Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Κρυπτογραφία: Μη Γραμμική Πολυπλοκότητα Ακολουθιών

Φανή Τσιμπίνη

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Δεκέμβριος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Κρυπτογραφία: Μη Γραμμική Πολυπλοκότητα Ακολουθιών

Φανή Τσιμπίνη

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2018

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η ασφάλεια των συμμετρικών κρυπτογραφικών αλγορίθμων βασίζεται σε μεγάλο βαθμό στα χαρακτηριστικά τυχαιότητας συγκεκριμένων ακολουθιών. Υπάρχουν διάφορα μέτρα αποτίμησης της τυχαιότητας των ακολουθιών, με ένα εκ των πλέον χαρακτηριστικών τη γραμμική πολυπλοκότητα, η οποία εκφράζει το μέγεθος του μικρότερου γραμμικού καταχωρητή ολίσθησης με ανάδραση (LFSR) ο οποίος μπορεί να παράγει τη συγκεκριμένη ακολουθία.

Ένα ευρύτερο μέτρο από τη γραμμική πολυπλοκότητα είναι η μη γραμμική πολυπλοκότητα, η οποία εκφράζει το μέγεθος του μικρότερου μη γραμμικού καταχωρητή ολίσθησης με ανάδραση (NLFSR) ο οποίος μπορεί να παράγει τη συγκεκριμένη ακολουθία. Η μη γραμμική πολυπλοκότητα έχει μελετηθεί επίσης από την ερευνητική κοινότητα, αλλά σε σημαντικά μικρότερο βαθμό από τη γραμμική.

Η παρούσα διατριβή εστιάζει στη μελέτη της μη γραμμικής πολυπλοκότητας ακολουθιών. Στο πλαίσιο αυτό, μελετήθηκε η μη γραμμική πολυπλοκότητα των κλειδοροών που παράγονται από τον κρυπτογραφικό αλγόριθμο RC4, έναν από τους πλέον γνωστούς και διαδεδομένους κρυπτογραφικούς αλγορίθμους ροής επί δεκαετίες. Επίσης, μελετήθηκε η μη γραμμική πολυπλοκότητα k σφαλμάτων, μία έννοια η οποία δεν έχει ουσιαστικά μελετηθεί στη βιβλιογραφία (σε αντίθεση με την αντίστοιχη γραμμική πολυπλοκότητα k σφαλμάτων). Με την ανάπτυξη κατάλληλων αλγορίθμων υπολογίστηκε η μη γραμμική πολυπλοκότητα ακολουθιών του RC4, ενώ πραγματοποιήθηκε και μία εκτίμηση (άνω φράγματα) της μη γραμμικής πολυπλοκότητας k σφαλμάτων των εν λόγω ακολουθιών. Τα πειραματικά αποτελέσματα καταδεικνύουν ότι τόσο η μη γραμμική πολυπλοκότητα όσο και η γραμμική πολυπλοκότητα k σφαλμάτων μπορεί να είναι σημαντικά χαμηλότερες από την θεωρητικά αναμενόμενη τιμή των τυχαίων ακολουθιών – ενώ επίσης ακόμα και αν η μη γραμμική πολυπλοκότητα είναι υψηλή ενδέχεται η πολυπλοκότητα k σφαλμάτων για μικρές τιμές του k να είναι σημαντικά μικρότερη.

Summary

The security of symmetric cryptographic algorithms is strongly dependent on the randomness properties of specific cryptographic sequences. There are several cryptographic measures to assess the pseudorandomness of cryptographic sequences. One the most prominent is the so-called linear complexity, which determines the size of the shortest Linear Feedback Shift Register (LFSR) that is capable to generate the whole sequence.

A generalized notion of the linear complexity is the nonlinear complexity, which in turn determines the size of the shortest Nonlinear Feedback Shift Register (NLFSR) that is capable to generate the whole sequence. The nonlinear complexity, although it constitutes a current research trend, has been studied to a much smaller extent with respect to the linear complexity.

This Thesis studies the nonlinear complexity of cryptographic sequences. In this framework, the nonlinear complexity of the keystreams that are being generated by the well-known RC4 stream cipher is being studied; the RC4 has been for decades one the most commonly-used stream ciphers in several applications. Apart from the nonlinear complexity, we also study the k-error nonlinear complexity of RC4 sequences, which has not been studied yet in the literature (which is not the case for the respective criterion of the k-error linear complexity). More precisely, via developing appropriate algorithms, we computed the nonlinear complexity of several RC4 keystreams, whilst we also proceeded in estimating some upper bounds on the k-error nonlinear complexity of these sequences. Our experiments illustrate that in some cases the actual values of the nonlinear complexities are much smaller that their expected values, whilst even if the nonlinear complexity is high it is probable that the k-error nonlinear complexity, for small values of k, is much smaller.

Ευχαριστίες

Θα ήθελα να εκφράσω τις πιο θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου Κωνσταντίνο Λιμνιώτη για την απεριόριστη στήριξη του, την συνεχή καθοδήγηση του και την αδιάκοπη ενθάρρυνση του για την εκπόνηση αυτης τις μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Ορισμός κρυπτογραφίας

Η κρυπτογραφία μπορεί να περιγράφει ότι στηρίζεται στην επιστήμη των μαθηματικών προκειμένου να κωδικοποιήσει και να αποκωδικοποιήσει διάφορα δεδομένα. Με άλλα λόγια πρόκειται για ένα σύνολο μαθηματικών διεργασιών που έχουν ως σκοπό την διασφάλιση κάποιων θεμάτων που αφορούν στην ασφάλεια μεταφοράς πληροφοριών, όπως για παράδειγμα την πιστότητα ταυτότητας του αποστολέα, εμπιστευτικότητα, και το αδιάβλητο της πληροφορίας. Οι τεχνικές κρυπτογράφησης κάνουν τα προσωπικά δεδομένα που είναι ευαίσθητα ασφαλισμένα προκειμένου να έχουν πρόσβαση σε αυτά μόνο όσοι επιθυμείται κάθε φορά.
Κατ' αυτόν τον τρόπο εξασφαλίζεται η ιδιωτικότητα τόσο στις επικοινωνίες όσο και κατά την αποθήκευση δεδομένων. Το τμήμα της πληροφορίας πριν την κρυπτογράφηση καλείται απλό κείμενο (plaintext). Μετά την κρυπτογράφηση προκύπτει νέο κείμενο-μήνυμα το οποίο καλείται κρυπτογράφημα (ciphertext).
Η χρήση αντίστροφου αλγορίθμου προκειμένου να επιτευχθεί η ανάκτηση του απλού κειμένου μέσω του κρυπτογραφήματος, καλείται αποκρυπτογράφηση. Συχνά παρατηρείται σύγχυση μεταξύ των όρων κρυπτογράφηση και κρυπτανάλυση παρόλο που οι δύο όροι είναι διαφορετικοί. Η κρυπτανάλυση είναι ο κλάδος που ασχολείται με την αποκωδικοποίηση και ανάλυση πληροφοριών σε κωδικοποιημένη μορφή χωρίς να χρησιμοποιεί αυτό που αναφέρθηκε προηγουμένως ως αντίστροφος αλγόριθμος αποκρυπτογράφησης – ο οποίος πρέπει να μπορεί να εφαρμοστεί μόνο από εξουδιοτημένους παραλήπτες. Η κρυπτανάλυση ουσιαστικά αναφέρεται σε τεχνικές «καταστρατήγησης» της κρυπτογράφησης. Εικόνα(βλέπε παράγραφο 5.2)

Αναφορικά με τον αλγόριθμο κρυπτογράφησης, πρόκειται για μία συνάρτηση που χρησιμοποιείται προκειμένου να κρυπτογραφήσει και να αποκρυπτογραφήσει κάποια

πληροφορία. Καθώς ο αλγόριθμος γίνεται πιο σύνθετος μικραίνει η πιθανότητα να τον διαβάλλουν. Ο αλγόριθμος κρυπτογράφησης δουλεύει σε συνεργασία με το λεγόμενο κλειδί (key) ώστε να κρυπτογραφηθεί το απλό κείμενο που αναφέρθηκε προηγουμένως. Ένα απλό κείμενο είναι δυνατόν να κωδικοποιηθεί σε διάφορα κρυπτογραφήματα, ανάλογα με το κλειδί που θα χρησιμοποιηθεί.

1.1.1 Συμμετρική κρυπτογραφία

Η συμμετρική κρυπτογραφία στηρίζεται σε ένα μόνο κλειδί το οποίο καλείται συμμετρικό κλειδί ή μυστικό κλειδί. Με το κλειδί αυτό πραγματοποιείται κρυπτογράφηση και αποκρυπτογράφηση. Ο παραλήπτης και ο αποστολέας είναι οι μόνοι που ξέρουν και λειτουργούν το συμμετρικό κλειδί. Στην παρακάτω εικόνα-σχήμα παρουσιάζεται η συμμετρική κρυπτογραφία. Οι πληροφορίες που πρόκειται να κρυπτογραφηθούν αποτελούν το αρχικό κείμενο (plaintext) και κρυπτογραφούνται με την βοήθεια μυστικού ή συμμετρικού κλειδιού. Η κρυπτογράφηση παράγει ως έξοδό της ένα κείμενο σε μη κατανοητή μορφή το οποίο καλείται κρυπτογράφημα (ciphertext). Η πληροφορία που μεταφέρεται εξασφαλίζει την ασφάλειά για τον λόγο ότι το κρυπτογράφημα μεταφέρεται σε μη κατανοητή μορφή. Η λειτουργία της επανάκτησης της πρώτης πληροφορίας με την χρήση του μυστικού κλειδιού καλείται αποκρυπτογράφηση. Εικόνα(βλέπε παράγραφο 5.2)

Η συμμετρική κρυπτογραφία έχει μια μακρά ιστορία πάρα πολλών ετών . Κλασσικό παράδειγμα κώδικά κρυπτογραφίας είναι ο αλγόριθμος που είχε φτιάξει ο Ιούλιος Καίσαρας και είναι κώδικάς αντικατάστασης απλής μορφής. Στην νεότερη εποχή υπάρχουν φημισμένοι κώδικες όπως είναι ο AES (το σημερινό πρότυπο κρυπτογράφησης), ο DES (το παλαιότερο πρότυπο κρυπτογράφησης) και ο RC4 (αλγόριθμος της κατηγορίας των κρυπταλγορίθμων ροής, στους οποίους εστιάζει η παρούσα διατριβή).

Βασικό προτέρημα της συμμετρικής κρυπτογραφίας είναι η μεγάλη ταχύτητα κατά την κρυπτογράφηση και αποκρυπτογράφηση που είναι ικανή να ξεπεράσει τα 95 Mbps. Ακόμη, βασικό προτέρημα είναι και οι λίγες ανάγκες σε υπολογιστική ισχύ και μνήμη.

Για τους παραπάνω λόγους είναι εφικτό να εφαρμοστεί σε περιπτώσεις κινητών τηλεφώνων ή smart card. Τα ανωτέρω ισχύουν ιδίως για μία κατηγορία συμμετρικών κρυπταλγορίθμων, τους κρυπταλγορίθμους ροής, που περιγράφονται στο Κεφάλαιο 2.

Ένας από τους κύριους λόγους που η συμμετριική κρυπτογραφία περιορίζεται είναι η απαίτηση της ανταλλαγής του κλειδιού από τον παραλήπτη προς τον αποστολέα. Το ότι ο παραλήπτης και ο αποστολέας έχουν από κοινού το συμμετρικό κλειδί προτού γίνει η αποστολή της πληροφορίας αποτελεί την μόνη δικλείδα ασφαλείας για την συμμετρική κρυπτογραφία. Για τον λόγο αυτό καθίσταται αναγκαία η επιτυχία μίας ζεύξης ασφαλείας για την μεταβίβαση του μυστικού κλειδιού. Η ασφαλής ανταλλαγή του μυστικού κλειδιού καθίσταται ακόμα πιο χρονοβόρα στη περίπτωση που ο αποστολέας με τον παραλήπτη δεν γνωρίζονται μεταξύ τους. Αν ισχύει κάτι τέτοιο προκύπτει η ανάγκη να πιστοποιηθεί η ταυτότητα του αποστολέα και του παραλήπτη προκειμένου να μην γίνει η μεταφορά του κλειδιού σε κάποιον τρίτο οποίος δεν έχει την ανάλογη εξουσιοδότηση.
Τις περισσότερες φορές στην μυστική κρυπτογραφία η μεταβίβαση του κλειδιού πραγματοποιείται διαμέσου μίας ζεύξης φυσικής (κατ ιδίαν ανταλλαγή του κλειδιού) ή διαμέσου κάποιου τρίτου ατόμου εγνωσμένης εμπιστοσύνης το οποίο αναλαμβάνει την μεταβίβαση του κλειδιού. Βασικός ανασταλτικός παράγοντας της παραπάνω διαδικασίας είναι επίσης και η δυσχέρεια που εμφανίζεται όταν αυξάνονται οι χρήστες. Όταν το σύνολο των χρηστών που επιθυμούν να έρθουν σε επικοινωνία αυξάνεται, μοιραία αυξάνεται και ο αριθμός των κλειδιών που θα απαιτούνται για την κάθε ξεχωριστή επικοινωνία. Προκειμένου να πραγματοποιηθεί επικοινωνία μεταξύ x χρηστών, χρειάζονται x2/2 μοναδικά μυστικά κλειδιά, συνυπολογιζομένων και των κλειδιών που κατέχει ο κάθε χρήστης για αυτόν.
Το ζήτημα του key management, δηλαδή του τρόπου με τον οποίο θα διαχειρίζονται τα κλειδιά μεγεθύνεται περαιτέρω διότι το κάθε κλειδί οφείλει να υποστεί αντικατάσταση από ένα νέο προκειμένου να επιτυγχάνεται μείωση στα δεδομένα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. (Schoenmakers, 1999)

1.1.2 Ασύμμετρη κρυπτογραφία

Το 1975 οι Martin Helman και Whitefild Diffie υπέδειξαν μία καινούρια μέθοδο προκειμένου να μικρύνουν τα ζητήματα της κρυπτογραφίας δημοσίου κλειδιού. Η μέθοδος αυτή καλείται ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού και στηρίζεται σε ένα ζευγάρι κλειδιών (key pair). Σε αυτό το ζευγάρι, παρόλο που αλληλεξαρτώνται από μαθηματική σχέση, τα επιμέρους κλειδιά διαφέρουν αρκετά, τόσο που αν ξέρει κάποιος το ένα από τα δύο να μην μπορεί να παράγει το άλλο. Από το παραπάνω προκύπτει ότι κάποιο εκ των δύο κλειδιών υπάρχει η δυνατότητα να είναι ευρέως γνωστό. Για τον παραπάνω λόγο το κλειδί αυτό καλείται δημόσιο και με αυτόν πραγματοποιείται η κρυπτογράφηση των δεδομένων. Ως εκ τούτου, το άλλο κλειδί πρέπει να παραμένει ιδιωτικό. Για τον παραπάνω λόγο καλείται ιδιωτικό κλειδί και με αυτό πραγματοποιείται η αποκρυπτογράφηση των δεδομένων. Τα κύρια γνωρίσματα του ιδιωτικού κλειδιού και του δημόσιου κλειδικού παρατίθενται παρακάτω:

- Και οι δύο κατηγορίες κλειδιών προκύπτουν την ίδια στιγμή από εξειδικευμένο πρόγραμμα λογισμικού.
- Το ιδιωτικό και το δημόσιο δεν ταυτίζονται μεταξύ τους. Παρ' όλα αυτά, αλληλεξαρτώνται αμφιμονοσήμαντα προκειμένου να μπορεί να πραγματοποιηθεί μέσω αυτών αποκρυπτογράφηση και κρυπτογράφηση δεδομένων. Η τεχνική που προκύπτουν τα δύο κλειδιά διασφαλίζει πως το καθένα εξαρτάται μοναδικώς σε σχέση με το άλλο και πως δεν υπάρχει άλλο κλειδί που να είναι ικανό να προκύψει από το άλλο.
- Και οι δύο κατηγορίες κλειδιών (ιδιωτικά και δημόσια) που δημιουργούν ένα ζεύγος συμπληρώνουν το ένα το άλλο. Ως εκ τούτου κρυπτογραφούνται πληροφορίες από το ένα κλειδί και είναι δυνατόν να αποκρυπτογραφηθούν μόνο από το άλλο και αντιστρόφως. Έτσι, κάποιο μήνυμα το οποίο είναι κρυπτογραφημένο με την χρήση δημόσιου κλειδιού είναι δυνατόν να αποκρυπτογραφηθεί αποκλειστικά με την χρήση του ιδιωτικού κλειδιού που αντιστοιχεί σε αυτό.
- Κάθε αποστολέας ή παραλήπτης που είναι σε κάποιο σύστημα επικοινωνίας ασύμμετρης κρυπτογραφίας κατέχει ένα ιδιωτικό και ένα δημόσιο κλειδί.

Αναφορικά με το ιδιωτικό κλειδί ισχύουν τα παρακάτω:

- Η προστασία του έγκειται στον ιδιοκτήτη του
- Η χρήση του γίνεται είτε για να αποκρυπτογραφηθούν μηνύματα που προορίζονται για τον ιδιοκτήτη του είτε για υπογραφούν ψηφιακά μηνύματα που ο

ιδιοκτήτης τους θα στείλει (προκειμένου ο παραλήπτης να μπορεί να αυθεντικοποιήσει την προέλευση αλλά και την ακεραιότητα των δεδομένων).

Αναφορικά με το δημόσιο κλειδί ισχύουν τα παρακάτω:

- Η διανομή του γίνεται απρόσκοπτα και μπορεί να έχει πρόσβαση ο καθένας σε αυτό
- Μπορεί να γίνει χρήση του για να πιστοποιηθούν ψηφιακές υπογραφές (χρησιμοποιείται το δημόσιο κλειδί του αποστολέα)
- Μπορεί να γίνει χρήση του για να κρυπτογραφηθούν μηνύματα (χρησιμοποιείται το δημόσιο κλειδί του παραλήπτη)
- Μπορεί να αποθηκευτεί σε ψηφιακά πιστοποιητικά τα οποία αποτελούν την απόδειξη για το ποιος είναι ο κάτοχος του κλειδιού.

Αν και τα κλειδιά που είναι δημόσια είναι δυνατόν να παρέχονται σε όλους χωρίς περιορισμούς, τα κλειδιά που είναι ιδιωτικά δεν προβλέπεται να γνωστοποιούνται πέραν του αποστολέα και του παραλήπτη, δηλαδή σε φορείς που δεν έχουν την αντίστοιχη εξουσιοδότηση. Στην εικόνα(Βλέπε παράγραφο 5.2) που παρατίθεται παρακάτω παρουσιάζεται ο τρόπος με τον οποίο γίνεται η ασύμμετρη κρυπτογράφηση. Ο μεν αποστολέας κάνει την κρυπτογράφηση της πληροφορίας που επιθυμεί να στείλει στον παραλήπτη χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη που παρέχεται όπως προείπαμε χωρίς περιορισμούς. Το μήνυμα που έχει κρυπτογραφηθεί καταλήγει στον παραλήπτη που είναι σε θέση να το αποκρυπτογραφήσει με την χρήση του ιδιωτικού του κλειδιού. (Cramer & Shoup,1998)

Η κρυπτογραφία ασύμμετρου κλειδιού επιλέγεται κατά την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών όπως επίσης και κατά την ψηφιακή υπογραφή δεδομένων. Η κρυπτογραφία ασύμμετρου κλειδιού έχει ασφάλεια η οποία προκύπτει από το ότι καθίσταται μη εφικτή η παραγωγή του ιδιωτικού κλειδιού με υπολογιστικό τρόπο μέσω του δημοσίου κλειδιού. Στην θεωρία, ωστόσο, το ιδιωτικό κλειδί έχει την δυνατότητα κάθε φορά να υπολογίζεται. Για να γίνει όμως αυτό απαιτείται τόσο μεγάλη υπολογιστική ισχύς και μνήμη καθώς και χρόνος και κόστος ώστε ουσιαστικά να μην είναι εφικτό στην πράξη.

