ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΒΑΣΙΣΜΕΝΗ ΣΕ ΔΙΚΤΥΩΜΑΤΑ ΑΚΕΡΑΙΩΝ ΘΕΩΡΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

Διπλωματική Εργασία

της

Χριστίνας Ζερβοπούλου

Θεσσαλονίκη, Οκτώβριος 2013

ΚΡΥΠΤΟΓΡΑΦΙΑ ΒΑΣΙΣΜΕΝΗ ΣΕ ΔΙΚΤΥΩΜΑΤΑ ΑΚΕΡΑΙΩΝ ΘΕΩΡΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

Ζερβοπούλου Χριστίνα

Πτυχίο Μηχανικού Η/Υ και Τηλεπικοινωνιών, ΑΤΕΙ Λάρισας, 2006

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ
ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Δρ. Γ.Χ. Στεφανίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/11/2013

Γ.Χ. Στεφανίδης	Δ. Χρήστου – Βαρσακέλης	Ι. Μαυρίδης
.....	.....	.....

Ζερβοπούλου Χριστίνα

.....

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται το είδος εκείνο της κρυπτογραφίας το οποίο χρησιμοποιεί δικτυώματα ακέραιων αριθμών, τόσο στις διαδικασίες της κρυπτογράφησης κι αποκρυπτογράφησης ενός μηνύματος, όσο και στις συναρτήσεις διασποράς και τις ψηφιακές υπογραφές. Η κρυπτογραφία με χρήση δικτυωμάτων, η οποία αποτελεί τμήμα της λεγόμενης μετα-κβαντικής κρυπτογραφίας, γεννήθηκε το 1996 με το κρυπτοσύστημα Ajtai–Dwork κι έκτοτε χαίρει παγκόσμιου ερευνητικού ενδιαφέροντος και μελέτης κι αποτελεί μία ιδιαίτερα σύγχρονη και ανταγωνιστική τεχνική σε παλαιότερα είδη κρυπτογραφίας, όπως ο αλγόριθμος RSA (Rivest – Shamir – Adleman) και η κρυπτογραφία ελλειπτικών καμπυλών (Elliptic Curve Cryptography – ECC). Αυτό το είδος κρυπτογραφίας έχει ως βάση κάποια δυσεπίλυτα –υπολογιστικά – μαθηματικά προβλήματα που ανακύπτουν από τη χρήση δικτυωμάτων, όπως το πρόβλημα της εύρεσης του βραχύτερου διανύσματος (Shortest Vector Problem – SVP) σε ένα δικτύωμα ακεραίων σε ένα n–διάστατο Ευκλείδειο χώρο ή το πρόβλημα της εύρεσης του εγγύτερου (εξωτερικού) διανύσματος (Closest Vector Problem – CVP) σε ένα δοθέν διάνυσμα συγκεκριμένου δικτυώματος σε ένα n–διάστατο Ευκλείδειο χώρο, καθώς επίσης και διάφορες παραλλαγές αυτών των δύο βασικών προβλημάτων. Εκτός από τα παραπάνω, παρουσιάζονται εδώ οι πιο γνωστοί αλγόριθμοι αναγωγής της βάσης ενός δικτυώματος, όπως ο LLL (Lenstra – Lenstra – Lovász), ο HKZ (Hermite – Korkine – Zolotarev) κ.ά., καθώς και τα πιο γνωστά κρυπτοσυστήματα (Ajtai – Dwork (AD), Goldreich – Goldwasser – Halevi (GGH), NTRU) που είναι βασισμένα σε δικτυώματα ακεραίων. Η παρούσα διπλωματική εργασία ασχολείται επίσης με την πιο γνωστή συνάρτηση διασποράς αυτού του είδους, τη LASH–x και αναφέρεται στην κρυπτανάλυσή της. Επίσης, παρουσιάζονται οι συναρτήσεις διασποράς SWIFFT και SWIFFTX που βασίζονται σε γρήγορους μετασχηματισμούς Fourier αλλά και οι ψηφιακές υπογραφές με χρήση δικτυωμάτων (GGH, NTRUSign). Τέλος, καταγράφονται τα τρέχοντα ανοιχτά ζητήματα σε αυτό το ερευνητικό πεδίο.

Λέξεις Κλειδιά: Κρυπτογραφία Δημοσίου Κλειδιού, Δικτυώματα Ακεραίων, LLL, GGH, NTRU, LASH–x, Μετα–κβαντική Κρυπτογραφία

Abstract

This thesis deals with the kind of cryptography that uses integer lattices in the processes of message encryption/decryption, hash functions and digital signatures. Cryptography based on lattices, which is part of the so called post-quantum cryptography, was born in 1996 with Ajtai–Dwork cryptosystem and since then enjoys global research interest and study, as it is a very modern and competitive technique to older types of cryptography such as RSA algorithm and elliptic curve cryptography (Elliptic Curve Cryptography – ECC). Lattice–based cryptography is based on some hard–to–solve math problems arising from the use of lattices, such as the problem of finding the shortest vector (Shortest Vector Problem – SVP) in an integer lattice in an n–dimensional Euclidean space, or the problem of finding the closest (exterior) vector (Closest Vector Problem – CVP) to a given vector in a n–dimensional given lattice and variants of these two fundamental problems. Apart from the above the most common lattice basis reduction algorithms are presented here, such as LLL (Lenstra – Lenstra – Lovász), HKZ (Hermite – Korkine – Zolotarev), etc., and the best known cryptosystems (Ajtai–Dwork (AD), Goldreich–Goldwasser–Halevi (GGH), NTRU) that are based on integer lattices. This thesis also deals with the most well–known hash function of this kind, the LASH–x, and refers to its cryptanalysis. SWIFFT and SWIFFTX hash functions, based on Fast Fourier Transformations, are presented but also digital signatures using lattices (GGH, NTRUSign). Finally, current open issues in this field of research are recorded.

Keywords: Public Key Cryptography, Integer Lattices, LLL, GGH, NTRU, LASH–x, Post–Quantum Cryptography

Ευχαριστίες

Με την ολοκλήρωση της παρούσης διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα αυτής, Καθηγητή, κ. Γ.Χ. Στεφανίδη, για την ενθάρρυνσή του να μελετήσω ένα τόσο ενδιαφέρον θέμα και την πολύτιμη καθοδήγησή του σε κάθε στάδιο της δημιουργίας της. Επιθυμώ να εκφράσω τη βαθιά ευγνωμοσύνη μου για την εμπιστοσύνη που επέδειξε στο πρόσωπό μου και την ουσιαστική συμβολή του.

Ακόμη, θα ήθελα να ευχαριστήσω την οικογένειά μου, αλλά και τους φίλους μου, για την κατανόηση και την ψυχολογική συμπαράσταση που πάντα μου προσφέρουν.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

- AES (Advanced Encryption Standard) – Προηγμένο Πρότυπο Κρυπτογράφησης
- ECDSA (Elliptic Curve Digital Signature Algorithm) – Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικών Καμπυλών
- FSE (Fast Software Encryption) – Γρήγορη Κρυπτογράφηση Λογισμικού
- GCHQ (Government Communications Headquarters) – Αρχηγείο Κυβερνητικών Υπηρεσιών (ΗΠΑ)
- IBE (Identity–based Encryption) – Κρυπτογράφηση βασισμένη στην ταυτότητα
- IEEE (Institute of Electrical and Electronics Engineers) – Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
- NBS (National Bureau of Standards) – Εθνικό Γραφείο Προτύπων
- NIST (National Institute of Standards and Technology) – Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας
- PKI (Public Key Infrastructure) – Υποδομή Δημοσίου Κλειδιού

Κεφάλαιο 1
Εισαγωγή

Η κρυπτογραφία αποτελεί κλάδο της επιστήμης της *κρυπτολογίας*, η οποία αναφέρεται στη μελέτη της ασφαλούς επικοινωνίας. Κρυπτολογία είναι η επιστήμη που μελετά μαθηματικές τεχνικές, ώστε να παρέχει στις ψηφιακές πληροφορίες αυθεντικότητα, στις ψηφιακές επικοινωνίες μυστικότητα (απόρρητο) και άλλες παρεμφερείς ιδιότητες, συμπεριλαμβανομένης της ασφαλούς εφαρμογής των τεχνικών αυτών. Η κρυπτολογία αποτελεί ένα θεμελιώδη καταλύτη για ασφαλείς και αξιόπιστες υποδομές και ένα διεπιστημονικό ερευνητικό τομέα με υψηλές, στρατηγικές επιπτώσεις για τη βιομηχανία και για την κοινωνία στο σύνολό της.

Συγκεκριμένα, η κρυπτολογία διακρίνεται σε δύο μεγάλους κλάδους, την *κρυπτογραφία*, η οποία ασχολείται με τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων και την *κρυπτανάλυση*, η οποία αφορά τη μελέτη διαδικασιών για την παραβίαση αυτών.

Η διεθνής βιβλιογραφία βρίθει ορισμών για την κρυπτογραφία. Οι περισσότεροι από αυτούς αναφέρονται στην απαίτηση για μυστικότητα της επικοινωνίας μεταξύ δύο ή περισσοτέρων άκρων σε ένα σύστημα επικοινωνίας: «Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή» [1]. Όσον αφορά τη βασική ορολογία που χρησιμοποιείται στην κρυπτογραφία και συγκεκριμένα τις έννοιες που αντιστοιχούν στο πεδίο ορισμού και στο σύνολο τιμών της διαδικασίας της κρυπτογράφησης, αυτές έχουν ως εξής: Το A συμβολίζει ένα πεπερασμένο σύνολο που λέγεται αλφάβητο ορισμού [7]. Το M συμβολίζει ένα σύνολο που λέγεται χώρος μηνυμάτων. Το σύνολο M αποτελείται από συμβολοσειρές συμβόλων από ένα αλφάβητο ορισμού. Ένα στοιχείο του M λέγεται μήνυμα απλού κειμένου ή απλό κείμενο (plaintext). Το C συμβολίζει ένα σύνολο που λέγεται χώρος κρυπτοκειμένων. Το C αποτελείται από συμβολοσειρές συμβόλων από ένα αλφάβητο ορισμού, το οποίο μπορεί να διαφέρει από το αλφάβητο ορισμού για το M. Ένα στοιχείο του C λέγεται κρυπτοκείμενο (ciphertext) [7]. Ο όρος «κρυπτοκείμενο» συναντάται στη βιβλιογραφία και ως κρυπτογράφημα. Όσον αφορά τις έννοιες που αφορούν τους μετασχηματισμούς κρυπτογράφησης και αποκρυπτογράφησης, αυτές έχουν ως εξής: Το K συμβολίζει ένα σύνολο που λέγεται χώρος κλειδιών ή

κλειδοχώρος . Ένα στοιχείο του K λέγεται κλειδί. Κάθε στοιχείο $e \in K$ προσδιορίζει κατά μοναδικό τρόπο μια αμφιμονοσήμαντη αντιστοιχία από το M στο C, που συμβολίζεται με E_e. Η E_e λέγεται συνάρτηση κρυπτογράφησης ή μετασχηματισμός κρυπτογράφησης . Να σημειωθεί ότι η E_e πρέπει να είναι αμφιμονοσήμαντη αντιστοιχία, εάν πρόκειται η διαδικασία να είναι αντιστρέψιμη, και για κάθε διακεκριμένο κρυπτοκείμενο να είναι ανακτήσιμο ένα μοναδικό μήνυμα απλού κειμένου. Για κάθε $d \in K$, η D_d συμβολίζει μία αμφιμονοσήμαντη αντιστοιχία από το C στο M (δηλ., $D_d : C \rightarrow M$). Η D_d λέγεται συνάρτηση αποκρυπτογράφησης ή μετασχηματισμός αποκρυπτογράφησης [7]. Η διαδικασία εφαρμογής του μετασχηματισμού E_e σε ένα μήνυμα $m \in M$ αναφέρεται συνήθως ως κρυπτογράφηση του m. Η διαδικασία εφαρμογής του μετασχηματισμού D_d σε ένα κρυπτοκείμενο c αναφέρεται συνήθως ως αποκρυπτογράφηση του c. Ένα σχήμα κρυπτογράφησης αποτελείται από ένα σύνολο μετασχηματισμών κρυπτογράφησης $\{E_e : e \in K\}$ και ένα αντίστοιχο σύνολο μετασχηματισμών αποκρυπτογράφησης $\{D_d : d \in K\}$ με την ιδιότητα ότι, για κάθε $e \in K$ υπάρχει ένα μοναδικό κλειδί $d \in K$ τέτοιο, ώστε $D_d = E_e^{-1}$, δηλαδή, $D_d(E_e(m)) = m$ για κάθε $m \in M$. Ένα σχήμα κρυπτογράφησης μερικές φορές αναφέρεται ως κρυπταλγόριθμος. Το κλειδί e λέγεται κλειδί κρυπτογράφησης (encryption key) και το κλειδί d αποτελεί το κλειδί αποκρυπτογράφησης (decryption key). Μαζί αναφέρονται ως ζεύγος κλειδιών και συμβολίζονται μερικές φορές με (e, d). Να σημειωθεί ότι τα e και d θα μπορούσαν να είναι ίδια. Η κατασκευή ενός σχήματος κρυπτογράφησης απαιτεί να επιλέγουμε έναν χώρο μηνυμάτων M, έναν χώρο κρυπτοκειμένων C, έναν χώρο κλειδιών K, ένα σύνολο μετασχηματισμών κρυπτογράφησης $\{E_e : e \in K\}$ και το αντίστοιχο σύνολο μετασχηματισμών αποκρυπτογράφησης $\{D_d : d \in K\}$ [7]. Τέλος, κάλυμμα ενός μηνύματος (padding) ονομάζουμε το επιπρόσθετο κείμενο το οποίο πρέπει να προσθέσουμε στο αρχικό κείμενο προκειμένου αυτό να αποκτήσει ένα συγκεκριμένο μήκος, σύμφωνο με τις απαιτήσεις ενός αλγόριθμου κρυπτογράφησης. Το κάλυμμα ενός μηνύματος αφαιρείται κατά την αποκρυπτογράφησή του. Συνήθως το κείμενο που προστίθεται είναι το μήκος του αρχικού κειμένου ακολουθούμενο από μηδενικό ή αντίστροφα.

