Τεχνολογικο Εκπαιδευτικο Ίδρυμα
Καλαματας/Παραρτημα Σπαρτης

Πτυχιακη Εργασια

Σχεδιαστικές Αρχές και Κρυπτανάλυση της Συνάρτησης Κατακερματισμού GRINDAHL

Φοιτήτριες:
Κριεμπάρδη Γεωργία
Κλεισιάρη Φρειδερίκη

Επιβλέπων:
Μακροδημήτρης Γεώργιος

19 Οκτωβρίου 2011

Περιεχόμενα

Πρόλογος

Η παρούσα εργασία εκπονήθηκε στα πλαίσια του προγράμματος προπτυχιακών σπουδών του τμήματος "Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών" του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Καλαμάτας στο παράρτημα της Σπάρτης.

Αντικείμενο της εργασίας είναι η μελέτη των συναρτήσεων κατακερματισμού (hash functions) που εφαρμόζονται στην Κρυπτογραφία, μέσω της ανάλυσης της οικογένειας συναρτήσεων Grindahl. Ακόμη, γίνεται εκτενής μελέτη των θεμάτων ασφαλείας που αφορούν τις συναρτήσεις κατακερματισμού.

Θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα κ. Μακροδημήτρη Γεώργιο, για την ευκαιρία που μας προσέφερε να ασχοληθούμε με ένα πραγματικά σύγχρονο θέμα στον τομέα της Κρυπτογραφίας, καθώς και για τις υποδείξεις του καθ' όλη τη διάρκεια εκπόνησης της εργασίας.

Σπάρτη 19 Οκτωβρίου 2011

Κριεμπάρδη Γεωργία
Κλεισιάρη Φρειδερίκη

Κεφάλαιο 1

Εισαγωγή

Στη σύγχρονη κρυπτογραφία με τον όρο συνάρτηση κατακερματισμού (hash function) εννοούμε μια σαφώς ορισμένη διαδικασία ή αλλιώς μηχανισμό, ο οποίος στην είσοδό του δέχεται ένα μπλοκ δεδομένων οποιουδήποτε μεγέθους και στην έξοδό του δίνει μια συμβολοσειρά (string) συγκεκριμένου, σταθερού μήκους -τη λεγόμενη τιμή κατακερματισμού (hash value). Χαρακτηριστική ιδιότητα μιας οποιασδήποτε συνάρτησης κατακερματισμού είναι η εξαιρετική της "ευαισθησία" στα δεδομένα εισόδου. Για την ακρίβεια, η παραμικρή αλλαγή στην είσοδό της επιστρέφει ένα αποτέλεσμα εντελώς διαφορετικό σε σύγκριση με το προηγούμενο. Στα πλαίσια της κρυπτογραφίας, η είσοδος μιας συνάρτησης κατακερματισμού ονομάζεται μήνυμα (message) ενώ το αποτέλεσμά της σύνοψη μηνύματος ή απλά σύνοψη (digest).

Οι συναρτήσεις κατακερματισμού είναι ένα από τα βασικά στοιχειά της κρυπτογραφίας. Σε αυτό το πλαίσιο οφείλουν να ικανοποιούν ορισμένα κριτήρια ασφαλείας (security properties) όπως αντίσταση προαπεικόνισης (preimage resistance), δευτερεύουσα αντίσταση προ-απεικόνισης (second preimage resistance) και αντίσταση συγκρούσεων (collision resistance) [1]. Το πρώτο κριτήριο αναφέρεται στην ιδιότητα μίας συνάρτησης να αντιστοιχίζει με ευκολία το μήνυμα στη σύνοψη, αλλά να καθιστά αδύνατη την αντίστροφη διαδικασία, δηλαδή την εύρεση του μηνύματος δεδομένης της σύνοψης. Το δεύτερο κριτήριο αναφέρεται στην περίπτωση όπου με δεδομένο ένα μήνυμα είναι υπολογιστικά δύσκολη η εύρεση ενός άλλου μηνύματος, που να οδηγεί στην ίδια σύνοψη. Το τρίτο αναφέρεται στη δυσκολία υπολογισμού δύο μηνυμάτων που να οδηγούν στην ίδια έξοδο.

Μία εφικτή μέθοδος κατασκευής συναρτήσεων κατακερματισμού προ-

τάθηκε από τους Merkle και Damgård. Αυτή χρησιμοποιεί μία επαναληπτική διαδικασία, όπου σε κάθε επανάληψη μία συνάρτηση εισόδου καθορισμένου μήκους, η οποία αναφέρεται ως συνάρτηση συμπίεσης (compression function), ενημερώνει μία εσωτερική κατάσταση του αλγορίθμου, η οποία αναφέρεται ως μεταβλητή αλυσίδωσης (chaining variable), με τμήμα του μηνύματος. Με ορισμένες προσαυξήσεις (padding) του μηνύματος που πρόκειται να κατακερματιστεί, το πρόβλημα της της κατασκευής μίας συνάρτησης κατακερματισμού με αντίσταση συγκρούσεων, απλοποιείται στο πρόβλημα εύρεσης συνάρτησης συμπίεσης με την εν λόγω ιδιότητα.

Σχεδόν όλες οι συναρτήσεις κατακερματισμού λειτουργούν με τη χρήση συνάρτησης συμπίεσης. Η κατασκευή της τελευταίας μπορεί να γίνει με τρεις τρόπους. Ο πρώτος χρησιμοποιεί ένα δύσκολο πρόβλημα όπως παραγοντοποίηση πρώτων αριθμών, εύρεση μικρών διανυσμάτων σε πλέγματα (lattices) ή ακόμα και επίλυση εξισώσεων δευτέρου βαθμού με πολλαπλές μεταβλητές. Η συνάρτηση συμπίεσης που κατασκευάζεται με τη μέθοδο αυτή προσφέρει μεγάλη ασφάλεια, έχει όμως αυξημένες υπολογιστικές απαιτήσεις και κατ' επέκταση χαμηλή απόδοση. Ο δεύτερος τρόπος περιλαμβάνει κρυπτογραφικούς αλγορίθμους δέσμης (block ciphers). Αυτοί τεμαχίζουν σε τμήματα (blocks) το αρχικό κείμενο που πρόκειται να κρυπτογραφηθεί και κρυπτογραφούν κάθε τμήμα ξεχωριστά [2]. Ο τρίτος τρόπος είναι η κατασκευή της συνάρτησης συμπίεσης από το μηδέν, όπως για παράδειγμα στους αλγορίθμους SHA-1 και MD5. Ο τρόπος αυτός ενέχει τον κίνδυνο να γίνουν κατανοητές οι αρχές λειτουργίας της συνάρτησης συμπίεσης, καθιστώντας την μη ασφαλή για την κρυπτογράφηση των δεδομένων.

Η δυσκολία δημιουργίας μίας συνάρτησης κατακερματισμού που να είναι ασφαλής στις παρούσες και μελλοντικές επιθέσεις, οδήγησε το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) στη διοργάνωση ενός διαγωνισμού, για τη δημιουργία αλγορίθμων κατακερματισμού. Ταυτόχρονα, νέες συναρτήσεις κατακερματισμού έχουν δημοσιευτεί, όπως οι FORK-256 , RadioGatún και Grindahl. Η τελευταία αποτελεί και το αντικείμενο της παρούσας εργασίας.

Κεφάλαιο 2

Αλγόριθμος κρυπτογράφησης Rijndael

2.1 Εισαγωγή

Ο αλγόριθμος κρυπτογράφησης Rijndael [10] αποτελεί τη βάση για την περιγραφή της συνάρτησης κατακερματισμού Grindahl, που αποτελεί το κυρίαρχο αντικείμενο μελέτης της παρούσας εργασίας. Είναι λοιπόν σκόπιμο, να παρουσιαστούν οι αρχές του αλγορίθμου αυτού.

Ο Rijndael είναι ένας αλγόριθμος κρυπτογράφησης κατά τμήματα (block cipher), με μεταβλητό μήκος τμημάτων και κλειδιού. Το μήκος του τμήματος και του κλειδιού μπορούν να καθοριστούν ανεξάρτητα, στα 12,192 ή 256 δυαδικά ψηφία [13]. Η στρατηγική σχεδιασμού του αλγορίθμου παρέχει προστασία, ενάντια στις μεθόδους γραμμικής και διαφορικής κρυπτανάλυσης.

2.2 Η κατάσταση, το κλειδί κρυπτογράφησης και ο αριθμός των γύρων

Ορίζουμε την "κατάσταση" του τμήματος κρυπτογραφήματος, ως το ενδιάμεσο αποτέλεσμα της διαδικασίας κρυπτογράφησης. Η κατάσταση αρχικοποιείται με χαρακτήρες κειμένου, με τη σειρά $\alpha_{0,0}$, $\alpha_{1,0}$, $\alpha_{2,0}$, $\alpha_{3,0}$, $\alpha_{0,1}$, $\alpha_{1,1}$, ... Οι μετασχηματισμοί του κάθε γύρου βασίζονται σε μετασχηματισμούς που λειτουργούν επί της κατάστασης. Στο τέλος της διαδικασίας κρυπτογράφησης, το κρυπτογραφημένο κείμενο (ciphertext) διαβάζεται από την κατάσταση, παίρνοντας τις ψηφιολέξεις της κατάστασης

κατά την ίδια σειρά.

Η κατάσταση μπορεί να απεικονιστεί ως πίνακας ψηφιολέξεων. Ο πίνακας αυτός έχει τέσσερις γραμμές, ενώ ο αριθμός των στηλών συμβολίζεται ως N_b και ισούται με το μέγεθος του τμήματος διαιρεμένου με το 32. Το κλειδί κρυπτογράφησης μπορεί να απεικονιστεί ως πίνακας τεσσάρων γραμμών, ενώ ο αριθμός των στηλών συμβολίζεται με N_k και ισούται με το μέγεθος του κλειδιού διαιρεμένου με το 32. Μπορούμε να δούμε τους πίνακες κατάστασης και κλειδιού στο Σχήμα 2.2.

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Σχήμα 2.1: Πίνακες κατάστασης και κλειδιού για $N_b = 6$ και $N_k = 4$ αντίστοιχα [10]

Ο αριθμός των γύρων, που συμβολίζεται ως N_r, εξαρτάται από τις τιμές N_b και N_k. Ορισμένες ενδεικτικές τιμές φαίνονται στο Σχήμα 2.2.

		N_b		
		4	6	8
N_k	4	10	12	14
	6	12	12	14
	8	14	14	14

Σχήμα 2.2: Αριθμός γύρων, N_r, συναρτήσει των $N_b = 6$ και $N_k = 4$ [10]

2.3 Ο κυκλικός μετασχηματισμός

Ο κυκλικός μετασχηματισμός αποτελείται από τέσσερις επιμέρους μετασχηματισμούς. Ακολουθεί ο κυκλικός μετασχηματισμός σε ψευδογλώσσα C:

```
Round(State,RoundKey){
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}
```

Ο τελευταίος γύρος της κρυπτογράφησης είναι λίγο διαφορετικός, όπως φαίνεται και στον επόμενο ψευδοκώδικα:

```
FinalRound(State,RoundKey) {
ByteSub(State);
ShiftRow(State);
AddRoundKey(State,RoundKey);
}
```

Όπως φαίνεται από τα παραπάνω, στον τελευταίο γύρο ο μετασχηματισμός MixColumn δεν εκτελείται. Στη συνέχεια παρατίθενται οι λειτουργίες κάθε επιμέρους μετασχηματισμού.

ByteSub. Ο μετασχηματισμός ByteSub είναι μία μη γραμμική αντικατάσταση ψηφιολέξης, η οποία επιδρά ανεξάρτητα σε κάθε ψηφιολέξη κατάστασης. Ο πίνακας αντικατάστασης (substitution table / S-box) είναι αντιστρέψιμος και προκύπτει από τη σύνθεση δύο μετασχηματισμών:

1 Αρχικά, παίρνει τον πολλαπλασιαστικό αντίστροφο (multiplicative inverse) στο σύνολο $GF(2^8)$, όπου GF σημαίνει πεδίο Galois, με το μηδενικό στοιχείο να αντιστοιχίζεται στον εαυτό του.

2 Έπειτα εφαρμόζει τον μετασχηματισμό συσχέτισης

ShiftRow. Στο μετασχηματισμό ShiftRow, οι τελευταίες τρεις γραμμές της κατάστασης ολισθαίνουν κυκλικά κατά διαφορετικό αριθμό θέσεων. Η γραμμή 1 ολισθαίνει κατά C_1 ψηφιολέξεις, η γραμμή 2 κατά C_2 και η γραμμή 3 κατά C_3 ψηφιολέξεις. Ο αριθμός των θέσεων ολίσθησης C_1, C_2

και C_3 εξαρτάται από το μήκος του τμήματος N_b. Μπορούμε να δούμε τις τιμές αυτές στο Σχήμα 2.3.

N_b	C_1	C_2	C_3
4	1	2	3
6	1	2	3
8	1	3	4

Σχήμα 2.3: Αριθμός θέσεων ολίσθησης για διαφορετικά μεγέθη τμημάτων [10]

MixColumn. Στο μετασχηματισμό MixColumn, οι στήλες της κατάστασης θεωρούνται πολυώνυμα στο σύνολο $GF(2^8)$ και πολλαπλασιάζονται σε αριθμητική modulo $x^4 + 1$ με ένα πολυώνυμο $c(x)$, το οποίο δίνεται από τη σχέση $c(x) = 3x^3 + x^2 + x + 2$. Η πράξη του μετασχηματισμού φαίνεται στο Σχήμα 2.4, όπου έχουμε ουσιαστικά την εξίσωση $b(x) = c(x) \otimes a(x)$.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2\,3\,1\,1 \\ 1\,2\,3\,1 \\ 1\,1\,2\,3 \\ 3\,1\,1\,2 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Σχήμα 2.4: Μετασχηματισμός MixColumn [10]

Τέλος, έχει απομείνει να οριστεί η συνάρτηση AddRoundKey. Σε αυτή, ένα κλειδί γύρου (round key) εφαρμόζεται σε κάθε κατάσταση. Η εφαρμογή αυτή γίνεται μέσω της πράξης XOR, μεταξύ των δυαδικών ψηφίων του κλειδιού και της κατάστασης. Το μέγεθος του κλειδιού είναι ίδιο με το μέγεθος του τμήματος, δηλαδή N_b.

Κεφάλαιο 3

Περιγραφή Grindahl

3.1 Εισαγωγή

Με τον όρο Grindahl αναφερόμαστε σε μία οικογένεια συναρτήσεων κατακερματισμού, οι οποίες βασίζονται στη στρατηγική Συνένωσε-Μετέθεσε-Απέκοψε (Concatenate-Permute-Truncate). Στην περίπτωσή μας η μετάθεση χρησιμοποιεί τις σχεδιαστικές αρχές του Rijndael, οι οποίες έχουν υιοθετηθεί και στην ανάπτυξη του Προηγμένου Προτύπου Κρυπτογράφησης (Advanced Encryption Standard - AES). Συγκεκριμένα, ορίζονται δύο αλγόριθμοι μεγέθους εξόδου (σύνοψης) 256-bit και 512-bit. Ακόμη, θεωρείται ότι η συνάρτηση συμπίεσης είναι δεδομένη και δέχεται εισόδους δεδομένου μήκους.

3.2 Γενική στρατηγική

Στην ενότητα αυτή περιγράφεται η στρατηγική με την οποία σχεδιάζεται μία συνάρτηση κατακερματισμού μήκους n-bit. Με m συμβολίζεται το μέγεθος της κατάστασης (state size) και με b το μέγεθος του μηνύματος (message size), απαιτώντας $m \geq n$ και $b > 0$. Ακόμη, ορίζεται η συνάρτηση $trunc_k(x)$ η οποία περιέχει τα k λιγότερο σημαντικά δυαδικά ψηφία του x. Τέλος, ως $P : \{0,1\}^{m+b} \rightarrow \{0,1\}^{m+b}$ συμβολίζεται η μη γραμμική μετάθεση (non-linear permutation), ενώ s_0 είναι η αρχική κατάσταση με $|s_0| = m$.