Το κυριότερο προτέρημα της κρυπτογραφίας δημοσίου κλειδιού έγκειται στο ότι δεν χρειάζεται ανταλλαγή μυστικού κλειδιού. Το δημόσιο κλειδί υπάρχει ελεύθερο χωρίς περιορισμούς, το οποίο σημαίνει ότι η χρήση του είναι πολύ πιο απλή και ευχερής σε αντίθεση με το ιδιωτικό κλειδί που το γνωρίζει αποκλειστικά ο κάτοχος-ιδιοκτήτης του. Ως εκ τούτου, η παραποίησή του καθίσταται πιο δυσχερής. Ακόμη στην ασύμμετρη κρυπτογραφία είναι εφικτή η πραγματοποίηση κάποιας ιδιαίτερα βασικής λειτουργίας που σχετίζεται με την κρυπτογραφία: η ψηφιακή υπογραφή δεδομένων.

Η ασύμμετρη κρρυπτογραφία αξιώνει υψηλή υπολογιστική ισχύ η οποία είναι περίπου 90 φορές πιο μεγάλη σε σχέση με εκείνη που χρειάζεται στην συμμετρική κρυπτογραφία. Ακόμα, είναι ιδιαίτερα χρονοβόρα ιδίως στην περίπτωση των μεγάλων μηνυμάτων. Έτσι, τις περισσότερες φορές κρυπτογραφούνται συμμετρικά κλειδιά αντί δεδομένων χρησιμοποιώντας την διαδικασία ψηφιακού φακέλου που αναφέρεται παρακάτω.

1.1.3 Υβριδική κρυπτογραφια ψηφιακού φακέλου

Σημαντικό πλεονέκτημα στην εξασφάλιση επικοινωνίας με ασφάλεια ανάμεσα σε αποστολέα και παραλήπτη εμφανίζει η υβριδική κρυπτογραφία η οποία καλείται και ψηφιακός φάκελος (digital envelope). Η κρυπτογραφία αυτή χρησιμοποιεί τόσο μεθόδους της ασύμμετρης κρυπτογραφίας όσο και της συμμετρικής. Η κατασκευή ψηφιακού φακέλου πραγματοποιείται με τον παρακάτω τρόπο: Αρχικά φτιάχνεται ένα μυστικό κλειδί με την βοήθεια αλγόριθμου κρυπτογράφησης συμμετρικού κλειδιού (για παράδειγμα, AES). Τα δεδομένα της πληροφορίας κρυπτογραφούνται με το μυστικό κλειδί που φτιάχτηκε προηγουμένως. Έπειτα το μυστικό κλειδί κρυπτογραφείται από το δημόσιο κλειδί του παραλήπτη. Τέλος, τα κρυπτογραφημένα κείμενα που έχουν προκύψει συνιστούν έναν ψηφιακό φάκελο στην διάθεση του παραλήπτη.

Ο παραλήπτης έχει την δυνατότητα να κάνει χρήση του ψηφιακού φακέλου κατόπιν απόκρυπτογράφησης που κάνει με το ιδιωτικό κλειδί που κατέχει στο κρυπτογραφημένο μυστικό κλειδί. Με την βοήθεια του μυστικού κλειδιού αποκρυπτογραφούνται οι αρχικές πληροφορίες (Plaintext) από τον παραλήπτη. Αφού επιτελεστεί ασφαλής επικοινωνία ανάμεσα στις δύο οντότητες το μυστικό κλειδί πηγαίνει για καταστροφή.

Μέσω της υβριδικής κρυπτογραφίας είναι δυνατόν να αντιμετωπιστούν κάποια βασικά μειονεκτήματα της ασύμμετρης κρυπτογραφίας. Ειδικότερα η ασύμμετρη κρυπτογραφία εμφανίζει το μειονέκτημα ότι είναι χρονοβόρα σε σχέση με την κρυπτογραφία μυστικού κλειδιού, κυρίως όσον αφορά στην κρυπτογράφηση εκτεταμένων μηνυμάτων.
Αξίζει να αναφερθεί πως και όταν πρόκειται για κρυπτογράφηση σε μεγάλα μηνύματα τις περισσότερες φορές γίνεται χρήση ψηφιακού φακέλου. Έτσι αποτρέπεται κάθε παρανόηση σε σχέση με το αν το αποτέλεσμα που προκύπτει από την αποκρυπτογράφηση είναι μυστικό κλειδί ή δεδομένα.

1.1.4 Κύριες έννοιες – σημασία των ακολουθιών στην κρυπτογράφηση

Ο κύριος σκοπός στην κρυπτογράφηση εστιάζεται στο να επικοινωνήσουν δύο άτομα με ασφάλεια προκειμένου άλλα άτομα να μην έχουν την δυνατότητα να «μπουν ανάμεσα» στην επικοινωνία τους ή να καταλάβουν την ουσία και το νόημα της επικοινωνίας τους. Σχήμα(βλέπε παράγραφο 5.2)

- Κάθε σύστημα κρυπτογράφησης δηλαδή θεωρείται ένα ολοκληρωμένο σύνολο με κρυπτογράφηση και αποκρυπτογράφηση το οποίο συνίσταται από πέντε στοιχεία: D, E, k, C, P. D καλείται η αντίστροφη συνάρτηση (μετασχηματισμός) της αποκρυπτογράφησης.
- E καλείται ο μετασχηματισμός της κρυπτογράφησης ή συνάρτηση κρυπτογράφησης.
- K καλείται ο χώρος του συνόλου των πιθανών κλειδιών (κλειδοχώρος)
- C καλείται ο χώρος του συνόλου των δυνατών μηνυμάτων κρυπτογράφησης (κρυπτοκειμένων)
- P καλείται ο χώρος του συνόλου των μηνυμάτων (ανοικτών κειμένων)

Η E, δηλαδή η κρυπτογραφική συνάρτηση λαμβάνει δύο παραμέτρους από χώρους P και k και δίνει ακολουθία η οποία βρίσκεται στον C. Η αντίστροφη συνάρτηση D λαμβάνει 2 παραμέτρους, το C και το k, και δίνει ακολουθία που βρίσκεται στον P.
Το σύνηθες σύστημα κρυπτοσυστήματος περιγράφεται ως εξής:

- Ο αποστολέας διαλέγει κάποιο κλειδί με μήκος z από τον χώρο των κλειδιών με τυχαία επιλογή.
- Στη συνέχεια, ο αποστολέας στέλνει το κλειδί προς τον παραλήπτη διαμέσου κάποιου ασφαλούς καναλιού (π.χ. μέσω ασύμμετρης κρυπτογράφησης).
- Έπειτα, ο αποστολέας φτιάχνει μήνυμα μέσα από των χώρο που υπάρχουν μηνύματα.
- Η κρυπτογραφική συνάρτηση λαμβάνει τις δύο εισόδους, δηλαδή το μήνυμα και το κλειδί, παράγοντας μια κρυπτακολουθία με σύμβολα, που καλείται κρυπτογράφημα. Η ακολουθία που προκύπτει στέλνεται μέσα από κανάλι που δεν ελέγχεται για την ασφάλειά του.
- Η κρυπτογραφική συνάρτηση λαμβάνει σαν όρισμα το κρυπτογράφημα και το κλειδί και δίνει μία αντίστοιχη ακολουθία μηνύματος.

Το μη εξουσιοδοτημένο άτομο μπορεί να παρατηρεί την επικοινωνία που υπάρχει μεταξύ του παραλήπτη και του αποστολέα, μπορεί να λαμβάνει ενημέρωση σχετικά με την κρυπτακολουθία, όμως δεν γνωρίζει το κλειδί που έχει χρησιμοποιηθεί και δεν είναι έτσι εφικτό να ξαναφτιάξει το μήνυμα. Σε περίπτωση που το μη εξουσιοδοτημένο άτομο διαλέξει να κοιτάξει όλα τα μηνύματα θα λάβει χρήσιμες πληροφορίες σχετικά με το κλειδί. Σε περίπτωση λοιπόν που το μη εξουσιοδοτημένο άτομο επιθυμεί να λάβει γνώση μόνο για το συγκεκριμένο μήνυμα τότε μπορεί να κάνει μία εικασία σχετικά με την πληροφορία που περιέχεται μέσα στο μήνυμα.

1.1.5 Αντικείμενο της διατριβής

Προκειμένου οι κρυπτογραφικοί αλγόριθμοι να παρέχουν ασφάλεια, πρέπει να σχεδιάζονται κατά τρόπο τέτοιο ώστε να πληρούνται συγκεκριμένες ιδιότητες. Η παρούσα διατριβή εστιάζει στην ασφάλεια συμμετρικών κρυπτογραφικών αλγορίθμων και, ειδικότερα, στους κρυπταλγορίθμους ροής (stream ciphers). Η συγκεκριμένη κατηγορία αλγορίθμων, που περιγράφεται στο Κεφάλαιο 2, βασίζει την ασφάλειά της, σε μεγάλο βαθμό, στα χαρακτηριστικά τυχαιότητας μίας ακολουθίας που ονομάζεται κλειδοροή (keystream). Υπάρχουν διάφορα κρυπτογραφικά κριτήρια για την αποτίμηση της τυχαιότητας μιας ακολουθίας. Στη συγκεκριμένη διατριβή μελετάμε ειδικότερα τη λεγόμενη μη γραμμική πολυπλοκότητα (nonlinear complexity) λόγω του γεγονότος ότι δεν έχει μελετηθεί εκτενώς στη βιβλιογραφία, ενώ επίσης μελετάμε και

μία επέκταση αυτής, τη λεγόμενη μη γραμμική πολυπλοκότητα k σφαλμάτων. Το ερευνητικό ερώτημα που τέθηκε συνεπώς έχει να κάνει με τη συμπεριφορά γνωστών κρυπτογραφικών ακολουθιών σε σχέση με τα ανωτέρω κρυπτογραφικά κριτήρια.

Στο πλαίσιο αυτό, η παρούσα διατριβή μελέτησε την κλειδοροή που παράγει ένας γνωστός κρυπταλγόριθμος ροής, ο RC4, ως προς τα ανωτέρω κρυπτογραφικά κριτήρια. Ο RC4 αποτέλεσε για δεκαετίες τον βασικό κρυπτογραφικό αλγόριθμο σε πλήθος εφαρμογών (π.χ. στα ασύρματα δίκτυα ή στο πρωτόκολλο TLS για την ασφάλεια στο Διαδίκτυο). Μέσω ανάπτυξης κατάλληλων αλγορίθμων προκειμένου να μελετηθούν οι κλειδοροές που παράγονται από τον RC4, διαπιστώνεται ότι είναι πιθανό να παράγονται κλειδοροές οι οποίες να μην έχουν καλή συμπεριφορά ως προς τα συγκεκριμένα κριτήρια. Ως εκ τούτου, από την παρούσα διατριβή προκύπτει το συμπέρασμα ότι και η μη γραμμική πολυπλοκότητα (τόσο στην κλασική της μορφή όσο και των k σφαλμάτων) πρέπει να μελετώνται για την αποτίμηση της τυχαιότητας μιας κλειδοροής, το οποίο με τη σειρά του συνεπάγεται την ανάγκη εύρεσης κατά το δυνατόν αποδοτικών μεθόδων για τη μελέτη τους.

Κεφάλαιο 2
Κρυπταλγόριθμοι ροής

2.1 Λειτουργία των κρυπταλγορίθμων ροής

Οι κρυπταλγόριθμοι ροής (stream ciphers) βρίσκουν εφαρμογή στην κρυπτογράφηση μιας διαδοχικής ροής δεδομένων (data stream). Η διαδικασία αυτή προϋποθέτει αρχικά μια γεννήτρια κλειδοροής (keystream generator), η οποία χρησιμοποιείται ως «θύρα» για την είσοδο του μυστικού κλειδιού και είναι αυτή η οποία παράγει στην έξοδό της μια ψευδοτυχαία αλληλουχία bits, η οποία καλείται κλειδοροή (keystream). Έπειτα, έρχεται η στιγμή εφαρμογής της συνάρτησης XOR ανάμεσα στην κλειδοροη και στο αρχικό κείμενο με αποτέλεσμα να παράγεται μια κρυπτογραφημένη ροη δεδομένων.

Στη συνεχεία ακολουθεί μια εικόνα(βλέπε παράγραφο 5.2) που αναπαριστά τη διαδικασία που περιγράφηκε:

Η αποκρυπτογράφηση του κείμενου γίνεται ακλουθώντας ακριβώς την αντίστροφη διαδικασία. Στην περίπτωση που το ίδιο το κλειδί χρησιμοποιηθεί ως είσοδο στην γεννήτρια κλειδοροης, τότε η τελευταία θα συνθέσει ακριβώς την ίδια αλληλουχία bits (κλειδοροη) όπως αναφέρθηκε και προηγουμένως κατά τη διαδικασία της κρυπτογράφησης. Έτσι, όταν ανάμεσα στην κλειδοροή και στην κρυπτογραφημένη ακολουθία των δεδομένων εφαρμοστεί η συνάρτηση XOR τότε θα παραχθεί τελικά το αρχικό κείμενο.

Η κρυπτογράφηση με κρυπταλγόριθμο ροής αποτελεί έναν τύπο αλγόριθμου συμμετρικής κρυπτογράφησης. Το κύριο χαρακτηριστικό τους είναι ότι είναι ιδιαίτερα γρήγοροι αλγόριθμοι σε αντίθεση με την άλλη κατηγορία συμμετρικών αλγορίθμων, τους κρυπταλγόριθμους τμήματος (block ciphers) και επίσης χαρακτηρίζονται από

λιγότερη πολυπλοκότητα ως προς την κυκλωματική υλοποίηση. Όσον αφορά το λειτουργικό κομμάτι, οι stream ciphers λειτουργούν με bits, δηλαδή με μικρές μονάδες κειμένου (σε αντίθεση με τους block ciphers οι οποίοι επενεργούν σε ομάδες (blocks) από bits, συνήθως της τάξης των 128 bits). Επιπλέον, οι streamciphers έχουν το προτέρημα ότι δεν πολλαπλασιάζουν τα λάθη, δηλαδή εάν συμβεί κάποιο λάθος κατά τη μετάδοση της κρυπτογραφημένης πληροφορίας και συγχρόνως αλλάξει η τιμή ενός bit,τότε η συγκεκριμένη ακολουθία κατά την αποκρυπτογράφησή της θα εμφανίζει το σφάλμα σε ένα μόνο bit.

Όπως προαναφέρθηκε, μία λειτουργία που καλείται να κάνει ένας stream cipher είναι η παραγωγή ενός key stream, δηλαδή μιας συγκεκριμένης ακολουθίας bits που έχει τον ρόλο κλειδιού. Το key stream χρησιμοποιείται για την επίτευξη της κρυπτογράφησης καθώς συνδυάζεται με το plaintext, διαδικασία που γίνεται μέσω XOR πράξης. Η μέθοδος κατασκευής του key stream μπορεί να στηρίζεται ή όχι από τις τιμές που λαμβάνουν τόσο το plaintext όσο και cipher text: σε αυτήν την περίπτωση, οι stream ciphers ονομάζονται ασύγχρονοι, ενώ διαφορετικά ονομάζονται σύγχρονοι. Οι περισσότεροι εν λειτουργία stream ciphers είναι οι σύγχρονοι.

2.1.1 Πως κατασκευάζονται οι stream ciphers

Οι κρυπταλγοριθμοι ροής αποτελούνται από κάποια βασικά συστατικά. Ένα από τα κυριότερα είναι και η γεννήτρια της κλειδαροής (keystream) η οποία αποτελεί μια περιοδική ακολουθία. Η αρχή κάθε περιόδου καθορίζεται από το κλειδί έναρξης Κ, το όποιο καλείται και ως μυστικό κλειδί του κρυπτοσυστήματος. Οι λόγοι για τους οποίους η κλειδοροή χαρακτηρίζεται από περιοδικό χαρακτήρα είναι δυο. Πρώτον, η γεννήτρια κλειδορονης οφείλει να μπορεί να συνθέσει την ίδια ακολουθία σε δυο ξεχωριστές τοποθεσίες την ίδια χρονική στιγμή. Άρα, η πραγματοποίηση των γεννητριών αυτών πρέπει να γίνεται από συσκευές οι όποιες μπορούν με αξιοπιστία να ακολουθούσουν αυτή τη διαδικασία. Δεύτερον, οι μοναδικές συσκευές που μπορούν να αντιμετωπίσουν τον περιορισμό αυτό είναι οι μηχανές πεπερασμένων καταστάσεων, στην κατηγορία των οποίων συμπεριλαμβάνονται και οι ηλεκτρονικοί υπολογιστές. Στην περίπτωση που δεν υπήρχε αυτός ο περιορισμός της αξιόπιστης αναπαραγωγής της κλειδοροής τότε αφενός θα έπρεπε να υπήρχε ένα αξιόπιστο κανάλι μετάδοσης της κλειδοροής η

οποία θα είχε μέγεθος όσο και το απλό κείμενο, και αφετέρου ως γεννήτρια κλειδοροης θα μπορούσε να ήταν μια οποιαδήποτε πηγή τυχαίων αριθμών ή άπλα σύμβολων.
Συνεχίζοντας, είναι σαφές πως για την δημιουργία ενός κρυπταλγόριθμου ροής είναι απαραίτητος και ο συγχρονισμός των δυο γεννητριών κλειδοροής του εκάστοτε συστήματος (δηλαδή του αποστολέα και του παραλήπτη), γεγονός που είναι πολύ σημαντικό καθώς ένας ενεργός αντίπαλος μπορεί να αποσυγχρονίσει το κρυπτοσύστημα παρεμβάλλοντας επιπλέον σύμβολα ή αριθμούς σε αυτό με αποτέλεσμα η αποκρυπτογράφηση να οδηγεί σε ένα απλό κείμενο διαφορετικό από το αρχικό.

Το προτέρημα ενός κρυπταλγόριθμου ροής είναι η υψηλή ταχύτητα που έχει στη διαδικασία της κρυπτογράφησης και αυτό διότι επειδή το κάθε σύμβολο του αρχικού κείμενου δεν έχει σχέση με τα υπόλοιπα, είναι δυνατόν να κρυπτογραφηθεί και έπειτα να σταλεί τη στιγμή που θα εισαχθεί στο κρυπτοσύστημα. Αυτός είναι και ο κύριος λόγος που οι κρυπταλγόριθμοι ροής βρίσκουν πολλές εφαρμογές στην κρυπτογράφηση τηλεφωνικών συνδιαλέξεων και γενικότερα σε εφαρμογές τηλεδιάσκεψης.
Τέλος, οι σύγχρονοι κρυπταλγόριθμοι ροής εμφανίζουν το μειονέκτημα της χαμηλής «διάχυσης» (diffusion)., αφού ένα σύμβολο του μηνύματος τελικά επηρεάζει μόνο ένα σύμβολο του κρυπτοκειμένου. Από την άλληπλευρά βέβαια, αυτή η ιδιότητα εμφανίζει και ένα πλεονέκτημα: γνωρίζοντας πως η πληροφορία ενός σύμβολου του εισαγωγικού κείμενου περιέχεται μόνο σε ένα σύμβολο του κρυπτοκειμένου είναι σαφές πως σε περίπτωση σφάλματος μετάδοσης ενός σύμβολου του κρυπτογραφημένου κείμενου δεν θα υπάρχει καμιά επιρροή στα γειτονικά σύμβολα και το σφάλμα κατά τη διαδικασία της αποκρυπτογράφησης θα περιοριστεί στο αντίστοιχο σύμβολο του απλού κείμενου.