Υπάρχουν δύο σημαντικές αρχές που πρέπει να θυμόμαστε: η σύγχυση (confusion) και η διάχυση (diffusion) [93]. Ο σκοπός της σύγχυσης είναι να κάνει τη σχέση μεταξύ του κλειδιού και του κρυπτογραφήματος όσο το δυνατόν πιο περίπλοκη. Οι αλγόριθμοι κρυπτογράφησης που δεν προσφέρουν μεγάλη σύγχυση (όπως ο

Vigenere) είναι επιρρεπείς σε ανάλυση συχνοτήτων (μία τεχνική με βάση το γεγονός ότι μέσα σε ένα κείμενο ορισμένα γράμματα και συνδυασμοί γραμμάτων εμφανίζονται με ποικίλες συχνότητες).

Σε αντίθεση με τη σύγχυση, η διάχυση εξαπλώνει την επίδραση ενός και μοναδικού bit απλού κειμένου σε πολλά bits κρυπτοκειμένου. Συνήθως μιλάμε για δεδομένα διάχυσης, στα οποία η αλλαγή ενός μικρού μέρους των δεδομένων του απλού κειμένου μπορεί να επηρεάσει ολόκληρο το κρυπτοκείμενο. Αλλά μπορούμε επίσης να μιλάμε για κλειδί διάχυσης, στο οποίο αλλάζοντας ακόμη και ένα μικρό μέρος του κλειδιού, αλλάζει κάθε bit στο κρυπτογράφημα με δεδομένη πιθανότητα [93].

Σύμφωνα με τον Ron Rivest, η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων. Ως «αντίπαλοι» στη σύγχρονη κρυπτογραφία, εκτός από τα φυσικά πρόσωπα που επιδιώκουν να παρακολουθήσουν την επικοινωνία, θεωρούνται η πιθανή αλλοίωση του περιεχομένου του μηνύματος που επιχειρεί να αποστείλει ο πομπός στο δέκτη, η μη αντίληψη της ενδεχόμενης αλλοίωσης του περιεχομένου του μηνύματος από το δέκτη και η παραλαβή του μηνύματος από κάποιον που υποδύεται τον πραγματικό δέκτη, αλλά δεν είναι αυτός.

Στις μέρες μας, όπου η κατασκευή κβαντικών υπολογιστών για επικοινωνίες παγκόσμιας εμβέλειας θεωρείται από αρκετούς επιστήμονες ότι είναι προ των πυλών, η αναγκαιότητα για ύπαρξη ενός είδους κρυπτογραφίας που να μπορεί να αντισταθεί σε επιθέσεις από τέτοιες συσκευές, είναι προφανής. Η κβαντική κρυπτογραφία, η οποία αναφέρεται στη χρήση της κβαντομηχανικής (ιδίως της κβαντικής επικοινωνίας και των κβαντικών υπολογισμών) για την επίτευξη της μυστικότητας μεταξύ δύο επικοινωνούντων μερών, αποτελεί μία ασφαλή εναλλακτική λύση στην απειλή των κβαντικών υπολογιστών ενάντια σε πολλά από τα κρυπτοσυστήματα που χρησιμοποιούνται ευρέως σήμερα. Παρόλα αυτά, πολλοί κρυπτογράφοι ανά τον κόσμο ερευνούν νέους αλγόριθμους, ακόμα και εάν οι τρέχοντες, δημόσια γνωστοί, πειραματικοί κβαντικοί υπολογισμοί απέχουν πολύ από το να είναι αρκετά ισχυροί ώστε να επιτεθούν σε πραγματικά κρυπτοσυστήματα. Η μελέτη τέτοιων κρυπταλγορίθμων συχνά αναφέρεται ως μετα–κβαντική κρυπτογραφία [98] και οι ερευνητικές εργασίες αυτού του είδους δημοσιεύονται από τη σειρά συνεδρίων PQCrypto από το 2006.

Η μετα–κβαντική κρυπτογραφία δεν έχει κάποια σημασιολογική συσχέτιση με την κβαντική κρυπτογραφία, η οποία αναφέρεται στη χρήση κβαντικών φαινομένων για την επίτευξη απορρήτου. Καθιερώθηκε ως όρος από τον Dave Bernstein το 1999 και

ασχολείται με την έρευνα για κρυπτογραφικά εργαλεία, συνήθως κρυπτοσυστήματα δημοσίου κλειδιού, που δεν είναι αποτελεσματικά εύθραυστα εάν χρησιμοποιηθούν κβαντικοί υπολογιστές περισσότερο από αρχιτεκτονικές κλασσικών υπολογιστών [98]. Παραδείγματα κρυπτογραφικών συστημάτων, που, από όσο γνωρίζουμε σήμερα, είναι ασφαλή έναντι κβαντικών απειλών είναι το κρυπτοσύστημα McEliece (1978–R.M.McEliece) και διάφορα κρυπτοσυστήματα βασισμένα σε δικτυώματα ακεραίων, όπως το NTRU και το κρυπτοσύστημα των Goldwasser, Goldreich και Halevi (GGH) που θα παρουσιασθούν παρακάτω. Αντίθετα, τα περισσότερα από τα πρόσφατα συμμετρικά κρυπτογραφικά συστήματα (συμμετρικοί αλγόριθμοι κρυπτογράφησης και συναρτήσεις διασποράς) δεν είναι ασφαλή από τους κβαντικούς υπολογιστές. Ο κβαντικός αλγόριθμος του Grover [98] μπορεί να επιταχύνει επιθέσεις εναντίον συμμετρικών κρυπτοαλγορίθμων, αλλά αυτό μπορεί να αντισταθμιστεί με την αύξηση του μεγέθους του κλειδιού. Έτσι, η μετά–κβαντική κρυπτογραφία δεν επικεντρώνεται σε συμμετρικούς αλγόριθμους.

Η μετά–κβαντική κρυπτογραφία εστιάζει σε τέσσερις τύπους κρυπτογραφικών συστημάτων, τα οποία μπορεί να είναι σε θέση να αποκρούσουν επιθέσεις από κβαντικούς υπολογιστές. Η διαφορά μεταξύ αυτών είναι ότι βασίζονται σε διαφορετικές μαθηματικές δομές. Από αυτούς τους τύπους κρυπτογραφικών συστημάτων, οι δύο πρώτοι αφορούν σχήματα κρυπτογράφησης της επικοινωνίας, ενώ οι τελευταίοι αφορούν σχήματα ψηφιακών υπογραφών. Έτσι έχουμε:

- Κρυπτογραφία βασισμένη σε δικτυώματα ακεραίων, όπως τα κρυπτοσυστήματα NTRU και GGH
- Κρυπτογραφία βασισμένη σε κώδικες (διόρθωσης σφαλμάτων), όπως το κρυπτοσύστημα McEliece, αλλά και οι υπογραφές Niederreiter
- Ψηφιακές υπογραφές βασισμένες σε συναρτήσεις διασποράς (hash–based signatures), όπως οι υπογραφές Lamport και το σχήμα υπογραφής Merkle
- Ψηφιακές υπογραφές βασισμένες σε πολυμεταβλητά, τετραγωνικά πολυώνυμα, όπως το σχήμα Oil and Vinegar του Patarin (1997) και συγκεκριμένα η unbalanced εκδοχή του (UVO – Unbalanced Vinegar and Oil) [98].

Κάθε μία από αυτές τις ερευνητικές περιοχές παρουσιάζει ιδιαίτερο ενδιαφέρον για αυτήν την ιδιότητα κβαντικής αντίστασης που φέρει και έχει πολλά να προσφέρει στον τομέα της ασφάλειας των επικοινωνιών.

Στις σύγχρονες ερευνητικές τάσεις στην κρυπτογραφία συγκαταλέγονται, επίσης, εκτός από τα παραπάνω, η κρυπτογράφηση δημοσίου κλειδιού που βασίζεται στην ταυτότητα (identity–based encryption – IBE) [18, 78], η επίτευξη ασφαλούς επικοινωνίας σε μία ομάδα (secure group communication) [84], αλλά και η λεγόμενη «πράσινη» κρυπτογραφία (green cryptography) [44, 80]. Στην κρυπτογράφηση που βασίζεται στην ταυτότητα (IBE), το δημόσιο κλειδί είναι μία δημόσια γνωστή συμβολοσειρά που αντιπροσωπεύει ένα άτομο ή μία οργάνωση, η οποία θα μπορούσε να περιλαμβάνει μία διεύθυνση ηλεκτρονικού ταχυδρομείου, ένα όνομα τομέα (domain name), ή μία φυσική διεύθυνση IP [98]. Οι ασφαλείς επικοινωνίες σε μία ομάδα περιλαμβάνουν διάφορους τύπους υπηρεσιών, όπως τηλεδιάσκεψη, συνδρομητικές τηλεοπτικές υπηρεσίες (pay TV) κ.ά. Η ασφάλεια των επικοινωνιών πολλαπλής διανομής (multicast) περιλαμβάνει έλεγχο της ιδιότητας των μελών της ομάδας, ασφαλή διανομή κλειδιού, ασφαλή μεταφορά δεδομένων κα προστασία των πνευματικών δικαιωμάτων. Η έννοια της «πράσινης» κρυπτογραφίας υιοθετεί την αρχή της ανακύκλωσης της σχεδίασης κρυπτογραφικών στρατηγικών, συστατικών στοιχείων και αρχών. Σε αυτό το πεδίο έχουν αναπτυχθεί διάφοροι «ελαφρείς» (lightweight) κρυπταλγόριθμοι, από τον NOEKEON [97] το 2000 έως και τον KLEIN [32] το 2012, από τους οποίους όσον αφορά στην κατανάλωση ενέργειας υπερέχει ο PRESENT [17] που αναπτύχθηκε το 2007 και ακολουθεί ο NOEKEON, ενώ και ο γνωστότερος AES κυμαίνεται σε αρκετά καλά επίπεδα.

Υπάρχει επίσης έρευνα για το πώς υπάρχουσες τεχνικές κρυπτογράφησης πρέπει να τροποποιηθούν, ώστε να είναι σε θέση να αντιμετωπίσουν κβαντικούς πλέον αντιπάλους. Οποιαδήποτε περαιτέρω μελέτη σχετικά με όσα αναφέρθηκαν παραπάνω θεωρείται εκτός των σκοπών της παρούσης εργασίας.

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η παρούσα διπλωματική εργασία πραγματεύεται το είδος εκείνο της μετα-κβαντικής κρυπτογραφίας, το οποίο χρησιμοποιεί δικτυώματα ακεραίων (σύνολα σημείων σε n–διάστατο χώρο με περιοδική δομή) τόσο στις διαδικασίες της κρυπτογράφησης κι αποκρυπτογράφησης ενός μηνύματος, όσο και στις συναρτήσεις διασποράς και τις ψηφιακές υπογραφές.

Η κρυπτογραφία γεννήθηκε ως απάντηση στην ανάγκη για προάσπιση της πληροφορίας από εχθρικά ή κακόβουλα χέρια. Η πληροφορία μετατρέπεται από μία

κανονική, κατανοητή μορφή σε έναν «γρίφο», ο οποίος χωρίς τη γνώση κάποιου κρυφού μετασχηματισμού παραμένει ακατανόητος. Στις παλαιότερες μορφές κρυπτογράφησης η επεξεργασία γινόταν πάνω στη γλωσσική δομή του μηνύματος. Στις νεότερες μορφές, με την ανάπτυξη της τεχνολογίας και των ηλεκτρονικών υπολογιστών, η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου (modulus) [98].

Η προστασία της μεταφερόμενης διαμέσου ενός επικοινωνιακού συστήματος πληροφορίας επιστρατεύει στοιχεία από διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση. Εκτός από την κρυπτογραφία, όμως, έχει αναπτυχθεί και η κρυπτανάλυση. Η κρυπτογραφία και η κρυπτανάλυση βρίσκονται σε μία αέναη διαμάχη. Έτσι, ερευνώνται διαρκώς νέες μαθηματικές ιδέες, είτε από τη μία πλευρά (κρυπτογραφία), ώστε να προστατεύονται οι πληροφορίες από μη εξουσιοδοτημένους χρήστες, είτε από την άλλη (κρυπτανάλυση), προκειμένου να αποδεικνύεται η ανεπάρκεια της ασφάλειας ενός κρυπτογραφικού αλγορίθμου [98].

Η ανάγκη για μετα–κβαντική κρυπτογραφία προέκυψε από το γεγονός ότι τα περισσότερα δημοφιλή κρυπτοσυστήματα δημόσιου κλειδιού που υπάρχουν σήμερα (όπως είναι ο RSA και οι παραλλαγές του, καθώς και συστήματα που βασίζονται σε ελλειπτικές καμπύλες) βασίζονται στο πρόβλημα παραγοντοποίησης ακεραίων ή στο πρόβλημα του διακριτού λογαρίθμου και τα δύο εκ των οποίων θα είναι εύκολα επιλύσιμα σε αρκετά μεγάλους κβαντικούς υπολογιστές, χρησιμοποιώντας τον αλγόριθμο του Shor [98].

