Κεφάλαιο 6

Κρυπταλγόριθμοι Ροής

Πίνακας Περιεχομένων

6.1 Εισαγωγή

Οι *κρυπταλγόριθμοι ροής* αποτελούν μια σημαντική κλάση αλγορίθμων κρυπτογράφησης. Κρυπτογραφούν μεμονωμένους χαρακτήρες (συνήθως δυαδικά ψηφία) ενός μηνύματος απλού κειμένου, έναν τη φορά, χρησιμοποιώντας έναν μετασχηματισμό κρυπτογράφησης ο οποίος μεταβάλλεται με τον χρόνο. Αντίθετα, οι *κρυπταλγόριθμοι τμήματος* (Κεφάλαιο 7) έχουν την τάση να κρυπτογραφούν συγχρόνως ομάδες χαρακτήρων ενός μηνύματος απλού κειμένου χρησιμοποιώντας έναν συγκεκριμένο μηχανισμό κρυπτογράφησης. Οι κρυπταλγόριθμοι ροής γενικά είναι ταχύτεροι από τους κρυπταλγόριθμους τμήματος σε επίπεδο υλικού και έχουν λιγότερο πολύπλοκη διάταξη κυκλωμάτων. Είναι επίσης περισσότερο κατάλληλοι, και σε ορισμένες περιπτώσεις επιβάλλεται η χρήση τους (π.χ. σε μερικές εφαρμογές τηλεπικοινωνιών), όταν η προσωρινή μνήμη είναι περιορισμένη ή όταν πρέπει οι χαρακτήρες να τύχουν επεξεργασίας μεμονωμένα καθώς παραλαμβάνονται. Επειδή έχουν περιορισμένο ή και μηδενικό αριθμό σφαλμάτων μεταβίβασης, οι κρυπταλγόριθμοι ροής μπορεί επίσης να πλεονεκτούν σε καταστάσεις όπου είναι πολύ πιθανό να συμβούν σφάλματα μεταβίβασης.

Υπάρχει ένα τεράστιο υλικό θεωρητικής γνώσης πάνω στους κρυπταλγόριθμους ροής και έχουν προταθεί και αναλυθεί εκτενώς διάφορες αρχές σχεδίασης. Όμως, υπάρχουν σχετικά λίγοι πλήρως καθορισμένοι αλγόριθμοι κρυπταλγορίθμων ροής στη δημόσια βιβλιογραφία. Αυτή η ατυχής κατάσταση πραγμάτων μπορεί να εξηγηθεί μερικώς από το γεγονός ότι οι περισσότεροι κρυπταλγόριθμοι ροής που χρησιμοποιούνται στην πράξη έχουν την τάση να είναι ιδιωτικοί και εμπιστευτικοί. Αντίθετα, έχουν δημοσιευθεί αρκετές απτές προτάσεις κρυπταλγορίθμων τμήματος, μερικές από τις οποίες έχουν προτυποποιηθεί ή έχουν δημοσιοποιηθεί. Μολαταύτα, εξαιτίας των σημαντικών πλεονεκτημάτων τους, οι κρυπταλγόριθμοι ροής χρησιμοποιούνται σήμερα ευρέως και μπορούμε να αναμένουμε ολοένα αυξανόμενες απτές προτάσεις τα προσεχή χρόνια.

Περίγραμμα Κεφαλαίου

Στο υπόλοιπο τμήμα της §6.1 παρουσιάζουμε βασικές έννοιες που είναι σχετικές με τους κρυπταλγόριθμους ροής. Οι καταχωρητές ολίσθησης με ανάδραση, ειδικότερα οι καταχωρητές ολίσθησης με γραμμική ανάδραση (LFSR), είναι οι βασικοί δομικοί λίθοι των περισσοτέρων κρυπταλγόριθμων ροής που έχουν προταθεί· τους μελετάμε στην §6.2. Στην §6.3 παρουσιάζουμε τρεις γενικές τεχνικές για την αξιοποίηση των LFSR στην κατασκευή των κρυπταλγόριθμων ροής: τη χρήση μιας μη γραμμικής συνδυάζουσας (combining) συνάρτησης στις εξόδους μερικών LFSR (§6.3.1), τη χρήση μιας μη γραμμικής διηθίζουσας (filtering) συνάρτησης στα περιεχόμενα ενός μεμονωμένου LFSR (§6.3.2), και τη χρήση ενός (ή περισσοτέρων) LFSR για τη ρύθμιση του ρολογιού ενός άλλου (ή περισσοτέρων) LFSR (§6.3.3). Στην §6.3.3 παρουσιάζουμε δύο συγκεκριμένες προτάσεις για γεννήτριες ρυθμιζόμενες με ρολόι (χρονο-ρυθμιζόμενες), τη γεννήτρια εναλλασσόμενου βήματος και τη γεννήτρια συρρίκνωσης. Στην §6.4 παρουσιάζουμε έναν κρυπταλγόριθμο ροής ο οποίος δεν βασίζεται σε LFSR, συγκεκριμένα τον SEAL. Ολοκληρώνουμε στην §6.5 με αναφορές και περαιτέρω σημειώσεις κεφαλαίου.

6.1.1 Ταξινόμηση

Οι κρυπταλγόριθμοι ροής μπορεί να είναι συμμετρικού κλειδιού ή δημόσιου κλειδιού. Στο κεφάλαιο αυτό επικεντρώνουμε στους κρυπταλγόριθμους ροής συμμετρικού κλειδιού· το πιθανοκρατικό σχήμα κρυπτογράφησης δημόσιου κλειδιού Blum-Goldwasser (§8.7.2) είναι ένα παράδειγμα κρυπταλγόριθμου ροής δημόσιου κλειδιού.

6.1 Σημείωση (*κρυπταλγόριθμοι τμήματος και κρυπταλγόριθμοι ροής*) Οι κρυπταλγόριθμοι τμήματος επεξεργάζονται απλό κείμενο σε σχετικά μεγάλα τμήματα (π.χ. $n \geq 64$ bits). Η ίδια συνάρτηση χρησιμοποιείται για την κρυπτογράφηση διαδοχικών τμημάτων· έτσι, οι (αμιγείς) κρυπταλγόριθμοι τμήματος είναι *άνευ μνήμης* (memoryless). Αντίθετα, οι κρυπταλγόριθμοι ροής επεξεργάζονται το απλό κείμενο σε τμήματα τόσο μικρά όσο ένα μεμονωμένο bit και η συνάρτηση κρυπτογράφησης μπορεί να μεταβάλλεται καθώς υπόκειται σε επεξεργασία το απλό κείμενο· έτσι οι κρυπταλγόριθμοι ροής λέμε ότι έχουν μνήμη. Μερικές φορές λέγονται *κρυπταλγόριθμοι κατάστασης* επειδή η κρυπτογράφηση εξαρτάται όχι μόνο από το κλειδί και το απλό κείμενο, αλλά επίσης και από την τρέχουσα κατάσταση. Η διάκριση αυτή μεταξύ των κρυπταλγόριθμων τμήματος και ροής δεν είναι τελεσίδικη (βλ. Παρατήρηση 7.25)· η προσθήκη μιας μικρής ποσότητας μνήμης σε έναν κρυπταλγόριθμο τμήματος (όπως στον τρόπο CBC) έχει ως αποτέλεσμα έναν κρυπταλγόριθμο ροής με μεγάλα τμήματα.

(i) Το σημειωματάριο μιας χρήσης

Υπενθυμίζουμε (Ορισμός 1.39) ότι ο *κρυπταλγόριθμος Vernam* επί του δυαδικού αλφάβητου ορίζεται από την

$$c_i = m_i \oplus k_i, \text{ για } i = 1, 2, 3, ...$$

όπου $m_1, m_2, m_3, \ldots$ είναι τα ψηφία απλού κειμένου, $k_1, k_2, k_3, \ldots$ (η *κλειδορροή*) είναι τα ψηφία κλειδιού, $c_1, c_2, c_3, \ldots$ είναι τα ψηφία κρυπτοκειμένου, και $\oplus$ είναι η συνάρτηση XOR (πρόσθεση ανά bit modulo 2). Η αποκρυπτογράφηση ορίζεται από την $m_i = c_i \oplus k_i$. Αν τα ψηφία της κλειδορροής παράγονται ανεξάρτητα και τυχαία, ο κρυπταλγόριθμος Vernam λέγεται *σημειωματάριο μιας χρήσης* και είναι άνευ όρων ασφαλής (§1.13.3(i)) έναντι μιας επίθεσης κρυπτοκειμένου. Ακριβέστερα, αν M, C και K είναι τυχαίες μεταβλητές που συμβολί-

ζουν το απλό κείμενο, το κρυπτοκείμενο και το μυστικό κλειδί, αντίστοιχα, και αν $H()$ συμβολίζει τη συνάρτηση εντροπίας (Ορισμός 2.39) τότε είναι $H(M|C) = H(M)$. Ισοδύναμα, $I(M; C) = 0$ (βλ. Ορισμός 2.45): το κρυπτοκείμενο δεν συνεισφέρει καμία πληροφορία για το απλό κείμενο.

Ο Shannon απέδειξε ότι μία αναγκαία συνθήκη για να είναι μια κρυπτογράφηση συμμετρικού κλειδιού άνευ όρων ασφαλής, είναι η $H(K) \geq H(M)$. Δηλαδή, η αβεβαιότητα του μυστικού κλειδιού πρέπει να είναι τουλάχιστον τόσο μεγάλη όσο η αβεβαιότητα απλού κειμένου. Αν το κλειδί έχει δυαδικό μήκος k και τα bit κλειδιού επιλέγονται τυχαία και ανεξάρτητα, τότε $H(K) = k$, και η αναγκαία συνθήκη του Shannon για την άνευ όρων ασφάλεια γίνεται $k \geq H(M)$. Το σημειωματάριο μιας χρήσης είναι άνευ όρων ασφαλές ανεξάρτητα από τη στατιστική κατανομή του απλού κειμένου, και είναι βέλτιστο με την έννοια ότι το κλειδί του είναι το μικρότερο δυνατό μεταξύ όλων των σχημάτων κρυπτογράφησης που έχουν την ιδιότητα αυτή.

Ένα προφανές μειονέκτημα του σημειωματάριου μιας χρήσης είναι ότι το κλειδί θα πρέπει να είναι τόσο μεγάλο όσο το απλό κείμενο, κάτι που αυξάνει τη δυσκολία της διανομής κλειδιών και τη διαχείριση κλειδιών. Αυτό λειτουργεί σαν κίνητρο για τη σχεδίαση κρυπταλγόριθμων ροής όταν η κλειδορροή παράγεται *ψευδοτυχαία* από ένα μικρότερο μυστικό κλειδί, με την πρόθεση ότι η κλειδορροή εμφανίζεται τυχαία σε έναν αντίπαλο ο οποίος έχει υπολογιστικούς περιορισμούς. Τέτοιοι κρυπταλγόριθμοι ροής δεν προσφέρουν άνευ όρων ασφάλεια (αφού $H(K) << H(M)$), αλλά ελπίζουμε ότι είναι υπολογιστικά ασφαλείς (§1.13.3(iv)).

Οι κρυπταλγόριθμοι ροής ταξινομούνται συνήθως σε *σύγχρονους* και *ασύγχρονους*.

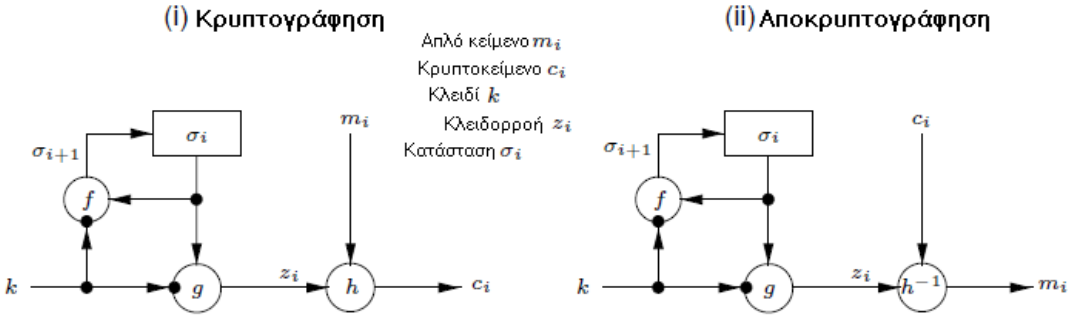
(ii) Σύγχρονοι κρυπταλγόριθμοι ροής

6.2 Ορισμός *Σύγχρονος* κρυπταλγόριθμος ροής είναι αυτός στον οποίο η κλειδορροή παράγεται ανεξάρτητα από το μήνυμα απλού κειμένου και από το κρυπτοκείμενο.

Η διεργασία κρυπτογράφησης ενός σύγχρονου κρυπταλγόριθμου ροής μπορεί να περιγραφεί από τις εξισώσεις:

$$\sigma_{i+1} = f(\sigma_i, k),$$
$$z_i = g(\sigma_i, k),$$
$$c_i = h(z_i, m_i),$$

όπου σ_0 είναι η *αρχική κατάσταση* και μπορεί να προσδιοριστεί από το κλειδί k, f είναι η *συνάρτηση επόμενης κατάστασης* η οποία συνδυάζει την κλειδορροή και το απλό κείμενο m_i για την παραγωγή του κρυπτοκειμένου c_i. Οι διεργασίες κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζονται στην Εικόνα 6.1. Ο τρόπος OFB ενός κρυπταλγόριθμου τμήματος (βλ. §7.2.2(iv)) είναι ένα παράδειγμα σύγχρονου κρυπταλγόριθμου ροής.



Εικόνα 6.1: *Γενικό μοντέλο ενός σύγχρονου κρυπταλγόριθμου ροής.*

6.3 Σημείωση (*ιδιότητες των σύγχρονων κρυπταλγόριθμων ροής*)

(i) *απαιτήσεις συγχρονισμού*. Σε έναν σύγχρονο κρυπταλγόριθμο ροής ο αποστολέας και ο παραλήπτης πρέπει να είναι *συγχρονισμένοι* – χρησιμοποιώντας το ίδιο κλειδί και λειτουργώντας στην ίδια θέση (κατάσταση) εντός του κλειδιού αυτού – για να επιτρέψουν την ενδεδειγμένη αποκρυπτογράφηση. Αν χαθεί ο συγχρονισμός εξαιτίας εισαγωγής ψηφίων κρυπτοκειμένου ή διαγραφής κατά τη διάρκεια της μεταβίβασης, τότε η αποκρυπτογράφηση αποτυγχάνει και μπορεί μόνο να αποκατασταθεί μέσω επιπρόσθετων τεχνικών για επανασυγχρονισμό. Οι τεχνικές για επανασυγχρονισμό περιλαμβάνουν επαναρχικοποίηση, τοποθέτηση ειδικών σημαδιών σε κανονικά διαστήματα στο κρυπτοκείμενο, ή, αν το απλό κείμενο περιέχει αρκετή περίσσεια, δοκιμή όλων των πιθανών όφσετ της κλειδορροής.

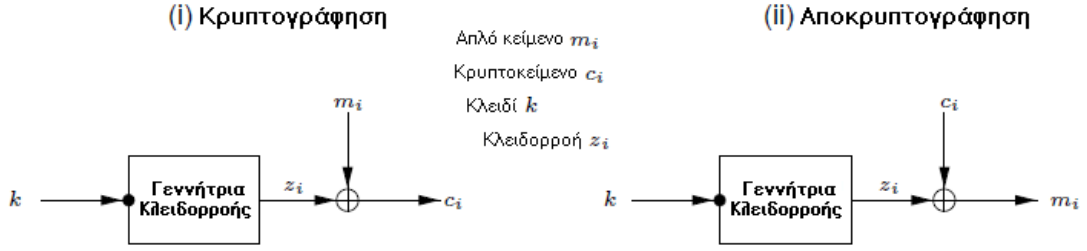
(ii) *μετάδοση κανενός σφάλματος*. Ένα ψηφίο κρυπτοκειμένου το οποίο τροποποιείται (αλλά δεν διαγράφεται) κατά τη διάρκεια της μεταβίβασης δεν επηρεάζει την αποκρυπτογράφηση άλλων ψηφίων του κρυπτοκειμένου.

(iii) *ενεργητικές επιθέσεις*. Ως συνέπεια της ιδιότητας (i), η εισαγωγή, διαγραφή ή επανάληψη ψηφίων του κρυπτοκειμένου από έναν ενεργό αντίπαλο έχει ως αποτέλεσμα την άμεση απώλεια του συγχρονισμού, και επομένως μπορεί ενδεχομένως να γίνει αντιληπτό από το μέλος που αποκρυπτογραφεί. Ως συνέπεια της ιδιότητας (ii) ένας ενεργός αντίπαλος μπορεί ενδεχομένως να είναι σε θέση να κάνει αλλαγές σε επιλεγμένα ψηφία του κρυπτοκειμένου και να γνωρίζει ακριβώς τί επίδραση έχουν αυτές οι αλλαγές στο απλό κείμενο. Αυτό δείχνει ότι πρέπει να εφαρμοστούν επιπρόσθετοι μηχανισμοί προκειμένου να παράσχουν πιστοποίηση αυθεντικότητας της πηγής των δεδομένων (βλ. §9.5.4).

Οι περισσότεροι από τους κρυπταλγόριθμους ροής που έχουν προταθεί μέχρι σήμερα στη βιβλιογραφία είναι προσθετικοί κρυπταλγόριθμοι ροής, τους οποίους ορίζουμε στη συνέχεια.

6.4 Ορισμός *Δυαδικός προσθετικός κρυπταλγόριθμος ροής* είναι ένας σύγχρονος κρυπταλγόριθμος ροής στον οποίο τα ψηφία της κλειδορροής, του απλού κειμένου και του κρυπτοκειμένου είναι δυαδικά ψηφία, και η συνάρτηση εξόδου h είναι η συνάρτηση XOR.

Οι δυαδικοί προσθετικοί κρυπταλγόριθμοι ροής παρουσιάζονται στην Εικόνα 6.2. Αναφερόμενοι στην Εικόνα 6.2, η *γεννήτρια κλειδορροής* απαρτίζεται από τη συνάρτηση επόμενης-κατάστασης f και τη συνάρτηση g (βλ. Εικόνα 6.1), και είναι επίσης γνωστή ως *γεννήτρια ρέοντος κλειδιού*.



Εικόνα 6.2: *Γενικό μοντέλο ενός δυαδικού προσθετικού κρυπταλγόριθμου ροής.*

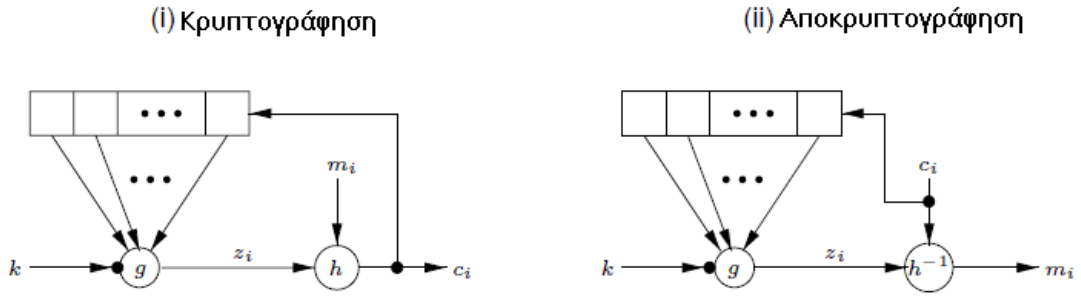
(iii) Ασύγχρονοι κρυπταλγόριθμοι ροής

6.5 Ορισμός *Ασύγχρονος* ή *αυτοσυγχρονιζόμενος* κρυπταλγόριθμος ροής είναι αυτός στον οποίο η κλειδορροή παράγεται ως συνάρτηση του κλειδιού και ενός συγκεκριμένου πλήθους προηγούμενων ψηφίων του κρυπτοκειμένου.

Η συνάρτηση κρυπτογράφησης ενός ασύγχρονου κρυπταλγόριθμου ροής μπορεί να περιγραφεί από τις εξισώσεις:

$$\begin{aligned} \sigma_i &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}), \\ z_i &= g(\sigma_i, k), \\ c_i &= h(z_i, m_i), \end{aligned}$$

όπου $\sigma_0 = (c_{-t}, c_{-t+1}, \ldots, c_{-1})$ είναι η (όχι μυστική) *αρχική κατάσταση*, k είναι το κλειδί, g είναι η συνάρτηση που παράγει την *κλειδορροή* z_i και h είναι η *συνάρτηση εξόδου* η οποία συνδυάζει την κλειδορροή και το απλό κείμενο m_i προκειμένου να παράγει το κρυπτοκείμενο c_i. Οι διεργασίες κρυπτογράφησης και αποκρυπτογράφησης παρουσιάζονται στην Εικόνα 6.3. Οι πλέον κοινοί ασύγχρονοι κρυπταλγόριθμοι ροής που χρησιμοποιούνται επί του παρόντος βασίζονται στους κρυπταλγόριθμους τμήματος σε τρόπο κρυπταλγόριθμου ανάδρασης 1-bit (βλ. §7.2.2(iii)).



Εικόνα 6.3: *Γενικό μοντέλο ενός ασύγχρονου κρυπταλγόριθμου ροής*

6.6 Σημείωση (*ιδιότητες των ασύγχρονων κρυπταλγόριθμων ροής*)

(i) *αυτο-συγχρονισμός*. Ο αυτο-συγχρονισμός είναι δυνατός αν τα ψηφία κρυπτοκειμένου διαγράφονται ή εισάγονται, επειδή η απεικόνιση κρυπτογράφησης εξαρτάται μόνο από ένα συγκεκριμένο πλήθος προηγούμενων χαρακτήρων κρυπτοκειμένου. Τέτοιοι κρυπταλγόριθμοι είναι ικανοί να επανεδραιώσουν την ενδεδειγμένη κρυπτογράφηση αυτόματα μετά την απώλεια του συγχρονισμού, μόνο με ένα συγκεκριμένο πλήθος μη ανακτήσιμων χαρακτήρων απλού κειμένου.

