxes είναι οι λεγόμενοι vectorial παρόλα αυτά πρέπει να έχουν καλές κρυπτογραφικές ιδιότητες και σαν αυτόνομες λογικές συναρτήσεις. Έτσι οι ιδιότητες που πρέπει να έχει μία λογική συνάρτηση για να έχει καλές

κρυπτογραφικές ιδιότητες θα πρέπει να εμπεριέχονται και στις vectorial λογικές συναρτήσεις. Βασικές κρυπτογραφικές ιδιότητες των λογικών συναρτήσεων είναι, η μη γραμμικότητα, , η ανθεκτικότητα σε αλγεβρικές επιθέσεις και ο αλγεβρικός βαθμός της συνάρτησης. Για να θεωρηθούν ότι οι ιδιότητες αυτές αποτελούν καλή κρυπτογραφική ιδιότητα είναι επιθυμητή ή όσον το δυνατόν πιο κοντινή τιμή από την μέγιστη τιμή της κάθε ιδιότητας. Έτσι ο μέγιστος αλγεβρικός βαθμός είναι $n-1$ (για ισοβαρείς συναρτήσεις), η μέγιστη μη γραμμικότητα $2^{n-1}-2^{\frac{n}{2}-1}$ όπου n το πλήθος των μεταβλητών (εφόσον το n είναι άρτιος αριθμός) και η μέγιστη αλγεβρική ανθεκτικότητα είναι $\lceil n/2 \rceil$. Παράλληλα, έχει καταδειχτεί ότι μία λογική συνάρτηση δεν πρέπει να μπορεί να προσεγγιστεί «ικανοποιητικά» από μία άλλη συνάρτηση η οποία εξαρτάται από μικρότερο πλήθος μεταβλητών. Ωστόσο, ως προς αυτό το κρυπτογραφικό κριτήριο, λίγα είναι γνωστά (π.χ. συμπεριφορά βέλτιστων, ως προς αυτό το κριτήριο συναρτήσεων).

Στην παρούσα διατριβή, μετά από εξέταση των 32 υποψήφιων αλγορίθμων στον διαγωνισμό του NIST, επιλέχθηκε ο αλγόριθμος Skinny για την ανάλυσή μας. Οι λόγοι επιλογής έγκεινται στο ότι, αφενός, ήταν ο μόνος αλγόριθμος εκ των 32 εμπεριέχει ένα S-box (διανυσματική λογική συνάρτηση), οπότε θα μπορούσε να μελετηθεί η ασφάλειά του ως προς τις λογικές συναρτήσεις, και αφετέρου οι εμπνευστές του ισχυρίζονται ότι ακολουθεί τη σχεδιαστική φιλοσοφία του πρότυπου αλγόριθμου AES. Η μελέτη των εξόδων του S-Box του κρυπτογραφικού αλγόριθμου Skinny μελετήθηκαν με την χρήση του εργαλείου SageMath, το οποίο είναι ένα ανοιχτού κώδικα εργαλείου παρόμοιου με ευρέως γνωστά εργαλεία όπως το Mathematica και το MATLAB.

Για να γίνει εκτενής μελέτη των εξόδων πρέπει να ελεγχθούν όλες οι πιθανές λογικές συναρτήσεις που προκύπτουν από τις 8 διαφορετικές λογικές συναρτήσεις που παράγονται στην έξοδο του αλγορίθμου. Το σύνολο των συναρτήσεων είναι 255 ($=2^8-1$) εκτός της μηδενικής συνάρτησης. Αφού δημιουργήθηκαν όλες οι πιθανές συναρτήσεις ελέγχθηκαν αρχικά ως προς τον αλγεβρικό τους βαθμού, την μη γραμμικότητα και την αντοχή σε αλγεβρικές επιθέσεις.

Παρατηρήθηκε ότι καμία από τις παραγόμενες συναρτήσεις δεν επιτυγχάνει τον μέγιστο αλγεβρικό βαθμό, ο οποίος είναι 7, αλλά ο μέγιστος βαθμός που επιτυγχάνεται είναι 6 με εμφάνιση σε ποσοστό 50,6 %. Ο δεύτερος πιο συχνός αλγεβρικός βαθμός είναι ο 5 που συναντάται σε ποσοστό 25,1 %. Αξιοσημείωτο είναι ότι 15 συναρτήσεις παρουσιάζουν

χαμηλό αλγεβρικό βαθμό 2, που οδηγεί σε χαμηλή γραμμική πολυπλοκότητα των συγκεκριμένων συναρτήσεων.

Η μη γραμμικότητα των παραγόμενων συναρτήσεων είναι ανάμεσα στο εύρος του 64 έως 112.. Η πιο συνήθης μη γραμμικότητα που συναντάται είναι η 96 που είναι σε 60 %. Μία πιθανώς κακή κρυπτογραφική ιδιότητα είναι ότι 32 συναρτήσεις από το σύνολο των συναρτήσεων, ήτοι 12,5 %, έχουν μη γραμμικότητα ίση με 64. Όπως φαίνεται στο παράρτημα Α.3, 6 συναρτήσεις που έχουν χαμηλό αλγεβρικό βαθμό 2 παρουσιάζουν και την χαμηλότερη μη γραμμικότητα, η οποία είναι 64.

Στην συνέχεια εφαρμόστηκε μία πρόσφατη τεχνική, που χρησιμοποιεί το λεγόμενο αλγόριθμο Lauder-Paterson (LPA), προκειμένου να διερευνηθεί αν κάποιες από τις συναρτήσεις του S-box του Skinny μπορούν να προσεγγιστούν ικανοποιητικά από άλλες συναρτήσεις χαμηλότερου βαθμού. Αξιοσημείωτο είναι ότι 72 συναρτήσεις από το σύνολο των συναρτήσεων, ήτοι 28,24 %, παρουσιάζουν τουλάχιστον ένα σημαντικό κρίσιμο σημείο που υποδεικνύει ότι θα μπορούσε να ήταν δυνατή η προσέγγιση της λογικής συνάρτησης από μία συνάρτηση με 7 μεταβλητές για την περίπτωση που τα απαιτούμενα για αλλαγή bits είναι λιγότερα από την χαμηλότερη μη γραμμικότητα (δηλαδή 64). Σε αυτήν την περίπτωση συναντώνται κρίσιμα σημεία της μορφής (32,x) που δείχνουν ότι με μόλις αλλαγή 32 bits μπορεί να προκύψει προσεγγιστική συνάρτηση με 7 μεταβλητές και χαμηλότερη γραμμική πολυπλοκότητα.