Η χρήση δικτυωμάτων ακέραιων αριθμών για το σχεδιασμό κρυπτογραφικών αλγορίθμων και κρυπτοσυστημάτων παρουσιάστηκε και προτάθηκε για πρώτη φορά το 1996 από τους Ajtai–Dwork και αποτελεί ένα πολύ ενδιαφέρον πεδίο μελέτης και έρευνας. Το πιο σημαντικό χαρακτηριστικό που διαθέτουν οι κρυπταλγόριθμοι αυτού του είδους είναι η αντίσταση σε επιθέσεις από κβαντικούς υπολογιστές, ενώ αξιοσημείωτο θεωρείται και το ότι για την απόδειξη της ασφάλειας ενός τέτοιου κρυπτοσυστήματος απαιτείται μόνο η απόδειξη δυσκολίας της χειρότερης περίπτωσης κάποιων προβλημάτων σχετικών με δικτυώματα ακεραίων και έπειτα, από το πρωτοποριακό εύρημα του Ajtai [11] το 1996, προκύπτει και η δυσκολία της μέσης περίπτωσης, η οποία θεωρείται ιδιαίτερα επιθυμητή ιδιότητα για ασφαλή κρυπτοσυστήματα. Το γεγονός αυτό δίνει σημαντικό πλεονέκτημα στην κρυπτογραφία αυτού του είδους έναντι άλλων ειδών κρυπτογραφίας, επίσης κβαντικά ανθιστάμενων.

Τα δύο χαρακτηριστικά που αναφέρθηκαν παραπάνω καθιστούν την κρυπτογραφία που βασίζεται σε δικτυώματα ένα ζωτικής σημασίας τμήμα της μετα–κβαντικής κρυπτογραφίας, η οποία ασχολείται με την έρευνα για κρυπτογραφικά εργαλεία, συνήθως κρυπτοσυστήματα δημοσίου κλειδιού, που δεν είναι αποτελεσματικά εύθραυστα εάν χρησιμοποιηθούν κβαντικοί υπολογιστές. Η κρυπτογραφία με χρήση δικτυωμάτων αποτελεί, δηλαδή, μία πολύ αξιόλογη πρόταση για προστασία των ευαίσθητων, προσωπικών μας δεδομένων από επιθέσεις με κβαντικούς υπολογιστές.

1.2 Σκοπός – Στόχοι

Σκοπός της παρούσης διπλωματικής εργασίας είναι η όσο το δυνατόν πληρέστερη και πιο κατανοητή παρουσίαση των δικτυωμάτων ακέραιων αριθμών ως στοιχείων της Αλγεβρικής Θεωρίας Αριθμών και η επεξήγηση της χρήσης τους στην κρυπτογραφία δημοσίου κλειδιού της σύγχρονης εποχής.

Στους επιμέρους στόχους της εργασίας συγκαταλέγονται:

- ✓ Η εξοικείωση του αναγνώστη με βασικές έννοιες της θεωρίας δικτυώματος.
- ✓ Η παρουσίαση και επεξήγηση κάποιων δυσεπίλυτων –υπολογιστικά– προβλημάτων που προκύπτουν από τη χρήση των δικτυωμάτων.
- ✓ Η εισαγωγή στη θεωρία αναγωγής της βάσης ενός δικτυώματος και η αναλυτική παράθεση των πιο σημαντικών αλγορίθμων αναγωγής της βάσης.
- ✓ Η περιγραφή (δημιουργία κλειδιών – κρυπτογράφηση – αποκρυπτογράφηση) των πιο γνωστών κρυπτοσυστημάτων που χρησιμοποιούν δικτυώματα ακεραίων.
- ✓ Η αναφορά σε συναρτήσεις διασποράς και ψηφιακές υπογραφές αυτού του είδους.
- ✓ Η καταγραφή των ανοιχτών ζητημάτων – προβλημάτων που υπάρχουν σε αυτήν την ερευνητική περιοχή και, τέλος,
- ✓ Η εξαγωγή κάποιων γενικών συμπερασμάτων όσον αφορά τη χρήση δικτυωμάτων ακέραιων αριθμών για κρυπτογραφικούς σκοπούς.

Για την κατανόηση του αντικειμένου της παρούσης εργασίας, απαιτούνται κάποιες βασικές γνώσεις Αφηρημένης Άλγεβρας και Αλγεβρικής Θεωρίας Αριθμών, οι οποίες παρατίθενται όσο το δυνατόν πιο σύντομα στο δεύτερο κεφάλαιο της εργασίας.

Η εργασία αυτή αποτελεί εισαγωγή στο είδος της κρυπτογραφίας που βασίζεται στη χρήση δικτυωμάτων ακέραιων αριθμών και ως τέτοια, παρουσιάζει το απαιτούμενο

μαθηματικό υπόβαθρο, τους πιο γνωστούς αλγορίθμους, τα πιο ευρέως αποδεκτά κρυπτοσυστήματα αυτού του είδους με τα υποκείμενα μαθηματικά τους προβλήματα, τις συναρτήσεις διασποράς και τις ψηφιακές υπογραφές, οι οποίες χρησιμοποιούν δικτυώματα ακέραιων αριθμών. Έτσι, πιο πρόσφατα σχετικά με την κρυπτογραφία αυτού του είδους αντικείμενα, όπως το πρόβλημα της μάθησης με σφάλματα (Learning with Errors – LWE) του Oded Regev [73] που διατυπώθηκε το 2005, το πρόβλημα της μικρής ακέραιας λύσης (Short Integer Solution – SIS) [11], το σχήμα πλήρως ομομορφικής κρυπτογράφησης (Fully Homomorphic Encryption – FHE) του Craig Gentry [28] που διατυπώθηκε το 2009, κ.ά., απλά αναφέρονται εδώ και δε λαμβάνουν περαιτέρω μελέτη.

1.3 Συνεισφορά

Η παρούσα διπλωματική εργασία στοχεύει να αποτελέσει ένα εισαγωγικό εγχειρίδιο της κρυπτογραφίας που βασίζεται σε δικτυώματα ακέραιων αριθμών. Κατά τη συγγραφή της έγινε συστηματική προσπάθεια να παρουσιαστούν όλα τα δυσεπίλυτα –υπολογιστικά– προβλήματα που ανακύπτουν από τη χρήση των δικτυωμάτων και τα οποία παρουσιάζουν κρυπτογραφικό ενδιαφέρον και να συγκεντρωθούν οι περισσότεροι αλγόριθμοι αναγωγής της βάσης, είτε προσεγγιστικοί, είτε ακριβείς, καθώς και κάποιες παραλλαγές τους.

Παρόλο που η εργασία αυτή αποτελεί εισαγωγή στην κρυπτογραφία που βασίζεται σε δικτυώματα ακεραίων, έγινε εκτενής έρευνα στο εν λόγω πεδίο, προκειμένου να γίνει κάποια αναφορά και στις μεταγενέστερες του NTRU προσπάθειες σχεδιασμού και υλοποίησης κρυπτοσυστημάτων αυτού του είδους. Επίσης, δεδομένου ότι το είδος αυτό έχει αναδυθεί σχετικά πρόσφατα και έχει πολλά ακόμα να γίνουν, δόθηκε ιδιαίτερη σημασία και στις τρέχουσες ερευνητικές τάσεις όσον αφορά τα προβλήματα, τις τεχνικές και τις κρυπτογραφικές δομές που διαρκώς γεννά και χρησιμοποιεί η κρυπτογραφία, η βασισμένη σε δικτυώματα. Έτσι, ευελπιστούμε η εργασία αυτή να παρέχει ταυτόχρονα την εύκολη εξοικείωση με το αντικείμενο, αλλά και να αποτελέσει κίνητρο και εφαλτήριο για περαιτέρω ενασχόληση και μελέτη.

1.4 Βασική Ορολογία

Αναγωγή βάσης δικτυώματος (Lattice base reduction)

Διαδικασία εύρεσης μίας βάσης σε δικτύωμα ακεραίων, η οποία να αποτελείται από μικρά, σχεδόν ορθογώνια διανύσματα (δεδομένης μίας αρχικής βάσης ως είσοδο).

Αποδείξιμη ασφάλεια (Proved security)

Απόδειξη ισοδυναμίας του μαθηματικού μοντέλου του κρυπτοσυστήματος με κάποιο πολύ γνωστό δύσκολο στην επίλυσή του πρόβλημα (από τη θεωρία αριθμών). Χαρακτηριστικό παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων.

Γεωμετρία αριθμών (Geometry of numbers)

Κλάδος των Μαθηματικών που ασχολείται με την επίλυση προβλημάτων της Θεωρίας Αριθμών (και όχι μόνο) με γεωμετρικές μεθόδους.

Δικτύωμα ακέραιων αριθμών (Integer lattice)

Σύνολο όλων των ακέραιων γραμμικών συνδυασμών δύο γραμμικώς ανεξάρτητων διανυσμάτων ενός διανυσματικού χώρου.

Κβαντική κρυπτογραφία (Quantum cryptography)

Κλάδος της κρυπτογραφίας, ο οποίος αναφέρεται στη χρήση της κβαντομηχανικής για την εκτέλεση κρυπτογραφικών εργασιών ή την παραβίαση κρυπτογραφικών συστημάτων.

Κρυπταναλυτικές επιθέσεις (Cryptanalytic attacks)

Εχθρικές ενέργειες με στόχο την παραβίαση κάποιου κρυπτογραφικού συστήματος, δηλαδή ανάλογα με τις απαιτήσεις, η εύρεση του κλειδιού της κρυπτογράφησης, η εύρεση του μηνύματος ή ενός ισοδύναμου αλγορίθμου που θα συμβάλλει στην ανάγνωση του (κρυφού) μηνύματος.

Κρυπτογραφία δημοσίου κλειδιού (Public Key cryptography)

Μέθοδος κρυπτογράφησης στην οποία ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης

συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Ονομάζεται και ασύμμετρη κρυπτογράφηση.

Μετα–κβαντική κρυπτογραφία (Post–Quantum cryptography)

Κλάδος της κρυπτογραφίας, ο οποίος ασχολείται με την έρευνα για κρυπτογραφικά εργαλεία, συνήθως κρυπτοσυστήματα δημοσίου κλειδιού, που δεν είναι αποτελεσματικά εύθραυστα εάν χρησιμοποιηθούν κβαντικοί υπολογιστές.

Μονόδρομη συνάρτηση (One–way function)

Μαθηματική συνάρτηση η οποία είναι εύκολο να υπολογισθεί, αλλά πολύ δύσκολο να αντιστραφεί.

Συνάρτηση διασποράς (Hash function)

Μαθηματική συνάρτηση η οποία, έχοντας ως είσοδο μία αυθαίρετου μεγέθους ομάδα δεδομένων, δίνει έξοδο μία καθορισμένου μεγέθους στοιχειοσειρά (string), συνήθως έναν ακέραιο αριθμό, πολύ μικρότερη από την είσοδο.

Συνάρτηση κερκόπορτας (Trap–door function)

Μαθηματική συνάρτηση η οποία μας επιτρέπει να αντιστρέψουμε μία συνάρτηση μίας κατεύθυνσης (one-way function).

Ψηφιακή υπογραφή (Digital signature)

Μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου.

Random Oracle (Τυχαίο Μαντείο)

Τυχαία μαθηματική συνάρτηση η οποία απεικονίζει κάθε πιθανό ερώτημα σε μία σταθερού μήκους τυχαία απόκριση από το πεδίο τιμών.

1.5 Διάρθρωση της μελέτης

Στο **πρώτο κεφάλαιο** αυτής της εργασίας, την Εισαγωγή, παρουσιάζεται το ιδιαίτερα ενδιαφέρον γνωστικό πεδίο της κρυπτογραφίας, οι τομείς στους οποίους αυτή χρησιμοποιείται και η σπουδαιότητά της.

Το **δεύτερο κεφάλαιο** αυτής της εργασίας, το Θεωρητικό Υπόβαθρο, διακρίνεται σε δυο μεγάλες υποενότητες: τις Μαθηματικές Έννοιες και τη Βιβλιογραφική Επισκόπηση. Στην πρώτη υποενότητα, παρατίθεται το απαραίτητο μαθηματικό υπόβαθρο (Ομάδες, Πεπερασμένα σώματα, Δακτύλιοι $\mathbb{Z}_p$ και $\mathbb{Z}_n$, Πράξεις με υπόλοιπα), ώστε να είναι σε θέση ο αναγνώστης να κατανοήσει τα όσα παρουσιάζονται στα επόμενα κεφάλαια. Στη δεύτερη υποενότητα, παρατίθενται μία όσο το δυνατόν πληρέστερη βιβλιογραφική ανασκόπηση, ώστε να αποκτήσει ο αναγνώστης μία σφαιρική αντίληψη για το εν λόγω αντικείμενο.

Στο **τρίτο κεφάλαιο** αυτής της εργασίας, την Κρυπτογραφία Βασισμένη σε Δικτυώματα Ακεραίων, γίνεται λόγος για τα δυσεπίλυτα –υπολογιστικά– προβλήματα που ανακύπτουν από τη χρήση δικτυωμάτων ακεραίων και παρουσιάζονται οι σημαντικότεροι αλγόριθμοι αναγωγής της βάσης ενός δικτυώματος.

Στο **τέταρτο κεφάλαιο** αυτής της εργασίας, τα Κρυπτοσυστήματα Βασισμένα σε Δικτυώματα Ακεραίων, παρουσιάζονται οι διαδικασίες δημιουργίας των κλειδιών, κρυπτογράφησης και αποκρυπτογράφησης στα πιο σημαντικά κρυπτοσυστήματα που έχουν υλοποιηθεί με βάση αυτήν την τεχνική.

Στο **πέμπτο κεφάλαιο** αυτής της εργασίας, τις Συναρτήσεις Διασποράς και Ψηφιακές Υπογραφές Βασισμένες σε Δικτυώματα Ακεραίων, περιγράφεται η συνάρτηση διασποράς LASH–x και η κρυπτανάλυσή της. Ακόμη, παρουσιάζονται οι συναρτήσεις SWIFFT και SWIFFTX που βασίζονται σε γρήγορους μετασχηματισμούς Fourier. Επίσης, παρουσιάζονται και επεξηγούνται τα δύο πιο βασικά σχήματα ψηφιακών υπογραφών που κάνουν χρήση δικτυωμάτων ακέραιων αριθμών (GGH και NTRUSign).