(ii) *περιορισμένη μετάδοση σφαλμάτων*. Ας υποθέσουμε ότι η κατάσταση ενός ασύγχρονου κρυπταλγόριθμου ροής εξαρτάται από t προηγούμενα ψηφία κρυπτοκειμένου. Αν ένα μεμονωμένο ψηφίο κρυπτοκειμένου είναι τροποποιημένο (ή ακόμη και διαγραμμένο ή εισηγμένο) κατά τη μεταβίβαση, τότε η κρυπτογράφηση μέχρι t μεθεπόμενων ψηφίων κρυπτοκειμένου μπορεί να είναι εσφαλμένη, μετά την οποία η σωστή αποκρυπτογράφηση ξαναρχίζει (επανέρχεται).

(iii) *ενεργές επιθέσεις*. Η ιδιότητα (ii) συνεπάγεται ότι η οποιαδήποτε τροποποίηση ψηφίων κρυπτοκειμένου από έναν ενεργό αντίπαλο έχει ως αποτέλεσμα μερικά άλλα ψηφία κρυπτοκειμένου να κρυπτογραφηθούν λανθασμένα και ως εκ τούτου να βελτιωθεί (συγκρινόμενη με σύγχρονους κρυπταλγόριθμους ροής) η πιθανότητα ανίχνευσης από το μέλος που αποκρυπτογραφεί. Ως συνέπεια της ιδιότητας (i), είναι δυσκολότερο (απ' ότι για σύγχρονους κρυπταλγόριθμους ροής) να ανιχνευτεί η εισαγωγή, διαγραφή ή επανάληψη ψηφίων κρυπτοκειμένου από έναν ενεργό αντίπαλο. Αυτό δείχνει ότι πρέπει να εφαρμοστούν επιπρόσθετοι μηχανισμοί προκειμένου να παρέχεται πιστοποίηση αυθεντικότητας της πηγής των δεδομένων και εγγύηση ακεραιότητας των δεδομένων (βλ. §9.5.4).

(iv) διάχυση της στατιστικής του απλού κειμένου. Επειδή κάθε ψηφίο απλού κειμένου επηρεάζει ολόκληρο το κρυπτοκείμενο που ακολουθεί, οι στατιστικές ιδιότητες του απλού κειμένου διασκορπίζονται μέσα στο κρυπτοκείμενο. Έτσι οι ασύγχρονοι κρυπταλγόριθμοι ροής μπορεί να είναι πιο ανθεκτικοί από τους σύγχρονους κρυπταλγόριθμους ροής έναντι επιθέσεων που βασίζονται στην περίσσεια απλού κειμένου.

6.2 Καταχωρητές ολίσθησης με ανάδραση

Οι καταχωρητές ολίσθησης με ανάδραση, ειδικότερα οι καταχωρητές ολίσθησης με γραμμική ανάδραση, είναι οι βασικές συνιστώσες πολλών γεννητριών κλειδορροής. Στην §6.2.2 μελετάμε τη γραμμική πολυπλοκότητα των δυαδικών ακολουθιών, ενώ στην §6.2.2 παρουσιάζουμε τον αλγόριθμο Berlekamp-Massey για τον υπολογισμό της. Τελικά, εξετάζουμε τους καταχωρητές ολίσθησης με μη γραμμική ανάδραση στην §6.2.4.

6.2.1 Καταχωρητές ολίσθησης με γραμμική ανάδραση

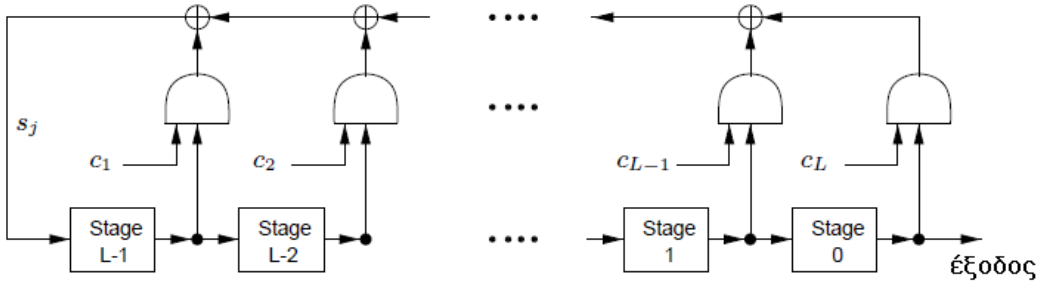
Οι καταχωρητές ολίσθησης με γραμμική ανάδραση (LFSR) χρησιμοποιούνται σε πολλές από τις γεννήτριες κλειδορροής που έχουν προταθεί στη βιβλιογραφία. Υπάρχουν αρκετοί λόγοι γι' αυτό:

1. Οι LFSR ταιριάζουν καλά σε υλοποιήσεις υλικού·
2. μπορούν να παράγουν ακολουθίες μεγάλης περιόδου (Γεγονός 6.12)·
3. μπορούν να παράγουν ακολουθίες με καλές στατιστικές ιδιότητες (Γεγονός 6.14)· και
4. εξαιτίας της δομής τους, μπορούν εύκολα να αναλυθούν χρησιμοποιώντας αλγεβρικές τεχνικές.

6.7 Ορισμός Ένας καταχωρητής ολίσθησης με γραμμική ανάδραση (LFSR – Linear Feedback Shift Register) μήκους L συνίσταται σε L *στάδια* (ή *στοιχεία καθυστέρησης*) αριθμητικά 0, 1, ..., $L-1$, με το καθένα να είναι ικανό να αποθηκεύει 1 bit και να έχει μία είσοδο και μία έξοδο· και ένα ρολόι το οποίο ελέγχει την κίνηση των δεδομένων. Κατά τη διάρκεια κάθε μονάδας χρόνου εκτελούνται οι εξής λειτουργίες:

(i) εξάγεται το περιεχόμενο του σταδίου 0 και αποτελεί μέρος της *ακολουθίας εξόδου*·
(ii) το περιεχόμενο του σταδίου i μετακινείται στο στάδιο $i-1$ για κάθε i, $1 < i < L-1$· και
(iii) το νέο περιεχόμενο του σταδίου $L-1$ είναι το *bit ανάδρασης* s_j το οποίο υπολογίζεται με πρόσθεση modulo 2 των προηγούμενων περιεχομένων ενός συγκεκριμένου υποσυνόλου των σταδίων 0, 1, ..., $L-1$.

Η Εικόνα 6.4 παρουσιάζει έναν LFSR. Αναφερόμενοι στη εικόνα, κάθε c_i είναι 0 ή 1· τα κλειστά ημικύκλια είναι πύλες AND· και το bit ανάδρασης s_j είναι το άθροισμα modulo 2 των περιεχομένων εκείνων των σταδίων i, $1 < i < L-1$, για τα οποία είναι $c_{L-i} = 1$.



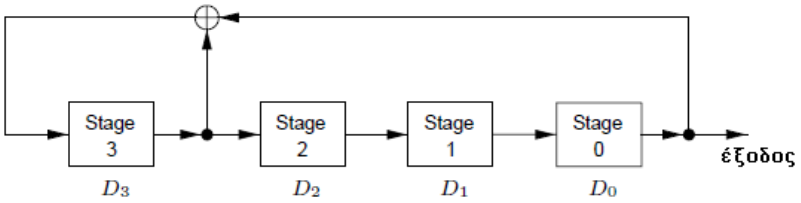
Εικόνα 6.4: *Καταχωρητής ολίσθησης με γραμμική ανάδραση (LFSR) μήκους L.*

6.8 Ορισμός Ο LFSR της Εικόνας 6.4 συμβολίζεται $\langle L, C(D)\rangle$, όπου $C(D) = 1 + c_1D + c_2D^2 + \ldots + c_LD^L \in \mathbb{Z}_2[D]$ είναι το *πολυώνυμο σύνδεσης*. Ο LFSR λέγεται ότι είναι *μη-ιδιάζων* αν ο βαθμός του $C(D)$ είναι L (δηλ. $c_L = 1$). Αν το αρχικό περιεχόμενο του σταδίου i είναι $s_i \in \{0, 1\}$, για κάθε i, $1 < i < L-1$, τότε η $[s_{L-1}, \ldots, s_1, s_0]$ λέγεται *αρχική κατάσταση* του LFSR.

6.9 Γεγονός Αν η αρχική κατάσταση του LFSR στην Εικόνα 6.4 είναι $[s_{L-1}, \ldots, s_1, s_0]$, τότε η ακολουθία εξόδου $s = s_0, s_1, s_2, \ldots$ προσδιορίζεται μονοσήμαντα από την ακόλουθη αναδρομή:

$$s_j = (c_1s_{j-1} + c_2s_{j-2} + \ldots + c_Ls_{j-L}) \bmod 2, \text{ για } j > L.$$

6.10 Παράδειγμα (*ακολουθία εξόδου ενός LFSR*) Θεωρούμε τον LFSR $\langle 4, 1 + D + D^4\rangle$ που απεικονίζεται στην Εικόνα 6.5.



Εικόνα 6.5: *Ο LFSR $\langle 4, 1 + D + D^4\rangle$ του Παραδείγματος 6.10.*

Αν η αρχική κατάσταση του LFSR είναι η [0, 0, 0, 0], τότε η ακολουθία εξόδου είναι η μηδενική ακολουθία. Οι παρακάτω πίνακες δείχνουν τα περιεχόμενα των σταδίων D_3, D_2, D_1, D_0 στο τέλος κάθε μονάδας χρόνου t όταν η αρχική κατάσταση είναι [0,1,1,0].

t	D_3	D_2	D_1	D_0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1
3	0	1	0	0
4	0	0	1	0
5	0	0	0	1
6	1	0	0	0
7	1	1	0	0

t	D_3	D_2	D_1	D_0
8	1	1	1	0
9	1	1	1	1
10	0	1	1	1
11	1	0	1	1
12	0	1	0	1
13	1	0	1	0
14	1	1	0	1
15	0	1	1	0

Η ακολουθία εξόδου είναι $s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \ldots$, και είναι περιοδική με περίοδο 15 (βλ. Ορισμός 5.25). □

Η σημασία τού να είναι ένας LFSR μη-ιδιάζων εξηγείται με το Γεγονός 6.11.

6.11 Γεγονός Κάθε ακολουθία εξόδου (δηλ. για όλες τις δυνατές αρχικές καταστάσεις) ενός LFSR $\langle L, C(D)\rangle$ είναι περιοδική, αν και μόνο αν το πολυώνυμο σύνδεσης $C(D)$ έχει βαθμό L.

Αν ένας LFSR $\langle L, C(D)\rangle$ είναι *ιδιάζων* (δηλ. το $C(D)$ έχει βαθμό μικρότερο του L), τότε δεν είναι όλες οι ακολουθίες εξόδου περιοδικές. Όμως, οι ακολουθίες εξόδου είναι *σε τελευταία ανάλυση περιοδικές*· δηλαδή, οι ακολουθίες που παίρνουμε αγνοώντας ένα πεπερασμένο πλήθος όρων στην αρχή είναι περιοδικές. Για το υπόλοιπο αυτού του κεφαλαίου θα υποθέσουμε ότι όλοι οι LFSR είναι *μη-ιδιάζοντες*. Το Γεγονός 6.12 προσδιορίζει τις περιόδους των ακολουθιών εξόδου ορισμένων ειδικών τύπων από τους μη-ιδιάζοντες LFSR.

6.12 Γεγονός (*περίοδοι των ακολουθιών εξόδου των LFSR*) Έστω $C(D) \in \mathbb{Z}_2[D]$ ένα πολυώνυμο σύνδεσης βαθμού L.

(i) Αν το $C(D)$ είναι ανάγωγο επί του $\mathbb{Z}_2$ (βλ. Ορισμός 2.190), τότε κάθε μια από τις $2^L - 1$ μη μηδενικές αρχικές καταστάσεις του μη-ιδιάζοντος LFSR $\langle L, C(D)\rangle$ παράγει μια ακολουθία εξόδου με περίοδο ίση με τον μικρότερο θετικό ακέραιο N τέτοιον, ώστε το $C(D)$ να διαιρεί το $1 + D^N$ στο $\mathbb{Z}_2[D]$. (Σημείωση: ισχύει πάντα ότι αυτός ο N είναι διαιρέτης του $2^L - 1$).

(ii) Αν το $C(D)$ είναι ένα πρωτεύον πολυώνυμο (βλ. Ορισμός 2.228), τότε κάθε μια από τις $2^L - 1$ μη μηδενικές αρχικές καταστάσεις του μη-ιδιάζοντος LFSR $\langle L, C(D)\rangle$ παράγει μια ακολουθία εξόδου με μέγιστη δυνατή περίοδο $2^L - 1$.

Μια μέθοδος παραγωγής πρωτευόντων πολυωνύμων επί του $\mathbb{Z}_2$ ομοιόμορφα στην τύχη δίνεται στον Αλγόριθμο 4.78. Ο Πίνακας 4.8 παρουσιάζει ένα πρωτεύον πολυώνυμο βαθμού m επί του $\mathbb{Z}_2$, για κάθε m, $1 \le m \le 299$. Το Γεγονός 6.12(ii) λειτουργεί ως κίνητρο για τον ακόλουθο ορισμό.

6.13 Ορισμός Αν το $C(D) \in \mathbb{Z}_2[D]$ είναι ένα πρωτεύον πολυώνυμο βαθμού L, τότε ο $\langle L, C(D)\rangle$ λέγεται LFSR *μέγιστου μήκους*. Η έξοδος ενός LFSR μέγιστου μήκους με μη μηδενική αρχική κατάσταση λέγεται *m-ακολουθία*.

Το Γεγονός 6.14 καταδεικνύει ότι οι ακολουθίες εξόδου των LFSR μέγιστου μήκους έχουν καλές στατιστικές ιδιότητες.

6.14 Γεγονός (*στατιστικές ιδιότητες των m-ακολουθιών*) Έστω s μια m-ακολουθία η οποία παράγεται από έναν LFSR μέγιστου μήκους με μήκος L.

(i) Έστω k ένας ακέραιος, $1 \le k \le L$ και $\overline{s}$ μια υπακολουθία της s μήκους $2^L + k - 2$. Τότε κάθε μη μηδενική ακολουθία μήκους k εμφανίζεται ακριβώς 2^{L-k} φορές ως ακολουθία της $\overline{s}$. Επιπλέον, η μηδενική ακολουθία μήκους k εμφανίζεται ακριβώς $2^{L-k} - 1$ φορές ως υπακολουθία της $\overline{s}$. Με άλλα λόγια, η κατανομή των προτύπων (μοτίβων) που έχουν συγκεκριμένο μήκος το πολύ L είναι σχεδόν ομοιόμορφη.

(ii) Η s ικανοποιεί τα αξιώματα τυχαιότητας του Golomb (§ 5.4.3). Δηλαδή, κάθε m-ακολουθία είναι επίσης μια pn-ακολουθία (βλ. Ορισμός 5.29).

6.15 Παράδειγμα (*m-ακολουθία*) Αφού το $C(D) = 1 + D + D^4$ είναι ένα πρωτεύον πολυώνυμο επί του $\mathbb{Z}_2$, ο LFSR $\langle 4, 1 + D + D^4\rangle$ είναι ένας LFSR μέγιστου μήκους. Άρα, η ακολουθία εξόδου αυτού του LFSR είναι μια m-ακολουθία μέγιστης δυνατής περιόδου $N = 2^4 - 1 = 15$ (βλ. Παράδειγμα 6.10). Το Παράδειγμα 5.30 πιστοποιεί ότι αυτή η ακολουθία εξόδου ικανοποιεί τις ιδιότητες τυχαιότητας του Golomb.

6.2.2 Γραμμική πολυπλοκότητα

Σε αυτή την υποενότητα συνοψίζουμε επιλεγμένα αποτελέσματα σχετικά με τη γραμμική πολυπλοκότητα των ακολουθιών. Υποθέτουμε ότι όλες οι ακολουθίες είναι δυαδικές ακολουθίες. Συμβολισμός: με s συμβολίζουμε μια άπειρη ακολουθία της οποίας οι όροι είναι $s_0, s_1, s_2,$

…, όπου το s^n συμβολίζει μια πεπερασμένη ακολουθία μήκους n της οποίας οι όροι είναι s_0, s_1, …, s_{n-1} (βλ. Ορισμός 5.24).

6.16 Ορισμός Λέμε ότι ένας LFSR *παράγει* μια ακολουθία s αν υπάρχει κάποια αρχική κατάσταση για την οποία η ακολουθία εξόδου του LFSR είναι s. Παρόμοια, λέμε ότι *παράγει* μια πεπερασμένη ακολουθία s^n αν υπάρχει κάποια αρχική κατάσταση για την οποία η ακολουθία εξόδου του LFSR έχει την s^n ως τους πρώτους n όρους.

6.17 Ορισμός Η *γραμμική πολυπλοκότητα* μιας άπειρης δυαδικής ακολουθίας s, συμβολικά $L(s)$, ορίζεται ως εξής:

(i) αν s είναι η μηδενική ακολουθία $s = 0, 0, 0, \ldots$, τότε $L(s) = 0$
(ii) αν κανένας LFSR δεν παράγει την s, τότε $L(s) = \infty$
(iii) διαφορετικά, $L(s)$ είναι το μήκος του βραχύτερου LFSR που παράγει την s.

6.18 Ορισμός Η *γραμμική πολυπλοκότητα* μιας πεπερασμένης δυαδικής ακολουθίας s^n, συμβολικά $L(s^n)$, είναι το μήκος του βραχύτερου LFSR που παράγει μια ακολουθία η οποία έχει την s^n ως τους πρώτους n όρους.

Τα Γεγονότα 6.19 - 6.22 συνοψίζουν μερικά βασικά αποτελέσματα σχετικά με τη γραμμική πολυπλοκότητα.

6.19 Γεγονός (*ιδιότητες της γραμμικής πολυπλοκότητας*) Έστω s και t δυο δυαδικές ακολουθίες:

(i) Για οποιοδήποτε $n \geq 1$, η γραμμική πολυπλοκότητα της υπακολουθίας s^n ικανοποιεί την $0 \leq L(s^n) \leq n$.
(ii) $L(s^n) = 0$, αν και μόνο αν η s^n είναι η μηδενική ακολουθία μήκους n.
(iii) $L(s^n) = n$, αν και μόνο αν $s^n = 0, 0, 0, \ldots, 0, 1$.
(iv) Αν η s είναι περιοδική με περίοδο N, τότε $L(s) \leq N$.
(v) $L(s \oplus t) \leq L(s) + L(t)$, όπου $s \oplus t$ συμβολίζει την XOR ανά bit των s και t.

6.20 Γεγονός Αν το πολυώνυμο $C(D) \in \mathbb{Z}_2[D]$ είναι ανάγωγο επί του $\mathbb{Z}_2$ και έχει βαθμό L, τότε κάθε μια από τις $2^L - 1$ μη μηδενικές αρχικές καταστάσεις του μη ιδιάζοντος LFSR $\langle L, C(D)\rangle$ παράγει μια ακολουθία εξόδου με γραμμική πολυπλοκότητα L.

6.21 Γεγονός (*αναμενόμενη τιμή και διακύμανση της γραμμικής πολυπλοκότητας μιας τυχαίας ακολουθίας*) Έστω ότι η s^n επιλέγεται ομοιόμορφα στην τύχη από το σύνολο όλων των δυαδικών ακολουθιών μήκους n, και έστω $L(s^n)$ η γραμμική πολυπλοκότητα της s^n. Έστω ότι $B(n)$ συμβολίζει τη συνάρτηση αρτιότητας: $B(n) = 0$, αν n άρτιος· $B(n) = 1$, αν n περιττός.

(i) Η αναμενόμενη γραμμική πολυπλοκότητα της s^n είναι

$$E(L(s^n)) = \frac{n}{2} + \frac{4 + B(n)}{18} - \frac{1}{2^n}\left(\frac{n}{3} + \frac{2}{n}\right).$$

Άρα, για μετρίως μεγάλο n, είναι $E(L(s^n)) \approx \frac{n}{2} + \frac{2}{9}$, αν n άρτιος, και $E(L(s^n)) \approx \frac{n}{2} + \frac{5}{18}$, αν n περιττός.

(ii) Η διακύμανση της γραμμικής πολυπλοκότητας της s^n είναι

$$\frac{86}{81} - \frac{1}{2^n}\left(\frac{14 - B(n)}{27}n + \frac{82 - 2B(n)}{81}\right) - \frac{1}{2^{2n}}\left(\frac{1}{9}n^2 + \frac{4}{27}n + \frac{4}{81}\right).$$

Αρα, είναι $\mathrm{Var}(L(s^n)) \approx \frac{86}{81}$ για μετρίως μεγάλο n.

6.22 Γεγονός (*αναμενόμενη τιμή της γραμμικής πολυπλοκότητας μιας τυχαίας περιοδικής ακολουθίας*) Έστω ότι η s^n έχει επιλεγεί ομοιόμορφα στην τύχη από το σύνολο όλων των δυαδικών ακολουθιών μήκους n, όπου $n = 2^i$ για κάποιο συγκεκριμένο $t \geq 1$, και έστω s η n-περιοδική άπειρη ακολουθία που παίρνουμε με επανάληψη της ακολουθίας s^n. Τότε η αναμενόμενη γραμμική πολυπλοκότητα της s είναι $E(L(s^n)) = n - 1 + 2^{-n}$.

Στη συνέχεια παρουσιάζουμε την κατατομή (profile) της γραμμικής πολυπλοκότητας μιας δυαδικής ακολουθίας.

6.23 Ορισμός Έστω $s = s_0, s_1, \ldots$, μια δυαδική ακολουθία και έστω ότι L_N συμβολίζει τη γραμμική πολυπλοκότητα της υπακολουθίας $s^N = s_0, s_1, \ldots, s_{N-1}$, $N > 0$. Η ακολουθία $L_1, L_2, \ldots$, λέγεται *κατατομή της γραμμικής πολυπλοκότητας της* s. Παρόμοια, αν $s^n = s_0, s_1, \ldots, s_{n-1}$, είναι μια πεπερασμένη δυαδική ακολουθία, η ακολουθία $L_1, L_2, \ldots, L_n$ λέγεται κατατομή της γραμμικής πολυπλοκότητας της s^n.

Η κατατομή της γραμμικής πολυπλοκότητας μιας ακολουθίας μπορεί να υπολογιστεί χρησιμοποιώντας τον αλγόριθμο Berlekamp-Massey (Αλγόριθμος 6.30)· δείτε επίσης τη Σημείωση 6.31. Οι ακόλουθες ιδιότητες της κατατομής της γραμμικής πολυπλοκότητας μπορούν να προκύψουν από το Γεγονός 6.29.