Έστω d μήνυμα το οποίο πρέπει να κατακερματιστεί, το οποίο υποτίθεται ότι είναι ήδη προσαυξημένο. Το επιθυμητό είναι να χωριστεί σε t αριθμό τμημάτων (blocks) μεγέθους b δυαδικών ψηφίων το καθένα, δηλαδή $d = d_1 || \cdots || d_t, |d_i| = b$. Η διαδικασία είναι η εξής:

Για κάθε $0 < i \leq t$

$S_i \leftarrow d_i \| s_{i-1}$	συνένωσε (concatenate)
$\tilde{S} \leftarrow P(S_i)$	μετέθεσε (permute)
$s_i \leftarrow trunc_m(\tilde{S})$	απέκοψε (truncate)

Έτσι, ένα τμήμα μηνύματος συνενώνεται με την κατάσταση ώστε να δημιουργήσει μία επεκτεταμένη κατάσταση (extended state), πάνω στην οποία θα εφαρμοστεί μία μετάθεση P. Ακολούθως, η επεκτεταμένη κατάσταση αποκόπτεται ώστε να διαμορφωθεί η νέα κατάσταση. Τα βήματα αυτά συντελούν έναν γύρο εισόδου (input round).

Ακόμη, ορίζεται ένας μετασχηματισμός εξόδου (σύνοψης) ο οποίος αποτελείται από κενούς γύρους (blank rounds) και από μία αποκοπή στο τέλος. Ένας κενός γύρος είναι ουσιαστικά η παρακάτω ακολουθία:

Για $t < i \leq t + v_{br}, v_{br} \geq 0$

$$\tilde{S}_i \leftarrow P(\tilde{S}_{i-1})$$

Δηλαδή οι κενοί γύροι λειτουργούν μόνο στην επεκτεταμένη κατάσταση, πράγμα που σημαίνει ότι στην επεξεργασία του τελευταίου τμήματος του μηνύματος d_t η λειτουργία της αποκοπής μπορεί να εφαρμοστεί.Η έξοδος της συνάρτησης κατακερματισμού θα είναι λοιπόν $trunc_n(\tilde{S}_{t+v_{br}})$.

3.3 Αντιστρεψιμότητα

Με τον όρο αντιστρεψιμότητα (invertibility) εννοείται η δυνατότητα ανάκτησης του μηνύματος, μέσω ορισμένου μετασχηματισμού της εξόδου. Υπό αυτή την έννοια η συνάρτηση κατακερματισμού θα μπορούσε να είναι αντιστρέψιμη, αφού χρησιμοποιεί την μετάθεση P. Δηλαδή, αν η μετάθεση P είναι ευάλωτη σε επιθέσεις κατά τις οποίες από την έξοδο είναι δυνατόν να υπολογιστούν τόσο το μήνυμα όσο και η αρχική κατάσταση, τότε καθίσταται ευάλωτη και η ίδια η συνάρτηση κατακερματισμού. Κάτι τέτοιο μπορεί να αποφευχθεί, αν η μετάθεση P έχει ιδιότητες κρυπτογράφησης τέτοιες ώστε ο επιτιθέμενος να μην μπορεί να εκμεταλλευθεί την αρχική κατάσταση που έχει αποκαλύψει.

Η πιθανότητα επιτυχίας μίας επίθεσης του τύπου "επίθεση της συνάντησης στο ενδιάμεσο" (meet in the middle attack), εξαρτάται από το μέγεθος της κατάστασης, δηλαδή του m. Αν δεν εντοπιστούν αδυναμίες

της μετάθεσης P, ώστε να οδηγήσουν στην αποκάλυψη της αρχικής κατάστασης, τότε οι επιθέσεις του τύπου "εσωτερική σύγκρουση" (internal collision), δηλαδή συγκρούσεις πριν τους κενούς γύρους, και "επίθεση της συνάντησης στο ενδιάμεσο" έχουν πολυπλοκότητα $2^{m/2}$. Υπό την προϋπόθεση ότι δεν υπάρχει καμία επίθεση δευτερεύουσας αντίστασης προ-απεικόνισης η οποία να είναι καλύτερη της εξαντλητικής αναζήτησης, δηλαδή τοποθετούμε ένα άνω φράγμα για τη δυνατότητα επίθεσης δευτερεύουσας αντίστασης προ-απεικόνισης, το μέγεθος της κατάστασης πρέπει να επιλεγεί έτσι ώστε $m \geq 2n$.

3.4 Προσέγγιση του σχεδιασμού μετάθεσης

Μία γνωστή οικογένεια μεταθέσεων είναι εκείνη του αλγορίθμου κρυπτογράφησης κατά τμήματα του Rijndael. Ορισμένες από αυτές μάλιστα υιοθετήθηκαν από την Αμερικανική κυβέρνηση στα πλαίσια του Προηγμένου Προτύπου Κρυπτογράφησης (AES). Με βάση τον αλγόριθμο του Rijndael θα αναπτυχθεί μία προσέγγιση για την κατασκευή της μετάθεσης P.

Αρχικά, τοποθετούμε τις επεκταμένες καταστάσεις σε ένα πίνακα (μητρώο) δυαδικών ψηφίων. Συμβολίζοντας τον πίνακα με α, οι διαστάσεις του είναι $v_{rw} \times v_{cl}$. Τα στοιχεία του πίνακα α θα συμβολίζονται με με $\alpha_{i,j}$, όπου i είναι η γραμμή και j η στήλη. Η αρίθμηση ξεκινά από το 0 και οι δείκτες υπολογίζονται βάσει της αριθμητικής modulov_{rw} και v_{cl} αντίστοιχα. Ο πίνακας των επεκταμένων καταστάσεων λοιπόν είναι:

$$\alpha = \begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \cdots & \alpha_{0,v_{cl}-1} \\ \alpha_{1,0} & \alpha_{1,1} & \cdots & \alpha_{1,v_{cl}-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{v_{rw}-1,0} & \alpha_{v_{rw}-1,1} & \cdots & \alpha_{v_{rw}-1,v_{cl}-1} \end{pmatrix}$$

Υποθέτουμε ότι το μέγεθος του μηνύματος b είναι πολλαπλάσιο του 8, οπότε μπορούμε να ορίσουμε ως $v_{mb} = b/8$ τον αριθμό των ψηφιολέξεων (bytes) που αποτελούν ένα τμήμα του μηνύματος. Σύμφωνα με την διαδικασία κατακερματισμού, η λειτουργία της αποκοπής ακολουθείται από εκείνη της συνένωσης, με το επόμενο τμήμα του μηνύματος. Αυτό σημαίνει ότι ένας αριθμός από v_{mb} ψηφιολέξεις της επεκταμένης κατάστασης θα αντικατασταθούν. Βέβαια, οι ψηφιολέξεις αυτές υπολο-

γίζονται μόνο κατά τον γύρο της τελευταίας εισόδου.

Για την σχεδίαση της συνάρτησης κατακερματισμού Grindahl χρησιμοποιούνται οι ακόλουθοι μετασχηματισμοί:

SubBytes. Η μη γραμμική συνάρτηση αντικατάστασης (substitution function) SubBytes ορίζεται όπως και στην περίπτωση του Rijndael. Ως συνάρτηση αντικατάστασης ορίζουμε τη σχέση εκείνη, που χρησιμοποιείται για να αποσυχετίσει το κλειδί (key) από το κρυπτογραφημένο μήνυμα.

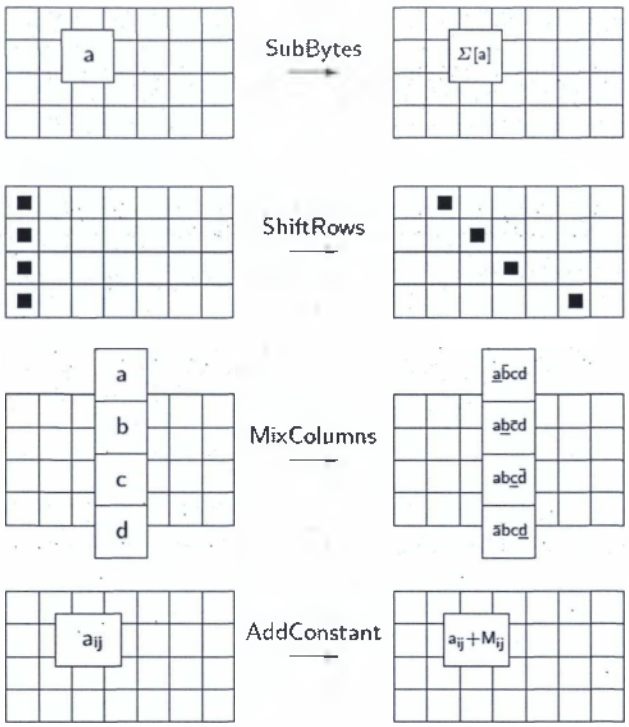
ShiftRows. Ο μετασχηματισμός αυτός ολισθαίνει κυκλικά (cyclic shift) τις ψηφιολέξεις, κατά έναν αριθμό θέσεων σε κάθε γραμμή. Σημειώνουμε τις σταθερές περιστροφής (rotation constants) ως ακολουθίες. Δηλαδή για την v_{rw}-άδα έχουμε την ακολουθία $(\rho_0, \rho_1, \cdots, \rho_{v_{rw}-1})$ των ακεραίων $0 \leq \rho_i < v_{cl}$, με το ρ_i να περιέχει τον αριθμό των θέσεων που θα ολισθήσουν προς τα δεξιά οι ψηφιολέξεις της γραμμής i.

MixColumns. Ο μετασχηματισμός αυτός είναι ίδιος με εκείνον στην περίπτωση του Rijndael για $v_{rw} = 4$. Για διαφορετική τιμή του v_{rw} ο μετασχηματισμός πρέπει να επαναπροσδιοριστεί. Η σημαντική ιδιότητα της διάδοσης της μέγιστης διαφοράς (maximal difference) πρέπει να διατηρείται. Με άλλα λόγια, όταν υπάρχει μία διαφορά σε $k > 0$ ψηφιολέξεις πριν την εφαρμογή του μετασχηματισμού, τότε μετά την εφαρμογή του θα πρέπει να έχουν αλλάξει τουλάχιστον $v_{rw} - k + 1$ ψηφιολέξεις.

AddConstant. Ο μετασχηματισμός αυτός αντικαθιστά τον αντίστοιχο AddRoundKey του Rijndael. Σκοπός του είναι να εισάγει ασυμμετρία σε κάθε γύρο. Έχοντας τον πίνακα επεκταμένων καταστάσεων α, που παρουσιάστηκε παραπάνω, καθώς και έναν άλλο πίνακα M ίδιου μεγέθους, ο μετασχηματισμός ορίζεται ως εξής:

$$AddConstant(\alpha) = M \oplus \alpha$$

Στο Σχήμα 3.1 που ακολουθεί φαίνονται γραφικά οι προηγούμενοι μετασχηματισμοί. Η εφαρμογή τους γίνεται σε ένα πίνακα α μεγέθους 4×7. Με Σ συμβολίζουμε την συνάρτηση αντικατάστασης, ενώ οι σταθερές περιστροφής είναι (1,2,3,5).



Σχήμα 3.1: Μετασχηματισμοί των επεκταμένων καταστάσεων [3]

Οι παραπάνω μετασχηματισμοί εφαρμόζονται σε έναν πίνακα ψηφιολέξεων. Μπορούν ωστόσο να εφαρμοστούν και σε συμβολοσειρά (string), υπό την προϋπόθεση ότι θα γίνει η αντιστοίχιση μεταξύ των ψηφιολέξεων των επεκταμένων καταστάσεων του πίνακα και της συμβολοσειράς. Η αντίστροφη διαδικασία, δηλαδή η αντιστοίχιση των ψηφιολέξεων της συμβολοσειράς σε πίνακα είναι επίσης εφικτή. Αρχικά θεωρούμε ότι έχουμε τη συμβολοσειρά x, μήκους $8v_{rw}v_{cl}$ δυαδικών ψηφίων. Η αντιστοίχιση, μεταξύ της επεκταμένης κατάστασης α και της συμβολοσειράς x, γίνεται χωρίζοντας τη συμβολοσειρά σε $v_{rw}v_{cl}$ αριθμό τμημάτων μήκους 8 δυαδικών ψηφίων το καθένα, τα οποία συμβολίζουμε με $x_0, \cdots x_{v_{rw}v_{cl}}$, και αναθέτοντας $\alpha_{i,j} = x_{i+v_{rw}j}$, όπου $0 \leq i < v_{rw}$ και $0 \leq j < v_{cl}$. Η αντιστοιχία αυτή είναι αντιστρέψιμη.

Χρησιμοποιώντας τους παραπάνω μετασχηματισμούς, η μετάθεση P ορίζεται ως:

$$P(\alpha) = MixColumns \circ ShiftRows \circ SubBytes \circ AddConstant(\alpha)$$

3.5 Παράμετροι σχεδιασμού μετάθεσης

Στην ενότητα αυτή παρουσιάζονται ορισμένες παράμετροι που αφορούν το σχεδιασμό της μετάθεσης.

3.5.1 Σταθερές περιστροφής

Με τον όρο σταθερές περιστροφής (rotation constants) αναφερόμαστε στον αριθμό των θέσεων ολίσθησης, όπως αυτός ορίζεται στο μετασχηματισμό ShiftRows που παρουσιάστηκε νωρίτερα. Οι σταθερές αυτές πρέπει να επιλεγούν με τρόπο, ο οποίος να διασφαλίζει ότι ολόκληρη η κατάσταση εξαρτάται από το μήνυμα εισόδου, το ταχύτερο δυνατό, αφού οι πρώτες v_{mb} ψηφιολέξεις της κατάστασης αντικαθίστανται από τον αντίστοιχο αριθμό bytes της εισόδου σε κάθε γύρο.

Αρκετά διανύσματα σταθερών περιστροφής εγγυώνται διάχυση (diffusion) μετά από τον ίδιο αριθμό γύρων μ. Ορισμένα από αυτά, όμως, είναι προτιμότερα διότι μεγαλύτερο τμήμα της κατάστασης εξαρτάται από κάθε ψηφιολέξη του μηνύματος έπειτα από $\{\mu-1, \mu-2, \cdots, \mu-n\}$ γύρους.

Μία μέθοδος επιλογής σταθερών περιστροφής δεδομένης της γεωμετρίας της επεκταμένης κατάστασης παρουσιάζεται στην εργασία των Knudsen,Rechberger,Thomsen [3]. Σύμφωνα με αυτή, έστω R_1 το σύνολο των v_{rw}-άδων των σταθερών περιστροφής που εγγυώνται βέλτιστη διάχυση. Αυτό θα μπορούσε να συμβεί για παράδειγμα όταν όλες οι ψηφιολέξεις της κατάστασης αντιστοιχίζονται άμεσα με όλες τις ψηφιολέξεις του μηνύματος. Συνεχίζοντας, έστω $R_2 \subseteq R_1$ το υποσύνολο σταθερών περιστροφής του R_1 που δίνουν την ίδια εγγύηση στους κενούς γύρους. Αυτό θα μπορούσε να γίνει όταν καμία ψηφιολέξη κατάστασης δεν αντικαθίσταται με κάποια από εκείνες του μηνύματος εισόδου. Συμβολίζουμε με $f_j(d_i)$ τον αριθμό των bytes της κατάστασης που επηρεάζονται από το byte εισόδου d_i, έπειτα από το πέρας j γύρων. Ακόμη, έστω μ ο αριθμός των γύρων που απαιτούνται ώστε κάθε ψηφιολέξη της κατάστασης να επηρεαστεί από την αντίστοιχη της εισόδου. Επίσης θεωρούμε ότι το $R_3 \subseteq R_2$ είναι το υποσύνολο του R_2 για το οποίο το άθροισμα

$$\sum_{j=1}^{\mu-1} \sum i = 0^{v_{mb}-1} f_j(d_i)$$

είναι μέγιστο. Αν ταξινομήσουμε λεξικογραφικά το υποσύνολο R_3, τότε η επιλογή των σταθερών περιστροφής πρέπει να είναι το πρώτο διάνυσμα, εξαρτάται από τη γεωμετρία του προβλήματος, του ταξινομημένου αυτού υποσυνόλου.

3.5.2 Γεωμετρία κατάστασης

Οι επιλογές των v_{rw} και v_{cl}, δηλαδή των διαστάσεων του πίνακα καταστάσεων, αποτελούν έναν συμβιβασμό (tradeoff) μεταξύ δύο διαφορετικών ιδιοτήτων. Αν οι δύο αριθμοί είναι σχεδόν ίδιοι τότε η διάχυση συμβαίνει ταχύτερα, σε σχέση με την περίπτωση όπου έχουμε περισσότερες στήλες από ότι γραμμές. Αντίθετα, μία επιλογή μεγάλης τιμής για την διάσταση v_{rw}, αλλά με μία μόνο στήλη να χρησιμοποιείται για το μήνυμα εισόδου, η επεκταμένη κατάσταση χρειάζεται να είναι λίγο μεγαλύτερη της εξόδου. Πρακτικά, η διάσταση v_{rw} επιλέγεται να είναι πολλαπλάσιο του 4, έτσι ώστε οι μετασχηματισμοί SubBytes και MixColumns να εκτελούνται μαζί στα συστήματα αρχιτεκτονικής 32 δυαδικών ψηφίων.