2.1.2 Δημιουργία κρυπταλγόριθμου ροής από κρυπταλγόριθμο τμήματος

Ένας κρυπταλγόριθμος τμήματος χαρακτηρίζεται από υψηλή «διάχυση» και «σύγχυση» (όπως ορίζονται στη συνέχεια), ιδιότητες οι οποίες θα μπορούσαν εύκολα να χρησιμοποιηθούν για τη κατασκευή μιας γεννήτριας κλειδοροής για ένα κρυπταλγόριθμο ροής. Η διαδικασία αρχίζει με την κρυπτογράφηση ενός εισαγωγικού

απλού κείμενου που εισάγεται στον κρυπταλγόριθμο τμήματος, όπως είναι το [001....00]. Σε κάθε περίπτωση κρυπτογράφησης το κρυπτογραφημένο κείμενο του κρυπταλγόριθμου τμήματος καλείται ως απλό κείμενο, ενώ από τα επαναλαμβανόμενα αποτελέσματα διαλέγεται το πρώτο σύμβολο του τμήματος του κρυπτογραφημένου κείμενου και εξάγεται στη συνεχεία από τη γεννήτρια κλειδοροής, έτοιμο για λειτουργιά από έναν κρυπταλγοριθμο ροής.
Στην παρακάτω εικόνα(βλέπε παράγραφο 5.2) απεικονίζεται συνοπτικά αυτή η διαδικασία:

2.1.3 Δημιουργία αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής

Για την δημιουργία ενός αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής είναι απαραίτητη η συμβολή μιας γεννήτριας κλειδοροής με δυο εισόδους. Έτσι, είναι εύκολο να χρησιμοποιήσουμε τη μία από τις δύο για την κατασκευή ενός κρυπταλγόριθμου ροής που δεν θα έχει το μειονέκτημα της έλλειψης συγχρονισμού. Επίσης, για τη σύνθεση ενός τέτοιου κρυπταλγόριθμου είναι εξίσου απαραίτητη και η ύπαρξη ενός επιπροσθέτου συστατικού του κρυπταλγόριθμου, ο καταχωρητής ολίσθησης. Αυτός χρησιμοποιείται ως ένα μέσο αποθήκευσης x στοιχείων που απαιτούνται ως είσοδος στον κρυπταλγόριθμο τμήματος. Σε κάθε διαδικασίας κρυπτογράφησης του σύμβολου του απλού κείμενου, θα προκύπτει ένα σύμβολο το όποιο θα αποθηκεύεται στην πρώτη θέση του καταχωρητή ολίσθησης. Με τον τρόπο αυτό, στην επομένη κρυπτογράφηση το σύμβολο αυτό θα μεταφερθεί στη δεύτερη θέση με σκοπό να δώσει τη πρώτη θέση στο νέο σύμβολο που θα εισήχθη. Όταν ολοκληρωθούν οι x κρυπτογραφήσεις, το σύμβολο αυτό αποσυνδέεται από τον καταχωρητή. Έτσι, στην περίπτωση που υπάρξει κάποια αυθαίρετη εισαγωγή κρυπτοκειμένου κατά τη διαδικασία ή συμβεί κάποιο σφάλμα, τότε η διαδικασία αποκρυπτογράφησης θα ξανά-επανέλθει στην ορθή λειτουργία ύστερα από x αποκρυπτογραφήσεις από το τελευταίο λάθος.
Στην συνεχεία απεικονίζεται εν συντομία η διαδικασία δημιουργίας ενός αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής αναπαριστώντας τη συνδεσμολογία του: Εικόνα(βλέπε παράγραφο 5.2)

2.1.4 Άλλες τεχνικές

Η πλειοψηφία των κρυπταλγορίθμων ροής δεν βασίζεται σε κρυπταλγορίθμους τμήματος αλλά υπάρχουν ειδικές, «ad hoc», κατασκευές των γεννητριών κλειδοροής – γιατί, τελικά, η σχεδίαση ενός κρυπταλγορίθμου ροής ανάγεται σε σχεδίαση μιας γεννήτριας κλειδοροής. Το κρίσιμο ζήτημα πάντα είναι το να παράγεται μία κλειδοροή με καλά χαρακτηριστικά τυχαιότητας, όπως περιγράφεται και στη συνέχεια.

2.1.5 Οι One-Time Pad (cipher Vernam)

Αρχικά, παρατηρείται πως εκτός από το δυαδικό αλφάβητο ο Cipher Vernam συχνά ορίζεται και ως ci = mi ⊕ ki.. για i=1,2,3.., όπου m1, m2, m3, ... συμβολίζουν τα ψηφία του αρχικού μηνύματος. Αντίστοιχα για k1, k2, k3,.. χρησιμοποιούνται τα ψηφία του κλειδιου (keystream, εξού και το αρχικό ''k'') και για c1, c2, c3, . τα ψηφία του κρυπτογραφήματος. Το σύμβολο ⊕ αντιπροσωπεύει την λειτουργία του XOR. Έτσι συμπεραίνουμε πως η αποκρυπτογράφηση σε μια εξίσωση ορίζεται ως mi=ci ⊕ ki. Στην περίπτωση που τα k1, k2, k3 παράγονται ανεξάρτητα, είναι τυχαία και χρησιμοποιούνται μόνο μία φορά για την κρυπτογράφηση ενός μηνύματος και δεν ξαναχρησιμοποιούνται, τότε το κρυπτοσύστημα Vernam καλείται one- time pad και είναι ασφαλής όσον αφορά επιθέσεις σε κρυπτογραφήματα.

Η ασφάλεια του one time pad αποδεικνύεται βάσει τη σχετικής θεωρίας του Claude Shannon . (Shannon , 1949). Δηλαδή εάν τα K M και C που αναφέρονται στο εισαγωγικό μήνυμα, είναι τυχαίες παράμετροι και εάν το H δηλώνει τη σχέση της εντροπίας τότε ένα κρυπτογραφικό σύστημα είναι απεριόριστα ασφαλές αν και μόνο αν H(M|C)= H(M). Άρα το κρυπτογράφημα θα είναι ασφαλές καθώς δεν θα παρέχει πληροφορίες σχετικά με το αρχικό μήνυμα. Ο Claude Shannon κατέδειξα ότι απαραίτητη προϋπόθεση για να είναι μια συμμετρική κρυπτογράφηση ασφαλής είναι το H(K)>H(M), σύμφωνα με τον Shannon, συμπεραίνουμε και την αβεβαιότητα του μυστικού κλειδιού καθώς αυτή είναι σε μεγάλη σε τέτοιο βαθμό όσο και αυτή του κρυπτογραφήματος.

Στην περίπτωση που τα bits του κλειδιού επιλέγονται ανεξάρτητα και το μήκος του κλειδιού είναι k τότε H(K)=k και η υποχρεωτική συνθήκη του Shannon για απεριόριστη

ασφάλεια διαμορφώνεται ως εξής: k>=H(M). Το μεγάλο πλεονέκτημα λοιπόν του one time pad είναι ότι παρέχει απεριόριστη ασφάλεια.

Παρόλα αυτά, όμως υπάρχει και ένα ολοφάνερο αρνητικό στοιχειό του one-time pad το όποιο αφόρα το κλειδί καθώς το τελευταίο πρέπει να είναι τόσο μεγάλο όσο και το αρχικό μήνυμα το όποιο δυσχεραίνει τη διανομή και τη διαχείριση του.

Οι stream ciphers προσπαθούν, ουσιαστικά, να προσομοιάσουν το one time pad. Στους stream ciphers, η κλειδοροή (που παίζει το ρόλο που έχει το κλειδί στο one time pad) παράγεται από ένα μικρότερο μυστικό κλειδί, με στόχο να φαίνεται ότι είναι τυχαία σε έναν αντίπαλο. Αυτών των ειδών οι stream ciphers παρόλο που δεν προσφέρουν απεριόριστη ασφάλεια, έχουν ως στόχο το να είναι υπολογιστικά ασφαλείς.

2.1.6 Οι σύγχρονοι stream ciphers

Ως σύγχρονος stream cipher ορίζεται αυτός στον όποιο το key stream παράγεται ανεξάρτητα από το κρυπτογράφημα και το εισαγωγικό μήνυμα.
Οι εξισώσεις που περιγράφουν μια διαδικασία κρυπτογράφησης από σύγχρονο stream cipher είναι οι εξής:

$$\sigma i+1=f(\sigma i,k),\ zi=g(\sigma i,k),\ ci=h(zi,mi).$$

Ως σ0 ορίζεται η αρχική κατάσταση και καθορίζεται από το k (κλειδί). Ως f η επομένη συνάρτηση, ως g η συνάρτηση που παράγει το key stream zi,
ως h η συνάρτηση παράγωγης η οποία συνδέεται με το αρχικό μήνυμα mi και το key stream με σκοπό να γίνει η παράγωγη του κρυπτογραφήματος ci. Παρακάτω φαίνονται κάποιες εικόνες που αναπαριστούν τις διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης ενός σύγχρονου μοντέλου stream cipher. Εικόνες(βλέπε παράγραφο 5.2)

2.1.7 Τα χαρακτηριστικά ενός σύγχρονου stream cipher

- Προυποθέσεις συγχρονισμού. Είναι απαραίτητο κατα τη διάρκεια ενός σύγχρονου stream cipher ο παραλήπτης να είναι συγχρονισμένος με τον αποστολέα

προκειμένου να επιτευχθεί η σωστή κρυπτογράφηση. Στην περίπτωση που ενδεχόμενα ψηφία εισαγωγής ή διαγραφής του κρυπτογραφήματος διακόψουν τον συγχρονισμό, κατά τη διαδικασία της μετόδοσης, τότε αποτυγχάνεται η αποκρυπτογράφηση και μπορεί να αποκατασταθεί πάλι μόνο μέσω κάποιων τεχνικών που θα επιφέρουν πάλι τον συγχρονισμό.

- Όχι μετάδοση λαθών. Μία πολύ σημαντική ιδιότητα που παρέχει ο σύγχρονος stream cipher είναι πως στην περίπτωση που ένα ψηφίο του κρυπτογραφήματος τροποποιηθεί, αλλά δεν διαγραφεί, κατά τη διαδικασία της μετάδοσης τότε αυτό δεν θα επηρεάσει την αποκρυπτογράφηση των υπολοίπων ψηφίων του κρυπτογραφήματος.
- Ενεργές επιθέσεις. Παρατηρήθηκε απο το πρώτο χαρακτηριστικό πως η εισαγωγή, η διαγραφή, ή η αντικατάσταση ψηφίων κρυπτογραφήματος από κάποιον ενεργό αντίπαλο μπορεί να προκαλέσει άμεση έλλειψη συγχρονισμού και πιθανότατα να γίνει αντιληπτό από τον αποκρυπτογραφέα. Αντίστοιχα παρατηρήθηκε από το β) χαρακτηριστικό πως κάποιος ενεργός αντίπαλος ο οποίος θα είναι σε θέση να τροποποιεί κάποια συγκεκριμένα ψηφία του κρυπτογραφήματος θα μπορεί έτσι να επιδιώξει κάποια αλλαγή στο αρχικό μήνυμα.

2.1.8 Αυτοσυγχρονιζόμενοι stream ciphers

Ως αυτοσυγχρονιζόμενος/ ασύγχρονος stream cihper ορίζεται αυτός στον οποίο το keystream παράγεται μέσω του κλειδιού και ως μόνιμο αριθμό των προηγούμενων ψηφίων κρυπτογραφημάτων.

Οι εξισώσεις που περιγράφουν μια διαδικασία συνάρτησης κρυπτογράφησης από έναν αυτοσυγχρονιζόμενο stream cipher είναι οι εξής:

ci=h(zi,mi), zi=g(σi,k) και σι=(ci-t,ci-t+1,....ci-1)

Όπου σι=(ci-t,ci-t+1,....ci-1) συμβολίζεται η εισαγωγική κατάσταση, g η συνάρτηση παραγωγής του keystream zi, k το κλειδί, και h η τελική συνάρτηση που συνδυάζει το

εισαγωγικό μήνυμα mi με το keystream με στόχο τον σχηματισμό του κρυπτογραφήματος ci. Παρακάτω απεικονίζονται μερικές είκονες αναφορικά με τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μέσω ενός αυτοσυγχρονιζόμενου stream cipher.

2.1.9 Τα κυριότερα χαρακτηριστικά ενός αυτοσυγχρονιζόμενου μοντέλου stream cipher

- Αυτοσυγχρονισμός. Στην περίπτωση που τα ψηφία των κρυπτογραφημάτων εισάγονται ή διαγράφονται υπάρχει σαν ενδεχόμενο ο αυτοσυγχρονισμός καθώς μόνο ένας σταθερός αριθμός προηγούμενων χαρακτήρων κρυπτογραφημάτων καθορίζει την χαρτογράφηση της αποκρυπτογράφησης. Οι stream ciphers που συγκαταλέγονται σε αυτήν την κατηγορία είναι ικανοί να επανέλθουν αυτόματα στη σωστή αποκρυπτογράφηση, και μετά από έλλειψη συγχρονισμού. Βεβαίως, υπάρχει και ένας συγκεκριμένος μικρός αριθμός από το εισαγωγικό μήνυμα που δεν μπορεί να ανακτηθεί.

- Περιορισμένη διάδοση σφάλματος. Με δεδομένο πως η φύση ενός αυτοσυγχρονιζόμενου stream cipher καθορίζεται από t προηγούμενα ψηφία κρυπτογραφήματος επάγεται το συμπέρασμα πως εάν ένα μοναδικό ψηφίο του κρυπτογραφήματος τροποποιηθεί (δηλ. διαγράφει ή εισήχθη) ,κατά τη διαδικασία της μετάδοσης, τότε η αποκρυπτογράφηση περισσότερων από t συνεχόμενα ψηφία του κρυπτογραφήματος που θα ακολουθήσει θα είναι ορθή, χωρίς να απορρίπτεται η πιθανότητα πως θα προηγηθεί μια εσφαλμένη.

- Ενεργές επιθέσεις. Σύμφωνα με την προηγούμενη ιδιότητα συμπεραίνουμε πως μια εσκεμμένη τροποποίηση ψηφιών από έναν ενεργό αντίπαλο προκαλεί την λανθασμένη αποκωδικοποίηση άλλων ψηφιών του κρυπτογραφήματος. Αντίστοιχα και το α) χαρακτηριστικό έχει ως συνέπεια τη δύσκολη ανίχνευση κάποιων τροποποιήσεων (εισαγωγή, διαγραφή ή αντικατάσταση ψηφίων) από έναν ενεργό αντίπαλο. Με αφορμή λοιπόν, αυτά τα δυο είδη επιθέσεων, κυρίως όμως της δεύτερης, είναι απαραίτητο να ληφθούν πρόσθετα μέτρα που αποσκοπούν στην παροχή αυθεντικότητας της προέλευσης των δεδομένων καθώς και εγγυήσεις ακεραιότητας αυτών.

- Διάδοση στατιστικών του αρχικού μηνύματος. Γνωρίζοντας πως κάθε ψηφίο του εισαγωγικού μηνύματος παίζει σημαντικό ρολό στη διαμόρφωση του επόμενου κρυπτογραφήματος, επέρχεται η σύναψη πως οι στατιστικές ιδιότητες του αρχικού μηνύματος εξαπλώνονται μέσω του κρυπτογραφήματος. Συνεπώς, το συμπέρασμα που προκύπτει είναι πως οι αυτοσυγχρονιζόμενοι stream ciphers ίσως πλεονεκτούν σε αυθεντικότητα από τους συγχρόνους όσο αφόρα τις επικείμενες επιθέσεις στον πλεονασμό του εισαγωγικού μηνύματος.

2.1.10 Κύριες επιθέσεις στους stream ciphers

Α) Επίθεση στο κείμενο του κρυπτογραφήματος (cipher text only-attack)

Στην cipher text only-attack περίπτωση ο σκοπός του ενεργού αντίπαλου είναι να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο ή να εντοπίσει το αντίστοιχο κλειδί για την επίτευξη του στόχου καθώς αυτός έχει είσοδο μόν σε συγκεκριμένα τμήματα του κρυπτοκειμένου.

Β) Επίθεση με γνωστό απλό κείμενο (Known-plaintext attack)

Στην περίπτωση αυτή ο κύριος στόχος του ενεργού αντίπαλου είναι η ανακάλυψη ενός συγκεκριμένου κλειδιού, όπου όμως ο αντίπαλος γνωρίζει κάποιες από τις αντιστοιχίες ενός απλού κείμενου με το αντίστοιχο κρυφοκαιόμενο. Στην περίπτωση των κρυπταλγορίθμων ροής, η γνώση αυτή του επιτιθέμενου ισοδυναμεί με γνώση ενός τμήματος της κλειδοορής.

Γ) Επίθεση με επιλεγμένο απλό κείμενο (Chosen- Plaintext attack)

Στην περίπτωση επίθεσης με επιλεγμένο απλό κείμενο ο αντίπαλος δεν γνωρίζει το κλειδί για την αποκρυπτογράφηση του κρυπτογραφήματος. Παράλυτα, έχει τη δυνατότητα πρόσβασης στο κρυπτοσύστημα και είναι επίσης εφικτό για αυτόν να ζητήσει την κρυπτογράφηση μηνυμάτων της επιλογής του. Έτσι, με τη μέθοδο αυτή

είναι πιθανό να ανακαλύψει τη σωστή αντιστοιχία του απλού κείμενου με το αντίστοιχο άγνωστο κρυπτογραφημένο κείμενο.

Δ) Επίθεση προσαρμόσιμου επιλεγμένου απλού κείμενου (Adaptive chosen- plaintext attack)

Πρόκειται για μια ιδιαίτερη και σημαντική μέθοδο επίθεσης καθώς ο αντίπαλος υλοποιεί μια επίθεση με ένα επιλεγμένο απλό κείμενο. Επίσης, αυτός χρησιμοποιεί μια ειδική μεθοδολογία αναφορικά με την οποία η επομένη επιλογή του απλού κείμενου θα εξαρτάται από τις προηγούμενες, με απώτερο σκοπό την ταχύτερη ανακάλυψη του κλειδιού μέσω μια εξαντλητικής αναζήτησης, τη λεγόμενη Exhaustive Search.

Ε) Επίθεση με επιλεγμένο κρυπτογραφημένο κείμενο (Chosen-cipher text attack)

Η Chosen cipher text attack μέθοδος είναι μια μέθοδος για την οποία γίνεται η υπόθεση ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης και μπορεί να επιλέγει κρυπτοκείμενα προκειμένου να μαθαίνει πώς αυτά θα αποκρυπτογραφούνται. Το πιο επικίνδυνο σημείο όμως είναι ότι αυτός επιδιώκει την ανακάλυψη του κλειδιού αποκρυπτογράφησης ώστε στο μέλλον να μπορεί να αποκρυπτογραφεί τα νέα κρυπτογραφημένα κείμενα όταν δεν θα έχει δυνατή είσοδο στον αντίστοιχο αλγόριθμο αποκρυπτογράφησης.

ΣΤ) Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου (Adaptive chosen cipher text attack)

Τέλος, κατά την επίθεση προσαρμόσιμου επιλεγμένου κρυφοκαιόμενου παρατηρούνται αρκετές ομοιότητες με την αντίστοιχη του προσαρμόσιμου επιλεγμένου απλού κείμενου. Ωστόσο, η διαφορά που έχουν αυτές οι δυο μέθοδοι και που χάρις αυτήν διαφοροποιούνται είναι πως κατά την πρώτη ο ενεργός αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης.