6.24 Γεγονός (*ιδιότητες της κατατομής της γραμμικής πολυπλοκότητας*) Έστω $L_1, L_2, \ldots$ η κατατομή της γραμμικής πολυπλοκότητας μια ακολουθίας $s = s_0, s_1, \ldots$.

(i) Αν $j > i$, τότε $L_j \geq L_i$.

(ii) $L_{N+1} > L_N$ είναι δυνατό μόνο αν $L_N \leq N/2$.

(iii) Αν $L_{N+1} > L_N$, τότε $L_{N+1} + L_N = N + 1$.

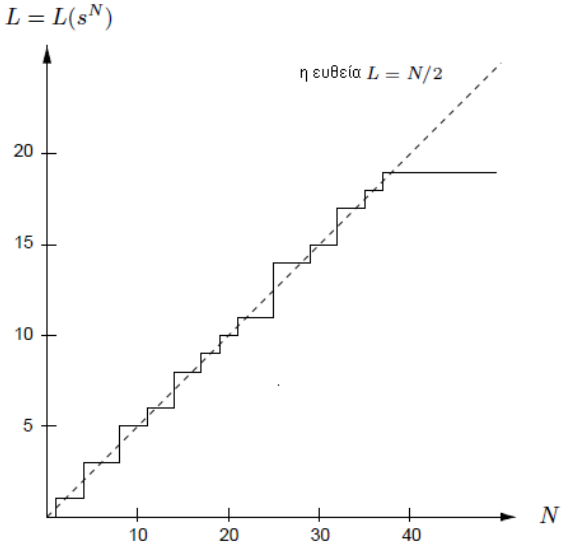
Η κατατομή της γραμμικής πολυπλοκότητας μιας ακολουθίας s μπορεί να παρασταθεί γραφικά παριστώντας τα σημεία (N, L_N), $N \geq 1$, στο $N \times L$ επίπεδο και συνδέοντας διαδοχικά σημεία με μια οριζόντια γραμμή ακολουθούμενη απο μια κατακόρυφη γραμμή, αν είναι αναγκαίο (βλ. Εικόνα 6.6). Το Γεγονός 6.24 μπορεί μετά να ερμηνευτεί ως πρόταση που λέει ότι το γράφημα μιας κατατομής της γραμμικής πολυπλοκότητας δεν φθίνει. Επιπλέον, ένα (κατακόρυφο) πήδημα στο γράφημα μπορεί να εμφανιστεί μόνο κάτω από την ευθεία $L = N/2$· αν εμφανίζεται ένα πήδημα, τότε είναι συμμετρικό ως προς τη γραμμή αυτή. Το Γεγονός 6.25 δείχνει ότι η αναμενόμενη κατατομή της γραμμικής πολυπλοκότητας μιας τυχαίας ακολουθίας θα πρέπει να ακολουθεί στενά τη γραμμή $L = N/2$.

6.25 Γεγονός (*αναμενόμενη κατατομή της γραμμικής πολυπλοκότητας μιας τυχαίας ακολουθίας*) Έστω ότι $s = s_0, s_1, \ldots$είναι μια τυχαία ακολουθία και ότι L_N είναι η γραμμική πολυπλοκότητα της ακολουθίας $s^N = s_0, s_1, \ldots, s_{N-1}$, για κάθε $N \geq 1$. Για ένα συγκεκριμένο $N \geq 1$, το αναμενόμενο μικρότερο j, για το οποίο είναι $L_{N+j} > L_N$, είναι το 2 αν $L_N \leq N/2$, ή το $2 + 2L_N - N$, αν $L_N > N/2$. Επιπλέον, η αναμενόμενη αύξηση στη γραμμική πολυπλοκότητα είναι 2, αν $L_N \geq N/2$, ή $2 + 2L_N + 2$, αν $L_N < N/2$.

6.26 Παράδειγμα (*κατατομή της γραμμικής πολυπλοκότητας*) Θεωρούμε την 20-περιοδική ακολουθία s με κύκλο

$$s^{20} = 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0.$$

Η κατατομή της γραμμικής πολυπλοκότητας της s είναι 1, 1, 1, 3, 3, 3, 3, 5, 5, 5, 6, 6, 6, 8, 8, 8, 9, 9, 10, 10, 11, 11, 11, 11, 14, 14, 14, 14, 15, 15, 15, 17, 17, 17, 18, 18, 19, 19, 19, 19, …. Η Εικόνα 6.6 δείχνει το γράφημα της κατατομής της γραμμικής πολυπλοκότητας της s. □



Εικόνα 6.6: *Κατατομή της γραμμικής πολυπλοκότητας της 20-περιοδικής ακολουθίας του Παραδείγματος 6.26.*

Όπως συμβαίνει με όλους τους στατιστικούς ελέγχους για τυχαιότητα (βλ. §5.4), η συνθήκη ότι μια ακολουθία s έχει μια κατατομή της γραμμικής πολυπλοκότητας η οποία προσομοιάζει στενά εκείνη μιας τυχαίας ακολουθίας είναι *αναγκαία*, αλλά όχι *ικανή*, για να θεωρείται η s τυχαία. Το σημείο αυτό διασαφηνίζεται στο ακόλουθο παράδειγμα.

6.27 Παράδειγμα (*Περιορισμοί της κατατομής της γραμμικής πολυπλοκότητας)* Η κατατομή της γραμμικής πολυπλοκότητας της ακολουθίας s που ορίζεται ως:

$$s_i = \begin{cases} 1, & \text{αν } i = 2^j - 1 \text{ για κάποιο } j \geq 0 \\ 0, & \text{διαφορετικά} \end{cases}$$

ακολουθεί τη γραμμή $L = N/2$ όσο το δυνατό πιο στενά. Δηλαδή, $L(s^n) = \lfloor (N+1)/2 \rfloor$, για κάθε $N \geq 1$. Όμως, η ακολουθία s προφανώς δεν είναι τυχαία. □

6.2.3 Αλγόριθμος Berlekamp-Massey

Ο Αλγόριθμος Berlekamp-Massey (Αλγόριθμος 6.30) είναι ένας αποδοτικός αλγόριθμος για τον προσδιορισμό της γραμμικής πολυπλοκότητας μιας πεπερασμένης δυαδικής ακολουθίας s^n μήκους n (βλ. Ορισμός 6.18). Ο αλγόριθμος κάνει n επαναλήψεις, με τη N-οστή επανάληψη να υπολογίζει τη γραμμική πολυπλοκότητα της υπακολουθίας s^n που αποτελείται από τους πρώτους N όρους της s^n. Η θεωρητική βάση για τον αλγόριθμο είναι το Γεγονός 6.29.

6.28 Ορισμός Θεωρούμε την πεπερασμένη δυαδική ακολουθία $s^{N+1} = s_0, s_1, \ldots, s_{N-1}, s_N$. Για το $C(D) = 1 + c_1D + c_2D^2 + \ldots + c_LD^L$ έστω ότι $\langle L, C(D)\rangle$ είναι ο LFSR ο οποίος παράγει την υπακολουθία $s^N = s_0, s_1, \ldots, s_{N-1}$. Η *επόμενη ασυμφωνία* d_N είναι η διαφορά μεταξύ του s_N και του $(N+1)$-οστού όρου που παράγεται από τον LFSR: $d_N = (s_N + \sum_{i=1}^{L} c_i s_{N-i}) \bmod 2$.

6.29 Γεγονός Έστω $s^N = s_0, s_1, \ldots, s_{N-1}$ μια πεπερασμένη δυαδική ακολουθία γραμμικής πολυπλοκότητας $L = L(s^n)$ και έστω ότι $\langle L, C(D)\rangle$ είναι ένας LFSR ο οποίος παράγει την s^N.

(i) Ο LFSR $\langle L, C(D)\rangle$ παράγει επίσης την $s^{N+1} = s_0, s_1, \ldots, s_{N-1}, s_N$, αν και μόνο αν η επόμενη ασυμφωνία d_N είναι ίση με 0.

(ii) Αν $d_N = 0$, τότε $L(s^{N+1}) = L$.

(iii) Ας υποθέσουμε ότι $d_N = 1$. Έστω m ο μεγαλύτερος ακέραιος $< N$ τέτοιος, ώστε $L(s^m) < L(s^N)$ και ότι $\langle L(s^m), B(D)\rangle$ είναι ένας LFSR μήκους $L(s^m)$ ο οποίος παράγει την s^m. Τότε ο $\langle L', C'(D)\rangle$ είναι ένας LFSR με το μικρότερο μήκος ο οποίος παράγει την s^{N+1}, όπου

$$L' = \begin{cases} L, & \text{αν } L > N/2 \\ N+1-L, & \text{αν } L \le N/2 \end{cases}$$

και $C'(D) = C(D) + B(D)\cdot D^{N-m}$.

6.30 Ο Αλγόριθμος Berlekamp-Massey

ΕΙΣΟΔΟΣ: μια δυαδική ακολουθία $s^n = s_0, s_1, \ldots, s_{n-1}$ μήκους n.

ΕΞΟΔΟΣ: η γραμμική πολυπλοκότητα $L(s^n)$ με $0 \le L(s^n) \le n$.

1. *Αρχικοποίηση.* $C(D) \leftarrow 1$, $L \leftarrow 0$, $m \leftarrow -1$, $B(D) \leftarrow 1$, $N \leftarrow 0$.
2. **while** $(N < n)$ **do**

   2.1 *υπολογισμός της επόμενης ασυμφωνίας d.* $D \leftarrow (s_N + \sum_{i=1}^{L} c_i s_{N-i}) \bmod 2$.

   2.2 **if** $d = 1$ **then do**

   $T(D) \leftarrow C(D)$, $C(D) \leftarrow C(D) + B(D)\cdot D^{N-m}$.

   if $L \le N/2$ **then** $L \leftarrow N + 1 - L$, $m \leftarrow N$, $B(D) \leftarrow T(D)$

   2.3 $N \leftarrow N + 1$.
3. **return**(L).

6.31 Σημείωση (*ενδιάμεσα αποτελέσματα στον αλγόριθμο Berlekamp-Massey*) Στο τέλος κάθε επανάληψης του βήματος 2, $\langle L, C(D)\rangle$ είναι ένας LFSR με το μικρότερο μήκος ο οποίος παράγει την s^N. Άρα, ο Αλγόριθμος 6.30 μπορεί επίσης να χρησιμοποιηθεί για τον υπολογισμό της κατατομής της γραμμικής πολυπλοκότητας (Ορισμός 6.23) μιας πεπερασμένης ακολουθίας.

6.32 Γεγονός Ο χρόνος εκτέλεσης του αλγορίθμου Berlekamp-Massey (Αλγόριθμος 6.30) για τον υπολογισμό της γραμμικής πολυπλοκότητας μιας δυαδικής ακολουθίας δυαδικού μήκους n είναι $O(n^2)$ πράξεις bit.

6.33 Παράδειγμα (*Αλγόριθμος Berlekamp-Massey*) Ο Πίνακας 6.1 δείχνει τα βήματα του Αλγορίθμου 6.30 για τον υπολογισμό της γραμμικής πολυπλοκότητας μιας δυαδικής ακολουθίας $s^n = 0, 0, 1, 1, 0, 1, 1, 1, 0$ μήκους $n = 9$. Η ακολουθία αυτή βρίσκουμε ότι έχει γραμμική πολυπλοκότητα 5 κα ένας LFSR που την παράγει είναι ο $\langle 5, 1 + D^3 + D^5\rangle$.

6.34 Γεγονός Έστω s^n μια πεπερασμένη δυαδική ακολουθία μήκους n και έστω ότι η γραμμική πολυπλοκότητα της s^n είναι L. Τότε υπάρχει ένας μοναδικός LFSR μήκους L ο οποίος παράγει την s^n, αν και μόνο αν $L \leq n/2$.

Μια σημαντική συνέπεια του Γεγονότος 6.34 και του Γεγονότος 6.24(iii) είναι η εξής.

6.35 Γεγονός Έστω s μια (άπειρη) δυαδική ακολουθία γραμμικής πολυπλοκότητας L και έστω ότι t είναι μια (πεπερασμένη) υπακολουθία της s μήκους τουλάχιστο $2L$. Τότε ο αλγόριθμος Berlekamp-Massey (με το βήμα 3 τροποποιημένο ώστε να επιστρέφει το L και το $C(D)$) με είσοδο t προσδιορίζει έναν LFSR μήκους L ο οποίος παράγει την s.

s_N	d	$T(D)$	$C(D)$	L	m	$B(D)$	N
–	–	–	1	0	−1	1	0
0	0	–	1	0	−1	1	1
0	0	–	1	0	−1	1	2
1	1	1	$1+D^3$	3	2	1	3
1	1	$1+D^3$	$1+D+D^3$	3	2	1	4
0	1	$1+D+D^3$	$1+D+D^2+D^3$	3	2	1	5
1	1	$1+D+D^2+D^3$	$1+D+D^2$	3	2	1	6
1	0	$1+D+D^2+D^3$	$1+D+D^2$	3	2	1	7
1	1	$1+D+D^2$	$1+D+D^2+D^5$	5	7	$1+D+D^2$	8
0	1	$1+D+D^2+D^5$	$1+D^3+D^5$	5	7	$1+D+D^2$	9

Πίνακας 6.1: *Τα βήματα του αλγορίθμου Berlekamp-Massey για το Παράδειγμα 6.33.*

6.2.4 Καταχωρητές ολίσθησης με μη γραμμική ανάδραση

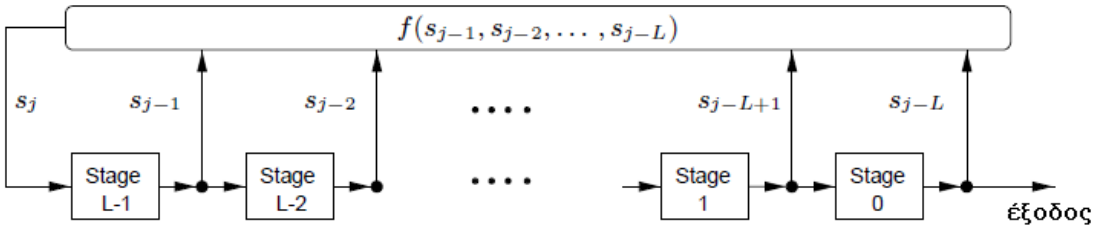
Σε αυτή την υποενότητα συνοψίζουμε επιλεγμένα αποτελέσματα για τους καταχωρητής ολίσθησης με μη γραμμική ανάδραση. Μια συνάρτηση με n δυαδικές εισόδους και μία δυαδική έξοδο λέγεται *Μπουλιανή συνάρτηση* n μεταβλητών· υπάρχουν 2^{2^n} διαφορετικές Μπουλιανές συναρτήσεις n μεταβλητών.

6.36 Ορισμός Ένας (γενικός) *καταχωρητής ολίσθησης με ανάδραση* (FSR – Feedback Shift Register) μήκους L αποτελείται από L *στάδια* (stage) ή *στοιχεία υστέρησης*, αριθμημένα 0, 1, …, $L-1$, με το καθένα να είναι σε θέση να αποθηκεύει ένα bit και που έχει μία είσοδο, και ένα ρολόι το οποίο ρυθμίζει την κίνηση των δεδομένων. Κατά τη διάρκεια κάθε μονάδας χρόνου εκτελούνται οι ακόλουθες λειτουργίες:

(i) το περιεχόμενο του σταδίου 0 εξάγεται και αποτελεί μέρος τη ακολουθίας εξόδου·
(ii) το περιεχόμενο του σταδίου i μετακινείται στο στάδιο $i-1$ για κάθε i, $1 \leq i \leq L-1$· και
(iii) το νέο περιεχόμενο του σταδίου $L-1$ είναι το *bit ανάδρασης* $s_j = f(s_{j-1}, s_{j-2}, \ldots, s_{j-L})$, όταν η *συνάρτηση ανάδρασης* f είναι μια Μπουλιανή συνάρτηση και s_{j-i} είναι το προηγούμενο περιεχόμενο του σταδίου $L-i$, $1 \leq i \leq L$.

Αν το αρχικό περιεχόμενο του σταδίου i είναι $s_i \in \{0, 1\}$, για κάθε $1 \leq i \leq L-1$, τότε η $[s_{L-1}, \ldots, s_1, s_0]$ λέγεται *αρχική κατάσταση* του FSR.

Στην Εικόνα 6.7 απεικονίζεται ένας FSR. Να σημειωθεί ότι αν η *συνάρτηση ανάδρασης* f είναι μια γραμμική συνάρτηση, τότε ο FSR είναι ένας LFSR (Ορισμός 6.7). Διαφορετικά, ο FSR λέγεται *μη γραμμικός* FSR.



Εικόνα 6.7: *Ένας καταχωρητής ολίσθησης (FSR) μήκους L.*

6.37 Γεγονός Αν η αρχική κατάσταση του FSR στην Εικόνα 6.7 είναι $[s_{L-1}, \ldots, s_1, s_0]$, τότε η ακολουθία εξόδου $s = s_0, s_1, \ldots$, προσδιορίζεται μονοσήμαντα από την ακόλουθη αναδρομή:

$$s_j = f(s_{j-1}, s_{j-2}, \ldots, s_{j-L}), \text{ για κάθε } j \geq L.$$

6.38 Ορισμός Ένας FSR λέγεται ότι είναι *μη-ιδιάζων*, αν και μόνο αν κάθε ακολουθία εξόδου του FSR (δηλ. για όλες τις δυνατές αρχικές καταστάσεις) είναι περιοδική.

6.39 Γεγονός Ένας FSR με *συνάρτηση ανάδρασης* $f(s_{j-1}, s_{j-2}, \ldots, s_{j-L})$ είναι μη-ιδιάζων, αν και μόνο αν η f είναι της μορφής $f = s_{j-L} \oplus g(s_{j-1}, s_{j-2}, \ldots, s_{j-L+1})$ για μια Μπουλιανή συνάρτηση g.

Η περίοδος της ακολουθίας εξόδου ενός μη-ιδιάζοντος FSR μήκους L είναι το πολύ 2^L.

6.40 Ορισμός Αν η περίοδος της ακολουθίας εξόδου (για οποιαδήποτε αρχική κατάσταση) ενός μη-ιδιάζοντος FSR μήκους L είναι 2^L, τότε ο FSR λέγεται *FSR de Bruijn* και η ακολουθία εξόδου λέγεται ακολουθία *de Bruijn*.

6.41 Παράδειγμα (*ακολουθία de Bruijn*) Θεωρούμε τον FSR μήκους 3 με τη γραμμική συνάρτηση ανάδρασης $f(x_1, x_2, x_3) = 1 \oplus x_2 \oplus x_3 \oplus x_1x_2$. Οι ακόλουθοι πίνακες παρουσιάζουν τα περιεχόμενα των 3 σταδίων του FSR στο τέλος κάθε μονάδας του χρόνου t όταν η αρχική κατάσταση είναι [0,0,0].

t	Stage 2	Stage 1	Stage 0
0	0	0	0
1	1	0	0
2	1	1	0
3	1	1	1

t	Stage 2	Stage 1	Stage 0
4	0	1	1
5	1	0	1
6	0	1	0
7	0	0	1

Η ακολουθία εξόδου είναι η ακολουθία de Bruijn με κύκλο 0, 0, 0, 1, 1, 1, 0, 1. □

Το Γεγονός 6.42 καταδεικνύει ότι η ακολουθία εξόδου FSR *de Bruijn* έχει καλές στατιστικές ιδιότητες (συγκρίνετε με το Γεγονός 6.14(i)).

6.42 Γεγονός (*στατιστικές ιδιότητες των ακολουθιών de Bruijn*) Έστω s μια ακολουθία *de Bruijn* η οποία παράγεται από ένα FSR *de Bruijn* μήκους L. Έστω k ένας ακέραιος, $1 \leq k \leq L$ και $\overline{s}$ μια υπακολουθία της s μήκους $2^L + k - 1$. Τότε κάθε ακολουθία μήκους k εμφανίζεται ακριβώς 2^{L-k} φορές ως υπακολουθία της $\overline{s}$. Με άλλα λόγια, η κατανομή των προτύπων που έχουν συγκεκριμένο μήκος το πολύ L είναι ομοιόμορφη.

6.43 Σημείωση (*μετατροπή ενός LFSR μέγιστου μήκους σε ένα FSR de Bruijn*) Έστω R_1 ένας LFSR μέγιστου μήκους L, με συνάρτηση (γραμμικής) ανάδρασης $f(s_{j-1}, s_{j-2}, \ldots, s_{j-L})$.Τότε ο FSR R_2

με συνάρτηση ανάδρασης $g(s_{j-1}, s_{j-2}, \ldots, s_{j-L}) = f \oplus \overline{s}_{j-1}\overline{s}_{j-2}\cdots\overline{s}_{j-L+1}$ είναι ένας FSR de Bruijn. Εδώ, $\overline{s}_i$ συμβολίζει το συμπλήρωμα του s_i. Η ακολουθία εξόδου του R_2 προκύπτει από εκείνη του R_1 απλά προσθέτοντας ένα 0 στο τέλος κάθε υπακολουθίας με $L-1$ μηδενικά που εμφανίζονται στην ακολουθία εξόδου R_1.

6.3 Κρυπταλγόριθμοι ροής βασισμένοι σε LFSR

Όπως αναφέραμε στην αρχή της §6.2.1, οι καταχωρητές ολίσθησης με γραμμική ανάδραση χρησιμοποιούνται ευρέως σε γεννήτριες κλειδορροής επειδή αρμόζουν καλά για υλοποίηση υλικού, παράγουν ακολουθίες που έχουν μεγάλες περιόδους και καλές στατιστικές ιδιότητες, και αναλύονται εύκολα με χρήση αλγεβρικών τεχνικών. Δυστυχώς, οι ακολουθίες εξόδου των LFSR είναι επίσης εύκολα προβλέψιμες, όπως μπορούμε να δούμε με τον εξής συλλογισμό. Ας υποθέσουμε ότι η ακολουθία εξόδου s ενός LFSR έχει γραμμική πολυπλοκότητα L. Το πολυώνυμο σύνδεσης $C(D)$ ενός LFSR μήκους L που παράγει την s μπορεί να προσδιοριστεί αποδοτικά με χρήση του αλγορίθμου Berlekamp-Massey (Αλγόριθμος 6.30) από μια (βραχεία) υπακολουθία t της s που έχει μήκος τουλάχιστο $n = 2L$ (βλ. Γεγονός 6.35). Έχοντας προσδιορίσει το $C(D)$, ο LFSR $\langle L, C(D)\rangle$ μπορεί τότε να αρχικοποιηθεί με οποιαδήποτε υποσυμβολοσειρά της t που έχει μήκος L, και να χρησιμοποιηθεί για να παραχθεί το υπόλοιπο τμήμα της ακολουθίας s. Ένας αντίπαλος μπορεί να αλλάζει τη ζητούμενη υπακολουθία t της s εξαπολύοντας μια επίθεση γνωστού ή επιλεγμένου απλού κειμένου (§1.13.1) στον κρυπταλγόριθμο ροής: αν ο αντίπαλος γνωρίζει την υπακολουθία κρυπτοκειμένου $c_1, c_2, \ldots, c_n$, τα αντίστοιχα bit κλειδορροής προκύπτουν ως $m_i \oplus c_i$, $1 \le i \le n$.