Στο **έκτο κεφάλαιο** αυτής της εργασίας αναφέρονται τα ανοιχτά προβλήματα που υπάρχουν ακόμη σε αυτό το πεδίο, τα οποία καθορίζουν και την κατεύθυνση της μελλοντικής έρευνας. Επίσης, καταγράφονται τα συμπεράσματα που συνήχθησαν από τη μελέτη αυτού του αντικειμένου.

Η παρούσα εργασία ολοκληρώνεται με το Παράρτημα και τις Βιβλιογραφικές Αναφορές.

Κεφάλαιο 2
Θεωρητικό Υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζονται αρχικά όλες οι προαπαιτούμενες μαθηματικές γνώσεις που χρειάζεται να έχει κάποιος για να κατανοήσει το αντικείμενο της κρυπτογραφίας που βασίζεται σε δικτυώματα ακεραίων. Στο υπόλοιπο τμήμα του κεφαλαίου παρατίθενται μία βιβλιογραφική επισκόπηση της κρυπτογραφίας αυτού του είδους.

2.1 Μαθηματικές Έννοιες

Η μοδιακή αριθμητική (modular arithmetic) ή αριθμητική των υπολοίπων είναι απαραίτητη γνώση πριν από οποιαδήποτε άλλη αναφορά στο αντικείμενο της κρυπτογραφίας γενικότερα. Έχει εφαρμοσθεί σε κρυπταλγόριθμους που βασίζονται τόσο στη δυσκολία της παραγοντοποίησης μεγάλων ακεραίων (π.χ. RSA, κ.ά.), όσο και στη δυσκολία της εύρεσης του διακριτού λογάριθμου μίας κυκλικής ομάδας της μορφής $(\mathbb{Z}_p)^x$, (π.χ. ElGamal, κ.ά.), αλλά και στη δυσκολία εύρεσης του διακριτού λογάριθμου σε μία ελλειπτική καμπύλη.

Η ιδιότυπη αυτή αριθμητική είναι ιδιαίτερα σημαντική, καθώς συμβάλλει στο να παραμείνουν μικροί οι αριθμοί στους υπολογισμούς μας, πράγμα το οποίο διευκολύνει τόσο την επεξεργασία τους, δηλαδή την εκτέλεση αριθμητικών πράξεων με αυτούς, όσο και την αποθήκευσή τους. Στη μοδιακή αριθμητική αναφερόμαστε στο πρώτο τμήμα αυτής της ενότητας.

Στο δεύτερο τμήμα, παραθέτουμε κάποιες βασικές γνώσεις αφηρημένης άλγεβρας. Αφηρημένη Άλγεβρα (επίσης, μοντέρνα ή σύγχρονη) είναι μία κοινή ονομασία για την υποπεριοχή της άλγεβρας που μελετά αλγεβρικές δομές, όπως ομάδες, δακτυλίους, σώματα, διανυσματικούς χώρους, modules και άλγεβρες. Ο όρος «αφηρημένη άλγεβρα» επινοήθηκε στα τέλη του 20ου αιώνα για τη διάκριση αυτού του τομέα από τα άλλα μέρη της άλγεβρας.

Ολοκληρώνουμε την ενότητα με το μαθηματικό υπόβαθρο παρουσιάζοντας την έννοια του δικτυώματος ακέραιων αριθμών και άλλα βασικά στοιχεία της θεωρίας δικτυώματος.

2.1.1 Μοδιακή Αριθμητική

Η μοδιακή αριθμητική είναι ένα σύστημα αριθμητικής ακεραίων, όπου οι αριθμοί περιτυλίσσονται γύρω από μία ορισμένη τιμή, το μοδιακό (modulus) ή υπόλοιπο ή πρότυπο. Με απλά λόγια, οι αριθμητικές πράξεις (πρόσθεση – πολλαπλασιασμός) μεταξύ θετικών ακεραίων παράγουν αποτέλεσμα μικρότερο από τους ακέραιους αυτούς.

Έτσι, εάν θέλουμε να υπολογίσουμε με τι ισούται ένας συγκεκριμένος αριθμός m modulo έναν αριθμό n, εκτελούμε ακέραια διαίρεση και το αποτέλεσμά μας είναι το υπόλοιπο της διαίρεσης. Με τον ίδιο τρόπο, εκτελούμε αριθμητικές πράξεις με περισσότερους αριθμούς modulo έναν αριθμό n και το αποτέλεσμά τους θα παίρνει παντα τιμές από το σύνολο $\{0, 1, \dots, n-1\}$. Στη συνέχεια ακολουθούν κάποια παραδείγματα, ώστε να γίνει πλήρως κατανοητή η αριθμητική αυτή.

- $137 \equiv 5\ (mod\ 11)$
- $137 + 43 \equiv 4\ (mod\ 11)$
- $13 \times 7 \equiv 3\ (mod\ 11)$
- $13 \times 11 \equiv 0\ (mod\ 11)$
- $13 \times 5 \equiv 10\ (mod\ 11)$
- $13 \times 11 \equiv 3\ (mod\ 5)$

Η σχέση "$\equiv (mod\ n)$" ονομάζεται ισοτιμία (congruence). Γενικά, η ισοτιμία $a \equiv b\ (mod\ n)$ δηλώνει ότι το a και το b αφήνουν το ίδιο υπόλοιπο, όταν διαιρούνται με το n. Ισχύουν τα εξής:

- $a\ (mod\ n) + b\ (mod\ n) \equiv (\alpha + b)\ (mod\ n)$
- $a\ (mod\ n) \times b\ (mod\ n) \equiv (\alpha \times b)\ (mod\ n)$

Εάν $a \times b \equiv 1\ (mod\ n)$, ο b είναι ένας αντίστροφος για το $a\ (mod\ n)$. Παραδείγματος χάριν, ο αντίστροφος του 19 $(mod\ 17)$ είναι το 9. Αυτό ισχύει επειδή: $9 \times 19 \equiv 1\ (mod\ 17)$. Ο αντίστροφος ενός αριθμού συμβολίζεται με τη δύναμη του αριθμού εις την -1 , δηλαδή $19^{-1} \equiv 9\ (mod\ 17)$. Μπορεί να χρησιμοποιηθεί ο Ευκλείδειος αλγόριθμος για να ελέγξει εάν οι αριθμοί α και n έχουν κοινούς παράγοντες και, σε περίπτωση που δεν έχουν, να υπολογίσει τον αντίστροφο του $\alpha\ (mod\ n)$.

Παρατηρούμε ότι, όλα τα αποτελέσματα των παραπάνω πράξεων κυμαίνονται από 0 μέχρι 10, δηλαδή $n-1$, αφού δουλεύουμε στο μοδιακό 11. Επίσης, από το τελευταίο παράδειγμα συμπεραίνουμε ότι, εάν αλλάξουμε μοδιακό, αλλάζει και το αποτέλεσμα της πράξης, ακόμα κι αν οι αριθμοί (τελεστέοι) παραμένουν ίδιοι. Ακόμη, εάν το αποτέλεσμα της πράξης είναι μικρότερο από το μοδιακό το οποίο επιλέγουμε κάθε φορά, αυτό παραμένει ως έχει, δηλαδή ίσο με το αποτέλεσμα της κοινής αριθμητικής:

- $3+7 \equiv 10\ (mod\ 11)$
- $3 \times 2 \equiv 6\ (mod\ 11)$

Η μοντέρνα προσέγγιση της μοδιακής αριθμητικής αναπτύχθηκε από τον Carl Friedrich Gauss στο βιβλίο του Disquisitiones Arithmeticae, που δημοσιεύθηκε το 1801. Αποκαλείται και ωρολογιακή αριθμητική, διότι ασχολούμαστε με μία πεπερασμένη ομάδα αριθμών με κυκλική διάταξη, όπως ακριβώς είναι και οι αριθμοί σε ένα ρολόι.

2.1.2 Βασικές Αλγεβρικές Δομές

Όπως προαναφέρθηκε, οι αλγεβρικές δομές περιλαμβάνουν τις ομάδες, τους δακτυλίους, τα σώματα, τους διανυσματικούς χώρους, τα modules, καθώς και διάφορες άλγεβρες. Στο πλαίσιο αυτής της εργασίας, αναγκαία είναι η παρουσίαση βασικών μόνο αλγεβρικών δομών, οι οποίες περιλαμβάνουν τις τέσσερεις πρώτες δομές που αναφέρθηκαν παραπάνω. Αναφερόμαστε, επίσης και στην έννοια των πολυωνυμικών δακτυλίων, η γνώση των οποίων χρειάζεται στη συνέχεια.

Ομάδα (μεταθέσεων) – Group

Ο Galois πρώτος χρησιμοποίησε τον όρο ομάδα: μία συλλογή από μεταθέσεις που το γινόμενο τους ανήκει σε αυτή τη συλλογή. Ο Cayley το 1854 έδωσε τον πρώτο αφηρημένο ορισμό ομάδας.

Ορισμός 2.1.2.1 Ομάδα (G, +) ή (G, *) είναι ένα σύνολο *G* με μια δυαδική πράξη + ή * στο *G το οποίο* ικανοποιεί τα ακόλουθα 3 αξιώματα:

- Η πράξη της ομάδας είναι ***προσεταιριστική***, δηλαδή:

  $\alpha + (b + c) = (\alpha + b) + c$ για κάθε $a, b, c \in G$. (αντίστοιχα για *)

- Υπάρχει ένα στοιχείο 0 ή 1 $\in G$, που λέγεται ***ουδέτερο στοιχείο***, τέτοιο ώστε

  $a + 0 = 0 + a = a$ για κάθε $a \in G$ *(G προσθετική)* ή

$a * 1 = 1 * a = a$ για κάθε $a \in G$. *(G πολλαπλασιαστική*

- Για κάθε $a \in G$ υπάρχει ένα στοιχείο $-\alpha \in G$ *(G προσθετική)* ή

  α^{-1} *(G πολλαπλασιαστική)* που λέγεται ***αντίστροφο*** του a, τέτοιο ώστε

  $a + (-a) = (-a) + \alpha = 0$ ή $a * \alpha^{-1} = \alpha^{-1} * \alpha = 1$.

Σε γενικές γραμμές, ομάδα είναι η μικρότερη αλγεβρική δομή, μέσα στην οποία μπορούμε να λύσουμε μια οποιαδήποτε εξίσωση πρώτου βαθμού.

Δακτύλιος – Ring

Από ιστορικής απόψεως, ο πρώτος δακτύλιος που μελετήθηκε ήταν ο δακτύλιος $\mathbb{Z}$ των ακεραίων. Ο όρος «δακτύλιος» χρησιμοποιήθηκε για πρώτη φορά από τον Hilbert το 1897, στο έργο του «Zahlbericht» («έκθεση αριθμών»), το οποίο αποτέλεσε το κύριο σύγγραμμα της αλγεβρικής θεωρίας αριθμών για τουλάχιστον τριάντα χρόνια από την εμφάνισή του.

Στη σύγχρονη αλγεβρική θεωρία αριθμών, δακτύλιος ονομάζεται η αλγεβρική δομή που αποτελείται από ένα σύνολο R με δύο διμελείς πράξεις, συμβολικά $+$ (πρόσθεση) και $\times$ (πολλαπλασιασμός) στο R, έτσι ώστε:

- (R, +) είναι μια αβελιανή ομάδα με **ουδέτερο στοιχείο** που συμβολίζεται με 0.
- Η πράξη $\times$ είναι **προσεταιριστική**. Δηλαδή:

  $a \times (b \times c) = (a \times b) \times c$ για κάθε $a, b, c \in R$.
- Υπάρχει **πολλαπλασιαστικό ουδέτερο στοιχείο**, που συμβολίζεται με το 1,

  με $1 \neq 0$, τέτοιο ώστε $1 \times a = a \times 1 = a$ για κάθε $a \in R$.
- Η πράξη $\times$ είναι **επιμεριστική** ως προς την +. Δηλαδή:

  $a \times (b + c) = (a \times b) + (a \times c)$ και

  $(b + c) \times a = (b \times a) + (c \times a)$ για κάθε $a, b, c \in R$.

Ορισμός 2.1.2.2 Έστω R ένας δακτύλιος και $m \in R^*$, όπου $R^* = (R \backslash \{0\})$

Τότε $a \equiv b \ (mod\ n) \Leftrightarrow n \mid a - b \Leftrightarrow a - b = n \cdot c,\ c \in R$

Πρόταση 2.1.2.1 Έστω R ένας δακτύλιος και $m \in R^*$.

$$\text{Εάν} \begin{cases} a_1 \equiv b_1 \ (mod\ n) \\ a_2 \equiv b_2 (mod\ n) \end{cases} \text{τότε} \begin{cases} a_1 + a_2 \equiv b_1 + b_2 (mod\ n) \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 (mod\ n) \end{cases}$$

Ορισμός 2.1.2.3 Έστω R ένας δακτύλιος και $m \in R^*$. Για το $\alpha \in R$ γράφουμε $[\alpha]$ ή $\bar{\alpha}$ για το σύνολο των $\alpha' \in R$, που είναι τέτοια, ώστε $\alpha' \equiv \alpha \ (mod\ n)$. Το σύνολο $[\alpha]$ λέγεται κλάση ισοτιμίας του α και συμβολίζουμε το σύνολο όλων των κλάσεων ισοτιμίας με $R/(n)$ ή R/nR ή R_n. Έτσι,

$$R/(n) = \{[\alpha] : \alpha \in R\}.$$

Προσθέτουμε και πολλαπλασιάζουμε κλάσεις ισοτιμίας χρησιμοποιώντας τους κανόνες: $[\alpha] + [b] = [\alpha + b]$ και $[\alpha] \cdot [b] = [\alpha \cdot b]$. Το $R/(n)$ ονομάζεται δακτύλιος πηλίκο (quotient ring) του R με το n. Οι δύο παραπάνω τύποι ορίζουν κανόνες πρόσθεσης και πολλαπλασιασμού στο σύνολο των κλάσεων ισοτιμίας που καθιστούν το $R/(n)$ δακτύλιο.