Από τα παραπάνω λοιπόν επάγεται το συμπέρασμα πως είναι πολλές οι μέθοδοι επίθεσης που μπορεί να χρησιμοποιήσει ένας ενεργός αντίπαλος προκειμένου να αποκρυπτογραφήσει το κρυπτοκείμενο. Για τον λόγο αυτό ο αλγόριθμος χαρακτηρίζεται από δυο σημαντικές ιδιότητες που συμβάλουν στην αύξηση την προστασίας του από κάποιον ενεργό αντίπαλο. Αυτές είναι η Σύγχυση (Confusion) και η Διάχυση (Diffusion).

- Σύγχυση (Confusion): Πρόκειται για την πιο ισχυρή ιδιότητα προστασίας του αλγορίθμου κρυπτογράφησης, κατά την οποία ο αντίπαλος δεν είναι σε θέση να μπορεί να μαντέψει τις μεταβολές που θα πραγματοποιηθούν στο κρυφοκαιόμενο, δεδομένης μιας αλλαγής στο απλό κείμενο. Έτσι, βγαίνει το πόρισμα πως ένας αλγόριθμος χαρακτηρίζεται από υψηλή σύγχυση όταν οι σχέσεις μεταξύ του κρυπτογραφημένου κείμενου και του απλού κείμενου είναι ιδιαίτερα πολύπλοκες, με αποτέλεσμα ο αντίπαλος να πρέπει να δαπανήσει αρκετό χρόνο προκειμένου να τις προσδιορίσει.

- Διάχυση (Diffusion): Η δεύτερη ικανότητα που χαρακτηρίζει έναν αλγόριθμο κρυπτογράφησης είναι η διάχυση. Μέσω της ικανότητας αυτής ένα τμήμα του απλού κείμενου έχει τη δυνατότητα να μεταβάλλει όσο τον δυνατόν περισσότερα τμήματα του κρυπτογραφημένου κείμενου. Δηλαδή, γίνεται αντιληπτό πως ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα συγκεκριμένο και στοιχειώδεις τμήμα του απλού κείμενου έχει την δυνατότητα να επιδράσει σε όλα τα τμήματα του κρυπτογραφημένου κείμενου, ανεξαρτήτως της όποιας τοποθεσίας που κατέχουν αυτά στο απλό κείμενο.

Για να είναι ασφαλής λοιπόν ένας κρυπταλγόριθμος ροής, είναι απαραίτητο να ικανοποιούνται ορισμένες συνθήκες σχετικά με τη γεννήτρια κλειδορονης και τη ψευυδοτυχαια ακολουθία των bits που αυτή συνθέτει. Συγκεκριμένα, οι παράμετροι που επηρεάζουν τον βαθμό ασφάλειας ενός κρυπταλγόριθμου ροής είναι οι εξής:

- Η ψευδοτυχαία ακολουθία bits (κλειδοροή) που παράγεται από την γεννήτρια κλειδοροής θα πρέπει να έχει αρκετά μεγάλη περίοδο επανάληψης. Γνωρίζοντας πως η γεννήτρια κλειδοροής είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο το μυστικό κλειδί και συνθέτει στην έξοδο την κλειδοροή, είναι προφανές πως η κλειδοροή που θα παραχθεί από ένα της σημείο και μετά θα έχει περιοδικό χαρακτήρα. Συγκεκριμένα υστέρα από κάποιων αριθμό bits της κλειδοροής, αυτή θα επαναλαμβάνεται αρχίζοντας τώρα από την αρχή. Στην περίπτωση που η περίοδος

επανάληψης είναι πολλή μικρή, τότε το γεγονός αυτό καθιστά τον κρυπταλγόριθμο ροής σημαντικά ευάλωτο σε προσπάθειες κρυπταναλυσης από ενεργούς αντίπαλους. Έτσι, η περίοδος επανάληψης του κρυπτοκειμένου πρέπει να έχει μια μεγάλη έκταση προσδίδοντας της ασφάλεια σε πιθανές επιθέσεις.

- Η ακολουθία bits της κλειδοροής θα πρέπει να μοιάζει πολύ με τυχαία. Μια μαθηματική συνάρτηση που παίρνει μέρος στην γεννήτρια κλειδοροής θα ωφελούσε να επιλεγεί ειδικά έτσι ώστε το αποτέλεσμα που θα δώσει να προσεγγίζει όσο το δυνατόν περισσότερο το τυχαίο. Υπάρχουν κατάλληλες μέθοδοι δοκιμής της καταλληλότητας της γεννήτριας κλειδορονης, οι οποίοι χρησιμοποιούν διαφόρους ελέγχους τυχαιότητας (randomness tests) σε αυτή. Σε καμιά περίπτωση όμως παράγωγης της κλειδοροής αυτή δεν μπορεί να είναι εντελώς τυχαία, γιατί εν τέλει η κλειδοροή παράγεται από κάποια ντετερμινιστική διαδικασία (τη διαδικασία που υλοποιεί η εκάστοτε γεννήτρια κλειδοροής). Για αυτόν τον λόγο η ακολουθία ονομάζεται ψευδοτυχαία ακολουθία bits.

- Η κλειδοροή θα πρέπει να έχει μεγάλη γραμμική πολυπλοκότητα (linear complexity): Είναι γνωστό πως μέσω των γραμμικών μεθόδων μπορούν εύκολα να παραχθούν οποιεσδήποτε ακολουθίες δυαδικών ψηφιών όπως για παράδειγμα υπολογίζοντας την επομένη τιμή σύμφωνα με τις προηγούμενες της αλληλουχίας. Στην περίπτωση που οι προηγούμενες τιμές που απαιτούνται για τον υπολογισμό της επόμενης τιμής είναι σχετικά μικρές σε αριθμό και αυτές χρησιμοποιούνται στον υπολογισμό, τότε αναφέρεται πως η ακολουθία έχει μικρή γραμμική πολυπλοκότητα. Αντίστοιχα, εάν στον υπολογισμό χρησιμοποιούνται προηγούμενες τιμές οι όποιες είναι πολλές σε αριθμό τότε η ακολουθία αυτή θα έχει μεγάλη γραμμική πολυπλοκότητα. Μια κλειδοροή με μεγάλη γραμμική πολυπλοκότητα είναι αναγκαία προϋπόθεση για την ασφάλεια των κρυπτογραφημένων δεδομένων απέναντι σε προσπάθειες κρυπτανάλυσης τους από πιθανούς ενεργούς αντίπαλους.

Οι μέθοδοι που αναλύθηκαν προηγουμένως είναι αναγκαίες προκειμένου να εξασφαλίσουν έναν κρυπταλγόριθμο ροής αξιόπιστο, όχι όμως και επαρκείς. Για να θεωρηθεί ένας κρυπταλγόριθμος ροής αξιόπιστος σε πιθανές επιθέσεις θα πρέπει να εξασφαλίζει πως ακόμη και όταν κάποιος αποκτήσει μια πληροφορία για κάποιο κομμάτι της αλληλουχίας κλειδοροής να μην μπορεί υπολογιστικά να αποκομίσει αντίστοιχα πληροφορίες για άλλα κομμάτια της ακολουθίας.

2.1.11 Περιγραφή του RC4 αλγόριθμου ροής

Ο κρυπταλγόριθμος RC4 αποτελεί έναν από τους πιο γνωστούς και διαδεδομένους κρυπταλγόριθμους ροής και αυτό διότι χρησιμοποιείται αρκετά από πρωτόκολλα ασφάλειας (όπως το TLS). Θεωρήθηκε για πολλές δεκαετίες ασφαλής. Από το 2015 έχει διατυπωθεί ότι πρέπει να σταματήσει να υλοποιείται για λόγους ασφάλειας – εν τούτοις εξακολουθεί να συναντάται ακόμα και σήμερα (π.χ. πολλές ιστοσελίδες τον υποστηρίζουν, στο πλαίσιο υλοποίησης του πρωτοκόλλου TLS).

Ο RC4 αποτελεί έναν κρυπταλγόριθμο ροής σύμφωνα με τον όποιο το αλφάβητο του απλού κείμενου αποτελείται από τα γράμματα του συνόλου {0,1}^8. Οι χώροι αποθήκευσης απαρτίζονται από δυο πινάκες τους T[0..255] και S[0..255], όπου το κάθε στοιχείο του πίνακα αντιστοιχεί σε μια δυαδική λέξη της τάξεως των 8 bits.

Η έναρξη της διαδικασίας κρυπτογράφησης με έναν RC4 γίνεται με την αρχικοποίηση των πινάκων.

S[i] = i για $0 \leq i \leq 255$,

T[i] = K[i mod k] , για $0 \leq i \leq 255$, όπου K[j] η j-στη οκτάδα των bits του κλειδιού και k το μέγεθος του κλειδιού. Η έκφραση i mod k είναι αυτή που προκαλεί την ανακύκλωση των τιμών 1,2,3,4..,k μέχρι ότου τα bits του κλειδιού να γεμίσουν τον πινάκα T.

Εν συνεχεία το κλειδί T παίζει σημαντικό ρόλο καθώς είναι αυτό το οποίο ελέγχει την αντιμετάθεση που πραγματοποιούν τα στοιχεία του S. Στη συνέχεια, περιγράφονται οι σχέσεις που εξηγούν αυτή την αντιμετάθεση:

$j \leftarrow 0$: αρχική τιμή

$j \leftarrow j + S[i] + T[i] \bmod 256$ για $0 \leq i \leq 255$.

αντιμετάθεση: $S[i] \leftrightarrow S[j]$ για $0 \leq i \leq 255$.

Τελική διαδικασία είναι αυτή κατά την οποία παράγεται η ακολουθία της κλειδοροής:

$i \leftarrow 0, j \leftarrow 0$: αρχικές τιμές

$i \leftarrow i + 1 \bmod 256$, n φορες

$j \leftarrow j + S[i] \bmod 256$, n φορές

αντιμετάθεση S[i] ↔ S [j] , n φόρες

t ← S[i] + S [j] mod 256 , n φόρες

k=S[t] , n φορές

όπου n το μέγεθος του απλού κειμένου κατά την κρυπτογράφηση ή του κρυπτοκειμένου κατά την αποκρυπτογράφηση. Όταν ολοκληρώνεται η διαδικασία του κύκλου των υπολογισμών, η μεταβλητή k είναι αυτή που συμβολίζει την κλειδοροή, η οποία έχει την ικανότητα να συνδυάζεται με τα δεδομένα (απλό κείμενο ή κρυπτογραφημένο κείμενο) μέσω μιας αποκλειστικής διάζευξης (πράξη XOR).

Στη συνεχεία απεικονίζεται μια εικόνα(βλέπε παράγραφο 5.2) σχετικά με τα σταδία λειτουργίας του RC4.

Συνοπτικα τα χαρακτηριστικα ενος RC4 ειναι:

• Αποτελείται από δύο πίνακες, τον S[0,1,.., 255] και τον T[0,1,.., 255]

• Κάθε στοιχείο των πινάκων είναι 1 bit

• Γίνεται η αρχικοποίηση – S[i]=i για 0<=i<=255 και T[i]=K[i mod k] για 0<=i<=255 με K[j] το j-οστό bit του κλειδιού και k το μέγεθος του κλειδιού

• Αντιμετάθεση των στοιχείων του πίνακα S με τον πίνακα του κλειδιού T – j□0: αρχική τιμή – j□j+S[i]+T[i] mod 256 και S[i]□□S[j] για 0<=i<=255

Συνοπτικά η διαδικασία που ακόλουθη ένας RC4 κρυπταλγοριθμος ροής είναι η εξής:

i ← 0, j ← 0

i ← i + 1 mod256, n φορές

j ← j +S [i] mod 256, n φορές

αντιμετάθεση: S[i] ↔ S[j] , n φορές

t← S[i] + S [j] mod 256, n φορές

k=S[t] , n φορές

Ένας ακόμη σημαντικός κρυπταλγόριθμος ροής που έπαιξε πολύ σημαντικό ρολό τη δεκαετία του 1993 είναι ο αλγόριθμος SEAL (Software-optimized Encryption Algorithm). Αυτός αποτελεί έναν δυαδικό προσθετικό κρυπταλγόριθμο ροής, είναι σχετικά καινούριος και για αυτόν τον λόγο δεν έχει υποστεί αναλυτική έρευνα όσο αφορά την κρυπτογραφική του ικανότητα. Το ισχυρό του στοιχείο που τον χαρακτηρίζει είναι πως αποτελεί έναν από τους λιγοστούς κρυπταλγόριθμους ροής που κατασκευάστηκε για αποδοτικές υλοποιήσεις λογισμικού και συγκεκριμένα για επεξεργαστές 32- bit.

Τέλος, πρέπει να σημειωθεί ότι το νέο πρότυπο του γνωστού πρωτοκόλλου TLS, το TLS 1.3., έχει αντικαταστήσει τον RC4 με έναν νέο κρυπταλγόριθμο ροής, τον λεγόμενο αλγόριθμος Chacha20.

2.1.12 Καταχωρητές ολίσθησης με ανάδραση (FSR)

Μία δομή που συναντάται σε πολλές γεννήτριες κλειδοροής είναι ο καταχωρητής ολίσθησης με ανάδραση (Feedback Shift Register – FSR), ο οποίος μπορεί να είναι είτε γραμμικός (LFSR) είτε μη γραμμικός (NLFSR).

Ας υποθέσουμε ότι το πεπερασμένο σώμα Fq αποτελείται από q στοιχεία. Τελικά περιοδική ακολουθία (ultimately periodic) καλείται αυτή η οποία είναι της μορφής $y = \{y_i\}$, $i \geq 0$, με στοιχεία στο σώμα Fq, εφόσον υπάρχουν ακέραιοι $T > 0$ και $t0 \geq 0$ τέτοιοι ώστε $y_{i+T} = y_i \ \forall \ i \geq t0$. Ο μικρότερος ακέραιος T που χαρακτηρίζεται από την παραπάνω ιδιότητα καλείται πρωταρχική περίοδος της ακολουθίας y (fundamental period) ή αλλιώς περίοδος. Η προ-περίοδος (preperiod) της y εκφράζεται από τον ακέραιο t0. Στην περίπτωση που $t0 = 0$, τότε η ακολουθία y ονομάζεται περιοδική (periodic). Αν μια αλληλουχία παίρνει τιμές στο $F2 = \{0, 1\}$ (δηλαδή q=2), τότε ονομάζεται δυαδική ακολουθία. Η δυαδική ακολουθία αποτελεί τη συνηθέστερη περίπτωση για κρυπτογραφικές εφαρμογές.

Μια αλληλουχία πεπερασμένου μήκους με Z στοιχεία συμβολίζεται με y^Z. Για κάθε τέτοια πεπερασμένη αλληλουχία y^Z = y0y1...yZ-1 και για κάθε j≤ Z χαρακτηρίζουμε με y^j την υπακολουθία y0y1 . . . yj−1 που απαρτίζεται από τα πρώτα j στοιχεία της y. Κάθε υπακολουθία τέτοιου είδους (substring) ονομάζεται πρόθεμα (prefix) της y^Z. Εάν j<Z τότε η επακολουθία y^j ονομάζεται γνήσιο πρόθεμα (proper prefix) της y^Z. Ορίζεται επίσης, y^j = yiyi+1 . . . yj για κάθε i ≤ j - συνεπώς, y^j = y0^ j−1. Στην περίπτωση που j=Z-1, τότε κάθε επακολουθία yi^j ονομάζεται επίθεμα (suffix) της y^Z. Αντίστοιχα, εάν ισχύει i>0 για ένα επίθεμα τότε αυτό καλείται γνήσιο επίθεμα (proper suffix).

Κάθε περιοδική ή τελικά περιοδική ακολουθία μπορεί να παραχθεί από καταχωρητή ολίσθησης με ανάδραση (FeedBack Shift Register, FSR), ο οποίος αποτυπώνεται στο επόμενο σχήμα(βλέπε παράγραφο 5.2).

Ένας καταχωρητής ο όποιος στο σώμα Fq έχει μνήμη z τότε θα αποτελείται από z θέσεις μνήμης ή αλλιώς βαθμίδες, κάθε μια εκ των οποίων μπορεί να περιέχει ένα στοιχείο του σώματος Fq. Το περιεχόμενο της κάθε θέσης μνήμης κινείται μια θέση προς τα δεξιά σύμφωνα με κάθε δευτερόλεπτο, ενώ η τιμή της αριστερότερης κλίμακας εξαρτάται από την πράξη ανάδρασης h. Επάγεται το συμπέρασμα δηλαδή πως κάθε αλληλουχία που συντίθενται από έναν καταχωρητή τέτοιου είδους ικανοποιεί πλήρως την αναδρομική σχέση που έπεται: yi+n = h(yi+n−1, . . . , yi), i ≥ 0, όπου η συνάρτηση h : Fq^z → Fq είναι μη γραμμική στη γενική περίπτωση, και στην πλειοψηφία των περιπτώσεων ο σταθερός ορός της συνάρτησης h είναι άσος με το 0.

Η κατάσταση (state) του FSR καθορίζεται κάθε χρονική στιγμή από τα στοιχεία των θέσεων μνήμης. Δηλαδή αν ορίσουμε x την παραγόμενη αλληλουχία από έναν FSR τότε η κατάσταση του για κάθε χρονική στιγμή i ≥ 0 δίνεται από το διάνυσμα (xi+z-1 xi+z-2 .... xi). Είναι πασιφανές πως ένας FSR μήκους z μπορεί να επέλθει από q^z διαφορετικές καταστάσεις. Έτσι, καταλαβαίνουμε πως q^z είναι η μέγιστη περίοδος που μπορεί να έχει μια αλληλουχία που συντίθεται από έναν FSR z βαθμίδων.

Μια παρατήρηση αναφορικά με τους FSR των οποίων η συνάρτηση ανάδρασης έχει σταθερό όρο ίσο με το μηδέν είναι πως η βέλτιστη δυνατή περίοδος της ακολουθίας εξόδου τους είναι q^z-1 διότι εάν ο FSR επέλθει από τη μηδενική κατάσταση τότε θα σταθεροποιηθεί σε αυτή.

Στο υπόλοιπο κομμάτι της ενότητας θα θεωρηθεί ότι ο σταθερός όρος της συνάρτησης ανάδρασης θα είναι πάντα 0.

Στην ιδιαίτερη περίπτωση των δυαδικών αλληλουχιών, το διάγραμμα ενός καταχωρητή ολίσθησης με ανάδραση (όπως αυτό που αναφέρθηκε πρώτα) απεικονίζει άμεσα και την πραγματοποίηση του σε βαθμό λογικών πυλών. Συγκεκριμένα, οι θέσεις μνήμης του καταχωρητή αντιστοιχούν σε flip-flops και οι πολλαπλασιασμοί και οι προσθέσεις που χρησιμοποιούνται στη συνάρτηση ανάδρασης h πραγματοποιούνται ως απλοί πολλαπλασιαστές και αθροιστές αντίστοιχα σε κλίμακα bit. Στην γενική περίπτωση που οι όποιες πράξεις λαμβάνουν χωρά πάνω σε κάποιο πεπερασμένο σώμα Fq, τότε οι πολλαπλασιασμοί και οι προσθέσεις πάνω στο σώμα αυτό θα έχουν πολυπλοκότερη πραγματοποίηση. Επιπλέον, μια συνάρτηση ανάδρασης h καλείται λογική συνάρτηση (Boolean Function) με n μεταβλητές, εάν και μονό εάν η παραγόμενη ακολουθία είναι δυαδική.

Το μέγεθος του μικρότερου FSR που παράγει μία ακολουθία αποτελεί ένα σημαντικό για αυτήν κρυπτογραφικό κριτήριο, όπως περιγράφεται στο επόμενο κεφάλαιο.

Κεφάλαιο 3
(Μη) γραμμική πολυπλοκότητα ακολουθιών

Στη δεκαετία του 1950, οι γραμμικοί καταχωρητές ολίσθησης με ανάδραση Linear Feedback Shift Registers – LFSR) εισήχθησαν στην εφαρμογή της κρυπτογράφησης ροής.