6.44 Σημείωση (*χρήση των LFSR σε γεννήτριες κλειδορροών*) Αφού ένα καλά σχεδιασμένο σύστημα θα πρέπει να είναι ασφαλές σε επιθέσεις γνωστού απλού κειμένου, ένας LFSR δεν θα πρέπει ποτέ να χρησιμοποιηθεί από μόνος του ως γεννήτρια κλειδορροής. Παρόλα αυτά, οι LFSR είναι επιθυμητοί εξαιτίας του πολύ χαμηλού κόστους υλοποίησης τους. Στην ενότητα αυτή εξετάζουμε τρεις γενικές μεθοδολογίες για την καταστροφή των ιδιοτήτων γραμμικότητας των LFSR:

(i) χρήση μιας μη γραμμικής συνάρτησης συνδυασμού στις εξόδους μερικών LFSR (§6.3.1)·
(ii) χρήση μιας μη γραμμικής συνάρτησης διήθησης στα περιεχόμενα ενός μεμονωμένου LFSR (§6.3.2)· και
(iii) χρήση της εξόδου ενός (ή περισσοτέρων) LFSR για τη ρύθμιση του ρολογιού ενός άλλου (ή περισσοτέρων) LFSR (§6.3.3).

Επιθυμητές ιδιότητες των βασισμένων σε LFSR γεννητριών κλειδορροών

Για όλα ουσιαστικά τα πιθανά μυστικά κλειδιά, η ακολουθία εξόδου μιας βασισμένης σε LFSR γεννήτριες κλειδορροής θα πρέπει να έχει τις ακόλουθες ιδιότητες:

1. μεγάλη περίοδο·
2. μεγάλη γραμμική πολυπλοκότητα· και
3. καλές στατιστικές ιδιότητες (π.χ., όπως περιγράφονται στο Γεγονός 6.14).

Τονίζουμε ότι οι ιδιότητες αυτές είναι μόνο *αναγκαίες* συνθήκες προκειμένου μια γεννήτρια κλειδορροής να θεωρηθεί κρυπτογραφικά ασφαλής. Αφού δεν είναι γνωστές μαθηματικές αποδείξεις της ασφάλειας τέτοιων γεννητριών μπορούν μόνο να θεωρηθούν *υπολογιστικά α-*

σφαλείς (§ 1.13.3 (iv)) μετά τη διαπίστωση ότι έχουν αντέξει σε εξονυχιστική δημόσια έρευνα.

6.45 Σημείωση (*πολυώνυμο σύνδεσης*) Αφού μια επιθυμητή ιδιότητα για μια γεννήτρια κλειδορροής είναι να έχουν οι ακολουθίες εξόδου μεγάλες περιόδους, οι συνιστώσες LFSR θα πρέπει πάντοτε να επιλέγονται ώστε να είναι LFSR μέγιστου μήκους, δηλαδή οι LFSR θα πρέπει να είναι της μορφής $\langle L, C(D)\rangle$, όπου $C(D) \in \mathbb{Z}_2[D]$ είναι ένα πρωτεύον πολυώνυμο βαθμού L (βλ. Ορισμός 6.13 και Γεγονός 6.12(ii)).

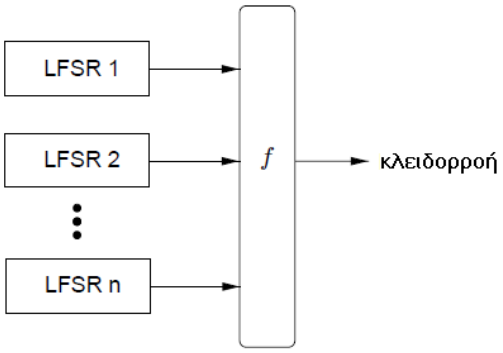
6.46 Σημείωση (*γνωστό πολυώνυμο σύνδεσης και μυστικό πολυώνυμο σύνδεσης*) Οι LFSR σε μια βασισμένη σε LFSR γεννήτρια κλειδορροής μπορεί να έχουν *γνωστά* ή *μυστικά* πολυώνυμα σύνδεσης. Για γνωστές συνδέσεις, το μυστικό κλειδί γενικά συνίσταται στα αρχικά περιεχόμενα των συνιστωσών LFSR. Για μυστικές συνδέσεις, το μυστικό κλειδί για τη γεννήτρια κλειδορροής γενικά συνίσταται και στα αρχικά περιεχόμενα και στις συνδέσεις.

Για τους LFSR μήκους L με μυστικές συνδέσεις, τα πολυώνυμα σύνδεσης θα πρέπει να επιλεγούν ομοιόμορφα στην τύχη απο το σύνολο όλων των πρωτευόντων πολυωνύμων βαθμού L επί του $\mathbb{Z}_2$. Οι μυστικές συνδέσεις γενικά προτείνονται αντί των γνωστών συνδέσεων καθώς οι πρώτες είναι ανθεκτικότερες σε ορισμένες επιθέσεις οι οποίες χρησιμοποιούν προυπολογισμό για την ανάλυση της συγκεκριμένης σύνδεσης, και επειδή οι πρώτες είναι επιδεικτικότερες σε στατιστική ανάλυση. Οι LFSR μυστικής σύνδεσης έχουν το μειονέκτημα ότι απαιτούν υλοποίηση επιπλέον κυκλωμάτων στο υλικό. Όμως, εξαιτίας της επιπλέον ενδεχόμενης ασφάλειας με τις μυστικές συνδέσεις, αυτό το κόστος μπορεί μερικές φορές να αντισταθμιστεί επιλέγοντας βραχύτερους LFSR.

6.47 Σημείωση (*αραιό και πυκνό πολυώνυμο σύνδεσης*) Για τους σκοπούς της υλοποίησης, είναι πλεονεκτικότερο να επιλέξουμε έναν LFSR ο οποίος είναι *αραιός*· δηλαδή μόνο λίγοι από τους συντελεστές του πολυωνύμου σύνδεσης είναι μη μηδενικοί. Τότε μόνο ένας μικρός αριθμός συνδέσεων πρέπει να γίνει μεταξύ των σταδίων του LFSR προκειμένου να υπολογίσουμε το bit ανάδρασης. Π.χ., το πολυώνυμο σύνδεσης μπορεί να επιλεγεί να είναι ένα πρωτεύον τριώνυμο (βλ. Πίνακα 4.8). Όμως, σε ορισμένες βασισμένες σε LFSR γεννήτριες κλειδορροών μπορούν να εξαπολυθούν ειδικές επιθέσεις αν χρησιμοποιούνται αραιά πολυώνυμα σύνδεσης. Άρα, συνιστάται γενικά να μη χρησιμοποιούνται αραιά πολυώνυμα σύνδεσης σε βασισμένες σε LFSR γεννήτριες κλειδορροών.

6.3.1 Γεννήτριες μη γραμμικού συνδυασμού

Μια γενική τεχνική για την καταστροφή της γραμμικότητας που ενυπάρχει στους LFSR είναι να χρησιμοποιούνται αρκετοί LFSR σε παραλληλία. Η κλειδορροή παράγεται ως μια μη γραμμική συνάρτηση f των εξόδων των συνιστωσών LFSR· η κατασκευή αυτή παρουσιάζεται στην Εικόνα 6.8. Τέτοιες γεννήτριες κλειδορροών λέγονται *γεννήτριες μη γραμμικών συνδυασμών* και η f λέγεται *συνδυάζουσα συνάρτηση*. Το υπόλοιπο τμήμα αυτής της υποενότητας καταδεικνύει το γεγονός ότι η συνάρτηση f πρέπει να ικανοποιεί ορισμένα κριτήρια προκειμένου να ανθίσταται σε ορισμένες ειδικού τύπου κρυπτογραφικές επιθέσεις.



Εικόνα 6.8: *Μια γεννήτρια μη γραμμικού συνδυασμού. Η f είναι μια μη γραμμική συνδυάζουσα συνάρτηση.*

6.48 Ορισμός Ένα γινόμενο m διακεκριμένων μεταβλητών λέγεται m-οστής τάξης γινόμενο των μεταβλητών. Κάθε Μπουλιανή συνάρτηση $f(x_1, x_2, \ldots, x_n)$ μπορεί να γραφτεί ως άθροισμα modulo 2 διαφορετικών m-οστής τάξης γινομένων των μεταβλητών της, $0 \le m \le n$· αυτή η έκφραση λέγεται *αλγεβρική κανονική μορφή* της f. Η μη *γραμμική τάξη* της f είναι η μέγιστη των τάξεων των όρων που εμφανίζονται στην αλγεβρική κανονική μορφή της.

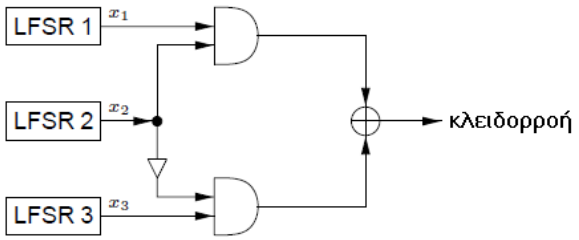
Παραδείγματος χάρη, η Μπουλιανή συνάρτηση $f(x_1, x_2, x_3, x_4, x_5) = 1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3x_4x_5$ έχει μη γραμμική τάξη 4. Να σημειωθεί ότι η μέγιστη δυνατή μη γραμμική τάξη μιας Μπουλιανής συνάρτησης n μεταβλητών είναι n. Το Γεγονός 6.49 καταδεικνύει ότι η ακολουθία εξόδου μιας γεννήτριας μη γραμμικού συνδυασμού έχει υψηλή γραμμική πολυπλοκότητα, με την προϋπόθεση ότι έχει εφαρμοστεί μια συνδυάζουσα συνάρτηση f υψηλής μη γραμμικής τάξης.

6.49 Γεγονός Ας υποθέσουμε ότι n LFSR μέγιστου μήκους, των οποίων τα μήκη $L_1, L_2, \ldots, L_n$ είναι διαφορετικά ανά δύο και μεγαλύτερα του 2, συνδυάζονται με μια γραμμική συνάρτηση $f(x_1, x_2, \ldots, x_n)$ (όπως στη Εικόνα 6.8), η οποία εκφράζεται σε αλγεβρική κανονική μορφή. Τότε η γραμμική πολυπλοκότητα της κλειδορροής είναι $f(L_1, L_2, \ldots, L_n)$. Η έκφραση $f(L_1, L_2, \ldots, L_n)$ αποτιμάται επί των ακεραίων, αντί επί του $\mathbb{Z}_2$).

6.50 Παράδειγμα (*γεννήτρια Geffe*) Η γεννήτρια Geffe, όπως απεικονίζεται στην Εικόνα 6.9, ορίζεται από τρεις LFSR μέγιστου μήκους των οποίων τα μήκη L_1, L_2, L_3 είναι ανά δύο σχετικά πρώτοι, με μη γραμμική συνδυάζουσα συνάρτηση

$$f(x_1, x_2, x_3) = x_1x_2 \oplus (1+ x_2)x_3 = x_1x_2 \oplus x_2x_3 \oplus x_3.$$

Η παραγόμενη κλειδορροή έχει περίοδο $(2^{L_1} - 1)(2^{L_2} - 1)(2^{L_3} - 1)$ και γραμμική πολυπλοκότητα $L = L_1L_2 + L_2L_3 + L_3$.



Εικόνα 6.9: *Η γεννήτρια Geffe.*

Η γεννήτρια Geffe είναι κρυπτογραφικά ασθενής επειδή διαρρέει πληροφορία για τις καταστάσεις των LFSR1 και LFSR2 μέσα στην ακολουθία εξόδου. Για να το δούμε αυτό, έστω ότι $x_1(t)$, $x_2(t)$, $x_3(t)$, $z(t)$ συμβολίζουν τα t-οστά bit εξόδου των LFSR 1, 2, 3 και της κλειδορροής, αντίστοιχα. Τότε η *πιθανότητα συσχέτισης* της ακολουθίας $x_1(t)$ προς την ακολουθία $z(t)$ είναι

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

Παρόμοια, $P(z(t) = x_3(t)) = 3/4$. Για τον λόγο αυτό, παρότι έχει υψηλή περίοδο και μετρίως υψηλή γραμμική πολυπλοκότητα, η γεννήτρια Geffe υποκύπτει σε επιθέσεις συσχέτισης, όπως περιγράφουμε στη Σημείωση 6.51. □

6.51 Σημείωση (*επιθέσεις συσχέτισης*) Ας υποθέσουμε ότι n LFSR μέγιστου μήκους R_1, R_2, …, R_n με μήκη L_1, L_2, …, L_n, αντίστοιχα, χρησιμοποιούνται σε μια γεννήτρια μη γραμμικού συνδυασμού. Αν τα πολυώνυμα σύνδεσης των LFSR και η συνδυάζουσα συνάρτηση f είναι δημόσια γνωστά, τότε το πλήθος των διαφορετικών κλειδιών της γεννήτριας είναι $\prod_{i=1}^{n}(2^{L_i}-1)$. (Ενα κλειδί αποτελείται από τις αρχικές καταστάσεις των LFSR). Υποθέτουμε ότι υπάρχει μια συσχέτιση μεταξύ της κλειδορροής και της ακολουθίας εξόδου του R_1, με πιθανότητα συσχέτισης $p > 1/2$. Αν ένα αρκούντως μεγάλο τμήμα της κλειδορροής είναι γνωστό (π.χ. όπως είναι δυνατό να συμβεί στα πλαίσια μιας επίθεσης γνωστού απλού κειμένου σε έναν δυαδικό προσθετικό κρυπταλγόριθμο ροής), η αρχική κατάσταση του R_1 μπορεί να βρεθεί μετρώντας τον αριθμό των συμπτώσεων μεταξύ της κλειδορροής και όλων των δυνατών μετατοπίσεων της ακολουθίας εξόδου R_1, μέχρι να συμφωνήσει ο αριθμός αυτός με την πιθανότητα συσχέτισης p. Κάτω από αυτές τις συνθήκες, η εύρεση της αρχικής κατάστασης του R_1 θα απαιτήσει το πολύ $2^{L_1}-1$ δοκιμές. Στην περίπτωση που υπάρχει μια συσχέτιση μεταξύ της κλειδορροής και των ακολουθιών εξόδου καθενός από τους R_1, R_2, …, R_n, η (μυστική) αρχική κατάσταση καθενός από τους LFSR μπορεί να προσδιοριστεί ανεξάρτητα, με περίπου $\sum_{i=1}^{n}(2^{L_i}-1)$ δοκιμές συνολικά· ο αριθμός αυτός είναι σημαντικά μικρότερος από το συνολικό πλήθος των διαφορετικών κλειδιών. Με παρόμοιο τρόπο μπορούμε να εκμεταλλευτούμε τις συσχετίσεις μεταξύ των ακολουθιών εξόδου συγκεκριμένων υποσυνόλων των LFSR και της κλειδορροής.

Παίρνοντας υπόψη τη Σημείωση 6.51, η συνδυάζουσα συνάρτηση f θα πρέπει να επιλεγεί προσεκτικά έτσι, ώστε να μην υπάρχει στατιστική εξάρτηση μεταξύ οποιουδήποτε μικρού υποσυνόλου των ακολουθιών των LFSR και της κλειδορροής. Η συνθήκη αυτή μπορεί να ικανοποιηθεί αν η f επιλεγεί να είναι με ανοσία σε συσχέτιση m-οστής τάξης.

6.52 Ορισμός Έστω ότι X_1, X_2,…, X_n είναι ανεξάρτητες δυαδικές μεταβλητές, με κάθε μια να παίρνει τις τιμές 0 ή 1 με πιθανότητα ½. Μια Μπουλιανή συνάρτηση $f(x_1, x_2,\ldots, x_n)$ είναι *με ανοσία σε συσχέτιση m-οστής τάξης* αν για κάθε υποσύνολο των m τυχαίων μεταβλητών X_{i_1}, X_{i_2}, ..., X_{i_m} με $1 \le i_1 < i_2 < \ldots < i_m \le n$, η τυχαία μεταβλητή $Z = f(x_1, x_2,\ldots x_n)$ είναι στατιστικά ανεξάρτητη του τυχαίου διανύσματος $(X_{i_1}, X_{i_2}, \ldots X_{i_m})$· ισοδύναμα, $I = (Z; X_{i_1}, X_{i_2}, \ldots, X_{i_m}) = 0$ (βλ. Ορισμός 2.45).

Παραδείγματος χάρη, η συνάρτηση $f(x_1, x_2,\ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$ είναι με ανοσία σε συσχέτιση $(n-1)$-οστής τάξης. Υπό το φως του Γεγονότος 6.49, το ακόλουθο γεγονός μας δείχνει ότι υπάρχει ένας ανταγωνισμός μεταξύ της επίτευξης υψηλής γραμμικής πολυπλοκότητας και υψηλής ανοσίας σε συσχέτιση με μια συνδυάζουσα συνάρτηση.

6.53 Γεγονός Αν μια Μπουλιανή συνάρτηση $f(x_1, x_2,\ldots, x_n)$ είναι με ανοσία σε συσχέτιση m-οστής τάξης, όπου $1 \le m \le n$, τότε η μη γραμμική τάξη της συνάρτησης f είναι το πολύ $n - m$. Επιπλέον, αν η f είναι *ισοσταθμισμένη* (δηλ. ακριβώς οι μισές από τις τιμές εξόδου της f είναι 0) τότε η μη γραμμική τάξη της f είναι το πολύ $n - m - 1$, για $1 \le m \le n - 2$.

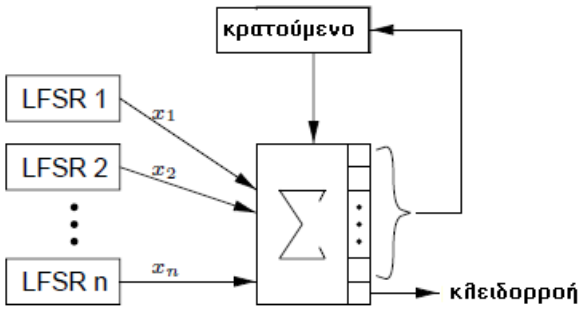
Ο ανταγωνισμός μεταξύ της υψηλής γραμμικής πολυπλοκότητας και υψηλής ανοσίας σε συσχέτιση μπορεί να αποφευχθεί επιτρέποντας να έχει *μνήμη* η μη γραμμική συνδυάζουσα συνάρτηση f. Επεξηγούμε αυτό το σημείο με τη γεννήτρια άθροισης.

6.54 Παράδειγμα (*γεννήτρια άθροισης*) Η συνδυάζουσα συνάρτηση στη γεννήτρια άθροισης βασίζεται στο γεγονός ότι η πρόσθεση ακεραίων, όταν ιδωθεί στο $\mathbb{Z}_2$, είναι μια μη γραμμική συνάρτηση με μνήμη της οποίας η ανοσία σε συσχέτιση είναι μέγιστη. Για να το δούμε αυτό στην περίπτωση που είναι $n = 2$, έστω ότι $a = a_{m-1}2^{m-1} + \ldots + a_1 2 + a_0$ και $b = b_{m-1}2^{m-1} + \ldots + b_1 2 + b_0$ είναι οι δυαδικές αναπαραστάσεις δύο ακεραίων a και b.Τότε τα bit του $z = a + b$ δίνονται από τον αναδρομικό τύπο

$$\begin{aligned} z_j &= f_1(a_j, b_j, c_{j-1}) = a_j \oplus b_j \oplus c_{j-1} \quad 0 \le j \le m \\ c_j &= f_2(a_j, b_j, c_{j-1}) = a_j b_j \oplus (a_j \oplus b_j)c_{j-1}, \quad 0 \le j \le m-1 \end{aligned}$$

όπου c_j είναι το κρατούμενο bit και $c_{-1} = a_m = b_m = 0$. Να σημειωθεί ότι η f είναι με ανοσία σε συσχέτιση $2^{\eta\varsigma}$ τάξης, ενώ f_2 είναι μη γραμμική συνάρτηση *χωρίς μνήμη*. Το κρατούμενο bit c_{j-1} μεταφέρει όλη τη μη γραμμική επιρροή των λιγότερων σημαντικών bit των a και b (δηλαδή των $a_{j-1}, \ldots, a_1, a_0$ και $b_{j-1}, \ldots, b_1, b_0$).

Η γεννήτρια άθροισης, όπως απεικονίζεται στην Εικόνα 6.10, ορίζεται από τους LFSR μέγιστου μήκους των οποίων τα μήκη $L_1, L_2, \ldots, L_n$ είναι ανά δύο σχετικά πρώτοι.