Εν συνεχεία βρέθηκαν 71 συναρτήσεις, ήτοι 27,84 %, που παρουσιάζουν κρίσιμο σημείο με το οποίο είναι δυνατή η προσέγγιση της συνάρτησης με συνάρτηση με 6 μεταβλητές, 11 συναρτήσεις, ήτοι το 4,31 %, παρουσιάζει σημαντικό κρίσιμο σημείο για περαιτέρω μείωση των μεταβλητών που μπορεί να προσεγγίσει την συνάρτηση, δηλαδή με 6 μεταβλητές. Ακόμα 17 συναρτήσεις, ήτοι 6,67 %, διαθέτουν κρίσιμο σημείο, ώστε να μπορούν να προσεγγιστούν από συνάρτηση με 4 μεταβλητές, 5 συναρτήσεις, ήτοι 1,96 %, παρουσιάζουν σημαντικό κρίσιμο σημείο για μείωση 5 μεταβλητών. Τέλος, 3 συναρτήσεις, ήτοι 1,18 %, εμφανίζουν σημαντικό κρίσιμο σημείο με το οποίο μπορούν να προσεγγιστούν από συνάρτηση με μόλις 2 μεταβλητές, κάτι το οποίο αποτελεί μία κακή κρυπτογραφική ιδιότητα που χρήζει περαιτέρω έρευνας.

Από τα αποτελέσματα της έρευνας αναδεικνύεται ότι οι ιδιότητες των λογικών συναρτήσεων του S-box δεν είναι όλες ισχυρές, γεγονός το οποίο δημιουργεί σαφώς κάποιες ανησυχίες. Θα πρέπει βέβαια να αποσαφηνιστεί ότι η μη εκπλήρωση μίας κρυπτογραφικής ιδιότητας (ή και περισσότερων) από μόνη της δεν αποτελεί απόδειξη ευπάθειας του αλγορίθμου συνολικά: εξαρτάται από το υπόλοιπο τμήμα του αλγορίθμου αλλά και τον τρόπο με τον οποίο η λογική συνάρτηση (εν προκειμένω, το S-box) χρησιμοποιείται εντός αυτού. . Παρόλα αυτά όμως, καθίσταται σαφές ότι οι ασθενείς κρυπτογραφικές ιδιότητες, που παρουσιάστηκαν παραπάνω σε κάποιες εκ των περιπτώσεων, χρήζουν περαιτέρω επιστημονικής έρευνας και ανάλυσης, λαμβάνοντας υπόψη και όλον τον αλγόριθμο συνολικά. Εξάλλου, ιδίως η χρήση του LPA, λόγω του ότι είναι μία εξαιρετικά νέα τεχνική (ήτοι δεν ήταν γνωστή όταν εκκίνησε ο διαγωνισμός του NIST και σχεδιάστηκαν οι εν λόγω αλγόριθμοι), μπορεί πράγματι να καταδείξει ευπάθειες που δεν ήταν δυνατόν να ανιχνευτούν έγκαιρα κατά τη σχεδίαση του αλγορίθμου.

Εν κατακλείδι, η παρούσα διατριβή αναδεικνύει το γνωστό ζήτημα της δυσκολίας σχεδίασης λογικών συναρτήσεων οι οποίες να πληρούν όλα τα γνωστά κρυπτογραφικά κριτήρια. Με τη σειρά του, αυτό δίνει περαιτέρω έμφαση στην ανάγκη μελέτης όλων των ιδιοτήτων, προκειμένου να γίνεται προσεχτική επιλογή της λογικής συνάρτησης κάθε φορά. Τα νέα αποτελέσματα που μπορεί να παρέχει, με αποτελεσματικό τρόπο, η χρήση του LPA μπορούν να συνεισφέρουν σημαντικά σε αυτήν την κατεύθυνση. Τα αποτελέσματα της διατριβής, τα οποία εφαρμόστηκαν σε κρυπτογραφικό αλγόριθμο ο οποίος εξετάζεται αυτή τη στιγμή από την ερευνητική κοινότητα, επικυρώνουν αυτόν τον ισχυρισμό.