Τις επόμενες δεκαετίες, δεδομένου ότι ήταν εύκολο να εφαρμοστούν από τα τεχνολογικά υλικά της εποχής και να γίνει η επεξεργασία τους γρήγορα, οι LFSR συνιστούσαν συχνά τις γεννήτριες ακολουθιών ψευδοτυχαίων ακολουθιών.

Το πιο σημαντικό είναι ότι λόγω της υιοθέτησης της χρήσης των LFSRs στη ροή κρυπτογράφησης, οι κρυπτογράφοι και οι μαθηματικοί μπορούσαν να χρησιμοποιήσουν αυστηρή μαθηματική θεωρία για να αναλύσουν την ασφάλειά τους γιατί οι μαθηματικές τους ιδιότητες είναι πλήρως θεμελιωμένες.

Ωστόσο, η γραμμική πολυπλοκότητα (linear complexity) μίας ακολουθίας, όπως την περιγράψαμε ανωτέρω και στο Κεφάλαιο 2, ορίζεται ως το μέγεθος του μικρότερου LFSR ο οποίος παράγει μία ακολουθία. Συνεπώς, είναι σημαντικό να μην υπάρχει μικρός LFSR ο οποίος παράγει μία ακολουθία. Επίσης, οι LFSR δεν μπορούν από μόνοι τους να αποτελούν γεννήτριες κλειδοροής, γιατί αναπόφευκτα παράγουν ακολουθίες χαμηλής γραμμικής πολυπλοκότητας (στην καλύτερη περίπτωση, ίση με το μέγεθός τους).

Μία ευρύτερη έννοια της γραμμικής πολυπλοκότητας μιας ακολουθίας είναι η μη γραμμική πολυπλοκότητα αυτής, όπως περιγράφεται στη συνέχεια.

3.1 Πολυπλοκότητα ακολουθίας

Μη γραμμική πολυπλοκότητα (nonlinear complexity) ή πιο απλά πολυπλοκότητα ακολουθίας ορίζεται ως το μήκος του μικρότερου FSR που παράγει την ακολουθία. Κάθε FSR που παράγει μία ακολουθία με μήκος όσο το αντίστοιχο της πολυπλοκότητάς της ορίζεται ως ο ελάχιστος FSR της ακολουθίας. Ομοίως, γραμμική πολυπλοκότητα ακολουθίας (linear complexity) ορίζεται το μήκος του μικρότερου LFSR ο οποίος παράγει την ακολουθία. Ο ελάχιστος LFSR για μία ακολουθία ορίζεται με όμοιο τρόπο.

Από τα παραπάνω προκύπτει εύλογα ότι c(y) είναι η μη γραμμική πολυπλοκότητα, και lc(y) είναι αντίστοιχα η μη γραμμική για δεδομένη ακολουθία y, τότε ισχύει ότι c(y) ≤ lc(y).

Για μία ακολουθία yN = y0y1 . . . yN−1 με πεπερασμένο μήκος, ορίζεται ως προφίλ πολυπλοκότητας (complexity profile) η ακολουθία c(y1), c(y2). . . , c(yN), όπου. Οι αριθμοί αυτοί είναι ακέραιοι. Κατά όμοιο τρόπο ορίζεται και το προφίλ γραμμικής πολυπλοκότητας (linear complexity profile) (). R. Lidl and H. Niederreiter, 1986)

3.1.1 Γραμμική πολυπλοκότητα

Αναφορικά με την γραμμική πολυπλοκότητα ακολουθιών πεπερασμένου μήκους έχουν διεξαχθεί πολλές μελέτες, οι οποίες έχουν καταλήξει σε ορισμένες πολύ σημαντικές ιδιότητες. Οι τρεις κορυφαίες εξ αυτών είναι οι εξής:

1. Αν j > i, τότε lc(yj) ≥ lc(yi).

2. Αν lc(yi+1) > lc(yi), τότε lc(yi) ≤ i/2 .

3. Αν lc(y i+1) > lc(yi), τότε lc(yi+1) + lc(yi) = i + 1.

Οι ιδιότητες αυτές στην πράξη, περιγράφουν ότι αν αυξηθεί της γραμμικής πολυπλοκότητας σε μία ακολουθία πεπερασμένων αριθμών, τότε η νέα γραμμική πολυπλοκότητα είναι συμμετρική σε σχέση με την προηγούμενη, ως προς την f(N) = N/2 , όπου N = 1, 2, ... Εικόνα(βλέπε παράγραφο 5.2)

Η αναμενόμεμη τιμή της γραμμικής πολυπλοκότητας μίας τυχαίας ακολουθίας έχει αποδειχθεί ότι ισούται με N/2, όπου N το μέγεθός της.

3.1.2 Αλγόριθμος Berlekamp-Massey (BMA)

Για να υπολογιστεί το ελάχιστο LFSR που παράγεται από μία ακολουθία μπορεί να χρησιμοποιηθεί ο αλγόριθμος Berlekamp - Massey (BMA). Ο αλγόριθμος αυτός είναι ιδιαίτερα διαδεδομένος για την υλοποίηση του σκοπού αυτού και πρωτοεμφανίστηκε για να καταφέρει Berlekamp το 1967 να αποκωδικοποιήσει κώδικες BCH. Μετά από δύο χρόνια σειρά είχε ο Massey να χρησιμοποιήσει τον αλγόριθμο αυτό για να βρει το ελάχιστο LFSR που απαιτείται για να παραχθεί η ακολουθία yN. Ο αλγόριθμος αυτός ουσιαστικά εκτελεί μια αναδρομή για να υπολογίσει το πολυώνυμο ανάδρασης του ελάχιστου LFSR σε όλες τις υπακολουθίες yi , 1 ≤ i ≤ N.

Σε κάθε βήμα του αλγορίθμου (χρονικές στιγμές n, όπου 0 ≤ n < N), πραγματοποιείται ο εξής έλεγχος: «αν ο τρέχων ελάχιστος LFSR της υπακολουθίας yn παράγει την υπακολουθία yn+1 ». Αν η συνθήκη αυτή ισχύσει, τότε ο τρέχων LFSR αποτελεί και τον ελάχιστο LFSR για την υπακολουθία yn+1 και παραμένει αμετάβλητος (δηλαδή d = 0). Αν η συνθήκη δεν ισχύσει στο τρέχον βήμα, τότε ελέγχεται αν η γραμμική πολυπλοκότητα της ακολουθίας yn+1 είναι μεγαλύτερη ή ίση από την γραμμική πολυπλοκότητα της ακολουθίας yn.

Στην περίπτωση που η γραμμική πολυπλοκότητα της yn+1 είναι ίση (δηλαδή, 2 lc(yn) > n) ή μεγαλύτερη (δηλαδή 2 lc(yn) ≤ n), τότε εισάγεται ένας ακόμη όρος, μια «διορθωτική συνάρτηση» στο πολυώνυμο ανάδρασης του ελάχιστου LFSR της ακολουθίας yn για να προσδιοριστεί αντίστοιχα το πολυώνυμο ανάδρασης του ελάχιστου LFSR της ακολουθίας yn+1. Η συνάρτηση αυτή είναι πλήρως ορισμένη και έχει σχέση με το πολυώνυμο ανάδρασης του ελάχιστου LFSR της ακολουθίας yj , όπου το j, j < n συμβολίζει την πιο πρόσφατη χρονική στιγμή που σημειώθηκε αύξηση στην τιμή της γραμμικής πολυπλοκότητας.

Στην περίπτωση των δυαδικών ακολουθιών, ο αλγόριθμος Berlekamp-Massey γίνεται ακόμα πιο απλός, διότι σε αυτές τις περιπτώσεις οι συναρτήσεις που προστίθενται είναι πράξεις XOR. Για παράδειγμα, σε μία δυαδική ακολουθία με μήκος N, ο αλγόριθμος

Berlekamp-Massey έχει πολυπλοκότητα O (N2). Εικόνα(βλέπε παράγραφο 5.2) (J. L. Massey.,1969)

3.1.3 Ιδιότητες αλγόριθμου Berlekamp-Massey

Ο αλγόριθμος Berlekamp-Massey έχει μια πολύ σπουδαία ιδιότητα ως προς το προφίλ γραμμικής πολυπλοκότητάς του, το οποίο τον καθιστά ένα ιδιαίτερα ισχυρό εργαλείο για την κρυπτογράφηση. Η ιδιότητα αυτή είναι η εξής: «ο ελάχιστος LFSR μίας ακολουθίας yN είναι μοναδικός αν και μόνο αν lc(yN) ≤ N/2». Αυτό στην πράξη, σημαίνει ότι αν η γραμμική πολυπλοκότητα για μία ακολουθία είναι L, τότε αρκεί να γνωρίζουμε μόνο ένα πλήθος 2L διαδοχικών στοιχείων της ακολουθίας αυτής, ώστε χρησιμοποιώντας τον αλγόριθμο Berlekamp - Massey, να προσδιοριστεί ολόκληρη η ακολουθία. Έτσι, ο BMA έθεσε τη γραμμική πολυπλοκότητα ως ένα από τα πλέον σημαντικά κρυπτογραφικά κριτήρια, καθώς μία ακολουθία, όταν χρησιμοποιείται ως κλειδοροή σε έναν αλγόριθμο κρυπτογραφικής ροής πρέπει να έχει όσο τον δυνατόν μεγαλύτερη γραμμική πολυπλοκότητα.

Μία συνέπεια του αλγορίθμου Berlekamp-Massey είναι η εξής: αν μία ακολουθία έχει γραμμική πολυπλοκότητα N, τότε χρειάζεται να είναι γνωστά μονάχα 2N διαδοχικά bits της ακολουθίας αυτής ώστε να είναι εφικτός ο πλήρης προσδιορισμός ολόκληρης της ακολουθίας – και αυτό γιατί στην περίπτωση αυτή ο μοναδικός LFSR που την παράγει είναι μοναδικός και άρα μπορεί να βρεθεί με τον αλγόριθμο αυτόν.

Μία τυχαία ακολουθία λοιπόν δεν αναμένεται να μπορεί να «προβλεφθεί» από τον αλγόριθμο Berlekamp-Massey αφού η γραμμική της πολυπλοκότητα αναμένεται να είναι N/2. Βέβαια, όπως ήδη είδαμε νωρίτερα, οι κλειδοροές στην πράξη δεν είναι τελείως τυχαίες αλλά ψευδοτυχαίες.

3.1.4 Ιδιότητες μη γραμμικής πολυπλοκότητας

Η μη γραμμική πολυπλοκότητα δεν έχει μελετηθεί στον ίδιο βαθμό με τη γραμμική. Παρακάτω θα δούμε κάποιες σημαντικές ιδιότητες που έχει η μη γραμμική πολυπλοκότητα της ακολουθίας $yN = y0\ y1 \ldots yN-1$ μήκους N, (όπου N φυσικός), και παίρνει τιμές σε οποιοσδήποτε σώμα. Οι αποδείξεις παραλείπονται, χάριν οικονομίας του κειμένου.

1. Η τιμή της μη γραμμικής πολυπλοκότητας c(y) της ακολουθίας y υπολογίζεται ως εξής: Έστω L ο μεγαλύτερος ακέραιος αριθμός που ικανοποιεί την ακόλουθη ιδιότητα: υπάρχουν i, j, N, ακέραιοι, για τους οποίους ισχύει ότι $0 \leq i < j \leq N - 1 - L$ που να ικανοποιούν τις ακόλουθες ισότητες:

i. $yi\,i+L-1 = yj\,j+L-1$

ii. $yi+L \neq yj+L$.

Τότε, ισχύει ότι $c(yN) = L + 1$.

2. Έστω $c(yn-1) = m$ και ότι για την ακολουθία $yn-1$ ο ελάχιστος FSR της δεν μπορεί να παράξει την yn . Ισχύει ότι $c(yn-1) = c(yn)$ □ η υπακολουθία $yn-m-1n-2$

δεν αποτελεί τμήμα της $yn-1$.

3. Έστω $c(yn-1) = m$. Αποδεικνύεται ότι αν ο ελάχιστος FSR της $yn-1$ δεν παράγει ο ίδιος το τελευταίο στοιχείο $(yn-1)$ της συνάρτησης, τότε ισχύει ότι $c(yn) > m$ □ υπάρχει i ακέραιος, που να ικανοποιούνται οι σχέσεις:

i. $0 \leq i < n - m - 1$

ii. $yi\,i+n-1 = yn-m-1n-2$

iii. $yi+m \neq yn-1$

4. Οι προηγούμενες δύο ιδιότητες μπορούν να συνδυαστούν για τον προσδιορισμό μιας ικανής και αναγκαίας συνθήκης ούτως ώστε όποτε προστεθεί το n-ιοστό στοιχείο της, να σημειωθεί αύξηση της πολυπλοκότητάς της.

5. Έστω $c(yn-1) = m$ και έστω $c(yn-1) < c(yn)$. Αν υπάρχουν i, n ακέραιοι που να ισχύει ότι:

i. $i \leq n - m - 1$

ii. $0 \leq j < i$

iii. $y_{j+m-1} = y_{i+m-1}$

τότε ισχύει και η σχέση: $c(y_n) = c(y_{n-1}) + (n - m - i) = n - i$

6. Αποδεικνύεται ότι για τον ακέραιο i που ορίστηκε αμέσως προηγουμένως, , αν με $t_0(n-1)$ συμβολίσουμε την προ – περίοδο και με $T(n-1)$ την περίοδο για μια ακολουθία που έχει μήκος yn-1, ισχύει ότι: $i = t_0(n-1) + T(n-1)$

7. Σε συνέχεια του προηγουμένου, αποδεικνύεται εύκολα ότι $t_0(n-1) = j$ και

$T(n-1) = i - j$. Έτσι, συνεπάγεται ότι αν k οριστεί η αύξηση $c(y_n) - c(y_{n-1})$,ισχύει ότι: $k = n - m - (t_0(n-1) + T(n-1))$

8. Αν υπάρχει ακολουθία y_n και k ακέραιος, που να επαληθεύουν τις παρακάτω ισότητες:

i. $c(y_{n-1}) = m$

ii. $c(y_n) = m + k$

τότε κάθε υπακολουθία της y_n με μήκος $m + k$ είναι διαφορετική από την αμέσως προηγούμενη και την αμέσως επόμενη.

9. Σε συνέχεια του προηγουμένου, για την ίδια ακολουθία y_n, αν για τον ακέραιο k ισχύει $1 \leq k$, και επεκτείνουμε την y_n κατά k πλήθους στοιχεία, τότε και η νέα ακολουθία y_{n+k} θα έχει την ίδια πολυπλοκότητα, δηλαδή $c(y_{n+k}) = m + k$

Τέλος, ενδιαφέρον έχουν και οι ακόλουθες παρατηρήσεις:

1. Αποδεικνύεται ότι, για μία ακολουθία y που παίρνει τιμές σε οποιοδήποτε πεπερασμένο σώμα, ένα DAWG (directed acyclic word graph - κατευθυνόμενος ακυκλικός γράφος λέξεων) είναι ικανό για να προσδιορίσει το προφίλ της μη γραμμικής πολυπλοκότητας της ακολουθίας y, δηλαδή ότι οι λέξεις του γράφου είναι κατάλληλα επιλεγμένες υπακολουθίες της y.

2. Υπάρχει μία προσεγγιστική κατανομή της μη γραμμικής πολυπλοκότητας για τυχαίες δυαδικές ακολουθίες, πράγμα ιδιαίτερα χρήσιμο για την εκτίμηση της

ψευδοτυχαιότητας των ακολουθιών αυτών. Η τιμή αυτή για δυαδικές ακολουθίες είναι 2log2N, όπου N το μέγεθος της ακολουθίας.

3. Μπορεί να υπολογιστεί ένα ελάχιστο μη γραμμικό FSR το οποίο να παράγει μία οποιαδήποτε ακολουθία στο F2. Για τον υπολογισμό αυτό αξιοποιούνται οι ιδιότητες του πίνακα του ισοδύναμου γραμμικού συστήματος εξισώσεων, καθώς με τη λύση του συστήματος αυτού προσδιορίζεται η συνάρτηση ανάδρασης του ελάχιστου FSR.

4. Τέλος, για γραμμικές πολυπλοκότητες οποιασδήποτε τιμής, μπορούν να κατασκευαστούν ακολουθίες που να έχουν τη μέγιστη δυνατή τιμή μη γραμμικής πολυπλοκότητας.

3.1.5 k-error γραμμική πολυπλοκότητα

Μία υψηλή γραμμική πολυπλοκότητα αποτελεί αναγκαία αλλά όχι ικανή συνθήκη λειτουργίας για μία ακολουθία προκειμένου αυτή να μπορεί να έχει ισχυρή κρυπτογράφηση. Επομένως, απαιτούνται να γίνουν ακόμα επιπλέον δοκιμές προκειμένου να προσδιοριστούν ποια χαρακτηριστικά πρέπει να έχει μια ακολουθία για να είναι πιο ισχυρή ως προς το κομμάτι της κρυπτογράφησης. Ο Rueppel έχει αποδείξει ότι το προφίλ γραμμικής πολυπλοκότητας είναι χρήσιμο για το σκοπό αυτό.

Το γραμμικό προφίλ πολυπλοκότητας μιας ακολουθίας πεπερασμένου μήκους (s) λαμβάνεται με την γραφική παράσταση της γραμμικής πολυπλοκότητας των sos1…sn, για n = 1, 2, ... Ο Rueppel ισχυρίζεται ότι μια κρυπτογραφικά ισχυρή ακολουθία θα πρέπει να έχει μια γραμμική πολυπλοκότητα κοντά στο μέγιστο δυνατό και αυτή η πολυπλοκότητα θα πρέπει να ακολουθεί τη συνάρτηση n / 2 "στενά αλλά ακανόνιστα".

Παρακάτω, ακολουθεί ο ορισμός ενός μέτρου της πολυπλοκότητας των περιοδικών ακολουθιών που έχει εφαρμογή στο πρόβλημα της αναγνώρισης κρυπτογραφικά ισχυρών ψευδοτυχαίων ακολουθιών.

Ορισμός 4.1 Η γραμμική πολυπλοκότητα του k-σφάλματος της περιοδικής ακολουθίας πεπερασμένου μήκους (s) = (sos1…sn,) που καλείται cs, είναι η μικρότερη γραμμική

πολυπλοκότητα που μπορεί να ληφθεί όταν τροποποιηθούν οποιαδήποτε k (το πολύ) ψηφία της, όπου το k είναι προφανώς μικρότερο ή ίσο με το μήκος της ακολουθίας.

Το k- error (σφάλμα k χαρακτήρων της ακολουθίας) της γραμμικής πολυπλοκότητας μπορεί να ερμηνευθεί ως το χειρότερο δυνατό μέτρο της γραμμικής πολυπλοκότητας όταν συμβαίνουν k ή λιγότερα σφάλματα, δηλαδή όταν αλλοιωθούν k ή λιγότερα ψηφία της ακολουθίας - εξού και ο όρος «σφάλμα γραμμικής πολυπλοκότητας».

Όπως είναι φανερό, για την ειδική περίπτωση που k = 0, η γραμμική πολυπλοκότητα 0-σφάλματος οποιασδήποτε ακολουθίας είναι απλώς η συνηθισμένη γραμμική πολυπλοκότητα.

