Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Σύγχρονες Επιθέσεις σε Κρυπταλγορίθμους Ροής: Κρυπτογραφικές Ιδιότητες Συναρτήσεων

Αλέξανδρος Μαγκούτης

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Αύγουστος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Σύγχρονες Επιθέσεις σε Κρυπταλγορίθμους Ροής: Κρυπτογραφικές Ιδιότητες Συναρτήσεων

Αλέξανδρος Μαγκούτης

Επιβλέπων Καθηγητής
Δρ. Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Αύγουστος 2014

Περίληψη

Οι κρυπταλγόριθμοι ροής μελετώνται εκτενώς τα τελευταία χρόνια μιας και μπορούν να χρησιμοποιηθούν σε πλήθος εφαρμογών (πχ. επικοινωνίες) λόγω της απλότητας υλοποίησης τους και της ταχύτητας τους έναντι άλλων γνωστών μεθόδων κρυπτογράφησης. Γενικότερα, το πιο σημαντικό χαρακτηριστικό για έναν αλγόριθμο κρυπτογράφησης είναι η ασφάλεια που παρέχει. Ωστόσο, υπάρχουν και άλλα επιθυμητά χαρακτηριστικά είναι η ταχύτητα, η κατανάλωση ισχύος και η απλότητα υλοποίησης – σε αυτά τα χαρακτηριστικά, οι κρυπταλγόριθμοι ροής πλεονεκτούν έναντι άλλων κρυπτογραφικών αλγορίθμων. Η ασφάλεια των κρυπτογραφικών αλγορίθμων ροής (stream ciphers) έγκειται σε μεγάλο βαθμό σε συγκεκριμένα χαρακτηριστικά που πρέπει να ικανοποιούν οι κρυπτογραφικές λογικές συναρτήσεις που υπεισέρχονται κατά την κατασκευή τους. Έχουν προταθεί διάφορες κατασκευές συναρτήσεων που να εξασφαλίζουν την ικανοποίηση πολλών κρυπτογραφικών κριτηρίων, ωστόσο το εν λόγω ερευνητικό πεδίο παραμένει ενεργό ιδίως ως προς την αντιμετώπιση σύγχρονων επιθέσεων όπως οι αλγεβρικές επιθέσεις (algebraic attacks). Στόχος είναι η κατασκευή συναρτήσεων με μέγιστη αλγεβρική ανθεκτικότητα (algebraic immunity) και ταυτόχρονη ικανοποίηση των υπολοίπων κρυπτογραφικών κριτηρίων οι οποίες θα μπορούν να χρησιμοποιηθούν από σύγχρονους κρυπταλγόριθμους ροής ως μη γραμμικά φίλτρα για τη δημιουργία ασφαλούς κλειδοροής.

Στην παρούσα εργασία πραγματοποιείται μία επισκόπηση των πλέον σημαντικών επιθέσεων που μπορούν να εφαρμοστούν σε κρυπταλγορίθμους ροής, καθώς και των αντίστοιχων ιδιοτήτων που πρέπει να ικανοποιεί μία συνάρτηση προκειμένου να αποτρέπονται οι επιθέσεις αυτές. Έμφαση θα δοθεί στο κριτήριο της αλγεβρικής ανθεκτικότητας των συναρτήσεων, το οποίο είναι πολύ σημαντικό γιατί χαρακτηρίζει το συνολικό κρυπτογραφικό σύστημα ως προς την ασφάλειά του έναντι των ισχυρών αλγεβρικών επιθέσεων. Γνωστές κατασκευές συναρτήσεων με τη μέγιστη δυνατή αλγεβρική ανθεκτικότητα μελετώνται ως προς άλλα κρυπτογραφικά κριτήρια, ενώ επίσης νέες συναρτήσεις, που δεν έχουν εξεταστεί μέχρι σήμερα, μελετώνται τόσο ως προς την αλγεβρική τους ανθεκτικότητα όσο και ως προς λοιπά κρυπτογραφικά κριτήρια. Από την ανάλυση αυτή – με χρήση εργαλείων λογισμικού όπως η γλώσσα R και το Matlab - διαφαίνονται αλληλοσυσχετίσεις και εξαρτήσεις μεταξύ των διαφόρων κρυπτογραφικών κριτηρίων των λογικών συναρτήσεων, ενώ επίσης προκύπτει ότι οι νέες συναρτήσεις μπορούν πράγματι να επιτύχουν σημαντικές κρυπτογραφικές ιδιότητες.

Summary

Stream ciphers are widely used in many applications, especially in those cases where high performance and low power dissipation are also needed – apart from security. Moreover, stream ciphers are in general simpler than block ciphers and can be implemented easily. Hence, using stream ciphers is the best choice for ensuring security in many important applications (e.g. wireless or mobile communications).

The security provided by stream ciphers mainly rests with the properties of the underlying Boolean functions that are used as "building blocks" of the cipher. Several cryptographic criteria of functions are known as prerequisites to thwart specific type of attacks; moreover, several constructions of cryptographically strong functions have been also proposed. However, there is still room for research in this area, owing to the fact that new types of attacks are mounted – like algebraic attacks that have been effectively mounted during the last decade. Hence, the ultimate goal is to construct functions achieving the maximum possible immunity against algebraic attacks, without sacrificing other cryptographic criteria.

This thesis studies the most common attacks on stream ciphers, focusing on the powerful class of algebraic attacks. Emphasis is also given on establishing the main cryptographic criteria that should be satisfied by any cryptographic function, in order to ensure tolerance against these attacks. A class of cryptographic functions that has been recently proposed in order to thwart algebraic attacks - the so-called Carlet-Feng function - is further examined with respect to other cryptographic criteria. Moreover, we study a new class of functions with regard to immunity against algebraic attacks, as well as with respect to other cryptographic measures. Experimental results via appropriate software tools (R, Matlab) exhibit that this new class of function may achieve nice cryptographic properties.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου, που είναι πάντα δίπλα μου και όλους τους καθηγητές μου στο Μεταπτυχιακό Πρόγραμμα Σπουδών «Πληροφοριακά και Επικοινωνιακά Συστήματα» του Ανοικτού Πανεπιστημίου Κύπρου. Ιδιαίτερα θα ήθελα να ευχαριστήσω τον επιβλέποντα της παρούσας Διπλωματικής Διατριβής, Δρ. Λιμνιώτη ο οποίος ως Καθηγητής – Σύμβουλος της Θεματικής Ενότητας «ΠΕΣ-621 Κρυπτογραφία» με ενέπνευσε να ασχοληθώ με το συγκεκριμένο θέμα.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Κάθε μέρα, εκατομμύρια άνθρωποι επικοινωνούν ηλεκτρονικά, είτε είναι μέσω ηλεκτρονικού ταχυδρομείου (e-mail) , είτε μέσω κινητών τηλεφώνων, είτε χρησιμοποιούν διάφορες υπηρεσίες, όπως τα ATM των τραπεζών. Σε όλες αυτές τις μορφές επικοινωνίας δεν υπάρχει «αποκλειστικής χρήσης» κανάλι μετάδοσης των δεδομένων. Όλα τα κανάλια επικοινωνίας, είτε είναι ο χαλκός των καλωδίων, είτε είναι η ατμόσφαιρα είναι κοινόχρηστα! Πως διασφαλίζεται η ασφάλεια των επικοινωνιών σε ένα τέτοιο περιβάλλον;

Η κρυπτογραφία είναι αυτή που εγγυάται στους χρήστες ασφαλείς συναλλαγές στον ηλεκτρονικό κόσμο. Μάλιστα η διαρκής αύξηση των πληροφοριών που διαβιβάζονται σε ηλεκτρονική μορφή έχει οδηγήσει σε αυξημένη εξάρτηση από την κρυπτογραφία, η οποία πλέον βρίσκεται σχεδόν σε όλες τις μορφές επικοινωνίας, συνήθως με τρόπο διαφανή προς τους χρήστες.

Η λέξη Κρυπτογραφία (Cryptography) είναι σύνθετη και αποτελείται από τα συνθετικά «κρυπτός» και «γράφω», γράφω δηλαδή κάτι με τέτοιο τρόπο, ώστε κάποιος που το διαβάζει να μην το καταλαβαίνει. Ένας σύγχρονος ορισμός είναι ο εξής: Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή.

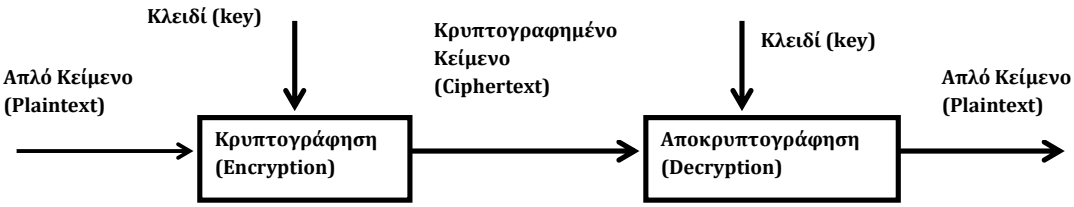
Αν και η χρήση της έχει ξεκινήσει από την αρχαιότητα (αντικατάσταση, αναδιάταξη χαρακτήρων) οι σύγχρονοι αλγόριθμοι κρυπτογράφησης διαφέρουν αρκετά ως προς την πολυπλοκότητα και τη συχνότητα χρήση τους. Οι βασικές αρχές που πρέπει να ακολουθούνται σε σύγχρονους κρυπταλγορίθμους διατυπώθηκαν το 1949 από τον Claude Shannon [32]. Στην εργασία αυτή η κρυπτογραφία μετατρέπεται σε αυστηρό επιστημονικό πεδίο, όπου ορίζεται η έννοια του κρυπτοσυστήματος και η απόλυτη ασφάλεια. Από τότε και σε συνδυασμό με την εξέλιξη των τηλεπικοινωνιών η έρευνα στο χώρο της κρυπτογραφίας είναι αλματώδης.

1.1 Σύγχρονοι αλγόριθμοι Κρυπτογράφησης

Στις μέρες μας η Κρυπτογραφία έχει αναχθεί σε επιστήμη, με τις εφαρμογές της διαρκώς να πληθαίνουν. Η κρυπτογραφία χρησιμοποιείται ως ένα χρήσιμο εργαλείο στην ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Οι κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δύο μεγάλες κατηγορίες, τους συμμετρικούς (symmetric) και τους ασύμμετρους (asymmetric) ή δημοσίου κλειδιού (public key).

1.2 Συμμετρικοί αλγόριθμοι κρυπτογράφησης

Στους αλγορίθμους αυτής της κατηγορίας χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση το οποίο συνήθως ονομάζεται «μυστικό κλειδί» (secret key). Το τυπικό σχήμα κρυπτογράφησης είναι το εξής:



Σχήμα 1.1: Συμμετρική κρυπτογράφηση

Αν E και D συμβολίζουν τις συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα, τότε ο μαθηματικός φορμαλισμός που τις περιγράφει είναι: $E_k(m)=c$ και $D_k(c)=m$, όπου m το αρχικό μήνυμα και c το κρυπτοκείμενο. Ο δείκτης k υποδηλώνει την εξάρτηση αυτών των δύο

συναρτήσεων από το ίδιο μυστικό κλειδί. Ουσιαστικά οι δύο αυτές συναρτήσεις είναι αντίστροφες και ισχύει $D_k(E_k(m)) = m$.

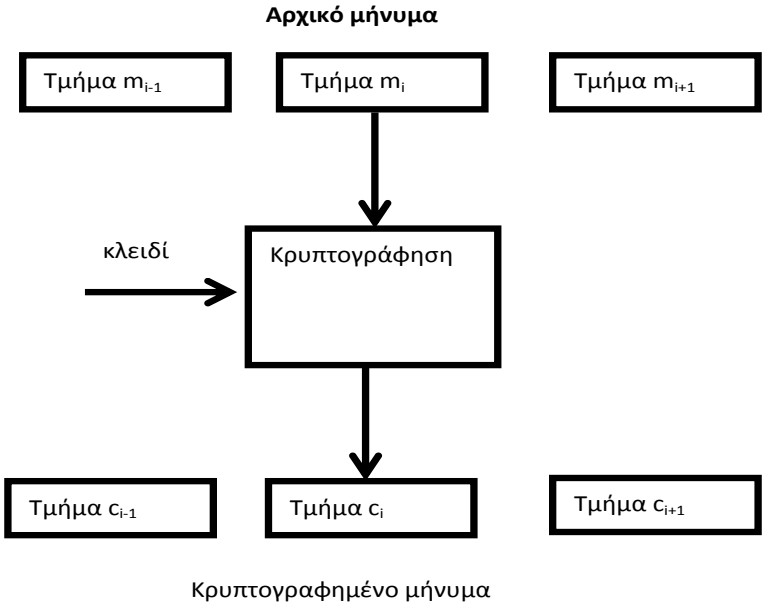
Όπως παρατηρούμε απαραίτητη προϋπόθεση για να αποκρυπτογραφηθεί το μήνυμα είναι να γνωρίζουν οι δύο συνδιαλεγόμενοι το μυστικό κλειδί. Αυτό εισάγει μια δυσκολία καθώς οι συνδιαλεγόμενοι συνήθως βρίσκονται σε πολύ μακρινές αποστάσεις και θα απαιτηθεί κάποια άλλη μέθοδος (την οποία θα δούμε παρακάτω) ώστε να γίνει η ανταλλαγή του μυστικού κλειδιού, καθώς θεωρούμε ότι το κανάλι επικοινωνίας είναι ανασφαλές.

Τους συμμετρικούς κρυπταλγορίθμους τους διακρίνουμε σε δύο κατηγορίες, τους αλγορίθμους ροής (stream ciphers) και τους αλγορίθμους τμήματος (block ciphers).

1.2.1 Αλγόριθμοι Τμήματος

Τα περισσότερα κρυπτογραφικά συστήματα χρησιμοποιούν συμμετρικούς αλγορίθμους τμήματος. Σε αυτούς τους αλγορίθμους, το αρχικό μήνυμα διαιρείται σε τμήματα σταθερού μήκους (πχ 128 bit) και το κάθε τμήμα κρυπτογραφείται ξεχωριστά. Γίνεται επαναληπτική εφαρμογή των ίδιων πράξεων (αντιμεταθέσεις, αντικαταστάσεις) χρησιμοποιώντας κάθε φορά μέρος του μυστικού κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round) και τα αποτελέσματα του κάθε γύρου μπορούν είτε απλά να συνθέσουν το κρυπτοκείμενο είτε να χρησιμοποιηθούν από τους επόμενους γύρους ώστε να επιτευχθεί μεγαλύτερη πολυπλοκότητα. Η δομή ενός κρυπταλγορίθμου τμήματος παρουσιάζεται στο Σχήμα 1.2.

Το1949 ο Claude Shannon εισήγαγε την ιδέα των δικτύων αντικατάστασης-μετάθεσης (substitution-permutation (S-P) networks) προκειμένου να παράγεται μία «ισχυρή» κρυπτογράφηση που δημιουργεί σύγχυση (confusion) και διάχυση (diffusion) στο αρχικό μήνυμα. Τα δίκτυα αυτά αποτελούν τη βάση πολλών μοντέρνων αλγορίθμων τμήματος (πχ DES).



Σχήμα 1.2: Δομή κρυπταλγορίθμου τμήματος

Το 1976 ο αλγόριθμος Lucifer της IBM ορίστηκε σαν πρότυπο κρυπτογράφησης με το όνομα DES (Data Encryption Standard) από το NIST (National Institute for Standards and Technology). Λόγω του μικρού μήκους κλειδιού που είχε (56 bit) αντικαταστάθηκε το 2000 από τον αλγόριθμο Rijndael, γνωστός ως AES (Advanced Encryption Standard). Ο αλγόριθμος AES έχει 10-15 γύρους ανάλογα με το μήκος του κλειδιού και σε κάθε γύρο λαμβάνουν χώρα οι εξής πράξεις: Αντικατάσταση byte (Byte substitution) με χρήση s-boxes , Ολίσθηση (Shift row), Συνδυασμός πολλών bit (Mix Column) και Πρόσθεση (XOR) του κλειδιού.
Οι αλγόριθμοι τμήματος θεωρούνται γενικότερα πιο ασφαλής από τους κρυπταλγορίθμους ροής γι αυτό το λόγο συνήθως προτιμούνται σε εφαρμογές όταν δε συντρέχουν οι «ειδικοί» λόγοι που θα αναφερθούν στην επόμενη ενότητα.
Άλλοι γνωστοί αλγόριθμοι αυτής της κατηγορίας είναι ο 3- DES, IDEA, Twofish.

1.2.2 Αλγόριθμοι Ροής

Οι κρυπταλγόριθμοι ροής είναι μια εξίσου πολύ σημαντική κατηγορία αλγορίθμων κρυπτογράφησης. Κρυπτογραφούν ξεχωριστούς χαρακτήρες (συνήθως δυαδικά ψηφία) ενός απλού κειμένου, έναν κάθε φορά, χρησιμοποιώντας ένα μετασχηματισμό ο οποίος διαφοροποιείται με το χρόνο, σε αντίθεση με τους αλγορίθμους τμήματος οι οποίοι, όπως είδαμε και πιο πάνω κρυπτογραφούν ολόκληρα τμήματα (block) του κειμένου χρησιμοποιώντας τον ίδιο μετασχηματισμό. Οι αλγόριθμοι ροής υλοποιούνται πολύ εύκολα σε υλικό (hardware) και

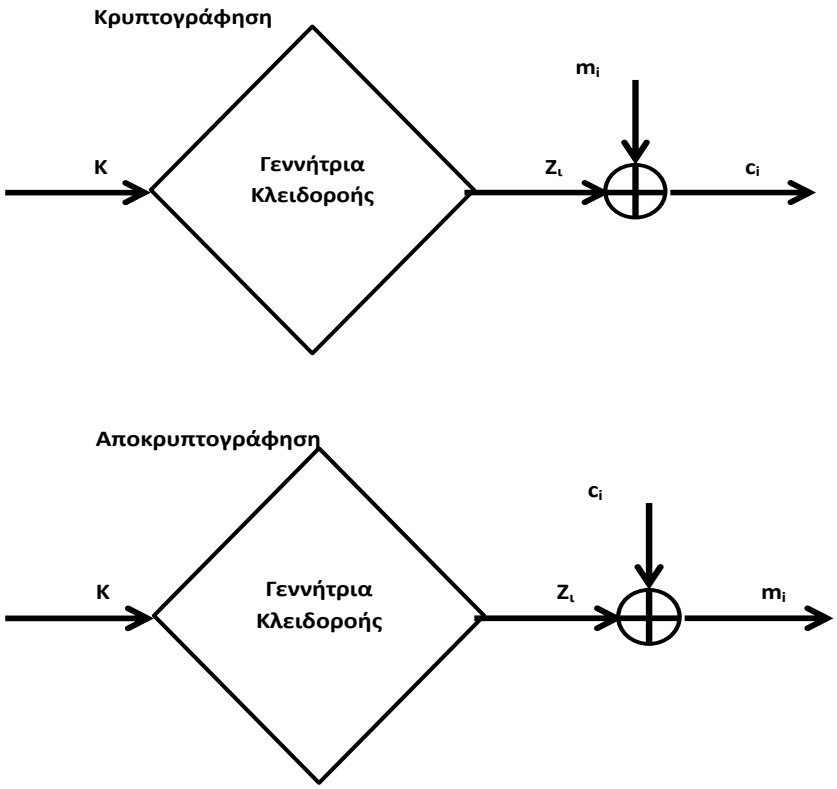
είναι ταχύτεροι από τους αλγορίθμους τμήματος. Λόγω της λειτουργίας τους είναι προτιμότεροι ή ακόμη και απαραίτητοι σε συγκεκριμένες εφαρμογές, όπως οι τηλεπικοινωνίες, στις οποίες απαιτείται μεγάλη ταχύτητα μετάδοσης, δεν υπάρχει δυνατότητα ενδιάμεσης αποθήκευσης (buffering) και οι χαρακτήρες πρέπει να κρυπτογραφούνται άμεσα μόλις παραλαμβάνονται. Ένα επίσης μεγάλο πλεονέκτημα είναι ότι δεν υπάρχει διάδοση σφάλματος, με άλλα λόγια, αν κάποιος χαρακτήρας παραληφθεί λάθος τότε θα κρυπτογραφηθεί και θα παραδοθεί λάθος μόνο ο συγκεκριμένος χαρακτήρας αλλά κανένας από τους επόμενους.

Υπάρχουν πολλοί και διάφοροι τρόποι σχεδιασμού αλγορίθμων ροής, αλλά κανένας μέχρι τώρα δεν έχει οριστεί ως διεθνώς αποδεκτό πρότυπο κρυπτογράφησης σε αντίθεση με τους block ciphers όπου για πλέον των δύο δεκαετιών υπήρξε ως πρότυπο ο αλγόριθμος DES, τον ακολούθησε ως πρότυπο ο AES (ο οποίος και παραμένει μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι αρκετοί κρυπταλγόριθμοι ροής χρησιμοποιούνται σε εμπιστευτικές εφαρμογές (πχ. στρατιωτικές επικοινωνίες) και ποτέ δεν έχουν δημοσιοποιηθεί οι λεπτομέρειες υλοποίησης τους. Αν και θεωρούνται λιγότερο ασφαλείς από τους αλγορίθμους τμήματος ,χρησιμοποιούνται ευρέος λόγω των πλεονεκτημάτων που παρουσιάζουν.

Η γενική δομή της λειτουργίας των προσθετικών αλγορίθμων ροής (additive stream ciphers), που είναι και η πιο απλή περίπτωση, παρουσιάζεται στο σχήμα 1.3.

Η κρυπτογράφηση γίνεται πάνω σε μια ροή από bits. Χρησιμοποιείται μια γεννήτρια ψευδοτυχαίας ακολουθίας bits (keystream generator) η οποία παράγει την κλειδοροή Z_i (keystream). Κάθε bit της κλειδοροής προστίθεται modulo 2 (πράξη XOR) σε ένα bit του αρχικού μηνύματος m_i και προκύπτει ένα ψηφίο κρυπτοκειμένου. Το μυστικό κλειδί K καθορίζει την αρχική κατάσταση της γεννήτριας της κλειδοροής. Η αποκρυπτογράφηση λόγω της πράξης XOR είναι το ίδιο απλή, κάθε bit της κλειδοροής προστίθεται mod 2 σε κάθε bit του κρυπτοκειμένου και δίνει το αρχικό μήνυμα!

Για την κρυπτογράφηση ισχύει: $c_i = z_i \oplus m_i$ και για την αποκρυπτογράφηση $m_i = z_i \oplus c_i$



Σχήμα 1.3: Λειτουργία κρυπταλγορίθμων ροής

Το πιο γνωστό μοντέλο αλγορίθμου ροής είναι το σημειωματάριο μιας χρήσης (one-time pad) ή αλγόριθμος Vernam [35] στον οποίο χρησιμοποιείται μια τυχαία ακολουθία bits (κλειδοροή) η οποία προστίθεται (XOR) στα bits του αρχικού μηνύματος. Βασικές προϋποθέσεις είναι η απόλυτη τυχαιότητα της κλειδοροής καθώς και το μέγεθός της να είναι ίσο με το μέγεθος του μηνύματος. Ο Shannon [33] απέδειξε ότι ο αλγόριθμος του Vernam είναι απεριόριστα ασφαλής, υπό την έννοια ότι αν κάποιος γνωρίζει το κρυπτοκείμενο δεν μπορεί να αντλήσει απολύτως καμία πληροφορία για το αρχικό μήνυμα. Αν και είναι ιδανικός αλγόριθμος κρυπτογράφησης στην πράξη δεν μπορεί να εφαρμοστεί καθώς για μεγάλα μηνύματα απαιτούνται εξίσου μεγάλα κλειδιά με αποτέλεσμα τη δύσκολη ανταλλαγή τους, επιπλέον, δεν μπορούν να παραχθούν, από υπολογιστικά συστήματα, απόλυτα τυχαίες ακολουθίες (παρά μόνο ακολουθίες που προσομοιάζουν την τυχαία συμπεριφορά – ψευδοτυχαίες).

Όλοι οι αλγόριθμοι ροής σχεδιάζονται με τέτοιο τρόπο ώστε να προσομοιάζουν τη λειτουργία του αλγορίθμου του Vernam.

Οι αλγόριθμοι ροής χρησιμοποιούνται σε πλήθος εφαρμογών τη σημερινή εποχή. Οι σημαντικότεροι είναι οι εξής:

- Ο RC4 σε πληθώρα εφαρμογών, όπως το πρωτόκολλο SSL/TLS, στην ασύρματη μετάδοση (Wi-Fi) στα πρωτόκολλα WEP, WPA, στο πρωτόκολλο κρυπτογράφησης του BitTorrent, προαιρετικά στο Kerberos. [36]
- Ο A5/1 χρησιμοποιείται στο σύστημα GSM της κινητής τηλεφωνίας.[01]
- Ο E0 χρησιμοποιείται στο πρωτόκολλο Bluetooth.
- Διάφοροι «μυστικοί» αλγόριθμοι σε στρατιωτικές εφαρμογές.

Επίσης σημαντικοί αλγόριθμοι αυτής της κατηγορίας είναι οι:

- Κατάλληλοι για software: HC-128, Rabbit, Salsa20/12, SOSEMANUK
- Κατάλληλοι για hardware: Grain v1, MICKEY 2.0, Trivium

1.3 Ασύμμετροι αλγόριθμοι κρυπτογράφησης

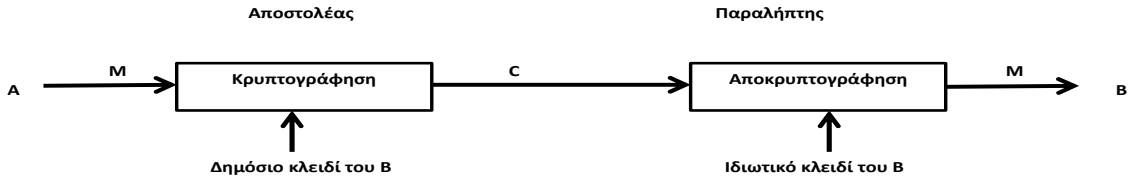
Ανεξάρτητα από τις σχεδιαστικές λεπτομέρειες όλοι οι συμμετρικοί αλγόριθμοι κρυπτογράφησης (τμήματος και ροής) έχουν μια σημαντική προϋπόθεση για την επίτευξη της μυστικότητας, το μυστικό κλειδί θα πρέπει να το γνωρίζουν ο αποστολέας, ο παραλήπτης και κανείς άλλος. Το πρόβλημα που προκύπτει είναι το πως θα καταφέρει ο αποστολέας με τον παραλήπτη να ανταλλάξουν μεταξύ τους το μυστικό κλειδί, χωρίς αυτό να διαρρεύσει σε τρίτους, δεδομένης της φυσικής απόστασης που συχνά υπάρχει μεταξύ τους (πχ. αγορά αγαθών μέσω διαδικτύου) .