3.6 Παράμετροι σχεδιασμού του μετασχηματισμού της εξόδου

Ο αριθμός των κενών γύρων, v_{br}, πρέπει να επιλεγεί με τέτοιο τρόπο ώστε το τελευταίο τμήμα του μηνύματος να επηρεάζει όλες τις ψηφιολέξεις εξόδου. Ο μετασχηματισμός της εξόδου πρέπει να έχει μία επιπλέον ιδιότητα, η οποία θα του δίνει τη συμπεριφορά μίας ψευδοτυχαίας (pseudo-random) συνάρτησης. Αυτό βέβαια δεν είναι εύκολο να επιτευχθεί μιας και ο μετασχηματισμός της εξόδου είναι αντιστρέψιμη συνάρτηση, υπάρχει δηλαδή ένας τρόπος μετασχηματισμού της στο αρχικό μήνυμα. Είναι βέβαιο, όμως, το γεγονός ότι μία ψευδοτυχαία συμπεριφορά θα δυσκόλευε τον επιτιθέμενο, στην προσπάθειά του να εντοπίσει εξωτερικές συγκρούσεις (external collisions).

Όταν ο αριθμός των κενών γύρων είναι v_{br}, η χρήση της μετάθεσης P, μετά το τελευταίο τμήμα, συγκεντρώνεται στην κατάσταση $v_{br}+1$. Κατά τη διάρκεια των γύρων αυτών δεν υπάρχει αντικατάσταση των ψηφιολέξεων των καταστάσεων από το μήνυμα εισόδου. Αφού λοιπόν καθοριστεί ο χρόνος για να συμβεί το παραπάνω, έστω ότι ισούται με μ γύρους, τότε η επιλογή του αριθμού των κενών γύρων θα είναι $v_{br} \geq \mu - 1$.

Κεφάλαιο 4

Συναρτήσεις κατακερματισμού Grindahl

4.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζονται οι συναρτήσεις κατακερματισμού Grindahl. Πρόκειται για δύο συναρτήσεις, οι οποίες έχουν μέγεθος εξόδου 256 δυαδικών ψηφίων (256-bit) και 512 δυαδικών ψηφίων (512-bit) αντίστοιχα [3]. Θεωρούμε ότι και στις δύο συναρτήσεις οι αρχικές καταστάσεις αποτελούνται μόνο από μηδενικά. Σημαντική ακόμη παράμετρος είναι και ο κανόνας προσαύξησης (padding rule) ο οποίος θα παρουσιαστεί στην ενότητα που ακολουθεί.

4.2 Κανόνας προσαύξησης

Ο κανόνας προσαύξησης ακολουθείται και από τους δύο αλγόριθμους που θα παρουσιαστούν στη συνέχεια. Αρχικά, προσαρτούμε (append) το δυαδικό ψηφίο "1" στο μήνυμα, ενώ φροντίζουμε ώστε να συμπληρώσουμε με δυαδικά ψηφία "0" το τελευταίο τμήμα του μηνύματος, αφού το πιθανότερο είναι ότι κατά την τμηματοποίηση, το τελευταίο κομμάτι δεν θα έχει από μόνο του το ίδιο μέγεθος με τα υπόλοιπα. Στη συνέχεια, προσαρτούμε στο προσαυξημένο μήνυμα τον αριθμό των τμημάτων στα οποία διαιρέθηκε το μήνυμα εισόδου. Ο αριθμός αυτός καταλαμβάνει 64 δυαδικά ψηφία (64-bit). Το τελευταίο σημαίνει ότι η συνάρτηση κατακερματισμού μπορεί να χειριστεί μήνυμα το οποίο αποτελείται από $2^{64} - 1$ τμήματα, συμπεριλαμβανομένων και των προσαυξήσεων.

4.3 Grindahl-256

Αρχικά, πρέπει να σημειώσουμε ότι όλες οι σταθερές που εμφανίζονται αναπαρίστανται στο δεκαεξαδικό σύστημα (hexadecimal).Η συνάρτηση κατακερματισμού Grindahl-256 ορίζει τις παρακάτω τιμές σταθερών:

Πίνακας 4.1: Σταθερές για Grindahl-256.

v_{rw}	4
v_{cl}	13
v_{mb}	4
v_{br}	8

Έτσι, η επεκταμένη κατάσταση έχει 4 σειρές και 13 στήλες, ενώ το μήνυμα εισόδου είναι μεγέθους 32 δυαδικών ψηφίων. Στις λειτουργίες της συνένωσης και της αποκοπής, τα 32 δυαδικά ψηφία του μηνύματος θα αντικαταστήσουν την πρώτη στήλη της επεκταμένης κατάστασης. Ακόμη, εισάγονται 8 κενοί γύροι οι οποίοι απαιτούνται για την μετατροπή της εξόδου (σύνοψης).

Όσον αφορά τις σταθερές περιστροφής που απαιτούνται για τη λειτουργία της ShiftRows αυτές είναι οι (1,2,4,10). Η επιλογή τους βασίζεται στη μέθοδο που περιγράφηκε στην υπο-ενότητα "Σταθερές περιστροφής". Οι σταθερές αυτές εγγυώνται ότι κάθε ψηφιολέξη του μηνύματος θα επηρεάσει ολόκληρη την επεκταμένη κατάσταση, έπειτα από το πέρας τεσσάρων γύρων. Οι μετασχηματισμοί SubBytes και MixColumns ορίζονται όπως και στην περίπτωση του Rijndael. Τέλος, ο μετασχηματισμός AddConstant ορίζεται ως:

$$\alpha_{3,12} \leftarrow \alpha_{3,12} \oplus 01$$

4.4 Grindahl-512

Αρχικά, πρέπει να σημειώσουμε ότι όλες οι σταθερές που εμφανίζονται αναπαρίστανται στο δεκαεξαδικό σύστημα. Ορίζουμε τις τιμές των σταθερών που χρησιμοποιεί η υπό μελέτη συνάρτηση κατακερματισμού:

Πίνακας 4.2: Σταθερές για Grindahl-512.

v_{rw}	8
v_{cl}	13
v_{mb}	8
v_{br}	8

Οι τιμές των σταθερών επισημαίνουν ότι κάθε κατάσταση έχει 8 σειρές και 13 στήλες, ενώ το μέγεθος του μηνύματος εισόδου είναι 64 δυαδικά ψηφία, τα οποία βέβαια αντικαθιστούν την πρώτη στήλη της επεκταμένης κατάστασης.

Οι κατάλληλες σταθερές περιστροφής, για το μετασχηματισμό ShiftRows, είναι οι (1,2,3,4,5,6,7,8), οι οποίες διαχέονται πλήρως μετά από τρεις γύρους. Οι σταθερές αυτές προκύπτουν από τη μέθοδο που περιγράφεται στην υπο-ενότητα "Σταθερές περιστροφής". Ο μετασχηματισμός MixColumns ορίζεται ως:

$$MixColumns(\alpha) = A \cdot \alpha$$

όπου

$$A = \begin{pmatrix} 02 & 0c & 06 & 08 & 01 & 04 & 01 & 01 \\ 01 & 02 & 0c & 06 & 08 & 01 & 04 & 01 \\ 01 & 01 & 02 & 0c & 06 & 08 & 01 & 04 \\ 04 & 01 & 01 & 02 & 0c & 06 & 08 & 01 \\ 01 & 04 & 01 & 01 & 02 & 0c & 06 & 08 \\ 08 & 01 & 04 & 01 & 01 & 02 & 0c & 06 \\ 06 & 08 & 01 & 04 & 01 & 01 & 02 & 0c \\ 0c & 06 & 08 & 01 & 04 & 01 & 01 & 02 \end{pmatrix}$$

Στο παραπάνω γινόμενο οι ψηφιολέξεις θεωρούνται στοιχεία του πεδίου $\mathbb{F}_{256}$, όπως αυτό ορίζεται στον Rijndael. Ο μετασχηματισμός αυτός εγγυάται μέγιστη διάδοση διαφορών, αφού ο κώδικας διόρθωσης λαθών στο πεδίο $\mathbb{F}_{256}$, με αρχικό πίνακα $[IA^T]$, είναι μέγιστης απόστασης διαχωρίσιμος (maximum distance separable - MDS). Ο μετασχηματισμός SubBytes ορίζεατι όπως και στον Rijndael, ενώ ο AddConstant είναι ο ακόλουθος:

$$\alpha_{7,12} \leftarrow \alpha_{7,12} \oplus 01$$

4.5 Ασφαλής συνάρτηση συμπίεσης

Οι μέθοδοι για κατασκευή συναρτήσεων κατακερματισμού Grindahl, μεταβλητού μήκους εισόδων, μπορούν εύκολα να χρησιμοποιηθούν για ανάπτυξη συναρτήσεων συμπίεσης, με σταθερό μήκος εισόδων. Έστω ότι H είναι ένα στιγμιότυπο της οικογένειας συναρτήσεων Grindahl με αρχική κατάσταση s_0, όπου έχει εφαρμοστεί προσαύξηση. Αυτό σημαίνει, ότι το H δέχεται μηνύματα των οποίων το μέγεθος είναι ακέραιο πολλαπλάσιο του b (σε δυαδικά ψηφία). Αν το μέγεθος της εξόδου του H είναι n, τότε ορίζεται η συνάρτηση συμπίεσης:

$$h : \{0,1\}^{tb} \rightarrow \{0,1\}^n$$

Παρατηρούμε ότι η συνάρτηση συμπίεσης παίρνει μόνο ένα όρισμα ως είσοδο, ενώ συνήθως τέτοιου είδους συναρτήσεις λαμβάνουν δύο εισόδους, μία μεταβλητή αλυσίδωσης και ένα τμήμα μηνύματος. Όμως στην προσέγγισή μας χρησιμοποιούμε τις μεταβλητές αυτές ως μία ενιαία. Αυτό συμβαίνει διότι σε περίπτωση επίθεσης, ο επιτιθέμενος επιθυμεί να αποκτήσει τον έλεγχο των μεταβλητών αλυσίδωσης, όμως η ενοποίηση των μεταβλητών αλυσίδωσης και μηνύματος που εφαρμόσαμε, θα δυσκολεύει σημαντικά το έργο του. Η ενοποίηση αυτή στις περισσότερες περιπτώσεις είναι απλά συνένωση των δύο μεταβλητών, οπότε η συνάρτηση συμπίεσης ορίζεται ως:

$$h : \{0,1\}^n \times \{0,1\}^{tb-n} \rightarrow \{0,1\}^n$$

οπότε

$$h(c, x) = H(c||x)$$

Η επιλογή της παραμέτρου t, επισημαίνει ότι υπάρχει ένας συμβιβασμός μεταξύ ταχύτητας συμπίεσης και ασφάλειας. Πράγματι, μειώνοντας την τιμή της παραμέτρου t αυξάνεται η ασφάλεια, όμως μειώνεται η ταχύτητα, διότι ο αριθμός των κενών γύρων αυξάνεται σε σχέση με τους γύρους εισόδου.Στην περίπτωση που απαιτείται μία επιπλέον είσοδος για τη συνάρτηση συμπίεσης, τότε είναι προτιμότερο αυτή να λάβει τη μορφή προθέματος στις ήδη ενοποιημένες μεταβλητές αλυσίδωσης και μηνύματος.

Επιχειρώντας να γίνουμε πιο συγκεκριμένοι, σχετικά με τον τις παραμέτρους λειτουργίας της συνάρτησης συμπίεσης, μπορούμε να εστιάσουμε στις λεπτομέρειές της, όταν βασίζεται στους Grindahl-256 και

Grindahl-512. Αρχικά επιλέγεται η παράμετρος t να ισούται με $40 + s$. Το s δηλώνει τον αριθμό των τμημάτων εισόδου που χρησιμοποιούνται επιπλέον είσοδοι (όπως για παράδειγμα κλειδιά, μετρητές), όπου βέβαια μπορεί $s = 0$. Έτσι, οι συναρτήσεις συμπίεσης λαμβάνουν είσοδο μήκους $(40 + s)v_{mb}$ ψηφιολέξεων. Αυτό αντιστοιχεί σε $1280 + 32s$ δυαδικά ψηφία και $2560 + 64s$ δυαδικά ψηφία για τους Grindahl-256 και Grindahl-512 αντίστοιχα. Από τα δυαδικά ψηφία αυτά 1024 και 2048 αντίστοιχα, αποτελούν το μήνυμα εισόδου, ενώ τα υπόλοιπα ανήκουν στη μεταβλητή αλυσίδωσης και στην επιπλέον είσοδο (αν υπάρχει.)

Κεφάλαιο 5

Ανάλυση τρόπων επίθεσης στη συνάρτηση κατακερματισμού

5.1 Εισαγωγή

Στο κεφάλαιο αυτό εμβαθύνουμε στις μεθόδους με τις οποίες κάποιος κακόβουλος χρήστης, μπορεί να αποκαλύψει τον τρόπο με τον οποίο λειτουργεί η συνάρτηση κατακερματισμού. Οι μέθοδοι αναφέρονται στη βιβλιογραφία με τον όρο "κρυπτανάλυση" ο οποίος σημαίνει: μελέτη και επινόηση μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας, έχοντας ως άγνωστες ποσότητες τον κρυφό μετασχηματισμό, το κλειδί, με βάση το οποίο αυτός πραγματοποιήθηκε και το κρυπτογραφημένο μήνυμα. Βασικός στόχος της είναι, ανάλογα με της απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή, να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το (κρυφό) μήνυμα [11]. Στην ανάλυση των μεθόδων, εστιάζουμε το ενδιαφέρον μας στο πώς εφαρμόζονται στις συναρτήσεις κατακερματισμού Grindahl [8].

5.2 Διαφορική κρυπτανάλυση

Η διαφορική κρυπτανάλυση εξετάζει ζεύγη κρυπτογραμματων, των οποίων τα αρχικά μηνύματα διαφέρουν σε συγκεκριμένες θέσεις (chosenplaintext attack). Προσομοιώνοντας τον αλγόριθμο, κάποια κλειδιά είναι πιο πιθανά από κάποια άλλα, με δεδομένη την προηγούμενη συνθήκη. Όσο πιο πολλά κρυπτογραφήματα αναλύονται, τόσο πιο πολλά κλειδιά απορρίπτονται ως λιγότερο πιθανά [14].

Πιο συγκεκριμένα, εξετάζεται η δοκιμή δύο διαφορετικών μηνυμάτων, έστω M και M', ξεκινώντας από την αρχική κατάσταση s_0, ενώ η δοκιμή διαρκεί k επαναλήψεις. Αυτό που αναζητείται, είναι ο διαδικασία με την οποία η συνάρτηση κατακερματισμού θα αποδώσει ίδια αποτελέσματα, για τα διαφορετικά μηνύματα M και M'. Μία επιτυχημένη αναζήτηση αυτού του είδους θα μπορούσε να είναι η $trunc_{256}(S_m + 8) = trunc_{256}(S_{m'} + 8)$. Αυτό σημαίνει, ότι ενδιαφερόμαστε για επιθέσεις που αφορούν συγκρούσεις και δευτερεύουσα αντίσταση προ-απεικόνισης.

Η παραπάνω αναζήτηση δεν μπορεί να εφαρμοστεί κατά τους κενούς γύρους, μιας και δεν γίνεται επεξεργασία τμημάτων του μηνύματος, οπότε και υπάρχει μικρό περιθώριο δοκιμών στο στάδιο αυτό. Αντίθετα, η αναζήτηση γίνεται ευκολότερα όταν αφορά εσωτερικές συγκρούσεις (internal collisions). Στις ενότητες που ακολουθούν εξετάζουμε τους τρόπους που μας καθιστούν επιτυχή την αναζήτηση, με μεγάλη πιθανότητα επιτυχίας.