Εικόνα 6.10: *Η γεννήτρια άθροισης.*

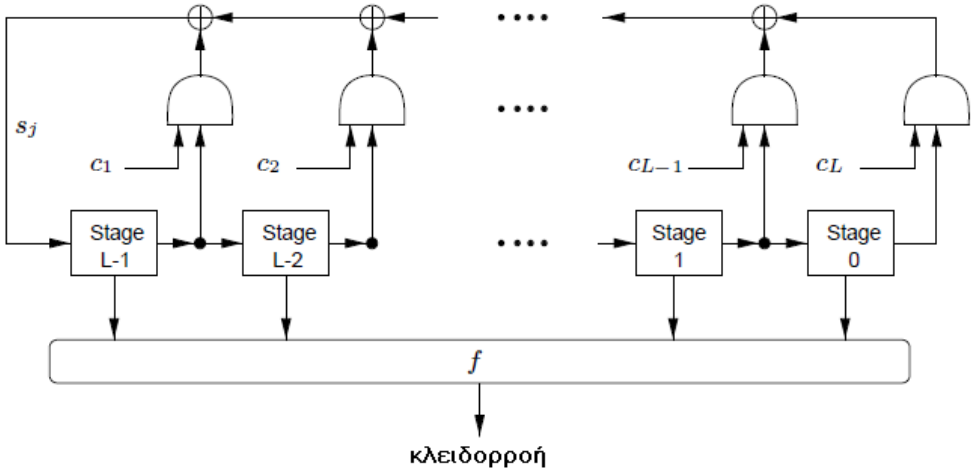
Το μυστικό κλειδί αποτελείται από τις αρχικές καταστάσεις των LFSR, και ένα αρχικό (ακέραιο) κρατούμενο C_0. Η κλειδορροή παράγεται ως εξής. Τη χρονική στιγμή j, $(j \ge 1)$ οι LFSR βηματίζουν παράγοντας τα bit εξόδου $x_1, x_2, \ldots, x_n$ και υπολογίζεται το άθροισμα *ακεραίων* $S_j = \sum_{i=1}^{n} x_i + C_{j-1}$. Το bit κλειδορροής είναι $S_j \bmod 2$ (το λιγότερο σημαντικό bit του

S_j). Η περίοδος της κλειδορροής είναι $\prod_{i=1}^{n}(2^{L_i}-1)$, ενώ η γραμμική πολυπλοκότητά της είναι κοντά στον αριθμό αυτό.

Αν και η γεννήτρια άθροισης έχει υψηλή περίοδο, γραμμική πολυπλοκότητα και ανοσία σε συσχέτιση, είναι ευάλωτη σε ορισμένες επιθέσεις συσχέτισης και σε μια επίθεση γνωστού απλού κειμένου που βασίζεται στο 2-adic πλάτος (span) (βλ. σελ.31).

6.3.2 Γεννήτριες μη γραμμικού φίλτρου

Μια άλλη γενική τεχνική για την καταστροφή της γραμμικότητας που ενυπάρχει στους LFSR είναι να παράγουμε την κλειδορροή σαν κάποια μη γραμμική συνάρτηση των σταδίων ενός μεμονωμένου LFSR· η κατασκευή αυτή παρουσιάζεται στην Εικόνα 6.11. Τέτοιες γεννήτριες κλειδορροών λέγονται *γεννήτριες μη γραμμικού φίλτρου* και η f λέγεται *συνάρτηση διήθησης*.



Εικόνα 6.11: *Μια γεννήτρια μη γραμμικού φίλτρου. Η f είναι μια μη γραμμική Μπουλιανή συνάρτηση διήθησης.*

Το Γεγονός 6.55 περιγράφει τη γραμμική πολυπλοκότητα της ακολουθίας εξόδου μιας γεννήτριας μη γραμμικού φίλτρου.

6.55 Γεγονός Ας υποθέσουμε ότι έχουμε κατασκευάσει μια γεννήτρια μη γραμμικού φίλτρου χρησιμοποιώντας έναν LFSR μέγιστου μήκους με μήκος L και μια συνάρτηση διήθησης f μη γραμμικής τάξης m (όπως στη Εικόνα 6.11).

(i) (*Φράγμα του κλειδιού*) Η γραμμική πολυπλοκότητα της κλειδορροής είναι το πολύ $L_m = \sum_{i=1}^{m}\binom{L}{i}$.

(ii) Για έναν συγκεκριμένο LFSR μέγιστου μήκους με μήκος τον πρώτο L, το κλάσμα των Μπουλιανών συναρτήσεων f μη γραμμικής τάξης m που παράγουν ακολουθίες μέγιστης γραμμικής πολυπλοκότητας L_m είναι

$$P_m \approx \exp(-L_m/(L\cdot 2^L)) > e^{-1/L}.$$

Επομένως, για μεγάλο L, οι περισσότερες από τις γεννήτριες παράγουν ακολουθίες των οποίων η γραμμική πολυπλοκότητα ικανοποιεί το άνω φράγμα που αναφέρεται στο (i).

Η μη γραμμική συνάρτηση f που επιλέγουμε για μια γεννήτρια φίλτρου θα πρέπει να περιλαμβάνει πολλούς όρους, με τον καθένα να έχει τάξη που δεν υπερβαίνει τη μη γραμμική τάξη της f.

6.56 Παράδειγμα (*γεννήτρια σακιδίου*) Η γεννήτρια κλειδορροής σακιδίου ορίζεται από έναν LFSR μέγιστου μήκους $\langle L, C(D)\rangle$ και ένα modulus $Q = 2^L$. Το μυστικό κλειδί αποτελείται από L ακέραια βάρη σακιδίου $\alpha_1, \alpha_2, \ldots, \alpha_L$ δυαδικού μήκους L το καθένα, και την αρχική κατάσταση LFSR. Υπενθυμίζουμε ότι το πρόβλημα αθροίσματος υποσυνόλου (§3.10) είναι ο προσδιορισμός ενός υποσυνόλου των βαρών σακιδίου με άθροισμα (που έχουν άθροισμα) έναν δεδομένο ακέραιο s, με την προϋπόθεση ότι ένα τέτοιο υποσύνολο υπάρχει· το πρόβλημα αυτό είναι **NP**-δύσκολο (Γεγονός 3.91). Η κλειδορροή παράγεται ως εξής: τη χρονική στιγμή j ο LFSR βηματίζει και υπολογίζεται το άθροισμα σακιδίου $S_j = \sum_{i=1}^{L} x_i a_i \bmod Q$, όπου $[x_L, \ldots, x_2, x_1]$ είναι η κατάσταση του LFSR τη χρονική στιγμή j. Τελικά, εξάγονται επιλεγμένα bit του S_j (μετά τη μετατροπή του S_j στη δυαδική του αναπαράσταση) προκειμένου να αποτελέσουν ένα τμήμα της κλειδορροής (τα $\lceil \lg L \rceil$ λιγότερο σημαντικά bit του S_j θα πρέπει να παραλειφθούν). Η γραμμική πολυπλοκότητα της κλειδορροής είναι τότε στην πραγματικότητα σίγουρο ότι είναι $L(2^L - 1)$.

Αφού η κατάσταση ενός LFSR είναι ένα δυαδικό διάνυσμα, η συνάρτηση που απεικονίζει την κατάσταση του LFSR στο άθροισμα σακιδίου S_j είναι όντως μη γραμμική. Συγκεκριμένα, έστω ότι η συνάρτηση f ορίζεται από την $f(x) = \sum_{i=1}^{L} x_i a_i \bmod Q$, όπου $[x_L, \ldots, x_2, x_1]$ είναι μια κατάσταση. Αν x και y είναι δύο καταστάσεις τότε, γενικά, $f(x \oplus y) \neq f(x) + f(y)$. □

6.3.3 Γεννήτριες ρυθμιζόμενες με ρολόι

Σε γεννήτριες μη γραμμικού συνδυασμού και σε γεννήτριες μη γραμμικού φίλτρου, οι συνιστώσες LFSR χρονίζονται κανονικά· δηλαδή η κίνηση των δεδομένων σε όλους τους LFSR ρυθμίζεται με το ίδιο ρολόι. Η κύρια ιδέα πίσω από μια *γεννήτρια ρυθμιζόμενη με ρολόι* είναι να εισαγάγουμε μη γραμμικότητα στις γεννήτριες κλειδορροών που βασίζονται σε LFSR, έχοντας την έξοδο ενός LFSR να ελέγχει τον *χρονισμό* (δηλ. τον βηματισμό) ενός δεύτερου LFSR. Αφού ο δεύτερος LFSR χρονίζεται κατά έναν *μη κανονικό* τρόπο, ελπίζουμε ότι επιθέσεις που βασίζονται στην κανονική κίνηση των LFSR μπορεί να αποτύχουν. Στην υποενότητα αυτή περιγράφουμε δυο γεννήτριες που ρυθμίζονται με ρολόι: (i) η γεννήτρια εναλλασσόμενου βήματος και (ii) η γεννήτρια συρρίκνωσης.

(i) Η γεννήτρια εναλλασσόμενου βήματος

Η γεννήτρια εναλλασσόμενου βήματος χρησιμοποιεί έναν LFSR R_1 για να ρυθμίζει τον βηματισμό δύο LFSR, των R_2 και R_3. Η κλειδορροή που παράγεται είναι η XOR των ακολουθιών εξόδου των R_2 και R_3.

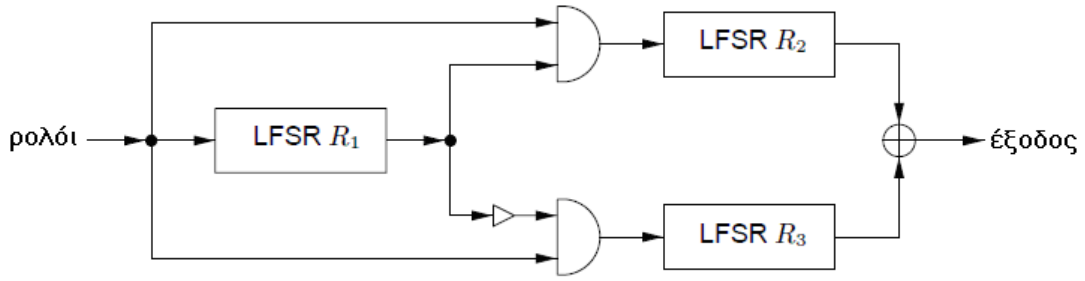
6.57 Αλγόριθμος Γεννήτρια εναλλασσόμενου βήματος

ΠΕΡΙΛΗΨΗ: ένας LFSR ρύθμισης R_1 χρησιμοποιείται για να βηματίζει επιλεκτικά δύο άλλους LFSR, R_2 και R_3.
ΕΞΟΔΟΣ: μια ακολουθία η οποία είναι η XOR ανά bit των ακολουθιών εξόδου των R_2 και R_3.

Τα ακόλουθα βήματα επαναλαμβάνονται μέχρι να παραχθεί μια κλειδορροή επιθυμητού μήκους.

1. Ο καταχωρητής R_1 χρονίζεται.
2. Αν η έξοδος του R_1 είναι 1 τότε:
   Ο R_2 χρονίζεται· ο R_3 δεν χρονίζεται αλλά το προηγούμενο bit εξόδου του επαναλαμβάνεται.
   (Για τον πρώτο κύκλο ρολογιού, "το προηγούμενο bit εξόδου" του R_3 θεωρείται ότι είναι 0.)
3. Αν η έξοδος του R_1 είναι 0 τότε:
   Ο R_3 χρονίζεται· ο R_2 δεν χρονίζεται αλλά το προηγούμενο bit εξόδου του επαναλαμβάνεται.
   (Για τον πρώτο κύκλο ρολογιού, "το προηγούμενο bit εξόδου" του R_2 θεωρείται ότι είναι 0.)
3. Τα bit εξόδου των R_3 και R_2 υπόκεινται σε XOR· το bit που προκύπτει είναι μέρος της κλειδορροής.

Τυπικότερα, έστω ότι οι ακολουθίες εξόδου των LFSR R_1, R_2 και R_3 είναι $\alpha_0, \alpha_1, \alpha_2, \ldots, b_0, b_1, b_2, \ldots, c_0, c_1, c_2, \ldots$, αντίστοιχα. Ορίζουμε $b_{-1} = c_{-1} = 0$. Τότε η κλειδορροή που παράγεται από τη γεννήτρια εναλλασσόμενου βήματος είναι $x_0, x_1, x_2, \ldots$, όπου $x_j = b_{t(j)} \oplus c_{j-t(j)-1}$ και $t(j) = (\sum_{i=1}^{m} a_i) - 1$ για κάθε $j \geq 0$. Η γεννήτρια εναλλασσόμενου βήματος απεικονίζεται στην Εικόνα 6.12.



Εικόνα 6.12: *Η γεννήτρια εναλλασσόμενου βήματος.*

6.58 Παράδειγμα (*γεννήτρια εναλλασσόμενου βήματος με τεχνηέντως μικρές παραμέτρους*) Θεωρούμε μια γεννήτρια εναλλασσόμενου βήματος με συνιστώσες LFSR τους $R_1 = \langle 3, 1 + D^2 + D^3 \rangle$, $R_2 = \langle 4, 1 + D^3 + D^4 \rangle$ και $R_3 = \langle 5, 1 + D^3 + D^4 + D^5 \rangle$. Υποθέτουμε ότι οι αρχικές καταστάσεις των R_1, R_2 και R_3 είναι [0,0,1], [1,0,1,1] και [0,1,0,0,1], αντίστοιχα.

Η ακολουθία εξόδου του R_1 είναι ακολουθία περιόδου 7, με κύκλο

$$\alpha^7 = 1, 0, 0, 1, 0, 1, 1.$$

Η ακολουθία εξόδου του R_2 είναι ακολουθία περιόδου 15, με κύκλο

$$b^{15} = 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0.$$

Η ακολουθία εξόδου του R_3 είναι ακολουθία περιόδου 31, με κύκλο

$$c^{31} = 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0.$$

Η κλειδορροή που παράγεται είναι

x = 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, …. □

Το Γεγονός 6.59 αποδεικνύει, με την υπόθεση ότι ο R_1 παράγει ακολουθία de Bruign (βλ. Ορισμός 6.40), ότι η ακολουθία εξόδου μιας γεννήτριας εναλλασσόμενου βήματος ικανοποιεί τις βασικές απαιτήσεις υψηλής περιόδου, υψηλής γραμμικής πολυπλοκότητας και καλών στατιστικών ιδιοτήτων.

6.59 Γεγονός (*ιδιότητες της γεννήτριας εναλλασσόμενου βήματος*) Ας υποθέσουμε ότι ο R_1 παράγει μια ακολουθία de Bruijn 2^{L_1}. Επιπλέον, υποθέτουμε ότι οι R_2 και R_3 είναι LFSR μέγιστου μήκους, με μήκη L_2 και L_3, αντίστοιχα, τέτοια ώστε $\gcd(L_2, L_3) = 1$. Έστω x η ακολουθία εξόδου της γεννήτριας εναλλασσόμενου βήματος από τους R_1, R_2 και R_3.

(i) Η ακολουθία x έχει περίοδο $2^{L_1} \cdot (2^{L_2} - 1) \cdot (2^{L_3} - 1)$.

(ii) Η γραμμική πολυπλοκότητα $L(x)$ της x ικανοποιεί τη διπλή ανισότητα

$$(L_2 + L_3) \cdot 2^{L_1 - 1} < L(x) \leq \cdot (L_2 + L_3) \cdot 2^{L_1}.$$

(iii) Η κατανομή των προτύπων στη x είναι σχεδόν ομοιόμορφη. Ακριβέστερα, έστω P μια δυαδική συμβολοσειρά μήκους t bit, όπου $t \leq \min(L_2, L_3)$. Αν $x(t)$ συμβολίζει t διαδοχικά bit στη x, τότε η πιθανότητα να είναι $x(t) = P$, είναι

$$(1/2)^t + O(1/2^{L_2 - t}) + O(1/2^{L_3 - t}).$$

Αφού μια ακολουθία de Bruijn μπορεί να ληφθεί από την ακολουθία εξόδου s ενός LFSR μέγιστου μήκους (με μήκος L) προσθέτοντας απλά ένα 0 στο τέλος κάθε υπακολουθίας των $L - 1$ μηδενικών που εμφανίζονται στην s (βλ. Σημείωση 6.43), είναι εύκολο να περιμένουμε ότι οι ισχυρισμοί υψηλής περιόδου, υψηλής γραμμικής πολυπλοκότητας και καλών στατιστικών ιδιοτήτων στο Γεγονός 6.59 ισχύουν επίσης όταν R_1 είναι ένας LFSR μέγιστου μήκους. Να σημειωθεί, όμως, ότι αυτό δεν έχει ακόμη αποδειχθεί.

6.60 Σημείωση (*ασφάλεια της γεννήτριας εναλλασσόμενου βήματος*) Οι LFSR R_1, R_2 και R_3 θα πρέπει να επιλεγούν ώστε να είναι LFSR μέγιστου μήκους με μήκη L_1, L_2 και L_3 που είναι ανά δυο σχετικά πρώτοι: $\gcd(L_1, L_2) = 1$, $\gcd(L_2, L_3) = 1$, $\gcd(L_1, L_3) = 1$. Επιπλέον τα μήκη θα πρέπει να είναι περίπου ίδια. Αν $L_1 \approx l$, $L_2 \approx l$ και $L_3 \approx l$, η καλύτερη γνωστή επίθεση στη γεννήτρια εναλλασσόμενου βήματος είναι μια επίθεση διαίρει-και-βασίλευε στον καταχωρητή ρύθμισης R_1, η οποία απαιτεί 2^l βήματα κατά προσέγγιση. Έτσι, αν $l \approx 128$, η γεννήτρια είναι ασφαλής έναντι των γνωστών, προς το παρόν, επιθέσεων.

(ii) Η γεννήτρια συρρίκνωσης

Η γεννήτρια συρρίκνωσης είναι μια σχετικά νέα γεννήτρια κλειδορροής, η οποία έχει προταθεί το 1993. Ωστόσο, εξαιτίας της απλότητάς της και των αποδείξιμων ιδιοτήτων της, είναι μια πολλά υποσχόμενη υποψήφια για εφαρμογές κρυπτογράφησης υψηλής ταχύτητας. Στη γεννήτρια συρρίκνωσης χρησιμοποιείται ένας LFSR ρύθμισης R_1 για να συλλέγει ένα μέρος της ακολουθίας εξόδου ενός δεύτερου LFSR R_2. Η κλειδορροή που παράγεται είναι, επομένως, μια *συρρικνωμένη* εκδοχή (γνωστή επίσης ως μια *ακανόνιστα αποδεκατισμένη υπακολουθία*) της ακολουθίας εξόδου R_2, όπως καθορίζεται στον Αλγόριθμο 6.61 και απεικονίζεται στην Εικόνα 6.13.

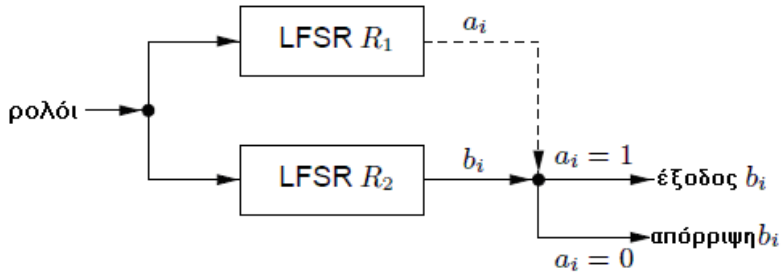
6.61 Αλγόριθμος Γεννήτρια συρρίκνωσης

ΠΕΡΙΛΗΨΗ: ένας LFSR ρύθμισης R_1 χρησιμοποιείται για να ρυθμίζει την έξοδο ενός δευτέρου LFSR R_2.

Τα ακόλουθα βήματα επαναλαμβάνονται μέχρι να παραχθεί μια κλειδορροή επιθυμητού μήκους.

1. Οι καταχωρητές R_1 και R_2 χρονίζονται.
2. Αν η έξοδος του R_1 είναι 1, το bit εξόδου του R_2 αποτελεί μέρος της κλειδορροής.
3. Αν η έξοδος του R_1 είναι 0, το bit εξόδου του R_2 απορρίπτεται.

Τυπικότερα, έστω ότι οι ακολουθίες εξόδου των LFSR R_1 και R_2 είναι $a_0, a_1, a_2, \ldots$, και $b_0, b_1, b_2, \ldots$, αντίστοιχα. Τότε η κλειδορροή που παράγεται από τη γεννήτρια συρρίκνωσης είναι $x_0, x_1, x_2, \ldots$, όπου $x_j = b_{i_j}$ και για κάθε $j \geq 0$, i_j είναι η θέση του j-οστού 1 στην ακολουθία $a_0, a_1, a_2, \ldots$.



Εικόνα 6.13: *Η γεννήτρια συρρίκνωσης*

6.62 Παράδειγμα (*γεννήτρια συρρίκνωσης με τεχνηέντως μικρές παραμέτρους*) Θεωρούμε μια γεννήτρια συρρίκνωσης με συνιστώσες LFSR τους $R_1 = \langle 3, 1 + D + D^3 \rangle$, $R_2 = \langle 5, 1 + D^3 + D^5 \rangle$. Υποθέτουμε ότι οι αρχικές καταστάσεις των R_1 και R_2 είναι [1,0,0] και [0,0,1,0,1], αντίστοιχα. Η ακολουθία εξόδου του R_1 είναι ακολουθία περιόδου 7, με κύκλο

$$a^7 = 0, 0, 1, 1, 1, 0, 1$$

ενώ η ακολουθία εξόδου του R_2 είναι ακολουθία περιόδου 31, με κύκλο

$$b^{31} = 1,0,1,0,0,0,0,1,0,0,1,0,1,1,0,0,1,1,1,1,1,0,0,0,1,1,0,1,1,1,0.$$

Η κλειδορροή που παράγεται είναι

$$x = 1,0,0,0,0,1,0,1,1,1,1,1,0,1,1,1,0,\ldots.$$

□

Το Γεγονός 6.63 αποδεικνύει ότι η ακολουθία εξόδου μιας γεννήτριας συρρίκνωσης ικανοποιεί τις βασικές απαιτήσεις υψηλής περιόδου, υψηλής γραμμικής πολυπλοκότητας και καλών στατιστικών ιδιοτήτων.

6.63 Γεγονός (*ιδιότητες της γεννήτριας συρρίκνωσης*) Έστω ότι R_1 και R_2 είναι LFSR μέγιστου μήκους, με μήκη L_1 και L_2, αντίστοιχα, και έστω x μια ακολουθία εξόδου της γεννήτριας συρρίκνωσης που σχηματίζεται από τους R_1 και R_2.

(i) Αν $\gcd(L_2, L_3) = 1$, τότε η x έχει περίοδο $(2^{L_2} - 1) \cdot 2^{L_1 - 1}$.