Το 1976 προτάθηκε από τους W.Diffie και M.Hellman μια κρυπτογραφική μέθοδος διαφορετικής λογικής από τα συμμετρικά κρυπτοσυστήματα. Το μοντέλο αυτό ονομάζεται κρυπτογραφία Δημοσίου Κλειδιού ή Ασύμμετρη Κρυπτογραφία (asymmetric key cryptography). [10] Στην ασύμμετρη κρυπτογραφία κάθε χρήστες έχει ένα ζευγάρι κλειδιών e και d κατάλληλα επιλεγμένα έτσι ώστε το ένα αντιστρέφει το άλλο. Το ένα από τα δύο (e) είναι διαθέσιμο σε όλους και ονομάζεται δημόσιο κλειδί ενώ το άλλο παραμένει μυστικό (d) και ονομάζεται ιδιωτικό κλειδί. Απαραίτητη προϋπόθεση για την ασφάλεια του συστήματος είναι η γνώση του δημοσίου κλειδιού να μη μπορεί να οδηγήσει στην εύρεση του ιδιωτικού κλειδιού. Αν το μυστικό κλειδί διαρρεύσει ο αλγόριθμος είναι ανασφαλής πλέον και θα πρέπει να δημιουργηθεί άλλο ζεύγος κλειδιών.

Όταν αναφερόμαστε σε κρυπτοσύστημα δημόσιου κλειδιού, χρησιμοποιούμε τον όρο «ιδιωτικό κλειδί», για να αναφερθούμε στη μυστική ποσότητα που δεν είναι γνωστή στο ευρύτερο κοινό και ειδικότερα στον επιτιθέμενο. Αυτός ο όρος χρησιμοποιείται για λόγους διάκρισης από τα

συμμετρικά κρυπτοσυστήματα, όπου η μυστική ποσότητα αναφέρεται ως «μυστικό κλειδί». Σε ένα ασύμμετρο κρυπτοσύστημα ο αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο αποκρυπτογράφησης, με τη μόνη διαφορά ότι κατά την αποκρυπτογράφηση χρησιμοποιείται το αντίστοιχο κλειδί. [38]

Ο τρόπος λειτουργίας των κρυπτοσυστημάτων δημοσίου κλειδιού φαίνεται στο σχήμα 1.4:



Σχήμα 1.4: Αλγόριθμος Δημοσίου κλειδιού

Όταν κάποιος αποστολέας Α θέλει να στείλει ένα μήνυμα σε κάποιο παραλήπτη Β τότε θα κρυπτογραφήσει το μήνυμα Μ με το δημόσιο κλειδί του Β (το οποίο είναι ευρέως γνωστό σε όλους, άρα διαθέσιμο και στον Α) και θα δημιουργηθεί το κρυπτοκείμενο C. Στη συνέχεια το κρυπτοκείμενο θα αποσταλεί μέσω (του ανασφαλούς) καναλιού επικοινωνίας και θα φτάσει στον παραλήπτη Β ή/και σε κάποιον υποκλοπέα. Το κρυπτοκείμενο θα μπορεί να αποκρυπτογραφηθεί μόνο από τον κάτοχο του ιδιωτικού κλειδιού, δηλαδή τον Β.

Η ασύμμετρη κρυπτογραφία απαιτεί περισσότερους πόρους και χρόνο από τη συμμετρική. Στην πράξη σήμερα εφαρμόζεται συνδυασμός των δύο μεθόδων (πχ. πρωτόκολλο SSL/TLS). Με χρήση κρυπτογραφίας δημοσίου κλειδιού γίνεται ανταλλαγή του μυστικού κλειδιού και όχι όλων των μηνυμάτων, αίροντας το πρόβλημα της διανομής κλειδιού των συμμετρικών αλγορίθμων. Στη συνέχεια το μυστικό αυτό κλειδί θα χρησιμοποιηθεί μεταξύ των επικοινωνούντων για την υπόλοιπη συνομιλία με κάποιο γνωστό συμμετρικό αλγόριθμο.

Ένα ακόμη πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι η δημιουργία ψηφιακών υπογραφών διασφαλίζοντας την αυθεντικοποίηση του αποστολέα και την ακεραιότητα του μηνύματος. Η ψηφιακή υπογραφή είναι ένα σύνολο χαρακτήρων (string of data) και δημιουργείται από ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί του υπογράφοντα χρησιμοποιείται για να επαληθευθεί ότι η υπογραφή δημιουργήθηκε χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί. Η ψηφιακή υπογραφή δημιουργείται κατά τέτοιο τρόπο, ώστε να είναι αδύνατο να παραχθεί και

πάλι η ίδια ψηφιακή υπογραφή, χωρίς τη γνώση του ιδιωτικού κλειδιού. Η αυθεντικοποίηση του συνόλου των χαρακτήρων, είναι μία διεργασία με την οποία ο παραλήπτης ενός μηνύματος μπορεί να βεβαιωθεί για την πηγή προέλευσης του μηνύματος.

Ο πιο γνωστός και ευρέως χρησιμοποιούμενος αλγόριθμος αυτής της κατηγορίας είναι ο αλγόριθμος RSA, ο οποίος πήρε το όνομά του από τους εμπνευστές του Rivest, Shamir, Adleman. [28] Χρησιμοποιείται τόσο για κρυπτογράφηση, όσο και για δημιουργία ψηφιακής υπογραφής και είναι ο βασικός αλγόριθμος δημοσίου κλειδιού του πρωτοκόλλου SSL/TLS.

1.4 Αντικείμενο και Δομή της Διατριβής

Η παρούσα διπλωματική διατριβή εντάσσεται στο χώρο της συμμετρικής κρυπτογραφίας και πιο συγκεκριμένα στους αλγορίθμους ροής. Όπως ήδη έχουμε δει οι κρυπταλγόριθμοι ροής είναι αρκετά απλοί στην κατασκευή τους και η ασφάλειά τους βασίζεται στις ιδιότητες της παραγόμενης κλειδοροής. Η παραγόμενη κλειδοροή είναι κατάλληλη προς χρήση σε κρυπτογραφικές εφαρμογές μόνον εάν είναι δυσδιάκριτη ως προς μια τυχαία ακολουθία, δηλ. είναι υπολογιστικά αδύνατη η εύρεση της αντίστοιχης απλής της περιγραφής. Ο βαθμός τυχαιότητας δοθείσας κλειδοροής αποτιμάται μέσω της ικανοποίησης ενός μεγάλου αριθμού (πιθανώς αντικρουόμενων) κρυπτογραφικών κριτηρίων που θα αναλυθούν στην επόμενη ενότητα. Ακόμα όμως και αν η παραγόμενη κλειδοροή παρουσιάζει χαρακτηριστικά τυχαιότητας, η ασφάλεια του αλγορίθμου μπορεί να πληγεί αν η γεννήτρια της κλειδοροής δεν εμφανίζει κάποια συγκεκριμένα κρυπτογραφικά χαρακτηριστικά. Αυτό είναι και το βασικό αντικείμενο που πραγματεύεται η παρούσα διατριβή, αφού μελετώνται τα κύρια κρυπτογραφικά χαρακτηριστικά που πρέπει να έχουν οι συναρτήσεις οι οποίες υπεισέρχονται στην κατασκευή μιας γεννήτριας κλειδοροής.

Η δομή της διατριβής , όπως διαρθρώνεται ανά κεφάλαιο είναι η ακόλουθη:
Στο **κεφάλαιο 2** παρουσιάζονται οι επιθυμητές ιδιότητες των κρυπτογραφικών συναρτήσεων (nonlinearity, correlation immunity, algebraic immunity), οι οποίες προκύπτουν ως αναγκαία προϋπόθεση για την αντιμετώπιση γνωστών επιθέσεων (Berlekamp-Massey, επιθέσεις συσχέτισης κτλ.).
Στο **κεφάλαιο 3** περιγράφονται εκτενώς οι αλγεβρικές επιθέσεις (algebraic attacks) και οι γρήγορες αλγεβρικές επιθέσεις (fast algebraic attacks), οι οποίες αποτελούν ένα πιο πρόσφατο είδος επιθέσεων που παραμένει μέχρι σήμερα εξαιρετικά ενεργός ερευνητικός χώρος.

Παρουσιάζονται οι γνωστές κατασκευές συναρτήσεων με μέγιστη ανθεκτικότητα σε αλγεβρικές επιθέσεις (algebraic immunity) και αναφέρονται επιτυχείς αλγεβρικές επιθέσεις σε πραγματικά συστήματα (Toyocrypt).

Στο **κεφάλαιο 4** γίνεται μελέτη των κρυπτογραφικών ιδιοτήτων συγκεκριμένων συναρτήσεων. Για το σκοπό αυτό θα χρησιμοποιείται η γλώσσα προγραμματισμού R και το πακέτο Boolfun, ενώ για τις γρήγορες αλγεβρικές επιθέσεις (fast algebraic attacks) χρησιμοποιήθηκε το λογισμικό FAA Equation Finder του Simon Fischer (το οποίο, κατά την εκπόνηση της διατριβής, ήταν διαθέσιμο στην προσωπική του σελίδα). Θα μελετηθεί το πώς συμπεριφέρονται συναρτήσεις με συγκεκριμένη δομή ως προς την αλγεβρική πολυπλοκότητα, ενώ επίσης θα ελεγχθεί για πρώτη φορά μία συγκεκριμένη οικογένεια συναρτήσεων με χαρακτηριστική δομή.

Τέλος στο **κεφάλαιο 5** γίνεται η σύνοψη των αποτελεσμάτων.

Κεφάλαιο 2
Κρυπτογραφικές Ιδιότητες Συναρτήσεων

Η ασφάλεια ενός αλγορίθμου ροής – και, κατ' επέκταση, του κρυπτοσυστήματος που τον περιέχει - έγκειται στην ψευδοτυχαιότητα της παραγόμενης κλειδοροής. Βασικός στόχος είναι η γεννήτρια κλειδοροής να παράγει ακολουθία k με ευαπόδεικτες ιδιότητες που αφορούν κριτήρια όπως η περιοδικότητα, πολυπλοκότητα υλοποίησης, βαθμός γραμμικότητας και καλά στατιστικά χαρακτηριστικά.

2.1 Ψευδοτυχαίες ακολουθίες

Ορισμός 2.1: Η γεννήτρια τυχαίων ακολουθιών (*random bit generator)* είναι μια συσκευή ή ένας αλγόριθμος που παράγουν μια ακολουθία με στατιστικά ανεξάρτητα δυαδικά ψηφία.
Πρακτικά η δημιουργία και χρήση τυχαίων ακολουθιών δεν είναι αποδοτική σε περιβάλλοντα κρυπτοσυστημάτων. Η λύση σε αυτό είναι η χρήση γεννητριών ψευδοτυχαίων ακολουθιών.

Ορισμός 2.2: Η γεννήτρια ψευδοτυχαίων ακολουθιών (pseudorandom bit generator –PRBG) είναι ένας ντετερμινιστικός αλγόριθμος ο οποίος παίρνοντας μια τυχαία ακολουθία μήκους k παράγει μια ακολουθία μήκους l>>k η οποία «μοιάζει» τυχαία. Η είσοδος στον PRBG αλγόριθμο ονομάζεται σπόρος (seed) ενώ η έξοδος ψευδοτυχαία ακολουθία.
Η παραγόμενη ακολουθία δεν είναι τυχαία. Στόχος είναι δυσδιάκριτη αναγνώριση μιας ψευδοτυχαίας ακολουθίας από μια πραγματικά τυχαία.

Ορισμός 2.3 : Μια ακολουθία αριθμών είναι ψευδοτυχαία όταν:

- περνά όλους τους γνωστούς στατιστικούς ελέγχους περί τυχαιότητας (στατιστική απαίτηση).
- η ακολουθία είναι απρόβλεπτη, δηλαδή δοθέντος ενός τμήματος της ακολουθίας αυτής είναι υπολογιστικά αδύνατο για τον αντίπαλο να καθορίσει τον αμέσως επόμενο αριθμό (κρυπτογραφική απαίτηση).

Στην κρυπτογραφία μας ενδιαφέρει περισσότερο η αξιόπιστη παραγωγή «τυχαίων» ακολουθιών. Στους κρυπταλγόριθμους ροής, η γεννήτρια κλειδοροής θα πρέπει να βασίζεται σε γεννήτρια ψευδοτυχαίων ακολουθιών μιας και πραγματικά τυχαίες ακολουθίες δεν μπορούν να αναπαραχθούν δεύτερη φορά.
Ποιες όμως ακολουθίες θεωρούνται «τυχαίες» και κατ' επέκταση κατάλληλες για χρήση σε αλγορίθμους ροής; Τα 3 πρώτα κριτήρια προτάθηκαν από τον Golomb [13]. Θεωρώντας ότι η ακολουθία είναι δυαδική, δηλαδή, αποτελείται από τα ψηφία 0 και 1 , θα πρέπει να πληρεί τα παρακάτω κριτήρια:

1. Το πλήθος των ψηφίων 0 θα πρέπει να είναι ίσο με το πλήθος των ψηφίων 1 ή να διαφέρει κατά ένα. (Balance property)
2. Αν ως διαδρομή (run) ορίζουμε ένα τμήμα οσοδήποτε μήκους μίας ακολουθίας που αποτελείται μόνο από μηδενικά ή μόνο από άσους, τότε σε μία περίοδο οι μισές διαδρομές έχουν μήκος 1, το ¼ των διαδρομών έχουν μήκος 2, το 1/8 μήκος 3 κ.ο.κ. Η ισχύς της συνθήκης εξετάζεται όσο ο αριθμός των διαδρομών είναι μεγαλύτερος ή ίσος από 2l, όπου l το μήκος της διαδρομής. (run property)
3. Η συνάρτηση αυτοσυσχέτισης $C(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i \oplus a_{i+\tau}}$,για την ακολουθία $a_0 a_1 \ldots$ περιόδου N μπορεί να πάρει μόνο δύο τιμές: να είναι σταθερή (ίση με K) για $\tau \neq 0$, και τιμή N για $\tau=0$. (two-level autocorrelation property)

Για κάποια χρόνια θεωρήθηκε ότι κάθε ακολουθία μεγάλης περιόδου N που πληρεί τα κριτήρια τυχαιότητας του Golomb είναι μία κρυπτογραφικά ισχυρή ακολουθία. Πλέον μία γεννήτρια κλειδοροής θεωρείται κρυπτογραφικά ισχυρή αν οι ακολουθίες που παράγει «περνάνε επιτυχώς» τα τεστ τυχαιότητας που έχει θέσει ο NIST. (NIST SP 800-22) [30]

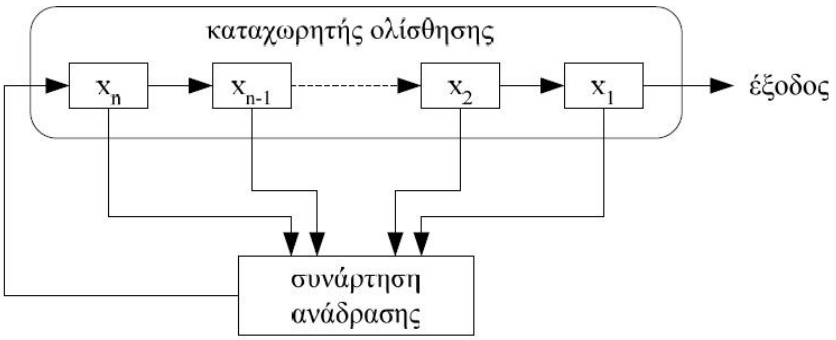
2.2 Γεννήτριες Ψευδοτυχαίων Ακολουθιών

Υπάρχουν διάφορες υλοποιήσεις γεννητριών ψευδοτυχαίων ακολουθιών. Στην παρούσα Διπλωματική Διατριβή θα ασχοληθούμε με τους Γραμμικούς Καταχωρητές Ολίσθησης με Ανάδραση (Linear Feedback Shift Registers- LFSR) οι οποίοι έχουν πολλά ενδιαφέροντα και επιθυμητά χαρακτηριστικά.

2.2.1 Γραμμικοί Καταχωρητές Ολίσθησης με Ανάδραση

Οι καταχωρητές ολίσθησης (shift registers) ανήκουν στην κατηγορία των μηχανών πεπερασμένης κατάστασης (finite state machines). Μια μηχανή πεπερασμένης κατάστασης ορίζεται ως η συσκευή η ο οποία αποτελείται από έναν πεπερασμένο αριθμό καταστάσεων όπου η μεταπήδηση από τη μια κατάσταση στην άλλη ορίζεται από την υπάρχουσα κατάσταση και την είσοδο. Η είσοδος ορίζεται ως μια ακολουθία από ένα πεπερασμένο σύνολο στοιχείων. Η έξοδος μιας μηχανής πεπερασμένης κατάστασης είναι μια ακολουθία από ένα πεπερασμένο σύνολο στοιχείων.

Οι καταχωρητές ολίσθησης με ανάδραση είναι αυτοί των οποίων η έξοδος τροφοδοτείται από μια συνάρτηση της οποίας το αποτέλεσμα τροφοδοτείται με τη σειρά του στην είσοδο του καταχωρητή, όπως φαίνεται στο σχήμα 2.1.



Σχήμα 2.1: Γραμμικός καταχωρητής ολίσθησης με ανάδραση

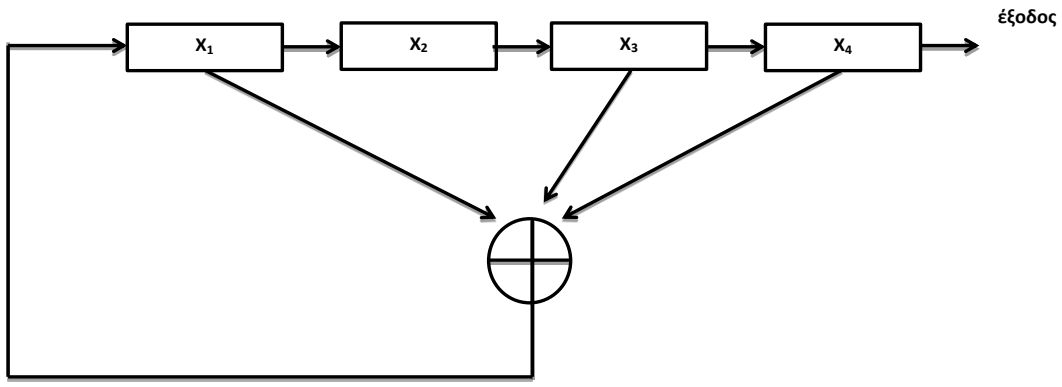
Έστω $f:\{0,1\}^n \rightarrow \{0,1\}$ η συνάρτηση ανάδρασης. Αν η f μπορεί να εκφραστεί με τη μορφή:

$$f(x_1, x_2, \ldots, x_n) = c_1x_1 + c_2x_2 + \ldots + c_nx_n \mod 2,$$

όπου οι σταθερές c_i είναι 0 ή 1, η συνάρτηση είναι γραμμική, και η αντίστοιχη γεννήτρια ονομάζεται καταχωρητής ολίσθησης με γραμμική ανάδραση (linear feedback shift register-LFSR). Οι LFSR χρησιμοποιούνται στις πιο πολλές γεννήτριες κλειδοροής που έχουν προταθεί. Οι λόγοι είναι οι εξής:

- Έχουν μελετηθεί εκτενώς, έχουν καλή μαθηματική περιγραφή και οι ιδιότητές τους αναλύονται εύκολα.
- Μπορούν να παράγουν ακολουθίες μέγιστης περιόδου. Η μέγιστη περίοδος ενός καταχωρητή με μνήμη n bits είναι ίση με 2^n-1 (εξαιρείται η κατάσταση όπου όλα τα x_i είναι μηδενικά).
- Μπορούν να παράγουν ακολουθίες με καλά στατιστικά χαρακτηριστικά που ικανοποιούν πάντα και τα 3 κριτήρια τυχαιότητας του Golomb.
- Είναι εύκολα υλοποιήσιμοι σε υλικό (hardware).

Ο LFSR είναι ένα ψηφιακό κύκλωμα, που αποτελείται από N βαθμίδες (θέσεις μνήμης). Το περιεχόμενο κάθε μιας είναι είτε 0 είτε 1. Η συνάρτηση ανάδρασης είναι μια πύλη XOR (πρόσθεση $\oplus$ ή mod2), η οποία έχει ως εισόδους κάποιες από τις βαθμίδες του LFSR (μπορεί να είναι οποιεσδήποτε και οσεσδήποτε).



Σχήμα 2.2: Γραμμικός Καταχωρητής Ολίσθησης με Ανάδραση - LFSR

Το σύνολο των τιμών των βαθμίδων του LFSR σε κάθε χρονική στιγμή ονομάζεται κατάσταση (state) του LFSR. Κάθε χρονική στιγμή, η κατάσταση του LFSR μεταβάλλεται με την ενεργοποίηση του παλμού του ρολογιού (clock) του συστήματος. Σε κάθε νέα κατάσταση:

- Η τιμή της πρώτης βαθμίδας του LFSR προκύπτει από τις τιμές της προηγούμενης κατάστασης, βάσει της πρόσθεσης XOR που υλοποιεί ο LFSR.

- Οι τιμές των άλλων βαθμίδων προκύπτουν από ολίσθηση προς τα δεξιά των τιμών όλων των βαθμίδων της προηγούμενης κατάστασης.

Όπως ήδη είπαμε, ένας LFSR μήκους N μπορεί να διέλθει το πολύ από 2^N -1 διαφορετικές καταστάσεις, επομένως μπορεί να παράγει ακολουθίες με μέγιστη δυνατή περίοδο 2^N -1. Οι LFSRs που επιτυγχάνουν τη μέγιστη δυνατή περίοδο ονομάζονται πρωταρχικοί (primitive), ενώ οι ακολουθίες που παράγονται από τέτοιους καταχωρητές ονομάζονται ακολουθίες μέγιστου μήκους (maximal-length sequences ή m-sequences). Το αν κάποιος LFSR είναι πρωταρχικός εξαρτάται αποκλειστικά από την ανάδραση.

Κάθε LFSR, ανάλογα με την ανάδρασή του, περιγράφεται μονοσήμαντα από ένα συγκεκριμένο πολυώνυμο μιας μεταβλητής (με συντελεστές 0,1) που ονομάζεται χαρακτηριστικό πολυώνυμο του LFSR. Ένας LFSR μεγέθους N είναι πρωταρχικός αν και μόνο αν το χαρακτηριστικό του πολυώνυμο είναι πρωταρχικό (primitive) στο πεπερασμένο σώμα GF(2^N).

Γνωρίζοντας ήδη ποια πολυώνυμα είναι πρωταρχικά, μπορούμε πολύ εύκολα να κατασκευάσουμε πρωταρχικούς LFSRs οποιουδήποτε μήκους N και επομένως και ακολουθίες μεγίστου μήκους 2^{N-1} .

2.2.2 Ασφάλεια που παρέχουν οι LFSRs.

Όπως ήδη είδαμε οι LFSRs έχουν χαρακτηριστικά που τους κάνουν ελκυστικούς για χρήση σε κρυπτογραφικές υλοποιήσεις με σημαντικότερα την εύκολη υλοποίηση και την παραγωγή ακολουθιών με μεγάλη περίοδο και καλά χαρακτηριστικά τυχαιότητας. Παρόλα αυτά όμως και λόγω της απλότητας των προσθετικών αλγορίθμων ροής (πράξη mod2 κάθε bit μηνύματος με ένα bit κλειδοροής) δεν μπορούν να χρησιμοποιηθούν απευθείας σε κρυπτογραφικές συναρτήσεις καθώς θα καταστήσει τον κρυπτογραφικό αλγόριθμο ευάλωτο σε επιθέσεις τύπου γνωστού μηνύματος (known-plaintext). Αν ξέρουμε ένα κομμάτι του αρχικού μηνύματος και το αντίστοιχο κρυπτοκείμενο τότε μπορούμε μα βρούμε κάποια bits της κλειδοροής , δηλαδή την τρέχουσα κατάσταση του LFSR! Αυτό υπό προϋποθέσεις θα μπορούσε να μας οδηγήσει σε αποκρυπτογράφηση όλου του μηνύματος!

Μια ακολουθία οποιουδήποτε μεγέθους $k_0k_1k_2$… μπορεί να παραχθεί από πολλούς διαφορετικούς LFSR. Για μία δοθείσα ακολουθία, το μέγεθος του μικρότερου LFSR που την παράγει ονομάζεται γραμμική πολυπλοκότητα (linear complexity) της ακολουθίας. Προφανώς, για κάθε ακολουθία μεγίστου μήκους περιόδου 2^N-1, η γραμμική της πολυπλοκότητα είναι N αφού ο LFSR που την παράγει είναι N βαθμίδων.

Ο αλγόριθμος Berlekamp-Massey [21], δοθείσης μιας ακολουθίας, υπολογίζει όχι μόνο τη γραμμική της πολυπλοκότητα αλλά και τον μικρότερο LFSR που την παράγει. Μάλιστα αν η περίοδος μίας ακολουθίας είναι N και η γραμμική της πολυπλοκότητα είναι L<N/2, τότε ο μικρότερος LFSR μήκους L που την παράγει είναι μοναδικός! Αυτό πρακτικά σημαίνει ότι για να υπολογιστεί ο μοναδικός αυτός LFSR με το μικρότερο μέγεθος χρησιμοποιώντας τον αλγόριθμο Berlekamp-Massey, αρκεί να γνωρίζουμε οποιαδήποτε 2L διαδοχικά bits της ακολουθίας. Η παρατήρηση αυτή έχει εξαιρετική σημασία από τη σκοπιά της κρυπτανάλυσης, διότι συνεπάγεται ότι γνωρίζοντας 2L διαδοχικά bits μπορούμε να βρούμε τη γεννήτρια όλης της ακολουθίας, δηλαδή ολόκληρη την ακολουθία ! Συνεπώς, έχοντα στα χέρια μας την κλειδοροή, μπορεί πλέον να αποκρυπτογραφηθεί όλο το μήνυμα.

Τα συμπεράσματα που προκύπτουν είναι τα εξής:

1. Μία ακολουθία για να χρησιμοποιηθεί ως κλειδί στην κρυπτογραφία, πρέπει να έχει όσο γίνεται υψηλότερη γραμμική πολυπλοκότητα και
2. Οι LFSRs **δεν είναι κατάλληλοι** από μόνοι τους για την παραγωγή κλειδοροής. Θα πρέπει να χρησιμοποιηθούν σε συνδυασμό με πιο σύνθετες δομές.

2.2.3 Παραγωγή ακολουθιών μεγάλης πολυπλοκότητας

Στην προηγούμενη ενότητα επισημάνθηκε η ανάγκη για υψηλή γραμμική πολυπλοκότητα λόγω του αλγορίθμου Berlekamp- Massey. Μια μέθοδος να αυξηθεί η γραμμική πολυπλοκότητα είναι να χρησιμοποιηθούν παράλληλα με κάποιον LFSR άλλες, μη γραμμικές, διατάξεις.

Ορισμός 2.4: Μία λογική συνάρτηση n μεταβλητών είναι μία έκφραση της Άλγεβρας Boole που περιλαμβάνει τις n μεταβλητές εισόδου, τους τελεστές των πράξεων της Άλγεβρας Boole και μία μεταβλητή εξόδου που είναι συνάρτηση των μεταβλητών εισόδου. Η κάθε μία από τις n μεταβλητές εισόδου μπορεί να πάρει δύο μόνο τιμές, το λογικό "1" και το λογικό "0". Επομένως, όλοι οι δυνατοί συνδυασμοί των μεταβλητών εισόδου είναι 2^n. Για κάθε συνδυασμό των μεταβλητών εισόδου, η μεταβλητή εξόδου παίρνει μία μόνο τιμή: το λογικό "1" ή το λογικό "0". Ο πίνακας αληθείας της λογικής συνάρτησης περιγράφει αυτή τη σχέση εισόδων-εξόδου.