5.3 Ανάλυση των αποκομμένων διαφορών

Η ανάλυση των αποκομμένων διαφορών (truncated differences) είναι μία ειδική περίπτωση διαφορικής κρυπτανάλυσης [4]. Σε αυτή ο επιτιθέμενος ελέγχει μόνο αν τα δύο μηνύματα εισόδου, έστω M και M', παράγουν διαφορετική σύνοψη, και όχι το κατά πόσο διαφέρουν οι συνόψεις μεταξύ τους. Απλοποιείται επομένως σημαντικά η πολυπλοκότητα της μεθόδου ανάλυσης.

Στη συνέχεια, ο επιτιθέμενος επιχειρεί να εντοπίσει μία ακολουθία αποκομμένων διαφορών, που έχει προκύψει από μία σειρά γύρων στους οποίους οι ενεργές ψηφιολέξεις είναι λίγες. Σε αυτή την ακολουθία εντοπισμού διαφορών (differential path), οι αποκομμένες διαφορές μπορούν να σβηστούν κατά τη διάρκεια δύο μόλις μετασχηματισμών σε κάθε επανάληψη. Οι μετασχηματισμοί αυτοί είναι ο MixColumns και ο $trunc c_m(\cdot)$, με την εκμετάλλευση του τελευταίου μόνο κατά το τέλος της επανάληψης. Με άλλα λόγια, χρησιμοποιώντας τον μετασχηματισμό MixColumns, το πλήθος των αποκομμένων διαφορών σε μία στήλη μπορεί να μειωθεί και οι θέσεις του να αλλάξουν · διαφορετικά, μία αποκομμένη διαφορά διαγράφεται όταν πηγαίνει στην πρώτη στήλη του πίνακα α, προς το τέλος της επανάληψης, εξαιτίας του μετασχηματισμού αποκοπής ($trunc c_m(\cdot)$).

Από τη στιγμή που ξεκινήσει η διαδικασία αναζήτησης των αποκομμένων διαφορών, το ενδιαφέρον στρέφεται στα τμήματα του μηνύματος που τροφοδοτούνται σε κάθε επανάληψη, προκειμένου να εξασφαλιστεί η επιθυμητή συμπεριφορά του μετασχηματισμού MixColumns. Αυτά τα τμήματα του μηνύματος λειτουργούν ως σήματα, με ενδείξεις "ενεργό"/"μη-ενεργό", αφού οι ψηφιολέξεις του κάθε τμήματος δεν επηρεάζουν την εσωτερική κατάσταση για ορισμένο αριθμό γύρων.

5.4 Ανάλυση της μετάδοσης διαφορών κατά τον μετασχηματισμό MixColumns

Όπως έχει ήδη αναφερθεί, ο μετασχηματισμός MixColumns είναι κοινός στις προσεγγίσεις Grindahl και Rijndael. Ο μετασχηματισμός αυτός διαθέτει την ιδιότητα της μέγιστης απόστασης διαχωρισμού. Το ενδιαφέρον όμως στρέφεται στον τρόπο με τον οποίο αυτός μπορεί να υποδείξει διαφορές, που θα μπορούσαν ενδεχομένως να αποκαλύψουν τον τρόπο λειτουργίας της συνάρτησης κατακερματισμού. Ο αριθμός των "ενεργών" ψηφιολέξεων (δανειζόμαστε τον όρο από την ενότητα "ανάλυση των αποκομμένων διαφορών") της εισόδου και της εξόδου, που μπορεί να γίνει αντιληπτός από τον μετασχηματισμό MixColumns, είναι μεγαλύτερος ή ίσος του 5.

Εξετάζοντας ένα συγκεκριμένο ενδεχόμενο, υποθέτουμε ότι δίνεται ένα μήνυμα ως είσοδος, έστω $V = (A, B, C, D)$. Το μήνυμα αυτό αποτελείται από τις τέσσερις ψηφιολέξεις A, B, C και D. Η έξοδος της συνάρτησης κατακερματισμού για αυτή την είσοδο θα είναι $W = (A', B', C', D')$, όπου τα A', B', C', D' είναι και πάλι τέσσερις ψηφιολέξεις. Συμβολίζουμε τον μετασχηματισμό MixColumns ως εξής:

$$MC : V \longrightarrow W$$

αλλιώς

$$MC : (A, B, C, D) \longrightarrow (A', B', C', D')$$

Ορίζουμε ακόμη τη συνάρτηση $D_i(V_1, V_2)$, η οποία επιστρέφει **1** αν η i-οστή ψηφιολέξη των V_1, V_2 είναι διαφορετική, αλλιώς η συνάρτηση επιστρέφει 0. Η συνάρτηση $D_i(\cdot)$ είναι ουσιαστικά αυτή που υποδεικνύει την εύρεση αποκομμένης διαφοράς. Ορίζουμε επίσης την συνάρτηση $ND(V_1, V_2)$ η οποία συγκεντρώνει τις διαφορές αυτές. Χρησιμοποιώντας

τις σχέσεις αυτές, για να περιγράψουμε το συμπέρασμα στο οποίο καταλήξαμε στην προηγούμενη παράγραφο, έχουμε ότι: αν $W_1 = MC(V_1)$ και $W_2 = MC(V_2)$, με $V_1 \neq V_2$, τότε

$$ND(V_1, V_2) + ND(W_1, W_2) \geq 5$$

Μία επίσης ενδιαφέρουσα ιδιότητα, προκύπτει από το γεγονός ότι κάθε ψηφιολέξη εισόδου στον μετασχηματισμό MixColumns ορίζει μία μετάθεση σε κάθε ψηφιολέξη εξόδου. Έτσι, με $W_1 = MC(V_1)$,$W_2 = MC(V_2)$ και $V_1 \neq V_2$ να λαμβάνονται τυχαία από ομοιόμορφη κατανομή, σχηματίζοντας έτσι 4 τυχαία διανύσματα με 8 στοιχεία το καθένα ($\{0,1\}^{4\times 8}$), έχουμε για κάθε $1 \leq i \leq 4$:

$$P_D = P\left[D_i(W_1, W_2) = 0\right] = \frac{256^3-1}{256^4-1} \simeq 2^{-8}$$
$$\overline{P_D} = P\left[D_i(W_1, W_2) = 1\right] = 1 - P_D \simeq 1 - 2^{-8}$$

Ο σκοπός είναι να υπολογιστεί η πιθανότητα, με την οποία μία προκαθορισμένη μάσκα (fixed mask) αποκομμένων διαφορών που αφορά την είσοδο, αντιστοιχίζεται με μία προκαθορισμένη μάσκα αποκομμένων διαφορών της εξόδου. Για παράδειγμα, επιθυμούμε να γνωρίζουμε την πιθανότητα με την οποία δύο είσοδοι, έστω V_1 και V_2, που διαφέρουν στις δύο πρώτες ψηφιολέξεις, μπορούν να δώσουν εξόδους που να διαφέρουν στις τρεις πρώτες ψηφιολέξεις, μέσω του μετασχηματισμού MixColumns.

Οι πιθανότητες που θέλουμε να γνωρίζουμε, μπορούν να υπολογιστούν με δύο τρόπους. Σύμφωνα με τον πρώτο, ο υπολογισμός μπορεί να γίνει με χρήση κανόνων πιθανοτήτων, πράγμα που σημαίνει κατασκευή πολύπλοκων μαθηματικών εξισώσεων, καθώς και μελέτη κατανομών. Σύμφωνα με το δεύτερο τρόπο, ο υπολογισμός μπορεί να γίνει εμπειρικά, μέσω δοκιμών για όλες τις τιμές του μηνύματος εισόδου (εξαντλητική αναζήτηση). Το τελευταίο είναι εφικτό, διότι ο μετασχηματισμός MixColumns είναι γραμμική συνάρτηση, επομένως συμπεριφέρεται με τον ίδιο τρόπο για εισόδους που αντιστοιχούν είτε σε τιμές είτε σε διαφορές.

Στον Πίνακα 5.1 που ακολουθεί μπορούμε να δούμε τις προσεγγίσεις των πιθανοτήτων που αφορούν το σενάριο, κατά το οποίο δύο είσοδοι των τεσσάρων ψηφιολέξεων η καθεμία, που διαφέρουν σε D_I ψηφιολέξεις σε προκαθορισμένες θέσεις, οδηγούν σε ίδιου μήκους εξόδους, που διαφέρουν σε D_O ψηφιολέξεις, πάλι σε προκαθορισμένες θέσεις. Η επεξεργασία αφορά φυσικά τον μετασχηματισμό MixColumns, ενώ οι τιμές είναι λογαριθμικές με βάση το δύο.

Πίνακας 5.1: Προσέγγιση πιθανοτήτων για το αποτέλεσμα του MixColumns.

	D_0	0	1	2	3	4
D_1						
0		0	$-\infty$	$-\infty$	$-\infty$	$-\infty$
1		$-\infty$	$-\infty$	$-\infty$	$-\infty$	0
2		$-\infty$	$-\infty$	$-\infty$	-8	0
3		$-\infty$	$-\infty$	-16	-8	0
4		$-\infty$	-24	-16	-8	0

5.5 Ύπαρξη ψηφίων ελέγχου

Η αλλαγή των ψηφιολέξεων εισόδου προκαλεί αλλαγή των ψηφιολέξεων κατάστασης, αλλά η μεταβολή αυτή δεν συμβαίνει αμέσως. Στον Πίνακα 5.2 που ακολουθεί φαίνεται η αντιστοιχία μεταξύ των αλλαγών των τμημάτων του μηνύματος, που συμβολίζεται με M_k, και των αλλαγών των στηλών των καταστάσεων s, έπειτα από 1,2 και 3 επαναλήψεις.

Πίνακας 5.2: Αντιστοίχιση αλλαγών μεταξύ ψηφιολέξεων μηνύματος και κατάστασης για 1,2,3 επαναλήψεις.

	00	01	02	03	04	05	06	07	08	09	10	11	12
A_k		√											
B_k			√										
C_k					√								
D_k											√		

	00	01	02	03	04	05	06	07	08	09	10	11	12
A_k			√	√		√						√	
B_k				√	√		√						√
C_k		√				√	√		√				
D_k		√						√				√	√

Μπορούμε να παρατηρήσουμε από τον Πίνακα 5.2 ότι στην τελευταία επανάληψη, σχεδόν όλα τα ψηφία της κάθε κατάστασης έχουν αλλάξει. Ακόμη, παρατηρούμε τον τρόπο με τον οποίο απεικονίζονται οι ψηφιολέξεις-ενδείξεις "ενεργό"/"μη-ενεργό", οι οποίες σημειώνονται με "√" για την κατάσταση "ενεργό", όσον αφορά την ανάλυση αποκομμένων διαφορών. Σε επόμενο κεφάλαιο θα είμαστε σε θέση να ελέγξουμε το αποτέλεσμα του MixColumns, με βάση τις ενδείξεις αυτές.

	00	01	02	03	04	05	06	07	08	09	10	11	12
A_k	√		√	√	√	√	√	√	√	√			√
B_k	√	√		√	√	√	√	√	√	√	√		
C_k			√	√		√	√	√	√	√	√	√	√
D_k	√	√	√	√	√	√			√	√		√	√

5.6 Γενική στρατηγική εντοπισμού αποκομμένων διαφορών

Στις προηγούμενες ενότητες αναπτύξαμε τους τρόπους με τους οποίους γίνεται ο εντοπισμός των αποκκομένων διαφορών. Στο σημείο αυτό πρέπει να προσδιορίσουμε, τη διαδικασία παραγωγής κατάλληλων εισόδων, που θα αποκαλύψουν τις διαφορές αυτές. Εκ πρώτης όψεως κάτι τέτοιο φαίνεται δύσκολο και επιβεβαιώνεται σύμφωνα με την Ιδιότητα 1 της σχετικής εργασίας του Knudsen [4]:

Ιδιότητα1: Μία εσωτερική σύγκρουση για την συνάρτηση Grindahl-256 απαιτεί τουλάχιστον 5 επαναλήψεις. Επιπρόσθετα, οποιοδήποτε χαρακτηριστικό το οποίο ξεκινά ή τελειώνει στην επεκταμένη κατάσταση, περιέχεται χωρίς αλλαγές, τουλάχιστον στον γύρο κατά τον οποίο τουλάχιστον οι μισές από τις ψηφιολέξεις της επεκταμένης κατάστασης (εξαιρουμένης της πρώτης στήλης) είναι "ενεργές".

Η ιδιότητα αυτή μπορεί να διαπιστωθεί μέσω της "επίθεσης συνάντησης στο ενδιάμεσο". Η επίθεση αυτή όμως απαιτεί εξαντλητική αναζήτηση. Με μία βελτίωση του αλγορίθμου που χρησιμοποιεί, ώστε να εκτελείται ταχύτερα, μπορούμε να επιβεβαιώσουμε ότι μία εσωτερική σύγκρουση για τον Grindahl-256 απαιτεί τουλάχιστον 6 επαναλήψεις. Μία ακόμη παρατήρηση είναι ότι εισάγοντας διαφορές στην κατάσταση, οδηγούμαστε, έπειτα από μικρό αριθμό επαναλήψεων, σε ένα ζεύγος επεκταμένων καταστάσεων εντελώς διαφορετικό. Μάλιστα, το διαφοροποιημένο αυτό ζεύγος παραμένει σχεδόν σταθερό. Αυτό επιβεβαιώνεται από το γεγονός ότι η πιθανότητα το διαφοροποιημένο ζεύγος να παραμείνει διαφοροποιημένο, έπειτα από τον μετασχηματισμό του μέσω του MixColumns, είναι $P_A = (1 - 2^{-8})^{4 \cdot}$ δηλαδή για τις 12 στήλες της επεκταμένης κατάστασης (εξαιρείται η πρώτη εξού και το 12) έχουμε πιθανότητα $P_A^{12} \simeq 2^{-0,27}$. Καταλήγουμε λοιπόν στο συμπέρασμα ότι είναι ευκολότερο να ξεκινήσουμε, από ένα ζεύγος επεκταμένων καταστάσεων εντελώς διαφοροποιημένων, ώστε να προχωρήσουμε στην αναζήτηση εσωτερικών συγκρούσεων.

5.7 Εύρεση ακολουθίας αποκομμένου διαφορικού

Στην ενότητα αυτή γίνεται μία πιο συγκεκριμένη προσέγγιση του τρόπου εύρεσης μίας ακολουθίας, ή αλλιώς μονοπατιού (path), κινήσεων που θα αποκαλύψουν τον τρόπο λειτουργίας της συνάρτησης κατακερματισμού. Όπως παρουσιάστηκε μέχρι τώρα, το ενδιαφέρον εστιάζεται στην παραγωγή ζευγών επεκταμένων καταστάσεων, τα οποία θα προσφέρουν κάποια πληροφορία. Ένα τέτοιο ζεύγος είναι το εντελώς διαφοροποιημένο (all-difference), διαφορές σε όλα τα ψηφία των δύο μελών, λόγω της ευκολίας παραγωγής του.

Στην περίπτωση της συνάρτησης Grindahl, οι αποκομμένες διαφορές διαδίδονται το ίδιο γρήγορα, είτε ξεκινήσουμε δοκιμάζοντας εισόδους, με σκοπό να καταλήξουν στην ίδια έξοδο, είτε ξεκινήσουμε από ίδιες εξόδους και πηγαίνοντας προς τα πίσω, να καταλήξουμε στις εισόδους που τις προκάλεσαν. Συγκεκριμένα, αν εξετάζουμε μία σύγκρουση στο τέλος της επανάληψης k, τότε θα πρέπει να δοκιμάσουμε όλες τις μάσκες αποκομμένων διαφορών, που εφαρμόζονται στα τμήματα του μηνύματος εισόδου κατά τις επαναλήψεις k, $k-1$ κ.ο.κ. Ταυτόχρονα πρέπει να δοκιμάζονται και όλες οι πιθανές μεταβάσεις των αποκομμένων διαφορών, μέσω της χρήσης του μετασχηματισμού MixColumns, μέχρι να καταλήξουμε σε ένα εντελώς διαφοροποιημένο ζεύγος επεκταμένων καταστάσεων. Ο αλγόριθμος αυτός φαίνεται υπολογιστικά απαιτητικός, μπορεί όμως να βελτιωθεί σημαντικά με την χρήση συγκεκριμένης στρατηγικής. Αυτή θα έχει ως βάση της την πρώιμη ματαίωση (early-abort), δηλαδή θα υπολογίζεται το κόστος του τρέχοντος μονοπατιού και θα ματαιώνεται η περαιτέρω εξέτασή του, αν το κόστος υπολογισμού του ξεπερνά τις 2^{128} πράξεις. Έτσι, ο αλγόριθμος θα συνεχίσει να εξετάζει τα υπόλοιπα μονοπάτια, αποφεύγοντας το μεγάλο υπολογιστικό κόστος των περιττών πράξεων. Μία ακόμη βελτίωση που προκαλεί η εν λόγω στρατηγική, είναι η έγκαιρη ματαίωση εξέτασης ενός μονοπατιού όταν ο αριθμός των επαναλήψεων, τις οποίες εξετάζουμε πηγαίνοντας προς τα πίσω, γίνεται αρκετά μεγάλος.