Παράρτημα Α
Αλγόριθμος SKINNY

Α.1 Έξοδος S-Box του Αλγόριθμου SKINNY

uint8_t S8 [256] = {

0x65 ,0 x4c ,0 x6a ,0 x42 ,0 x4b ,0 x63 ,0 x43 ,0 x6b ,0 x55 ,0 x75 ,0 x5a ,0 x7a ,0 x53 ,0 x73 ,0 x5b ,0 x7b ,0x35 ,0 x8c ,0 x3a ,0 x81 ,0 x89 ,0 x33 ,0 x80 ,0 x3b ,0 x95 ,0 x25 ,0 x98 ,0 x2a ,0 x90 ,0 x23 ,0 x99 ,0 x2b ,0xe5 ,0 xcc ,0 xe8 ,0 xc1 ,0 xc9 ,0 xe0 ,0 xc0 ,0 xe9 ,0 xd5 ,0 xf5 ,0 xd8 ,0 xf8 ,0 xd0 ,0 xf0 ,0 xd9 ,0 xf9 ,0xa5 ,0 x1c ,0 xa8 ,0 x12 ,0 x1b ,0 xa0 ,0 x13 ,0 xa9 ,0 x05 ,0 xb5 ,0 x0a ,0 xb8 ,0 x03 ,0 xb0 ,0 x0b ,0 xb9 ,0x32 ,0 x88 ,0 x3c ,0 x85 ,0 x8d ,0 x34 0 x84 ,0 x3d ,0 x91 ,0 x22 ,0 x9c ,0 x2c ,0 x94 ,0 x24 ,0 x9d ,0 x2d ,0x62 ,0 x4a ,0 x6c ,0 x45 ,0 x4d ,0 x64 ,0 x44 ,0 x6d ,0 x52 ,0 x72 ,0 x5c ,0 x7c ,0 x54 ,0 x74 ,0 x5d ,0 x7d ,0xa1 ,0 x1a ,0 xac ,0 x15 ,0 x1d ,0 xa4 ,0 x14 ,0 xad ,0 x02 ,0 xb1 ,0 x0c ,0 xbc ,0 x04 ,0 xb4 ,0 x0d ,0 xbd ,0xe1 ,0 xc8 ,0 xec ,0 xc5 ,0 xcd ,0 xe4 ,0 xc4 ,0 xed ,0 xd1 ,0 xf1 ,0 xdc ,0 xfc ,0 xd4,0xf4,0xdd ,0 xfd ,0x36 ,0 x8e ,0 x38 ,0 x82 ,0 x8b ,0 x30 ,0 x83 ,0 x39 ,0 x96 ,0 x26 ,0 x9a ,0 x28 ,0 x93 ,0 x20 ,0 x9b ,0 x29 ,0x66 ,0 x4e ,0 x68 ,0 x41 ,0 x49 ,0 x60 ,0 x40 ,0 x69 ,0 x56 ,0 x76,0 x58 ,0 x78 ,0 x50 ,0 x70 ,0 x59 ,0 x79 ,0xa6 ,0 x1e ,0 xaa ,0 x11 ,0 x19 ,0 xa3 ,0 x10 ,0 xab ,0 x06 ,0 xb6 ,0 x08 ,0 xba ,0 x00 ,0 xb3 ,0 x09 ,0 xbb ,0xe6 ,0 xce ,0 xea ,0 xc2 ,0 xcb ,0 xe3 ,0 xc3 ,0 xeb ,0 xd6 ,0 xf6 ,0 xda ,0 xfa ,0 xd3 ,0 xf3 ,0 xdb ,0 xfb ,0x31 ,0 x8a ,0 x3e ,0 x86 ,0x8f,0x37 ,0 x87 ,0 x3f ,0 x92 ,0 x21 ,0 x9e ,0 x2e ,0 x97 ,0 x27 ,0 x9f ,0 x2f ,0x61 ,0 x48 ,0 x6e ,0 x46 0 x4f ,0 x67 ,0 x47 ,0 x6f ,0 x51 ,0 x71 ,0 x5e ,0 x7e ,0 x57 ,0 x77 ,0 x5f ,0 x7f ,0xa2 ,0 x18 ,0 xae ,0 x16 ,0 x1f ,0 xa7 ,0 x17 ,0 xaf ,0 x01 ,0 xb2 ,0 x0e ,0 xbe ,0 x07 ,0 xb7 ,0 x0f ,0 xbf ,0xe2 ,0 xca ,0 xee ,0 xc6 ,0 xcf ,0 xe7 ,0 xc7 ,0 xef ,0 xd2 ,0 xf2 ,0 xde ,0 xfe ,0 xd7,0xf7,0 xdf ,0 xff};