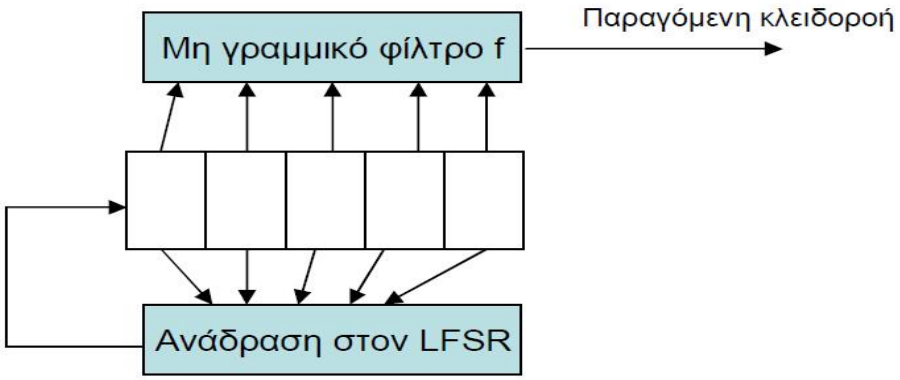
Ορισμός 2.5: Μία λογική συνάρτηση μπορεί να αναπαρασταθεί με διάφορες μαθηματικές εκφράσεις. Η πιο συνηθισμένη για τις κρυπτογραφικές συναρτήσεις είναι Αλγεβρική Κανονική

Μορφή (Algebraic Normal Form), δηλαδή, XOR (modulo 2) άθροισμα των γινομένων των μεταβλητών της.

Ορισμός 2.6: Βαθμός μίας συνάρτησης f , deg(f) είναι το πλήθος των μεταβλητών που εμφανίζονται στο μεγαλύτερο γινόμενο στην Αλγεβρική Κανονική Μορφή της.
Για παράδειγμα, η λογική συνάρτηση $f(x_1,x_2,x_3,x_4,x_5)=x_1 \oplus x_2x_3 \oplus x_2x_5 \oplus x_1x_3x_4$, έχει βαθμό deg(f)= 3 . Ο μέγιστος βαθμός μη γραμμικότητας που μπορεί να έχει μια συνάρτηση n μεταβλητών είναι n.

Γεννήτριες κλειδοροής με μη γραμμικά φίλτρα

Η χρήση μη γραμμικών φίλτρων δεν αλλάζει τη λειτουργία του LFSR. Ο LFSR παραμένει βασικό στοιχείο της γεννήτριας αλλά η έξοδος της κλειδοροής δε λαμβάνεται από την έξοδό του, αλλά από τη μη γραμμική συνάρτηση f.



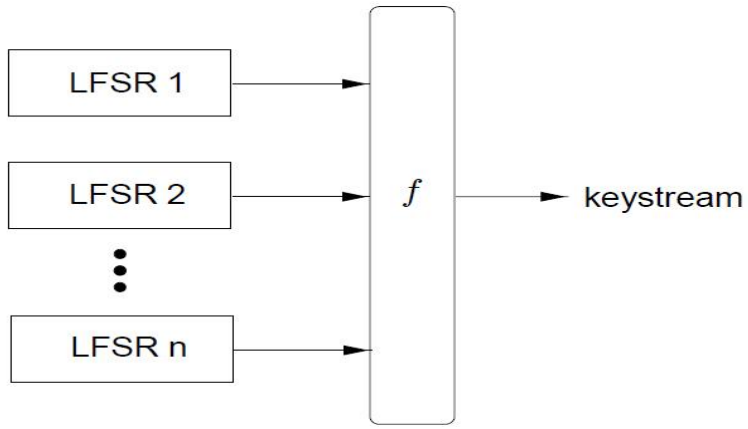
Σχήμα 2.3: Γεννήτρια κλειδοροής με μη γραμμικό φίλτρο

Η συνάρτηση f ονομάζεται μη γραμμικό φίλτρο (nonlinear filter function). Η συνάρτηση f θα πρέπει να είναι ισοβαρής έτσι ώστε να εξασφαλίζεται ομοιόμορφη κατανομή των bits 0,1 στην παραγόμενη κλειδοροή. Το αποτέλεσμα που επιτυγχάνεται με αυτή τη διάταξη είναι μεγάλη περίοδος (λόγω του πρωταρχικού LFSR) και υψηλή γραμμική πολυπλοκότητα (λόγω του φίλτρου). Αν και για δοθείσα συνάρτηση f δεν μπορεί να προσδιοριστεί επακριβώς η γραμμική πολυπλοκότητα, υπάρχουν συγκεκριμένες κατασκευές συναρτήσεων που, αν χρησιμοποιηθούν ως μη γραμμικά φίλτρα, παράγουν κλειδοροή εγγυημένα πολύ υψηλής γραμμικής πολυπλοκότητας, δηλαδή, αποδεικνύεται μαθηματικά ένα υψηλό κάτω φράγμα για την τιμή της

γραμμικής πολυπλοκότητας. Επίσης, αποδείχθηκε από τον Key [34] ότι το άνω φράγμα αυτής είναι: $\sum_{i=1}^{d} = \binom{N}{i}$ όπου deg(f)=d και N το μέγεθος του LFSR.

Γεννήτριες κλειδοροής με μη γραμμικούς συνδυαστές

Μια άλλη μέθοδος είναι οι μη γραμμικοί συνδυαστές. Αντί για ένας, χρησιμοποιούνται περισσότεροι LFSRs των οποίων οι έξοδοι «τροφοδοτούν» τις εισόδους μίας μη γραμμικής συνάρτησης (combinatorial function).

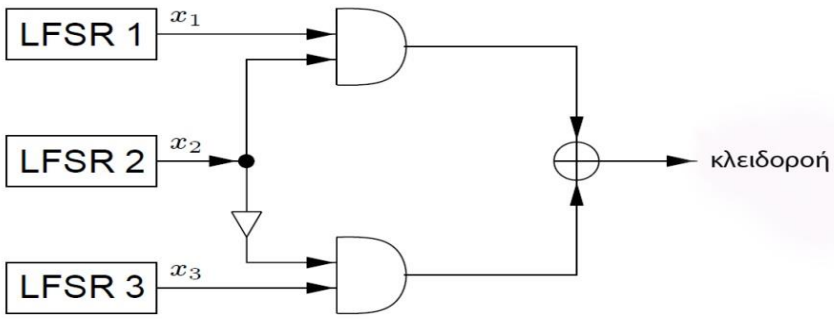


Σχήμα 2.4: Γεννήτρια κλειδοροής με μη γραμμικούς συνδυαστές (Σχήμα από το βιβλίο Handbook of Applied Cryptography [24])

Με κατάλληλη επιλογή της f και των LFSRs, μπορεί να διασφαλιστεί μεγάλη περίοδος της κλειδοροής (ιδανικά: ίση με το ελάχιστο κοινό πολλαπλάσιο των περιόδων των ακολουθιών που παράγουν οι LFSRs).

Αν L1, L2,…,Ln είναι οι γραμμικές πολυπλοκότητες (ανά δύο διαφορετικές μεταξύ τους) των ακολουθιών που παράγονται από τους LFSRs, τότε η γραμμική πολυπλοκότητα της παραγόμενης κλειδοροής ισούται με: f(L1,L2,…,Ln) , που σημαίνει ότι θα πρέπει η μη γραμμική συνάρτηση να είναι μεγάλου βαθμού για να επιτευχθεί υψηλή γραμμική πολυπλοκότητα.

Χαρακτηριστικό παράδειγμα γραμμικού συνδυαστή είναι η γεννήτρια Geffe (Geffe Generator)



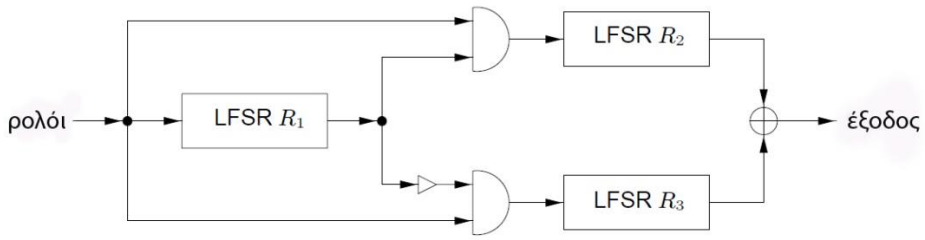
Σχήμα 2.5: Geffe Generator

Η γεννήτρια Geffe (σχήμα 2.5) αποτελείται από 3 πρωταρχικούς LFSR μήκους L_1, L_2, L_3 ανά δύο πρώτα μεταξύ τους , και συνδυάζονται με τη μη γραμμική συνάρτηση:
$f(x_1,x_2,x_3) = x_1x_2 \oplus (1 + x_2)x_3 = x_1x_2 \oplus x_2x_3 \oplus x_3$. Η κλειδοροή έχει περίοδο $(2^{L1} -1)\ (2^{L2} -1)\ (2^{L3} -1)$ και γραμμική πολυπλοκότητα $L = L_1L_2 + L_2L_3 + L_3$. Αν και φαίνεται να παρέχει ικανοποιητική ασφάλεια, δεν είναι κρυπτογραφικά ισχυρή διότι διαρρέει πληροφορία για την κατάσταση των LFSR 1 και LFSR 2 (όπως θα δούμε στην ενότητα 3.1)

Γεννήτριες Ελεγχόμενου Χρονισμού

Στις γεννήτριες ελεγχόμενου χρονισμού (clocked-controlled generators), το ρολόι ενός LFSR καθορίζεται από την έξοδο κάποιου άλλου LFSR.

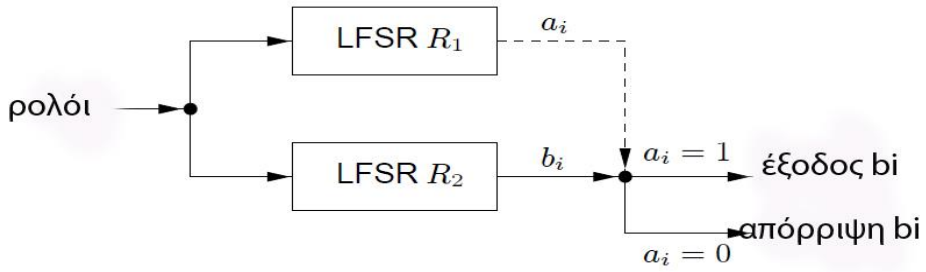
Παράδειγμα: Στη γεννήτρια εναλλαγής βήματος (alternating step generator) η έξοδος του LFSR R_1 χρησιμοποιείται ως ρολόι στους LFSR R_2 και R_3. Η κλειδοροή προκύπτει από το XOR άθροισμα των δύο LFSR R_2 και R_3.



Σχήμα 2.6: Γεννήτρια ελεγχόμενου χρονισμού (Σχήμα από το βιβλίο Handbook of Applied Cryptography [24])

Γεννήτρια συρρίκνωσης (shrinking generator)

Η γεννήτρια συρρίκνωσης είναι σχετικά νέα υλοποιήσεις γεννήτριας κλειδοροής. Το κύκλωμά της είναι ιδιαίτερα απλό. Ένας LFSR R_1 καθορίζει το αν θα λαμβάνεται ή όχι υπόψη η έξοδος ενός άλλου LFSR R_2. Η τελική κλειδοροή είναι ένα «τυχαίο» αποδεκάτισμα (decimation) της εξόδου του LFSR.



Σχήμα 2.7: Γεννήτρια Συρρίκνωσης (Σχήμα από το βιβλίο Handbook of Applied Cryptography [24])

2.3 Επιθέσεις σε κρυπταλγορίθμους ροής

Οι κρυπταλγόριθμοι ροής, όπως είδαμε, έχουν ευρεία εφαρμογή σε πολλούς και διαφορετικούς τομείς. Αναμενόμενο ήταν να υπάρξουν προσπάθειες κρυπτανάλυσης είτε από κακόβουλους χρήστες , είτε από ερευνητικό ενδιαφέρον.

Με την επιλογή κατάλληλων σύνθετων δομών για την κατασκευή γεννητριών κλειδοροής (π.χ. μη γραμμικά φίλτρα, μη γραμμικοί συνδυαστές κτλ.) επιτυγχάνουμε την παραγωγή ακολουθιών με καλά κρυπτογραφικά χαρακτηριστικά (όπως η υψηλή γραμμική πολυπλοκότητα, η οποία τις καθιστά μη προβλέψιμες). Παρόλα αυτά, αυτό δεν σημαίνει ότι έχει κατασκευαστεί ένας ασφαλής αλγόριθμος: οι ίδιες οι συναρτήσεις που υπεισέρχονται στην κατασκευή μιας γεννήτριας κλειδοροής μπορούν να «επιτρέψουν», αν δεν έχουν κατάλληλες ιδιότητες, τη διενέργεια επιτυχών επιθέσεων (όπως θα δούμε στη συνέχεια).

Στις επιθέσεις θεωρούμε ότι το κανάλι επικοινωνίας είναι ανασφαλές, υπό την έννοια ότι ο επιτιθέμενος μπορεί να έχει πρόσβαση πάντα σε ολόκληρο κρυπτοκείμενο. Επίσης, θεωρούμε ότι

γνωρίζει τις λεπτομέρειες υλοποίησης του κάθε αλγορίθμου (όπως ισχύει στην πράξη[1]), αλλά δεν γνωρίζει το μυστικό κλειδί.

Η πιο απλή επίθεση που μπορεί να εφαρμοστεί σε όλους τους αλγορίθμους κρυπτογράφησης , αλλά και η πιο χρονοβόρα, είναι η εξαντλητική αναζήτηση ή αλλιώς επίθεση ωμής βίας (brute force). Ο επιτιθέμενος δοκιμάζει διαδοχικά όλα τα πιθανά κλειδιά μέχρι να βρει το αρχικό κείμενο. Αυτή η μέθοδος δεν είναι αποδοτική για «μεγάλο» μέγεθος κλειδιού, πχ από 128bit και πάνω για τα σύγχρονα δεδομένα. (Όταν ο DES προτυποποιήθηκε από τον NIST , το μέγεθος κλειδιού 56bit θεωρούνταν ικανοποιητικό, αλλά πλέον αυτό αποτελεί την αδυναμία του συγκεκριμένου αλγορίθμου)
Δεδομένου ότι τα κλειδιά των σύγχρονων κρυπταλγορίθμων είναι αρκούντως μεγάλα, οι επιτιθέμενοι έπρεπε να ψάξουν «ευαίσθητα» σημεία ή λάθη στην υλοποίηση κάθε αλγορίθμου.
Στους αλγορίθμους ροής λόγω της υλοποίησής τους βρήκαν εφαρμογή κάποιες επιθέσεις που περιγράφονται στη συνέχεια.

2.3.1 Επιθέσεις Συσχέτισης (Correlation Attacks)

Για να γίνει κατανοητή αυτή η κατηγορία επιθέσεων, ας αναλογιστούμε εκ νέου τον Geffe Generator του σχήματος 2.5, για τον οποίο μπορούμε εύκολα να επιβεβαιώσουμε ότι ισχύει :

$$P(z(t) = x_1(t)) = P(x_2(t) = 1)+P(x_2(t) = 0)\ \ P(x_3(t) = x_1(t))=\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}$$

Με άλλα λόγια, αν ένα bit της κλειδοροής ισούται με 1, τότε η πιθανότητα να ισούται με 1 και το αντίστοιχο bit εξόδου του πρώτου και τρίτου LFSR είναι αρκετά μεγάλη (75%).
Λόγω αυτού του γεγονότος είναι επιρρεπείς σε ένα είδος επιθέσεων που ονομάζονται Επιθέσεις Συσχέτισης (Correlation Attacks). Αν η έξοδος της γεννήτριας ταυτίζεται με την έξοδο κάποιου από τους LFSR με πιθανότητα p > ½, τότε αν ένα ικανοποιητικά μεγάλο τμήμα της κλειδοροής είναι γνωστό, μπορεί να ευρεθεί η αρχική κατάσταση του εν λόγω καταχωρητή (δηλαδή τμήμα του κλειδιού).
Επομένως για να είναι μια γεννήτρια κατάλληλη για κρυπτογραφικές συναρτήσεις θα πρέπει να μην εμφανίζει στατιστική εξάρτηση της εξόδου της με κάποιο υποσύνολο των εισόδων της. Για να επιτευχθεί αυτό θα πρέπει να χρησιμοποιηθούν κατάλληλες συναρτήσεις, οι οποίες χαρακτηρίζονται ως ανεπηρέαστες στη συσχέτιση (correlation immune).

[1] Εξαίρεση αποτελούν οι στρατιωτικές εφαρμογές, όπου και οι λεπτομέρειες του αλγορίθμου παραμένουν μυστικές. Τέτοιοι αλγόριθμοι δεν μπορούν να τύχουν, προφανώς, ευρείας χρήσης (π.χ. για ασφάλεια στο Διαδίκτυο).

Οι Επιθέσεις Συσχέτισης προτάθηκαν το 1984 από τον Siegenthaler [29] και με μικρές παραλλαγές μπορούν να χρησιμοποιηθούν και για επιθέσεις σε γεννήτριες μη γραμμικών φίλτρων. Μία συνάρτηση f είναι ανθεκτική σε συσχετίσεις τάξης t (t-h order correlation-immune) αν, για οποιεσδήποτε μεταβλητές $x_{i1},\ldots,x_{it}$ και οποιεσδήποτε τιμές των $b_{i1},..,b_{it}$, ισχύει:

$P(f(x)=0 \mid x_{i1}=b_{i1}, x_{i2}=b_{i2},....x_{it}=b_{it}) = P(f(x)=0)$ [19]

Αποδεικνύεται ότι όσο ποιο μεγάλη είναι η τάξη t της συνάρτησης, τόσο ποιο μικρός είναι ο βαθμός της.

2.3.2 Επιθέσεις προσεγγίσεων (Approximation Attacks)

Έστω μια συνάρτηση συνδυαστή f η οποία διαφέρει από μια γραμμική συνάρτηση g σε πολύ λίγες θέσεις στον πίνακα αλήθειας. Έστω ότι με χρήση της f η γεννήτρια παράγει κλειδοροή k. Αν η f αντικατασταθεί από τη γραμμική συνάρτηση g, θα παραχθεί κλειδοροή k' με μικρή γραμμική πολυπλοκότητα. Επομένως, γνωρίζοντας λίγα bit από την κλειδοροή k' και χρησιμοποιώντας τον αλγόριθμο Berlekamp-Massey θα βρούμε τον LFSR που την παράγει. Με αυτό τον τρόπο αποκαλύπτεται η κλειδοροή k' η οποία διαφέρει από την k σε λίγα μόνο bit. Άρα, θα έχουμε καταφέρει να μαντέψουμε σωστά το μεγαλύτερο τμήμα της κλειδοροής.

Φαίνεται λοιπόν η ανάγκη να μην μπορεί η συνάρτηση f να προσεγγιστεί ικανοποιητικά από καμία γραμμική συνάρτηση.[11]

Γενικεύοντας, θα πρέπει η συνάρτηση f να μη μπορεί να προσεγγιστεί ικανοποιητικά από καμία συνάρτηση χαμηλού βαθμού (πρακτικά βαθμού 2).

Για την μαθηματική διατύπωση των ανωτέρω, παραθέτουμε τους ακόλουθους ορισμούς:

Ορισμός 2.7: Η Hamming απόσταση (distance) δύο συναρτήσεων f, g: $wt(f \oplus g)$ υποδηλώνει το πλήθος των θέσεων στους πίνακες αληθείας στις οποίες οι συναρτήσεις διαφέρουν μεταξύ τους.

Ορισμός 2.8: Η μη γραμμικότητα (nonlinearity) μίας συνάρτησης $nl(f)$ ισούται με το μικρότερο πλήθος θέσεων στον πίνακα αληθείας της οι οποίες, αν μεταβληθούν, θα μετατρέψουν τη συνάρτηση σε γραμμική (βαθμού 1). Δηλαδή, $nl(f) = \min_g \left(\mathrm{wt}\left(\mathrm{f}+\mathrm{g}\right)\right)$ για όλες τις γραμμικές συναρτήσεις g.

Αντίστοιχα, η μη γραμμικότητα τάξης r (r-th nonlinearity) μίας συνάρτησης $nl_r(f)$ ισούται με το μικρότερο πλήθος θέσεων στον πίνακα αληθείας της οι οποίες, αν μεταβληθούν, θα μετατρέψουν τη συνάρτηση σε βαθμού το πολύ r. Δηλαδή, $\min_g(wt(f \oplus g))$, για όλες τις συναρτήσεις g, τέτοιες ώστε $\deg(g) \le r$.

Από τους ορισμούς προκύπτει ότι $nl(f) \ge nl_2(f) \ge nl_3(f)$...

Για να είναι ανθεκτικές οι κρυπτογραφικές συναρτήσεις σε επιθέσεις προσέγγισης θα πρέπει να είναι υψηλής μη γραμμικότητας. Κυρίως έχει μελετηθεί η μη γραμμικότητα πρώτης τάξης και λιγότερο η μη γραμμικότητα δεύτερης τάξης.

Για άρτιο n , η μέγιστη δυνατή μη γραμμικότητα είναι $2^{(n-1)} - 2^{(\frac{n}{2}-1)}$, και οι συναρτήσεις που το επιτυγχάνουν λέγονται bent. Για περιττό n, δεν γνωρίζουμε ποια είναι η μέγιστη δυνατή μη γραμμικότητα που μπορεί να επιτευχθεί. Θα πρέπει να επισημανθεί ωστόσο ότι οι συναρτήσεις bent δεν είναι ισοβαρείς (balanced) - κάτι που το θέλουμε σε κρυπτογραφικές εφαρμογές. Αν περιοριστούμε λοιπόν στις balanced συναρτήσεις, δεν γνωρίζουμε ποια είναι η μέγιστη δυνατή μη γραμμικότητα ακόμα και για άρτιο n.

Παράδειγμα: Η λογική συνάρτηση:

$f(X_1, X_2, X_3) = X_2 \oplus X_3 \oplus X_1X_2 \oplus X_1X_3 \oplus X_2X_3 \oplus X_1X_2X_3$ έχει το μέγιστο βαθμό συνάρτησης 3 μεταβλητών $\deg(f) = 3$, αλλά ο πίνακας αληθείας της διαφέρει από τη γραμμική συνάρτηση $g(X_1, X_2, X_3) = X_1 \oplus 1$ σε μόνο μία θέση! (στη 000).

Επομένως η συνάρτηση έχει μη γραμμικότητα $nl(f) = 1$ και είναι ευαίσθητη σε επιθέσεις προσεγγίσεων.

Οι Αλγεβρικές Επιθέσεις (algebraic attacks), οι οποίες είναι οι τελευταίες που προτάθηκαν χρονικά, θα μελετηθούν εκτενώς στο επόμενο κεφάλαιο.

Κεφάλαιο 3
Αλγεβρικές επιθέσεις

Στο κεφάλαιο αυτό μελετάμε μία πιο πρόσφατη κατηγορία επιθέσεων, τις αλγεβρικές επιθέσεις (algebraic attacks). Οι επιθέσεις αυτές έχουν μία σχετικά απλή φιλοσοφία, η οποία βασίζεται στη χρήση έξυπνων τεχνικών προκειμένου να απλοποιηθούν οι σύνθετες μαθηματικές εκφράσεις που περιγράφουν τα συμμετρικά κρυπτογραφικά συστήματα, κατά τρόπο τέτοιο ώστε να είναι υπολογιστικά εφικτή η ανάκτηση από αυτές του μυστικού κλειδιού.

Οι αλγεβρικές επιθέσεις προτάθηκαν για εφαρμογή τόσο σε κρυπταλγορίθμους ροής (stream ciphers) όσο και σε κρυπταλγορίθμους τμήματος (block ciphers): αν και υπάρχουν διαφορές στον τρόπο προσέγγισης, η βασική φιλοσοφία που αναφέρθηκε παραπάνω είναι η ίδια. Είναι σημαντικό να αναφερθεί ότι έχουν αποδειχθεί ιδιαίτερα αποτελεσματικές ακόμα και σε περιπτώσεις που άλλα είδη επιθέσεων απέτυχαν: για παράδειγμα, με χρήση αλγεβρικών επιθέσεων υπήρξε επιτυχής κρυπτανάλυση του αλγόριθμου τμήματος KeeLoq, ο οποίος χρησιμοποιείται σε συστήματα συναγερμού αυτοκινήτων [08]. Σε κάθε περίπτωση, από τη μελέτη των αλγεβρικών επιθέσεων ανέκυψε ένα νέο κρυπτογραφικό κριτήριο για τις συναρτήσεις που υπεισέρχονται στα κρυπτογραφικά συστήματα, η λεγόμενη αλγεβρική ανθεκτικότητα (algebraic immunity).

Για τη μελέτη των αλγεβρικών επιθέσεων θα εστιάσουμε στους σύγχρονους αλγόριθμους ροής, των οποίων η γεννήτρια κλειδοροής παράγεται από εφαρμογή μη γραμμικού φίλτρου στις καταστάσεις ενός LFSR (βλ. παραπάνω Σχήμα 2.3). Ο λόγος που περιοριζόμαστε σε αυτά τα κρυπτοσυστήματα είναι ότι αποτελούν τις βασικές κατηγορίες κρυπτογραφικών συστημάτων στα οποία εφαρμόστηκαν για πρώτη φορά οι αλγεβρικές επιθέσεις [06] ενώ επίσης προσφέρονται για κατανόηση του τρόπου εφαρμογής των επιθέσεων αυτών. Για να μοντελοποιήσουμε το πρόβλημα, συμβολίζουμε με L τη γραμμική συνάρτηση ανάδρασης που περιγράφει τη μετάβαση από τη μία κατάσταση του LFSR στην επόμενη: θεωρούμε ότι το L είναι γνωστό σε όλους, και μόνο η αρχική κατάσταση του LFSR (που αποτελεί και το μυστικό κλειδί) είναι μυστική. Η κλειδοροή παράγεται από την εφαρμογή μιας γνωστής μη γραμμικής

συνάρτησης f (μη γραμμικό φίλτρο). Έστω ότι (k_0,…..,k_{n-1}) είναι η αρχική κατάσταση του LFSR και $b_0b_1b_2$… η παραγόμενη κλειδοροή. Τότε ισχύουν οι εξής σχέσεις:

$$\begin{cases} b_0 = f \quad (k_0, \ldots, k_{n-1}) \\ b_1 = f\,(L\ (k_0, \ldots, k_{n-1})) \\ b_2 = f\,(L^2(k_0, \ldots, k_{n-1})) \\ \quad\quad \vdots \end{cases}$$

Ο στόχος της κρυπτανάλυσης (άρα, και των αλγεβρικών επιθέσεων) είναι η ανάκτηση του μυστικού κλειδιού k = (k_0,…..,k_{n-1}) δοθέντος κάποιου υποσυνόλου των bits της κλειδοροής.

3.1 Περιγραφή επιθέσεων

Οι αλγεβρικές επιθέσεις ανήκουν στην κατηγορία των επιθέσεων γνωστού αρχικού μηνύματος (known plaintext attack), δηλαδή θεωρούμε ότι γνωρίζουμε κάποια bits του αρχικού μηνύματος καθώς επίσης βέβαια και τα αντίστοιχα bits του κρυπτοκειμένου. Αξίζει να σημειωθεί ότι τα bits που χρειάζεται να γνωρίζουμε δεν απαιτείται να είναι συνεχόμενα.