Γίνεται εμφανές, ότι ο ταχύτερος τρόπος για να βρούμε την επιθυμητή ακολουθία, είναι η προσθήκη αποκομμένων διαφορών σε όλα τα τμήματα του μηνύματος. Ακόμη, θα χρησιμοποιήσουμε τις ψηφιολέξεις του μηνύματος εισόδου που θα εισάγουμε, ως ψηφιολέξεις ελέγχου (control bytes), ώστε να επιτεθούμε μέσω ανεξάρτητων τμημάτων του

μονοπατιού σε συγκεκριμένες φάσεις λειτουργίας της συνάρτησης κατακερματισμού, αυξάνοντας έτσι την πιθανότητα επιτυχίας (εύρεση δηλαδή του σωστού μονοπατιού). Αυτό σημαίνει ότι είναι προτιμότερο να μην βιαζόμαστε να προσθέτουμε αποκομμένες διαφορές, αφού τότε το μονοπάτι να διαρκεί αρκετές επαναλήψεις, αυξάνοντας τον αριθμό των ψηφιολέξεων του μηνύματος που θα εισάγονται (και κατ' επέκταση των ψηφιολέξεων ελέγχου), δίνοντάς μας περισσότερη ευελιξία στον έλεγχο που ασκούμε.

Ένα παράδειγμα χρήσης της τεχνικής αυτής δίνεται συγκρίνοντας τις επόμενες περιπτώσεις. Στην πρώτη περίπτωση έχουμε την κατάσταση στην οποία μπορούμε να εντοπίσουμε ένα μονοπάτι, ξεκινώντας από ένα ζεύγος επεκταμένων καταστάσεων εντελώς διαφοροποιημένο, και απαιτώντας τέσσερις επαναλήψεις, για να καταλήξουμε σε σύγκρουση, με πιθανότητα επιτυχίας 2^{-312}. Στη δεύτερη περίπτωση τα μόνα που αλλάζουν, είναι ο αριθμός των απαιτούμενων επαναλήψεων που είναι οκτώ , καθώς και της πιθανότητας επιτυχίας που είναι 2^{-440}. Η δεύτερη περίπτωση είναι προτιμότερη της πρώτης, παρά την μικρότερη πιθανότητα επιτυχίας. Αυτό προκύπτει από το γεγονός, ότι στην πρώτη περίπτωση μπορούμε να εισάγουμε μόλις τέσσερα ζεύγη λέξεων εισόδου, ενώ στη δεύτερη οκτώ. Έχουμε δηλαδή περισσότερους βαθμούς ελευθερίας, τους οποίους μπορούμε να εκμεταλλευτούμε για να κατανοήσουμε τη λειτουργία της συνάρτησης. Βέβαια η προσθήκη περισσότερων επαναλήψεων σταματά να προσφέρει πλεονεκτήματα έπειτα από έναν αριθμό.

5.8 Εύρεση διαφορικού μονοπατιού

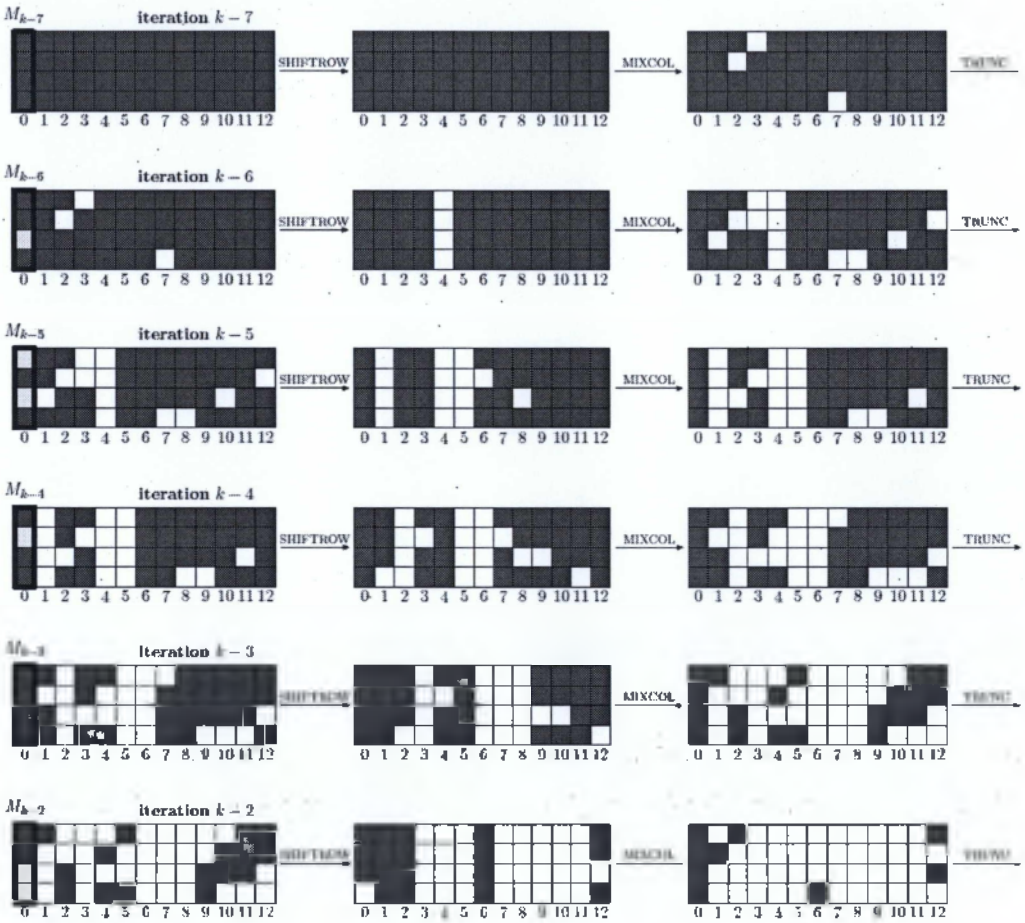
Στο σημείο αυτό περιγράφεται η εύρεση μίας ακολουθίας εισόδων για την πρόκληση σύγκρουσης. Η ακολουθία αυτή των ενεργειών, που βασίζεται στην παρακολούθηση των διαφορών στις επεκταμένες καταστάσεις, ονομάζεται "διαφορικό μονοπάτι" (differential path). Βασίζεται στην ιδέα που περιγράφηκε στην προηγούμενη ενότητα("Εύρεση ακολουθίας αποκομμένου διαφορικού").

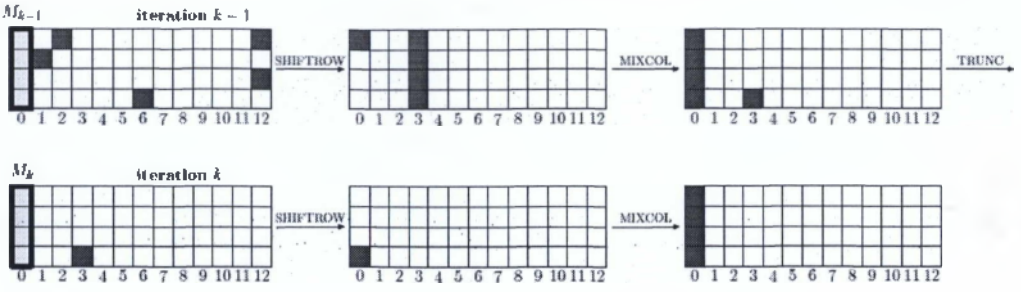
Το παράδειγμα εύρεσης του διαφορικού μονοπατιού φαίνεται γραφικά στο Σχήμα 5.8. Σημειώνουμε με k τον αριθμό της τελευταίας επανάληψης του διαφορικού μονοπατιού. Αρχικά, επιβεβαιώνεται ότι ότι όλοι οι μετασχηματισμοί MixColumns οδηγούν σε έγκυρες μεταβάσεις. Το μονοπάτι του παραδείγματος έχει πιθανότητα επιτυχίας $2^{-55\times 8} =$

2^{-240}, αλλά εισάγει αρκετά τμήματα μηνυμάτων τα οποία, όπως αναφέραμε, επιτρέπουν ανεξάρτητες επιθέσεις σε επιμέρους στάδια της συνάρτησης κατακερματισμού.

Σκοπός μας είναι να βρούμε ένα ζεύγος μηνυμάτων το οποίο να ακολουθεί το αναμενόμενο διαφορικό μονοπάτι. Για το λόγο αυτό, δεν εξετάζουμε μία προς μία τις επαναλήψεις, αλλά εστιάζουμε στο τι συμβαίνει κατά την εισαγωγή των ψηφιολέξεων των μηνυμάτων (μεγέθους 4 ψηφιολέξεων το καθένα). Έτσι, δοκιμάζουμε διαδοχικά ζεύγη μηνυμάτων και παρατηρούμε το αποτέλεσμα του μετασχηματισμού MixColumns, έως ότου οι μεταβάσεις να ταιριάζουν στο αναμενόμενο διαφορικό μονοπάτι. Το τελευταίο είναι εκείνο το οποίο έχουμε διαπιστώσει ότι οδηγεί σε σύγκρουση των εξόδων.

Στον Σχήμα 5.2 δίνονται όλες οι εξαρτήσεις μεταξύ των αποτελεσμάτων του μετασχηματισμού MixColumns, και των τμημάτων του μηνύματος εισόδου. Οι εξαρτήσεις αυτές λειτουργούν ως ψηφιολέξεις ελέγχου κατά τη διαδικασία που φαίνεται στο Σχήμα 5.1. Στο Σχήμα 5.2 φαίνεται κόστος όλων των μεταβάσεων καθώς και ο αριθμός των ψηφιολέξεων εισόδου που έχουν εισαχθεί σε κάθε επανάληψη. Η δεύτερη στήλη του Σχήματος 5.2 δείχνει τις θέσεις των στηλών της κατάστασης, στην οποία επιβάλουμε (μέσω των ψηφίων ελέγχου) μία διαφορική μετάβαση (differential transistion) κατά τον μετασχηματισμό MixColumns, ενώ η πρώτη στήλη δείχνει τον αριθμό της επανάληψης στην οποία συμβαίνει αυτό. Στην τρίτη στήλη, φαίνεται για κάθε μετάβαση το κόστος υπολογισμού σε ψηφιολέξεις (για παράδειγμα, αν έχει κόστος c τότε η πιθανότητα μετάβασης είναι $2^{-c\times 8}$). Οι υπόλοιπες επτά στήλες του Σχήματος 5.2 αντιπροσωπεύουν ένα ζεύγος λέξεων εισόδου, οι οποίες θα χρησιμοποιηθούν ως ψηφιολέξεις ελέγχου (τα γράμματα a ή A, b ή B, c ή C, d ή D είναι αντίστοιχα η πρώτη,δεύτερη,τρίτη και τέταρτη ψηφιολέξη του μηνύματος που εισάγουμε). Τα κεφαλαία γράμματα σημαίνουν ότι έχουμε δύο ψηφιολέξεις ελέγχου (εισάγουμε μία διαφορά για το τμήμα αυτό), ενώ τα μικρά γράμματα, ότι έχουμε μία ψηφιολέξη ελέγχου (δεν εισάγουμε διαφορά για το τμήμα αυτό). Ακόμη, σημειώνεται με "-" ή "×" το γεγονός ότι η μετάβαση λόγω του MixColumns της αντίστοιχης γραμμής, έχει επηρεαστεί από την ψηφιολέξη ελέγχου που φαίνεται στην αντίστοιχη στήλη. Οι εξαρτήσεις που σημειώνονται με "×" είναι αυτές που προσφέρονται για την επικείμενη επίθεση, καθώς επισημαίνουν τις εξαρτήσεις του αποτελέσματος του MixColumns από το τελευταίο τμήμα μηνύματος που εισήχθη.


M_{k-7}
iteration $k-7$
SHIFTROW
MIXCOL
M_{k-6}
iteration $k-6$
SHIFTROW
MIXCOL
TRUNC
M_{k-5}
iteration $k-5$
SHIFTROW
MIXCOL
TRUNC
M_{k-4}
iteration $k-4$
SHIFTROW
MIXCOL
TRUNC
iteration $k-3$
MIXCOL
iteration $k-2$
0 1 2 3 4 5 6 7 8 9 10 11 12



Σχήμα 5.1: Αποκομμένο διαφορικό μονοπάτι για 8 επαναλήψεις, ξεκινώντας από καταστάσεις πλήρως διαφοροποιημένες [8]

Στο σημείο αυτό είναι χρήσιμο να εξηγήσουμε την παραπάνω εικόνα (Σχήμα 5.1). Τα σκιασμένα κελιά σημαίνουν ότι υπάρχουν διαφορές για τη συγκεκριμένη ψηφιολέξη, ενώ τα λευκά, ότι δεν υπάρχει καμία διαφορά. Κάθε γραμμή αντιπροσωπεύει μία επανάληψη. Η πρώτη στήλη δείχνει τις διαφορές της κατάστασης μόλις ανανεωθεί μέσω των τεσσάρων ψηφιολέξεων του μηνύματος. Η δεύτερη στήλη δείχνει το ίδιο με την πρώτη αφού πρώτα εφαρμοστεί ο μετασχηματισμός ShiftRows. Η τρίτη στήλη αντιπροσωπεύει την εσωτερική κατάσταση μετά την εφαρμογή του μετασχηματισμού MixColumns. Οι μετασχηματισμοί AddConstant SubBytes δεν επιδρούν στο διαφορικό μονοπάτι, οπότε δεν απεικονίζονται στο Σχήμα. Ακόμη, οι τέσσερις πρώτες ψηφιολέξεις που αποτελούν την πρώτη στήλη των καταστάσεων, στα κουτιά που βρίσκονται αριστερά, αντιστοιχούν στις λέξεις του μηνύματος που εισέρχονται σε κάθε επανάληψη, όπου οι λέξεις αυτές εξυπηρετούν τους σκοπούς του ελέγχου. Τέλος, οι τέσσερις πρώτες ψηφιολέξεις που αποτελούν την πρώτη στήλη των καταστάσεων, μετά την μετάβασή τους λόγω του μετασχηματισμού MixColumns, δεν συμμετέχουν στον εντοπισμό διαφορών, μιας και πρόκειται να αποκοπούν στη συνέχεια.

it	col	cost	message blocks inserted																													
			$k-8$				$k-7$				$k-6$				$k-5$				$k-4$				$k-3$				$k-2$			
			A	B	C	D	A	B	C	D	A	B	c	D	a	B	c	D	A	b	C	D	A	B	C	D	A	B	c	d
k-7	2	1	–					×																						
	3	1	×	×																										
	7	1				×																								
k-6	1	1		–		–			–	–	×																			
	2	1	–		–	–	–					×																		
	3	2	–	–	–	–	×	×																						
	7	1	–	–	–					×																				
	8	1	–	–	–	–			×																					
	10	1		–	–									×																
	12	1	–		–	–		×		×																				
k-5	2	1	–	–	–	–	–		–	–	–					×														
	3	1	–	–	–	–	–	–	–	–	×	×																		
	8	1	–	–	–	–	–	–	–	–			×																	
	9	1	–	–	–	–	×	×	×	×																				
	11	1	–	–	–	–			–	–	×		×	×																
k-4	1	1	–	–	–	–	–	–	–	–		–		–			–	–	×											
	3	1	–	–	–	–	–	–	–	–	–	–	–	–	×	×														
	4	2	–	–	–	–	–	–	–	–	–	–		–		–					×									
	7	1	–	–	–	–	–	–	–	–	–	–	–					×												
	9	1	–	–	–	–	–	–	–	–	×	×	×	×																
	10	1	–	–	–	–	–	–	–	–		–	–									×								
	11	1	–	–	–	–	–	–	–	–			–	–	×		×	×												
	12	1	–	–	–	–	–	–	–	–	–		–	–		×		×												
k-3	1	3	–	–	–	–	–	–	–	–	–	–	–	–		–		–			–	–	×							
	2	2	–	–	–	–	–	–	–	–	–	–	–	–	–		–	–	–					×							
	4	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–		–		–					×						
	5	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	×		×										
	9	2	–	–	–	–	–	–	–	–	–	–	–	–	×	×	×	×													
	10	2	–	–	–	–	–	–	–	–	–	–	–	–		–	–									×				
	11	1	–	–	–	–	–	–	–	–	–	–	–	–			–	–	×		×	×								
	12	2	–	–	–	–	–	–	–	–	–	–	–	–	–		–	–		×		×								
k-2	1	3	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		–		–			–	–	×			
	2	3	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		–	–	–					×		
	6	3	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–			×	×					
	12	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–		–	–		×		×				
k-1	3	3	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	×	×		
COST			**0**				**0**				**0**				**1**				**2**				**6**				**5**			

Σχήμα 5.2: Εξαρτήσεις μεταξύ τμημάτων μηνυμάτων και ψηφιολέξεων που αντιστοιχούν στο παράδειγμα του Σχήματος 5.1 [8]

Κεφάλαιο 6

Επιθέσεις στη συνάρτηση κατακερματισμού

6.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο είδαμε του τρόπους με τους οποίους πραγματοποιείται η κρυπτανάλυση (cryptanalysis). Έχοντας λοιπόν αναπτύξει τη θεωρία που κρύβεται πίσω από τις επιθέσεις στους αλγορίθμους κατακερματισμού [12], είμαστε σε θέση να παρουσιάσουμε τα είδη επιθέσεων (αναλαμβάνουμε δηλαδή το ρόλο του επιτιθέμενου), όπως αυτά εφαρμόζονται, στη συνάρτηση Grindahl. Αυτές είναι η επίθεση γενεθλίων (birthday attack), η επίθεση σύγκρουσης (collision attack), η επίθεση επέκτασης μήκους (length-extension attack),η επίθεση πολλαπλών συγκρούσεων (multi-collisions attack) και η επίθεση αγέλης (herding attack).