Α.2 Πρόγραμμα Αλλαγής Δεκαεξαδικού Πίνακα σε Δυαδική Ακολουθία

```
#include <stdio.h>
int main()
{
        char S8[256] = {
'6' ,'4' ,'6' ,'4' ,'4' ,'6' ,'4' ,'6' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,
'3' ,'8' ,'3' ,'8' ,'8' ,'3' ,'8' ,'3' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,
'e' ,'c' ,'e' ,'c' ,'c' ,'e' ,'c' ,'e' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,
'a' ,'1' ,'a' ,'1' ,'1' ,'a' ,'1' ,'a' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,
'3' ,'8' ,'3' ,'8' ,'8' ,'3' ,'8' ,'3' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,
'6' ,'4' ,'6' ,'4' ,'4' ,'6' ,'4' ,'6' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,
'a' ,'1' ,'a' ,'1' ,'1' ,'a' ,'1' ,'a' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,
'e' ,'c' ,'e' ,'c' ,'c' ,'e' ,'c' ,'e' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,
'3' ,'8' ,'3' ,'8' ,'8' ,'3' ,'8' ,'3' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,
'6' ,'4' ,'6' ,'4' ,'4' ,'6' ,'4' ,'6' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,
'a' ,'1' ,'a' ,'1' ,'1' ,'a' ,'1' ,'a' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,
'e' ,'c' ,'e' ,'c' ,'c' ,'e' ,'c' ,'e' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,
'3' ,'8' ,'3' ,'8' ,'8' ,'3' ,'8' ,'3' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,
'6' ,'4' ,'6' ,'4' ,'4' ,'6' ,'4' ,'6' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,
'a' ,'1' ,'a' ,'1' ,'1' ,'a' ,'1' ,'a' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,
'e' ,'c' ,'e' ,'c' ,'c' ,'e' ,'c' ,'e' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,
'3' ,'8' ,'3' ,'8' ,'8' ,'3' ,'8' ,'3' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,'9' ,'2' ,
'6' ,'4' ,'6' ,'4' ,'4' ,'6' ,'4' ,'6' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,'5' ,'7' ,
'a' ,'1' ,'a' ,'1' ,'1' ,'a' ,'1' ,'a' ,'0', 'b' ,'0' ,'b' ,'0' ,'b' ,'0' ,'b' ,
'e' ,'c' ,'e' ,'c' ,'c' ,'e' ,'c' ,'e' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f' ,'d' ,'f'
};

char s7[256] ={
'5' ,'c' ,'a' ,'2' ,'b' ,'3' ,'3' ,'b' ,'5' ,'5' ,'a' ,'a' ,'3' ,'3' ,'b' ,'b' ,
'5' ,'c' ,'a' ,'1' ,'9' ,'3' ,'0' ,'b' ,'5' ,'5' ,'8' ,'a' ,'0' ,'3' ,'9' ,'b' ,
'5' ,'c' ,'8' ,'1' ,'9' ,'0' ,'0' ,'9' ,'5' ,'5' ,'8' ,'8' ,'0' ,'0' ,'9' ,'9' ,
'5' ,'c' ,'8' ,'2' ,'b' ,'0' ,'3' ,'9' ,'5' ,'5' ,'a' ,'8' ,'3' ,'0' ,'b' ,'9' ,
'2' ,'8' ,'c' ,'5' ,'d' ,'4' ,'4' ,'d' ,'1' ,'2' ,'c' ,'c' ,'4' ,'4' ,'d' ,'d' ,
'2' ,'a' ,'c' ,'5' ,'d' ,'4' ,'4' ,'d' ,'2' ,'2' ,'c' ,'c' ,'4' ,'4' ,'d' ,'d' ,
'1' ,'a' ,'c' ,'5' ,'d' ,'4' ,'4' ,'d' ,'2' ,'1' ,'c' ,'c' ,'4' ,'4' ,'d' ,'d' ,
'1' ,'8' ,'c' ,'5' ,'d' ,'4' ,'4' ,'d' ,'1' ,'1' ,'c' ,'c' ,'4' ,'4' ,'d' ,'d' ,
'6' ,'e' ,'8' ,'2' ,'b' ,'0' ,'3' ,'9' ,'6' ,'6' ,'a' ,'8' ,'3' ,'0' ,'b' ,'9' ,
'6' ,'e' ,'8' ,'1' ,'9' ,'0' ,'0' ,'9' ,'6' ,'6' ,'8' ,'8' ,'0' ,'0' ,'9' ,'9' ,
'6' ,'e' ,'a' ,'1' ,'9' ,'3' ,'0' ,'b' ,'6' ,'6' ,'8' ,'a' ,'0' ,'3' ,'9' ,'b' ,
```

```
'6' ,'e' ,'a' ,'2' ,'b' ,'3' ,'3' ,'b' ,'6' ,'6' ,'a' ,'a' ,'3' ,'3' ,'b' ,'b' ,
'1' ,'a' ,'e' ,'6' ,'f' ,'7' ,'7' ,'f' ,'2' ,'1' ,'e' ,'e' ,'7' ,'7' ,'f' ,'f' ,
'1' ,'8' ,'e' ,'6' ,'f' ,'7' ,'7' ,'f' ,'1' ,'1' ,'e' ,'e' ,'7' ,'7' ,'f' ,'f' ,
'2' ,'8' ,'e' ,'6' ,'f' ,'7' ,'7' ,'f' ,'1' ,'2' ,'e' ,'e' ,'7' ,'7' ,'f' ,'f' ,
'2' ,'a' ,'e' ,'6' ,'f' ,'7' ,'7' ,'f' ,'2' ,'2' ,'e' ,'e' ,'7' ,'7' ,'f' ,'f'
};
        int x[8],i,j;
        for (i=0;i<256;i++)
        {
                switch(S8[i])
                {
                        case '0':
                                x[0]=0;
                                x[1]=0;
                                x[2]=0;
                                x[3]=0;
                                break;
                        case '1':
                                x[0]=0;
                                x[1]=0;
                                x[2]=0;
                                x[3]=1;
                                break;
                        case '2':
                                x[0]=0;
                                x[1]=0;
                                x[2]=1;
                                x[3]=0;
                                break;
                        case '3':
                                x[0]=0;
                                x[1]=0;
                                x[2]=1;
                                x[3]=1;
```

```
            break;
    case '4':
            x[0]=0;
            x[1]=1;
            x[2]=0;
            x[3]=0;
            break;
    case '5':
            x[0]=0;
            x[1]=1;
            x[2]=0;
            x[3]=1;
            break;
    case '6':
            x[0]=0;
            x[1]=1;
            x[2]=1;
            x[3]=0;
            break;
    case '7':
            x[0]=0;
            x[1]=1;
            x[2]=1;
            x[3]=1;
            break;
    case '8':
            x[0]=1;
            x[1]=0;
            x[2]=0;
            x[3]=0;
            break;
    case '9':
            x[0]=1;
            x[1]=0;
```

```
            x[2]=0;
            x[3]=1;
            break;
    case 'a':
            x[0]=1;
            x[1]=0;
            x[2]=1;
            x[3]=0;
            break;
    case 'b':
            x[0]=1;
            x[1]=0;
            x[2]=1;
            x[3]=1;
            break;
    case 'c':
            x[0]=1;
            x[1]=1;
            x[2]=0;
            x[3]=0;
            break;
    case 'd':
            x[0]=1;
            x[1]=1;
            x[2]=0;
            x[3]=1;
            break;
    case 'e':
            x[0]=1;
            x[1]=1;
            x[2]=1;
            x[3]=0;
            break;
    case 'f':
```

```
                x[0]=1;
                x[1]=1;
                x[2]=1;
                x[3]=1;
                break;
}
for (j=0;j<256;j++)
{
        switch(s7[i])
        {
                case '0':
                        x[4]=0;
                        x[5]=0;
                        x[6]=0;
                        x[7]=0;
                        break;
                case '1':
                        x[4]=0;
                        x[5]=0;
                        x[6]=0;
                        x[7]=1;
                        break;
                case '2':
                        x[4]=0;
                        x[5]=0;
                        x[6]=1;
                        x[7]=0;
                        break;
                case '3':
                        x[4]=0;
                        x[5]=0;
                        x[6]=1;
                        x[7]=1;
                        break;
```

```
case '4':
        x[4]=0;
        x[5]=1;
        x[6]=0;
        x[7]=0;
        break;
case '5':
        x[4]=0;
        x[5]=1;
        x[6]=0;
        x[7]=1;
        break;
case '6':
        x[4]=0;
        x[5]=1;
        x[6]=1;
        x[7]=0;
        break;
case '7':
        x[4]=0;
        x[5]=1;
        x[6]=1;
        x[7]=1;
        break;
case '8':
        x[4]=1;
        x[5]=0;
        x[6]=0;
        x[7]=0;
        break;
case '9':
        x[4]=1;
        x[5]=0;
        x[6]=0;
```

```
            x[7]=1;
            break;
        case 'a':
            x[4]=1;
            x[5]=0;
            x[6]=1;
            x[7]=0;
            break;
        case 'b':
            x[4]=1;
            x[5]=0;
            x[6]=1;
            x[7]=1;
            break;
        case 'c':
            x[4]=1;
            x[5]=1;
            x[6]=0;
            x[7]=0;
            break;
        case 'd':
            x[4]=1;
            x[5]=1;
            x[6]=0;
            x[7]=1;
            break;
        case 'e':
            x[4]=1;
            x[5]=1;
            x[6]=1;
            x[7]=0;
            break;
        case 'f':
            x[4]=1;
```

```
                                x[5]=1;
                                x[6]=1;
                                x[7]=1;
                                break;
                        }
                }

        printf("%d%d%d%d%d%d%d%d\n",x[0],x[1],x[2],x[3],x[4],x[5],x[6],x[7]);
        }
        return 0;
}
```

A.3 Πιθανοί Συνδυασμοί των Λογικών Συναρτήσεων που προκύπτουν από το S-Box του Skinny