(ii) Η γραμμική πολυπλοκότητα $L(x)$ της x ικανοποιεί τη διπλή ανισότητα

$$L_2 \cdot 2^{L_1 - 2} < L(x) \leq L_2 \cdot 2^{L_1 - 1}.$$

(iii) Ας υποθέσουμε ότι τα πολυώνυμα σύνδεσης για τους R_1 και R_2 επιλέγονται ομοιόμορφα στην τύχη από το σύνολο όλων των πρωτευόντων πολυωνύμων βαθμού L_1 και L_2, αντίστοιχα, επί του $\mathbb{Z}_2$. Τότε η κατανομή των προτύπων στη x είναι σχεδόν ομοιόμορφη. Ακριβέστερα, αν P είναι μια δυαδική συμβολοσειρά μήκους t bit και $x(t)$ συμβολίζει t διαδοχικά bit στη x, τότε η πιθανότητα να είναι $x(t) = P$, είναι

$$(1/2)^t + O(t/2^{L_2}).$$

6.64 Σημείωση (*ασφάλεια της γεννήτριας εναλλασσόμενου βήματος*) Υποθέτουμε ότι οι LFSR R_1 και R_2 που είναι συνιστώσες της γεννήτριας συρρίκνωσης έχουν μήκη L_1 και L_2, αντίστοιχα. Αν τα πολυώνυμα σύνδεσης για τους R_1 και R_2 είναι γνωστά (αλλά τα αρχικά περιεχόμενα των R_1 και R_2 δεν είναι), η καλύτερη γνωστή επίθεση για ανάκτηση του μυστικού κλειδιού απαιτεί $O(2^{L_1} \cdot L_2^3)$ βήματα. Από την άλλη μεριά, αν χρησιμοποιηθούν μυστικά (και μεταβλητά) πολυώνυμα σύνδεσης, η καλύτερη γνωστή επίθεση απαιτεί $O(2^{L_1} \cdot L_1 \cdot L_2)$ βήματα. Υπάρχει επίσης μια επίθεση μέσω της γραμμικής πολυπλοκότητας της γεννήτριας συρρίκνωσης η οποία απαιτεί $O(2^{L_1} \cdot L_2^2)$ βήματα (ανεξάρτητα από το εάν οι συνδέσεις είναι γνωστές ή μυστικές), αλλά η επίθεση αυτή απαιτεί $2^{L_1} \cdot L_2$ διαδοχικά bit από την ακολουθία εξόδου και είναι, επομένως, ανέφικτη για μετρίως μεγάλα L_1 και L_2. Για μέγιστη ασφάλεια, οι R_1 και R_2 θα πρέπει να είναι LFSR μέγιστου μήκους και τα μήκη τους θα πρέπει να ικανοποιούν τη σχέση $\gcd(L_1, L_2) = 1$. Επιπλέον, θα πρέπει να χρησιμοποιηθούν μυστικές συνδέσεις. Υποκείμενη σε αυτούς τους περιορισμούς, αν $L_1 \approx l$, $L_2 \approx l$, η γεννήτρια συρρίκνωσης έχει ένα επίπεδο ασφάλειας προσεγγιστικά ίσο με 2^{2l}. Έτσι, αν $L_1 \approx 64$ και $L_2 \approx 64$, η γεννήτρια εμφανίζεται να είναι ασφαλής έναντι όλων των, επί του παρόντος, γνωστών επιθέσεων.

6.4 Άλλοι κρυπταλγόριθμοι ροής

Ενώ οι βασισμένοι σε LFSR κρυπταλγόριθμοι ροής που εξετάσαμε στην §6.3 αρμόζουν σε υλοποιήσεις υλικού, δεν είναι επιδεκτικοί σε υλοποιήσεις λογισμικού. Αυτό έχει ως αποτέλεσμα να διατυπωθούν πρόσφατα διάφορες προτάσεις για κρυπταλγόριθμους ροής που είναι σχεδιασμένοι ειδικότερα για γρήγορες υλοποιήσεις λογισμικού. Οι περισσότερες προτάσεις είναι είτε ιδιωτικές (χρησιμοποιούνται κατά αποκλειστικότητα), είτε είναι σχετικά νέες και δεν έχουν υποστεί εξονυχιστικό έλεγχο από την κρυπτογραφική κοινότητα· για τον λόγο αυτό δεν τις παρουσιάζουμε στην ενότητα αυτή, αλλά αντίθετα τις αναφέρουμε μόνο στις σημειώσεις στο τέλος του κεφαλαίου, στη σελίδα 36.

Δύο πολλά υποσχόμενοι κρυπταλγόριθμοι ροής σχεδιασμένοι ειδικά για γρήγορη υλοποίηση λογισμικού είναι οι SEAL και RC4. Παρουσιάζουμε τον SEAL στην §6.4.1. Ο RC4 χρησιμοποιείται σε εμπορικά προϊόντα και έχει ένα μεταβλητό μέγεθος κλειδιού, αλλά παραμένει ιδιωτικός και δεν τον παρουσιάζουμε εδώ. Δύο άλλοι ευρέως χρησιμοποιούμενοι κρυπταλγόριθμοι ροής που δεν βασίζονται σε LFSR είναι οι τρόποι λειτουργίας OFB (Output Feedback – Ανάδραση Εξόδου, βλ. §7.2.2(iv)) και CFB (Cipher Feedback – Ανάδραση κρυπταλγόριθμου, βλ. §7.2.2(iii)) των κρυπταλγόριθμων τμήματος. Μια άλλη κλάση γεννητριών κλειδορροών που δεν βασίζονται σε LFSR είναι εκείνες των οποίων η ασφάλεια εναπόκειται στο δυσεπίλυτο ενός υποκείμενου αριθμοθεωρητικού προβλήματος· οι γεννήτριες αυτές είναι πολύ πιο αργές από εκείνες που βασίζονται σε LFSR και τις εξετάζουμε στην §5.5.

6.4.1 SEAL

Ο SEAL (Software-optimized Encryption Algorithm) είναι ένας δυαδικός προσθετικός κρυπταλγόριθμος ροής (βλ. Ορισμός 6.4) ο οποίος προτάθηκε το 1993. Επειδή είναι σχετικά νέος, δεν έχει υποστεί εξονυχιστική έρευνα από την κρυπτογραφική κοινότητα. Τον παρουσιάζουμε όμως εδώ επειδή είναι ένας από τους λίγους κρυπταλγόριθμους ροής που σχεδιάστηκε ειδικά για αποδοτικές υλοποιήσεις λογισμικού και, ειδικότερα, για επεξεργαστές 32-bit.

Ο SEAL είναι μια ψευδοτυχαία συνάρτηση που αυξάνει το μήκος και η οποία απεικονίζει έναν αριθμό ακολουθίας n 32-bit σε μία κλειδορροή L-bit υπό τον έλεγχο ενός μυστικού κλειδιού a 160-bit. Στο στάδιο της προ-επεξεργασίας (βήμα 1 του Αλγορίθμου 6.68), το κλειδί επιμηκύνεται σε μεγαλύτερους πίνακες χρησιμοποιώντας τη συνάρτηση παραγωγής πίνακα G_a που καθορίζεται στον Αλγόριθμο 6.67· η συνάρτηση αυτή βασίζεται στον Secure Hash Algorithm (Ασφαλής Αλγόριθμος Διασποράς) SHA-1 (Αλγόριθμος 9.53). Ως επακόλουθο αυτής της προ-επεξεργασίας, η παραγωγή της κλειδορροής απαιτεί 5 εντολές μηχανής ανά byte και είναι μια τάξη μεγέθους ταχύτερη απ' ότι ο DES (Αλγόριθμος 7.82).

Ο ακόλουθος συμβολισμός χρησιμοποιείται στον SEAL για τις ποσότητες 32-bit A, B, C, D, X_i και Y_j:

- $\overline{A}$: συμπλήρωμα ανά bit του A
- $A \wedge B$, $A \vee B$, $A \oplus B$: ανά bit AND, περιεκτικό OR, αποκλειστικό OR
- "$A \hookleftarrow s$": αποτέλεσμα 32-bit της περιστροφής του A στα αριστερά μέσω s θέσεων
- "$A \hookrightarrow s$": αποτέλεσμα 32-bit της περιστροφής του A στα δεξιά μέσω s θέσεων
- $A + B$: άθροισμα mod 2^{32} των μη προσημασμένων ακεραίων A και B
- $f(B,C,D) \stackrel{def}{=} (B \wedge C) \vee (\overline{B} \wedge D)$ · $g(B,C,D) \stackrel{def}{=} (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ · $h(B,C,D) \stackrel{def}{=} B \oplus C \oplus D$
- $A||B$: συνένωση των A και B
- $(X_1, \ldots, X_j) \leftarrow (Y_1, \ldots, Y_j)$: ταυτόχρονες αναθέσεις $(X_i \leftarrow Y_i)$, όπου η $(Y_1, \ldots, Y_j)$ υπολογίζεται πριν από οποιαδήποτε ανάθεση.

6.65 Σημείωση (*SEAL 1.0 και SEAL 2.0*) Η συνάρτηση παραγωγής πίνακα (Αλγόριθμος 6.67) για την πρώτη εκδοχή του SEAL βασίζεται στον Secure Hash Algorithm (SHA). Ο SEAL 2.0 διαφέρει από τον SEAL 1.0 ως προς το ότι η συνάρτηση παραγωγής πίνακα για τον πρώτο βασίζεται στον τροποποιημένο Hash Algorithm SHA-1 (Αλγόριθμος 9.53).

6.66 Σημείωση (*πίνακες*) Η παραγωγή πίνακα (βήμα 1 του Αλγορίθμου 6.68) χρησιμοποιεί τη συνάρτηση συμπίεσης του SHA-1 για να αναπτύξει το μυστικό κλειδί a σε μεγαλύτερους πίνακες T, S και R. Αυτοί οι πίνακες μπορούν να προϋπολογιστούν, αλλά μετά την εδραίωση του μυστικού κλειδιού a. Οι πίνακες T και S είναι μεγέθους 2K byte και 1K byte, αντίστοιχα. Το μέγεθος του πίνακα R εξαρτάται από το επιθυμητό δυαδικό μήκος L της κλειδορροής — κάθε 1K byte της κλειδορροής απαιτεί 16 byte του R.

6.67 Αλγόριθμος Συνάρτηση παραγωγής πίνακα για τον SEAL 2.0

$G_a(i)$

ΕΙΣΟΔΟΣ: μια συμβολοσειρά 160-bit a και ένας ακέραιος i, $0 \le i < 2^{32}$.

ΕΞΟΔΟΣ: μια συμβολοσειρά 160-bit, συμβολικά $G_a(i)$.

1. *Ορισμός σταθερών*. Ορισμός τεσσάρων σταθερών 32-bit (στο δεκαεξαδικό): y_1 = 0x5a827999, y_2 = 0x6ed9eba1, y_3 = 0x8f1bbcdc, y_4 = 0xca62c1d6.
2. Συνάρτηση παραγωγής πίνακα.
   (*αρχικοποίηση 80 λέξεων 32-bit* $X_0, X_1, \ldots, X_{79}$)
   Ανάθεση $X_0 \leftarrow i$. **for** j από 1 έως 15 **do** $X_j \leftarrow$ 0x00000000.
   for j από 16 έως 79 **do** $X_j \leftarrow ((X_{j-3} \oplus X_{j-8} \oplus X_{j-14} \oplus X_{j-16}) \lll 1)$.
   (*αρχικοποίηση μεταβλητών εργασίας*)
   Διάσπαση της συμβολοσειράς 160-bit a σε πέντε λέξεις 32-bit: $a = H_0H_1H_2H_3H_4$.
   $(A, B, C, D, E) \leftarrow (H_0, H_1, H_2, H_3, H_4)$.
   (*εκτέλεση τεσσάρων γύρων των 20 βημάτων, μετά ανανέωση· t είναι μια πρόσκαιρη μεταβλητή*)
   (*Γύρος 1*) **for** j από 0 έως 19 **do**
   $t \leftarrow ((A \lll 5) + f(B, C, D) + E + X_j + y_1)$,
   $(A, B, C, D, E) \leftarrow (t, A, B \lll 30, C, D)$.
   (*Γύρος 2*) **for** j από 20 έως 39 **do**
   $t \leftarrow ((A \lll 5) + h(B, C, D) + E + X_j + y_2)$,
   $(A, B, C, D, E) \leftarrow (t, A, B \lll 30, C, D)$.
   (*Γύρος 3*) **for** j από 40 έως 59 **do**
   $t \leftarrow ((A \lll 5) + g(B, C, D) + E + X_j + y_3)$,
   $(A, B, C, D, E) \leftarrow (t, A, B \lll 30, C, D)$.
   (*Γύρος 4*) **for** j από 60 έως 79 **do**
   $t \leftarrow ((A \lll 5) + h(B, C, D) + E + X_j + y_4)$,
   $(A, B, C, D, E) \leftarrow (t, A, B \lll 30, C, D)$.
   (*ανανέωση αλληλουχίας τιμών*)
   $(H_0, H_1, H_2, H_3, H_4) \leftarrow (H_0 + A, H_1 + B, H_2 + C, H_3 + D, H_4 + E)$.
   (*ολοκλήρωση*) Η τιμή της $G_a(i)$ είναι η συμβολοσειρά 160-bit $H_0||H_1||H_2||H_3||H_4$.

6.68 Αλγόριθμος Γεννήτρια κλειδορροής για τον SEAL 2.0

SEAL(a, n)
ΕΙΣΟΔΟΣ: μια συμβολοσειρά 160-bit (το μυστικό κλειδί), ένας (όχι μυστικός) ακέραιος n, $0 \le n < 2^{32}$ (ο αριθμός ακολουθίας), και το επιθυμητό δυαδικό μήκος L της κλειδορροής.
ΕΞΟΔΟΣ: η κλειδορροή y δυαδικού μήκους L', όπου L' είναι το μικρότερο πολλαπλάσιο του 128 το οποίο είναι $\ge L$.

1. *Δημιουργία πίνακα*. Δημιουργία των πινάκων T, S και R, των οποίων οι καταχωρήσεις είναι λέξεις 32-bit. Η συνάρτηση F που χρησιμοποιείται παρακάτω ορίζεται από την $F_a(i) = H^i_{i \bmod 5}$, όπου $H^i_0H^i_1H^i_2H^i_3H^i_4 = G_a(\lfloor i/5 \rfloor)$ και όπου η συνάρτηση G_a ορίζεται στον Αλγόριθμο 6.67.
   1.1 **for** i από 0 έως 511 **do** $T[i] \leftarrow F_a(i)$
   1.2 **for** j από 0 έως 255 **do** $S[j] \leftarrow F_a(0x00001000 + j)$.
   1.3 **for** k από 0 έως $4\lceil (L - 1)/8192 \rceil - 1$ **do** $R[k] \leftarrow F_a(0x00002000 + k)$.
2. *Αρχικοποίηση διαδικασίας*. Το ακόλουθο είναι μια περιγραφή της υπορουτίνας

`Initialize`(n, l, A, B, C, D, n_1, n_2, n_3, n_4) η οποία δέχεται ως είσοδο μια λέξη 32-bit n και έναν ακέραιο l, και εξάγει οκτώ λέξεις 32-bit A, B, C, D, n_1, n_2, n_3 και n_4. Η υποροutίνα αυτή χρησιμοποιείται στο βήμα 4.

$A \leftarrow n \oplus R[4l]$, $B \leftarrow (n \hookrightarrow 8) \oplus R[4l+1]$, $C \leftarrow (n \hookrightarrow 16) \oplus R[4l+2]$,

$D \leftarrow (n \hookrightarrow 24) \oplus R[4l+3]$.

for j από 0 έως 2 **do**

$$P \leftarrow A \wedge \text{0x000007fc},\ B \leftarrow B + T[P/4],\ A \leftarrow (A \hookrightarrow 9),$$
$$P \leftarrow B \wedge \text{0x000007fc},\ C \leftarrow C + T[P/4],\ B \leftarrow (B \hookrightarrow 9),$$
$$P \leftarrow C \wedge \text{0x000007fc},\ D \leftarrow D + T[P/4],\ C \leftarrow (C \hookrightarrow 9),$$
$$P \leftarrow D \wedge \text{0x000007fc},\ A \leftarrow A + T[P/4],\ D \leftarrow (D \hookrightarrow 9).$$

$(n_1, n_2, n_3, n_4) \leftarrow (D, B, A, C)$.

$$P \leftarrow A \wedge \text{0x000007fc},\ B \leftarrow B + T[P/4],\ A \leftarrow (A \hookrightarrow 9).$$
$$P \leftarrow B \wedge \text{0x000007fc},\ C \leftarrow C + T[P/4],\ B \leftarrow (B \hookrightarrow 9).$$
$$P \leftarrow C \wedge \text{0x000007fc},\ D \leftarrow D + T[P/4],\ C \leftarrow (C \hookrightarrow 9).$$
$$P \leftarrow D \wedge \text{0x000007fc},\ A \leftarrow A + T[P/4],\ D \leftarrow (D \hookrightarrow 9).$$

3. Αρχικοποίηση του y ώστε να είναι η κενή συμβολοσειρά και $l \leftarrow 0$.
4. Επανάληψη των εξής:

   4.1 Εκτέλεση της διαδικασίας `Initialize`(n, l, A, B, C, D, n_1, n_2, n_3, n_4).

   4.2 **for** i από 0 έως 64 **do**

$$P \leftarrow A \wedge \text{0x000007fc},\ B \leftarrow B + T[P/4],\ A \leftarrow (A \hookrightarrow 9),\ B \leftarrow B \oplus A,$$
$$Q \leftarrow B \wedge \text{0x000007fc},\ C \leftarrow C \oplus T[Q/4],\ B \leftarrow (B \hookrightarrow 9),\ C \leftarrow C + B,$$
$$P \leftarrow (P + C) \wedge \text{0x000007fc},\ D \leftarrow D + T[P/4],\ C \leftarrow (C \hookrightarrow 9),\ D \leftarrow D \oplus C,$$
$$Q \leftarrow (Q + D) \wedge \text{0x000007fc},\ A \leftarrow A \oplus T[Q/4],\ D \leftarrow (D \hookrightarrow 9),\ A \leftarrow A + D,$$
$$P \leftarrow (P + A) \wedge \text{0x000007fc},\ B \leftarrow B \oplus T[P/4],\ A \leftarrow (A \hookrightarrow 9),$$
$$Q \leftarrow (Q + B) \wedge \text{0x000007fc},\ C \leftarrow C + T[Q/4],\ B \leftarrow (B \hookrightarrow 9),$$
$$P \leftarrow (P + C) \wedge \text{0x000007fc},\ D \leftarrow D \oplus T[P/4],\ C \leftarrow (C \hookrightarrow 9),$$
$$Q \leftarrow (Q + D) \wedge \text{0x000007fc},\ A \leftarrow A + T[Q/4],\ D \leftarrow (D \hookrightarrow 9),$$
$$y \leftarrow y \,\|\, (B + S[4i-4]) \,\|\, (C \oplus S[4i-3]) \,\|\, (D + S[4i-2]) \,\|\, (A \oplus S[4i-1]).$$

   if $y \geq L$ bit σε μήκος τότε return(y) και στοπ.

   if i είναι περιττός, ανάθεση (A, C)←(A + n_1, C + n_2). Διαφορετικά, (A, C)←(A + n_3, C + n_4).

   4.3 Ανάθεση $l \leftarrow l + 1$.

6.69 Σημείωση (*επιλογή της παραμέτρου L*) Στις περισσότερες εφαρμογές του SEAL 2.0 είναι αναμενόμενο ότι $L \leq 2^{19}$· μεγαλύτερες τιμές του L είναι επιτρεπτές, αλλά αυτό θα έχει ως συνέπεια έναν μεγαλύτερο πίνακα R. Μια προτιμητέα μέθοδος για τη δημιουργία μιας μεγαλύτερης κλειδορροής, χωρίς να απαιτείται μεγαλύτερος πίνακας R, είναι ο υπολογισμός της συνένωσης των κλειδορροών SEAL(a, 0), SEAL(a, 1), SEAL(a, 2), …. Αφού ο αριθμός ακολουθίας είναι $n > 2^{32}$, είναι δυνατό να πάρουμε με τον τρόπο αυτό μια ακολουθία μήκους μέχρι 2^{51} bit, με $L = 2^{19}$.

6.70 Παράδειγμα (*διανύσματα δοκιμών για τον SEAL 2.0*) Ας υποθέσουμε ότι το κλειδί a είναι η (δεκαεξαδική) συμβολοσειρά 160-bit

```
67452301 efcdab89 98badcfe 10325476 c3d2e1f0
```

n = 0x013577af, και L = 32768 bit. Ο πίνακας R αποτελείται από τις λέξεις R[0], R[1], …, R[15]:

```
5021758d ce577c11 fa5bd5dd 366d1b93 182cff72 ac06d7c6
2683ead8 fabe3573 82a10c96 48c483bd ca92285c 71fe84c0
bd76b700 6fdcc20c 8dada151 4506dd64
```

Ο πίνακας T αποτελείται από τις λέξεις $T[0]$, $T[1]$, …, $T[511]$:

```
92b404e5 56588ced 6c1acd4e bf053f68 09f73a93 cd5f176a
b863f14e 2b014a2f 4407e646 38665610 222d2f91 4d941a21
........ ........ ........ ........ ........ ........
3af3a4bf 021e4080 2a677d95 405c7db0 338e4b1e 19ccf158
```

Ο πίνακας S αποτελείται από τις λέξεις $S[0]$, $S[1]$, …, $S[255]$:

```
907c1e3d ce71ef0a 48f559ef 2b7ab8bc 4557f4b8 033e9b05
4fde0efa 1a845f94 38512c3b d4b44591 53765dce 469efa02
........ ........ ........ ........ ........ ........
bd7dea87 fd036d87 53aa3013 ec60e282 1eaef8f9 0b5a0949
```

Η έξοδος y του Αλγορίθμου 6.68 αποτελείται από 1024 λέξεις $y[0]$, $y[1]$, …, $y[1023]$:

```
37a00595 9b84c49c a4be1e05 0673530f 0ac8389d c5878ec8
da6666d0 6da71328 1419bdf2 d258bebb b6a42a4d 8a311a72
........ ........ ........ ........ ........ ........
547dfde9 668d50b5 ba9e2567 413403c5 43120b5a ecf9d062
```

Η πράξη XOR των 1024 λέξεων του y είναι 0x098045fc. □

6.5 Σημειώσεις και περαιτέρω αναφορές

§6.1

Αν και κάπως ξεπερασμένη, από τον Rueppel[1075] παρέχεται μια συνεκτική εισαγωγή στην ανάλυση και σχεδίαση των κρυπταλγόριθμων ροής. Για μια ενημερωμένη και εκτενέστερη ανασκόπηση, δείτε το Rueppel[1081]. Μια άλλη ανασκόπηση που συνιστούμε είναι αυτή του Robshow[1063].