3.1.1 Μία πρώτη προσέγγιση

Ανακαλώντας το μοντέλο του μη γραμμικού φίλτρου, μπορούμε να δούμε ότι τη χρονική στιγμή t, το τρέχον bit b_t της κλειδοροής ικανοποιεί μία εξίσωση της μορφής f(s) = b_t, όπου s η τρέχουσα κατάσταση του LFSR. Η f είναι υψηλού βαθμού, οπότε από την ανωτέρω σχέση, ακόμα και αν γνωρίζουμε το b_t, δεν μπορούμε αλγεβρικά να υπολογίσουμε το s. Η κύρια ιδέα των αλγεβρικών επιθέσεων, όπως περιγράφηκε από τον Courtois το 2003 [05] έχει να κάνει με τον πολλαπλασιασμό της πολυωνυμικής παράστασης f(s), με ένα κατάλληλο πολυώνυμο g(s), τέτοιο ώστε το γινόμενο fg να είναι μία συνάρτηση χαμηλού βαθμού d. Τότε, αν για παράδειγμα ισχύει b_t = 0, προκύπτει η εξίσωση f(s)g(s) = 0 η οποία είναι χαμηλού βαθμού. Η παράσταση αυτή αποτελεί μια εξίσωση πολλαπλών μεταβλητών χαμηλού βαθμού d ως προς τα bits k_i της αρχικής κατάστασης. Συνεπώς, αν έχουμε μια τέτοια εξίσωση για κάθε ένα από τα πολλά bits της

κλειδοροής, τότε θα διαθέτουμε ένα σύστημα πολλών εξισώσεων που θα μπορούν ενδεχομένως να επιλυθούν[2] (οι εξισώσεις εξακολουθούν να μην είναι γραμμικές, κάτι που – αν ίσχυε - θα επέτρεπε την άμεση επίλυσή τους, αλλά είναι χαμηλού βαθμού και για αυτό μπορούν να εφαρμοστούν τεχνικές επίλυσής τους).

Γενικότερα, για κάθε γνωστό bit της κλειδοροής $b_t = f(s)$ τη χρονική στιγμή t, για οποιαδήποτε συνάρτηση g ισχύει:

$$f(s) \cdot g(s) = b_t \cdot g(s),$$

και, εφόσον η κατάσταση τη χρονική στιγμή t είναι $s = L^t(k_0,\ldots, k_{n-1})$, (όπου με L^t συμβολίζουμε την εφαρμογή της γραμμικής ανάδραση L του LFSR t φορές) η ανωτέρω σχέση γράφεται:

$$f(L^t(k_0,\ldots, k_{n-1})) \cdot g(L^t(k_0,\ldots, k_{n-1})) = b_t \cdot g(L^t(k_0,\ldots, k_{n-1}))$$

Στο ίδιο άρθρο, περιγράφηκαν τα εξής σενάρια, που όλα υπάγονται στην (πρωτοεμφανιζόμενη τότε) κατηγορία των αλγεβρικών επιθέσεων:

1. Έστω ότι υπάρχει συνάρτηση g χαμηλού βαθμού, τέτοια ώστε το γινόμενο f·g να είναι επίσης χαμηλού βαθμού. Τότε, αν συμβολίσουμε με h το γινόμενο f·g, προκύπτει μία εξίσωση της μορφής $h(s) = b_t \cdot g(s)$, όπου ανεξαρτήτως της τιμής του bit b_t (0 ή 1) αποτελεί μία εξίσωση χαμηλού βαθμού με αγνώστους τα bit του κλειδιού $k_0,\ldots, k_{n-1}$.

2. Έστω ότι υπάρχει συνάρτηση g χαμηλού βαθμού, τέτοια ώστε $f \cdot g = 0$. Τότε, αν $b_t = 1$, προκύπτει μία εξίσωση της μορφής $g(s)=0$, η οποία αποτελεί μία εξίσωση χαμηλού βαθμού με αγνώστους τα bit του κλειδιού $k_0,\ldots, k_{n-1}$.

3. Έστω ότι υπάρχει συνάρτηση g οποιουδήποτε βαθμού (μπορεί να είναι και μεγάλου), τέτοια ώστε το γινόμενο f·g να είναι χαμηλού βαθμού. Τότε, αν συμβολίσουμε με h το

[2] Η επίλυση εξισώσεων χαμηλού βαθμού δεν θα μελετηθεί εδώ: σχετικές τεχνικές περιγράφονται στα άρθρα που παρατίθενται στη βιβλιογραφία

γινόμενο $f \cdot g$, και εφόσον αν $b_t = 0$, προκύπτει μία εξίσωση της μορφής $h(s) = 0$, η οποία αποτελεί μία εξίσωση χαμηλού βαθμού με αγνώστους τα bit του κλειδιού $k_0, \ldots, k_{n-1}$.

Επίσης, περιγράφονται και πρακτικές εφαρμογές των ανωτέρω (η περίπτωση του Toyocrypt θα περιγραφεί στη συνέχεια). Σε κάθε περίπτωση, διαφαίνεται ότι η εύρεση κατάλληλων συναρτήσεων g, όταν κάτι τέτοιο είναι εφικτό, μπορούν να οδηγήσουν στην απλοποίηση των σύνθετων εξισώσεων που εκφράζουν τη συσχέτιση του μυστικού κλειδιού με την παραγόμενη κλειδοροή.

3.1.2 Συστηματική προσέγγιση

Η ανωτέρω περιγραφή των αλγεβρικών επιθέσεων για τους κρυπταλγορίθμους ροής συστηματοποιήθηκε μετέπειτα από τους Meier, Pasalic, Carlet [23]. Συγκεκριμένα, οι συγγραφείς του εν λόγω άρθρου παρατήρησαν τα εξής:

Ας ανακαλέσουμε την ανωτέρω περίπτωση 3. Τότε $f \cdot g = h \neq 0$. Αν πολλαπλασιάσουμε αυτήν την εξίσωση με την f, τότε επειδή ισχύει $f^2 = f$ (αφού η f είναι λογική συνάρτηση), παίρνουμε

$$f^2 \cdot g = f \cdot h = f \cdot g = h.$$

Με άλλα λόγια, $f \cdot h = h$. Επειδή η συνάρτηση h είναι χαμηλού βαθμού, στην ουσία είμαστε εκ νέου στο σενάριο 1. Συνεπώς, το σενάριο 3 είναι περιττό και δεν χρήζει εξέτασης (αφού, αν μπορεί να εφαρμοστεί το σενάριο 3, τότε μπορεί να εφαρμοστεί και το σενάριο 1). Η διαπίστωση αυτή υποδηλώνει ότι οι αλγεβρικές επιθέσεις μπορούν πάντα να περιοριστούν στα ανωτέρω σενάρια 1 και 2. Υπάρχει ωστόσο μια ενδιαφέρουσα σχέση μεταξύ των δύο: Ας υποθέσουμε ότι ισχύει $f \cdot g = h \neq 0$ για κάποιες συναρτήσεις g και h βαθμού το πολύ d (σενάριο 1). Ας υποθέσουμε επίσης ότι $g \neq h$. Τότε υπάρχει μια συνάρτηση g' βαθμού το πολύ d τέτοια ώστε να ισχύει $f \cdot g' = 0$ (σενάριο 2). Από την παραπάνω παρατήρηση προκύπτει το συμπέρασμα ότι η ανάγκη αντιμετώπισης των αλγεβρικών επιθέσεων επιβάλλει την εξής ιδιότητα: ούτε η f ούτε η συμπληρωματική της $f + 1$ πρέπει να έχουν συνάρτηση εκμηδενισμού (annihilating function) χαμηλού βαθμού (όπου συνάρτηση εκμηδενισμού για την f ονομάζεται κάθε συνάρτηση που αν πολλαπλασιαστεί με την f προκύπτει αποτέλεσμα 0).

Με την ανωτέρω ανάλυση και συμπεράσματα [20], θεσπίστηκε ένα συγκεκριμένο κρυπτογραφικό κριτήριο για την αποτίμηση μίας συνάρτησης f ως προς το κατά πόσον είναι επιρρεπής σε αλγεβρικές επιθέσεις. Το κριτήριο αυτό είναι η λεγόμενη αλγεβρική ανθεκτικότητα (algebraic immunity), συμβολίζεται με AI(f), και ορίζεται ως η ελάχιστη δυνατή τιμή ακέραιου αριθμού d τέτοια ώστε είτε η f είτε η συμπληρωματική τη f + 1 να έχουν μία συνάρτηση εκμηδενισμού βαθμού d. Συνεπώς, αναγκαία προϋπόθεση προκειμένου να είναι μία κρυπτογραφική συνάρτηση ανθεκτική σε αλγεβρικές επιθέσεις είναι να έχει υψηλή αλγεβρική ανθεκτικότητα. Για την αλγεβρική ανθεκτικότητα μιας οποιασδήποτε συνάρτησης f με n μεταβλητές έχει αποδειχτεί το εξής (τόσο από τον Meier [20], όσο και με μεταγενέστερες διαφορετικές αποδείξεις του ιδίου αποτελέσματος):

Θεώρημα 3.1: Για κάθε λογική συνάρτηση f με n μεταβλητές ισχύει $AI(f) \leq [\frac{n}{2}]$

Ως εκ τούτου, σχεδιαστικός στόχος κατά την κατασκευή αλγορίθμων ανθεκτικών σε αλγεβρικές επιθέσεις είναι η επιλογή f με υψηλή αλγεβρική ανθεκτικότητα (ιδανικά, με τη μέγιστη δυνατή, όπως περιγράφεται στο ανωτέρω Θεώρημα). Τέτοιες κατασκευές συναρτήσεων αποτελούν ένα σημαντικό πεδίο έρευνας (βλ. και Ενότητες 4.3, 4.4 στη συνέχεια).

3.2 Πρακτική εφαρμογή των επιθέσεων

Ο Courtois [05] περιέγραψε ένα παράδειγμα αποτελεσματικής εφαρμογής αλγεβρικών επιθέσεων στον κρυπταλγόριθμο ροής Toyocrypt (αλγόριθμος ο οποίος είχε προταθεί στην Ιαπωνική Κυβέρνηση, κατόπιν σχετικής πρόσκλησής της (Cryptrec). Για κάποια χρόνια υπήρχε η πεποίθηση ότι ο αλγόριθμος αυτός είναι ισχυρός, αφού δεν μπορούσε να εφαρμοστεί αποτελεσματικά καμία από τις γνωστές επιθέσεις κρυπτανάλυσης. Η λειτουργία του Toyocrypt βασίζεται στη χρήση ενός LFSR που αποτελείται από 128 βαθμίδες – δηλαδή, n = 128 – στον οποίο εφαρμόζεται μη γραμμικό φίλτρο f που περιγράφεται από την ακόλουθη σχέση:

$$f(s_0, .., s_{127}) = s_{127} + \sum_{i=0}^{62} s_i s_{\alpha_i} + s_{10}s_{23}s_{32}s_{42} +$$
$$+ s_1 s_2 s_9 s_{12} s_{18} s_{20} s_{23} s_{25} s_{26} s_{28} s_{33} s_{38} s_{41} s_{42} s_{51} s_{53} s_{59} + \prod_{i=0}^{62} s_i.$$

όπου τα {a_0, …, a_{62}} είναι κάποια μετάθεση του συνόλου {63,....., 125}. Το «αδύναμο», ως προς τις αλγεβρικές επιθέσεις, σημείο του αλγορίθμου – όπως θα διαφανεί στη συνέχεια - είναι ότι υπάρχει ένας μόνο όρος με βαθμό 17 και ένας όρος με βαθμό 63: οι υπόλοιποι όροι είναι χαμηλού βαθμού.

Για να εφαρμόσουμε αλγεβρική επίθεση στον Toyocrypt χρειάζεται να βρούμε μια συνάρτηση g τέτοια ώστε το γινόμενο f·g να είναι χαμηλού βαθμού. Παρατηρώντας τους όρους υψηλού βαθμού στην f(s), βλέπουμε ότι όλοι οι όροι βαθμού 4, 17 και 63 εμπεριέχουν τον κοινό παράγοντα $s_{23}s_{42}$. Σε κάθε χρονική στιγμή t, οι τιμές των s_{23} και s_{42} είναι διαφορετικοί γνωστοί συνδυασμοί των bits k_i του μυστικού κλειδιού. Συνεπώς, αν τη χρονική στιγμή t το αντίστοιχο bit της κλειδοροής είναι b_t, πολλαπλασιάζουμε την εξίσωση f(s) = b_t και τις δύο πλευρές με τη συνάρτηση g(s) = (s_{23} - 1), από όπου προκύπτει η σχέση:

$$f(s)\, s_{23} - f(s) = b_t\, (s_{23} - 1).$$

Μπορεί κανείς να δει εύκολα ότι στην παραπάνω εξίσωση θα έχουν εκλείψει όλοι οι όροι της f που εμπεριέχουν το s_{23}. Συνεπώς, παίρνουμε μία εξίσωση βαθμού 3 (χαμηλού). Αντίστοιχα μπορεί να εργαστεί κανείς με τον κοινό παράγοντα (s_{42} - 1). Άρα, για κάθε bit κλειδοροής, μπορούμε να έχουμε δύο εξισώσεις με βαθμό 3 ως προς τις μεταβλητές του s, και συνεπώς δύο εξισώσεις βαθμού 3 ως προς τις μεταβλητές k_i του μυστικού κλειδιού. Όπως καταδεικνύεται [05], η επίθεση αυτή απαιτεί 16 Gigabytes μνήμης και μόνο 20 kilobytes (μη συνεχόμενα μάλιστα) από την κλειδοροή. Η συγκεκριμένη επίθεση είναι η καλύτερη από όλες όσες έχουν κατά καιρούς προταθεί για τον αλγόριθμο Toyocrypt.

3.3 Βελτιωμένη εκδοχή των επιθέσεων

Υπάρχει μία παραλλαγή των αλγεβρικών επιθέσεων, γνωστές με το όνομα γρήγορες αλγεβρικές επιθέσεις (fast algebraic attacks), οι οποίες είναι ισχυρότερες από τις κλασικές αλγεβρικές επιθέσεις [07]. Η βασική ιδέα αυτών έγκειται στην εύρεση, δοθείσης κρυπτογραφικής

συνάρτησης f, μίας συνάρτησης g χαμηλού βαθμού τέτοιας ώστε η συνάρτηση h= f·g να έχει απλά έναν όχι πολύ υψηλό βαθμό (δεν χρειάζεται δηλαδή απαραίτητα ο βαθμός της h να είναι πολύ χαμηλός). Σε αυτήν την περίπτωση, είναι εφικτό να μειωθεί τα πλήθος των αγνώστων μεταβλητών στις παραγόμενες εξισώσεις. Αξίζει να σημειωθεί ότι η συνάρτηση g+h είναι ένας εκμηδενιστής της f (αφού f·(g+h)=0) και, αφού ο βαθμός της g+h (που καθορίζει την αποτελεσματικότητα των επιθέσεων αυτών) μπορεί να είναι μεγαλύτερος από την αλγεβρική ανθεκτικότητα της f: γίνεται σαφές λοιπόν ότι αν μία συνάρτηση έχει τη μέγιστη δυνατή αλγεβρική ανθεκτικότητα, αυτό δεν σημαίνει απαραίτητα ότι είναι ανθεκτική έναντι των γρήγορων αλγεβρικών επιθέσεων.

Εφόσον υπάρχουν g, h με τις ανωτέρω ιδιότητες, έχουμε:

$$h(L^t(k_0,\ldots..,k_{n-1})) = b_t \cdot g(L^t(k_0,\ldots..,k_{n-1}))$$

Τότε, υπάρχει ένας γραμμικός συνδυασμός των πρώτων $\sum_{i=0}^{\deg(h)} \binom{n}{i}$ εξισώσεων, τέτοιος ώστε το αριστερό σκέλος της ανωτέρω σχέσης να ισούται με 0. Στην ουσία, αυτός ο γραμμικός συνδυασμός δεν είναι τίποτα άλλο παρά η έκφραση του LFSR με το ελάχιστο δυνατό μήκος που παράγει την ακολουθία που περιγράφεται από το δεξιό σκέλος της ανωτέρω εξίσωσης. Άρα, ο γραμμικός συνδυασμός αυτός μπορεί να βρεθεί με τον αλγόριθμο Berlekamp-Massey. Από τη στιγμή που θα υπολογιστεί αυτός ο γραμμικός συνδυασμός, θα έχουμε εξισώσεις βαθμού το πολύ ίσου με το βαθμό της g (που είναι χαμηλός).

Το μόνο μειονέκτημα των γρήγορων αλγεβρικών επιθέσεων έναντι των κλασικών είναι ότι απαιτούν γνώση συνεχόμενων bit της κλειδοροής ή, ισοδύναμα, του αρχικού μηνύματος (και όχι οποιωνδήποτε bits). Το πλήθος των συνεχόμενων bits που απαιτούνται προκύπτει από το βαθμό της h.

Αν θελήσουμε να μοντελοποιήσουμε τις γρήγορες αλγεβρικές επιθέσεις, θα δούμε ότι αποσκοπούν στην εύρεση συναρτήσεων g, h με deg(g)=e, deg(h)=d, τέτοιων ώστε h= f·g και το e+d είναι όσο πιο μικρό γίνεται (με ιδιαίτερη σημασία ιδίως στη χαμηλή τιμή του e). [06] Αποδεικνύεται ότι υπάρχουν πάντα, για κάθε f, συναρτήσεις g, h τέτοιες ώστε e+d ≥ n (όπου n το πλήθος των μεταβλητών της f). Άρα, για να είναι η f ανθεκτική σε αυτές τις επιθέσεις, θα πρέπει

να μην υπάρχουν g, h τέτοιες ώστε e+d<n. Επίσης, έχει αποδειχθεί [25] ότι αν μία συνάρτηση f ικανοποιεί την ανωτέρω ιδιότητα, δηλαδή έχει τη βέλτιστη δυνατή συμπεριφορά ως προς την ανθεκτικότητα έναντι των γρήγορων αλγεβρικών επιθέσεων, τότε έχει και τη μέγιστη αλγεβρική ανθεκτικότητα $[\frac{n}{2}]$.

3.4 Κατασκευές ισχυρών συναρτήσεων

Με την εμφάνιση των αλγεβρικών επιθέσεων, άρχισαν να προτείνονται κατασκευές συναρτήσεων που να έχουν τη μέγιστη δυνατή αλγεβρική ανθεκτικότητα. Η πρώτη τέτοια κατασκευή προτάθηκε από τους Dalai, Maitra, Sarkar [09], η οποία είναι η λεγόμενη πλειοψηφική συνάρτηση (majority function) και έχει εξαιρετικά απλή περιγραφή: ωστόσο έχει πολύ χαμηλή μη γραμμικότητα (για την ακρίβεια, τη χαμηλότερη δυνατή, με βάση κάποια κάτω φράγματα που έχει αποδείξει ο Lobanov [20]). Η συνάρτηση πλειοψηφίας είναι συμμετρική (δηλ. η έξοδός της δεν αλλάζει όταν το βάρος Hamming του διανύσματος εισόδου είναι σταθερό). Υπάρχουν και άλλες κατασκευές συμμετρικών συναρτήσεων οι οποίες επιτυγχάνουν υψηλότερη μη γραμμικότητα: ωστόσο, πρόσφατα αποδείχθηκε ότι οι συμμετρικές συναρτήσεις αναμένεται να μην συμπεριφέρονται καλά ως προς τις γρήγορες αλγεβρικές επιθέσεις. Κατασκευές που τροποποιούν τις συναρτήσεις πλειοψηφίας, έτσι ώστε να προκύψουν νέες, μη συμμετρικές, συναρτήσεις με επίσης μέγιστη αλγεβρική ανθεκτικότητα έχουν επίσης προταθεί [05], [15], [17], ενώ έχουν προταθεί και άλλες ανεξάρτητες κατασκευές συναρτήσεων [02], [03]. Ωστόσο, όλες αυτές οι συναρτήσεις δεν έχουν υψηλή μη γραμμικότητα.

Μία πολύ σημαντική κατασκευή συναρτήσεων με τη μέγιστη δυνατή αλγεβρική ανθεκτικότητα έχει προταθεί από Carlet και Feng [04]. Οι συναρτήσεις αυτές (με εξαιρετικά απλή περιγραφή, η οποία παρατίθεται στο επόμενο κεφάλαιο) επιτυγχάνουν υψηλή μη γραμμικότητα (τη μέγιστη δυνατή, σε σχέση με οποιαδήποτε άλλη κατασκευή συναρτήσεων μεγίστης αλγεβρικής ανθεκτικότητας, τη στιγμή μάλιστα που τα πειραματικά αποτελέσματα δείχνουν ότι η μη γραμμικότητα είναι ακόμα υψηλότερη από τα διάφορα ψηλά κάτω φράγματα που αποδεικνύονται μαθηματικά), ενώ έχουν και πολύ καλή συμπεριφορά και ως προς την αντιμετώπιση των γρήγορων αλγεβρικών επιθέσεων. Με αφετηρία την πλούσια σε ιδιότητες αυτή οικογένεια συναρτήσεων, έχουν υπάρξει νέες κατασκευές που τροποποιούν τις συναρτήσεις Carlet-Feng χωρίς να μειώνεται η αλγεβρική ανθεκτικότητα [18], [29], [37].

Γενικότερα, η κατασκευή συναρτήσεων με τη μέγιστη δυνατή αλγεβρική ανθεκτικότητα, οι οποίες ταυτόχρονα να πληρούν και λοιπά κρυπτογραφικά κριτήρια, παραμένει ένα ανοιχτό ερευνητικό θέμα. Οι συσχετίσεις της αλγεβρικής ανθεκτικότητας με λοιπά κρυπτογραφικά κριτήρια επίσης είναι ζήτημα ανοιχτό προς διερεύνηση.

Κεφάλαιο 4
Μελέτη Κρυπτογραφικών Συναρτήσεων

Στο κεφάλαιο 4 θα μελετηθεί μια κατηγορία γνωστών συναρτήσεων, οι συναρτήσεις Carlet-Feng ως προς την ικανοποίηση των κρυπτογραφικών κριτηρίων. Η συγκεκριμένη οικογένεια συναρτήσεων έχει αποδειχθεί ότι έχει μέγιστη αλγεβρική ανθεκτικότητα, ενώ επίσης φαίνεται ότι πληροί και πλήθος άλλων κρυπτογραφικών κριτηρίων. Εκτός από τις συναρτήσεις Carlet-Feng, θα εξετάσουμε και μία άλλη οικογένεια συναρτήσεων ως προς την αλγεβρική της ανθεκτικότητα, η οποία δεν έχει μελετηθεί μέχρι τώρα αλλά ωστόσο, όπως θα εξηγήσουμε στη συνέχεια, παρουσιάζει κρυπτογραφικό ενδιαφέρον.

4.1 Αναπαράσταση Συναρτήσεων

Στην παρούσα ενότητα θα γίνει μια εισαγωγή, καθώς είναι απαραίτητο το μαθηματικό υπόβαθρο για την κατανόηση των αναπαραστάσεων των προς μελέτη συναρτήσεων. Θα αποφύγουμε, προς χάριν απλότητας τις πολλές λεπτομέρειες και τις αποδείξεις των θεωρημάτων (εξάλλου αποτελούν βασικά αποτελέσματα που παρατίθενται σε οποιοδήποτε εγχειρίδιο σχετικά με πεπερασμένα σώματα – π.χ. [16]).

4.1.1 Δακτύλιοι και Σώματα

Το μεγαλύτερο πλήθος των ευρέως γνωστών αριθμητικών συστημάτων, όπως των ακεραίων, ρητών, και πραγματικών αριθμών, χρησιμοποιούν τις δυαδικές πράξεις της πρόσθεσης και του πολλαπλασιασμού. Στη συνέχεια, ορίζουμε τον δακτύλιο, ο οποίος έχει βασικές κοινές ιδιότητες με τα προαναφερθέντα αριθμητικά συστήματα.

Ας θεωρήσουμε το μη–κενό σύνολο S και έστω S × S είναι το σύνολο όλων των διατεταγμένων ζευγών (s, t) με s, t ∈ S. Τότε, κάθε απεικόνιση από το σύνολο S×S στο S ονομάζεται (δυαδική) πράξη πάνω στο σύνολο S.

Ορισμός 4.1: Ένα τυχαίο μη–κενό σύνολο S μαζί με μία ή περισσότερες πράξεις πάνω στο S, ονομάζεται αλγεβρική δομή.

Ορισμός 4.2: Η ομάδα είναι ένα μη–κενό σύνολο G μαζί με μία δυαδική πράξη ∗ πάνω στο G, η οποία συμβολίζεται ως (G, ∗), τέτοια ώστε να ισχύουν οι ακόλουθες τρεις ιδιότητες:

1. Η πράξη ∗ είναι προσεταιριστική, δηλ. ισχύει a ∗ (b ∗ c) = (a ∗ b) ∗ c για κάθε a, b, c ∈ G.
2. Υπάρχει στοιχείο e ∈ G, που ονομάζεται μοναδιαίο στοιχείο, τέτοιο ώστε a ∗ e =e ∗ a = a για κάθε a ∈ G.
3. Για κάθε a ∈ G, υπάρχει αντίστροφο στοιχείο a−1 ∈ G τέτοιο ώστε a ∗ a−1 =a−1 ∗ a = e.

Εάν η ομάδα (G, ∗) ικανοποιεί επιπλέον την ιδιότητα:

4. Η πράξη ∗ είναι αντιμεταθετική, δηλ. ισχύει a ∗ b = b ∗ a για κάθε a, b ∈ G τότε ονομάζεται αβελιανή ή αντιμεταθετική ομάδα.

Ορισμός 4.3: Ο δακτύλιος (R,+, ·) είναι ένα σύνολο R, εφοδιασμένο με δύο δυαδικές πράξεις πάνω στο R που συμβολίζονται με + και ·, τέτοιες ώστε:

- Το σύνολο R είναι αντιμεταθετική ομάδα ως προς την πράξη +.
- Η πράξη · είναι προσεταιριστική, δηλ. ισχύει (a · b) · c = a · (b · c), για κάθε a, b, c ∈ R.
- Ισχύει η επιμεριστική ιδιότητα, δηλ. για κάθε a, b, c ∈ R έχουμε a · (b + c) =a · b + a · c και (b + c) · a = b · a + c · a.

Ορισμός 4.4: Σώμα είναι ένας δακτύλιος (F,+, ·) τέτοιος ώστε το σύνολο F∗ (το οποίο ορίζεται ως το σύνολο των στοιχείων του F πλην του μηδενικού) μαζί με την πράξη του πολλαπλασιασμού · να αποτελεί αντιμεταθετική ομάδα.

Σύμφωνα με τον ορισμό, σώμα είναι ένα σύνολο F στο οποίο ορίζονται δύο δυαδικές πράξεις, η πρόσθεση και ο πολλαπλασιασμός, και το οποίο περιέχει δύο διακριτά στοιχεία 0 και 1 (συμβολίζουμε το πολλαπλασιαστικό μοναδιαίο στοιχείο e με 1) με 0≠ 1. Επιπρόσθετα, το (F, +) είναι αντιμεταθετική ομάδα ως προς την πρόσθεση με το 0 ως μοναδιαίο στοιχείο, ενώ το (F∗, ·) είναι αντιμεταθετική ομάδα ως προς τον πολλαπλασιασμό με το 1 ως μοναδιαίο στοιχείο. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού συνδέονται μέσω της επιμεριστικής ιδιότητας a(b+c) = ab+ac. Η δεύτερη επιμεριστική ιδιότητα (b+c)a =ba+ca απορρέει από την αντιμεταθετικότητα του πολλαπλασιασμού. Το στοιχείο 0 ονομάζεται μηδενικό στοιχείο και το 1 ονομάζεται πολλαπλασιαστικό μοναδιαίο στοιχείο ή απλά μονάδα.