6.2 Επίθεση γενεθλίων

Η επίθεση γενεθλίων έχει τη βάση της στο παράδοξο των γενεθλίων (birthday paradox), το οποίο αποτελεί ένα πρόβλημα πιθανοτήτων [17]. Σύμφωνα με αυτό, αν ένα σύνολο n τυχαίων ατόμων τότε δύο άτομα θα έχουν την ίδια ημερομηνία γέννησης. Σύμφωνα με την αρχή του περιστερώνα (pigeon-hole principle) η πιθανότητα του γεγονότος αυτού είναι 100% όταν το n τείνει στον αριθμό 366, ενώ ακόμη και για $n = 57$ έχουμε πιθανότητα 99% [5] [6]. Πρόκειται λοιπόν για μία συχνή μέθοδο επίθεσης εναντίων των συναρτήσεων κατακερματισμού.

Στη δική μας περίπτωση αν P είναι η ιδανική μετάθεση, τότε οι εσωτερικές συγκρούσεις και οι συγκρούσεις δευτερεύουσας προ-απεικόνισης θα έχουν πολυπλοκότητα $2^{m/2}$. Η μετάθεση όμως δεν μπορεί να είναι ιδανική, το αντίθετο μάλιστα, αφού η πολυπλοκότητα μίας εσωτερικής σύγκρουσης, που εκμεταλλεύεται τις αδυναμίες της P, είναι το πολύ $2^{(m-b)/2}$ (όπου b υπενθυμίζουμε ότι είναι το μέγεθος του μηνύματος εισόδου). Αυτό το διαπιστώνουμε ακολουθώντας την επόμενη διαδικασία:

1. Υποθέτουμε ότι η πρώτη στήλη του πίνακα καταστάσεων αντικαθίσταται από το μήνυμα εισόδου.

2. Υπολογίζουμε την επεκταμένη κατάσταση διαφορετικών μηνυμάτων, πριν τους κενούς γύρους.

3. Προσαρτούμε δύο σταθερά τμήματα σε όλα τα μηνύματα.

4. Το πρώτο σταθερό τμήμα του μηνύματος αντικαθιστά την πρώτη στήλη της επεκταμένης κατάστασης.

5. Εφαρμόζεται η μετάθεση, όπου ο μετασχηματισμός ShiftRows μετακινεί v_{rw} ψηφιολέξεις στην πρώτη στήλη της επεκταμένης κατάστασης, οπότε η εφαρμογή του MixColumns ανακατατάσσει τις ψηφιολέξεις στη στήλη.

6. Το δεύτερο σταθερό τμήμα αντικαθιστά την στήλη στο τέλος του βήματος 5.

Μετά από αυτή τη διαδικασία, αν δύο επεκταμένες καταστάσεις συμφωνούν σε όλες τις ψηφιολέξεις εκτός από την πρώτη στήλη και τις ψηφιολέξεις που έχουν μετακινηθεί μέσα στην πρώτη στήλη από το πρώτο σταθερό τμήμα του μηνύματος, τότε οι δύο αυτές επεκταμένες καταστάσεις θα συμφωνούν σε όλες τις ψηφιολέξεις που ακολουθούν το δεύτερο σταθερό τμήμα της εισόδου. Ο αριθμός των μηνυμάτων που απαιτούνται για την επιτυχία της επίθεσης αυτής είναι $2^{(m-b)/2}$. Η διαδικασία που παρουσιάστηκε μπορεί να γενικευτεί ώστε να αντιστοιχεί με οποιοδήποτε τρόπο, μηνύματα εισόδου με επεκταμένες καταστάσεις.

Το γεγονός ότι η μετάθεση είναι αντιστρέψιμη συνάρτηση, καθιστά αντιστρέψιμη και τη συνάρτηση κατακερματισμού. Αυτό, την καθιστά ευάλωτη σε επιθέσεις συνάντησης στο ενδιάμεσο. Μία τέτοια επίθεση λειτουργεί ως εξής:

1. Υπολογίζουμε την ενδιάμεση επεκταμένη κατάσταση, για καθένα από τα $2^{(m-b)/2}$ διαφορετικά μηνύματα εισόδου τα οποία έχουν πανομοιότυπα τα τελευταία δύο τμήματα.

2. Δεδομένης μίας επιθυμητής κατάστασης της συνάρτησης κατακερματισμού, υπολογίζουμε πηγαίνοντας προς τα πίσω, την ενδιάμεση κατάσταση για τον ίδιο αριθμό μηνυμάτων εισόδου.

3. Με μεγάλη πιθανότητα θα υπάρξει ταίριασμα μεταξύ δύο συνόλων ενδιάμεσων καταστάσεων

Η διαδικασία αυτή αποδίδει την επιθυμητή δευτερεύουσα προ-απεικόνιση με πολυπλοκότητα $2^{(m-b)/2}$.

6.3 Επίθεση σύγκρουσης

Η επίθεση σύγκρουσης είναι εκείνη που κάνει χρήση των μεθόδων που παρουσιάστηκαν στο προηγούμενο κεφάλαιο. Η επίθεση σύγκρουσης, στη γενική της μορφή, επιχειρεί να εντοπίσει δύο μηνύματα εισόδου που να οδηγούν στην ίδια έξοδο, μετά την επεξεργασία του από τη συνάρτηση κατακερματισμού [7]. Ο τρόπος με τον οποίο επιλέγονται οι είσοδοι δεν είναι καθορισμένος, ούτε είναι καθορισμένες οι επιθυμητές τιμές της εξόδου. Στην περίπτωσή μας όμως, και έχοντας υπόψη το κεφάλαιο που παρουσιάστηκε με θέμα την κρυπτανάλυση, η επίθεση σύγκρουσης παίρνει πολύ συγκεκριμένη μορφή:

1. Ξεκινούμε με μία προκαθορισμένη αρχική τιμή και εκτελούμε ένα αριθμό επαναλήψεων, έχοντας εισάγει πολλές αποκομμένες διαφορές στα τμήματα των μηνυμάτων εισόδου, με σκοπό να καταλήξουμε γρήγορα σε ένα ζεύγος εντελώς διαφοροποιημένων καταστάσεων, τις οποίες συμβολίζουμε με A. Το βήμα αυτό δεν συμπεριλαμβάνεται στην ανάλυση πολυπλοκότητας της μεθόδου.

2. Με βάση το ζεύγος A παράγουμε $2^{14*8} = 2^{112}$ εντελώς διαφοροποιημένα ζεύγη καταστάσεων $A_1, ..., A_{2^{112}}$. Το βήμα αυτό απαιτεί $2^{112} \times 2^{0,27} = 2^{112,27}$ επαναλήψεις υπολογισμών.

3. Καθορίζουμε τις ψηφιολέξεις ελέγχου για κάθε επανάληψη: για τα τμήματα μηνύματος τα οποία εισήχθησαν στην αρχή των επαναλήψεων $k-8$, $k-7$, $k-6$ του μονοπατιού αποκομμένου διαφορικού (που φαίνεται στο Σχήμα 5.2), έχουμε περισσότερες εισερχόμενες ψηφιολέξεις ελέγχου από ότι χρειαζόμαστε. Πράγματι, για τα

μηνύματα που εισήχθησαν στις επαναλήψεις $k-8$, $k-7$, $k-6$ έχουμε αντίστοιχα 8, 8 και 7 ψηφιολέξεις ελέγχου, τη στιγμή που απαιτούμε αντίστοιχα 2, 7 και 7 ψηφιολέξεις, που συμφωνούν με τους βαθμούς ελευθερίας. Πιο συγκεκριμένα, για κάθε ζεύγος λέξεων μηνύματος (M_{k-i}, M'_{k-i}) που εισάγεται, οι ψηφιολέξεις του χρησιμοποιούνται προκειμένου να προσαρμόσουν τη συμπεριφορά του μετασχηματισμού MixColumns, όσον αφορά τις μεταβάσεις, όπου εμφανίζεται το σύμβολο "×" στη στήλη M_{k-i} στο Σχήμα 5.2. Για κάθε βήμα, το ολικό κόστος είναι ίσο με το άθροισμα από τα κόστη όλων των μεταβάσεων που προκαλεί ο MixColumns, μείον τον αριθμό των ψηφιολέξεων ελέγχου που διατίθενται από την M_{k-i}. Έτσι, διατηρούμε 2^{112} ζεύγη μηνυμάτων και καταστάσεων που συμφωνούν με το διαφορικό μονοπάτι. Για τις λέξεις μηνύματος που εισήχθησαν στην επανάληψη $k-5$, έχουμε 6 ψηφιολέξεις ελέγχου για 7 ψηφιολέξεις συνθηκών, συνεπώς κρατάμε μόνο 1 ζεύγος μηνυμάτων, εκ των 2^8, και πηγαίνουμε στην $(k-4)$-οστή λέξη μηνύματος με 2^{104} έγκυρα ζεύγη. Συνεχίζουμε κατά τον ίδιο τρόπο για τις τρεις τελευταίες λέξεις $k-4$, $k-3$ και $k-2$, έχοντας αντίστοιχα 7, 8 και 4 ψηφιολέξεις ελέγχου και απαιτώντας 9, 14 και ψηφιολέξεις συνθηκών αντίστοιχα. Επομένως, αναμένουμε να έχουμε ένα ζεύγος μηνυμάτων που ακολουθούν το διαφορικό μονοπάτι, και μάλιστα με υψηλή πιθανότητα, αν ξεκινήσουμε με $2^{14\times 8} = 2^{112}$ ζεύγη καταστάσεων εντελώς διαφοροποιημένων.

4. Προσθέτουμε ένα $(k+1)$-οστό τμήμα μηνύματος χωρίς αποκομμένες διαφορές, με σκοπό να επιβάλλουμε μία αποκοπή, έπειτα από την τελευταία επανάληψη k του διαφορικού μονοπατιού (οι τελευταίοι κενοί γύροι ολοκληρώνονται χωρίς αποκοπή).

Στο σημείο αυτό θα εξετάσουμε λεπτομερέστερα τις επιμέρους λειτουργίες της επίθεσης. Ξεκινάμε από τη στιγμή που ο επιτιθέμενος χρειάζεται να καθορίσει το ζεύγος μηνυμάτων, το οποίο θα δώσει ως είσοδο κατά το βήμα $k-5$ (έβδομη στήλη του Σχήματος 5.2). Οι προηγούμενες λέξεις του μηνύματος έχουν ήδη καθοριστεί κατά την επίθεση, οπότε εστιάζουμε στα "×" του Σχήματος 5.2. Κάποιες διαφορικές μεταβάσεις του μετασχηματισμού MixColumns, πρέπει να λειτουργούν όπως ενδείκνυται σύμφωνα με το μονοπάτι αποκομμένων διαφορικών, γεγονός που εισάγει κόστος υπολογισμού. Για παράδειγμα, στη δεύτερη στήλη της $(k-5)$-οστής επανάληψης, απαιτείται μετάβαση από τετραπλή αποκομμένη διαφορά σε τριπλή αποκομμένη διαφορά, πράγμα που μπορεί να συμβεί με πιθανότητα 2^{-8} και μάλιστα με κόστος μίας ψηφιολέξης. Για να συμβεί αυτό, πρέπει να χρησιμοποιήσουμε τη λέξη

μηνύματος που εισήχθη κατά την $(k-5)$-οστή επανάληψη (και πιο συγκεκριμένα χρειαζόμαστε τη δεύτερη ψηφιολέξη του μηνύματος), προκειμένου να τυχαιοποιήσουμε το στιγμιότυπο της μετάβασης. Υπάρχουν αρκετές πιθανότητες να βρούμε 2^8 έγκυρα ζεύγη για τη μετάβαση που περιγράψαμε, δύο ψηφιολέξεις ελέγχου για μία ψηφιολέξη συνθήκης. Επαναλαμβάνουμε την ίδια διαδικασία για τη μετάβαση της έβδομης στήλης της επανάληψης $k-4$ με την τέταρτη ψηφιολέξη του μηνύματος, οπότε έχουμε πάλι δύο ψηφιολέξεις ελέγχου για μία ψηφιολέξη συνθήκης. Στη συνέχεια, εντοπίζουμε το υποσύνολο του διανυσματικού γινομένου (cross product) των δύο συνόλων, που αποτελούνται από 2^8 ζεύγη ψηφιολέξεων, έτσι ώστε οι μεταβάσεις της η δωδέκατης στήλης κατά την επανάληψη $k-4$ να επιβεβαιωθούν (οπότε έχουμε κόστος μίας ψηφιολέξης για τη συνθήκη). Έτσι, διατηρούμε 2^8 έγκυρες υποψηφιότητες. Έπειτα, τροποποιούμε την πρώτη ψηφιολέξη του μηνύματος, ώστε να επηρεάσει τη μετάβαση της της τρίτης στήλης στην επανάληψη $k-4$· επειδή αυτό κοστίζει μία ψηφιολέψη ελέγχου για μία ψηφιολέξη συνθήκης, συνεχίζουν να μας απομένουν 2^8 έγκυρες υποψηφιότητες. Με την τελευταία ψηφιολέξη του μηνύματος εισόδου, αναζητούμε μία επιθυμητή μετάβαση για την ένατη στήλη, στην επανάληψη $k-3$, με κόστος μίας ψηφιολέξης ελέγχου για δύο ψηφιολέξεις συνθηκών. Βέβαια, πρέπει να συμπεριλάβουμε και το κόστος της ενδέκατης στήλης στην επανάληψη $k-4$, το οποίο είναι μία ψηφιολέψη συνθήκης. Συνοψίζοντας, η διαδικασία αυτή, που προσομοιώνει ένα βήμα, κοστίζει 2^8 δοκιμές, αφού έχουμε συνολικά έξι ψηφιολέξεις ελέγχου και επτά ψηφιολέξεις συνθήκης· επαναλαμβάνοντας την διαδικασία αυτή, για όλες τις λέξεις εισόδου που αποτελούν το διαφορικό μονοπάτι, καταλήγουμε στις 2^{112} δοκιμές που απαιτούνται για την επίθεση σύγκρουσης.