Η έννοια της άνευ όρων ασφάλειας παρουσιάστηκε στο κλασσικό πλέον άρθρο του Shannon [1120]. Ο Maurer [819] κάνει μια επισκόπηση του ρόλου της θεωρίας πληροφοριών στην κρυπτογραφία και, ειδικότερα, στη μυστικότητα, την πιστοποίηση αυθεντικότητας και τα σχήματα διαμοιρασμού μυστικών. Ο Maurer [811] επινόησε έναν τυχαιοκρατικό κρυπταλγόριθμο ροής ο οποίος είναι άνευ όρων ασφαλής “με υψηλή πιθανότητα”. Ακριβέστερα, ένας αντίπαλος δεν είναι σε θέση να πάρει μια οποιαδήποτε πληροφορία για το απλό κείμενο με πιθανότητα οσοδήποτε κοντά στο 1, εκτός κι αν ο αντίπαλος μπορεί να εκτελέσει ένα ανέφικτο υπολογισμό. Ο κρυπταλγόριθμος κάνει χρήση μιας δημόσια προσπελάσιμης πηγής τυχαίων bit της οποίας το μήκος είναι πολύ μεγαλύτερο από εκείνο όλων των απλών κειμένων που πρόκειται να κρυπτογραφηθούν, και μπορεί νοητά να γίνει πρακτικός. Ο κρυπταλγόριθμος του Maurer βασίζεται στον καθόλου πρακτικό κρυπταλγόριθμο *Rip van Winkle* των Massey και Ingermarsson [789], ο οποίος περιγράφεται από τον Ruepper [1081].

Μια τεχνική επίλυσης του προβλήματος επανασυγχρονισμού με σύγχρονους κρυπταλγόριθμους ροής, είναι αυτή στην οποία ο παραλήπτης στέλνει ένα αίτημα επανασυγχρονισμού στον αποστολέα, με το οποίο υπολογίζεται μια νέα εσωτερική κατάσταση ως (δημόσια) συνάρτηση της αρχικής εσωτερικής κατάστασης (ή του κλειδιού) και κάποιας δημόσιας πληροφορίας (όπως είναι ο χρόνος τη στιγμή του αιτήματος). Οι Daemen, Govaerts και Vandewalle

[291] έδειξαν ότι αυτή η προσέγγιση μπορεί να έχει ως αποτέλεσμα μια ολική απώλεια της ασφάλειας για κάποιες δημοσιευμένες προτάσεις κρυπταλγόριθμων ροής. Ο Proctor [1011] εξέτασε τον ανταγωνισμό μεταξύ της ασφάλειας και των προβλημάτων μετάδοσης σφαλμάτων που προκύπτουν κατά τη μεταβολή του αριθμού των ψηφίων του κρυπτοκειμένου ανάδρασης. Ο Maurer [808] παρουσίασε διάφορες προσεγγίσεις σχεδίασης ασύγχρονων κρυπταλγόριθμων ροής οι οποίες εν δυνάμει υπερέχουν των σχεδιάσεων που βασίζονται σε κρυπταλγόριθμους τμήματος, σε σχέση και με την ταχύτητα κρυπτογράφησης και με την ασφάλεια.

§6.2

Μια άριστη εισαγωγή στη θεωρία των γραμμικών και μη γραμμικών καταχωρητών ολίσθησης είναι το βιβλίο του Golomb [498]· δείτε επίσης τον Selmer [1107], τα Κεφάλαια 5 και 6 των Beker και Piper [84], και το Κεφάλαιο 8 των Lidl και Niederreiter [764]. Μια πολύ καλή θεώρηση των *m*-ακολουθιών μπορεί να βρεθεί στο Κεφάλαιο 10 του McEliece [830]. Παρόλο που η αντιμετώπιση σ' αυτό το κεφάλαιο έχει περιοριστεί σε ακολουθίες και καταχωρητές ολίσθησης με ανάδραση επί του δυαδικού σώματος $\mathbb{Z}_2$, πολλά από τα αποτελέσματα που παρουσιάζονται μπορούν να γενικευτούν σε ακολουθίες και καταχωρητές ολίσθησης με ανάδραση επί οποιουδήποτε πεπερασμένου σώματος $\mathbb{F}_q$.

Τα αποτελέσματα για την αναμενόμενη γραμμική πολυπλοκότητα και την κατατομή γραμμικής πολυπλοκότητας τυχαίων ακολουθιών (Γεγονότα 6.21, 6.22, 6.24 και 6.25) είναι από το Κεφάλαιο 4 του Rueppel [1075]· εμφανίζονται επίσης στο Rueppel [1077]. Οι Dai και Yang [294] επέκτειναν το Γεγονός 6.22 και βρήκαν φράγματα για την αναμενόμενη γραμμική πολυπλοκότητα μιας *n*-περιοδικής ακολουθίας για κάθε δυνατή τιμή του *n*. Τα φράγματα υποδηλώνουν ότι η αναμενόμενη γραμμική πολυπλοκότητα μιας τυχαίας περιοδικής ακολουθίας είναι κοντά στην περίοδο της ακολουθίας. Η κατατομή της γραμμικής πολυπλοκότητας της ακολουθίας που ορίσαμε στο Παράδειγμα 6.27 αποδείχθηκε από τον Dai [293]. Για περαιτέρω θεωρητική ανάλυση της κατατομής γραμμικής πολυπλοκότητας συμβουλευτείτε τις εργασίες του Niederreiter [927, 928, 929, 930]

Τα Γεγονότα 6.29 και 6.34 οφείλονται στον Massey [784]. Ο Αλγόριθμος Berlekamp-Massey (Αλγόριθμος 6.30) οφείλεται στον Massey και βασίζεται σε έναν προγενέστερο αλγόριθμο του Berlekamp [118] για αποκωδικοποίηση κωδίκων BCH. Μολονότι ο αλγόριθμος περιγράφεται στην §6.2.3 μόνο για δυαδικές ακολουθίες, μπορεί να γενικευτεί για την εύρεση της γραμμικής πολυπλοκότητας ακολουθιών επί οποιουδήποτε σώματος. Ο Blahut [144] εξετάζει λεπτομερώς τον αλγόριθμο Berlekamp-Massey και δίνει ορισμένες εκλεπτύνσεις του. Υπάρχει μια πληθώρα άλλων αλγορίθμων για τον υπολογισμό της γραμμικής πολυπλοκότητας μιας ακολουθίας. Παραδείγματος χάρη, οι Games και Chan [439], και ο Robshaw [1062], παρουσιάζουν αποδοτικούς αλγορίθμους για τον προσδιορισμό της γραμμικής πολυπλοκότητας δυαδικών ακολουθιών περιόδου 2^n· οι αλγόριθμοι αυτοί έχουν περιορισμένη πρακτική χρήση επειδή απαιτούν έναν πλήρη κύκλο της ακολουθίας.

Οι Jensen και Boekee [632] όρισαν την *πολυπλοκότητα μέγιστης τάξης* μιας ακολουθίας ως το μήκος του βραχύτερου καταχωρητή ολίσθησης με ανάδραση (όχι απαραίτητα γραμμική) (FSR) που μπορεί να παραγάγει την ακολουθία. Η αναμενόμενη πολυπλοκότητα μέγιστης τάξης μια τυχαίας δυαδικής ακολουθίας μήκους *n* είναι περίπου $2\lg n$. Έχει παρουσιαστεί έ-

νας αποδοτικός αλγόριθμος γραμμικού-χρόνου για τον υπολογισμό αυτού του μέτρου της πολυπλοκότητας· δείτε επίσης τους Jensen και Boekee [631].

Ένα άλλο μέτρο της πολυπλοκότητας, το μέτρο πολυπλοκότητας Ziv-Lempel, προτάθηκε από τους Ziv και Lempel [1273]. Το μέτρο αυτό ποσοτικοποιεί τον ρυθμό με τον οποίο εμφανίζονται νέα μοτίβα (πρότυπα – patterns) σε μια ακολουθία. Ο Mund [912] χρησιμοποίησε ένα ευρετικό επιχείρημα για την παραγωγή της αναμενόμενης πολυπλοκότητας Ziv-Lempel μιας τυχαίας δυαδικής ακολουθίας δεδομένου μήκους. Για μια λεπτομερή μελέτη των σχετικών ισχυρών και αδύναμων σημείων των μέτρων γραμμικής πολυπλοκότητας, πολυπλοκότητας μέγιστης τάξης και πολυπλοκότητας Ziv-Lempel δείτε τον Erdmann [372].

Οι Kolmogorov [704] και Chaitin [236] εισήγαγαν την έννοια της λεγόμενης *πολυπλοκότητας Turing-Kolmogorov-Chaitin*, η οποία μετρά το ελάχιστο μέγεθος της εισόδου μιας συγκεκριμένης καθολικής μηχανής Turing που μπορεί να παραγάγει μια δεδομένη ακολουθία· δείτε επίσης τον Martin-Löf [783]. Μολονότι αυτό το μέτρο πολυπλοκότητας είναι θεωρητικού ενδιαφέροντος, δεν υπάρχει γνωστός αλγόριθμος για τον υπολογισμό του και, κατά συνέπεια, δεν έχει φανερή πρακτική σημασία. Οι Beth και Dai [124] έχουν δείξει ότι η πολυπλοκότητα Turing-Kolmogorov-Chaitin είναι κατά προσέγγιση διπλάσια της γραμμικής πολυπλοκότητας για τις περισσότερες ακολουθίες επαρκούς μήκους.

Το Γεγονός 6.39 οφείλεται στους Golomb και Welch και εμφανίζεται στο βιβλίο του Golomb [498, σελ.115]. Ο Lai [725] έδειξε ότι το Γεγονός 6.39 είναι αληθές μόνο για τη δυαδική περίπτωση και απέδειξε τις αναγκαίες και ικανές συνθήκες για να είναι μη-ιδιάζων ένας FSR επί ενός γενικού πεπερασμένου σώματος.

Οι Klapper και Goresky [677] εισήγαγαν έναν νέο τύπο καταχωρητή ανάδρασης, τον καλούμενο καταχωρητή ολίσθησης με ανάδραση και κρατούμενο (FCSR), ο οποίος είναι εφοδιασμένος με βοηθητική μνήμη για την αποθήκευση του (ακέραιου) κρατούμενου (carry). Ένας FCSR είναι παρόμοιος με έναν LFSR (βλ. Εικόνα 6.4), εκτός του ότι τα περιεχόμενα των αντλημένων σταδίων του καταχωρητή ολίσθησης προστίθενται ως *ακέραιοι* στο τρέχον περιεχόμενο της μνήμης για τον σχηματισμό ενός αθροίσματος S. Το λιγότερο σημαντικό bit του S (δηλ., $S \bmod 2$) ανατροφοδοτείται (πίσω) στο πρώτο (το αριστερότερο) στάδιο του καταχωρητή ολίσθησης, ενόσω τα εναπομείναντα bit υψηλότερης τάξης (δηλ. τα $\lfloor S/2 \rfloor$) διατηρούνται ως η νέα τιμή της μνήμης. Αν ο FCSR έχει L στάδια, τότε ο χώρος που απαιτείται για τη βοηθητική μνήμη είναι το πολύ $\lg L$ bit. Οι FCSR μπορούν να αναλυθούν κατάλληλα χρησιμοποιώντας την άλγεβρα επί των 2-adic αριθμών ακριβώς όπως χρησιμοποιούμε την άλγεβρα επί των πεπερασμένων σωμάτων για να αναλύσουμε τους LFSR.

Μια περιοδική δυαδική ακολουθία μπορεί να παραχθεί με έναν FCSR. Το 2-*adic πλάτος* (span) μιας περιοδικής ακολουθίας είναι ο αριθμός των σταδίων και των bit μνήμης στον μικρότερο FCSR ο οποίος παράγει την ακολουθία. Έστω s μια περιοδική ακολουθία που έχει 2-adic πλάτος T· να σημειωθεί ότι T δεν είναι παρά η περίοδος τής s. Οι Klapper και Goresky [678] παρουσίασαν έναν αποδοτικό αλγόριθμο για την εύρεση ενός FCSR μήκους T ο οποίος παράγει την s, δοθέντων $2T + 2\lceil \lg T \rceil + 4$ από τα αρχικά bit της s. Μια εμπεριστατωμένη μελέτη των FCSR και του 2-adic πλάτους δίνεται από τους Klapper και Goresky [676].

§6.3

Οι Σημειώσεις 6.46 και 6.47 για την επιλογή πολυωνύμων σύνδεσης επισημάνθηκαν ουσιαστικά κατ' αρχήν από τους Meier και Staffelbach [834], και από τους Chepyzhov και Smeets [256], σε σχέση με τις γρήγορες επιθέσεις συσχέτισης στους κανονικά χρονισμένους LFSR.

Παρόμοιες παρατηρήσεις έγιναν από τους Coppersmith, Krawczyk και Mansour [279] σε σχέση με τη γεννήτρια συρρίκνωσης. Γενικότερα, για να ανθίστανται σε εξεζητημένες επιθέσεις συσχέτισης (π.χ. βλ. Meier και Staffelbach [834]), τα πολυώνυμα σύνδεσης δεν θα πρέπει να έχουν χαμηλού βάρους πολυωνυμικά πολλαπλάσια των οποίων οι βαθμοί δεν είναι αρκούντως μεγάλοι.

Ο Klapper [675] παρέχει παραδείγματα δυαδικών ακολουθιών οι οποίες έχουν υψηλή γραμμική πολυπλοκότητα, αλλά αυτή τους η γραμμική πολυπλοκότητα είναι χαμηλή όταν θεωρηθούν ως ακολουθίες (των οποίων τα στοιχεία συμβαίνει να είναι μόνο 0 ή 1) επί ενός μεγαλύτερου πεπερασμένου σώματος. Αυτό μας δείχνει ότι η υψηλή γραμμική πολυπλοκότητα (επί του $\mathbb{Z}_2$) από μόνη της είναι ανεπαρκής για την ασφάλεια. Το Γεγονός 6.49 αποδείχθηκε από τους Rueppel και Staffelbach [1085].

Η γεννήτρια Geffe (Παράδειγμα 6.50) προτάθηκε από τον Geffe [446]. Η γεννήτρια Pless (Διάταξη D του [978]) ήταν μια άλλη πρώιμη πρόταση για μια γεννήτρια μη γραμμικού συνδυασμού και χρησιμοποιεί τέσσερα J-K flip-flops για να συνδυάζει την έξοδο από οκτώ LFSR. Αυτή η γεννήτρια επίσης υποκύπτει σε μια επίθεση διαίρει-και-βασίλευε, όπως παρουσιάστηκε από τον Rubin [1074].

Η επίθεση γραμμικού συνδρόμου των Zeng, Yang και Rao [1265] είναι μια επίθεση γνωστού απλού κειμένου σε γεννήτριες κλειδορροών και βασίζεται σε προγενέστερη εργασία των Zeng και Huang [1263]. Είναι αποτελεσματική όταν η γνωστή κλειδορροή B μπορεί να γραφεί στη μορφή $B = A \oplus X$, όπου A είναι η ακολουθία εξόδου ενός LFSR με γνωστό πολυώνυμο σύνδεσης και η ακολουθία X είναι άγνωστη αλλά αραιή, με την έννοια ότι περιέχει περισσότερα 0 απ' ότι 1. Αν τα πολυώνυμα σύνδεσης της γεννήτριας Geffe είναι όλα γνωστά στον αντίπαλο και είναι πρωτεύοντα τριώνυμα βαθμών όχι μεγαλύτερων του n, τότε οι αρχικές καταστάσεις των τριών συνιστωσών LFSR (δηλ., το μυστικό κλειδί) μπορούν να ανακτηθούν αποδοτικά από ένα γνωστό τμήμα κλειδορροής μήκους $37n$ bit.

Η επίθεση συσχέτισης (Σημείωση 6.51) σε γεννήτριες μη γραμμικού συνδυασμού αναπτύχθηκαν αρχικά από τον Siegenthaler [1133] και δόθηκαν εκτιμήσεις για το μήκος της παρατηρούμενης κλειδορροής που απαιτείται για την επιτυχία της επίθεσης με υψηλή πιθανότητα. Η σπουδαιότητα της ανοσίας σε συσχέτιση στις μη γραμμικές συνδυάζουσες συναρτήσεις επισημάνθηκε από τον Siegenthaler [1132], ο οποίος ανέδειξε τον ανταγωνισμό μεταξύ υψηλής ανοσίας σε συσχέτιση και υψηλής μη γραμμικής τάξης (Γεγονός 6.53). Οι Meier και Staffelbach [834] παρουσίασαν δύο νέες, τις αποκαλούμενες, *ταχείες επιθέσεις συσχέτισης* οι οποίες είναι αποδοτικότερες από την επίθεση του Siegenthaler στην περίπτωση όπου οι συνιστώσες LFSR έχουν αραιά πολυώνυμα ανάδρασης, ή αν έχουν χαμηλού βάρους πολυωνυμικά πολλαπλάσια (π.χ. το καθένα να έχει λιγότερους από 10 μη μηδενικούς όρους) να μην είναι πολύ μεγάλου βαθμού. Παραπέρα επεκτάσεις και εκλεπτύνσεις των επιθέσεων συσχέτισης μπορούν να βρεθούν στις εργασίες των Mihaljević και Golić [874], Chepyzhov και Smeets [256], Golić και Mihaljević [491], Mihaljević και J. Golić [875], Mihaljević [873], Clark, Golić και Dawson [262], και Penzhorn και Kühn [967]. Μια εμπεριστατωμένη ανασκόπηση των επιθέσεων συσχέτισης σε κρυπταλγόριθμους ροής βασισμένους σε LFSR, είναι η δημοσίευση του Golić [486]· οι περιπτώσεις όπου η συνδυάζουσα συνάρτηση είναι άνευ μνήμης, ή με μνήμη, όπως επίσης όταν οι LFSR χρονίζονται κανονικά ή ακανόνιστα, εξετάζονται όλες.

Η γεννήτρια άθροισης (Παράδειγμα 6.54) προτάθηκε από τον Rueppel [1075, 1076]. Οι Meier και Staffelbach [837] παρουσίασαν επιθέσεις συσχέτισης σε γεννήτριες συνδυασμών που έχουν μνήμη, παραβίασαν τη γεννήτρια άθροισης που έχει δύο συνιστώσες LFSR, και ως αποτέλεσμα, σύστησαν τη χρήση αρκετών LFSR μετρίου μήκους στη γεννήτρια άθροισης, αντί απλά λίγων μακροσκελών LFSR. Παραδείγματος χάρη, αν μια γεννήτρια άθροισης χρησιμοποιεί δύο LFSR, με τον καθένα να έχει μήκος περίπου 200, και αν είναι γνωστά 50000 bit κλειδορροής, τότε η επίθεση των Meier και Staffelbach αναμένεται να χρειαστεί λιγότερες των 700 δοκιμών, όπου το κύριο βήμα σε κάθε δοκιμή περιλαμβάνει την επίλυση ενός συστήματος 400 × 400 δυαδικών γραμμικών εξισώσεων. Ο Dawson [312] παρουσίασε μια άλλη επίθεση γνωστού απλού κειμένου στις γεννήτριες άθροισης που έχουν δύο συνιστώσες LFSR, η οποία απαιτεί λιγότερα γνωστά bit κλειδορροής απ' ότι η επίθεση των Meier και Staffelbach. Η επίθεση του Dawson είναι ταχύτερη από αυτή των Meier και Staffelbach μόνο στην περίπτωση όπου και οι δύο LFSR είναι σχετικά σύντομοι. Πρόσφατα, οι Klapper και Goresky [678] έδειξαν ότι η γεννήτρια άθροισης έχει συγκριτικά χαμηλό 2-adic πλάτος (βλ. σελ. 218). Ακριβέστερα, αν a και b είναι δύο ακολουθίες με 2-adic πλάτη $\lambda_2(a)$ και $\lambda_2(b)$, αντίστοιχα, και αν s είναι το αποτέλεσμα του συνδυασμού τους με τη γεννήτρια άθροισης, τότε το 2-adic πλάτος τής s είναι το πολύ $\lambda_2(a) + \lambda_2(b) + 2\lceil \lg(\lambda_2(a)) \rceil + \lceil \lg(\lambda_2(b)) \rceil + 6$. Παραδείγματος χάρη, αν m-ακολουθίες περιόδου $2^L - 1$, για $L = 7, 11, 13, 15, 16, 17$, συνδυαστούν με τη γεννήτρια άθροισης, τότε το 2-adic πλάτος είναι λιγότερο από 2^{18}. Άρα, η γεννήτρια άθροισης είναι ευάλωτη σε επίθεση γνωστού απλού κειμένου όταν οι LFSR που αποτελούν συνιστώσες της, είναι όλοι σχετικά σύντομοι.

Η κατανομή πιθανότητας του κρατούμενου για την πρόσθεση n τυχαίων ακεραίων αναλύθηκε από τους Staffelbach και Meier [1167]. Αποδείχθηκε ότι το κρατούμενο ισοσταθμίζεται για άρτιο n και μεροληπτεί για n περιττό. Για $n = 3$ το κρατούμενο είναι ισχυρά μεροληπτικό, όμως η αμεροληψία συγκλίνει στο 0 καθώς το n τείνει στο ∞. Ο Golić [485] ανέδειξε τη σπουδαιότητα της συσχέτισης μεταξύ των γραμμικών συναρτήσεων της εξόδου και της εισόδου σε γενικούς συνδυαστές (combiner) με μνήμη, και εισήγαγε την αποκαλούμενη *μέθοδο γραμμικής ακολουθιακής προσέγγισης κυκλώματος*, για την εύρεση τέτοιων συναρτήσεων που παράγουν συσχετισμένες ακολουθίες. Ο Golić [488] το χρησιμοποίησε αυτό ως βάση για την ανάπτυξη μιας τεχνικής *γραμμικής κρυπτανάλυσης* για κρυπταλγόριθμους ροής, και πρότεινε στην ίδια εργασία έναν κρυπταλγόριθμο ροής, τον καλούμενο GOAL, συμπεριλαμβάνοντας αρχές τροποποιημένων αποκομμένων γεννητριών γραμμικών ισοτιμιών (βλ. σελ. 187), αυτοχρονο-ρύθμιση και τυχαία παραγόμενους συνδυαστές με μνήμη.