Ορισμός 4.5: Πεπερασμένο σώμα είναι ένα σώμα που περιέχει πεπερασμένο αριθμό στοιχείων, και ο αριθμός αυτός ονομάζεται τάξη του σώματος. Τα πεπερασμένα σώματα ονομάζονται και σώματα Galois.

Πρόταση 4.1: Εάν ο ακέραιος p είναι πρώτος, τότε η αλγεβρική δομή (Zp,+, ·) είναι σώμα.

Το σώμα (Z_p,+, ·), που ονομάζεται *σώμα κλάσεων υπολοίπων modulo p*, συμβολίζεται απλά ως Z_p ή F_p, και αποτελεί το πρώτο παράδειγμα πεπερασμένου σώματος [26], [27].

Ορισμός 4.6: Έστω F πεπερασμένο σώμα και έστω θετικός ακέραιος m τέτοιος ώστε mα = 0 για κάθε α ∈ F. Τότε, ο ελάχιστος θετικός ακέραιος με αυτήν την ιδιότητα ονομάζεται χαρακτηριστική του σώματος F, ή ισοδύναμα, λέμε ότι το σώμα F έχει χαρακτηριστική m.

Θεώρημα 4.1: Η χαρακτηριστική ενός πεπερασμένου σώματος F είναι πρώτος αριθμός.
Ένα σώμα είναι δυνατό να περιέχει υποσώματα. Το υποσύνολο K του σώματος F, το οποίο είναι σώμα ως προς τις πράξεις του F ονομάζεται υπόσωμα του F. Αντίστοιχα, το F ονομάζεται επέκταση του σώματος K. Εάν K ⊂ F, τότε λέμε ότι το K είναι γνήσιο υπόσωμα του F. Συνεπώς, το σώμα F_{p^n} έχει χαρακτηριστική p και περιέχει το F_p ως υπόσωμα. [14]

Θεώρημα 4.2: Αποδεικνύεται ότι για κάθε πεπερασμένο σώμα F, η πολλαπλασιαστική ομάδα F∗ είναι κυκλική.

Ορισμός 4.7: Ο γεννήτορας της κυκλικής ομάδας $F^*_{p^n}$ ονομάζεται πρωταρχικό στοιχείο του F_{p^n}. Το πολυώνυμο με ρίζες πρωταρχικά στοιχεία ονομάζεται πρωταρχικό πολυώνυμο [14]

4.1.2 Αναπαράσταση στοιχείων

Το πεπερασμένο σώμα F_{p^n} είναι n–διάστατος διανυσματικός χώρος στο F_p. Κάθε σύνολο n γραμμικώς ανεξάρτητων στοιχείων δύνανται να χρησιμοποιηθούν ως βάση του διανυσματικού χώρου. Διακρίνουμε δύο ιδιαίτερα σημαντικές βάσεις του F_{p^n} .

Η πρώτη είναι η πολυωνυμική βάση:

$\{1, \alpha, \ldots, \alpha^{n-1}\}$, που χρησιμοποιείται για την κατασκευή του F_{p^n} από ένα ανάγωγο πολυώνυμο f(z) στο F_p βαθμού n με $f(\alpha) = 0$.

Η δεύτερη είναι η κανονική βάση $\{\alpha, \alpha_p, \ldots, a^{p^{n-1}}\}$ στην περίπτωση που τα ανωτέρω στοιχεία είναι γραμμικά ανεξάρτητα στο F_p.

πολυωνυμική βάση			κανονική βάση			εκθετική
α^0	α^1	α^2	α^3	α^6	α^5	α^i
0	0	0	0	0	0	∞
1	0	0	1	1	1	0
0	1	0	0	1	1	1
0	0	1	1	0	1	2
1	1	0	1	0	0	3
0	1	1	1	1	0	4
1	1	1	0	0	1	5
1	0	1	0	1	0	6

Πίνακας 4.1: Αναπαραστάσεις του πεπερασμένου σώματος F_{2^3} όπως ορίζεται από το πολυώνυμο $f(z) = 1 + z + z^3$, όπου $f(\alpha) = 0$.

4.1.3 Κατασκευή Πεπερασμένων Σωμάτων

Το $Fp = \{0, 1, \ldots, p - 1\}$ είναι πεπερασμένο σώμα τάξης p, όπου p πρώτος αριθμός, και οι πράξεις της πρόσθεσης + και του πολλαπλασιασμού · πραγματοποιούνται modulo p. Ας θεωρήσουμε το θετικό ακέραιο n. Για να κατασκευάσουμε το πεπερασμένο σώμα F_{p^n} , τάξης p^n, επιλέγουμε ένα πολυώνυμο $f(z) \in F_p[z]$ βαθμού n το οποίο είναι ανάγωγο στο F_p. Επιπλέον, υποθέτουμε ότι α είναι στοιχείο τέτοιο ώστε $f(\alpha) = 0$.

Τότε, ορίζουμε $F_{p^n} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F_p\}$.

Θεώρημα 4.3: Το σύνολο F_{p^n} με πράξεις την πρόσθεση + και τον πολλαπλασιασμό ·,όπως ορίστηκαν παραπάνω, αποτελεί πεπερασμένο σώμα τάξης p^n.

Παράδειγμα. Ας θεωρήσουμε τον ακέραιο p = 2 και το πολυώνυμο $f(z) = 1 + z + z^3$, το οποίο είναι ανάγωγο (δηλαδή δεν διαιρείται από άλλο πολυώνυμο) στο F_2. Έστω α είναι ρίζα του πολυωνύμου f(z), και θεωρούμε το πεπερασμένο σώμα F_{2^3} που ορίζεται από τη σχέση $F_{2^3} = \{a_0 + a_1\alpha + a_2\alpha^2 : a_i \in F_2\}$.

Από τον Πίνακα 4.1 παρατηρούμε ότι $F_{2^3}^* = <a>$ δηλ. τα μη–μηδενικά στοιχεία του F_{2^3} αποτελούν κυκλική ομάδα τάξης 7 με γεννήτορα το στοιχείο α, όπου $\alpha^7 = 1$.

ως διάνυσμα	ως πολυώνυμο	ως δυνάμεις
0000	0	0
1000	1	1
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$1+\alpha$	α^4
0110	$\alpha+\alpha^2$	α^5
0011	$\alpha^2+\alpha^3$	α^6
1101	$1+\alpha+\alpha^3$	α^7
1010	$1+\alpha^2$	α^8
0101	$\alpha+\alpha^3$	α^9
1110	$1+\alpha+\alpha^2$	α^{10}
0111	$\alpha+\alpha^2+\alpha^3$	α^{11}
1111	$1+\alpha+\alpha^2+\alpha^3$	α^{12}
1011	$1+\alpha^2+\alpha^3$	α^{13}
1001	$1+\alpha^3$	α^{14}

Πίνακας 4.2: Τα στοιχεία του σώματος F_{2^4} , που ορίζεται από το πολυώνυμο $f(z) = 1 + z + z^4$ και $f(\alpha) = 0$

Συμπέρασμα: Κάθε διάνυσμα n στοιχείων (που αποτελείται από 0 ή 1) αντιστοιχεί σε ένα συγκεκριμένο στοιχείο του πεπερασμένου σώματος 2^n στοιχείων (το στοιχείο αυτό είναι μοναδικό). Το διάνυσμα αποτελεί τη διανυσματική αναπαράσταση του στοιχείου, το οποίο όμως έχει και εκθετική αναπαράσταση. Επίσης, για δοθέν πρωταρχικό στοιχείο a, γράφεται κατά μοναδικό τρόπο ως a^k για κάποιο k.

Κατά συνέπεια, μία λογική συνάρτηση f (Boolean function) μπορεί να περιγραφεί, εκτός από τον αναλυτικό πίνακα αληθείας της, και από το σύνολο των γραμμών του πίνακα αληθείας της οι οποίες αντιστοιχούν σε έξοδο ίση με 1. Το σύνολο αυτό (που, στην ουσία, είναι σύνολο διανυσμάτων μεγέθους n για μία συνάρτηση n μεταβλητών) ονομάζεται support της f (συμβολίζεται με supp(f)). Με βάση την παραπάνω ανάλυση, όπου αναδεικνύεται ότι υπάρχει μία ισοδυναμία μεταξύ των δυαδικών διανυσμάτων μεγέθους n και των στοιχείων του πεπερασμένου σώματος με 2^n στοιχεία, προκύπτει ότι το support μιας λογικής συνάρτησης (δηλ. τα διανύσματα τα οποία, αν τεθούν στην είσοδο, δίνουν έξοδο 1) μπορεί να περιγραφεί και ως σύνολο στοιχείων πεπερασμένου σώματος, τα οποία κάλλιστα μπορούν να γραφούν σε εκθετική μορφή. Η ανάλυση αυτή συχνά βοηθά στο να αναλύονται κρυπτογραφικές ιδιότητες των λογικών συναρτήσεων.

4.2 Εργαλεία που χρησιμοποιήθηκαν

Για τη μελέτη των συναρτήσεων χρησιμοποιήθηκαν τρία απαραίτητα εργαλεία λογισμικού, η γλώσσα προγραμματισμού R[31] , το λογισμικό MATLAB[22] και η ειδικού τύπου εφαρμογή FAA Equation Finder [12] .

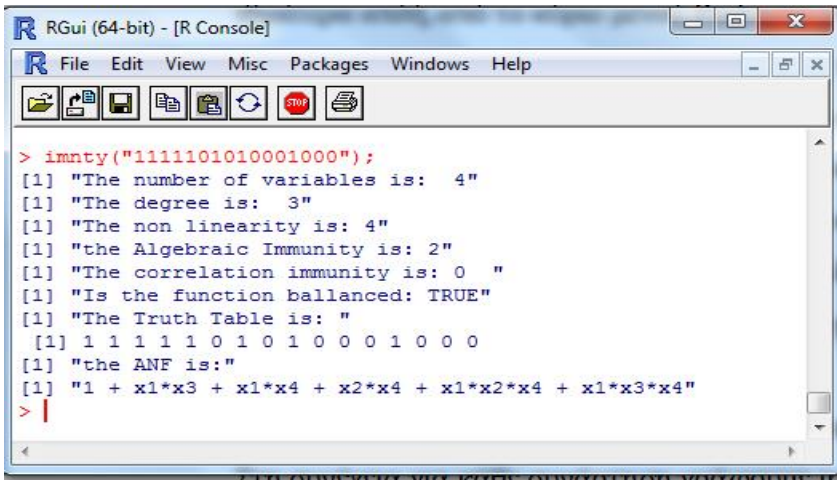
4.2.1 Η γλώσσα προγραμματισμού R

Το R είναι ένα υπολογιστικό πακέτο, όπως επίσης και μια γλώσσα προγραμματισμού, που προσφέρει δυνατότητες διαχείρισης και στατιστικής ανάλυσης δεδομένων καθώς και δυνατότητες κατασκευής γραφημάτων. Βασίζεται στην γλώσσα προγραμματισμού S (Bell Laboratories) και πρόκειται για λογισμικό ανοικτού κώδικα (open source) που διατίθεται ελεύθερα.

Η R μπορεί να χρησιμοποιηθεί είτε απευθείας με χρήση εντολών είτε να δημιουργήσει ο χρήστης τα δικά του προγράμματα. Επίσης είναι διαθέσιμα πολλά πακέτα, τα οποία διατίθενται ελεύθερα, προσανατολισμένα σε συγκεκριμένα πεδία. Στην παρούσα Διπλωματική Διατριβή χρησιμοποιήθηκε το πακέτο Boolfun. Το συγκεκριμένο πακέτο έχει έτοιμες υλοποιημένες συναρτήσεις για τις κρυπτογραφικές ιδιότητες των λογικών συναρτήσεων.

Για να χρησιμοποιηθεί το πακέτο Boolfun θα πρέπει πρώτα να εγκατασταθεί. Η διαδικασία είναι ιδιαίτερα απλή, από το κύριο μενού Packages -> Install Package(s) και επιλέγουμε Boolfun. Αφού το πακέτο εγκατασταθεί θα πρέπει κάθε φορά που ανοίγουμε το R να φορτώνεται το πακέτο με την εντολή library("boolfun"); ή από το κύριο μενού Packages -> Load Package.

Το γραφικό περιβάλλον της R είναι αρκετά εύχρηστο και φιλικό προς το χρήστη.



Εικόνα 4.1: Γραφικό περιβάλλον (GUI) της γλώσσας R.

Χρησιμοποιώντας τις δυνατότητες του πακέτου και της γλώσσας αναπτύχθηκε ένα πρόγραμμα το οποίο δέχεται ως είσοδο τον πίνακα αλήθειας μιας λογικής συνάρτησης και στην έξοδό του εκτυπώνει τις κρυπτογραφικές ιδιότητες της συνάρτησης: βαθμό (degree), μη γραμμικότητα (nonlinearity), αλγεβρική ανθεκτικότητα (algebraic immunity), ανθεκτικότητα σε συσχετίσεις (correlation immunity), ελέγχει αν η συνάρτηση είναι ισοβαρής, ενώ επίσης επιστρέφει και την Αλγεβρική Κανονική μορφή της.

Για να εκτελέσουμε το πρόγραμμα θα πρέπει πρώτα να το φορτώσουμε (File -> Source R code). Στη συνέχεια για κάθε συνάρτηση γράφουμε imnty("πίνακας αλήθειας σε δυαδική μορφή"); για παράδειγμα imnty("1111101010001000");

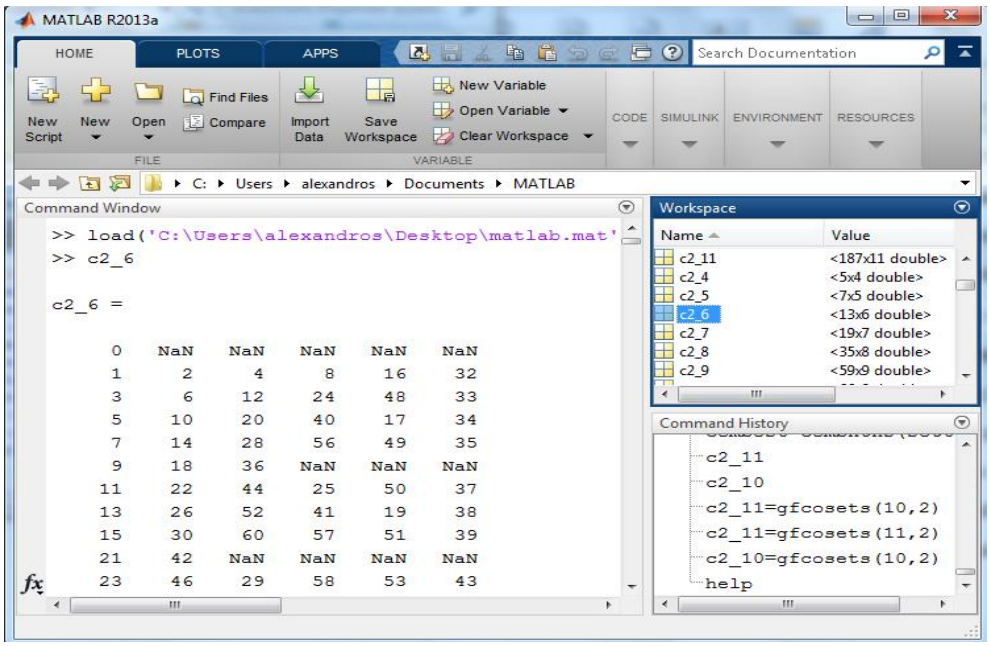
```
library("R.oo");
library("boolfun");

immunity<-function(x) {
        print(sprintf("The number of variables is:  %d",n(x)));
        print(sprintf("The degree is:  %d", deg(x)));
        print(sprintf("The non linearity is: %d", nl(x)));
        print(sprintf("the Algebraic Immunity is: %d",ai(x)));
        print(sprintf("The correlation immunity is: %d  ",ci(x)));
        print(sprintf("Is the function ballanced: %s", isBal(x)));
        print("The Truth Table is: ");
        print(tt(x));
        print("the ANF is:");
        print(ANF(x));
}

imnty<-function (y) {
k<-BooleanFunction(y);
immunity(k);
}
```

Εικόνα 4.2: Κώδικας προγράμματος σε γλώσσα R για τη μελέτη των κρυπτογραφικών κριτηρίων των συναρτήσεων.

4.2.2 Το λογισμικό MATLAB

Το λογισμικό MATLAB, που παίρνει το όνομά του από τις λέξεις MATrix LABoratory, είναι ένα σύγχρονο ολοκληρωμένο μαθηματικό πακέτο που χρησιμοποιείται εκτενώς στα πανεπιστήμια και στη βιομηχανία. Είναι ένα διαδραστικό (interactive) πρόγραμμα για αριθμητικούς υπολογισμούς και για κατασκευή γραφημάτων, αλλά παρέχει επίσης και τη δυνατότητα προγραμματισμού, κάτι που το καθιστά ένα χρησιμότατο εργαλείο για όλους όσους ασχολούνται με τις θετικές επιστήμες (και όχι μόνο).

Όπως υποδηλώνεται και από το όνομα του, το MATLAB είναι ειδικά σχεδιασμένο για υπολογισμούς με πίνακες, όπως η επίλυση γραμμικών συστημάτων, η εύρεση ιδιοτιμών και ιδιοδιανυσμάτων, η αντιστροφή τετραγωνικού πίνακα κλπ. Επιπλέον το πακέτο αυτό είναι εφοδιασμένο με πολλές επιλογές για γραφικά (δηλ. την κατασκευή γραφικών παραστάσεων) και προγράμματα γραμμένα στη δική του γλώσσα προγραμματισμού για την επίλυση άλλων προβλημάτων όπως η εύρεση των ριζών μη γραμμικής εξίσωσης, η επίλυση μη γραμμικών συστημάτων, η επίλυση προβλημάτων αρχικών τιμών με συνήθεις διαφορικές εξισώσεις κ.α. Η γλώσσα προγραμματισμού του MATLAB δίνει την ευχέρεια στον χρήστη να το επεκτείνει με δικά του προγράμματα. Επίσης ως MATLAB αναφέρεται η γλώσσα προγραμματισμού και όχι το πακέτο MATLAB. Το περιβάλλον εργασίας της MATLAB είναι εύχρηστο, αλλά θα πρέπει να σημειωθεί η πληθώρα επιλογών και εντολών που υπάρχουν το καθιστούν λίγο δύσκολο στη χρήση.



Εικόνα 4.3: Περιβάλλον εργασίας MATLAB

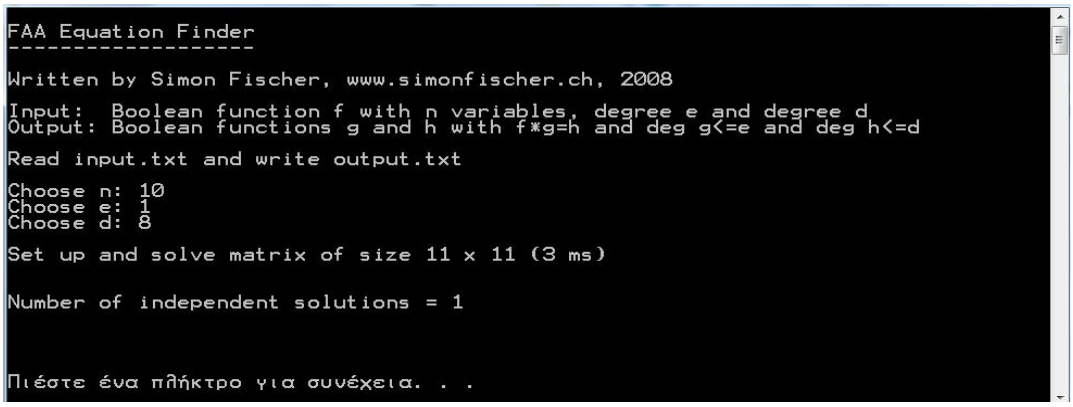
4.2.3 Λογισμικό για έλεγχο των γρήγορων αλγεβρικών επιθέσεων

Το λογισμικό FAA Equation Finder Version 1.0 είναι ένα πρόγραμμα για windows (console application) το οποίο δημιουργήθηκε από τον Simon Fischer και διατίθεται ελεύθερα. [12]

Το πρόγραμμα δέχεται ως είσοδο τον πίνακα αλήθειας μια συνάρτησης η οποία θα πρέπει να αποθηκευτεί στο αρχείο Input.txt. Στη συνέχεια ο χρήστης δίνει το βαθμό της συνάρτησης (ώστε να γίνει έλεγχος για πιθανά σφάλματα) , το άνω όριο για το βαθμό της συνάρτησης g (deg(g)=e)

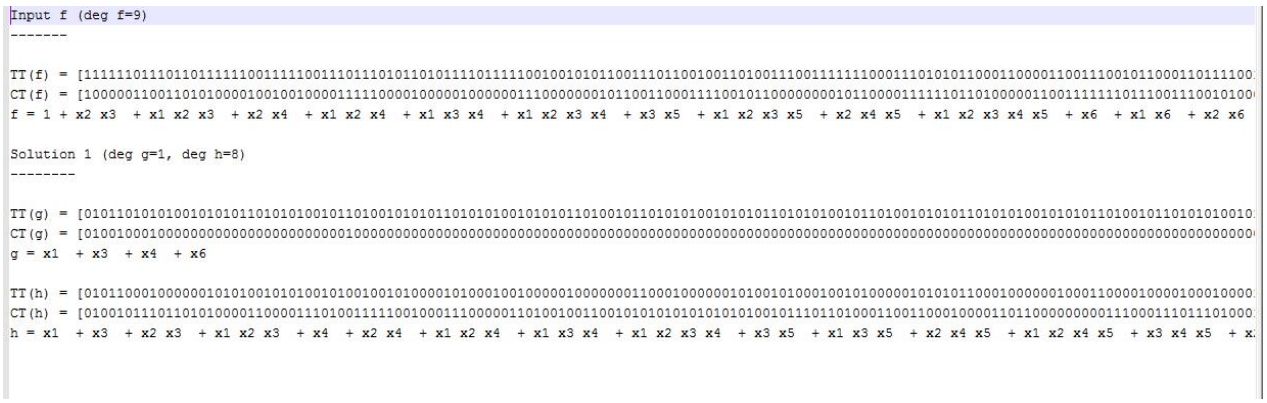
και τον επιθυμητό άνω όριο για το βαθμό της h (deg(h)=d). Η έξοδος αποθηκεύεται στο αρχείο output.txt .

Σημείωση: το αρχείο Input.txt και το πρόγραμμα FAAconsole.exe θα πρέπει να βρίσκονται στον ίδιο φάκελο. Στον ίδιο φάκελο θα παραχθεί και το αποτέλεσμα.



Εικόνα 4.4: FAA Equation Finder console

Στην εικόνα 4.4 φαίνεται το περιβάλλον εργασίας του προγράμματος. Για μια συνάρτηση 10 μεταβλητών ψάχνουμε g πρώτου βαθμού ώστε η h=fg να είναι βαθμού 8. Όπως φαίνεται στην εικόνα 4.5 έχουμε ένα αποτέλεσμα. Στο αποτέλεσμα βλέπουμε την αλγεβρική κανονική μορφή των συναρτήσεων και τους πίνακες αλήθειας.

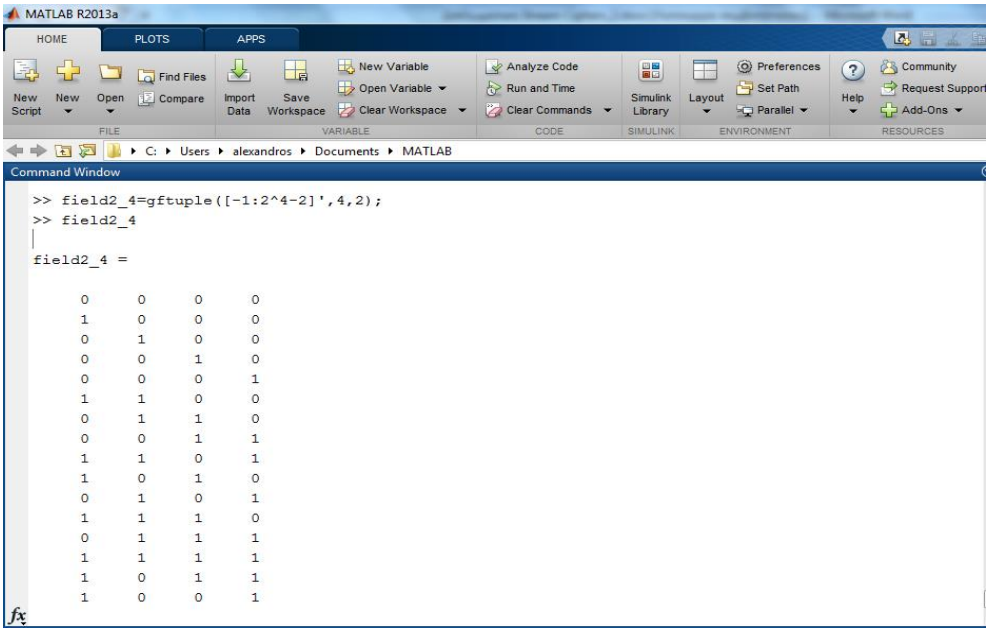


Εικόνα 4.5: Έξοδος προγράμματος FAA Equation Finder.

4.3 Συναρτήσεις Carlet-Feng

Οι Carlet–Feng περιγράψανε μια κλάση συναρτήσεων με μέγιστη αλγεβρική ανθεκτικότητα[03]. Οι συναρτήσεις αυτές περιγράφονται καλύτερα με την αναπαράσταση σε πεπερασμένα σώματα. Το support των συναρτήσεων αυτών περιγράφεται από τα στοιχεία $0, a^0, a^1, a^2, ..., a^{2^{(n-1)}-2}$ του πεπερασμένου σώματος GF(2^n) με 2^n στοιχεία (όπου α ένα οποιοδήποτε πρωταρχικό στοιχείο του σώματος). Για να μελετήσουμε τις κρυπτογραφικές ιδιότητες αυτών των συναρτήσεων θα μετατρέπουμε τα στοιχεία ενός πεπερασμένου σώματος στη δυαδική τους αναπαράσταση. Αυτό θα γίνει με τη βοήθεια της MATLAB Και συγκεκριμένα με την εντολή gftuple. Έπειτα, αφού φτιάξουμε τους πίνακες αλήθειας, με τη βοήθεια της R και του πακέτου Boolfun θα μελετήσουμε τις ιδιότητες της συνάρτησης.