Σώμα (Field)

Ορισμός 2.1.2.4 Σώμα (αλγεβρικό) ονομάζεται ένας αντιμεταθετικός δακτύλιος διαίρεσης, δηλαδή ένας αντιμεταθετικός δακτύλιος του οποίου κάθε μη μηδενικό στοιχείο έχει πολλαπλασιαστικό αντίστροφο.

Παραδείγματα

- Το σώμα των πραγματικών αριθμών $\mathbb{R}$
- Το σώμα των ρητών αριθμών $\mathbb{Q}$
- Το σώμα των μιγαδικών αριθμών $\mathbb{C}$
- Σώματα της μορφής $a + b * \sqrt{2}$ (γενικά $a + b * \sqrt{x}$)

Στο σημείο αυτό να επισημάνουμε ότι το σύνολο των ακεραίων $\mathbb{Z}$ δεν αποτελεί σώμα, δηλαδή ο αντίστροφος ενός ακέραιου ως προς τον πολλαπλασιασμό δεν είναι απαραίτητα ακέραιος. Το μικρότερο σώμα που περιέχει τους ακέραιους είναι οι ρητοί αριθμοί. Οι ακέραιοι αριθμοί αποτελούν αντιμεταθετικό δακτύλιο ως προς την πρόσθεση και τον πολλαπλασιασμό. Το άθροισμα και το γινόμενο δυο ακεραίων είναι δηλαδή και αυτό ακέραιος. Ισχύουν η αντιμεταθετική και η προσεταιριστική

ιδιότητα ως προς την πρόσθεση και τον πολλαπλασιασμό και ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.

Πολυωνυμικός Δακτύλιος (Polynomial Ring)

Ορισμός 2.1.2.5 Πολυωνυμικός ονομάζεται ο δακτύλιος που σχηματίζεται από το σύνολο των πολυωνύμων μίας η περισσοτέρων μεταβλητών με συντελεστές από τον ίδιο ή έναν άλλο δακτύλιο, ο οποίος συνηθέστερα αποτελεί ένα σώμα. Οι πολυωνυμικοί δακτύλιοι επηρέασαν μεγάλο μέρος των μαθηματικών.

Εάν R είναι ένας οποιοσδήποτε δακτύλιος, μπορούμε να δημιουργήσουμε ένα δακτύλιο πολυωνύμων με συντελεστές παρμένους από το R. Ο δακτύλιος αυτός συμβολίζεται με $R[x] = \{ a_0 + a_1x + a_2x^2 + \dots\dots + a_nx^n : n \geq 0$ και $a_0, a_1, a_2, \dots\dots, a_n \in \mathrm{R} \}$. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι δακτύλιοι πολυωνύμων, στους οποίους ο δακτύλιος R είναι ένα σώμα και μάλιστα ένα πεπερασμένο σώμα, δηλαδή:

$$F_p\ (= \mathbb{Z}/(p)) = \{0, 1, \dots\dots, \mathrm{p} - 1\}$$

Πρόταση 2.1.2.2 Έστω F ένα σώμα και $\alpha, \mathrm{m} \in F[x]$ δύο πολυώνυμα με $\mathrm{m} \neq 0$. Τότε η $[\alpha]$ είναι μία μονάδα (αντιστρέψιμο στοιχείο) του δακτυλίου πηλίκο $F[x]/(m)$, εάν και μόνο εάν $\gcd(a, \mathrm{m}) = 1$.

Πόρισμα 2.1.2.1 Έστω F ένα σώμα και $\mathrm{m} \in F[x]$ ένα ανάγωγο πολυώνυμο. Τότε ο δακτύλιος πηλίκο $F[x]/(m)$ είναι σώμα, δηλαδή κάθε μη μηδενικό στοιχείο του $F[x]/(m)$ έχει ένα πολλαπλασιαστικό αντίστροφο.

Επίσης, εάν $F = F_p$ είναι ένα πεπερασμένο σώμα και το m είναι βαθμού $d > 1$, τότε το $F_p[x]/(m)$ είναι ένα σώμα με p^d στοιχεία.

Διανυσματικός Χώρος (Vector Space)

Ορισμός 2.1.2.6 Διανυσματικός χώρος V επί ενός σώματος F είναι μια αβελιανή ομάδα $(V, +)$, μαζί με μια πράξη πολλαπλασιασμού : $F \times V \rightarrow V$ τέτοια, ώστε για κάθε $a, b \in F$ και $u, w \in V$, να ικανοποιούνται τα ακόλουθα αξιώματα:

- $a(u + w) = au + aw$.
- $(a + b)u = au + bu$.
- $(ab)u = a(bu)$.

- $1u = u$.

Τα στοιχεία του διανυσματικού χώρου V καλούνται ***διανύσματα***, ενώ τα στοιχεία του σώματος F καλούνται ***βαθμωτά***. Τέλος, η πράξη ομάδας + καλείται ***διανυσματική πρόσθεση***, ενώ η πράξη πολλαπλασιασμού καλείται ***βαθμωτός πολλαπλασιασμός***.

Διανυσματικοί Υπόχωροι (Vector Subspaces)

Ορισμός 2.1.2.7 Έστω V ένας διανυσματικός χώρος επί ενός σώματος F. Ένας υπόχωρος του V είναι μία προσθετική υποομάδα U της V η οποία είναι κλειστή ως προς τον βαθμωτό πολλαπλασιασμό, δηλ., au ϵ U για κάθε a ϵ F και u ϵ U.

Ένας υπόχωρος ενός διανυσματικού χώρου είναι επίσης ένας διανυσματικός χώρος. Με άλλα λόγια, εάν W μη κενό υποσύνολο ενός δ.χ. V, εφοδιασμένο με τις πράξεις του V είναι και αυτό δ.χ., τότε λέμε ότι είναι διανυσματικός υπόχωρος του V.

Γραμμικός Συνδυασμός (Linear Combination)

Ορισμός 2.1.2.8 Έστω S = $\{u_1 , u_2 ,\ldots, u_n\}$ ένα πεπερασμένο υποσύνολο ενός διανυσματικού χώρου V επί ενός σώματος F. Γραμμικός συνδυασμός του S είναι μια έκφραση της μορφής $a_1u_1 + a_2u_2 + \ldots + a_nu_n$, όπου κάθε $a_i \epsilon$ F.

Εάν $a_1 + a_2 + \ldots + a_n = 1$, τότε το παραπάνω διάνυσμα λέγεται **ομοπαραλληλικός συνδυασμός** (affine combination) των $u_1, u_2, \ldots, u_n$.

Γραμμική Ανεξαρτησία (Linear Independence)

Ορισμός 2.1.2.9 Το σύνολο S είναι **γραμμικά εξαρτημένο** επί του F εάν υπάρχουν βαθμωτά $a_1, a_2, \ldots, a_n$, όχι όλα μηδέν, τέτοια ώστε $a_1u_1 + a_2u_2 + \ldots + a_nu_n = 0$. Εάν δεν υπάρχουν τέτοια βαθμωτά, τότε το S είναι **γραμμικά ανεξάρτητο** επί του F.

Βάση και Διάσταση Διανυσματικού Χώρου (Vector Space Basis – Dimension)

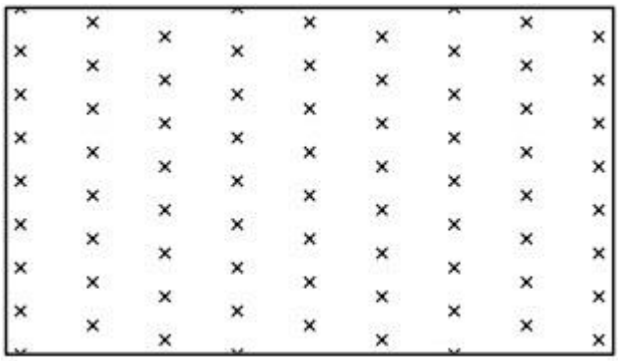
Έστω V ένας διανυσματικός χώρος. Εάν ο V έχει ένα πεπερασμένο σύνολο που τον παράγει, τότε έχει μια *βάση*. Εάν ο V έχει μια βάση, τότε στην πραγματικότητα όλες οι βάσεις έχουν το ίδιο πλήθος στοιχείων.

Ορισμός 2.1.2.10 Βάση (B) ενός διανυσματικού χώρου V είναι ένα υποσύνολό του, $B \subseteq V$, γραμμικά ανεξάρτητο, το οποίο παράγει (ολόκληρο) τον V.

Ορισμός 2.1.2.11 Διάσταση $(dimV)$ ενός δ.χ. V ονομάζεται το πλήθος στοιχείων μιας οποιασδήποτε βάσης του.

2.1.3 Δικτυώματα Ακεραίων (Integer Lattices)

Με τον όρο «δικτύωμα ακεραίων» αναφερόμαστε σε ένα σύνολο σημείων σε χώρο n–διαστάσεων με περιοδική δομή, όπως αυτή που απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 2.1.3.1 Δικτύωμα στον $\mathbb{R}^2$

Από ιστορικής απόψεως, τα δικτυώματα άρχισαν να διερευνούνται γύρω στα τέλη του 18ου αιώνα από διακεκριμένους μαθηματικούς όπως οι Lagrange, Gauss, και αργότερα από τον Minkowski. Η θεωρία δικτυώματος (lattice theory) είναι η μελέτη των συνόλων των αντικειμένων που είναι γνωστά ως δικτυώματα. Είναι αποτέλεσμα της μελέτης αλγεβρών Boole και παρέχει ένα πλαίσιο για την ενοποίηση της μελέτης των κατηγοριών (categories) ή των διατεταγμένων συνόλων (ordered sets) στα μαθηματικά. Η μελέτη της θεωρίας δικτυώματος γνώρισε μεγάλη ώθηση από μία σειρά άρθρων και ένα επακόλουθο βιβλίο–ορόσημο [2] που γράφτηκε από τον G.Birkhoff το 1967 και εκδόθηκε το 1979.

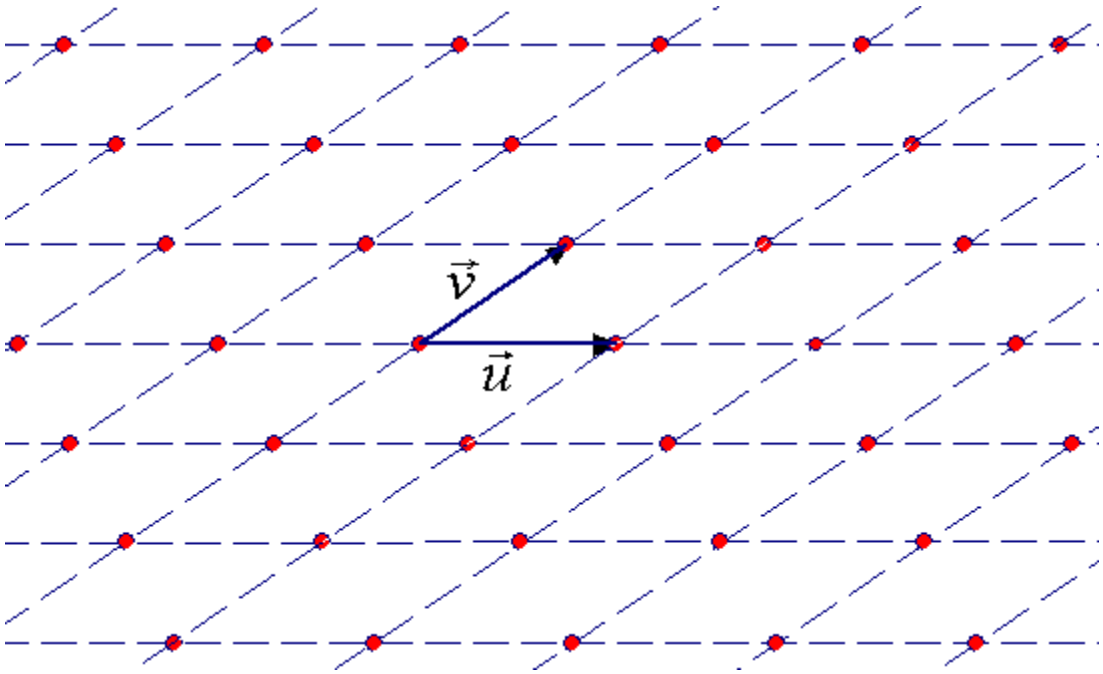
Στη σύγχρονη εποχή, τα δικτυώματα αποτελούν αντικείμενο ενεργού έρευνας στην επιστήμη των υπολογιστών. Χρησιμοποιούνται ως ένα αλγοριθμικό εργαλείο για την επίλυση μιας ευρείας ποικιλίας προβλημάτων. Έχουν, επίσης, πολλές εφαρμογές στην κρυπτογραφία και στην κρυπτανάλυση και από τη σκοπιά της υπολογιστικής πολυπλοκότητας διαθέτουν κάποιες μοναδικές ιδιότητες.

Η θεωρητική μελέτη των δικτυωμάτων (και ειδικότερα η σύνδεσή τους με τα κυρτά σώματα) συχνά καλείται γεωμετρία αριθμών, όνομα που αποδόθηκε σε αυτήν από τον Hermann Minkowski το 1910 στο ομότιτλο βιβλίο του. Η γεωμετρία των αριθμών αποτελεί ένα σημαντικό τμήμα της θεωρίας αριθμών, το οποίο έχει τις ρίζες του σε ιστορικά προβλήματα, όπως είναι οι γενικεύσεις σε υψηλές διαστάσεις του Ευκλείδειου

αλγόριθμου για τον υπολογισμό του Μ.Κ.Δ. δύο ακεραίων και η διαδικασία της διευθέτησης μη επικαλυπτόμενων σφαιρών μέσα σε ένα γραμμικό χώρο που τις περιέχει, η οποία είναι ευρέως γνωστή ως *sphere packing* [60].