Η γραμμική πολυπλοκότητα σφάλματος k μπορεί να παρέχει περισσότερες πληροφορίες σχετικά με την κρυπτογραφική ισχύ μιας ψευδοτυχαίας ακολουθίας σε σχέση με άλλες προτεινόμενες μεθόδους. Για παράδειγμα, μπορεί μία ακολουθία να έχει πολύ υψηλή γραμμική πολυπλοκότητα, αλλά μία άλλη ακολουθία που διαφέρει μόνο σε μία θέση από την αρχική να έχει πολύ μικρή γραμμική πολυπλοκότητα. Αυτό σημαίνει ότι η γραμμική πολυπλοκότητα 1 σφάλματος της αρχικής ακολουθίας είναι μικρή. Άρα, θα μπορούσαμε να προβλέψουμε την «αλλοιωμένη» εκδοχή της ακολουθίας (π.χ. με τον αλγόριθμο Berlekamp-Massey), το οποίο σημαίνει με πρόβλεψη σχεδόν της πραγματικής ακολουθίας (με μόνο σε ένα ψηφίο να έχουμε λάθος). (Takayasu et al, 1998)

3.1.6 Αλγόριθμος k-error γραμμικής πολυπλοκότητας

Η k-error γραμμική πολυπλοκότητα οποιασδήποτε ακολουθίας θα μπορούσε να υπολογιστεί με επαναλαμβανόμενη εφαρμογή του αλγορίθμου Berlekamp -Massey ή, σε κάποιες περιπτώσεις, με έναν άλλο γνωστό αλγόριθμο των Chan- Games (ο οποίος εφαρμόζεται σε περιοδικές κολουθίες με περίοδο 2n). Αλλά, για να βρούμε την γραμμική πολυπλοκότητα του k-σφάλματος της ακολουθίας (s) όπως την ορίσαμε προηγουμένως, αυτό θα απαιτούσε εφαρμογές του βασικού αλγορίθμου που είναι απαγορευτικά υψηλές, ακόμη και για μέτρια μεγέθη των πεπερασμένων αριθμών n και k.

Υπάρχει ένας πολύ αποδοτικός αλγόριθμος για τον υπολογισμό της k-error γραμμικής πολυπλοκότητας, που λειτουργεί για την περίπτωση των δυαδικών ακολουθιών με περίοδο 2n . Αυτός ο νέος αλγόριθμος, αναπτύχθηκε από τους Stamp και Martin το 1993 και επεκτάθηκε από τους Lauder και Paterson το 2003. Ο αλγόριθμος των Stamp και Martin, στην περίπτωση που k = 0, ταυτίζεται με τον αλγόριθμο των Games-Chan. Σε κάθε περίπτωση, λόγω της ύπαρξης αυτών των αλγορίθμων, η γραμμική πολυπλοκότητα k σφαλμάτων έχει μελετηθεί σε σημαντικό βαθμό από την ερευνητική κοινότητα.

Η μη γραμμική πολυπλοκότητα k σφαλμάτων ορίζεται αναλόγως. Ωστόσο, αφενός δεν υπάρχει κάποιος αποδοτικός αλγόριθμος για την εύρεσή της και αφετέρου – κατ' αναλογία με το γεγονός ότι η μη γραμμική πολυπλοκότητα έχει μελετηθεί πολύ λιγότερο από ό,τι η γραμμική – δεν έχει μελετηθεί από την ερευνητική κοινότητα.

Κεφάλαιο 4
Η μη γραμμική πολυπλοκότητα στον RC4

Στο παρόν κεφάλαιο περιγράφεται η πειραματική διαδικασία που ακολουθήθηκε για τον υπολογισμό της μη γραμμικής πολυπλοκότητας, αλλά και της μη γραμμικής πολυπλοκότητας k σφαλμάτων, για την κλειδοροή που παράγει ο γνωστός αλγόριθμος RC4.

Πειραματική διαδικασία

Θα εξετάσουμε τη μη γραμμική πολυπλοκότητα ακολουθιών αξιολογώντας τα ακόλουθα:

1. Αν διασφαλίζεται ότι το nonlinear complexity είναι ικανοποιητικό.

Αν η μη γραμμική πολυπλοκότητα είναι χαμηλότερη από το θεωρητικό μέγιστο: το χαρακτηριστικό αυτό των ακολουθιών αποτελεί μία ευπάθεια της ακολουθίας. Η ευπάθεια μίας ψευδοτυχαίας ακολουθίας γεννά προβληματισμούς ως προς τα χαρακτηριστικά της τυχαιότητάς της.

2. Αν διασφαλίζεται ότι το k-error nonlinear complexity είναι ικανοποιητικό.

Αν η μη γραμμική πολυπλοκότητα k σφαλμάτων να είναι πολύ μικρότερη από την αρχική μη γραμμική πολυπλοκότητα, τότε θα λέγαμε ότι υπάρχει ομοιότητα της ακολουθίας με κάποια άλλη χαμηλής μη γραμμικής πολυπλοκότητας.

Όταν συμβαίνει αυτό μπορούμε να εικάσουμε την ομοιότητα της ψευδοτυχαίας ακολουθίας με κάποια διαφορετική από την αρχική, και υπαρχει ευπάθεια στην αλλαγή μερικών χαρακτήρων (ενός , δύο ή τριών δηλαδή 1-error,2-error ή 3-error αντίστοιχα).

Επίσης η ακολουθία «που μοιάζει» με την υπό εξέταση, προφανώς έχει χαμηλότερο nonlinear complexity, και είναι πιο εύκολη στην αποκρυπρογράφησή της, κάτι που προφανώς είναι ανησυχητικό και για την αρχική μας ακολουθία.

Ικανοποιητική μη γραμμικη πολυπλοκότητα k σφαλμάτων θεωρείται αυτό που παραμένει ίδια ή μειώνεται ελάχιστα από την αρχική τιμή της μη γραμμικής πολυπλοκότητας.

3. Αν διασφαλίζεται ότι οι ακολουθίες είναι συνολικά καλές στα πλαίσια της μη γραμμικής πολυπλοκότητας (ουσιαστικά συγκεντρωτικά αποτελέσματα)

Στη συνέχεια θα εξετάσουμε τα συγκεντρωτικά στοιχεία των αποτελεσμάτων για διάφορα μεγέθη κλειδοροής (128, 256 και 512 αντίστοιχα) βγάζοντας ξεχωριστά συμπεράσματα για τις διάφορες περιπτώσεις.

4.1 Διαδικασία κατασκευής δυαδικών ακολουθίων

Για να δημιουργήσουμε δυαδικές ακολουθίες κλειδιών και στη συνέχεια να εξετάσουμε τη μη γραμμική πολυπλοκότητα τους ακολουθήσαμε την εξής μεθοδολογία:

- Επιλέξαμε δέκα φράσεις στις οποίες η δυαδική τους αναπαράσταση έχει μέγεθος 128 bits, δέκα φράσεις στις οποίες η δυαδική τους αναπαράσταση έχει μέγεθος 256 bits και δέκα φράσεις στις οποίες η δυαδική τους αναπαράσταση έχει μέγεθος 512 bits (σύνολο 30 φράσεις της αγγλικής γλώσσας), τις οποιές τις αποθηκεύσαμε σε 30 διαφορετικά αρχεία txt.

- Για κάθε μία από τις φράσεις χρησιμοποήσαμε τον αλγόριθμο κρυπτογράφησης RC4, μέσω του λογισμικού Cryptool 1.4.41 (https://www.cryptool.org/en/). Η διαδικασία της κρυπτογράφησης απαιτεί να εισαχθεί ένα δεκαεξαδικό κλειδί της επιλογής του χρήστη (το κλειδί της κρυπτογράφησης). Το παραγώμενο αρχείο είναι το κρυπτογραφημένο μήνυμα σε δεκαεξαδική μορφή.

- Στη συνέχεια, χρησιμοποιήσαμε τον αλγόριθμο Verman/OTP πάλι μέσω του λογισμικού Cryptool στο κρυπτογραφημένο μήνυμα βάζοντας σαν κλειδί το αρχικό αποθηκευμένο μήνυμα σε txt. Το παραγώμενο αποτέλεσμα είναι η κλειδοροή του αλγόριθμου RC4 (για το δοθέν κλειδί που θέσαμε παραπάνω) σε δεκαεξαδική μορφή.

- Τέλος με κατάλληλες μετατροπές τα κλειδιά αυτά μετατράπηκαν σε δυαδικές ακολουθίες που αποτέλεσαν την βάση της πειραματικής μας διαδικασίας.

4.1.2 Αλγόριθμος υπολογισμού μη γραμμικής πολυπλοκότητας

Το ερευνητικό κομμάτι της εργασίας ήταν άρρηκτα συνυφασμένο με την δημιουργία ενός νέου αλγορίθμου που υπολογίζει τη μη γραμμική πολυπλοκότητα δυαδικών ακολουθίων. Η υλοποίηση έγινε στη γλώσσα προγραμματισμού C++ η οποία είναι πολύ καλή στον χειρισμό των strings, και ως τέτοια έπρεπε να αντιμετωπιστεί η κλειδοροή.

Στη συνέχεια αναπτύχθηκε και παραμετρική τεχνική για τον υπολογισμό του k-error και η δυαδικές ακολουθίες επανεξετάζονταν για την μη γραμμική τους πολυπλοκότητα k σφαλμάτων.

Στο σημείο αυτό πρέπει να επισημάνουμε πως για λόγους υπολογιστικής ισχύς δεν εξέτασαμε όλες τις πιθανές αλλαγές k θέσεων. Για παράδειγμα για n=512 και k=3, οι συνδυασμοί είναι 22.238.720 και είναι το αποτέλεσμα της πράξης (συνδυασμοί 512 ανά 3).

Αυτό σημαίνει ότι λόγω χρονικής πολυπλοκότητας, δεν έγινε εξαντλητική αναζήτηση – γεγονός το οποίο σημαίνει ότι ακόμα και αν δεν βρίσκουμε ομοιότητα, δεν σημαίνει ότι αποκλείεται να υπάρχει. Όταν βρίσκουμε βέβαια, είναι αδιαμφισβήτητη (και ίσως να υπάρχει και ακόμα μεγαλύτερη).

Η υλοποίηση του αλγορίθμου παρατίθεται στο παράρτημα της παρούσας διατριβής.

Στη συνέχεια περιγράφονται αναλυτικά τα αποτελέσματα των πειραμάτων. Τα αποτελέσματα που λάβαμε για κάθε ακολουθία τα περιγράφουμε με τον όρο «πειραματικά».

4.1.3 Οι ακολουθίες αναλυτικά

Ακολουθία 1

11101000001100011100000110011110111001000011100100111100110111001011
01100100100110010111000100011101100010001011010001111010001 0

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 14

Πειραματική μη Γραμμική Πολυπλοκότητα: 11

1-error Πειραματική μη Γραμμική Πολυπλοκότητα: 11

2-error Πειραματική μη Γραμμική Πολυπλοκότητα: 11

3-error Πειραματική μη Γραμμική Πολυπλοκότητα: 11

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 11 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 2

10010100100100111010011001001001101101001111100100001110000010010010
10100010001000010010111101101011011101000100011011110101110 0

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα : 7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα :12

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :12

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 12

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :12

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 12 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 3

00000111000000110101110000101101011001110111001001100111100110011110
11001001110110011000010101111110110011101100101111011101100

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 14

Πειραματική μη Γραμμική Πολυπλοκότητα :13

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 13

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :13

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 13

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Σχετική Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 13 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 4

10010110100101110111010000000111010011001101111010010001000101000000
00000001110001110110100100010001000010110010101110100001001 0

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα :17

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 17

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 13

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 12

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 17 δηλαδή σημαντικά υψηλότερη από τη μέγιστη θεωρητική 14)

ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας δεν είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 5

10011111000100110001111011010100001101000111101110101010111000000101
10010001000001100110001011000111011111010101011110010101110 1

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 14

Πειραματική μη Γραμμική Πολυπλοκότητα: 14

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :14

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 14 ίση με τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 6

11110000011100000000011001110011011011010000011000111110011111001010
01100011101000111111110111101110111011110111110000101111111111010

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα :11

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :11

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :11

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :11

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 11 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 7

11000111111111011101010100110001111111010001001110011100101010101101
10000100001011101111101101110111101101111011101010111010100 1

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα :15

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :15

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :15

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 15

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 15 με τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 8

11000000000000110111011010010111010010010111110111100101000111010010
00100110101000100010001010110101011110111011011001101110001 0

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα :12

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :12

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :12

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :12

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 12 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 9

10101110000000010110000000101111010101010011011011000110100110110011
01110101010111101111011101000011011101110110100110101010000 1

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα: 12

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 12

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 12

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 12

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 12 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 10

01000100100101100111011000100011010101110101110000101011001000011010
01100000100110111011111100011110010011110001101001010100010 0

Bits 128

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :7

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :14

Πειραματική μη Γραμμική Πολυπλοκότητα: 11

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :11

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :11

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 11

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 11 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 14)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 11

01101111101010011000001001001010110001010101111011011110100101010010
00100101110111101011001011111011000001000110000100001100010100101010
01100101000110101101011010110100010001100011000010001100011101000100
10100000011011101001010100110100001000101110001010 11

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :16

Πειραματική μη Γραμμική Πολυπλοκότητα :16

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 16

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 16

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :16

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 16 με τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 12

00011111111000011111010110011111010001110110110100011001100111101101
10110010011000010101101110111110100111001110100011101000101001110000
10110010011101000100111111001000010001010111111001101101110010111110
11100000010101001111010011000010111011010101010101010

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα :14

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 14

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 14

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 14

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 14 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 13

10110111001100010101000001001111011011110101100110101111001000111010
11010110001111110110000000010101100010110101111111011001111110101010
11110011111100001001011010010000010001111001010100000101001000010011
10011000110110001010001001101101011111101111101010 11

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα :15

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :15

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 15

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 15

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Σχετική Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 15 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 14

11010000110110001111101101100110111010000110000111101001110100110111
10001001000001011001100100010100100101100001101101100111011110011101
01000010001100010111001100100111101110000011111011100101110010101110
01100001101010101111100001011101110110100100011000 01

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα :13

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 13

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 13

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 13

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 13 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 15

11000111011101000011101100010101011101101001111011110010101001010010
11010111000001100111011111010100100101101110101000001100000111111111
00101001111101001000100110001111000000010101110101110011001111100100
01000011000011001001011101001101010011010010001111111

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :16

Πειραματική μη Γραμμική Πολυπλοκότητα: 12

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 12

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 12

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 12

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 12 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 16

00110111101000010101100000011001001000101101110111100001101001001011
01110010011011010000111000110100111110110111001001101101000011100011
01001111011111000100110111101001111000100011110000010001101111110101
10000101101110000101101101100110001111110110000111100101010101010100
10011101000111100110010 1

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα :41

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 25

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 25

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 25

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 41 δηλαδή σημαντικά υψηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (Αν και μειώνεται σημαντικά η μη γραμμική πολυπλοκότητα με εισαγωγή κατάλληλων σφαλμάτων, εξακολουθεί να έχει τιμή υψηλότερη της θεωρητικά αναμενόμενης).

Ακολουθία 17

1100000000110000010101010110010011100000111111000101110100010111111010010011000100100110011101111010011100111011111110110010110010111111101111001000110111111010010010000000101000000110110000110000100111110010100001011011101110011110111100000111011110010011 00

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα: 17

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :13

2 error Πειραματική μη Γραμμική Πολυπλοκότητα: 13

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :13

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 17 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 16)

ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας δεν είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 18

11010101100011100000111111001010010011001111011111011111111000000101
11100111000001110000011011001011100110001111101100011011100010000110
00001000101010101111100100111001111001111110101000110000001110111001
11111001101101001000011101111011011010111110111111111

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 16

Πειραματική μη Γραμμική Πολυπλοκότητα: 14

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 14

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 14 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 19

10010110100111010011011110011101011001010101110000101011010011000101
00111110001010011101111101101101110000101001101011110010001101000011
11001100111111110000010100010111001001010011010010111100001101111101
00000101011101110000000100010000111100000100110101011

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :16

Πειραματική μη Γραμμική Πολυπλοκότητα :15

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :14

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 14

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Σχετική Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 15 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 16)

Σχετική ύπαρξη ομοιότητας (η ακολουθία είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 20

00110011011111000001000000001111000111101111101100101000010010111110001000010010111111011111101101101110111011000010010101101011011010010001101110010110110001111001000010010101001111001000101000001011001101111100010110100101100000011101000000111111110010

Bits 256

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 8

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :16

Πειραματική μη Γραμμική Πολυπλοκότητα :17

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 17

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 17

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :17

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 17 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 16)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 21

00100111100000111001111000011010011101101010111000000000110110011010
01110001001100011011001111111010001101101110111001000010010011111100
00011111001100110000110110111000000101011011100111101101100010100100
01001100001101101010110101111101000110101011011101010101100101111001
00011011010100101000101100001101110011111011011001001011101111010010 0
01110001010111101000001110000100001001111111110111010000000001100110
10010011101100101111110100011000011001010000110000000011110101001100
01110000001111010110011011000101111 0

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα:22

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 22

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 22

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :21

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 22 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η ακολουθία είναι σταθερή σε μεταβολές μερικών χαρακτήρων – ελάχιστη μείωση παρατηρείται στη μη γραμμική πολυπλοκότητα 3 σφαλμάτων, αλλά και πάλι παραμένει υψηλότερη από την αναμενόμενη θεωρητική).

Ακολουθία 22

00111010111011101111101010001001011010000000011101100010000010100000
11010100100011010101010101100100111111110101011110001010000111110100
10100110000101010001101111110001010001110110100000110101010110001110
00010011011100100011101100110100010000010100011100001110011111010001
00111111100001101011111110111101110010000100001111110101010011011010
10000000100101010101110001001111110110111010011100100101001000110110
11110101101111111100011100000001111110010111101111000010001001110110
00010011110001111101011101111111010 0

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 18

Πειραματική μη Γραμμική Πολυπλοκότητα :17

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 17

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :17

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :17

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Σχετική ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 17 δηλαδή λίγο χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 23

00000001101000000100110100111011010111101110110111010100110001101111
11110111001010000110001000110000101101001001110110110101000011101111
10101111101110111110110111101001110000000101100010010100011110010011
11011101111111010110111001010110011111010000111011010101101111111010 0
01100000111111110011101111110111001100101000111111010011011110110011
01111000110101111000001100110100000011010111010110101111101010000101
01011100101101100000110101111000100010011100001010001011110100101001
11111011010000110000000111111111000001

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα: 18

Πειραματική μη Γραμμική Πολυπλοκότητα :16

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :16

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 16

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :16

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 16 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 24

01110100100101110110110101000110001001010110001101000010011011101001
10000000101110011110110011000001110000111011010001000100000000100001
10010111000110100000001001011110101111000110111100110001010100010011
11011111111001000001000110111110010111010001010000010000001001010101
11111101101101000011111111000001110011001011110111100010110010000110
11110011011100011010110111111011101010001010000000100011000110001010 0
01111010010011011101001011001011001000110000101010101111001000110011
01000111111111111111111011001000011 11

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :17

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :17

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 17

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 17

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Σχετική ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 17 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 25

0101101101111100110100110111101000000010001111000110000101110001111001011000001111001010001100100001001100111000111000001111000110010101100001000010001011011010010000000011011110101100101110011100110010101100110100000101101101001101110000010101011011111111001000111101111101000001111101000010111011100010010010101010000010100011100111000001010100101101011111011010011001100010110100001110100100010100101010101001001110001110010100001101111011001000100011011010110111001010110011100110010010001010110001111010011011

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :16

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 16

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :16

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 16

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 16 δηλαδή χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 26

10100000110101111101100000110000011100111101111010101100010001011010
10100110110010110010011000001100101001011110010110110000011100100101
00000011111101010010110001000100000001011011010000010110110111000101
00011100000111010100110100000110100111000110101011111011010111100110
11100100101011001111111101110100110100101100011011100001111101010001
11110001110000100100001111000010110011111101101110100001000100010101
11000110110110010100001110001110000111001110000111101011111001101000
01110100100010000101000010101011001O

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :15

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 15

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :15

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 15

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 15 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 27

1100001111001100001101100110110100000001110010001100000010111110111001001001000111000100000010101011001111010001000101000000000011011001001101110010011001110011101101001011100000011000100011111110101010011010100001101000101000000001101100001101110101101000011011001001000001111100100100100100100000111101111001010011110011010100110111110000110010101000000010011101011010000110011011000011100101110101010011000110000101000000111001001011001001110111100111010011001001011101010111110001001011010010110001000110101