Το Γεγονός 6.55(i) οφείλεται στον Key [670], ενώ το Γεγονός 6.55 (ii) αποδείχθηκε από τον Rueppel [1075]. Οι Massey και Serconek [794] έδωσαν μια εναλλακτική απόδειξη του φράγματος του Key η οποία βασίζεται στον Διακριτό Μετασχηματισμό Fourier (DFT). Ο Siegenthaler [1134] περιέγραψε μια επίθεση συσχέτισης σε γεννήτρια μη γραμμικού φίλτρου. Ο Ferré [418] έχει εφαρμόσει ταχείες επιθέσεις συσχέτισης σε τέτοιες γεννήτριες. Ο Anderson [29] παρουσίασε άλλες συσχετίσεις οι οποίες μπορεί να είναι χρήσιμες για τη βελτίωση της επιτυχίας των επιθέσεων συσχέτισης. Μια επίθεση, η καλούμενη *επίθεση αντιστροφής*, η οποία προτάθηκε από τον Golić [490] μπορεί να είναι αποτελεσματικότερη από την επίθεση του Anderson. Ο Golić παρέχει επίσης μια σειρά από κριτήρια σχεδίασης για γεννήτριες μη γραμμικού φίλτρου. Ο Ding [349] εισήγαγε την έννοια της διαφορικής κρυπτανάλυσης για γεννήτριες μη γραμμικού φίλτρου όπου ο LFSR αντικαθίσταται από έναν απλό μετρητή που έχει μια οποιαδήποτε περίοδο.

Η *επίθεση γραμμικής συμβιβαστότητας* των Zeng και Rao [1264] είναι μια επίθεση γνωστού απλού κειμένου σε γεννήτριες κλειδορροών, η οποία μπορεί να ανακαλύψει περίσσειες κλειδιών σε διάφορες γεννήτριες. Είναι αποτελεσματική σε καταστάσεις όπου είναι δυνατό να απομονώσουμε κάποιο τμήμα k_1 του μυστικού κλειδιού k και να σχηματίσουμε ένα γραμμικό σύστημα εξισώσεων $Ax = b$ όπου ο πίνακας A προσδιορίζεται από το k_1, και το b προσδιορίζεται από τη γνωστή κλειδορροή. Το σύστημα των εξισώσεων θα πρέπει να έχει την ιδιότητα ότι είναι συμβιβαστό (και με υψηλή πιθανότητα έχει μία μοναδική λύση) αν το k_1 είναι η αληθής τιμή του υποκλειδιού, ενώ είναι ασυμβίβαστο με υψηλή πιθανότητα, διαφορετικά. Σε αυτές τις συγκρίσεις, μπορεί κάποιος να εξαπολύσει μια εξαντλητική αναζήτηση του k_1, και στη συνέχεια να εξαπολύσει μια ξεχωριστή επίθεση για τα εναπομείναντα bit του k. Αν τα δυαδικά μήκη των k_1 και k είναι l_1 και l, αντίστοιχα, η επίθεση μας δείχνει ότι το επίπεδο ασφάλειας της γεννήτριας είναι $2^{l_1} + 2^{l-l_1}$, αντί για 2^l.

Η *πολυσύνθετη γεννήτρια* (multiplexer generator) προτάθηκε από τον Jennings [637]. Χρησιμοποιούνται δύο LFSR μέγιστου μήκους που έχουν μήκη L_1 και L_2, τα οποία είναι αριθμοί σχετικά πρώτοι. Έστω h ένας θετικός ακέραιος που ικανοποιεί την $h \leq \min(L_1, \lg L_2)$. Μετά από κάθε κύκλο ρολογιού επιλέγονται τα περιεχόμενα ενός συγκεκριμένου υποσυνόλου h σταδίων του πρώτου LFSR και μετατρέπονται σε έναν ακέραιο t του διαστήματος $[0, L_2 - 1]$ χρησιμοποιώντας μια 1-1 απεικόνιση θ. Τελικά, το περιεχόμενο του σταδίου t του δεύτερου LFSR είναι έξοδος ως τμήμα της κλειδορροής. Υποθέτοντας ότι τα πολυώνυμα σύνδεσης των LFSR είναι γνωστά, η επίθεση γραμμικής συμβιβαστότητας παρέχει μια επίθεση γνωστού απλού κειμένου στην πολυσύνθετη γεννήτρια, απαιτώντας μια γνωστή ακολουθία κλειδορροής μήκους $N \geq L_1 + L_2 2^h$ και 2^{L_1+h} ελέγχους γραμμικής συμβιβαστότητας. Αυτό δείχνει ότι η επιλογή της απεικόνισης θ και ο δεύτερος LFSR δεν συνεισφέρουν σημαντικά στην ασφάλεια της γεννήτριας.

Η επίθεση γραμμικής συμβιβαστότητας έχει επίσης μελετηθεί από τους Zeng, Yang και Rao [1264] για τη *γεννήτρια εσωτερικού γινομένου πολλαπλών ταχυτήτων* των Massey και Rueppel [793]. Στη γεννήτρια αυτή, δύο LFSR με μήκη L_1 και L_2 χρονίζονται σε διαφορετικούς ρυθμούς και τα περιεχόμενά τους συνδυάζονται στον χαμηλότερο ρυθμό ρολογιού παίρνοντας το εσωτερικό γινόμενο των $\min(L_1, L_2)$ σταδίων των δύο LFSR. Η εργασία των Zeng et al. [1266] είναι μια ευανάγνωστη ανασκόπηση που περιγράφει την αποτελεσματικότητα των επιθέσεων γραμμικής συμβιβαστότητας και γραμμικού συνδρόμου, κατά την κρυπτανάλυση των κρυπταλγόριθμων ροής.

Η γεννήτρια σακιδίου (Παράδειγμα 6.56) προτάθηκε από τους Rueppel και Massey [1084] και αναλύθηκε εκτενώς από τον Rueppel [1075], όμως, δεν δόθηκαν συγκεκριμένες προτάσεις για την επιλογή των κατάλληλων παραμέτρων (το μήκος L του LFSR και τα βάρη σακιδίου) για τη γεννήτρια. Δεν έχουν ανακοινωθεί στη βιβλιογραφία αδύνατα σημεία της γεννήτριας σακιδίου.

Η ιδέα της χρήσης της εξόδου ενός καταχωρητή για τη ρύθμιση του βηματισμού ενός άλλου καταχωρητή, χρησιμοποιήθηκε σε αρκετούς δρομείς μηχανών (ρότορες) κατά τη διάρκεια του δευτέρου παγκοσμίου πολέμου, όπως είναι, για παράδειγμα, ο κρυπταλγόριθμος German Lorenz SZ40. Μια περιγραφή αυτού του κρυπταλγόριθμου και επίσης μια εκτενής ανασκόπηση των χρονο-ρυθμιζόμενων καταχωρητών ολίσθησης, παρέχεται από τους Gollmann και Chambers [496].

Η γεννήτρια εναλλασσόμενου βήματος (Αλγόριθμος 6.57) προτάθηκε το 1987 από τον Günther [528], ο οποίος επίσης απέδειξε το Γεγονός 6.59 και περιέγραψε την επίθεση διαίρει-και-βασίλευε που μνημονεύσαμε στη Σημείωση 6.60. Η γεννήτρια εναλλασσόμενου βήματος βασίζεται στη γεννήτρια *stop-and-go* των Beth και Piper [126]. Στη γεννήτρια stop-and-go ένας καταχωρητής ρύθμισης R_1 χρησιμοποιείται για να ρυθμίζει τον βηματισμό ενός άλλου καταχωρητή R_2, ως εξής. Αν η έξοδος του R_1 είναι 1, τότε ο R_2 χρονίζεται· αν η έξοδος του R_1 είναι 0, τότε ο R_2 δεν χρονίζεται, επαναλαμβάνεται όμως η προηγούμενη έξοδός του. Η έξοδος του R_2 υπόκειται σε XOR με την ακολουθία εξόδου ενός τρίτου καταχωρητή R_3 ο οποίος χρονίζεται στον ίδιο ρυθμό με τον R_1. Οι Beth και Piper έδειξαν πώς μπορεί μια συνετή επιλογή των καταχωρητών R_1, R_2 και R_3 να εγγυηθεί ότι η ακολουθία εξόδου έχει υψηλή γραμμική πολυπλοκότητα και περίοδο, καθώς και καλές στατιστικές ιδιότητες. Δυστυχώς, η γεννήτρια υποκύπτει στην επίθεση γραμμικού συνδρόμου των Zeng, Yang και Rao [1265] (δείτε επίσης στη σελ. 32)· αν τα πολυώνυμα σύνδεσης των R_1 και R_2 είναι πρωτεύοντα τριώνυμα βαθμού όχι μεγαλύτερου του n, και γνωστά στον αντίπαλο, τότε οι αρχικές καταστάσεις των τριών συνιστωσών LFSR (δηλ., το μυστικό κλειδί) μπορεί να ανακτηθούν αποδοτικά από ένα τμήμα γνωστού απλού κειμένου μήκους $37n$ bit.

Μια άλλη παραλλαγή της γεννήτριας stop-and-go είναι η γεννήτρια *βήμα-1/βήμα-2* που οφείλεται στους Gollmann και Chambers [496]. Η γεννήτρια αυτή χρησιμοποιεί δύο καταχωρητές μέγιστου μήκους R_1 και R_2 που έχουν το ίδιο μήκος. Ο καταχωρητής R_1 χρησιμοποιείται για να ρυθμίζει τον βηματισμό του R_2, ως εξής. Αν η έξοδος του R_1 είναι 0, τότε ο R_2 χρονίζεται μία φορά· αν η έξοδος του R_1 είναι 1, τότε ο R_2 χρονίζεται δύο φορές προτού παραγάγει το επόμενο bit εξόδου. Ο Živković [1274] πρότεινε μια *εμφυτευμένη επίθεση συσχέτισης* στον R_2 της οποίας η πολυπλοκότητα είναι $O(2^{L_2})$, όπου L_2 είναι το μήκος του R_2.

Κυκλικός καταχωρητής μήκους L είναι ένας LFSR με πολυώνυμο ανάδρασης $C(D) = 1 + D^L$. Ο Gollmann [494] πρότεινε τη *συρροή* (cascading) n κυκλικών καταχωρητών του ιδίου μήκους p (πρώτος) διατάσσοντας τους σειριακά, κατά τέτοιον τρόπο που όλοι, εκτός από τον πρώτο καταχωρητή, να είναι χρονο-ρυθμιζόμενοι από τον προκάτοχό τους· η *p-κύκλου συρροή* του Goollmann μπορεί να ιδωθεί ως μια επέκταση της γεννήτριας stop-and-go (σελ. 35). Ο πρώτος καταχωρητής χρονίζεται κανονικά και το bit εξόδου του είναι το bit εισόδου στον δεύτερο καταχωρητή. Γενικά, αν το bit εισόδου στον i-οστό καταχωρητή (για $i \geq 2$) τη χρονική στιγμή t είναι a_t, τότε ο i-οστός καταχωρητής χρονίζεται αν $a_t = 1$· αν $a_t = 0$, ο καταχωρητής δεν χρονίζεται, αλλά επαναλαμβάνεται το προηγούμενο bit εξόδου του. Το bit εξόδου του i-οστού καταχωρητή υπόκειται σε XOR με το a_t και το αποτέλεσμα γίνεται το bit εισόδου στον $(i + 1)$-οστό καταχωρητή. Η έξοδος του τελευταίου καταχωρητή είναι η έξοδος της συρροής p-κύκλου. Η αρχική (μυστική) κατάσταση ενός κυκλικού καταχωρητή που είναι μια από τις συνιστώσες δεν θα πρέπει να είναι το διάνυσμα με όλα του τα στοιχεία 0 ή το διάνυσμα με όλα του τα στοιχεία 1. Ο Gollmann απέδειξε ότι η περίοδος της ακολουθίας εξόδου είναι p^n. Επιπλέον, αν το p είναι πρώτος τέτοιος, ώστε το 2 να είναι ένας γεννήτορας του $\mathbb{Z}_p^*$, τότε η ακολουθία εξόδου έχει γραμμική πολυπλοκότητα p^n. Αυτό μας συνιστά ισχυρά τη χρήση μακροσκελών συρροών (δηλ., μεγάλο n) βραχύτερων καταχωρητών αντί σύντομων συρροών μακροσκελέστερων καταχωρητών. Μια παραλλαγή της συρροής Gollmann, η καλούμενη *συρροή m-ακολουθιών*, έχει στη θέση των κυκλικών καταχωρητών τους LFSR μέγιστου μήκους που έχουν το ίδιο μήκος L. Ο Chambers [237] έδειξε ότι η ακολουθία εξόδου μιας τέτοιας συρροής m-ακολουθιών έχει περίοδο $(2^L - 1)^n$ και γραμμική πολυπλοκότητα τουλάχι-

στο $L(2^L - 1)^{n-1}$. Οι Park, Lee και Goh [964] επέκτειναν προγενέστερη εργασία του Menicocci [845] και ανακοίνωσαν την παραβίαση συρροών m-ακολουθιών των 9 σταδίων, όπου κάθε LFSR έχει μήκος 100· συνέστησαν επίσης ότι οι συρροές m-ακολουθιών των 10 σταδίων μπορεί να μην είναι ασφαλείς. Οι Chambers και Gollmann [239] μελέτησαν μια επίθεση στις συρροές p-κύκλων και m-ακολουθιών, την καλούμενη *lock-in*, η οποία έχει ως αποτέλεσμα μια μείωση του τελικού κλειδοχώρου των συρροών.

Η γεννήτρια συρρίκνωσης (Αλγόριθμος 6.61) προτάθηκε το 1993 από τους Coppersmith, Krawczyk και Mansour [279], οι οποίοι απέδειξαν επίσης το Γεγονός 6.63 και περιέγραψαν τις επιθέσεις που μνημονεύσαμε στη Σημείωση 6.64. Ο ακανόνιστος ρυθμός εξόδου της γεννήτριας συρρίκνωσης μπορεί να ξεπεραστεί χρησιμοποιώντας μια σύντομη προσωρινή μνήμη για την έξοδο· η επίδραση μιας τέτοιας προσωρινής μνήμης αναλύεται από τους Kessler και Krawczyk [669]. Ο Krawczyk [716] αναφέρει μερικές τεχνικές βελτίωσης των υλοποιήσεων λογισμικού. Ένας συνολικός όγκος έργου των 2.5 Mbit/sec ανακοινώθηκε για μια υλοποίηση στη γλώσσα C σε έναν σταθμό εργασίας 33MHz IBM, όταν οι δύο καταχωρητές ολίσθησης έχουν ο καθένας μήκος στο διάστημα 61 – 64 bit και χρησιμοποιούνται μυστικές συνδέσεις. Η ασφάλεια της γεννήτριας συρρίκνωσης εξετάζεται περαιτέρω από τον Golić [487].

Μια γεννήτρια κλειδιών που σχετίζεται με τη γεννήτρια συρρίκνωσης είναι η γεννήτρια αυτόσυρρίκνωσης (SSG – self-shrinking generator) των Meier και Staffelbach [838]. Η SSG χρησιμοποιεί μόνο έναν LFSR μέγιστου μήκους R. Η ακολουθία εξόδου του R διαμερίζεται σε ζεύγη από bit. Η SSG εξάγει ένα 0 αν το ζεύγος είναι 10 και εξάγει ένα 1 αν το ζεύγος είναι 11· τα ζεύγη 01 και 00 απορρίπτονται. Οι Meier και Staffelbach απέδειξαν ότι η SSG μπορεί να υλοποιηθεί ως μια γεννήτρια συρρίκνωσης. Επιπλέον, η γεννήτρια συρρίκνωσης μπορεί να υλοποιηθεί ως μια γεννήτρια αυτο-συρρίκνωσης (της οποίας η συνιστώσα LFSR δεν είναι μέγιστου μήκους). Ακριβέστερα, αν οι συνιστώσες LFSR μιας γεννήτριας συρρίκνωσης έχουν πολυώνυμα σύνδεσης $C_1(D)$ και $C_2(D)$, η ακολουθία εξόδου μπορεί να παραχθεί από μια γεννήτρια αυτο-συρρίκνωσης με πολυώνυμα σύνδεσης $C(D) = C_1(D)^2 + C_2(D)^2$. Οι Meier και Staffelbach απέδειξαν επίσης ότι αν το μήκος του R είναι L, τότε η περίοδος και η γραμμική πολυπλοκότητα της ακολουθίας εξόδου της SSG είναι τουλάχιστο $2^{\lfloor L/2 \rfloor}$ και $2^{\lfloor L/2 \rfloor - 1}$, αντίστοιχα. Επιπλέον, παρείχαν ισχυρές ενδείξεις ότι η περίοδος αυτή και η γραμμική πολυπλοκότητα είναι όντως 2^{L-1} περίπου. Υποθέτοντας ένα τυχαία επιλεγμένο, αλλά γνωστό, πολυώνυμο σύνδεσης, η καλύτερη επίθεση στην SSG που παρουσιάστηκε από τους Meier και Staffelbach απαιτεί $2^{0.79L}$ βήματα. Ακριβέστερα, ο Mihaljević [871] παρουσίασε μία σημαντικά ταχύτερη πιθανοκρατική επίθεση στην SSG. Παραδείγματος χάρη, αν $L = 100$, τότε η νέα επίθεση απαιτεί 2^{57} βήματα και χρειάζεται ένα τμήμα της ακολουθίας εξόδου μήκους 4.9×10^8. Η επίθεση δεν έχει κάποια επίπτωση στην ασφάλεια της γεννήτριας συρρίκνωσης.

Μια πρόσφατη ανασκόπηση των τεχνικών επίθεσης σε χρονο-ρυθμιζόμενες γεννήτριες δίνεται από τον Gollmann [495]. Για κάποιες νεότερες τεχνικές επιθέσεων, δείτε τον Mihaljević [872], τους Golić και O'Connor [492] και τον Golić [489]. Ο Chambers [238] πρότεινε μια χρονο-ρυθμιζόμενη συρροή αποτελούμενη από LFSR μήκους 32 ο καθένας. Κάθε τμήμα 32-bit της ακολουθίας εξόδου μιας συνιστώσας LFSR περνά μέσω μιας αντιστρέψιμης συσκευής ανακατέματος (*S-box*), και η προκύπτουσα ακολουθία 32-bit χρησιμοποιείται για τη ρύθμιση του ρολογιού του επόμενου LFSR. Οι Baum και Blackburn [77] γενίκευσαν την έννοια ενός χρονο-ρυθμιζόμενου καταχωρητή ολίσθησης σε εκείνη του καταχωρητή που βασίζεται σε μια πεπερασμένη ομάδα.

§6.4

Ο SEAL (Αλγόριθμος 6.68) σχεδιάστηκε από τους Coppersmith και Rogaway [281] οι οποίοι τον κατοχύρωσαν ως πατέντα. Οι Rogaway και Coppersmith [1066] αναφέρουν μια ταχύτητα κρυπτογράφησης των 7.2Mbyte/sec, για μια υλοποίηση σε γλώσσα assembly σε επεξεργαστή 50 MHz 486 με L = 4096 bit, προϋποθέτοντας προ-υπολογισμένους πίνακες (βλ. Σημείωση 6.66).

Αν και ο κρυπταλγόριθμος ροής RC4 παραμένει ιδιωτικός, έχουν δημοσιευτεί περιγραφές του οι οποίες έχουν εξαγόμενα συμβατά με πιστοποιημένες υλοποιήσεις του RC4· για παράδειγμα, δείτε τον Schneier [1094]. Οι Blöcker και Dichtl [156] πρότειναν έναν κρυπταλγόριθμο ροής γρήγορου λογισμικού, τον καλούμενο *FISH* (Fibonacci Shrinking generator), ο οποίος βασίζεται στην αρχή της γεννήτριας συρρίκνωσης εφαρμοσμένη στη γεννήτρια Fibonacci με χρονική υστέρηση (γνωστή και ως προσθετική γεννήτρια) του Knuth [692, σελ. 27]. Ο Anderson [28] στη συνέχεια παρουσίασε μια επίθεση γνωστού απλού κειμένου στον FISH, η οποία απαιτεί μερικές (λίγες) χιλιάδες λέξεων 32-bit γνωστού απλού κειμένου και έναν παράγοντα έργου των 2^{40} περίπου υπολογισμών. Ο Anderson πρότεινε επίσης έναν κρυπταλγόριθμο ροής γρήγορου λογισμικού, τον καλούμενο *PIKE*, που βασίζεται στη γεννήτρια Fibonacci και τον κρυπταλγόριθμο ροής A5· μια περιγραφή του A5 δίνεται από τον Anderson [28].

Ο Wolfram [1251, 1252] πρότεινε έναν κρυπταλγόριθμο ροής βασισμένο σε μονοδιάστατα κυψελιδικά αυτόματα (cellular automata) με μη γραμμική ανάδραση. Οι Meier και Staffelbach [835] παρουσίασαν μια επίθεση γνωστού απλού κειμένου σ' αυτόν τον κρυπταλγόριθμο, η οποία ανέδειξε το γεγονός ότι μήκη κλειδιών των 127 bit, που προτάθηκαν από τον Wolfram [1252], δεν είναι ασφαλή· οι Meier και Staffelbach συστήνουν μήκη κλειδιών των 1000 bit περίπου.

Οι Klapper και Goresky [679] παρουσίασαν κατασκευές για τους FCSR (βλ. σελ. 31) των οποίων οι ακολουθίες εξόδου έχουν σχεδόν μέγιστη περίοδο, είναι ισοσταθμισμένες και είναι σχεδόν ακολουθίες de Bruijn, με την έννοια ότι για έναν συγκεκριμένο μη αρνητικό ακέραιο t, ο αριθμός εμφανίσεων δύο οποιωνδήποτε ακολουθιών t-bit ως υπακολουθιών μιας περιόδου διαφέρει το πολύ κατά 2. Τέτοιοι FCSR είναι καλοί υποψήφιοι για χρήση στην κατασκευή ασφαλών κρυπταλγόριθμων ροής, όπως ακριβώς χρησιμοποιήθηκαν LFSR μέγιστου μήκους στην §6.3. Οι Goresky και Klapper [518] εισήγαγαν μια γενίκευση των FCSR, τους καλούμενους d-FCSR, που βασίζονται σε *υποδιαιρεμένες* επεκτάσεις των 2-adic αριθμών (d είναι η υποδιαίρεση).

Μετάφραση: Γιώργος Χ. Στεφανίδης
Τμήμα Εφ. Πληροφορικής
Πανεπιστήμιο Μακεδονίας