Ονομασία Συνάρτησης	Συνδυασμός Αρχικών Συναρτήσεων
q1	b1+b2
q2	b1+b3
q3	b1+b4
q4	b1+b5
q5	b1+b6
q6	b1+b7
q7	b1+b8
q8	b2+b3
q9	b2+b4
q10	b2+b5
q11	b2+b6
q12	b2+b7
q13	b2+b8
q14	b3+b4
q15	b3+b5
q16	b3+b6
q17	b3+b7
q18	b3+b8

q19	b4+b5
q20	b4+b6
q21	b4+b7
q22	b4+b8
q23	b5+b6
q24	b5+b7
q25	b5+b8
q26	b6+b7
q27	b6+b8
q28	b7+b8
q29	b1+b2+b3
q30	b1+b2+b4
q31	b1+b2+b5
q32	b1+b2+b6
q33	b1+b2+b7
q34	b1+b2+b8
q35	b1+b3+b4
q36	b1+b3+b5
q37	b1+b3+b6
q38	b1+b3+b7
q39	b1+b3+b8
q40	b1+b4+b5
q41	b1+b4+b6
q42	b1+b4+b7
q43	b1+b4+b8
q44	b1+b5+b6
q45	b1+b5+b7
q46	b1+b5+b8
q47	b1+b6+b7
q48	b1+b6+b8
q49	b1+b7+b8
q50	b2+b3+b4
q51	b2+b3+b5
q52	b2+b3+b6
q53	b2+b3+b7

q54	b2+b3+b8
q55	b2+b4+b5
q56	b2+b4+b6
q57	b2+b4+b7
q58	b2+b4+b8
q59	b2+b5+b6
q60	b2+b5+b7
q61	b2+b5+b8
q62	b2+b6+b7
q63	b2+b6+b8
q64	b2+b7+b8
q65	b3+b4+b5
q66	b3+b4+b6
q67	b3+b4+b7
q68	b3+b4+b8
q69	b3+b5+b6
q70	b3+b5+b7
q71	b3+b5+b8
q72	b3+b6+b7
q73	b3+b6+b8
q74	b3+b7+b8
q75	b4+b5+b6
q76	b4+b5+b7
q77	b4+b5+b8
q78	b4+b6+b7
q79	b4+b6+b8
q80	b4+b7+b8
q81	b5+b6+b7
q82	b5+b6+b8
q83	b5+b7+b8
q84	b6+b7+b8
q85	b1+b2+b3+b4
q86	b1+b2+b3+b5

q87	b1+b2+b3+b6
q88	b1+b2+b3+b7
q89	b1+b2+b3+b8
q90	b1+b2+b4+b5
q91	b1+b2+b4+b6
q92	b1+b2+b4+b7
q93	b1+b2+b4+b8
q94	b1+b2+b5+b6
q95	b1+b2+b5+b7
q96	b1+b2+b5+b8
q97	b1+b2+b6+b7
q98	b1+b2+b6+b8
q99	b1+b2+b7+b8
q100	b1+b3+b4+b5
q101	b1+b3+b4+b6
q102	b1+b3+b4+b7
q10	b1+b3+b4+b8
q104	b1+b3+b5+b6
q105	b1+b3+b5+b7
q106	b1+b3+b5+b8
q107	b1+b3+b6+b7
q108	b1+b3+b6+b8
q109	b1+b3+b7+b8
q110	b1+b4+b5+b6
q111	b1+b4+b5+b7
q112	b1+b4+b5+b8
q113	b1+b4+b6+b7
q114	b1+b4+b6+b8
q115	b1+b4+b7+b8
q116	b1+b5+b6+b7
q117	b1+b5+b6+b8
q118	b1+b5+b7+b8
q119	b1+b6+b7+b8

q120	b2+b3+b4+b5
q121	b2+b3+b4+b6
q122	b2+b3+b4+b7
q123	b2+b3+b4+b8
q124	b2+b3+b5+b6
q125	b2+b3+b5+b7
q126	b2+b3+b5+b8
q127	b2+b3+b6+b7
q128	b2+b3+b6+b8
q129	b2+b3+b7+b8
q130	b2+b4+b5+b6
q131	b2+b4+b5+b7
q132	b2+b4+b5+b8
q133	b2+b4+b6+b7
q134	b2+b4+b6+b8
q135	b2+b4+b7+b8
q136	b2+b5+b6+b7
q137	b2+b5+b6+b8
q138	b2+b5+b7+b8
q139	b2+b6+b7+b8
q140	b3+b4+b5+b6
q141	b3+b4+b5+b7
q142	b3+b4+b5+b8
q143	b3+b4+b6+b7
q144	b3+b4+b6+b8
q145	b3+b4+b7+b8
q146	b3+b5+b6+b7
q147	b3+b5+b6+b8
q148	b3+b5+b7+b8
q149	b3+b6+b7+b8
q150	b4+b5+b6+b7
q151	b4+b5+b6+b8
q152	b4+b5+b7+b8

q153	b4+b6+b7+b8
q154	b5+b6+b7+b8
q155	b1+b2+b3+b4+b5
q156	b1+b2+b3+b4+b6
q157	b1+b2+b3+b4+b7
q158	b1+b2+b3+b4+b8
q159	b1+b2+b3+b5+b6
q160	b1+b2+b3+b5+b7
q161	b1+b2+b3+b5+b8
q162	b1+b2+b3+b6+b7
q163	b1+b2+b3+b6+b8
q164	b1+b2+b3+b7+b8
q165	b1+b2+b4+b5+b6
q166	b1+b2+b4+b5+b7
q167	b1+b2+b4+b5+b8
q168	b1+b2+b4+b6+b7
q169	b1+b2+b4+b6+b8
q170	b1+b2+b4+b7+b8
q171	b1+b2+b5+b6+b7
q172	b1+b2+b5+b6+b8
q173	b1+b2+b5+b7+b8
q174	b1+b2+b6+b7+b8
q175	b1+b3+b4+b5+b6
q176	b1+b3+b4+b5+b7
q177	b1+b3+b4+b5+b8
q178	b1+b3+b4+b6+b7
q179	b1+b3+b4+b6+b8
q180	b1+b3+b4+b7+b8
q181	b1+b3+b5+b6+b7
q182	b1+b3+b5+b6+b8
q183	b1+b3+b5+b7+b8
q184	b1+b3+b6+b7+b8
q185	b1+b4+b5+b6+b7