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :19

1 error Πειραματική μη Γραμμική Πολυπλοκότητα : 19

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 19

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :19

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 19 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 28

00110110000110111001110110101100001010110110000101101011000111110010
01100000010100100100111111110011001000111100010100101111010010110101
11101011110110001001100101000011011001110100111010001110110111110000
10000001010111110100000010001001110001100110010000111001011110111100
11111111100001000011010001110110010100010000110110010001010000001111
00000101011000010000110100010011100011111001001111011100011011100101 0
10010010000110010101010000111010011011101000110010001101110110001100
10001111001101111110011100101100011 1

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα: 9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :20

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :20

2 error Πειραματική μη Γραμμική Πολυπλοκότητα :20

3 error Πειραματική μη Γραμμική Πολυπλοκότητα: 20

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 20 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 29

1000010101100100110111000100011000001100101001011110011100100111011100000010111000111011110000100010000101000101010100011010000111110000010001100000000111001011100001100001111100111101011001010010111011011000010001101100011110010111110111011010110100001010010010001010010101110010001010010101100100100001010000011000110100011111010011001110001011011110110011111100001001000011001001010010010101101000000110000111100010011010111001100000100100111001011100101011100000111110010001110111010100111100010000000101101000

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα :19

1 error Πειραματική μη Γραμμική Πολυπλοκότητα :19

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 19

3 error Πειραματική μη Γραμμική Πολυπλοκότητα :19

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Μη ύπαρξη ευπάθειας (η μη γραμμική πολυπλοκότητα είναι 19 δηλαδή υψηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

Ακολουθία 30

10010000101001110100101110100111011111001101111110110000000101011101
01011001101011101011111001010010110000100110011001010101111100101111
00110011101001010110101110100100001010000110001110111011100111001111
10100101101011000101010111100101000111001000010100010101100001000101
11010100110110110111001110001111011011011000111110000011110001000111
01000000111000111010110111010000100111101100111101110111011001010
00001110010110010000000100101110101110110100100010110011011001010001
11101000100011110001101001010100101 0

Bits 512

Θεωρητική Ελάχιστη μη Γραμμική Πολυπλοκότητα :9

Θεωρητική Μέγιστη μη Γραμμική Πολυπλοκότητα :18

Πειραματική μη Γραμμική Πολυπλοκότητα: 15

1 error Πειραματική μη Γραμμική Πολυπλοκότητα: 15

2 error Πειραματική μη Γραμμική Πολυπλοκότητα : 15

3 error Πειραματική μη Γραμμική Πολυπλοκότητα : 15

Συμπεράσματα μη Γραμμικής Πολυπλοκότητας ακολουθίας

Ευπάθεια (η μη γραμμική πολυπλοκότητα είναι 15 δηλαδή σημαντικά χαμηλότερη από τη μέγιστη θεωρητική 18)

Μη ύπαρξη ομοιότητας (η μη γραμμική πολυπλοκότητα της ακολουθίας είναι σταθερή σε μεταβολές μερικών χαρακτήρων)

4.1.4 Συγκεντρωτικά αποτελέσματα

Οι ακολουθίες, όπως είναι φανερό ανωτέρω αξιολογήθηκαν στα ακόλουθα:

1. Αν διασφαλίζεται ότι το nonlinear complexity είναι ικανοποιητικό.

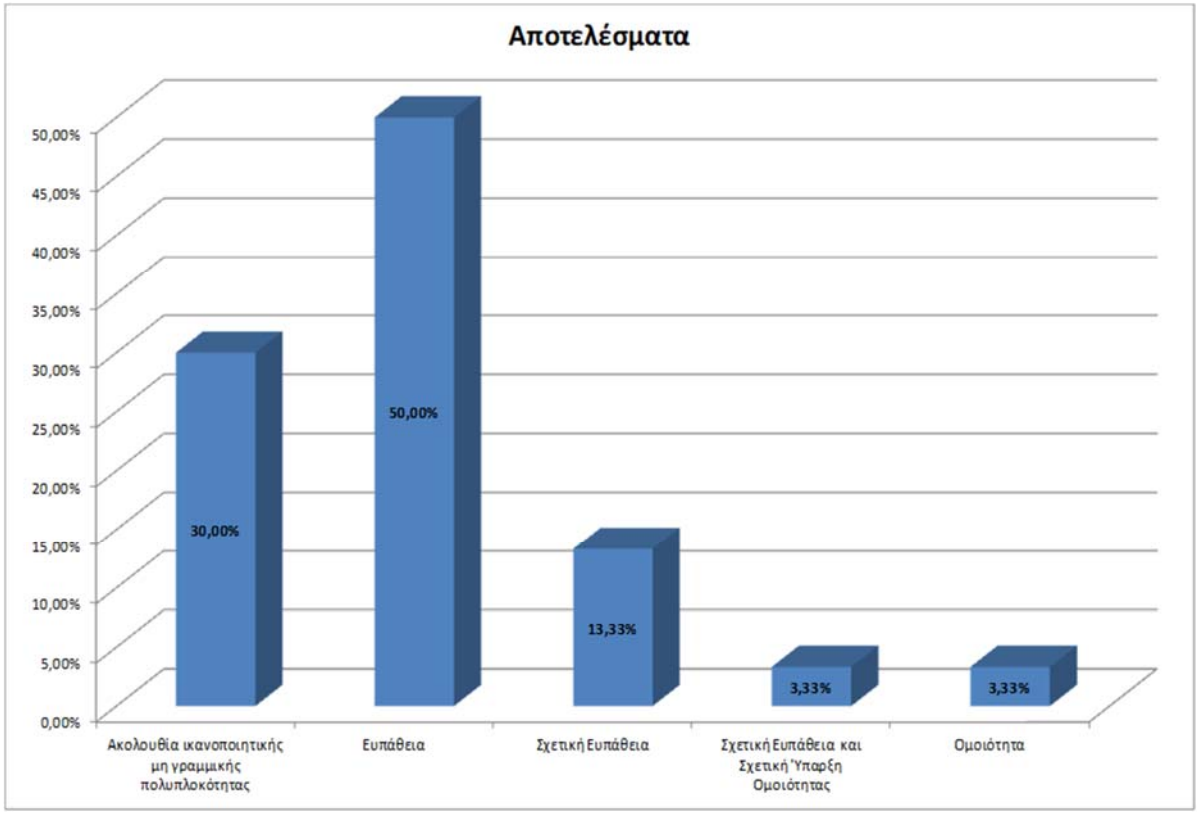
(μη ύπαρξη ευπάθειας)

2. Αν διασφαλίζεται ότι το k-error nonlinear complexity είναι ικανοποιητικό (Μη ύπαρξης ομοιότητας)

Στην ενότητα αυτή θα συνδυάσουμε αυτά τα δύο χαρακτηριστικά. Θεωρούμε ικανοποιητικές τις ακολουθίες που περνάνε με επιτυχία και τα δύο κριτήρια που έχουμε επιλέξει.

Ο πίνακας που ακολουθεί παρουσιάζει τα αποτελέσματα στο σύνολο των 30 ακολουθιών.

Χαρακτηρισμός	Αποτελέσματα	Πλήθος Ακολουθίων στην Κατηγορία
Ακολουθία ικανοποιητικής μη γραμμικής πολυπλοκότητας	30,00%	9
Ευπάθεια	50,00%	15
Σχετική Ευπάθεια	13,33%	4
Σχετική Ευπάθεια και Σχετική 'Υπαρξη Ομοιότητας	3,33%	1
Ομοιότητα	3,33%	1



Κεφάλαιο 5
Πρόλογος

Στη παρούσα εργασία εξετάσαμε τη μη γραμμική πολυπλοκότητα των δυαδικών ακολουθιών κλειδοροής που δημιουργούνται με τον αλγόριθμο RC4, οποίος χρησιμοποιείται μεταξύ των άλλων και στο ευρύτατα διαδεδομένο πρωτόκολλο επικοινωνίας TLS.

Τα αποτελέσματά μας επί κάποιων ενδεικτικών τυχαία επιλεγμένων ακολουθιών καταδεικνύουν πως μόνο το 30% των παραγόμενων ακολουθιών φτάνουν στο θεωρητικό μέγιστο της μη γραμμικής πολυπλοκότητας και έχουν ταυτόχρονα και ικανοποιητικό αποτέλεσμα ως προς τη μη γραμμική πολυπολοκότητα k σφαλμάτων.

Συμπερασματικά, αν και η παρούσα έρευνα εστίασε σε έναν μόνο κρυπταλγόριθμο και για σχετικά μικρά μεγέθη κλειδοροής, διαφαίνεται πως η μη γραμμική πολυπλοκότητα είναι ένα κριτήριο που πρέπει να εξετάζεται εξίσου με την γραμμική πολυπλοκότητα, και κατά συνέπεια οι σύγχρονοι κρυπταλγόριθμοι ροής (όπως ο Chacha-20 ο οποίος φαίνεται πως θα αντικασταστήσει τον RC4 στο πρωτόκολλο εεπικοινωνίας TLS) οφείλουν να είναι επαρκείς και σε αυτά τα χαρακτηριστικά. Το ίδιο ισχύει και για τη μη γραμμική πολυπλοκότητα k σφαλμάτων, η οποία δεν έχει μελετηθεί μέχρι σήμερα.

5.1 Μελλοντική έρευνα

Η παρούσα εργασία πιστεύουμε πως συνέλαβε στον επιστημονικό διάλογο για την ασφάλεια της κρυπτογράφησης εξετάζοντας με έναν αλγόριθμο που αναπτύχθηκε την μη γραμμικη πολυπλοκότητα αλλά και – για πρώτη φορά – τη μη γραμμική πολυπλοκότητα k σφαλμάτων σε έναν γνωστό κρυπταλγόριθμο ροής. Προφανώς, αντίστοιχη μελέτη πρέπει να γίνει σε ευρύτερο πλαίσιο, σε περισσότερες ακολουθίες κλειδοροής, μεγαλύτερων μεγεθών αλλά και για άλλους κρυπταλγορίθμους.

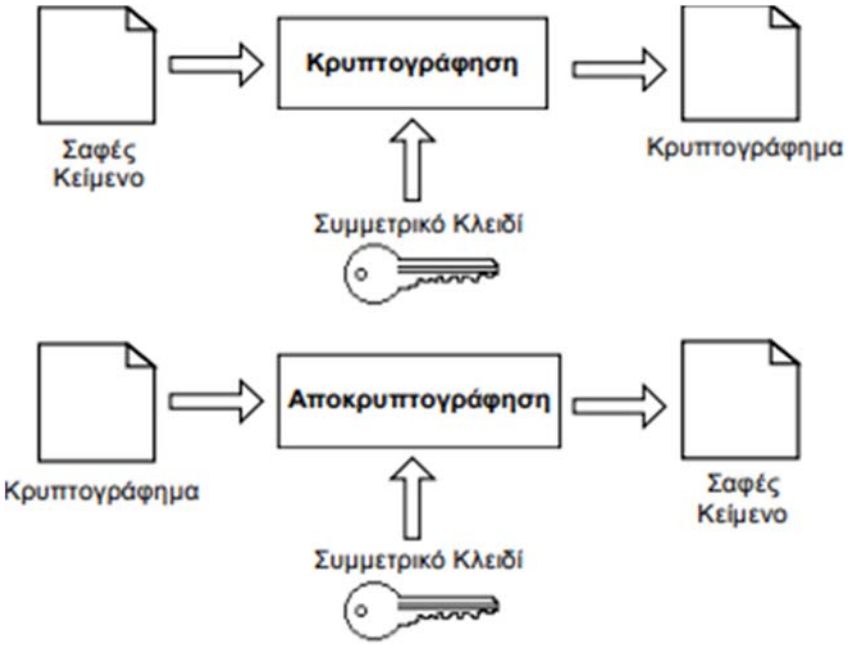
Οι μελλοντικές έρευνες θα πρέπει να λαμβάνουν υπόψη ότι στην αποτίμηση της ασφάλειας ακολουθιών θα πρέπει να εξετάζεται τόσο το nonlinear complexity όσο και το 1-error nonlinear complexity, οπότε πέρα από την προτεινόμενη μεθοδολογία, και θα πρέπει να διερευνηθούν και εναλλακτικές τεχνικές για τον αποδοτικό υπολογισμό τους.

5.2 Διαγράμματα-Σχήματα

Κεφάλαιο 1
Παράγραφος 1.1 Ορισμός κρυπτογραφίας

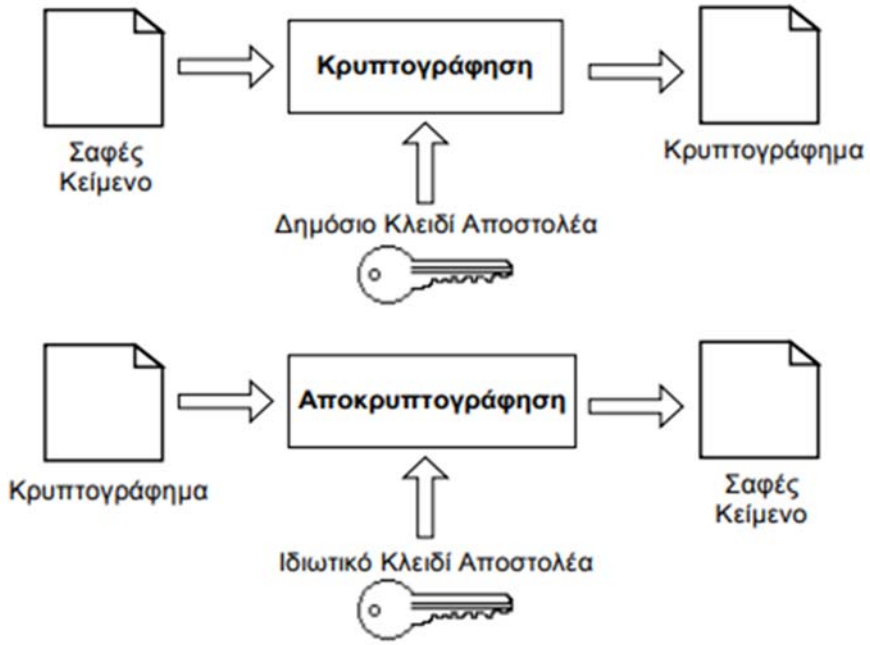
Εικόνα 1. Κρυπτογράφηση απλού κειμένου

Παράγραφος 1.1.1 Συμμετρική κρυπτογραφία



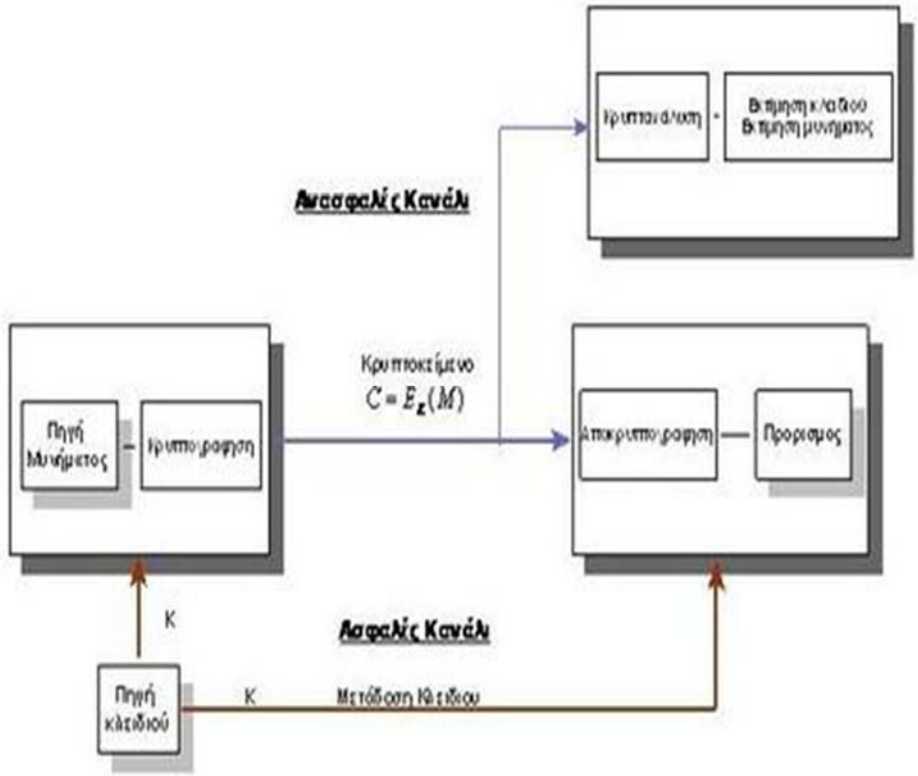
Εικόνα 2. Διάγραμμα ροής της συμμετρικής κρυπτογραφίας

Παράγραφος 1.1.2 Ασύμμετρη κρυπτογραφία



Εικόνα 3. Μέθοδος Κρυπτογράφησης Ασύμμετρου κλειδιού

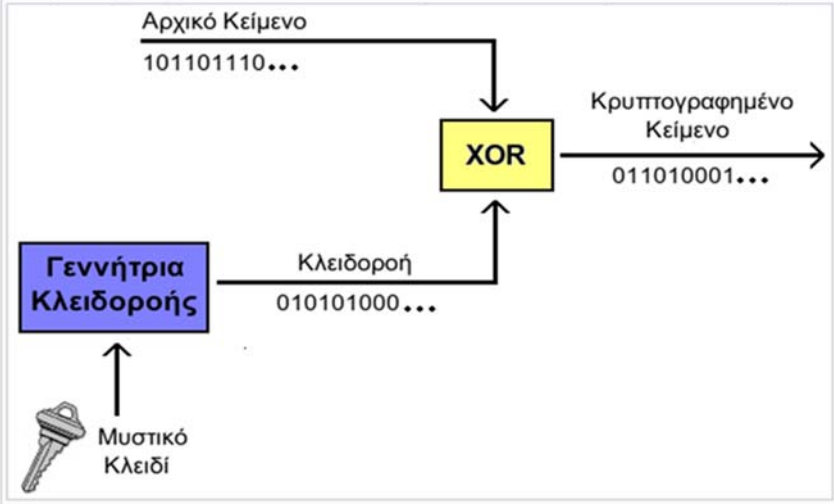
Παράγραφος 1.1.4 Κύριες έννοιες – σημασία των ακολουθιών στην κρυπτογράφηση



Εικόνα 4. Σύνηθες σύστημα κρυπτοσυστήματος

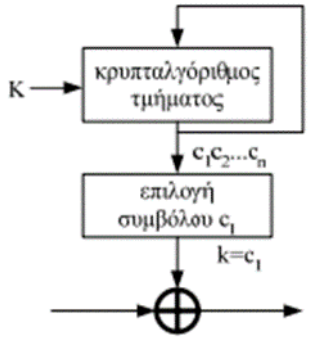
Κεφάλαιο 2

Παράγραφος 2.1 Λειτουργία των κρυπταλγορίθμων ροής



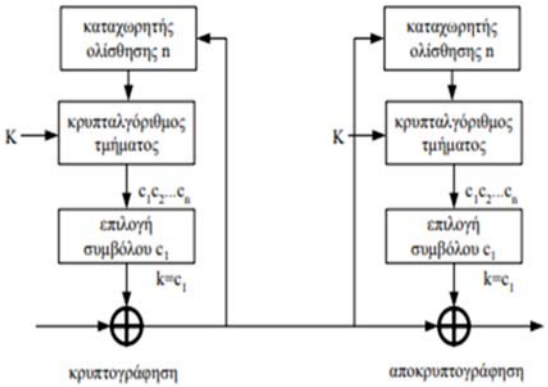
Εικόνα 5. Κρυπτογράφηση δεδομένων

Παράγραφος 2.1.2 Δημιουργία κρυπταλγόριθμου ροής από κρυπταλγόριθμο τμήματος



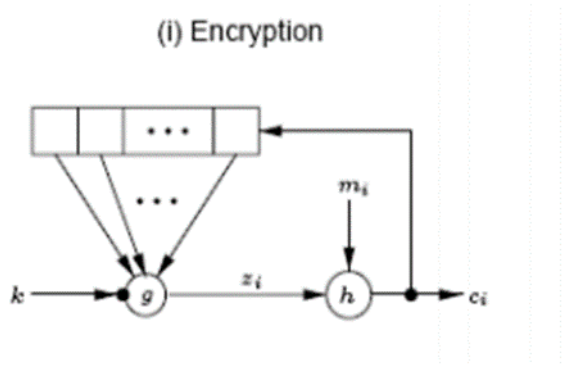
Εικόνα 6. Δημιουργία κρυπταλγόριθμου ροής από κρυπταλγόριθμο τμήματος