Για να βρούμε όλα τα στοιχεία του πεδίου p^m χρησιμοποιούμε την εντολή field=gftuple([-1:p^m-2]',m,p)



Εικόνα 4.6: Το περιβάλλον εργασίας της MATLAB- εκτέλεση εντολής gfuple

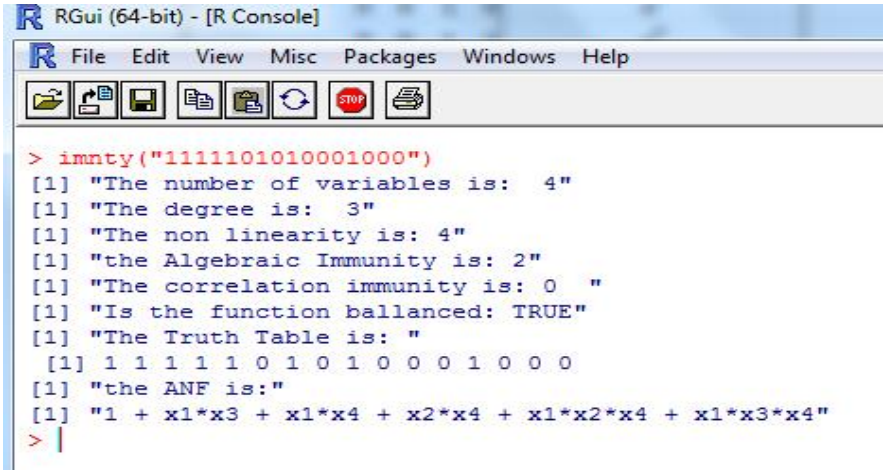
Τα στοιχεία είναι ταξινομημένα σύμφωνα με το πρωταρχικό τους πολυώνυμο $0, a^0, a^1, a^2, ..., a^{2^{(n-1)}}$ όπως στον πίνακα 4.2.

Βρίσκουμε τον πίνακα αλήθειας , όπου το support του είναι στις θέσεις $0, a^0, a^1, a^2, ..., a^6$

Δυαδική Αναπαράσταση	Εκθετική Αναπαράσταση	Πίνακας Αλήθειας για Carlet-Feng
0 0 0 0	0	1
0 0 0 1	a^3	1
0 0 1 0	a^2	1
0 0 1 1	a^6	1
0 1 0 0	a^1	1
0 1 0 1	a^9	0
0 1 1 0	a^5	1
0 1 1 1	a^{11}	0
1 0 0 0	a^0	1
1 0 0 1	a^{14}	0
1 0 1 0	a^8	0
1 0 1 1	a^{13}	0
1 1 0 0	a^4	1
1 1 0 1	a^7	0
1 1 1 0	a^{10}	0
1 1 1 1	a^{12}	0

Πίνακας 4.3: Εύρεση του πίνακα αλήθειας για μια συνάρτηση Carlet- Feng στο πεδίο F_{2^4}

Αν εκτελέσουμε στο περιβάλλον της R το πρόγραμμα, θα μας δώσει τα αποτελέσματα της εικόνας 4.7:



Εικόνα 4.7: Περιβάλλον εργασίας της R – Κρυπτογραφικές ιδιότητες της συνάρτησης με πίνακα αλήθειας "1111101010001000"

Παρατηρούμε ότι πράγματι η συνάρτηση έχει μέγιστο algebraic immunity αλλά και ελάχιστο correlation immunity (ουσιαστικά, δεν παρέχει ασφάλεια σε επιθέσεις συσχέτισης). Θα δοκιμάσουμε και για τα υπόλοιπα πεδία.

Ακολουθώντας την ίδια διαδικασία βρίσκουμε για τις υπόλοιπες συναρτήσεις ότι έχουν μέγιστο algebraic immunity και ελάχιστο correlation immunity.

Για το πεδίο 2^6:

> imnty("11111111010101111001000110010101010010010010000111100011000100001");

[1] "The number of variables is: 6"

[1] "The degree is: 5"

[1] "The non linearity is: 22"

[1] "the Algebraic Immunity is: 3"

[1] "The correlation immunity is: 0 "

[1] "Is the function ballanced: TRUE"

.....

Για το πεδίο 2^8:

>
imnty('11111110101110011100101111000011101000001101111011100001010011101001100100010000101100111010110011101010000101100011000110111101110101111000011001010010010101001001101000001110100110011111001011010011100100010110110101000001011001110111100010')

[1] "The number of variables is: 8"

[1] "The degree is: 7"

[1] "The non linearity is: 112"

[1] "the Algebraic Immunity is: 4"

[1] "The correlation immunity is: 0 "

[1] "Is the function ballanced: TRUE"

Εικόνα 4.8: Αποτέλεσμα συνάρτησης Carlet- Feng για n=8

Για το πεδίο 2^{10}:

>
imnty('11111101110110111111001111100111011010110101111011111001001010110011101100100111010011100111111100011101010110001100001100111001011000111011100111101100011101110000101000100001011101011011111100000000101000110001101000110001100110010011011000001001110101111011101010011110111010001010100100110111001000101001011011111110011011110100101011001010010010100110000111010000110110010110110000000000100110001101011110111110101010010100110000101010011111000111001010101110110000110100110100100101001010011111101110000000101110000011000001000111000000110101100000101001111001000101000010101011101100101101010100000100000011101100001010011011001100011101001100111000101100111010000111001010')

[1] "The number of variables is: 10"

[1] "The degree is: 9"

[1] "The non linearity is: 464"

[1] "the Algebraic Immunity is: 5"

[1] "The correlation immunity is: 0 "

[1] "Is the function ballanced: TRUE"

.....

Εικόνα 4.9: Αποτέλεσμα συνάρτησης Carlet- Feng για n=10

Συγκεντρωτικά τα αποτελέσματα για τις συναρτήσεις Carlet-Feng φαίνονται στον πίνακα 4.4.

Συνάρτηση Carlet-Feng	degree	nonlinearity	algebraic immunity	correlation immunity
n=4	deg=3	nl=4	ai=2	ci=0
n=5	deg=4	nl=10	ai=3	ci=0
n=6	deg=5	nl=22	ai=3	ci=0
n=7	deg=6	nl=54	ai=4	ci=0
n=8	deg=7	nl=112	ai=4	ci=0
n=9	deg=8	nl=232	ai=5	ci=0
n=10	deg=9	nl=464	ai=5	ci=0
n=11	deg=10	nl=980	ai=6	ci=0

Πίνακας 4.4: Κρυπτογραφικές ιδιότητες συναρτήσεων Carlet-Feng

Οι ίδιες συναρτήσεις δοκιμάστηκαν και για τις γρήγορες αλγεβρικές επιθέσεις με το πρόγραμμα FAA Equation Finder και αποδείχθηκε ότι είχαν ικανοποιητικά αποτελέσματα αλλά όχι τα βέλτιστα δυνατά. Συνήθως υπάρχουν συναρτήσεις g,h με βαθμούς e,και d αντίστοιχα (βλέπε Ενότητα 3.3) τέτοια ώστε e+d<n όπως φαίνεται στον Πίνακα 4.5 , αλλά συνήθως είναι e+d=n-1 (δηλαδή σχεδόν βέλτιστη συμπεριφορά ως προς τις γρήγορες αλγεβρικές επιθέσεις).

Συναρτήσεις Carlet-Feng	e	d	# συναρτήσεων g
n=4	1	2	1
	1	1	0
n=5	1	3	0
	2	2	0
n=6	1	4	1
	1	3	0
	2	3	0
n=7	1	5	0
	2	4	1
	2	3	0
	3	3	0
n=8	1	6	1
	1	5	0
	2	5	1
	2	4	0
n=9	1	7	0
	2	6	0
	3	5	0
	4	4	0
n=10	1	8	1
	1	7	0
	2	7	0
	3	6	4
	3	5	0
n=11	1	9	0
	2	8	1
	2	7	0
	3	7	0

Πίνακας 4.5: Fast Algebraic Attacks για συναρτήσεις Carlet- Feng

4.4 Κυκλοτομικές Κλάσεις (Cyclotomic Cosets)

Η κυκλοτομική κλάση του s modulo p^n, συμβολίζεται με C_s, και περιέχει τους ακεραίους $C_s = \{s, sp, \ldots, sp^{n_s-1}\}$, όπου n_s είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $sp^{n_s} \equiv s \pmod{p^n-1}$. Κάθε coset δηλαδή, αποτελείται από στοιχεία που το ένα είναι διπλάσιο του άλλου (mod 2^n-1).

Παράδειγμα. Έστω p = 2 και n = 4 (σώμα $GF(2^4)$). Οι κυκλοτομικές κλάσεις mod 15 είναι οι:
C1 = {1, 2, 4, 8} , C5 = {5, 10} ,C3 = {3, 6, 12, 9} , C7 = {7, 14, 13, 11} ,όπου πάντα έχουμε και την κυκλοτομική κλάση C0 = {0}.

Το MATLAB έχει εντολή γα την εύρεση των cosets ενός πεπερασμένου σώματος. Η εντολή γα τα πεδία Galois είναι η $gf\,\cos ets(m, p)$, όπου p πρώτος αριθμός για τις συναρτήσεις που μας ενδιαφέρουν, το p είναι πάντα ίσο με δύο.
Για το πεδίο $GF(2^8)$ έχουμε το αποτέλεσμα της εικόνας 4.10.

4.4.1 Συναρτήσεις που δημιουργούνται από cosets.

Στη συνέχεια θα μελετηθούν συναρτήσεις οι οποίες θα έχουν τα εξής χαρακτηριστικά: το support τους θα "καλύπτει" πλήρως συγκεκριμένα cosets (στην αναπαράστασή τους στο πεπερασμένο σώμα) και θα είναι ισοβαρής.

Οι συγκεκριμένες συναρτήσεις δεν έχουν μελετηθεί μέχρι σήμερα ως προς την αλγεβρική τους ανθεκτικότητα. Το κίνητρο που τις κοιτάμε είναι ότι ανήκουν σε μία ευρύτερη κατηγορία συναρτήσεων με το όνομα idempotents, οι οποίες γενικά είναι γνωστό ότι μπορούν να επιτύχουν υψηλή μη γραμμικότητα.
Πιο συγκεκριμένα, Idempotent είναι κάθε συνάρτηση η οποία έχει σταθερή τιμή σε κάθε κυκλοτομική κλάση - δηλαδή, αν για μία είσοδο η έξοδος είναι 1, τότε για οποιαδήποτε άλλη είσοδο του ίδιου coset η έξοδος είναι επίσης 1.
Παράδειγμα: Για το πεδίο $GF(2^4)$ μπορούν να χρησιμοποιηθούν το πρώτο, το τρίτο και το πέμπτο coset ως εκείνα που θα απαρτίζουν το support της f.
C1 = {1, 2, 4, 8}, C3 = {3, 6, 12, 9} , C7 = {7, 14, 13, 11}

```
>> gfcosets(8,2)
ans =
   0  NaN  NaN  NaN  NaN  NaN  NaN  NaN
   1    2    4    8   16   32   64  128
   3    6   12   24   48   96  192  129
   5   10   20   40   80  160   65  130
   7   14   28   56  112  224  193  131
   9   18   36   72  144   33   66  132
  11   22   44   88  176   97  194  133
  13   26   52  104  208  161   67  134
  15   30   60  120  240  225  195  135
  17   34   68  136  NaN  NaN  NaN  NaN
  19   38   76  152   49   98  196  137
  21   42   84  168   81  162   69  138
  23   46   92  184  113  226  197  139
  25   50  100  200  145   35   70  140
  27   54  108  216  177   99  198  141
  29   58  116  232  209  163   71  142
  31   62  124  248  241  227  199  143
  37   74  148   41   82  164   73  146
  39   78  156   57  114  228  201  147
  43   86  172   89  178  101  202  149
  45   90  180  105  210  165   75  150
  47   94  188  121  242  229  203  151
  51  102  204  153  NaN  NaN  NaN  NaN
  53  106  212  169   83  166   77  154
  55  110  220  185  115  230  205  155
  59  118  236  217  179  103  206  157
  61  122  244  233  211  167   79  158
  63  126  252  249  243  231  207  159
  85  170  NaN  NaN  NaN  NaN  NaN  NaN
  87  174   93  186  117  234  213  171
  91  182  109  218  181  107  214  173
  95  190  125  250  245  235  215  175
 111  222  189  123  246  237  219  183
 119  238  221  187  NaN  NaN  NaN  NaN
 127  254  253  251  247  239  223  191
```

Εικόνα 4.10: Cossets 2^8

Οι συναρτήσεις που καλύπτουν τα κριτήρια είναι 3 , καθώς για να είναι ισοβαρής η συνάρτηση απαιτούνται 2 cosets και συνολικά υπάρχουν 3 που μπορούν να χρησιμοποιηθούν.

$$\binom{3}{2} = \frac{3!}{2!(3-2)!} = 3$$

Οι συναρτήσεις έχουν support:

1. $\{a^1, a^2, a^4, a^8, a^3, a^6, a^{12}, a^9\}$

2. $\{a^1, a^2, a^4, a^8, a^7, a^{14}, a^{13}, a^{11}\}$
3. $\{a^3, a^6, a^{12}, a^9, a^7, a^{14}, a^{13}, a^{11}\}$

Με τη βοήθεια του πίνακα 4.3 σχηματίζονται οι πίνακες αλήθειας των 3 συναρτήσεων:

Δυαδική Αναπαράσταση	Εκθετική Αναπαράσταση	Συνάρτηση 1 Πίνακας αλήθειας	Συνάρτηση 2 Πίνακας αλήθειας	Συνάρτηση 3 Πίνακας αλήθειας
0 0 0 0	0	0	0	0
0 0 0 1	a^3	1	0	1
0 0 1 0	a^2	1	1	0
0 0 1 1	a^6	1	0	1
0 1 0 0	a^1	1	1	0
0 1 0 1	a^9	1	0	1
0 1 1 0	a^5	0	0	0
0 1 1 1	a^{11}	0	1	1
1 0 0 0	a^0	0	0	0
1 0 0 1	a^{14}	0	1	1
1 0 1 0	a^8	1	1	0
1 0 1 1	a^{13}	0	1	1
1 1 0 0	a^4	1	1	0
1 1 0 1	a^7	0	1	1
1 1 1 0	a^{10}	0	0	0
1 1 1 1	a^{12}	1	0	1

Πίνακας 4.6: Πίνακες αλήθειας συναρτήσεων στο πεδίο 2^4

Με τη χρήση της εντολής combntns του MATLAB μπορούμε να βρούμε όλους τους πιθανούς συνδυασμούς των cosets. Θεωρούμε για κάθε coset ότι το όνομά του είναι το πρώτο του στοιχείο, δημιουργούμε ένα set με τα κατάλληλα coset και στη συνέχεια βρίσκουμε τους συνδυασμούς.

```
>> set4=[1,3,7]

set4 =

   1   3   7

>> combos2_4=combntns(set4,2);
>> combos2_4

combos2_4 =

   1   3
   1   7
   3   7
```

Εικόνα 4.11: Πιθανοί συνδυασμοί με εντολή του MATLAB

4.4.2 Μελέτη συναρτήσεων κατασκευασμένων από Cyclotomic cosets.

Για το πεδίο $GF(2^4)$ είδαμε στην προηγούμενη υποενότητα τον τρόπο κατασκευής των επιθυμητών συναρτήσεων. Τα αποτελέσματα που παίρνουμε με τη βοήθεια του R είναι τα εξής:

```
> imnty('0111110000101001')
[1] "The number of variables is:  4"
[1] "The degree is:  3"
[1] "The non linearity is: 4"
[1] "the Algebraic Immunity is: 2"
[1] "The correlation immunity is: 0  "
[1] "Is the function ballanced: TRUE"
[1] "The Truth Table is: "
 [1] 0 1 1 1 1 1 0 0 0 0 1 0 1 0 0 1
[1] "the ANF is:"
[1] "x1 + x2 + x3 + x1*x2 + x1*x3 + x1*x4 + x1*x2*x3"
```

Εικόνα 4.12: Αποτελέσματα εκτέλεσης του προγράμματος στο περιβάλλον R για την πρώτη συνάρτηση 4 μεταβλητών

```
> imnty('0010100101111100');
[1] "The number of variables is:  4"
[1] "The degree is:  3"
[1] "The non linearity is: 4"
[1] "the Algebraic Immunity is: 2"
[1] "The correlation immunity is: 0  "
[1] "Is the function ballanced: TRUE"
[1] "The Truth Table is: "
 [1] 0 0 1 0 1 0 0 1 0 1 1 1 1 1 0 0
[1] "the ANF is:"
[1] "x2 + x3 + x1*x2 + x1*x3 + x1*x4 + x1*x2*x3"
```

Εικόνα 4.13: Αποτελέσματα εκτέλεσης του προγράμματος στο περιβάλλον R για τη δεύτερη συνάρτηση 4 μεταβλητών

```
> imnty("0101010101010101");
[1] "The number of variables is:  4"
[1] "The degree is:  1"
[1] "The non linearity is: 0"
[1] "the Algebraic Immunity is: 1"
[1] "The correlation immunity is: 0  "
[1] "Is the function ballanced: TRUE"
[1] "The Truth Table is: "
 [1] 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
[1] "the ANF is:"
[1] "x1"
```

Εικόνα 4.14: Αποτελέσματα εκτέλεσης του προγράμματος στο περιβάλλον R για την τρίτη συνάρτηση 4 μεταβλητών

Παρατηρούμε ότι οι 2 από τις 3 συναρτήσεις έχουν μέγιστο algebraic immunity.

Επίσης θα πρέπει να σημειωθεί ότι για κάθε συνάρτηση f , η συμπληρωματική της $f \oplus 1$,έχει την ίδια ακριβώς αλγεβρική ανθεκτικότητα.

Η ανθεκτικότητα σε fast algebraic attacks δεν είναι μέγιστη όμως.

Συναρτήσεις κατασκευασμένες από cosets για n=4 με max algebraic immunity	e	d	# συναρτήσεων g
111110000101001	1	2	1
	1	1	0
10100101111100	1	2	1
	1	1	0

Πίνακας 4.7: Αποτελέσματα fast algebraic attack για n=4

Πεδίο $GF(2^5)$:

Τα cosets αυτού του πεδίου είναι τα :

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

Εικόνα 4.15: Cosets πεδίου GF(2^5)

Παρατηρούμε ότι για να είναι η συνάρτηση balanced θα πρέπει για το support να χρησιμοποιήσουμε 3 cosets εκ των 1,3,5,7,11,15 και το στοιχείο 0, ώστε να έχουμε 16 σημεία.
Οι συνδυασμοί που υπάρχουν (και επιπλέον το σημείο 0) απεικονίζονται στην εικόνα 4.16.

```
combos2_5 =

   1    3    5
   1    3    7
   1    3   11
   1    3   15
   1    5    7
   1    5   11
   1    5   15
   1    7   11
   1    7   15
   1   11   15
   3    5    7
   3    5   11
   3    5   15
   3    7   11
   3    7   15
   3   11   15
   5    7   11
   5    7   15
   5   11   15
   7   11   15
```

Εικόνα 4.16: Πιθανοί συνδυασμοί cosets για κατασκευή συναρτήσεων που καλύπτουν τον κανόνα

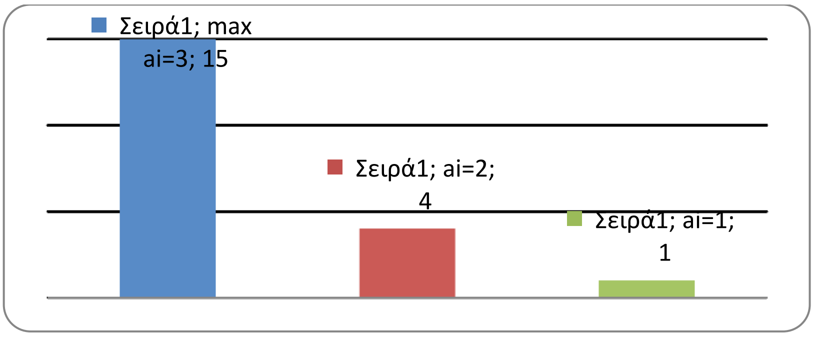
Τα αποτελέσματα που παίρνουμε για τις κρυπτογραφικές ιδιότητες φαίνονται στην εικόνα 4.17 , όπου deg είναι ο βαθμός της συνάρτησης, nl μη γραμμικότητα, ai η αλγεβρική ανθεκτικότητα και ci η ανθεκτικότητα σε συσχετίσεις.

Παρατηρούμε ότι μεγάλο ποσοστό των συναρτήσεων παρουσιάζουν μέγιστο algebraic immunity (εικόνα 4.18)

Αφού βρήκαμε τα αποτελέσματα για την αλγεβρική ανθεκτικότητα, στη συνέχεια δοκιμάζουμε τις γρήγορες αλγεβρικές επιθέσεις **μόνο** στις συναρτήσεις που έχουν μέγιστο algebraic immunity (ai).

coset 0,1,3,5	deg=4	nl=10	ai=3	ci=0	0 1 1 0 1 0 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0 1 0 0 0 0
coset 0,1,3,7	deg=4	nl=10	ai=3	ci=0	1 1 1 0 1 1 0 0 1 0 1 0 1 1 1 1 0 0 0 1 0 0 1 1 0 1 0 1 0 0 0 0
coset 0,1,3,11	deg=2	nl=12	ai=2	ci=0	1 1 1 1 1 0 0 1 1 0 1 0 0 0 1 1 0 0 0 0 0 1 1 0 0 1 0 1 1 1 0 0
coset 0,1,3,15	deg=4	nl=10	ai=3	ci=0	1 1 1 0 1 0 0 0 1 1 1 0 0 0 1 1 0 0 1 0 0 0 1 0 0 1 1 1 0 0 1 1
cosets 0,1,5,7	deg=4	nl=10	ai=3	ci=0	1 1 0 0 1 1 1 0 1 0 0 1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 1 0 0 0 0
cosets 0,1,5,11	deg=3	nl=12	ai=3	ci=0	1 1 0 1 1 0 1 1 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 0
cosets 0,1,5,15	deg=4	nl=10	ai=3	ci=0	1 1 0 0 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 0 1 0 1 0 1 0 1 1 0 0 1 1
cosets 0,1,7,11	deg=4	nl=10	ai=3	ci=0	1 1 0 1 1 1 0 1 1 0 0 0 1 1 0 0 0 0 0 1 0 1 1 1 0 0 0 1 1 1 0 0
cosets 0,1,7,15	deg=1	nl=0	ai=1	ci=1	1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
cosets 0,11,15	deg=4	nl=10	ai=3	ci=0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 1 1 1 1 1 1
cosets 0,3,5,7	deg=2	nl=12	ai=2	ci=0	1 0 1 0 0 1 1 0 0 0 1 1 1 1 1 1 0 1 0 1 1 0 0 1 1 1 0 0 0 0 0 0
coset 0,3,5,11	deg=4	nl=2	ai=2	ci=0	1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
coset 0,3,5,15	deg=3	nl=12	ai=3	ci=1	1 0 1 0 0 0 1 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 1 1 1 0 0 0 1 1
coset 0,3,7,11	deg=3	nl=12	ai=3	ci=0	1 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1 0 0 0 1 0 1 0 1 0 1 0 0 1 1 0 0
cosets 0,3,7,15	deg=4	nl=10	ai=3	ci=0	1 0 1 0 0 1 0 0 0 1 1 0 1 1 1 1 0 0 1 1 0 0 0 1 0 1 1 0 0 0 1 1
cosets 0,3,11,15	deg=3	nl=12	ai=3	ci=0	1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 0 1 0 0 1 0 0 0 1 1 0 1 1 1 1
cosets 0,5,7,11	deg=3	nl=12	ai=3	ci=1	1 0 0 1 0 1 1 1 0 0 0 1 1 1 0 0 0 1 0 1 1 1 0 1 1 0 0 0 1 1 0 0
cosets 0,5,7,15	deg=4	nl=10	ai=3	ci=0	1 0 0 0 0 1 1 0 0 1 0 1 1 1 0 0 0 1 1 1 1 0 0 1 1 0 1 0 0 0 1 1
cosets 0,5,11,15	deg=2	nl=12	ai=2	ci=0	1 0 0 1 0 0 1 1 0 1 0 1 0 0 0 0 0 1 1 0 1 1 0 0 1 0 1 0 1 1 1 1
cosets 0,7,11,15	deg=4	nl=10	ai=3	ci=0	1 0 0 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1

Εικόνα 4.17: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=5

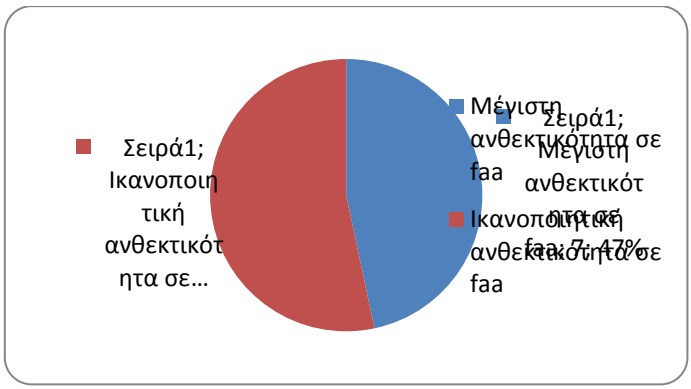


Εικόνα 4.18: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=5).

Συναρτήσεις κατασκευασμένες από cosets για n=5 με max algebraic immunity	e	d	# συναρτήσεων g
01101010101100111100101011010000	1	3	0
	2	2	0
11101100101011110001001101010000	1	3	4
	1	2	0
	2	2	0
11101000111000110010001001110011	1	3	0
	2	2	0
11001110100111000101101110010000	1	3	0
	2	2	0
11011011100100000100111010011100	1	3	2
	1	2	0
	2	2	0
11001010110100000110101010110011	1	3	0
	2	2	0
11011101100011000001011100011100	1	3	0
	2	2	0
11011001110000000010011000111111	1	3	4
	1	2	0
	2	2	0
10100010011100110110100011100011	1	3	2
	1	2	0
	2	2	0
10110101001011110001010101001100	1	3	2
	1	2	0
	2	2	0
10110101001011110001010101001100	1	3	0
	2	2	0
10110001011000110010010001101111	1	3	2
	1	2	0
	2	2	0
10010111000111000101110110001100	1	3	2
	1	2	0
	2	2	0
10000110010111000111100110100011	1	3	4
	1	2	0
	2	2	0
10010101010011000011010100101111	1	3	0
	2	2	0

Πίνακας 4.8: Αποτελέσματα fast algebraic attack για n=5

Παρατηρούμε ότι σχεδόν οι μισές από αυτές είναι ανθεκτικές σε fast algebraic attacks, ενώ οι υπόλοιπες έχουν σχεδόν βέλτιστη ανθεκτικότητα (e+d=n-1).



Εικόνα 4.19: Γραφική απεικόνιση της ανθεκτικότητας σε faa των συναρτήσεων με μέγιστη ai.