Κάποιος θα μπορούσε να διαφωνήσει με το γεγονός ότι απαιτείται να δοκιμάσουμε 2^{112} ζεύγη καταστάσεων εντελώς διαφοροποιημένων, όμως οι ψηφιολέξεις ελέγχου αυξάνουν το κόστος των βασικών λειτουργιών. Πράγματι, στο παράδειγμα που παρουσιάστηκε κάποια βήματα απαιτούν να ελέγξουν 2^8 ή 2^{16} τιμές λέξεων μηνύματος, με κάθε έλεγχο να χρειάζεται μόνο έναν υπολογισμό για τον μετασχηματισμό SubBytes (για ολόκληρη στήλη), ή μία με δύο επαναληπτικές διαδικασίες. Αυτά σημαίνουν ότι η πολυπλοκότητα της επίθεσης θα είναι υψηλότερη. Το επιχείρημα αυτό αληθεύει όταν ο επιτιθέμενος χρησιμοποιεί μία "αφελή" μέθοδο αναζήτησης. Η αρχική διαφωνία δεν ισχύει, καθώς με κάποιους υπολογισμούς πριν την εφαρμογή της επίθεσης, μειώνεται σημαντικά ο χρόνος αναζήτησης. Για παράδειγμα, μπορεί κάποιος

να παράγει όλες τις απαραίτητες πληροφορίες, για την γρήγορη εκτέλεση των αναζητήσεων που απαιτούνται στο τρίτο βήμα της επίθεσης σύγκρουσης, διαθέτοντας μόλις 2^{32} χρόνο και μνήμη για υπολογισμούς πριν την εφαρμογή της.

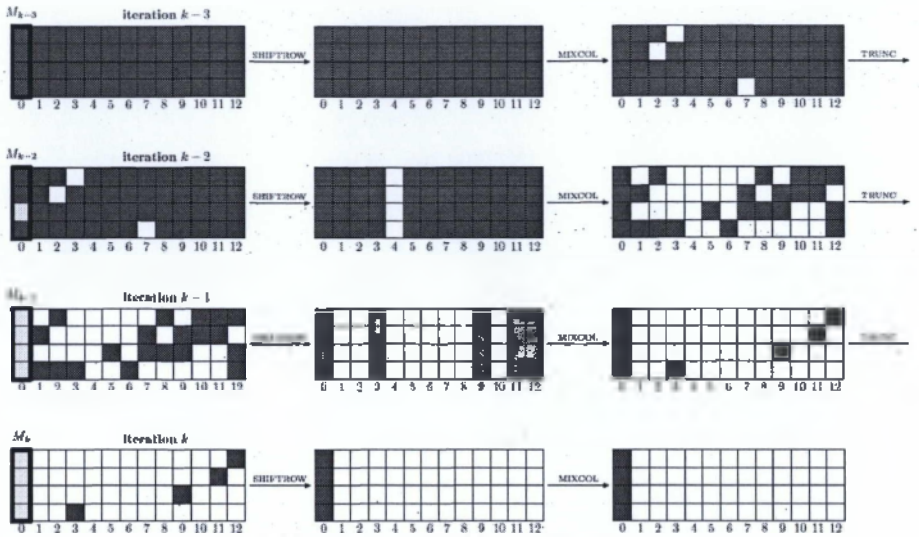
Μία ακόμη διαφωνία, θα μπορούσε να προκύψει από το γεγονός ότι στο κόστος υπολογισμού, δεν συμπεριλαμβάνονται οι μεταβάσεις από τις τετραπλές αποκομμένες διαφορές σε τετραπλές αποκομμένες διαφορές. Τέτοιες μεταβάσεις όμως έχουν μεγάλη πιθανότητα να συμβούν, της τάξη του $P_A = (1-2^8)^4 \simeq 2^{-0,02}$. Έτσι, έχουν μικρή επίδραση στην πολυπλοκότητα της επίθεσης, αναλογιζόμενοι ότι η λειτουργία αυτή κοστίζει πολύ λιγότερο από αυτές που προσμετρούνται (όπως για παράδειγμα οι επαναλήψεις).

6.4 Επίθεση δευτερεύουσας προ-απεικόνισης

Η επίθεση σύγκρουσης που παρουσιάστηκε στην προηγούμενη ενότητα, προσφέρει ένα σημαντικό πλεονέκτημα στον επιτιθέμενο: δεν χρειάζεται να γνωρίζει τις πραγματικές τιμές των διαφορών, μόνο την ύπαρξή τους. Έχουμε λοιπόν πολύ λίγους περιορισμούς κατά την εύρεση του διαφορικού μονοπατιού. Μπορούμε λοιπόν να δούμε, πώς το χαρακτηριστικό αυτό εφαρμόζεται σε επιθέσεις δευτερεύουσας προ-απεικόνισης.

Μπορούμε να δούμε τον τρόπο με τον οποίο εφαρμόζονται τα παραπάνω, μέσω του παραδείγματος του Σχήματος 6.1. Σε αυτό υποθέτουμε, ότι η δευτερεύουσα προ-απεικόνιση αποτελείται από ικανό αριθμό τμημάτων μηνύματος. Αν κάποιος θέλει να εντοπίσει μία δευτερεύουσα προ-απεικόνιση χρησιμοποιώντας αυτό το μονοπάτι, μόνο ο αριθμός των ψηφιολέξεων ελέγχου αλλάζει, συγκρινόμενος με εκείνον της αντίστοιχης περίπτωσης επίθεσης σύγκρουσης. Συγκεκριμένα, στην επίθεση σύγκρουσης είχαμε δύο ψηφιολέξεις ελέγχου, λόγω της εισαγωγής μη μηδενικών αποκομμένων διαφορών, ενώ πλέον απαιτείται μόλις μία ψηφιολέξη. Ακόμη, όταν εισάγεται μία μηδενική αποκομμένη διαφορά, έχουμε μία ψηφιολέξη ελέγχου για την επίθεση σύγκρουσης, ενώ δεν απαιτείται καμία ψηφιολέξη για την επίθεση δευτερεύουσας προ-απεικόνισης.

Χρησιμοποιώντας τις τεχνικές κρυπτανάλυσης που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, μπορούμε να βρούμε μία δευτερεύουσα προ-απεικόνιση σε περίπου $2^{28\times 8} = 2^{224}$ υπολογισμούς της συνάρτη-



Σχήμα 6.1: Μονοπάτι αποκομμένων διαφορών για την επίθεση δευτερεύουσας προ-απεικόνισης [8]

σης κατακερματισμού, τη στιγμή που απαιτούνται 2^{256} υπολογισμοί, όταν πρόκειται για την ιδανική συνάρτηση κατακερματισμού 256 δυαδικών ψηφίων (256-bit). Το μειονέκτημα της μεθόδου, είναι ότι απαιτεί η είσοδος να αποτελείται αρκετά τμήματα, προκειμένου να γίνουν οι απαραίτητες επαναλήψεις, που θα ακολουθούν το επιθυμητό διαφορικό μονοπάτι. Έτσι, η εν λόγω επίθεση πετυχαίνει όταν έχουμε τουλάχιστον 15 λέξεις εισόδου.

Μπορούμε να δούμε στο Σχήμα 6.2 τις εξαρτήσεις που αφορούν το παράδειγμα που παραθέσαμε. Οι εξαρτήσεις αυτές αφορούν τα τμήματα μηνύματος, τα οποία εισήχθησαν στα πλαίσια της επίθεσης δευτερεύουσας προ-απεικόνισης, έτσι ώστε να προκληθεί εσωτερική σύγκρουση στο τέλος της επανάληψης k. Για τα ζεύγη των λέξεων εισόδου που θα χρησιμοποιηθούν ως ψηφιολέξεις ελέγχου, σημειώνονται με κεφαλαίο γράμμα όταν περιέχουν μία ψηφιολέξη ελέγχου (εισαγωγή διαφοράς για το συγκεκριμένο τμήμα), και με μικρά γράμματα όταν δεν περιέχουν ψηφιολέξη ελέγχου (καμία εισαγωγή διαφοράς για το συγκεκριμένο τμήμα).

it	col	cost	message blocks inserted											
			$k-4$				$k-3$				$k-2$			
			A	B	C	D	A	B	C	D	A	B	c	D
k-3	2	1					×							
	3	1	×	×										
	7	1				×								
k-2	1	2		–		–			–	–	×			
	2	2	–		–	–	–					×		
	3	3	–	–	–	–	×	×						
	5	3	–	–	–	–	×		×					
	6	3	–	–	–			×	×					
	7	2	–	–	–					×				
	8	2	–	–	–	–			×					
	9	2	×	×	×	×								
	10	2		–	–									×
	11	2			–	–	×		×	×				
	12	1	–		–	–		×		×				
k-1	3	3	–	–	–	–	–	–	–	–	×	×		
	9	3	–	–	–	–	×	×	×	×				
	11	3	–	–	–	–			–	–	×		×	×
	12	3	–	–	–	–	–		–	–		×		×
COST			**0**				**16**				**12**			

Σχήμα 6.2: Εξαρτήσεις τμημάτων για την επίθεση δευτερεύουσας προαπεικόνισης [8]

6.5 Επίθεση επέκτασης μήκους

Στην επίθεση επέκτασης μήκους υποθέτουμε ότι H είναι η συνάρτηση κατακερματισμού, η οποία βασίζεται στην κατασκευή των Merkle και Damgård. Σύμφωνα με την κατασκευή αυτή, η μέθοδος υλοποίησης της συνάρτησης κατακερματισμού, βασίζεται στη συνάρτηση συμπίεσης $f : \{0,1\}^n \times \{0,1\}^b \rightarrow \{0,1\}^n$. Η έξοδος της συνάρτησης κατακερματισμού H είναι μεγέθους n.

Σύμφωνα με την επιτιθέμενους, η συνάρτηση H είναι επιρρεπής στην επίθεση επέκτασης μήκους. Δεδομένης μίας σύγκρουσης (όταν υπάρχουν για παράδειγμα δύο μηνύματα d και d', με $|d| = |d'|$, τέτοια ώστε $H(d) = H(d')$) έχουμε για κάθε κατάληξη x, ότι $H(d||x) = H(d'||x)$. Η επίθεση αυτή μπορεί να εφαρμοστεί μόνο όταν η σύγκρουση προκύψει πριν από τους κενούς γύρους. Αν $m > n$, δηλαδή το μέγεθος της εσωτερικής κατάστασης είναι μεγαλύτερο της εξόδου της συνάρτησης κατακερματισμού, και λάβουμε υπόψη μόνο την επίθεση γενεθλίων, τότε

μία εσωτερική σύγκρουση είναι δυσκολότερο να βρεθεί από ότι στην περίπτωση σύγκρουσης για ολόκληρη τη συνάρτηση κατακερματισμού.

Μία σχετική ιδιότητα της σχεδίασης των Merkle και Damgård είναι, ότι αν το μήκος ενός αγνώστου μηνύματος d, οπότε και της προσαύξησης p του d, είναι γνωστό, καθώς και ότι η $H(d)$ είναι γνωστή, τότε η $H(d||p||x)$ μπορεί να υπολογιστεί για κάθε κατάληξη x. Αυτή η επίθεση αποτελεί απειλή σε ορισμένους σχεδιασμούς, οι οποίοι χρησιμοποιούν συνάρτηση κατακερματισμού για επικύρωση μηνυμάτων.

Αυτού του είδους η επίθεση μπορεί να εφαρμοστεί στις συναρτήσεις κατακερματισμού Grindahl, μόνο αν ο επιτιθέμενος μπορέσει να μαντέψει σωστά τα $b + m - n$ δυαδικά ψηφία που αποκόπτονται. Αν το καταφέρει, τότε μπορεί να συνεχίσει προς τα πίσω, μέσω των κενών γύρων, και να αποκαλύψει την επεκταμένη κατάσταση έπειτα από την επεξεργασία του τελευταίου τμήματος του μηνύματος.

6.6 Επίθεση πολλαπλών συγκρούσεων

Μία επίθεση πολλαπλών συγκρούσεων είναι ένα σύνολο που αποτελείται από τουλάχιστον δύο μηνύματα, τα οποία οδηγούν όλα στην ίδια τιμή κατακερματισμού [16]. Η επίθεση έχει πολυπλοκότητα $t2^{n/2}$ ώστε να βρεθούν 2^t τρόποι πολλαπλής σύγκρουσης, για μία συνάρτηση κατακερματισμού των n δυαδικών ψηφίων, η οποία βασίζεται στον σχεδιασμό των Merkle και Damgård. Στην περίπτωση της συνάρτησης Grindahl η πολυπλοκότητα είναι $t2^{m/2}$. Αν συγκριθεί με την εξαντλητική μέθοδο αναζήτησης για πολλαπλές συγκρούσεις, που έχει πολυπλοκότητα τουλάχιστον 2^n, φαίνεται καθαρά το πλεονέκτημά της. Για το λόγο αυτό, αν κάποιος επιθυμεί να μπορεί να αντιμετωπίσει πλήρως τις επιθέσεις πολλαπλής σύγκρουσης, πρέπει να επιλέξει $m \geq 2n$.

6.7 Επίθεση αγέλης

Η επίθεση αυτή δείχνει ακόμη ένα μειονέκτημα της σχεδίασης με βάση των Merkle και Damgård. Σε αυτή, ένα δυαδικό δέντρο συγκρούσεων χρησιμοποιείται για να διαμορφώσει ένα αποτέλεσμα h της συνάρτησης κατακερματισμού, το οποίο δημοσιοποιεί ο επιτιθέμενος. Στη συνέχεια, επιλέγει ένα μήνυμα, εντοπίζει κάποιο μήνυμα που να το συνδέει με τα φύλλα του δυαδικού δέντρου, οπότε έχει ένα ολοκληρωμένο,

μερικώς επιλεγμένο μήνυμα d με την τιμή h.

Η πολυπλοκότητα της απλούστερης έκδοσης της επίθεσης αυτής, όταν εφαρμοστεί στη σχεδίαση Merkle και Damgård, είναι περίπου $2^{(2n-5)/3}$. Στην περίπτωση της συνάρτησης Grindahl, αντικαθιστώντας το n με m, αν εξασφαλίσουμε $m \geq (3n+5)/2$ τότε η πολυπλοκότητα της επίθεσης είναι ίδια με εκείνη της προ-απεικόνισης.

Υπάρχει και μία σημαντική παραλλαγή της επίθεσης αυτής, για την οποία η πολυπλοκότητα μειώνεται καθώς αυξάνεται το μέγεθος του μηνύματος d. Αν το μέγεθος του d είναι περίπου 2^r, τότε η πολυπλοκότητα είναι περίπου $2^{(2n-5)/3-r}$. Έτσι, για δεδομένο άνω φράγμα του μηνύματος, το m πρέπει να επιλεγεί ανάλογα, ώστε να μπορεί να υπάρχει προστασία από αυτό το είδος επίθεσης.

Κεφάλαιο 7

Εκτίμηση ασφάλειας για τη συνάρτηση κατακερματισμού

7.1 Εισαγωγή

Στο κεφάλαιο αυτό θα σχολιάσουμε το κατά πόσο η συνάρτηση κατακερματισμού Grindahl παραμένει ασφαλής απέναντι στις επιθέσεις. Πρέπει να σημειώσουμε, ότι από τις επιθέσεις που παρουσιάστηκαν εστιάζουμε στις εξής δύο: επιθέσεις γενεθλίων και επιθέσεις σύγκρουσης. Θα παρουσιάσουμε τις εκτιμήσεις ασφάλειας τόσο από την πλευρά εκείνου που αναπτύσσει τη συνάρτηση κατακερματισμού, όσο και από την πλευρά του επιτιθέμενου.

7.2 Η άποψη του κατασκευαστή

Σε προηγούμενο κεφάλαιο αναπτύξαμε τις συναρτήσεις Grindahl-256 και Grindahl-512, οι οποίες βασίζονται στην εργασία των Knudsen, Rechberger, και Thomsen [3]. Στην ίδια εργασία αναφέρονται οι εκτιμήσεις σχετικά με την ασφάλεια των συναρτήσεων αυτών, οι οποίες είναι:

Grindahl-256: η προσπάθεια για εύρεση συγκρούσεων, δευτερευουσών προ-απεικονίσεων και προ-απεικονίσεων, είναι της τάξης των 2^{128} επαναλήψεων.

Grindahl-256: η προσπάθεια για εύρεση συγκρούσεων, δευτερευουσών προ-απεικονίσεων και προ-απεικονίσεων, είναι της τάξης των 2^{256} επα-

ναλήψεων.