2.1.3.1 Βασικοί Ορισμοί

Όπως έχουμε ήδη αναφέρει, μπορούμε να πούμε ότι σε γενικές γραμμές, δικτύωμα ακέραιων αριθμών είναι ένα σύνολο σημείων σε n–διάστατο χώρο με περιοδική δομή. Πιο συγκεκριμένα, δικτύωμα είναι μια διακριτή προσθετική υποομάδα του $\mathbb{R}^{\boldsymbol{n}}$, δηλαδή ένα υποσύνολο του $\mathbb{R}^{\boldsymbol{n}}$, για το οποίο ισχύει η ιδιότητα της κλειστότητας ως προς την πρόσθεση και την αφαίρεση. Στην εικόνα που ακολουθεί, αναπαρίσταται γεωμετρικά ένα δικτύωμα ακεραίων βάσει δύο διανυσμάτων $\vec{u}$ και $\vec{v}$.



Εικόνα 2.1.3.1.1 Γεωμετρική απεικόνιση δικτυώματος στον $\mathbb{R}^{\boldsymbol{2}}$

Έστω $x_1, x_2, \ldots, x_n$ είναι μια βάση του $\mathbb{R}^{\boldsymbol{n}}$ και $n \geq 1$. Τότε, **δικτύωμα L** διάστασης n και βάσης $x_1, x_2, \ldots, x_n$ είναι το σύνολο όλων των γραμμικών συνδυασμών των διανυσμάτων της βάσης με ακέραιους συντελεστές, δηλαδή:

$$L = \mathbb{Z}\, x_1 + \mathbb{Z}\, x_2 + \ldots\ldots \mathbb{Z}\, x_n = \left\{\sum_{i=1}^{n} a_i x_i \,|a_{1,}\, a_{2,}\, \ldots, a_n \in \mathbb{Z}\right\}$$

Ορισμός 2.1.3.1.1 Δικτύωμα (Lattice).

Δοθέντων n γραμμικά ανεξάρτητων διανυσμάτων $b_1, b_2, \dots, b_n \in \mathbb{R}^m$, το δικτύωμα που παράγεται από αυτά ορίζεται ως $L\ (b_1, b_2, \dots, b_n) = \{\sum x_i\, b_i \mid x_i \in \mathbb{Z}\}$.

Αναφερόμαστε στην ακολουθία $b_1, b_2, \dots, b_n$ ως βάση (basis) του δικτυώματος. Η βάση ενός δικτυώματος δεν είναι μοναδική. Ισοδύναμα, εάν ορίσουμε το B ως έναν m×n πίνακα του οποίου οι στήλες είναι $b_1, b_2, \dots, b_n$, τότε το δικτύωμα που δημιουργείται από τον B είναι $L\ (B) = L\ (b_1, b_2, \dots, b_n) = \{B_x \mid x \in \mathbb{Z}^n\}$.

Λέμε ότι ο βαθμός του δικτυώματος είναι n και η διάστασή του είναι m. Εάν ισχύει ότι n = m, το δικτύωμα ονομάζεται πλήρες δικτύωμα.

Ορισμός 2.1.3.1.2 Δικτύωμα παραγόμενο από άλλο δικτύωμα (Lattice span).

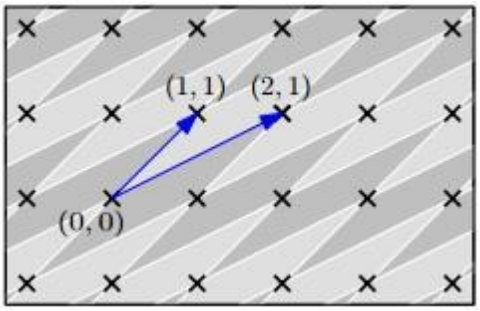
Εάν ένα δικτύωμα $L\ (B)$ είναι ο γραμμικός χώρος που παράγεται από τα διανύσματα ενός δικτυώματος , L , γράφουμε: $span\left(L(B)\right) = span(B) = \left\{B_y \mid y \in \mathbb{R}^n\right\}$.

Εάν το B είναι μία βάση ενός δικτυώματος $L(B)$, τότε είναι βάση και για το διανυσματικό χώρο $span(B)$, ενώ το αντίστροφο δεν ισχύει πάντα.

Ορισμός 2.1.3.1.3 Θεμελιώδες Παραλληλεπίπεδο (Fundamental Parallelepiped).

Για οποιαδήποτε βάση B ενός δικτυώματος $L(B)$ ορίζουμε $P(B) = \{B_x \mid x \in \mathbb{R}^n, \forall i: 0 \leq x_i < 1\}$.

Παραδείγματα θεμελιωδών παραλληλεπιπέδων παρουσιάζονται στις γκρι περιοχές του παρακάτω σχήματος.



Εικόνα 2.1.3.1.2 Θεμελιώδες Παραλληλεπίπεδο

Ορισμός 2.1.3.1.4 Μονομοδιακός Πίνακας (Unimodular Matrix).

Ένας μονομοδιακός (unimodular) πίνακας είναι ένας πίνακας, έστω $U \in \mathbb{Z}^{n\times n}$, με ορίζουσα ± 1. Για παράδειγμα, ο πίνακας $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ έχει ορίζουσα $+1$.

Λήμμα 2.1.3.1.1 Εάν ένας πίνακας, έστω U, έχει ορίζουσα ± 1, τότε και ο αντίστροφός του πίνακας, U^{-1}, θα έχει ορίζουσα ± 1.

Ορισμός 2.1.3.1.5 Ορίζουσα (Determinant).

Έστω ένα δικτύωμα $L(B)$ βαθμού n. Ορίζουμε την ορίζουσα του $L(B)$, που συμβολίζεται με $\det(L(B))$, ως το n–διάστατο όγκο του παραλληλεπιπέδου $P(B)$. Αυτό μπορεί να γραφεί συμβολικά, ως εξής: $\det\big(L(B)\big) \coloneqq \sqrt{\det(B^T B)}$.

Στην ειδική περίπτωση που το $L(B)$ είναι ένα πλήρες δικτύωμα, ο πίνακας B είναι ένας τετραγωνικός πίνακας και έχουμε $\det(L(B)) = |\det(B)|$. Η ορίζουσα ενός δικτυώματος είναι καλώς ορισμένη, με την έννοια ότι είναι ανεξάρτητη από την επιλογή της βάσης B του δικτυώματος. Επίσης, είναι αντιστρόφως ανάλογη της πυκνότητάς του, δηλαδή όσο μικρότερη είναι η ορίζουσα ενός δικτυώματος, τόσο πιο μεγάλη θα είναι η πυκνότητά του.

Ορισμός 2.1.3.1.6 Δυϊκό Δικτύωμα (Dual Lattice).

Το δυϊκό ενός δικτυώματος L είναι το σύνολο $\hat{L}$ όλων των διανυσμάτων $x \in span\ (L)$, έτσι ώστε το $\langle x, y\rangle$ να είναι ένας ακέραιος αριθμός για όλα τα $y \in (L)$.

Το δυϊκό δικτύωμα $\hat{L}$ ανήκει στον ίδιο διανυσματικό χώρο που ανήκει και το L, αλλά συνήθως δεν αποτελεί υποδικτύωμά του. Παραδείγματος χάριν, ακόμα και εάν το $L \subset \mathbb{Z}^n$ είναι ένα δικτύωμα ακεραίων, το δυϊκό του δικτύωμα θα περιέχει και μη ακέραια διανύσματα. Ο ορισμός του δυϊκού δικτυώματος ομοιάζει με τον ορισμό του δυϊκού για διανυσματικούς χώρους. Υπενθυμίζουμε ότι το δυϊκό ενός αφηρημένου διανυσματικού χώρου V ορίζεται ως το σύνολο των γραμμικών εξισώσεων $\phi : V \to \mathbb{R}$. Όταν $V \subseteq \mathbb{R}^n$, είναι συνηθισμένο να αναπαριστούμε τη συνάρτηση ϕ ως ένα διάνυσμα $v \in V$, τέτοιο ώστε $\phi(x) = \langle v, x\rangle$. Ο ορισμός του δυϊκού ενός δικτυώματος είναι ανάλογος με εκείνον για διανυσματικούς χώρους, αλλά με το $\mathbb{R}$ να αντικαθίστανται από

το $\mathbb{Z}$: Το δυϊκό ενός δικτυώματος L είναι το σύνολο των γραμμικών εξισώσεων $\phi : V \rightarrow \mathbb{Z}$, το οποίο αναπαρίσταται ως διανύσματα στο $span\ (L)$.

Ορισμός 2.1.3.1.7 Κυκλικό Δικτύωμα (Cyclic Lattice).

Σύμφωνα με τον D.Micciancio, κυκλικό ονομάζεται το δικτύωμα που είναι αναλλοίωτο από κυκλικές περιστροφές των συντεταγμένων.

Στα κύρια πλεονεκτήματα της χρήσης κυκλικών δικτυωμάτων συγκαταλέγονται η δυνατότητα για συνοπτικές αναπαραστάσεις, διότι ένα κυκλικό δικτύωμα μπορεί να αναπαριστά ένα n–διάστατο δικτύωμα με ένα και μόνο διάνυσμα, αλλά και η δυνατότητα κατασκευής μονόδρομων συναρτήσεων που βασίζονται στη δυσεπιλυσιμότητα χειρότερης περίπτωσης του SVP. Επίσης, ιδιαίτερα σημαντική είναι η αλγεβρική δομή των δικτυωμάτων αυτών, η οποία επιτρέπει γρήγορη αριθμητική (με χρήση του γρήγορου μετασχηματισμού Fourier–FFT), αλλά καθιστά δυνατή και την παραγωγή αποδείξεων. Τέλος, μεγάλο επίτευγμα της χρήσης κυκλικών δικτυωμάτων αποτελεί το κρυπτοσύστημα NTRU, το οποίο είναι μεν γρήγορο, στερείται δε των απαραίτητων αποδείξεων.

Τα ιδεώδη δικτυώματα μελετήθηκαν για πρώτη φορά στο πλαίσιο της κρυπτογραφίας από τους V.Lyubashevsky και D.Micciancio [50]. Τα δικτυώματα αυτά αποτελούν μία ειδική κατηγορία των γενικών δικτυωμάτων, αλλά και μία γενίκευση των κυκλικών δικτυωμάτων [54]. Η χρησιμότητά τους αποδίδεται στο γεγονός ότι πολύ αποτελεσματικές και πρακτικές συναρτήσεις διασποράς με αντίσταση στις συγκρούσεις, μπορούν να οικοδομηθούν βάσει της δυσεπιλυσιμότητας της εξεύρεσης ενός κατά προσέγγιση βραχύτερου διανύσματος σε τέτοια δικτυώματα. Σε γενικές γραμμές, τα ιδεώδη δικτυώματα είναι δικτυώματα που αντιστοιχούν στα ιδεώδη δακτυλίων της μορφής $\mathbb{Z}[x]/\langle f \rangle$ για κάποιο ανάγωγο πολυώνυμο f βαθμού n. Για λόγους απλότητας, θα επικεντρωθούμε μόνο σε δακτυλίους της μορφής $\mathbb{Z}[x]/\langle x^n + 1 \rangle$, καθώς έχει αποδειχθεί ότι αυτοί είναι οι πλέον χρήσιμοι δακτύλιοι για πρακτικές εφαρμογές.

Πριν προχωρήσουμε στον ορισμό του ιδεώδους δικτυώματος, θα πρέπει να ορίσουμε τις έννοιες «μονικό» πολυώνυμο (από τη θεωρία πολυωνύμων) και «ισομορφισμός» (από τη θεωρία ομάδων).

Ορισμός 2.1.3.1.8 Μονικό (monic) ονομάζεται το μονομεταβλητό (univariate) πολυώνυμο στο οποίο ο μεγαλύτερος συντελεστής (ο υψηλότερου βαθμού, μη μηδενικός συντελεστής) είναι ίσος με 1. Ως εκ τούτου, ένα μονικό πολυώνυμο έχει τη μορφή $x^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + c_0$. Με τον όρο «μονομεταβλητό» εννοούμε ότι το πολυώνυμο αποτελείται, εκτός από το σταθερό όρο, από δυνάμεις μίας μόνο μεταβλητής.

Ορισμός 2.1.3.1.9 Ισομορφισμός (isomorphism) δακτυλίων.

Ένας ισομορφισμός $\phi : R \to R'$ από έναν δακτύλιο R σε έναν δακτύλιο R' είναι ένας ομομορφισμός που είναι ένα–προς–ένα και επί του R'. Οι δακτύλιοι R και R' είναι τότε ισόμορφοι [4] .

Ορισμός 2.1.3.1.10 Ομομορφισμός (omomorphism) δακτυλίων.

Μία απεικόνιση $\phi : R \to R'$ ονομάζεται ομομορφισμός δακτυλίων $(R \; και \; R')$, εάν ισχύουν τα εξής:

1. $\phi\,(a + b) = \phi\,(a) \oplus \phi\,(b)$
2. $\phi\,(a \cdot b) = \phi\,(a) * \phi\,(b)$, για κάθε $a, b \in R$.

Εάν επιπλέον η φ είναι $1-1$ θα ονομάζεται *μονομορφισμός* δακτυλίων, ενώ εάν είναι $επί$ θα ονομάζεται *επιμορφισμός* δακτυλίων. Εάν τυχαίνει η φ να είναι $1-1$ και $επί$, τότε ονομάζεται, όπως προαναφέρθηκε, *ισομορφισμός* δακτυλίων.

Ορισμός 2.1.3.1.11 Ιδεώδες Δικτυώματος (Ideal Lattice).