q186	b1+b4+b5+b6+b8
q187	b1+b4+b5+b7+b8
q188	b1+b4+b6+b7+b8
q189	b1+b5+b6+b7+b8
q190	b2+b3+b4+b5+b6
q191	b2+b3+b4+b5+b7
q192	b2+b3+b4+b5+b8
q193	b2+b3+b4+b6+b7
q194	b2+b3+b4+b6+b8
q195	b2+b3+b4+b7+b8
q196	b2+b3+b5+b6+b7
q197	b2+b3+b5+b6+b8
q198	b2+b3+b5+b7+b8
q199	b2+b3+b6+b7+b8
q200	b2+b4+b5+b6+b7
q201	b2+b4+b5+b6+b8
q202	b2+b4+b5+b7+b8
q203	b2+b4+b6+b7+b8
q204	b2+b5+b6+b7+b8
q205	b3+b4+b5+b6+b7
q206	b3+b4+b5+b6+b8
q207	b3+b4+b5+b7+b8
q208	b3+b4+b6+b7+b8
q209	b3+b5+b6+b7+b8
q210	b4+b5+b6+b7+b8
q211	b1+b2+b3+b4+b5+b6
q212	b1+b2+b3+b4+b5+b7
q213	b1+b2+b3+b4+b5+b8
q214	b1+b2+b3+b4+b6+b7
q215	b1+b2+b3+b4+b6+b8
q216	b1+b2+b3+b4+b7+b8
q217	b1+b2+b3+b5+b6+b7
q218	b1+b2+b3+b5+b6+b8

q219	b1+b2+b3+b5+b7+b8
q220	b1+b2+b3+b6+b7+b8
q221	b1+b2+b4+b5+b6+b7
q222	b1+b2+b4+b5+b6+b8
q223	b1+b2+b4+b5+b7+b8
q224	b1+b2+b4+b6+b7+b8
q225	b1+b2+b5+b6+b7+b8
q226	b1+b3+b4+b5+b6+b7
q227	b1+b3+b4+b5+b6+b8
q228	b1+b3+b4+b5+b7+b8
q229	b1+b3+b4+b6+b7+b8
q230	b1+b3+b5+b6+b7+b8
q231	b1+b4+b5+b6+b7+b8
q232	b2+b3+b4+b5+b6+b7
q233	b2+b3+b4+b5+b6+b8
q234	b2+b3+b4+b5+b7+b8
q235	b2+b3+b4+b6+b7+b8
q236	b2+b3+b5+b6+b7+b8
q237	b2+b4+b5+b6+b7+b8
q238	b3+b4+b5+b6+b7+b8
q239	b1+b2+b3+b4+b5+b6+b7
q240	b1+b2+b3+b4+b5+b6+b8
q241	b1+b2+b3+b4+b5+b7+b8
q242	b1+b2+b3+b4+b6+b7+b8
q243	b1+b2+b3+b5+b6+b7+b8
q244	b1+b2+b4+b5+b6+b7+b8
q245	b1+b3+b4+b5+b6+b7+b8
q246	b2+b3+b4+b5+b6+b7+b8
q247	b1+b2+b3+b4+b5+b6+b7+b8

A.4 Πίνακας Παρουσίασης Ιδιοτήτων Συναρτήσεων

AA	algebric degree	nonlinearity	algebraic immunity
b1	6	64	3

b2	2	64	2
b3	2	64	2
b4	4	64	2
b5	2	64	2
b6	2	64	2
b7	5	64	3
b8	6	64	3
q1	4	64	3
q2	4	64	3
q3	3	64	2
q4	4	64	3
q5	4	96	3
q6	5	64	3
q7	6	96	4
q8	2	96	2
q9	4	64	2
q10	2	96	2
q11	2	96	2
q12	5	80	3
q13	6	76	4
q14	4	64	3
q15	2	64	2
q16	2	64	2
q17	5	96	3
q18	6	96	3
q19	4	96	3
q20	4	96	3
q21	5	64	3
q22	6	96	4
q23	2	96	2
q24	5	96	4
q25	6	64	3
q26	5	64	3
q27	6	80	3
q28	6	64	3
q29	4	64	3
q30	3	64	2
q31	4	64	3
q32	4	96	3
q33	5	80	3
q34	6	96	4
q35	3	96	3
q36	4	64	3
q37	4	96	3
q38	5	96	3
q39	6	96	4
q40	3	96	3

q41	3	96	3
q42	5	64	3
q43	6	96	4
q44	4	96	3
q45	5	96	4
q46	6	96	4
q47	5	64	3
q48	6	96	4
q49	6	96	4
q50	4	64	3
q51	2	96	2
q52	2	96	2
q53	5	96	3
q54	6	92	4
q55	4	96	3
q56	4	96	3
q57	5	96	4
q58	6	96	4
q59	2	112	2
q60	5	96	4
q61	6	76	4
q62	5	80	3
q63	6	84	4
q64	6	68	3
q65	4	96	3
q66	4	96	3
q67	5	96	4
q68	6	96	4
q69	2	96	2
q70	5	96	4
q71	6	96	3
q72	5	96	3
q73	6	80	3
q74	6	96	3
q75	4	112	3
q76	5	96	4
q77	6	96	4
q78	5	96	4
q79	6	100	4
q80	6	96	4
q81	5	96	4
q82	6	80	3
q83	6	64	3
q84	6	80	3
q85	3	96	3
q86	4	64	3
q87	4	96	3

q88	5	96	3
q89	6	96	4
q90	3	96	3
q91	3	96	3
q92	5	96	4
q93	6	96	4
q94	4	96	3
q95	5	96	4
q96	6	96	4
q97	5	80	3
q98	6	96	4
q99	6	96	4
q100	3	96	3
q101	3	96	3
q102	5	96	4
q103	6	108	4
q104	4	96	3
q105	5	96	4
q106	6	96	4
q107	5	96	3
q108	6	96	4
q109	6	96	4
q110	3	112	3
q111	5	96	4
q112	6	96	4
q113	5	96	4
q114	6	100	4
q115	6	96	4
q116	5	96	4
q117	6	96	4
q118	6	96	4
q119	6	96	4
q120	4	96	3
q121	4	96	3
q122	5	96	4
q123	6	96	4
q124	2	112	2
q125	5	96	4
q126	6	92	4
q127	5	96	3
q128	6	92	4
q129	6	92	3
q130	4	112	3
q131	5	96	4
q132	6	96	4
q133	5	64	3
q134	6	96	4