Για πεδία από $GF(2^6)$ και πάνω οι συνδυασμοί γίνονται πάρα πολλοί. Για το λόγο αυτό αντί να μελετηθούν όλες οι συναρτήσεις, θα θεωρούμε εκείνες που το support τους περιέχει μόνο εκείνα τα cosets των οποίων το βάρος (weight) είναι μικρότερο από n/2. Ως βάρος ορίζεται το πλήθος των '1' στη δυαδική αναπαράσταση των ακέραιων αριθμών που απαρτίζουν τα cosets (παρατηρούμε ότι τα στοιχεία ενός coset έχουν πάντα το ίδιο weight). Το μηδενικό στοιχείο, καθώς και το στοιχείο 1 (το οποίο αντιστοιχεί στο coset 0) μπορούν είτε να ανήκουν στο support είτε όχι. Παράδειγμα, για n=5, τα cosets αυτά είναι τα 1,3,5. Οπότε στο support θα έχουμε το μηδενικό στοιχείο και τα cosets 1,3,5. Σημειώνεται ότι αυτή η επιλογή έγινε λόγω του ότι, με αυτόν τον τρόπο, οι συναρτήσεις που εξετάζουμε προσομοιάζουν, ως προς τον τρόπο περιγραφής τους, τις συναρτήσεις πλειοψηφίας (majority functions) που αναφέραμε στην ενότητα 3.4 (αν και είναι διαφορετικές).
Για περιττούς n, με αυτό τον κανόνα προκύπτει μια και μοναδική συνάρτηση! Στη συνέχεια εργαζόμαστε ως εξής:

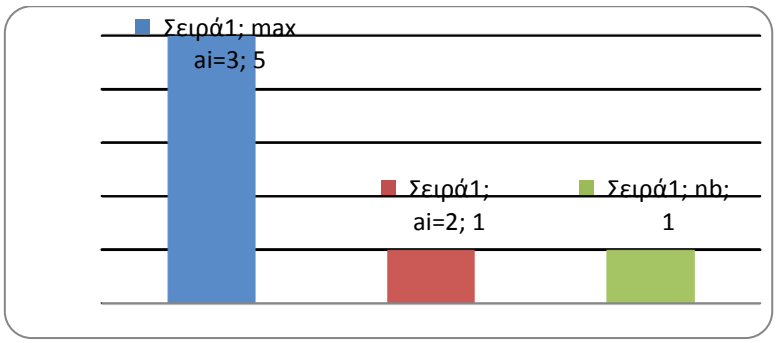
Αν θεωρήσουμε ότι το πρωταρχικό μας στοιχείο δεν είναι το a αλλά το a^3, τότε το support μας (με τον ίδιο κανόνα) περιέχει τα εξής cosets: $(\alpha^3)^1=\alpha^3$, $(\alpha^3)^3=\alpha^9$, $(\alpha^3)^5=\alpha^{15}$, δηλαδή τα cosets 3,5,15!!! (το α^9 είναι στο coset: 5 10 20 9 18)

Με τον ίδιο τρόπο μπορούμε να κατασκευάσουμε συναρτήσεις, όσες και τα πρωταρχικά πολυώνυμα.

Για n=6 , βρίσκουμε τις συναρτήσεις της εικόνας 4.20. Παρατηρούμε ότι 5 συναρτήσεις από τις 7 έχουν μέγιστη αλγεβρική ανθεκτικότητα.

deg=5	nl=20	ai=3	ci=0	0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 0 0 1 1 1 0 1 0 0 1 0 0 0 0 0 0 1 1 0
deg=4	nl=16	ai=2	ci=0	0 1 1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 0 1 0 1 0 1 1 1 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 0 0 1 1 0
	nb			0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 1 0
deg=3	nl=24	ai=3	ci=3	0 1 1 1 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 1 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 1 0 1 0 0 0 1 1 1 1 1 0 1 0 0 0 0 0 1 1 0
deg=5	nl=24	ai=3	ci=0	0 1 1 1 0 1 0 0 1 1 1 0 1 0 1 1 1 0 0 0 1 0 1 1 1 1 0 1 0 0 1 1 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 1 1 1 1 1 1 1 0 0 0 0 1 1 0
deg=5	nl=24	ai=3	ci=0	0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 1 1 1 1 1 1 0 0 0 0 1 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 1 1 1 0 0 0 1 0 1 1 1 1 0 1 0 0 1 1
deg=5	nl=24	ai=3	ci=0	0 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 1 1 1 1 1 1 0 0 1 0 0 1 1 0 0 0 0 1 1 0 1 0 0 1 0 0 0 1 0 0 0 1 1 1 1 1 1 1 0 0 1 0 0 1 1

Εικόνα 4.20: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=6



Εικόνα 4.21: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=6).

Δοκιμάζουμε αυτές τις 6 συναρτήσεις σε επιθέσεις fast algebraic attacks:

Συναρτήσεις κατασκευασμένες από cosets για n=6 με max algebraic immunity	e	d	# συναρτήσεων g
01111000111111111111000111100000000101000100111001110100100000110	1	4	5
	1	3	0
	2	3	4
	2	2	0
01110100111111111110000111101000100001001000101000111110100000110	1	4	7
	1	3	1
	1	2	0
	2	3	4
	2	2	0
01110100111010111000101111010011000010010010001000111111110000110	1	4	1
	1	3	0
	2	3	4
	2	2	0
00001001001000100011111110000110011101001110101110001011110100 11	1	4	1
	1	3	0
	2	3	4
	2	2	0
00100101101010101001111110010011000011010010001000111111100100 11	1	4	1
	1	3	0
	2	3	4
	2	2	0

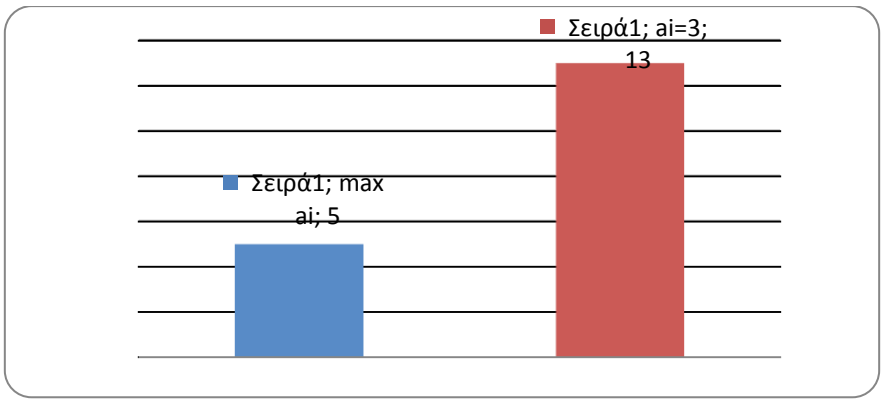
Πίνακας 4.9: Ανθεκτικότητα συναρτήσεων σε fast algebraic attacks

Για το $GF(2^7)$ κατασκευάστηκαν 18 συναρτήσεις. Οι κρυπτογραφικές ιδιότητες τους φαίνονται στην εικόνα 4.22: (αναλυτικά οι πίνακες αλήθειας στο παράρτημα 1).

Από τις συναρτήσεις που κατασκευάστηκαν με τον παραπάνω τρόπο, προκύπτουν τα παραπάνω δεδομένα. Οι 5 παρουσιάζουν μέγιστο algebraic immunity και οι υπόλοιπες max-1.

1	deg=5	nl=48	ai=4	ci=0
3	deg=4	nl=48	ai=3	ci=1
5	deg=6	nl=42	ai=3	ci=0
7	deg=6	nl=52	ai=3	ci=0
9	deg=5	nl=48	ai=4	ci=0
11	deg=5	nl=44	ai=3	ci=0
13	deg=5	nl=48	ai=4	ci=1
15	deg=5	nl=52	ai=3	ci=0
19	deg=6	nl=54	ai=3	ci=0
21	deg=5	nl=52	ai=4	ci=0
23	deg=6	nl=50	ai=4	ci=0
27	deg=5	nl=52	ai=3	ci=0
29	deg=6	nl=42	ai=3	ci=0
31	deg=6	nl=48	ai=3	ci=0
43	deg=6	nl=52	ai=3	ci=0
47	deg=5	nl=44	ai=3	ci=0
55	deg=6	nl=48	ai=3	ci=0
63	deg=6	nl=48	ai=3	ci=0

Εικόνα 4.22: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=7



Εικόνα 4.23: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=7).

Μελετώντας τις 5 συναρτήσεις για fast algebraic attacks βρίσκουμε τα εξής αποτελέσματα:

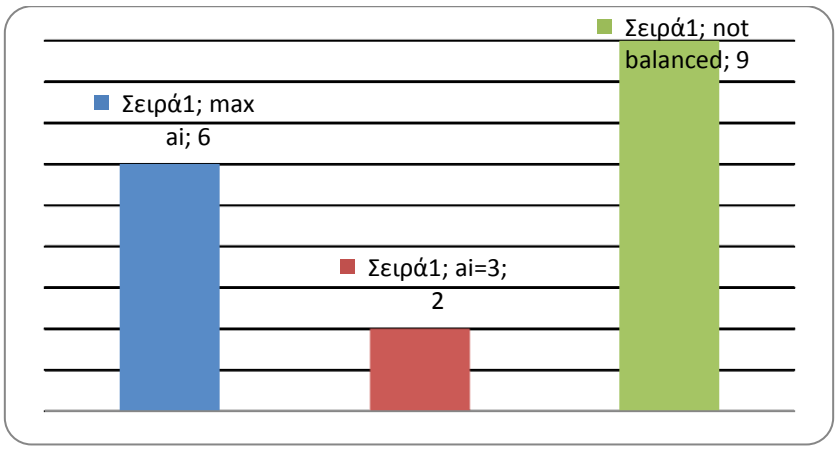
Συναρτήσεις κατασκευασμένες από cosets για n=7 με max algebraic immunity	e	d	# συναρτήσεων g
11111110111011011011110110110000100011110011010110001000100001110100111011110010001110110001000001110110100100000100	1	5	2
	1	4	0
	2	4	1
	2	3	0
10010011000111100111011001100111001101001101111101100101100001011000110010001110011101000011001101011110010000011111101000000001001	1	5	1
	1	4	0
	2	4	1
	2	3	0
11001011101100011001110100001100110010100001011011111010111111100010011001000010010101101101001100110001111111000000010110000011	1	5	2
	1	4	0
	2	4	1
	2	3	0
10110110010011000111010011111010011101011011010100010010111100110010110001000010110010101101001110111001111010001000110100000001	1	5	2
	1	4	0
	2	4	4
	2	3	0
10110100010011100110001011110011001101011110100100000101000000010101100110111101101010010010110011001110000000111111101001111100	1	5	0
	1	4	0
	2	4	1
	2	3	0

Πίνακας 4.10: Ανθεκτικότητα συναρτήσεων (n=7) σε fast algebraic attacks

Για το $GF(2^8)$, κατασκευάστηκαν με τον ίδιο κανόνα, 17 συναρτήσεις. Οι 6 από αυτές παρουσιάζουν μέγιστη αλγεβρική ανθεκτικότητα ενώ οι περισσότερες δεν είναι ισοβαρείς (nb)

1		deg=7	nl=96	ai=3	ci=0
285			nb		
299		deg=7	nl=106	ai=4	ci=0
301		deg=7	nl=110	ai=4	ci=0
333			nb		
351			nb		
355			nb		
357			nb		
361		deg=6	nl=104	ai=3	ci=0
369			nb		
391			nb		
397		deg=7	nl=104	ai=4	ci=0
425			nb		
451		deg=7	nl=96	ai=4	ci=0
463		deg=7	nl=108	ai=4	ci=0
487		deg=7	nl=104	ai=4	ci=0
501			nb		

Εικόνα 4.24: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=8



Εικόνα 4.25: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=8).

Οι 6 αυτές συναρτήσεις μελετήθηκαν ως προς την ανθεκτικότητά τους στις γρήγορες αλγεβρικές επιθέσεις. Τα αποτελέσματα περιέχονται στον πίνακα 4.11.

Συναρτήσεις κατασκευασμένες από cosets για n=8 με max algebraic immunity	e	d	# συναρτήσεων g
000111011111110000011101001101011010000001101111111101000001111110000100010 010101000111110101010010001111100101011001001110101010011111001000010101000 100010101001101111101001110000111011010011011110110100001010000010100101001 0101111010010011000110000111100	1	6	1
	1	5	0
	2	5	5
	2	4	0
	3	4	5
	3	3	0
000011000000000100111001101011010001101011100011101010100000000011001110100 10 110101100000111011010010000111111010010111100111001101001111010111110010111 0 000110000100010000001111111100011000011111011001010010001001111110011000100 1110111001010101011110011010100	1	6	3
	1	5	0
	2	5	1
	2	4	0
	3	4	7
	3	3	0
001000011011110111011100000000101111000000101100011100011110111001100010101 1 101011011110011101011011100000010001100000011011100010000100101100001101100 0 110011101011101111101100000011100111010000101110100111110110110001010101011 0011000100001011100001100111011	1	6	1
	1	5	1
	2	5	5
	2	4	0
	3	4	13
	3	3	0
011001100000100010011111110111110010101101011001010111100010111001000111111 010111011100101101100001110001000010101100111110010010110001000001001111011 111101111100001011000010000001101100111100011001111001110000001001000011010 0101110100010010110010100001011	1	6	3
	1	5	0
	2	5	9
	2	4	0
	3	4	1
	3	3	0
001110100100000110101111001111100110101110101110000110011101100001110010010 011011000001100011101101010011000010111001011001111110010001010111001100111 000001111110101011010010001111101100011101110001010100010110001000101011010	1	6	1
	1	5	0
	2	5	5
	2	4	0
	3	4	11
	3	3	0
001000011011110111011100000000101111000000101100011100011110111001100010101 1 101011011110011101011011100000010001100000011011100010000100101100001101100 0 110011101011101111101100000011100111010000101110100111110110110001010101011 0011000100001011100001100111011	1	6	1
	1	5	1
	2	5	5
	2	4	0
	3	4	13
	3	3	0

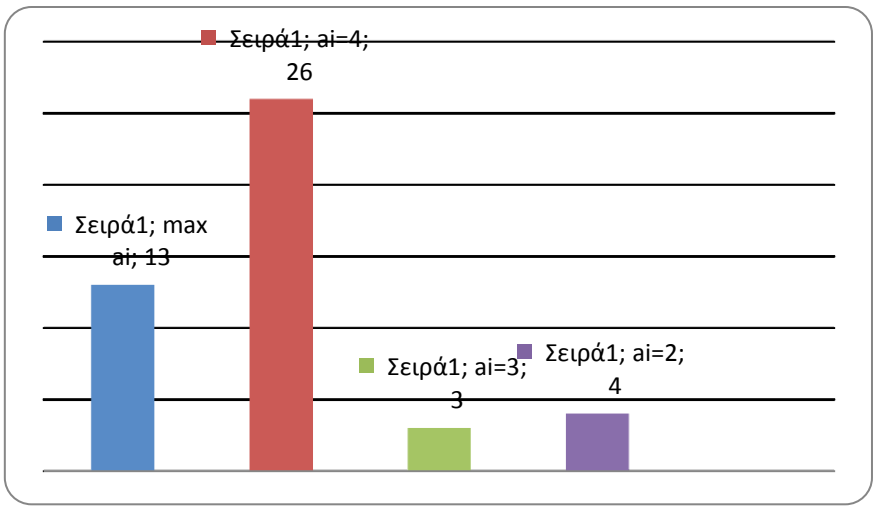
Πίνακας 4.11: Ανθεκτικότητα συναρτήσεων (n=8) σε fast algebraic attacks

Για το $GF(2^9)$ μελετήθηκαν 46 συναρτήσεις, όσες και τα πρωταρχικά πολυώνυμα:

deg=7	nl=224	ai=4	ci=0	deg=8	nl=218	ai=5	ci=0	deg=7	nl=224	ai=4	ci=0
deg=8	nl=228	ai=4	ci=0	deg=8	nl=226	ai=5	ci=0	deg=8	nl=206	ai=4	ci=0
	not balanced			deg=7	nl=216	ai=4	ci=0		not balanced		
deg=7	nl=224	ai=5	ci=0	deg=8	nl=230	ai=5	ci=0	deg=7	nl=188	ai=4	ci=0
deg=7	nl=216	ai=4	ci=0	deg=7	nl=232	ai=4	ci=0	deg=8	nl=206	ai=4	ci=0
deg=7	nl=232	ai=4	ci=0		not balanced			deg=8	nl=218	ai=4	ci=0
deg=7	nl=204	ai=4	ci=0	deg=7	nl=232	ai=5	ci=0	deg=7	nl=204	ai=5	ci=0
deg=8	nl=218	ai=4	ci=0	deg=8	nl=222	ai=5	ci=0	deg=6	nl=188	ai=5	ci=0
deg=8	nl=224	ai=4	ci=0	deg=7	nl=228	ai=4	ci=0				
	not balanced			deg=8	nl=186	ai=5	ci=0	deg=8	nl=232	ai=5	ci=0
deg=8	nl=198	ai=4	ci=0	deg=7	nl=204	ai=4	ci=0	deg=7	nl=188	ai=4	ci=0
	not balanced			deg=8	nl=228	ai=4	ci=0	deg=7	nl=228	ai=4	ci=0
deg=7	nl=224	ai=5	ci=0		not balanced			deg=7	nl=188	ai=4	ci=0
deg=7	nl=228	ai=4	ci=0	deg=8	nl=218	ai=5	ci=0	deg=8	nl=218	ai=4	ci=0
deg=8	nl=186	ai=5	ci=0	deg=8	nl=206	ai=4	ci=0	deg=8	nl=206	ai=4	ci=0
								deg=7	nl=216	ai=4	ci=0

Εικόνα 4.26: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=9

Από τις συναρτήσεις που μελετήθηκαν βρέθηκαν 13 με μέγιστη αλγεβρική ανθεκτικότητα.



Εικόνα 4.27: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=9).

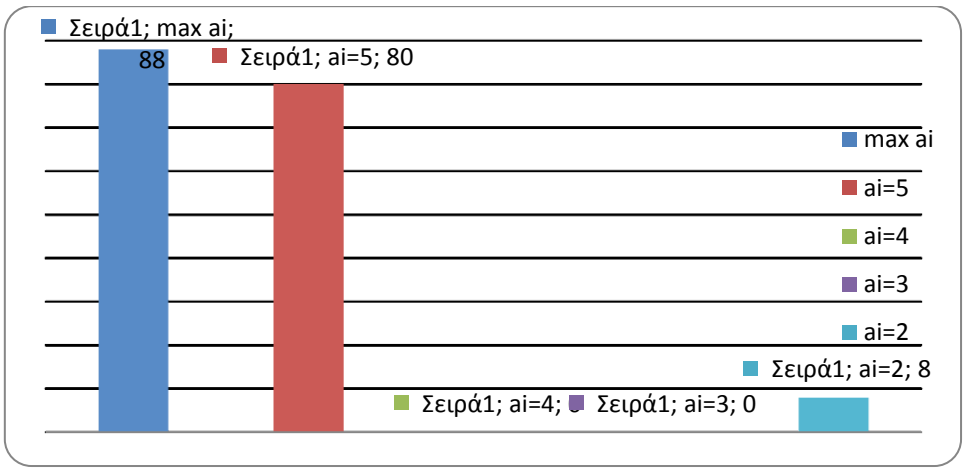
Τα αποτελέσματα που βρέθηκαν για τις fast algebraic attacks βρίσκονται στο παρακάτω πίνακα. Επειδή οι πίνακες αλήθειας των συναρτήσεων είναι μεγάλοι δεν συμπεριλαμβάνονται στον πίνακα αλλά υπάρχουν στο παράρτημα.

Παρατηρούμε ότι σε όλες τις συναρτήσεις υπάρχουν e,d τέτοια ώστε e+d=n-1, εκτός από μία που ισχύει e+d=n-2.

Συναρτήσεις κατασκευασμένες από cosets για n=9 με max algebraic immunity	e	d	# συναρτήσεων g
1	1	7	2
	1	6	0
	2	6	2
	2	5	0
	3	5	4
	3	4	0
2	1	7	2
	1	6	0
	2	6	2
	2	5	0
	3	5	4
	3	4	0
3	1	7	0
	2	6	4
	2	5	0
	3	5	0
	3	4	0
4	1	7	2
	1	6	0
	2	6	0
	3	5	6
	3	4	0
5	1	7	2
	1	6	0
	2	6	4
	2	5	0
	3	5	4
	3	4	0
6	1	7	2
	1	6	0
	2	6	4
	2	5	0
	3	5	2
	3	4	0
7	1	7	4
	1	6	0
	2	6	0
	3	5	0
8	1	7	0
	2	6	2
	2	5	0
	3	5	2
	3	4	0
9	1	7	0
	2	6	4
	2	5	0
	3	5	0
10	1	7	2
	1	6	0
	2	6	0
	3	5	6
	3	4	0
11	1	7	4
	1	6	0
	2	6	2
	2	5	0
	3	5	4
	3	4	0
12	1	7	10
	1	6	1
	1	5	0
	2	6	4
	2	5	0
	3	5	4
	3	4	0
13	1	7	2
	1	6	0
	2	6	2
	2	5	0
	3	5	2
	3	4	0

Πίνακας 4.12: Ανθεκτικότητα συναρτήσεων (n=9) σε fast algebraic attacks

Για $GF(2^{11})$ μελετήθηκαν 176 συναρτήσεις εκ των οποίων οι 88 είχαν μέγιστο algebraic immunity. Στην εικόνα 4.29 φαίνονται τα αποτελέσματα. Στην πρώτη στήλη (prim poly) η δυαδική αναπαράσταση των αριθμών, υποδηλώνει τους συντελεστές του πρωταρχικού πολυωνύμου. Για παράδειγμα το $(2053)_{10} = (100000000101)_2$ υποδηλώνει το πρωταρχικό πολυώνυμο $D^{11}+D^2+1$.



Εικόνα 4.28: Γραφική απεικόνιση των συναρτήσεων σε σχέση με την αλγεβρική τους ανθεκτικότητα (cosets με n=1).

prim poly						prim poly				
	deg=9	nl=972	ai=5	ci=0		3053	deg=10	nl=946	ai=5	ci=0
2053	deg=10	nl=946	ai=6	ci=0		3083	deg=9	nl=904	ai=6	ci=0
2071	deg=10	nl=946	ai=6	ci=0		3085	deg=10	nl=902	ai=6	ci=0
2091	deg=10	nl=934	ai=6	ci=0		3097	deg=10	nl=946	ai=6	ci=0
2093	deg=7	nl=90	ai=2	ci=0		3103	deg=9	nl=960	ai=5	ci=0
2119	deg=10	nl=956	ai=6	ci=0		3159	deg=9	nl=964	ai=5	ci=0
2147	deg=9	nl=904	ai=6	ci=0		3169	deg=10	nl=882	ai=5	ci=0
2149	deg=9	nl=972	ai=5	ci=0		3179	deg=10	nl=966	ai=6	ci=0
2161	deg=9	nl=904	ai=6	ci=0		3187	deg=9	nl=968	ai=5	ci=0
2171	deg=10	nl=902	ai=5	ci=0		3205	deg=9	nl=904	ai=5	ci=0
2189	deg=10	nl=946	ai=6	ci=0		3209	deg=9	nl=948	ai=5	ci=0
2197	deg=9	nl=960	ai=5	ci=0		3223	deg=10	nl=952	ai=5	ci=0
2207	deg=10	nl=946	ai=6	ci=0		3227	deg=9	nl=968	ai=6	ci=0
2217	deg=9	nl=924	ai=6	ci=0		3229	deg=9	nl=964	ai=6	ci=0
2225	deg=8	nl=24	ai=2	ci=0		3251	deg=10	nl=902	ai=6	ci=0
2255	deg=10	nl=962	ai=5	ci=0		3263	deg=10	nl=902	ai=6	ci=0
2257	deg=9	nl=904	ai=5	ci=0		3271	deg=10	nl=966	ai=5	ci=0
2273	deg=10	nl=962	ai=6	ci=0		3277	deg=10	nl=960	ai=5	ci=0
2279	deg=10	nl=902	ai=6	ci=0		3283	deg=10	nl=946	ai=6	ci=0
2283	deg=9	nl=968	ai=6	ci=0		3285	deg=10	nl=926	ai=6	ci=0
2293	deg=10	nl=926	ai=6	ci=0		3299	deg=9	nl=968	ai=6	ci=0
2317	deg=10	nl=962	ai=6	ci=0		3305	deg=10	nl=926	ai=5	ci=0
2323	deg=7	nl=90	ai=2	ci=0		3319	deg=10	nl=966	ai=6	ci=0
2341	deg=10	nl=952	ai=5	ci=0		3331	deg=10	nl=946	ai=5	ci=0
2345	deg=9	nl=924	ai=5	ci=0		3343	deg=10	nl=964	ai=6	ci=0
2363	deg=9	nl=924	ai=6	ci=0		3357	deg=10	nl=926	ai=6	ci=0
2365	deg=10	nl=966	ai=6	ci=0		3367	deg=9	nl=924	ai=5	ci=0
2373	deg=10	nl=882	ai=5	ci=0		3373	deg=10	nl=946	ai=6	ci=0
2377	deg=9	nl=924	ai=5	ci=0		3393	deg=9	nl=924	ai=6	ci=0
2385	deg=9	nl=948	ai=5	ci=0		3399	deg=9	nl=948	ai=5	ci=0
2395	deg=9	nl=924	ai=6	ci=0		3413	deg=10	nl=946	ai=5	ci=0
2419	deg=10	nl=968	ai=5	ci=0		3417	deg=12	nl=948	ai=5	ci=2
2421	deg=9	nl=964	ai=6	ci=0		3427	deg=7	nl=90	ai=2	ci=0
2431	deg=10	nl=946	ai=6	ci=0		3439	deg=9	nl=924	ai=6	ci=0
2435	deg=9	nl=948	ai=5	ci=0		3441	deg=9	nl=948	ai=6	ci=0
2447	deg=9	nl=904	ai=6	ci=0		3475	deg=9	nl=924	ai=5	ci=0
2475	deg=10	nl=928	ai=5	ci=0		3487	deg=10	nl=946	ai=5	ci=0
2477	deg=9	nl=964	ai=6	ci=0		3497	deg=10	nl=946	ai=5	ci=0
2489	deg=10	nl=960	ai=5	ci=0		3515	deg=10	nl=902	ai=6	ci=0
2503	deg=9	nl=904	ai=6	ci=0		3517	deg=9	nl=960	ai=5	ci=0
2521	deg=9	nl=968	ai=6	ci=0		3529	deg=9	nl=948	ai=6	ci=0
2533	deg=9	nl=960	ai=6	ci=0		3543	deg=9	nl=964	ai=6	ci=0
2551	deg=9	nl=904	ai=5	ci=0		3547	deg=9	nl=964	ai=6	ci=0
2561	deg=10	nl=956	ai=6	ci=0		3553	deg=10	nl=882	ai=6	ci=0
2567	deg=9	nl=960	ai=5	ci=0		3559	deg=9	nl=968	ai=6	ci=0
2579	deg=10	nl=964	ai=6	ci=0		3573	deg=9	nl=948	ai=6	ci=0
2581	deg=8	nl=24	ai=2	ci=0		3589	deg=9	nl=948	ai=6	ci=0
2601	deg=9	nl=948	ai=5	ci=0		3613	deg=10	nl=926	ai=6	ci=0
2633	deg=10	nl=942	ai=5	ci=0		3617	deg=9	nl=964	ai=5	ci=0
2657	deg=10	nl=952	ai=5	ci=0		3623	deg=10	nl=882	ai=5	ci=0
2669	deg=9	nl=964	ai=5	ci=0		3627	deg=9	nl=960	ai=5	ci=0
2681	deg=9	nl=964	ai=6	ci=0		3635	deg=10	nl=960	ai=5	ci=0
2687	deg=10	nl=946	ai=6	ci=0		3641	deg=10	nl=968	ai=6	ci=0
2693	deg=10	nl=902	ai=5	ci=0		3655	deg=10	nl=920	ai=5	ci=0
2705	deg=10	nl=942	ai=5	ci=0		3659	deg=9	nl=904	ai=6	ci=0
2717	deg=8	nl=928	ai=6	ci=0		3669	deg=9	nl=948	ai=5	ci=0
2727	deg=9	nl=924	ai=6	ci=0		3679	deg=9	nl=972	ai=5	ci=0
2731	deg=9	nl=972	ai=5	ci=0		3697	deg=9	nl=960	ai=6	ci=0
2739	deg=9	nl=948	ai=5	ci=0		3707	deg=10	nl=970	ai=6	ci=0
2741	deg=9	nl=948	ai=5	ci=0		3709	deg=9	nl=904	ai=5	ci=0
2773	deg=10	nl=858	ai=5	ci=0		3713	deg=10	nl=946	ai=5	ci=0
2783	deg=7	nl=90	ai=2	ci=0		3731	deg=9	nl=860	ai=5	ci=0
2793	deg=10	nl=946	ai=6	ci=0		3743	deg=10	nl=946	ai=6	ci=0
2799	deg=10	nl=954	ai=6	ci=0		3747	deg=10	nl=946	ai=6	ci=0
2801	deg=9	nl=880	ai=6	ci=0		3771	deg=9	nl=904	ai=5	ci=0
2811	deg=9	nl=904	ai=5	ci=0		3791	deg=10	nl=882	ai=6	ci=0
2819	deg=9	nl=948	ai=5	ci=0		3805	deg=9	nl=880	ai=5	ci=0
2825	deg=9	nl=964	ai=5	ci=0		3827	deg=8	nl=24	ai=2	ci=0
2833	deg=10	nl=952	ai=5	ci=0		3833	deg=9	nl=960	ai=5	ci=0
2867	deg=9	nl=964	ai=6	ci=0		3851	deg=10	nl=960	ai=6	ci=0
2879	deg=10	nl=962	ai=5	ci=0		3865	deg=10	nl=964	ai=6	ci=0
2881	deg=9	nl=952	ai=6	ci=0		3889	deg=10	nl=966	ai=5	ci=0
2891	deg=10	nl=960	ai=5	ci=0		3895	deg=9	nl=924	ai=6	ci=0
2905	deg=10	nl=926	ai=6	ci=0		3933	deg=7	nl=90	ai=2	ci=0
2911	deg=9	nl=948	ai=6	ci=0		3947	deg=9	nl=952	ai=5	ci=0
2917	deg=10	nl=902	ai=6	ci=0		3949	deg=9	nl=956	ai=6	ci=0
2927	deg=9	nl=944	ai=5	ci=0		3957	deg=9	nl=956	ai=6	ci=0
2941	deg=10	nl=902	ai=6	ci=0		3971	deg=9	nl=924	ai=6	ci=0
2951	deg=10	nl=962	ai=6	ci=0		3985	deg=9	nl=880	ai=6	ci=0
2955	deg=10	nl=926	ai=6	ci=0		3991	deg=9	nl=960	ai=6	ci=0
2963	deg=10	nl=966	ai=5	ci=0		3995	deg=10	nl=964	ai=5	ci=0
2965	deg=9	nl=960	ai=6	ci=0		4007	deg=10	nl=926	ai=6	ci=0
2991	deg=9	nl=968	ai=6	ci=0		4013	deg=9	nl=964	ai=5	ci=0
2999	deg=9	nl=964	ai=5	ci=0		4021	deg=9	nl=880	ai=5	ci=0
3005	deg=10	nl=958	ai=5	ci=0		4045	deg=10	nl=958	ai=5	ci=0
3017	deg=8	nl=28	ai=6	ci=0		4051	deg=10	nl=902	ai=5	ci=0
3035	deg=9	nl=948	ai=5	ci=0		4069	deg=10	nl=902	ai=6	ci=0
3037	deg=10	nl=946	ai=5	ci=0		4073	deg=9	nl=968	ai=5	ci=0
3047	deg=9	nl=95,24	ai=5	ci=0						

Εικόνα 4.29: Κρυπτογραφικές ιδιότητες συναρτήσεων για n=11

Έγινε δειγματοληπτικός έλεγχος αυτών που είχαν μέγιστη αλγεβρική ανθεκτικότητα για γρήγορες αλγεβρικές επιθέσεις. Παρατηρούμε πάλι, ότι είναι πολύ ανθεκτικές και αρκετές από αυτές έχουν τη μέγιστη ανθεκτικότητα.