Έστω $f \in \mathbb{Z}[x]$ είναι ένα μονικό πολυώνυμο βαθμού n και έστω ο δακτύλιος πηλίκο $\mathbb{Z}[x]/\langle f \rangle$. Χρησιμοποιώντας το καθιερωμένο σύνολο $\{(g \; mod \; f : g \in \mathbb{Z}[x])\}$ και ταυτοποιώντας τα πολυώνυμα με διανύσματα, ο δακτύλιος πηλίκο $\mathbb{Z}[x]/\langle f \rangle$ είναι ισομορφικός (ως μία προσθετική ομάδα) στο δικτύωμα ακεραίων $\mathbb{Z}^n$, δηλαδή, υπάρχει μία απεικόνιση $\phi : \mathbb{Z}[x]/\langle f \rangle \to \mathbb{Z}^n$ που είναι $1-1$ και $επί$ και, επίσης , οποιοδήποτε ιδεώδες $I \subseteq \mathbb{Z}[x]/\langle f \rangle$ καθορίζει ένα αντίστοιχο υποδικτύωμα ακεραίων $L(I) \subseteq \mathbb{Z}^n$. Ένα ιδεώδες δικτυώματος είναι ένα δικτύωμα ακεραίων $L(B) \subseteq \mathbb{Z}^n$, τέτοιο ώστε $B = \{g \; mod \; f : g \in I\}$ για κάποιο μονικό πολυώνυμο f βαθμού n και ένα ιδεώδες $I \subseteq \mathbb{Z}[x]/\langle f \rangle$.

Τα ιδεώδη δικτυώματα χρησιμεύουν ιδιαίτερα, όπως προαναφέρθηκε, στην κατασκευή πολύ αποτελεσματικών και πρακτικών συναρτήσεων διασποράς με αντίσταση στις συγκρούσεις, αλλά και γενικότερα, στην κατασκευή αποδοτικών κρυπτογραφικών αρχών. Επίσης, μας δίνουν τη δυνατότητα να κατασκευάσουμε *πλήρως ομομορφικά* (fully homomorphic) σχήματα κρυπτογράφησης [28]. Η ομομορφική κρυπτογράφηση είναι μία μορφή κρυπτογράφησης που επιτρέπει συγκεκριμένους τύπους υπολογισμών να πραγματοποιούνται επί ενός κρυπτοκειμένου και να δημιουργούν ένα κρυπτογραφημένο αποτέλεσμα το οποίο, όταν αποκρυπτογραφείται, ταιριάζει με το αποτέλεσμα των πράξεων που εκτελούνται στο απλό κείμενο. Υπάρχουν *μερικώς ομομορφικά* (partially homomorphic) και *πλήρως ομομορφικά* (fully homomorphic) σχήματα κρυπτογράφησης. Με τον όρο «*μερικώς ομομορφικά*» αναφερόμαστε σε κρυπτοσυστήματα που υποστηρίζουν ομομορφικούς υπολογισμούς μίας μόνο αριθμητικής πράξης (είτε πρόσθεσης, είτε πολλαπλασιασμού) στα απλά κείμενα, ενώ με τον όρο «*πλήρως ομομορφικά*» αναφερόμαστε σε κρυπτοσυστήματα που υποστηρίζουν τόσο την πρόσθεση, όσο και τον πολλαπλασιασμό (διατηρώντας έτσι τη δομή δακτυλίου των απλών κειμένων). Τα πλήρως ομομορφικά κρυπτοσυστήματα που έχουν αναπτυχθεί μέχρι στιγμής είναι λιγότερο αποδοτικά από τις μερικώς ομομορφικές υλοποιήσεις.

2.1.3.2 Ορθογωνιοποίηση Gram–Schmidt

Η ορθογωνιοποίηση Gram–Schmidt αποτελεί μία βασική διαδικασία της γραμμικής άλγεβρας και της αριθμητικής ανάλυσης. Είναι μία επαναληπτική μέθοδος για την ορθοκανονικοποίηση της βάσης ενός διανυσματικού χώρου. Η ορθογωνιοποίηση Gram–Schmidt παίρνει ένα οποιοδήποτε σύνολο n γραμμικά ανεξάρτητων διανυσμάτων και δημιουργεί ένα σύνολο n ορθογώνιων διανυσμάτων, δηλαδή διανυσμάτων κάθετων μεταξύ τους, ή με άλλα λόγια, διανύσματα που έχουν εσωτερικό γινόμενο ίσο με μηδέν.

Ορισμός 2.1.3.2.1 Ορθοκανονικά λέγονται τα ορθογώνια (κάθετα) διανύσματα, με μέτρο ίσο με τη μονάδα. Για τα διανύσματα αυτά ισχύει $\mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$ (δ_{ij} είναι το σύμβολο του Kronecker, το οποίο είναι ίσο με τη μονάδα για i=j και ίσο με το μηδέν για i≠j) [98].

Δοθείσης μιας αυθαίρετης βάσης $x_1, \ldots, x_n$, n–διάστατου δ.χ. V, ο αλγόριθμος Gram–Schmidt κατασκευάζει μία **ορθογώνια** βάση $v_1, \ldots, v_n$, για τον V. Αρχικά, θέτω $v_1 = x_1$. Τότε $v_2 = x_2 - \frac{\langle x_2, v_1 \rangle}{\|v_1\|^2} \cdot v_1$ και $v_3 = x_3 - \frac{\langle x_3, v_1 \rangle}{\|v_1\|^2} \cdot v_1 - \frac{\langle x_3, v_2 \rangle}{\|v_2\|^2} \cdot v_2$. Στο τέλος

της διαδικασίας Gram–Schmidt, κανονικοποιούμε την παραπάνω ορθογώνια βάση, διαιρώντας κάθε διάνυσμά της με το μέτρο του.

Παράδειγμα

Έστω μία αυθαίρετη βάση $B = x_1, \ldots, x_n$ του n–διάστατου διανυσματικού χώρου $\mathbb{R}^n$. Για n=3, θα βρισκόμαστε στον τρισδιάστατο Ευκλείδειο χώρο $\mathbb{R}^3$ και καθένα από τα 3 διανύσματα μιας οποιασδήποτε βάσης του $\mathbb{R}^3$ θα αποτελείται από 3 συντεταγμένες. Δηλαδή:

$$B_x = \{x_1, \ldots, x_n\} \text{ και αναλυτικότερα,}$$

$$B_x = \{x_1(x_{11}, x_{12}, x_{13}), \ldots, x_n\ (x_{n1}, x_{n2}, x_{n3})\}$$

Έτσι $B_x = x_1, x_2, x_3$ είναι μία βάση στον $\mathbb{R}^3$, με x_1= (4, –8, 8), x_2= (–3, 2, –4) και x_3=(−3, 1, 1). Θα έχουμε:

- $v_1 = (4, -8, 8)$
- $v_2 = (-3, 2, -4) - \frac{(-3, 2, -4)(4, -8, 8)}{(\sqrt{4^2+(-8)^2+8^2})^2} \cdot (4, -8, 8)$

  $= (-3, 2, -4) - \frac{(-60)}{144} \cdot (4, -8, 8) = (-3, 2, -4) - \frac{(-5)}{12} \cdot (4, -8, 8)$

  $= (-3, 2, -4) - (-\frac{5}{3}, \frac{10}{3}, -\frac{10}{3}) = (-\frac{9}{3}, \frac{6}{3}, -\frac{12}{3}) - (-\frac{5}{3}, \frac{10}{3}, -\frac{10}{3})$

  $= (-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})$

  $\Rightarrow v_2 = (-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})$
- $v_3 = (-3, 1, 1) - \frac{(-3, 1, 1)(4, -8, 8)}{\left(\sqrt{4^2+(-8)^2+8^2}\right)^2} \cdot (4, -8, 8)$

  $- \frac{(-3, 1, 1)(-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})}{(\sqrt{(-\frac{4}{3})^2+(-\frac{4}{3})^2+(-\frac{2}{3})^2})^2} \cdot (-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})$

  $= (-3, 1, 1) - (-\frac{1}{12}) \cdot (4, -8, 8) - \frac{1}{2} \cdot (-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})$

  $= (-3, 1, 1) - (-\frac{1}{3}, \frac{2}{3}, -\frac{2}{3}) - (-\frac{2}{3}, -\frac{2}{3}, -\frac{1}{3}) = (-2, 1, 2)$

  $\Rightarrow v_3 = (-2, 1, 2)$

Από την παραπάνω διαδικασία, ο αλγόριθμος Gram–Schmidt παρήγαγε την ορθογώνια βάση $B_v = v_1, v_2, v_3$ με: $v_1 = (4, -8, 8)$, $v_2 = (-\frac{4}{3}, -\frac{4}{3}, -\frac{2}{3})$ και

$v_3 = (-2, 1, 2)$. Όπως έχουμε προαναφέρει, για να κανονικοποιήσουμε τη B_v, χρειάζεται να διαιρέσουμε κάθε διάνυσμά της με το μέτρο του. Αρχικά, υπολογίζουμε το μέτρο κάθε διανύσματος ως εξής:

- $|v_1| = \sqrt{4^2 + (-8)^2 + 8^2} = \sqrt{144} = 12$
- $|v_2| = \sqrt{(-\frac{4}{3})^2 + (-\frac{4}{3})^2 + (-\frac{2}{3})^2} = \sqrt{4} = 2$
- $|v_3| = \sqrt{(-2)^2 + 1^2 + 2^2} = \sqrt{9} = 3$

Στη συνέχεια, διαιρούμε κάθε διάνυσμα της ορθογώνιας βάσης με το αντίστοιχο μέτρο του, οπότε έχουμε: $v_1 = (\frac{1}{3}, -\frac{2}{3}, \frac{2}{3})$, $v_2 = (-\frac{2}{3}, -\frac{2}{3}, -\frac{1}{3})$ και $v_3 = (-\frac{2}{3}, \frac{1}{3}, \frac{2}{3})$.

2.1.3.3 Διαδοχικά Ελάχιστα

Μία βασική παράμετρος ενός δικτυώματος είναι το μήκος του βραχύτερου, μη μηδενικού διανύσματός του. Στο σημείο αυτό, να επισημάνουμε ότι αναζητούμε ένα μη μηδενικό διάνυσμα, καθώς το μηδενικό διάνυσμα περιέχεται πάντα σε ένα δικτύωμα και η νόρμα του είναι 0. Αυτή η παράμετρος συμβολίζεται με λ_1. Νόρμα είναι μία συνάρτηση από τον $\mathbb{R}^n$ στον $\mathbb{R}$, η οποία σε κάθε διάνυσμα αντιστοιχεί ένα «μήκος» και ικανοποιεί τις ιδιότητες του παρακάτω ορισμού.

Ορισμός 2.1.3.3.1 Μία απεικόνιση (map) $\|\cdot\|: \mathbb{R}^n \to \mathbb{R}$ λέγεται νόρμα, εάν:

1. Είναι μη αρνητική και ισούται με μηδέν μόνο στο 0, δηλαδή, $\|x\| > 0$, για κάθε $x \in \mathbb{R}^n$, $\|0\| = 0$ και εάν $\|x\| = 0$, τότε $x = 0$.
2. Είναι θετικά ομογενής, δηλαδή $\|\lambda x\| = |\lambda| \cdot \|x\|$, για κάθε $x \in \mathbb{R}^n$, για κάθε $\lambda \in \mathbb{R}$.
3. Ικανοποιεί την τριγωνική ανισότητα, δηλαδή, $\|x + y\| \leq \|x\| + \|y\|$, για κάθε $x, y \in \mathbb{R}^n$.

Όπως προαναφέραμε, με τον όρο «μήκος» εννοούμε την Ευκλείδεια νόρμα, δηλαδή την απόσταση του διανύσματος από την αρχή των αξόνων, ή τη νόρμα l_2, η οποία ορίζεται ως $\|x\|_2 = \sqrt{\sum x_i^2}$. Συνήθως συμβολίζουμε αυτή τη νόρμα απλά με $\|x\|$.

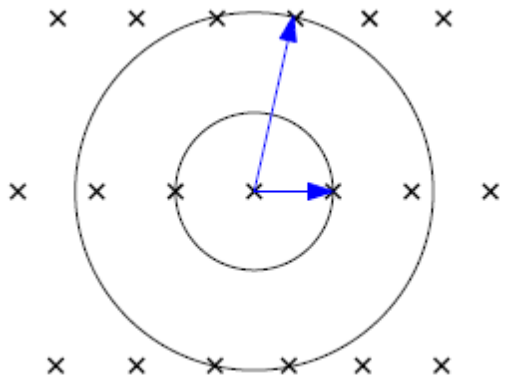
Ορισμός 2.1.3.3.2 Για οποιοδήποτε δικτύωμα L και οποιονδήποτε ακέραιο αριθμό k, με $k \leq rank\,(L)$, το i–οστό διαδοχικό ελάχιστο $\lambda k(L)$ ορίζεται ως το μικρότερο $r > 0$, τέτοιο ώστε το L να περιέχει τουλάχιστον k γραμμικά ανεξάρτητα διανύσματα με μήκος που οριοθετείται από το r [92].

Ένας ισοδύναμος τρόπος για να ορίσουμε το μήκος λ_1 είναι ο εξής: το μήκος του βραχύτερου, μη μηδενικού διανύσματος ενός δικτυώματος θα είναι το μικρότερο r, τέτοιο ώστε όλα τα σημεία του δικτυώματος που βρίσκονται εντός μίας σφαίρας ακτίνας r, να παράγουν ($span$) ένα διανυσματικό χώρο διάστασης 1.

Ορισμός 2.1.3.3.3 Έστω L ένα δικτύωμα βαθμού n. Για κάθε $i \in \{1, \dots, n\}$ ορίζουμε το i–οστό διαδοχικό ελάχιστο (successive minimum) ως

$$\lambda_1 (L) = \inf \{ r \mid \dim(span (L \cap \bar{B} (0, r))) \geq i \},$$

όπου $\bar{B}(0, r) = \{x \in R^m \mid \|x\| \leq r\}$ είναι η κλειστή σφαίρα ακτίνας r γύρω από το 0 και ως inf (από το infimum) συμβολίζεται το μεγαλύτερο κάτω φράγμα σε ένα υποσύνολο S ενός μερικώς διατεταγμένου συνόλου T. Το infimum είναι, δηλαδή, το μεγαλύτερο στοιχείο του T που είναι μικρότερο από ή ίσο με όλα τα στοιχεία του S [92].