Στην ίδια εργασία το ενδιαφέρον επικεντρώνεται στις επιθέσεις σύγκρουσης. Η συγκρούσεις μπορεί να είναι είτε εσωτερικές είτε εξωτερικές. Στην περίπτωση των εξωτερικών συγκρούσεων, ο αριθμός των κενών γύρων είναι αρκετός ώστε να εξαλείψει οποιοδήποτε διαφορικό, το χρησιμοποιεί μικρό αριθμό ενεργών ψηφιολέξεων. Στην περίπτωση των εσωτερικών συγκρούσεων, η ολοκληρωμένη κατάσταση η οποία έχει αρκετά μεγαλύτερο μέγεθος από το αντίστοιχο της εξόδου, πρέπει να συγκρουστεί με κάποια άλλη κατάσταση, εισάγοντας διαδοχικά διαφορετικά μηνύματα εισόδου. Για τον ίδιο σκοπό, και συγκεκριμένα για να αποδειχθεί η δυσκολία εφαρμογής τέτοιου είδους επιθέσεων στον Grindahl-256, γίνεται αναφορά στην Ιδιότητα 1, την οποία αναφέραμε στην ενότητα "Γενική στρατηγική εντοπισμού αποκομμένων διαφορών".

Παρά το γεγονός ότι δεν έγιναν εξαντλητικές αναζητήσεις για περισσότερους από 4 γύρους, φαίνεται εύκολα ότι μετά από δύο γύρους, είτε η αναζήτηση προχωρά προς τα εμπρός είτε προς τα πίσω, ένας μεγάλος αριθμός ψηφιολέξεων της κατάστασης έχει ήδη επηρεαστεί, οπότε είναι δύσκολη η μελέτη τέτοιου διαφορικού. Οι συγγραφείς καταλήγουν στο γεγονός ότι οι κλασσικές διαφορικές επιθέσεις δεν θα είναι επιτυχημένες στον Grindahl-256.

Στο ίδιο κλίμα κινούνται και οι εκτιμήσεις σχετικά με τον Grindahl-512. Συγκεκριμένα, υπάρχει ο ισχυρισμός ότι οι συγκρούσεις έπειτα από 4 γύρους εισαγωγής τμημάτων μηνύματος δεν μπορούν να προβλεφθούν. Ακόμη, λόγω της αποδοτικής τεχνικής συγκερασμού των ήδη χρησιμοποιημένων τμημάτων, πιστεύεται ότι καμία μέθοδος διαφορικής κρυπτανάλυσης δε θα οδηγήσει σε εσωτερικές συγκρούσεις.

7.3 Η άποψη του επιτιθέμενου

Τον ρόλο του επιτιθέμενου αναλαμβάνει ο Thomas Peyrin στην εργασία του [8]. Σύμφωνα με τον ίδιο, το πιο δύσκολο κομμάτι της επίθεσης είναι η εύρεση ενός κατάλληλου διαφορικού μονοπατιού. Αυτό όμως αντιμετωπίζεται, αφήνοντας τον αλγόριθμο να εξελιχθεί και τις διαφορές να μεταδίδονται, ώστε να καταλήξει κανείς σε ένα ζεύγος καταστάσεων εντελώς διαφοροποιημένο. Ακόμη, ενώ καλύτερα διαφορικά μονοπάτια μπορεί να βρεθούν με τη διατήρηση μικρής βαρύτητας για τις διαφορές (τα οποία είναι δύσκολο να βρεθούν), πιστεύεται ότι η

πολυπλοκότητα δε μειώνεται δραστικά σε σύγκριση με τις επιθέσεις σύγκρουσης, που παρουσιάστηκαν στην ίδια εργασία (και στην αντίστοιχη ενότητά μας "Επίθεση σύγκρουσης"). Είναι γεγονός ότι το κόστος πολυπλοκότητας αυξάνεται γρήγορα, εξαιτίας των επαναλήψεων του διαφορικού μονοπατιού (όπου πολύ λίγες ψηφιολέξεις ελέγχου είναι διαθέσιμες), ενώ τα βήματα αυτά θα συνεχίσουν να κοστίζουν πολύ, οποιοδήποτε διαφορικό μονοπάτι και αν ακολουθηθεί. Με άλλα λόγια, υπάρχει η δυνατότητα υπολογισμού ενός κάτω φράγματος στην πολυπλοκότητα της επίθεσης, με χρήση οπουδήποτε μονοπατιού αποκομμένου διαφορικού και ψηφιολέξεων ελέγχου.

Κεφάλαιο 8

Υλοποίηση συναρτήσεων κατακερματισμού Grindahl

8.1 Εισαγωγή

Στο κεφάλαιο αυτό θα εξετάσουμε τους τρόπους, με τους οποίους η συνάρτηση κατακερματισμού Grindahl εφαρμόζεται στην πράξη. Οι υλοποιήσεις των μελών αυτής της οικογένειας συναρτήσεων, μπορούν να αποκτήσουν χαρακτηριστικά που προέρχονται από την εκτενή έρευνα, η οποία έχει γίνει για τη βέλτιστη υλοποίηση του Προηγμένου Προτύπου Κρυπτογράφησης (Advanced Encryption Standard-AES). Ακόμη, οι επιθέσεις πλάγιου καναλιού (side-channel attacks), δηλαδή αυτές που εκμεταλλεύονται το φυσικό μέσο στο οποίο υλοποιείται το σύστημα, μπορεί να αποτελέσουν πρόβλημα, όταν η συνάρτηση κατακερματισμού χρησιμοποιείται για την επεξεργασία κλειδιού, χρησιμοποιείται ως συνάρτηση παραγωγής κλειδιού (key-derivation-function - KDF) ή χρησιμοποιείται ως σύστημα πιστοποίησης μηνύματος (message authentication code - MAC).

8.2 Υλοποίηση σε λογισμικό

Ο ρυθμός μίας συνάρτησης κατακερματισμού, η οποία επεξεργάζεται την είσοδο σε τμήματα, μετράται συνήθως με βάση τον αριθμό των τμημάτων που επεξεργάζεται για κάθε τμήμα κρυπτογραφημένου μηνύματος. Στην περίπτωση της συνάρτησης που εξετάζουμε, δανειζόμαστε αυτόν τον ορισμό όμως λαμβάνουμε υπόψη και το μέγεθος των επεκταμένων καταστάσεων, καθώς και το γεγονός ότι σε κάθε γύρο επεξεργάζονται v_{mb} ψηφιολέξεις, την ίδια στιγμή όπου στον AES-128

επεξεργάζονται 16 ψηφιολέξεις κάθε 10 γύρους. Έτσι, ο ρυθμός ενός στιγμιότυπου Grindahl είναι $\frac{10v_{mb}}{v_{mb}v_{bl}-v_{mb}}$. Επίσης, λαμβάνουμε υπόψη ότι οι v_{mb} ψηφιολέξεις, οι οποίες αντικαθίστανται από το επόμενο τμήμα μηνύματος, δε χρειάζεται να υπολογιστούν. Για παράδειγμα, ο ρυθμός των συναρτήσεων Grindahl-256 και Grindahl-512 είναι 5/6.

Σε μία βελτιωμένη υλοποίηση μέσω λογισμικού, της συνάρτησης Grindahl-n σε μία πλατφόρμα 32 δυαδικών ψηφίων (32-bit platform), απαιτούνται $n/64$ πίνακες των 256 λέξεων μήκους 32 δυαδικών ψηφίων η κάθε μία.

Σε πειραματική αξιολόγηση, η συνάρτηση κατακερματισμού Grindahl-256 υλοποιήθηκε σε γλώσσα προγραμματισμού C και εκτελέστηκε σε σύστημα με επεξεργαστή Pentium 4. Η συνάρτηση εκτελείται σε 32 κύκλους/ψηφιολέξη. Το αποτέλεσμα αυτό μπορεί να συγκριθεί με το αντίστοιχο του αλγορίθμου Rijndael-128, ο οποίος είναι υλοποιημένος στο πακέτο Crypto++, ο οποίος σύμφωνα με την ιστοσελίδα του, εκτελείται σε 33 κύκλους/ψηφιολέξη σε σύστημα με επεξεργαστή Pentium 4. Όπως αναμενόταν, η απόδοση είναι παρόμοια. Μία ακόμη σύγκριση μπορεί να γίνει με τον Secure Hash Algorithm - 256 (SHA-256), ο οποίος σε ίδιο σύστημα εκτελείται σε 45 κύκλους/ψηφιολέξη. Όσον αφορά την συνάρτηση Grindahl-512, είναι προτιμότερο να χρησιμοποιείται σε σύστημα αρχιτεκτονικής 64 δυαδικών ψηφίων (64-bit), ενώ η απόδοσή της αναμένεται ίδια με την αντίστοιχη της Grindahl-256.

8.3 Υλοποίηση σε υλικό

Οι σχεδιασμοί οι οποίοι δεν απαιτούν ειδικές διατάξεις για πηγή ενέργειας (passively powered), χρειάζονται έναν μικρό αριθμό ενεργών καταχωρητών ανά κύκλο ρολογιού. Σε αντίθεση με την οικογένεια συναρτήσεων κατακερματισμού Message-Digest Algorithm (MD4), ο σχεδιασμός σε υλικό της συνάρτησης Grindahl επιτρέπει μονοπάτια δεδομένων μικρού εύρους, χωρίς απώλειες απόδοσης. Ακόμη, συγκρινόμενος με την οικογένεια MD4, καθώς και άλλες προτάσεις, ο σχεδιασμός της συνάρτησης Grindahl απαιτεί μικρότερο αριθμό καταχωρητών, πράγμα που σημαίνει υλοποίηση με χαμηλό κόστος και μικρές απαιτήσεις σε ενέργεια. Εκτός αυτού, διάφοροι συμβιβασμοί που αφορούν την ταχύτητα μπορούν να εφαρμοστούν, όπως έχει συμβεί και στην περίπτωση του AES, οδηγώντας σε ακόμη μικρότερο αριθμό απαιτούμενων καταχωρητών.

Όταν η υλοποίηση αφορά υλικό χαμηλού κόστους, οι εκτιμώμενες απαιτήσεις της συνάρτησης Grindahl-256 ανέρχονται σε 5-6,000 ισοδύναμα πυλών (gate equivalents), όπου με τον όρο ισοδύναμα πυλών εννοούμε τη συγκριτική πολυπλοκότητα του υπό μελέτη σχεδιασμού σε σχέση με τις απαιτούμενες λογικές πύλες [9]. Αυτό αποτελεί σημαντικό πλεονέκτημα σε σχέση με την υλοποίηση του SHA-256 που απαιτεί 10,000 ισοδύναμα πυλών.

8.4 Απαιτήσεις σε μνήμη

Εξαιτίας των μικρών τμημάτων μηνύματος, η απαιτούμενη μνήμη για τις συναρτήσεις κατακερματισμού Grindahl-256 και Grindahl-512 είναι μικρή. Αυτό εξυπηρετεί υλοποιήσεις με περιορισμένους πόρους. Είναι αξιοσημείωτο το γεγονός, ότι ο τρόπος σχεδίασης των συναρτήσεων Grindahl απαιτεί μόνο $b + m$ δυαδικά ψηφία μνήμης για τη λειτουργία του. Αντίθετα, οι υλοποιήσεις των συναρτήσεων της οικογένειας MD4, απαιτούν $b+2m$ δυαδικά ψηφία μνήμης, όπου $b = 512$ και m είναι ίσο με το μέγεθος της εξόδου.

Στον Πίνακα 8.1 φαίνεται η σύγκριση των συναρτήσεων Grindahl με άλλες συναρτήσεις κατακερματισμού, αναφορικά με τις λειτουργικές απαιτήσεις σε μνήμη.

Πίνακας 8.1: Λειτουργικές απαιτήσεις σε μνήμη

128-bit ασφάλεια		256-bit ασφάλεια	
όνομα	μνήμη	όνομα	μνήμη
Grindahl-256	416	Grindahl-512	832
SHA-256	1024	SHA-512	2048
RadioGatún	812	RadioGatún	1566
FORK-256	1280	Whirlpool	1536
LASH-256	1536	LASH-512	3072

Κεφάλαιο 9

Συμπεράσματα και ανοικτά θέματα

Στην παρούσα εργασία μελετήθηκαν οι συναρτήσεις κατακερματισμού που εφαρμόζονται στην κρυπτογραφία. Συγκεκριμένα, έγινε η ανάλυση του τρόπου λειτουργίας δύο χαρακτηριστικών συναρτήσεων, των Grindahl-256 και Grindahl-512, ενώ μελετήθηκαν διεξοδικά οι αρχές λειτουργίας της οικογένειας συναρτήσεων στην οποία ανήκουν. Ακόμη, μελετήθηκαν σε βάθος οι τεχνικές κρυπτανάλυσης οι οποίες εφαρμόζονται στις συναρτήσεις κατακερματισμού, δίνοντας έμφαση στην ασφάλεια που προσφέρουν οι Grindahl-256 και Grindahl-512.

Ο σχεδιασμός των συναρτήσεων κατακερματισμού της οικογένειας Grindahl, περιέχει τις αρχές του αλγορίθμου Rijndael. Έτσι, υπόσχεται ότι ο επιτιθέμενος δε μπορεί να βρει μία αποδοτική μέθοδο εντοπισμού συγκρούσεων, ώστε να τη χρησιμοποιήσει στη συνέχεια για την αποκρυπτογράφηση των εξόδων της συνάρτησης. Η υπόσχεση αυτή όμως δεν ισχύει, τουλάχιστον για την έκδοση της συνάρτησης των 256 δυαδικών ψηφίων. Όπως είδαμε αναπτύσσοντας τις τεχνικές κρυπτανάλυσης και τις μεθόδους επίθεσης, για την Grindahl-256 απαιτούνται 2^{112} υπολογισμοί της συνάρτησης, σε αντίθεση με τον ισχυρισμό των κατασκευαστών για απαίτηση 2^{128} υπολογισμών [15].

Το κενό ασφαλείας που επισημάνθηκε, αποτελεί το έναυσμα για βελτιώσεις της συνάρτησης κατακερματισμού Grindahl. Οι βελτιώσεις αυτές αφορούν την αντίσταση στις επιθέσεις που αναφέρθηκαν, καθώς και τη θωράκιση απέναντι στις επιθέσεις που αφορούν τον εντοπισμό διαφορών και την εισαγωγή ψηφιολέξεων ελέγχου. Το ζητούμενο είναι ο επιτιθέμενος να χρειάζεται να κάνει 2^{128} πράξεις ή και περισσότε-

ρες, προκειμένου να είναι ασφαλής η συνάρτηση. Σε αυτό θα βοηθούσε μία παραλλαγή του μετασχηματισμού SubBytes, η οποία θα απέτρεπε τον άμεσο εντοπισμό διαφορών στις ψηφιολέξεις κατάστασης. Για την εφαρμογή της αλλαγής αυτής απαιτείται η προσθήκη επιπλέον στηλών στις καταστάσεις, ο ακριβής αριθμός του όμως, ο οποίος θα συνδυάζει ασφάλεια και αποδοτικότητα, παραμένει ανοικτό θέμα για περεταίρω έρευνα.

Τέλος, πρέπει να σημειωθεί ότι οι υλοποιήσεις των συναρτήσεων Grindahl-256 και Grindahl-512, υπερέχουν σε ταχύτητα έναντι άλλων προτάσεων. Όπως είδαμε, η υλοποίησή τους, τόσο σε λογισμικό όσο και σε υλικό, αποτελεί μία πολύ αποδοτική λύση για κρυπτογράφηση δεδομένων.

Βιβλιογραφία

[1] http://en.wikipedia.org/wiki/Cryptographic_hash_function

[2] http://el.wikipedia.org/wiki/Κρυπτογραφικοί_Αλγόριθμοι_Δέσμης

[3] Lars R. Knudsen, Christian Rechberger, and Søren S. Thomsen *Grindahl – a family of hash functions*

[4] L.R. Knudsen, *Truncated and Higher Order Differentials. In B. Preneel*, volume 1008 of Lecture Notes in Computer Science, Springer-Verlag, 1995.

[5] http://en.wikipedia.org/wiki/Birthday_problem

[6] http://en.wikipedia.org/wiki/Birthday_attack

[7] http://en.wikipedia.org/wiki/Collision_attack

[8] Thomas Peyrin, *Cryptanalysis of GRINDAHL*

[9] http://en.wikipedia.org/wiki/Gate_equivalent

[10] Joan Daemen and Vincent Rijmen, *The Block Cipher Rijndael*

[11] http://en.wikipedia.org/wiki/Cryptanalysis

[12] Friedrich L. Bauer *Decrypted Secrets*

[13] Joan Daemen, Vincent Rijmen, *AES Proposal: Rijndael*

[14] Elisabeth Oswald, Joan Daemen, Vincent Rijmen, *AES - The State of the Art of Rijndael's Security*

[15] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, Doug Whiting, *Improved Cryptanalysis of Rijndael*

[16] Antoine Joux *Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions*

[17] Robert Matthews, Fiona Stones *Coincidences: the truth is out there*