Συναρτήσεις κατασκευασμένες από cosets για n=11 με max algebraic immunity	e	d	# συναρτήσεων g
2053	1	9	0
	2	8	3
	2	7	0
2071	1	9	0
	2	8	3
	2	7	0
2091	1	9	0
	2	8	1
	2	7	0
2119	1	9	0
	2	8	1
	2	7	0
2147	1	9	1
	1	8	0
	2	8	1
	2	7	0
2273	1	9	0
	2	8	1
	2	7	0
2293	1	9	0
	2	8	1
	2	7	0
2521	1	9	2
	1	8	0
	2	8	1
	2	7	0
2801	1	9	2
	1	8	0
	2	8	3
	2	7	0
3343	1	9	0
	2	8	1
	2	7	0
3559	1	9	2
	1	8	0
	2	8	3
	2	7	0
3971	1	9	2
	1	8	0
	2	8	1
	2	7	0

Πίνακας 4.13: Ανθεκτικότητα συναρτήσεων (n=9) σε fast algebraic attacks

4.5 Σύγκριση των συναρτήσεων που μελετήθηκαν

Στην ενότητα αυτή θα κάνουμε μια σύγκριση των αποτελεσμάτων που βρήκαμε στο κεφάλαιο 4. Στον πίνακα 4.14 παρουσιάζονται οι βασικές κρυπτογραφικές ιδιότητες των συναρτήσεων που μελετήθηκαν. Από τις συναρτήσεις των cosets αναγράφεται η βέλτιστη τιμή.

	n=4		n=5		n=6		n=7		n=8		n=9		n=11	
Κρυπτογραφική ιδιότητα	C-F	Cosets	C-F	Cosets	C-F	Cosets	C-F	Cosets	C-F	Cosets	C-F	Cosets	C-F	Cosets
degree	3	3	4	4	5	5	6	6	7	7	8	8	10	10
nonlinearity	4	4	10	12	22	24	54	52	112	110	232	232	980	968
algebraic immunity	2	2	3	3	3	3	4	4	4	4	5	5	6	6
correlation immunity	0	0	0	1	0	3	0	1	0	0	0	0	0	0

Πίνακας 4.14: Σύγκριση κρυπτογραφικών ιδιοτήτων συναρτήσεων Carlet-Feng (C-F) με τις συναρτήσεις που κατασκευάσαμε από cosets.

			Συναρτήσεις Carlet-Feng	Συναρτήσεις από cosets
	e	d	# συναρτήσεων g	# συναρτήσεων g
n=4	1	2	1	1
	1	1	0	0
n=5	1	3	0	0
	2	2	0	0
n=6	1	4	1	1
	1	3	0	0
	2	3	0	4
	2	2	0	0
n=7	1	5	0	0
	2	4	1	1
	2	3	0	0
	3	3	0	0
n=8	1	6	1	1
	1	5	0	0
	2	5	1	5
	2	4	0	0
n=9	1	7	0	0
	2	6	0	2
	3	5	0	2
	4	4	0	0
n=11	1	9	0	0
	2	8	1	1
	2	7	0	0
	3	7	0	0

Πίνακας 4.15: Σύγκριση ανθεκτικότητας σε γρήγορες αλγεβρικές επιθέσεις συναρτήσεων Carlet-Feng (C-F) με τις συναρτήσεις που κατασκευάσαμε από cosets.

Παρατηρούμε n=5, n=6 οι συναρτήσεις κατασκευασμένες από cosets έχουν καλύτερη μη γραμμικότητα και καλύτερη ανθεκτικότητα σε συσχετίσεις. Για n=7,8,11 έχουν καλύτερη μη γραμμικότητα οι συναρτήσεις Carlet-Feng.

Στις γρήγορες αλγεβρικές επιθέσεις παρουσιάζουν όλες καλά χαρακτηριστικά, με τις συναρτήσεις Carlet-Feng να είναι λίγο πιο ανθεκτικές (Πίνακας 4.15).

Σε κάθε περίπτωση πάντως, επισημαίνεται ότι με την προτεινόμενη κατασκευή μπορούμε να επιτύχουμε και ανθεκτικότητα έναντι επιθέσεων συσχέτισης, κάτι στο οποίο φαίνεται ότι αποτυγχάνει να το επιτύχει η συνάρτηση Carlet-Feng.

Κεφάλαιο 5
Επίλογος

Η παρούσα διπλωματική διατριβή πραγματεύθηκε θέματα ασφάλειας των συμμετρικών κρυπταλγορίθμων ροής. Ειδικότερα, έγινε αναλυτική περιγραφή της βασικής δομής αλγορίθμων ροής (κυρίως των σύγχρονων προσθετικών αλγορίθμων ροής), προκειμένου να αναδειχθεί η σημασία των γεννητριών κλειδοροής για την ασφάλειά τους. Μελετήθηκαν τα επιθυμητά χαρακτηριστικά που πρέπει να έχει μια ακολουθία για να είναι κατάλληλη για κλειδοροή και διαπιστώθηκε πως η χρήση των γραμμικών καταχωρητών ολίσθησης με ανάδραση (LFSR), οι οποίοι γενικά εμφανίζουν πλεονεκτήματα ως προς την υλοποίηση, δεν επαρκούν από μόνοι τους προκειμένου να προσδώσουν ασφάλεια στον αλγόριθμο. Ακριβώς για αυτό το λόγο συνδυάζονται με πιο σύνθετες δομές (όπως είναι η εφαρμογή μη γραμμικού φίλτρου στις καταστάσεις ενός LFSR).

Η ασφάλεια των αλγορίθμων ροής βασίζεται σε μεγάλο βαθμό στις ιδιότητες των συναρτήσεων που χρησιμοποιούνται για την κατασκευή γεννητριών κλειδοροής. Στην παρούσα διπλωματική διατριβή περιγράφηκαν οι κύριες επιθέσεις σε κρυπταλγορίθμους ροής, καθώς και οι αντίστοιχες κρυπτογραφικές ιδιότητες που πρέπει να έχουν οι κρυπτογραφικές συναρτήσεις προκειμένου τα συστήματα να είναι ανθεκτικά στις επιθέσεις αυτές. Εστιάσαμε κυρίως στις λεγόμενες αλγεβρικές και στις γρήγορες αλγεβρικές επιθέσεις, λόγω του εξαιρετικού ερευνητικού ενδιαφέροντος που παρουσιάζουν τα τελευταία χρόνια.

Με τη χρήση κατάλληλου λογισμικού μελετήθηκαν ως προς τις κρυπτογραφικές τους ιδιότητες δύο κατηγορίες συναρτήσεων. Οι συναρτήσεις που προτάθηκαν από τους Carlet-Feng [03], προκειμένου να παρέχεται υψηλή ανθεκτικότητα έναντι των αλγεβρικών επιθέσεων, και μια νέα κατηγορία συναρτήσεων που δεν έχει μελετηθεί ως τώρα ως προς αυτήν την οπτική γωνία. Οι συναρτήσεις αυτές έχουν την ιδιότητα ότι μένουν σταθερές για τιμές εισόδου που αντιστοιχούν στην ίδια κυκλοτομική κλάση modulo 2^n-1 (όπου n το πλήθος των μεταβλητών). Από τα αποτελέσματα προέκυψε ότι μπορούν να κατασκευαστούν συναρτήσεις με μέγιστη αλγεβρική ανθεκτικότητα, πολύ καλή ανθεκτικότητα στις γρήγορες αλγεβρικές επιθέσεις, καθώς επίσης και

πολύ καλή μη γραμμικότητα όπως και οι συναρτήσεις Carlet-Feng (αν και φαίνεται ότι οι συναρτήσεις Carlet-Feng υπερτερούν ως προς τη μη γραμμικότητα για μεγάλες τιμές του n). Επιπλέον όμως, με την προτεινόμενη κατασκευή μπορούμε να επιτύχουμε και ανθεκτικότητα έναντι επιθέσεων συσχέτισης, κάτι στο οποίο φαίνεται ότι αποτυγχάνει να το επιτύχει η συνάρτηση Carlet-Feng.

Σε κάθε περίπτωση, η εύρεση συναρτήσεων που να ικανοποιούν όλα τα γνωστά κρυπτογραφικά κριτήρια παραμένει ένα σημαντικό ανοιχτό ερευνητικό πρόβλημα. Οι συναρτήσεις που μελετήσαμε φαίνεται ότι πράγματι χρήζουν περαιτέρω διερεύνησης και μαθηματικής θεμελίωσης (για παράδειγμα, είναι εξαιρετικά ενδιαφέρον να αποδειχθούν οι ειδικές ιδιότητες που πρέπει να έχει μία συνάρτηση αυτής της κατηγορίας για να εξασφαλίζεται η μέγιστη ανθεκτικότητα στις αλγεβρικές επιθέσεις). Σε κάθε περίπτωση, οι αλληλοσυσχετίσεις μεταξύ των διαφόρων κρυπτογραφικών κριτηρίων, όπου συχνά η βελτίωση του ενός οδηγεί στην επιδείνωση του άλλου, πρέπει να μελετηθούν περαιτέρω, γιατί η γνώση αυτή θα καθορίσει και τα «όρια» που υπάρχουν όσον αφορά τη σχεδίαση των κατά το δυνατόν βέλτιστων κρυπτογραφικών συναρτήσεων.

Βιβλιογραφία

[01] A. Biryukov, A. Shamir, D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC", Διαθέσιμο στο Δικτυακό τόπο: http://cryptome.org/a51-bsw.htm (τελευταία προσπέλαση 26/08/2014)

[02] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction", IEEE Trans. Inform. Theory, vol. 52, pp. 3105—3121, 2006.

[03] C. Carlet, "Constructing balanced functions with optimum algebraic immunity", Proc. IEEE Int. Symp. Inf. Theory (ISIT), pp. 451—455, 2007.

[04] C. Carlet, and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity",Asiacrypt 2008 (Lecture Notes in Computer Science, Springer), vol. 5350, pp. 425—440, 2008.

[05] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity", Des. Codes Cryptogr., vol. 52, pp. 303—338, 2009.

[06] N. Courtois, and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", Advances in Cryptology - Eurocrypt 2003, (Lecture Notes in Computer Science, Springer), vol. 2656, pp. 345—359, 2003.

[07] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback", Advances in Cryptology - Crypto 2003, (Lecture Notes in Computer Science, Springer), vol. 2729, pp. 176—194, 2003.

[08] N. Courtois, G. V. Bard and D. Wagner, "Algebraic and slide attacks on KeeLoq", FSE 2008 (Lecture Notes in Computer Science, Springer), vol. 5086, pp. 97—115, 2008.

[09] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity", Des. Codes Cryptogr., Springer, vol. 40, pp. 41—58, 2006.

[10] W. Diffie, M. E. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, vol IT-22,no. 6, pp.644-654, 1976

[11] C. Ding, G. Xiao and W. Shan, "The stability theory of stream ciphers", Lecture Notes in Computer Science, Springer, vol. 561, 1991.

[12] S. Fischer, "FAA Equation Finder", Διαθέσιμο στο Δικτυακό τόπο: http://simonfischer.ch/science/faa.html (τελευταία προσπέλαση 26/08/2014)

[13] S. W. Golomb, "Shift Register Synthesis", Holden-Day, San Francisco, 1969

[14] N. Kalouptsidis, Signal processing systems. Series in Telecommunications and Signal Processing. New York: Wiley, 1996

[15] N. Li,and W. Qi, "Construction and analysis of Boolean functions of 2t + 1 variables with maximum algebraic immunity", Advances in Cryptology - Asiacrypt 2006 (Lecture Notes in Computer Science, Springer), vol. 4284}, pp. 84—98, 2006.

[16] R. Lidl and H. Niederreiter, Finite fields. Encyclopedia of Mathematics and Its Applications, vol.20. Cambridge, U.K.: Cambridge University Press, 1996, 2nd ed.

[17] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, "Constructing Boolean functions in odd number of variables with maximum algebraic immunity", IEEE Int. Symp. Inf. Theory (ISIT), pp. 2686—2690, 2011.

[18] K. Limniotis, N. Kolokotronis,, and N. Kalouptsidis, "Secondary constructions of Boolean functions with maximum algebraic immunity", Cryptogr. Comm., Springer, vol. 5, pp. 179–199, 2013.

[19] K. Limniotis, "Algebraic attacks on stream ciphers: Recent developments and new results", Journal of Applied Mathematics and Bioinformatics (Special Issue: Cryptography and its Applications in the Armed Forces), Scienpress Ltd., vol. 3, pp. 57—81, 2013.

[20] M. Lobanov, "Tight bound between nonlinearity and algebraic immunity", Cryptology ePrint Archive, Report 2005/441 (2005), http://eprint.iacr.org.

[21] J. L. Massey, "Shift Register Sequences and BCH Decoding", IEEE Trans. on Information Theory, vol. IT-15, pp. 122-127, Jan. 1969

[22] "MATLAB" ,http://www.mathworks.com/products/matlab/ (τελευταία προσπέλαση 26/08/2014)

[23] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions", Advances in Cryptology - Eurocrypt 2004 (Lecture Notes in Computer Science, Springer), vol. 3027, pp. 474—491, 2004.

[24] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996

[25] E. Pasalic, "Almost fully optimized infinitive classes of Boolean functions resistant to (fast) algebraic cryptanalysis", ICISC 2008 (Lecture Notes in Computer Science, Springer), vol. 5461, pp. 399—414, 2008.

[26] V. S. Pless and W. C. Huffman, Handbook of coding theory, vol. I. Amsterdam, Netherlands: Elsevier Science, 1998

[27] V. S. Pless and W. C. Huffman, Handbook of coding theory, vol. II. Amsterdam, Netherlands: Elsevier Science, 1998.

[28] R. Rivest, A, Shamir, L. Adleman "A method for obtaining digital signatures and public key cryptosystems", Communcations of the ACM, February 1978.

[29] P. Rizomiliotis, "On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation", IEEE Trans. Inform. Theory, vol. 56, pp. 4014—4024, 2010.

[30] A. Rukhin et al, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Διαθέσιμο στο Δικτυακό τόπο: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (τελευταία προσπέλαση 26/08/2014)

[31] "The R Project for Statistical Computing", http://www.r-project.org/ (τελευταία προσπέλαση 26/08/2014)

[32] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, vol.28, n0.4, pp. 59-715, 1949O.

[33] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol.28, pp.656-715,1949.

[34] T. Siegenthaler, "Correlation immunity of nonlinear combining functions for cryptographic applications", IEEE Trans. Information Theory, vol. 30, pp. 776-780, 1984

[35] G. S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications", Journal American Institute of Electrical Engineers, vol.55, pp.109-115, 1926

[36] "RC4", Διαθέσιμο στο Δικτυακό τόπο: http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html (τελευταία προσπέλαση 26/08/2014)

[37] X. Zeng, C. Carlet, J. Shan, and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks", IEEE Trans. Inform. Theory, vol. 57, pp. 6310—6320, 2011.

[38] Β. Α. Κάτος - Γ.Χ. Στεφανίδης, "Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης", ΖΥΓΟΣ, 2003

Παράρτημα Α
Συναρτήσεις που μελετήθηκαν

Στο παράρτημα αναφέρονται συναρτήσεις και αποτελέσματα, τα οποία λόγω του όγκου τους κρίθηκε σκόπιμο να μην εισαχθούν στο κείμενο της Διπλωματικής Διατριβής.

Α.1 Συναρτήσεις

1	deg=5	nl=48	ai=4	ci=0	1111111011101101101111101101100001000111100110101100010001000011001110100111011110010001110110001000000111011010010000010100000100
3	deg=4	nl=48	ai=3	ci=1	1111010011101101011000011111110100111011111010000100010010011101010010010101010000001000000011011110011100011010001001110010011111001
5	deg=6	nl=42	ai=3	ci=0	1110011011100011010101111110110110111001111111110000010111111101110000000010000000010010101100100000110011000011011000000010110000001
7	deg=6	nl=52	ai=3	ci=0	1110011011100000101010101110100100011001110110100000000000010000111011101111111111101001101011011010000000111001101110110000001000111
9	deg=5	nl=48	ai=4	ci=0	1001001100011110011101100110011001101001101111101100101100010110110001100100011100111010000110011010111100100000111111010000000010001
11	deg=5	nl=44	ai=3	ci=0	1010111001000000010011100100100001000100100110100100010001000010000111111010111001111111001111101101011110110110111111010001000101011
13	deg=5	nl=48	ai=4	ci=1	1100101110110100011001110100001100110010100001011011111010111111110001001100100001001010110110100110011000111111110000000010110000001
15	deg=5	nl=52	ai=3	ci=0	1001100100011110101010101000101101110011000100101111111111101111000001011000010000101100101011010011101110011110100010001101000000001
19	deg=6	nl=54	ai=3	ci=0	1101000110111101011000001011001100011011010000001101100000000000110100110100010011100110001011111011011101011110100100010111011011000001
21	deg=5	nl=52	ai=4	ci=0	1011011001001100011101001111101001110101101101010001001011110011001011000100001011001010110100111011100111110100010001101000000001
23	deg=6	nl=50	ai=4	ci=0	1011010001001110011000101111001100110101111010010000010100000000101010011011101101010010010110011001110000000011111111010011111100
27	deg=5	nl=52	ai=3	ci=0	1010111001000010100111101001100111001001011111001001111111111001001001011101100011001110100000100100001010000101101110100010001110
29	deg=6	nl=42	ai=3	ci=0	1101000110111111101100011010110111101101101100101101110111011111010100000001010001100000001100000100101000010010010000001011101101101100
31	deg=6	nl=48	ai=3	ci=0	1000101100010010100111100000001011000100001011110111011011010110001010010110101010101111110111111100100001100011100101110110001101101100001110
43	deg=6	nl=52	ai=3	ci=0	1100100110110011100010110000001011000101001001010111011010000011000101010011101111010011010100101100010001100001011101110011010111111110
47	deg=5	nl=44	ai=3	ci=0	1001100100011100101010000001001001000110000000001111101000000001000011111011111111011010100110111100110011111001000111111110100111110 0
55	deg=6	nl=48	ai=3	ci=0	1110110011100001100010011001100011001011001000000100110100111010001100110111000110001011110011001010000011011111100000010111111101110
63	deg=6	nl=48	ai=3	ci=0	1000000010001001001000010010011110111000011001010011101110111001000010110001000011011100010011101111000100101101111101010111111011

Πίνακας Α1.1: Συναρτήσεις από cosets για n=7

Συναρτήσεις κατασκευασμένες από cosets για n=7 με max algebraic immunity	No. Συνάρτησης
1000011001101000000110111100010101011111000110101100101011000111011100000101111001010111100110011010100110100011011101110010 0111011111100100011110010101011110000010000000101010000111011011100001001110000101111111100100000010000111010101011111001100 0100100100100100101011010011010100010011000010101001010111110110011101110101100001010011001010101010100101101111111001001001 00001010010000101110101010011001000101111101111010111110010000001011000101000000000111001100001101100111011101111011011111000 0110011011110010	1
1000011001101000000110111100010101011111000110101100101011000111011100000101111001010111100110011010100110100011011101110010 0111011111100100011110010101011110000010000000101010000111011011100001001110000101111111100100000010000111010101011111001100 0100100100100100101011010011010100010011000010101001010111110110011101110101100001010011001010101010100101101111111001001001 00001010010000101110101010011001000101111101111010111110010000001011000101000000000111001100001101100111011101111011011111000 0110011011110010	2
1001101111000001011010111000000011110101011010000010110110011000011011010010110010110110000100001100001101001111011011110100 00100110000111100110111001110000000011001111101001011111011100010011011011100101000100111010011110100011110110000001010001001 100010010110000011100111110001100110110001000000011010011000101011011111001010011101001001111010011110011001010100110010101000 10011101111111000000110011101000010000011111010100001110011101100000100111010111100000110101111100101001111100111010001001111111 0010101101100110	3
1010001010000001100101000010110110101010001000111001100001111001101101000000000011010111111111011011010001011001110010101101011 0011010010001011010110000110010011011100101111011100001001100101011000010011101110011010100011101101110110101001001010100010 10110100000001110101010100111111011000100111111110001101110010101010000000011000101010101110101010011010010001111001001111100 01110001001101110110111011000110110000000001001011110110101000111111111001100110101001000010110010001110001100100111000000111 1100110110001101	4
1010011001001010001111011000110001010101001000001110111011001111001110000011110000110100110001011110111111010001011010101100111 011001101000001010111000101010111100011101011001110010000111011101000000001001100001011001001110000100010110111001010111111110100 01001101011011001101100010010001110001011010101000000001110100111101001011000111010011111001000001010100101111001101100100001 10001000011110101111111000111001010111111111111100011110101100101010011011100000001001011001111010011001100000000010011001010111 0110000001101001	5
1110011010010111101111011101101100011111110001101000101101110110110001101000011001000011111011001011111011011000100110000011 01011100111111011011100011011111101101001011000100001000001101010010000001101111100011110100011101001010101101111100001100000 010111110010101000101000011010111100000011111110001100100100000011101111100110001011101001000000000010000110000011001001100010 0001111001110111011001100110001101110011010001101100111011010011111111000000100111111000000011001010100110001011001000001010000010 0011110111101001	6
10110011010001010110111101000100010111101010101101000001100111000111010100101001100000100001000001010011101000111100110011100 01110110111100101100110101010011010001111011110011111100111110101100110000100000111101111100000110100010100100110111100101101 1110001001000000010101001101000111110000100000000101010010000111110111111111010001110010101100111111011010101001010010111010100110 11110110111111000000111000111000010010111100110001011001010011000001000010011010011011011000111010100111100101110101101010010 1000101001001001	8
1001101111000001011010111000000011110101011010000010110110011000011011010010110010110110000100001100001101001111011011110100 00100110000111100110111001110000000011001111101001011111011100010011011011100101000100111010011110100011110110000001010001001 100010010110000011100111110001100110110001000000011010011000101011011111001010011101001001111010011110011001010100110010101000 10011101111111000000110011101000010000011111010100001110011101100000100111010111100000110101111100101001111100111010001001111111 0010101101100110	9
1010001010000001100101000010110110101010001000111001100001111001101101000000000011010111111111011011010001011001110010101101011 0011010010001011010110000110010011011100101111011100001001100101011000010011101110011010100011101101110110101001001010100010 10110100000001110101010100111111011000100111111110001101110010101010000000011000101010101110101010011010010001111001001111100 01110001001101110110111011000110110000000001001011110110101000111111111001100110101001000010110010001110001100100111000000111 1100110110001101	10
1111101100011000100010110001001110110100010011010110010001000011100110101001001101110101000110011101000100111101010001111010 000011110000001000000011111111000011011110111111001100111100000010110011100000111100011010111000011000010101010000000010111100 101100000000001000101001101010100101111110000010110010010111011010101101000001000110101111111011101111011100010110011010101101101 0110000111100001111001110111000100001111101000100000010110000001000111111101101001110100011010001011001011011000110011010111 1101011111011101	11
1111100101001010101001101110000110101010010000100101000111101010100101100001111000011100001011100001011000101110110011111111 1011100001110111011001111010000001000111111111101101111000110111011101110001001110110001001000010100110010100000001010111110 1010110100110011000100110110100011101001000111110010101101001101110110100000101011010011111100001010111101110001001010011000111 1000011110110100111101010110010101101000001001111011000110111110001101010001100101100101000110001100001100010110001000000001010 0010010100001101	12
11100100001111101001010001111111000010101001011111010010011001111100100101101001101001001111011110011110010110000100100001011 1101100111100001100100011000111111100110000010110100000100011101100100100011010111011000101100001011100001001111110101110110 0111011000011111000110000011100110010011101111111001011001110101001000011010110001011011000010110000110011010101011001101010111 0110001000000011111100110001011110111100000101011110001100010011110100010100001111100101000001101011000011000101110110000000 1101010010011001	13

Πίνακας A1.2: Οι συναρτήσεις με Max algebraic immunity για n=9