Παράγραφος 2.1.3 Δημιουργία αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής

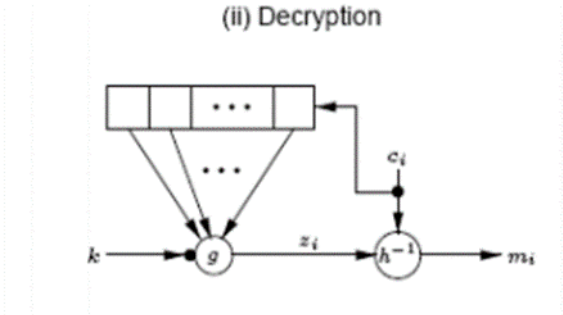


Εικόνα 7.Δημιουργία αυτοσυγχρονιζόμενου κρυπταλγόριθμου ροής

Παράγραφος 2.1.6 Οι σύγχρονοι stream ciphers

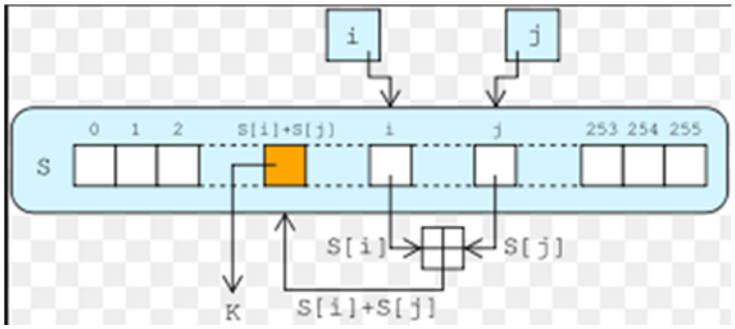


Εικόνα 8. Κρυπτογράφηση σύγχρονου stream cipher



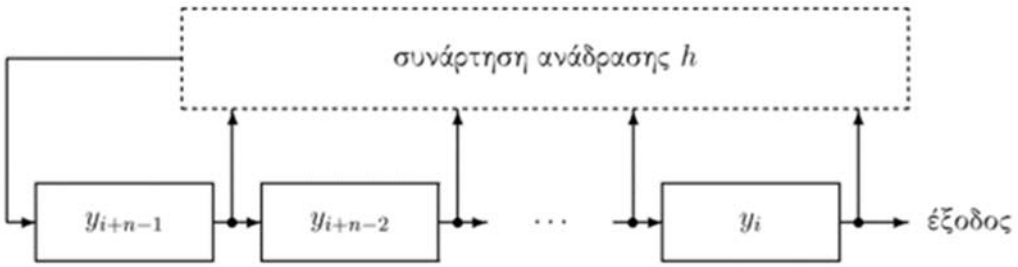
Εικόνα 9. Αποκρυπτογράφηση σύγχρονου stream cipher

Παράγραφος 2.1.11 Περιγραφή του RC4 αλγόριθμου ροής



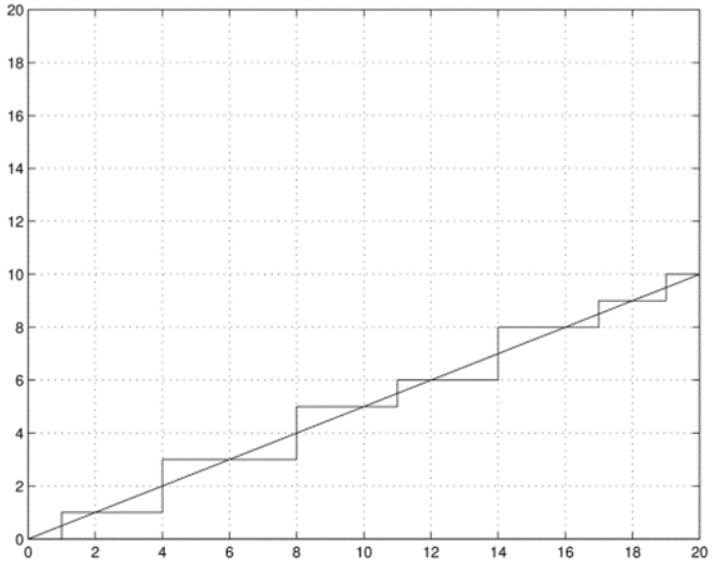
Εικόνα 10. Στάδια λειτουργίας RC4

Παράγραφος 2.1.12 Καταχωρητές ολίσθησης με ανάδραση (FSR)



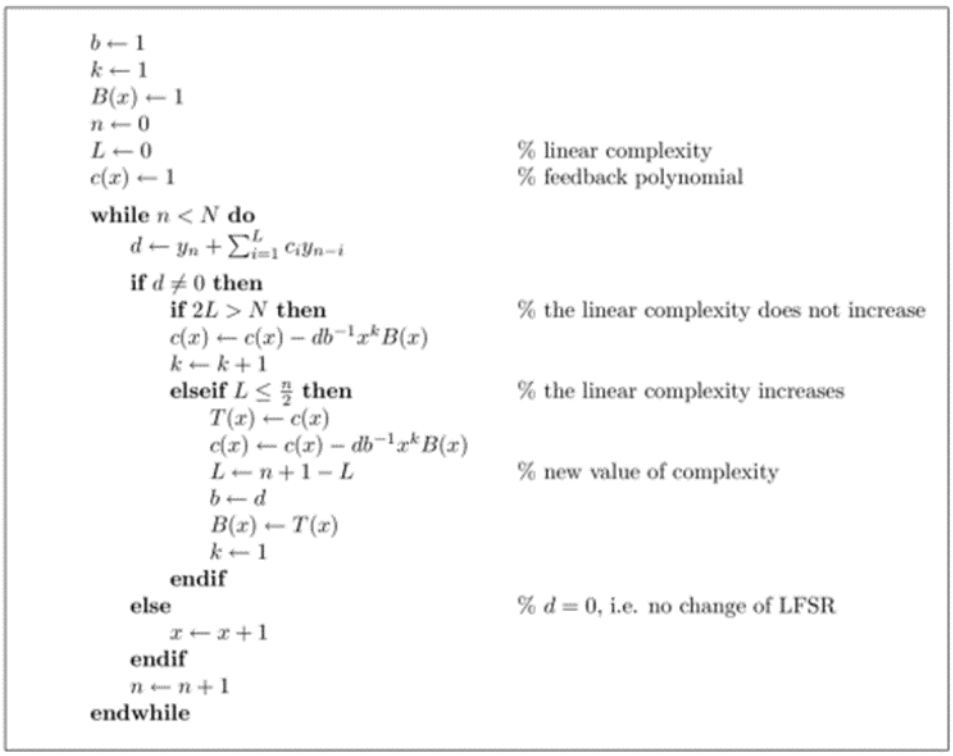
Εικόνα 11. Συνάρτηση ανάδρασης h

Κεφάλαιο 3
Παράγραφος 3.1.1 Γραμμική πολυπλοκότητα



Εικόνα 12. Προφίλ γραμμικής πολυπλοκότητας της ακολουθίας y20 = 10010011110001001110

Παράγραφος 3.1.2 Αλγόριθμος Berlekamp-Massey (BMA)



$b \leftarrow 1$
$k \leftarrow 1$
$B(x) \leftarrow 1$
$n \leftarrow 0$
$L \leftarrow 0$ % linear complexity
$c(x) \leftarrow 1$ % feedback polynomial
while $n < N$ **do**
  $d \leftarrow y_n + \sum_{i=1}^{L} c_i y_{n-i}$
  if $d \neq 0$ **then**
    if $2L > N$ **then** % the linear complexity does not increase
    $c(x) \leftarrow c(x) - db^{-1}x^k B(x)$
    $k \leftarrow k + 1$
    elseif $L \leq \frac{n}{2}$ **then** % the linear complexity increases
      $T(x) \leftarrow c(x)$
      $c(x) \leftarrow c(x) - db^{-1}x^k B(x)$
      $L \leftarrow n + 1 - L$ % new value of complexity
      $b \leftarrow d$
      $B(x) \leftarrow T(x)$
      $k \leftarrow 1$
    endif
  else % $d = 0$, i.e. no change of LFSR
    $x \leftarrow x + 1$
  endif
  $n \leftarrow n + 1$
endwhile

Εικόνα 13. Ο αλγόριθμος Berlekamp-Massey

Παράρτημα Α
Κώδικας k-error

Α.1 Κώδικας 1

```
#include "Helper.h"
#include <iostream>
#include <string>
#include <sstream>

using namespace std;

int main(int argc, char* argv[]) {

  //elenxw an o xristis mou exei dwsei parametrous
```

```
  if (argc < 2) {
    cout << "Prepei na eisagetai swsta tis parametrous." << endl;
    return 1;
  }

  cout << "Calculating..." << endl;

  string inputFile=Helper::getValue("-f","", argc, argv);
  string outputFile=Helper::getValue("-o","", argc, argv);
  int kError=Helper::getIntValue("-k",1, argc, argv);
  vector<string> akolouthies=Helper::readInputFile(inputFile);

  ofstream oFile(outputFile);
  if(!akolouthies.empty() && oFile.is_open()){
    for(auto ak : akolouthies) {
      int initComplexity=Helper::calculateComplexity(ak);
      oFile << "Initial complexity: " << initComplexity << " => ";

      string copyOfAk = ak;
      unordered_set<int> randomPicks = Helper::pickSet(ak.length()-1, kError);

      for (const auto& elem: randomPicks) {
        if(copyOfAk[elem] == '0')
          copyOfAk[elem] = '1';
        else
          copyOfAk[elem] = '0';
      }

      int kErrorComplexity=Helper::calculateComplexity(copyOfAk);
      oFile << "After altering "<< kError << " bits complexity: " << kErrorComplexity <<
"\r\n";
    }
    oFile.close();
  }
```

```
    cout << "Calculation ended" << endl;
    cout << "Exiting..." << endl;
    return 0;
}
```

Παράρτημα Β

Τελικός κώδικας

Β.1 Κώδικας 2

```
/*
 * Helper.h

 */

#ifndef HELPER_H_
#define HELPER_H_
#include <string>
#include <regex>
#include <fstream>
#include <vector>
#include <string>
#include <unordered_set>
#include <random>
using namespace std;

class Helper {
public:
   Helper(){}
   ~Helper(){}

   static vector<string> readInputFile(string file){
      vector<string> akolouthies;
      ifstream inputFile(file);

      if (inputFile.is_open()) {
```

```
        string line;
        while (getline(inputFile, line)) {

            if (!line.empty() && line[line.size() - 1] == '\r')
                line.erase(line.size() - 1);

            akolouthies.push_back(line);
        }
        inputFile.close();
    }
    return akolouthies;
}

static string getValue(string option,string defaultValue,int argc, char** argv){
    int index = -1;
    string value,argi;

    for (int i = 1; i < argc; i += 2) {
        argi = argv[i];
        if (argi.compare(option) == 0){
            index = i;
        }
    }

    if(index >= 0){
        value = argv[index + 1];
    }
    else{
        value = defaultValue;
    }

    return value;
}
```

```
   static int getIntValue(string option,int defaultValue,int argc, char** argv){
      string defValStr = to_string(defaultValue);
      string value = getValue(option, defValStr, argc, argv);
      int integerValue;

      if(isNumber(value)){
         integerValue=stoi(value);
      }
      else{
         //display message,get default
         integerValue=defaultValue;
      }
      return integerValue;
   }

   static bool isNumber(string token )
   {
      return regex_match( token, std::regex( ( "((\\+|-)?[[:digit:]]+)(\\.(([[:digit:]]+)?))?" )
) );
   }

   static int calculateComplexity(string source){
      int pos2check=0;//i 8esi pou exetazw ka8e fora
      int complexity=-1;

      string subSeq="";//ypakolou8ia
      bool notZeroSeq=false;

      //1st step
      size_t position = source.find_first_of("1");

      if(position<source.length()){
         //an mpei sto if simainei oti i akolou8ia DEN apoteleitai mono apo midenika
         notZeroSeq=true;
```

```
        complexity=position; //to arxiko complexity
        subSeq=source.substr (0,position+1); //i arxiki ypakolou8ia
        pos2check=position+1; // i arxiki 8esi pou exetazw einai i epomeni apo to 1o 1 pou vrika
    }

    if(notZeroSeq){
      //elengw an den exw ftasei sto telos tis akolou8ias
      while(pos2check<source.length()) {
        //to mustCheck xekinaei apo true se ka8e epanalipsi k ginetai false otan exw teleiwsei me to trexwn bit kai 8elw na paw sto epomeno
        bool mustCheck=true;
        while(mustCheck){
          string beforeLastNBits=subSeq.substr(0,subSeq.length() - complexity); //ta bits tis ypoakolou8ias prin apo ta n (oso einai to complexity) bits
          string lastNBits=subSeq.substr(subSeq.length() - complexity); //ta teleutaia n (oso einai to complexity) bits tis ypoakolou8ias

          //afairw apo tin ypoakolou8ia to teleutaio bit wste na psaxw se auti gia ta teleutaia n (oso einai to complexity) bits
          //to kanw auto gia na min mou vrei oti periexontai kai ta teleutaia n bits
          string toSearch=subSeq.substr(0,subSeq.length() - 1);

          //an exoun emfanistei nwritera
          if (toSearch.find(lastNBits) != string::npos) {
            char nextBit=source.at(pos2check);//pairnw to bit sti 8esi pou exetazw
            int indexOfLastNBits = beforeLastNBits.find(lastNBits);
            char nextBitOfFirstOccurence=source.at(indexOfLastNBits+lastNBits.length());//to epomeno bits apo tin 1h emfanisi sti ypoakolou8ia

            //an einai diaforetika
            if (nextBit!=nextBitOfFirstOccurence){
              //auxanetai to complexity
```

```
                complexity++;
            }
            else{
                //den auxanetai to complexity
                //pros8etw ton trexwn xaraktira pou vrisketai sti 8esi pos2check sto subsequence
                //k kanontas to mustCheck false proxwraw sto epomeno bit
                mustCheck=false;
                subSeq += source.at(pos2check);
                pos2check++;
            }
          }
          else{
            //pros8etw ton trexwn xaraktira pou vrisketai sti 8esi pos2check sto subsequence
            //k kanontas to mustCheck false proxwraw sto epomeno bit
            mustCheck=false;
            subSeq += source.at(pos2check);
            pos2check++;
          }
        }
      }
      return complexity;

    }
    else{
      return 0;
    }
  }

  static unordered_set<int> pickSet(int N, int k)
  {
    mt19937 gen(time(0));
    std::unordered_set<int> elems;
```

```
    for (int r = N - k; r < N; ++r) {
      int v = uniform_int_distribution<>(1, r)(gen);

      if (!elems.insert(v).second) {
        elems.insert(r);
      }
    }
    return elems;
  }
};

#endif /* HELPER_H_ */
```

Βιβλιογραφία

1. Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 452-473). Springer, Berlin, Heidelberg.
2. A. Blumer, J. Blumer, A. Ehrenfeucht, D. Haussler and R. McConnell. (1983) Linear Size Finite Automata for the Set of all Subwords of a Word: An Outline of Results, Bul. Eur. Assoc. Theor. Comp. Sci., no. 21, pp. 12–20, 1983.
3. A. G. Konheim. (1981) Cryptography, John Wiley & Sons, Inc., New York,
4. A. Lempel and J. Ziv. (1978) On the Complexity of Finite Sequences, IEEE Trans. on Info. Theory, vol. IT-22, no. 1, pp. 75–81, January 1976. F. J. MacWilliams and N. J. A. Sloane. The Theory of Error Correcting Codes, Amsterdam, North-Holland,
5. Berry Schoenmakers, 1999. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In In CRYPTO, pages 148–164. Springer-Verlag
6. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (Eds.). (2005). Handbook of elliptic and hyperelliptic curve cryptography. CRC press.
7. C. J. A. Jansen. (1989) Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods, PhD. Thesis, Technical University of Delft, Delft
8. C. H. Meyer and S. M. Matyas. (1982) Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, New York
9. Claude E. Shannon. (1949) Communication theory of secrecy systems. Bell System Technical Journal, 28(4):656–715
10. D. W. Davies and W. L. Price. (1984) Security for Computer Networks, John Wiley & Sons, Inc., Chichester, 1984.
11. Goldreich, O. (2009). Foundations of cryptography: volume 2, basic applications. Cambridge university press.
12. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004, August). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In International

workshop on cryptographic hardware and embedded systems (pp. 119-132). Springer, Berlin, Heidelberg.

13. Golomb, S. W., & Gong, G. (2005). Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press.
14. Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). Guide to elliptic curve cryptography. Springer Science & Business Media.
15. H. Fredricksen. (1982) A survey of full-length nonlinear shift register cycle algorithms, SIAM Rev., vol. 24, pp. 195–221, April 1982.
16. Jansen C.J.A., Boekee D.E. (1989) The Shortest Feedback Shift Register That Can Generate A Given Sequence. In: Brassard G. (eds) Advances in Cryptology — CRYPTO' 89 Proceedings.. Lecture Notes in Computer Science, vol 435. Springer, New York, NY
17. J. L. Massey. (1969) Shift-Register Synthesis and BCH Decoding, IEEE Trans. on Info. Theory, vol. IT-15
18. Liu, A., & Ning, P. (2008, April). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of the 7th international conference on Information processing in sensor networks (pp. 245-256). IEEE Computer Society.
19. Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Springer, Berlin, Heidelberg.
20. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 34.
21. R. Arratia, L. Gordon and M. S. Waterman. (1986) An Extreme Value Theory for Sequence Matching, The Annals of Statistics, vol. 14, no. 3, pp. 971–993, 1986.
22. R. A. Rueppel. (1984) New Approaches to Stream Ciphers, PhD. Thesis, Swiss Federal Institute of Technology, Zurich,
23. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, Advances in Cryptology — CRYPTO '98, volume 1462 of Lecture Notes in Computer Science, pages 13–25. Springer Berlin Heidelberg, 1998.
24. R. Lidl and H. Niederreiter. Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge, 1986.

25. Stallings, W. (2017). Cryptography and network security: principles and practice (p. 743). Upper Saddle River, NJ: Pearson.
26. Stinson, D. R. (2005). Cryptography: theory and practice. CRC press.
27. S. W. Golomb. (1967) Shift Register Sequences, Holden-Day Inc., San Francisco
28. S. Karlin, G. Ghandour, F. Ost, S. Tavare and L. J. Korn. (1983) New Approaches for Computer Analysis of Nucleic Acid Sequences, Proc. Natl. Acad. Sci. USA, vol. 80, pp. 5660–5664,
29. Takayasu et al, 1998, An Algorithm for the k-Error Linear Complexity of Sequences over GF(pm) with Period pn, p a Prime
30. Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005, March). Energy analysis of public-key cryptography for wireless sensor networks. In Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on (pp. 324-328). IEEE.