q135	6	96	4
q136	5	96	4
q137	6	84	4
q138	6	68	3
q139	6	92	4
q140	4	112	3
q141	5	96	4
q142	6	96	4
q143	5	96	4
q144	6	104	4
q145	6	96	4
q146	5	96	4
q147	6	80	3
q148	6	96	3
q149	6	80	3
q150	5	96	4
q151	6	100	4
q152	6	96	4
q153	6	104	4
q154	6	80	3
q155	3	96	3
q156	3	96	3
q157	5	96	4
q158	6	104	4
q159	4	96	3
q160	5	96	4
q161	6	96	4
q162	5	96	3
q163	6	96	4
q164	6	96	4
q165	3	112	3
q166	5	96	4
q167	6	96	4
q168	5	64	3
q169	6	96	4
q170	6	96	4
q171	5	96	4
q172	6	96	4
q173	6	96	4
q174	6	96	4
q175	3	112	3
q176	5	96	4
q177	6	108	4
q178	5	96	4
q179	6	104	4
q180	6	108	4
q181	5	96	4

q182	6	96	4
q183	6	96	4
q184	6	96	4
q185	5	96	4
q186	6	100	4
q187	6	96	4
q188	6	104	4
q189	6	96	4
q190	4	112	3
q191	5	96	4
q192	6	96	4
q193	5	96	4
q194	6	104	4
q195	6	96	4
q196	5	96	4
q197	6	92	4
q198	6	92	3
q199	6	92	4
q200	5	96	4
q201	6	96	4
q202	6	96	4
q203	6	96	4
q204	6	92	4
q205	5	96	4
q206	6	104	4
q207	6	96	4
q208	6	104	4
q209	6	80	3
q210	6	104	4
q211	3	112	3
q212	5	96	4
q213	6	104	4
q214	5	96	4
q215	6	104	4
q216	6	104	4
q217	5	96	4
q218	6	96	4
q219	6	96	4
q220	6	96	4
q221	5	96	4
q222	6	96	4
q223	6	96	4
q224	6	96	4
q225	6	96	4
q226	5	96	4
q227	6	104	4
q228	6	108	4

q229	6	104	4
q230	6	96	4
q231	6	104	4
q232	5	96	4
q233	6	104	4
q234	6	96	4
q235	6	104	4
q236	6	92	4
q237	6	96	4
q238	6	104	4
q239	5	96	4
q240	6	104	4
q241	6	104	4
q242	6	104	4
q243	6	96	4
q244	6	96	4
q245	6	104	4
q246	6	104	4
q247	6	104	4

Βιβλιογραφία

Federal Information Processing Standards Publication,. 2001. *Announcing the ADVANCED ENCRYPTION STANDARD (AES).* United States : United States National Institute of Standards and Technology (NIST), 2001.

A. Braeken and J. Lano. 2006. On the (Im)Possibility of Practical and Secure Nonlinear Filters and. *Selected Areas in Cryptography.* 2006.

A. Canteaut. 2016. *Lecture notes on Cryptographic Boolean Functions.* Pariw, France : s.n., 2016.

A. Canteaut. 2002. *On the correlations between a combining function and functions of fewer variables.* s.l. : Proceedings of the IEEE Information Theory Workshop, 2002. σσ. 78-81.

A. Canteaut, M. Videau. 2005. Symmetric Boolean functions. *IEEE Transactions on Information Theory.* 8, Aug 2005, 51, σσ. 2791-2811.

A. M. Youssef, G. Gong. 2001. Hyper-bent Functions',. *Advances in Cryptology.* 2001, σσ. 406-419.

A. Nordum. 2020. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. [συγγρ. βιβλίου] Amy Nordum. *IEEE Spectrum.* 2020.

A. Rueppel. 1986. *Analysis and Design of Stream Ciphers.* Berlin : Heidelberg: Springer-Verlag, 1986.

A. Rueppel. 1986. Linear Complexity and Random Sequences. *Advances in Cryptology.* 1986.

A. Salagean. 2005. On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two. *IEEE Transactions on Information Theory,.* Mar 2005, σσ. 1145-1150.

A.J. Menezes, S.A. Vanstone. 1996. Handbook of Applied Cryptography. *USA: CRC Press Inc.* 1st , 1996.

B. Lauder, K. G. Paterson. 2003. Computing the error linear complexity spectrum of a binary sequence of period 2/sup n/. *IEEE Transactions on Information Theory.* Jan 2003, σσ. 273-280.

B. Moeller. 2004. *Security of CBC Ciphersuites in SSL/TLS: Problems and Countermeasures.* 2004.

Babbage. 1990. On the relevance of the strict avalanche criterion. *Electronics Letters.* Mar 1990, σσ. 461-462.

C. Beierle, J. Jean, S. Kolbl, G. Leander, A. Moradi,T. Peyrin, Y. Sasaki, P. Sasdrich and S. Meng Sim. 2019. *SKINNY-AEAD and SKINNY-Hash.* SnT, University of Luxembourg, Luxembourg. 2019.

C. Ding, G. Xiao, W. Shan. 1991. The Stability Theory of Stream Ciphers. *Lecture Notes in Computer Science.* 1991.

C. Paar, J.Pelzl. 2010. *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlin : s.n., 2010.

C. Shannon. 1949. Bell System Technical Journal. *Communication Theory of Secrecy Systems.* 1949.

Commission of the European Communities. 2009. Internet of Things- An action plan for Europe. [συγγρ. βιβλίου] Commission of the European Communities. *Internet of Things- An action plan for Europe.* 2009.

D. Evans. 2011. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.* 2011.

D. Khang. 1963. *The Silicon Engine: A Timeline of Semiconductors in Computers.* 1963.

European Union. 2018. General Data Protection Regulation (GDPR) – Official Legal Text. [Ηλεκτρονικό] 25 May 2018. https://gdpr-info.eu/.

F. J. MacWilliams, N. J. A. Sloane. 1977. *The theory of error correcting codes.* North-Holland,Amsterdam: Elsevier : s.n., 1977.

F. Webster, E. Tavares. 1986. On the Design of S-Boxes. *Advances in Cryptology CRYPTO '85 Proceedings.* 1986, σσ. 523-534.

H. Niederreiter. 1999. Some Computable Complexity Measures for Binary Sequences. *Sequences and their Applications.* 1999.

H. Piper, F. Beker. 1982. *Cipher systems. The protection of communications.* London : Northwood Books, 1982.

IBM. 2016. https://www.IBM.com/blogs/internet-of-things/what-is-the-iot/. *What is the Internet of Things, and how does it work?* [Ηλεκτρονικό] 2016. [Παραπομπή: 17 1 2016.] https://www.IBM.com/blogs/internet-of-things/what-is-the-iot/.

Indian Business of Tech. 2016. How IoT's are Changing the Fundamentals of "Retailing". *Trak.in – Indian Business of Tech, Mobile & Startups.* 2016.

J. Gubbi, R. Buyya. Internet of Things (IoT): Future Generation Computer Systems. *Internet of Things (IoT): A vision, architectural elements, and future directions.*

J. L. Massey, D. J. Costello, and J. Justesen. 1973. Polynomial weights and code constructions. *IEEE.* Jan 1973, σσ. 101-110.

J. Lee. Roadmapping Workshop on Measurement Science for Prognostics and Health Management of Smart Manufacturing Systems Agenda. [συγγρ. βιβλίου] Jay Lee. *Keynote Presentation: Recent Advances and Transformation Direction of PHM.*

J. Massey. Jan. 1969. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory.* 1, Jan. 1969, Τόμ. 15.

J. Pieprzyk. Non-linearity of Exponent Permutations. *Advances in Cryptology.* s.l. : Proceedings of EuroCrypt'89, σ. 1989.

K. G. Paterson. 1994. Perfect maps. *IEEE Transactions on Information Theory.* 1994, Τόμ. 3, 40.

K. Gudeman. Next-Generation Internet of Battle things (IoBT) Aims to Help Keep Troops and Civilians Safe. [συγγρ. βιβλίου] Kim Gudeman. *ECE Illinois.*

K. Kurosawa, F. Sato, T. Sakata, W. Kishimoto. Mar 2000. A relationship between linear complexity. *IEEE Transactions on Information Theory.* 2, Mar 2000, 46.

K. Limniotis, N. Kolokotronis. 2019. *The error linear complexity spectrum as a cryptographic criterion of Boolean Functions.* s.l. : Submitted to IEEE Trans. Inform. Theory, 2019. σσ. 8345-8356. vol.65,no.12.

—. 2019. *The error linear complexity spectrum as a cryptographic criterion of Boolean Functions.* s.l. : Submitted to IEEE Trans. Inform. Theory, 2019.

L. Cameron. IEEE Computer Society. [συγγρ. βιβλίου] Lori Cameron. *"Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT".*

M. Aagaard, R. AlTawy, G. Gong,K. Mandal, and R. Rohit. 2019. *ACE: An Authenticated Encryption and Hash Algorithm.* Department of Electrical and Computer Engineering, University of Waterloo. Waterloo,CANADA : s.n., 2019.

M. Bilenko, R. J. Mooney, W. Cohen, P. Ravikumar, and S.E. Fienberg. April 2003. Adaptive Name Matching in Information Integration. *IEEE Intelligent Systems.* April April 2003, 18, σσ. 16-23.

M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος. 2011. *Σύγχρονη Κρυπτογραφία - Θεωρία και Εφαρμογές.* s.l. : Παπασωτηρίου, 2011.

M. Dworkin. 2001. *Recommendation for Block Cipher Modes of Operation.* s.l. : NIST, 2001.

M. Ersue, D. Romascanu,J. Schoenwaelder,A. Sehgal. 2014. IETF Internet Draft. [συγγρ. βιβλίου] M. Ersue, και συν. *Management of Networks with Constrained Devices: Use Cases.* 2014.

M. Matsui. 1994. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology.* s.l. : EUROCRYPT '93, 1994, σσ. 386-397.

M. Stamp, C. F. Martin. 1993. An algorithm for the k-error linear complexity of binary sequences with period 2/sup n/. *IEEE Transactions on Information Theory.* 4, 1993, 39.

M. Weiser. 1991. The Computer for the 21st Century. *The Computer for the 21st Century.* 1991, σσ. 94-104.

N. Dey, A. E. Hassanien. 2018. Springer International Publishing. *Internet of things and big data analytics toward next-generation intelligence.* 2018.

N. Tokareva. 2015. *Bent functions: results and applications to cryptography.* s.l. : Academic Press, 2015.

New Approaches to Stream Ciphers. **A. Rueppel. 1984.** Zurich : s.n., 1984. Swiss Federal Institute of Technology.

NIST. s.l. : NIST.

NIST Computer Security Division's (CSD) Security Technology Group(STG). 2012. Block cipher modes. [συγγρ. βιβλίου] NIST. *Cryptographic Toolkit.* 2012.

O. S. Rothaus. 1976. On "bent" functions. *Journal of Combinatorial Theory.* 3, May 1976, 20, σσ. 300-305.

P. Magrassi, T. Berg. 12 August 2002. A World of Smart Objects. *A World of Smart Objects.* 12 August 2002.

Piccolo: An ultralightweight ultralightweight. **K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai. 2011.** Nara, Japan : s.n., 2011. Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop.

R. Games, A. Chan. 1983. A fast algorithm for determining the complexity of a binary sequence. *IEEE Transactions on Information Theory.* 1, 1983, 29.

S. Li. 2017. Chapter 1: Introduction: Securing the Internet of Things. [συγγρ. βιβλίου] S. Li. *Securing the Internet of Things. Syngress.* 2017.

S.W. Golomb. 1981. *Shift Register Sequences.* Laguna, CA : USA:Aegean Par Press, 1981.

Sagemath. 2020. Copying.txt. [Ηλεκτρονικό] 2020. https://git.sagemath.org/sage.git/tree/COPYING.txt.

Scientific American. **Scientific American. April 2015.** April 2015. p.68.

T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, K. G. Paterson. 2009. Properties of the Error Linear Complexity Spectrum. *IEEE Transactions on Information Theory.* 10, 2009, 55.

T. Suzaki, K. Minematsu, S. Morioka, E. Kobayashi. 2012. *TWINE: A lightweight block cipher for multiple platforms.* s.l. : SAC, 2012.

T. W. Cusick, P. Stanica. 2017. Chapter 7 - Stream Cipher Design',. *Cryptographic Boolean Functions and Applications (Second Edition).* s.l. : Eds. Academic Press, 2017, σσ. 143-185.

V. Rijmen, J. Daemen. 2003. *AES Proposal: Rijndael.* s.l. : National Institute of Standards and Technology, 2003.

X. Liu, Y. Yang, K. R. Choo, H. Wang. 2018. Security and Privacy Challenges for Internet-of-Things and Fog Computing. *Wireless Communications and Mobile Computing.* 2018.