Εικόνα 2.1.3.3.1 Διαδοχικά ελάχιστα

2.2 Βιβλιογραφική Επισκόπηση

Στην ενότητα αυτή αρχικά κάνουμε μία σύντομη αναδρομή στην ιστορία της κρυπτογραφίας, από την αρχαιότητα έως σήμερα και στη συνέχεια, παραθέτουμε μία όσο το δυνατόν πιο πλήρη, εάν και σύντομη, επισκόπηση της βιβλιογραφίας που σχετίζεται με τη σύγχρονη κρυπτογραφία και ειδικότερα, με την κρυπτογραφία που χρησιμοποιεί δικτυώματα ακεραίων.

Η λέξη κρυπτογραφία (αγγλ.: cryptography) προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η ιστορία της κρυπτογραφίας μπορεί να χωριστεί σε τρεις φάσεις [93]:

(1) Από τους αρχαίους πολιτισμούς μέχρι τον δέκατο ένατο αιώνα και το πρώτο μέρος του εικοστού αιώνα, με σχετικά απλούς αλγορίθμους που έχουν σχεδιαστεί και υλοποιούνται με το χέρι.

(2) Η περίοδος του Β' Παγκοσμίου Πολέμου, όπου έχουμε εκτεταμένη χρήση ηλεκτρομηχανικών συσκευών κρυπτογράφησης και τέλος,

(3) Τα τελευταία πενήντα χρόνια, όπου έχουμε ακόμη πιο διαδεδομένη χρήση των ηλεκτρονικών υπολογιστών, η οποία υποστηρίζεται και από μία στέρεα μαθηματική βάση.

Η κρυπτογραφία αποτελεί έναν από τους παλαιότερους τομείς τεχνικής μελέτης, από τους οποίους μπορούμε να βρούμε αρχεία, έως και τουλάχιστον πριν από 4.000 χρόνια. Η κρυπτογραφία, δηλαδή, χρησιμοποιούνταν ήδη από την αρχαιότητα, στις ιδιωτικές επικοινωνίες, στην τέχνη και τη θρησκεία και για στρατιωτική και διπλωματική χρήση [93].

Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει πραγματικά με τον Claude Shannon, ο οποίος είναι αναμφισβήτητα ο πατέρας της μαθηματικής κρυπτογραφίας, με τη δουλειά που έκανε κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου όσον αφορά την ασφάλεια των επικοινωνιών. Ο Shannon με το άρθρο του «Θεωρία Επικοινωνίας Συστημάτων Μυστικότητας» που δημοσιεύτηκε το 1949 και λίγο αργότερα με το βιβλίο «Μαθηματική Θεωρία Επικοινωνίας» που συνέγραψε με τον Warren Weaver, ίδρυσε ουσιαστικά μία στέρεη θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση (μελέτη των μεθόδων για την ανάκτηση του νοήματος της κρυπτογραφημένης πληροφορίας) [93].

Μετά από αυτό, η κρυπτογραφία λίγο ή πολύ εξαφανίστηκε μέσα σε μυστικούς, κυβερνητικούς οργανισμούς επικοινωνιών, όπως η NSA και η GCHQ. Μέχρι τα μέσα της δεκαετίας του 1970, λίγη δουλειά δημοσιεύονταν, όταν όλα άλλαξαν. Στην πραγματικότητα, η πιο πρόσφατη τάση ήταν να μη διατηρούνται μυστικοί οι κρυπτογραφικοί αλγόριθμοι, οι αρχές και οι μελέτες, αλλά μόνο τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης [93].

Στα μέσα της δεκαετίας του 1970 προέκυψαν δύο σημαντικές εξελίξεις στον τομέα της κρυπτογραφίας, οι οποίες – ευτυχώς – είδαν το φως της δημοσιότητας. Πρώτα ήταν η δημοσίευση του προσχέδιου του Προτύπου Κρυπτογράφησης Δεδομένων (Data Encryption Standard – DES)στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε

από την IBM, ύστερα από πρόσκληση του Εθνικού Γραφείου Προτύπων NBS (του σημερινού NIST), σε μία προσπάθεια για ανάπτυξη ασφαλούς ηλεκτρονικής επικοινωνίας για τις επιχειρήσεις, όπως τράπεζες και άλλους, μεγάλους, χρηματοπιστωτικούς οργανισμούς. Μετά από κάποια τροποποίηση από την NSA, Μετά από κάποια τροποποίηση από την NSA, εκδόθηκε και δημοσιεύθηκε το 1977. Η απελευθέρωση των προδιαγραφών του DES από το NBS πυροδότησε την έκρηξη του δημόσιου και ακαδημαϊκού ενδιαφέροντος για την κρυπτογραφία [93].

Ο παλαιός DES αντικαταστάθηκε επίσημα από το προηγμένο πρότυπο κρυπτογράφησης (AES) το 2001. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον Rijndael, που υποβλήθηκε από δύο Βέλγους κρυπτογράφους, για να είναι ο AES. Ο αλγόριθμος DES και οι πιο ασφαλείς παραλλαγές του (όπως ο Triple DES) χρησιμοποιούνται ακόμα και σήμερα, έχοντας ενσωματωθεί σε πολλά εθνικά πρότυπα και πρότυπα οργανισμών. Ωστόσο , το 56–bit κλειδί έχει αποδειχθεί ότι είναι ανεπαρκές για προστασία από βίαιες επιθέσεις. Υπάρχουν επίσης κάποιες έγκυρες και αποτελεσματικές εναλλακτικές του AES, όπως ο αλγόριθμος Blowfish [93].

Ιδιαίτερη σημασία στην εξέλιξη της ιστορίας της κρυπτογραφίας έχει το άρθρο των Diffie και Hellman «New Directions in Cryptography» (Νέες Κατευθύνσεις στην Κρυπτογραφία), που δημοσιεύτηκε το 1976. Με το άρθρο αυτό γεννήθηκε η κρυπτογραφία δημοσίου κλειδιού και δημιουργήθηκε μία νέα και ευφυής μέθοδος για την ανταλλαγή κλειδιών, βασισμένη στη δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου. Μετά από δύο χρόνια, το 1978, οι Rivest, Shamir και Adleman ανακάλυψαν τον αλγόριθμο RSA, το πρώτο πρακτικό σχήμα κρυπτογράφησης και υπογραφής δημοσίου κλειδιού. Το σχήμα αυτό βασίστηκε στη δυσεπιλυσιμότητα της παραγοντοποίησης μεγάλων ακεραίων. Αυτή η εφαρμογή ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία αναζωογόνησε τις προσπάθειες για την εύρεση περισσότερο αποδοτικών μεθόδων παραγοντοποίησης. Στη δεκαετία του ‘80 σημειώθηκαν σημαντικές πρόοδοι σε αυτόν τον τομέα, αλλά καμία που να καθιστά το σύστημα RSA ανασφαλές. Μία άλλη κλάση ισχυρών και πρακτικών σχημάτων δημοσίου κλειδιού ανακαλύφθηκε από τον ElGamal το 1985. Τα σχήματα αυτά βασίζονται επίσης στο πρόβλημα διακριτού λογαρίθμου [93].

Τα δικτυώματα ακέραιων αριθμών άρχισαν να χρησιμοποιούνται στην κρυπτογραφία από το 1996 περίπου, με το πρωτοποριακό εύρημα του Miklos Ajtai [13] σχετικά με μία μονόδρομη συνάρτηση, η οποία βασίζεται στη δυσκολία της χειρότερης

περίπτωσης διαφόρων προβλημάτων που υπάρχουν σε δικτυώματα ακεραίων. Την ίδια χρονιά αναπτύχθηκε το κρυπτοσύστημα GGH [31] των Goldreich, Goldwasser και Halevi, ενώ δύο χρόνια μετά, οι Hoffstein, Pipher και Silverman παρουσίασαν το κρυπτοσύστημα NTRU [39]. Η συνάρτηση διασποράς LASH–x [91] προτάθηκε το 2006 και κρυπταναλύθηκε το 2007. Το GGH σχήμα ψηφιακών υπογραφών, το οποίο προτάθηκε το 1997 και το NTRUsign που προτάθηκε το 2003, έχουν ένα σοβαρό μειονέκτημα σε σχέση με τα παραδοσιακά σχήματα: κάθε υπογραφή που κυκλοφορεί διαρρέει πληροφορίες σχετικά με το ιδιωτικό (μυστικό) κλειδί και όταν έχουν ληφθεί επαρκώς πολλές υπογραφές, τότε μπορεί να υπολογιστεί (έστω και προσεγγιστικά) ένας συγκεκριμένος Gram πίνακας που σχετίζεται με το ιδιωτικό κλειδί. Το σχήμα υπογραφής GGH δεν προσέλκυσε μεγάλο ενδιαφέρον στην ερευνητική βιβλιογραφία, έως ότου η εταιρεία NTRU Cryptosystems, inc., πρότεινε το NTRUSign, στο οποίο επισημάνθηκαν όμως κάποιες ατέλειες από τους Gentry και Szydlo το 2006 (για ένα αδιατάρακτο σύστημα) και τελικά, το 2012 κρυπταναλύθηκε και το σχήμα με τις διαταραχές [29] από τους L. Ducas και P.Q. Nguyen.

Παρόλο που η χρήση των δικτυωμάτων για κρυπτογραφικούς σκοπούς μελετάται λιγότερο από 20 χρόνια και θεωρείται, συνεπώς, σχετικά πρόσφατο τμήμα της κρυπτογραφίας, σημαντικό τμήμα της επιστημονικής κοινότητας ασχολείται με την έρευνα σε αυτό το πεδίο και υπάρχει πληθώρα σχετικών εργασιών και δημοσιεύσεων στον ιστότοπο https://eprint.iacr.org/. Σύμφωνα με κάποιες από τις πιο σημαντικές από αυτές, τα πιο αξιοσημείωτα κρυπτογραφικά σχήματα που είναι βασισμένα σε δικτυώματα ακεραίων είναι το NTRU [39] που αναπτύχθηκε το 1996, το βασισμένο στο πρόβλημα της μάθησης με σφάλματα (LWE–based) κρυπτοσύστημα του O.Regev [73] το 2005, αλλά και το “NTRU–like” κρυπτοσύστημα των D.Stehle και R.Steinfeld [79], το οποίο φέρει και απόδειξη σχετικά με την ασφάλειά του και αναπτύχθηκε το 2011. Επίσης σημαντική και η ανάπτυξη νέων κρυπτογραφικών δομών και εννοιών, όπως τα δένδρα Bonsai (Bonsai Trees) [23]. Τα δένδρα Bonsai αποτελούν μία συλλογή αρχών και τεχνικών, οι οποίες μπορούν να χρησιμοποιηθούν με πολλούς τρόπους. Αναπτύχθηκαν για την επίλυση ορισμένων σημαντικών ανοικτών προβλημάτων σε αυτήν την περιοχή, όπως είναι η εύρεση ενός αποδοτικού και άνευ κατάστασης, “hash–and–sign” σχήματος υπογραφής στο καθιερωμένο μοντέλο (standard model), αλλά και η ανάπτυξη του πρώτου ιεραρχικού σχήματος κρυπτογράφησης βασισμένης στην ταυτότητα (Hierarchical Identity–based Encryption), επίσης στο καθιερωμένο μοντέλο, χωρίς

δηλαδή τυχαία μαντεία (random oracles). Περαιτέρω ανάλυση των σχημάτων αυτών θεωρείται εκτός των σκοπών της παρούσης εργασίας.

Κεφάλαιο 3
Κρυπτογραφία
Βασισμένη σε Δικτυώματα Ακεραίων

Με τον όρο «κρυπτογραφία βασισμένη σε δικτυώματα ακεραίων» αναφερόμαστε στις κρυπτογραφικές αρχές, τους αλγόριθμους κρυπτογράφησης/αποκρυπτογράφησης, τις συναρτήσεις διασποράς και τα σχήματα ψηφιακών υπογραφών, τα οποία χρησιμοποιούν Ευκλείδεια δικτυώματα ακέραιων αριθμών. Η κρυπτογραφία αυτού του είδους αποτελεί μία από τις πιο ενδιαφέρουσες και ταχύτατα εξελισσόμενες περιοχές στη μαθηματική κρυπτογραφία του σήμερα. Το πεδίο αυτό άρχισε να ερευνάται το 1996, με την πρωτοποριακή εργασία του Ajtai [11] και πρόσφατα, το 2009, πήρε μία δεύτερη πνοή με το επαναστατικό έργο του Gentry [28] σχετικά με την πλήρως ομομορφική (fully homomorphic) κρυπτογράφηση.

Το ενδιαφέρον που υπάρχει για την κρυπτογραφία αυτού του είδους οφείλεται σε διάφορους συγκλίνοντες παράγοντες. Από θεωρητικής πλευράς, η κρυπτογραφία που χρησιμοποιεί δικτυώματα ακεραίων υποστηρίζεται από ισχυρές εγγυήσεις ασφάλειας χειρότερης περίπτωσης/μέσης περίπτωσης. Από πρακτικής πλευράς, η κρυπτογραφία αυτή έχει αποδειχθεί να είναι πολύ ευέλικτη, χαρακτηριστικό το οποίο οδηγεί σε μια άνευ προηγουμένου ποικιλία εφαρμογών, από απλές (και αποτελεσματικές) συναρτήσεις διασποράς, σε πολύπλοκες και ισχυρές αρχές κρυπτογράφησης δημοσίου κλειδιού, με αποκορύφωμα την περίφημη πρόσφατη ανάπτυξη πλήρως ομομορφικής κρυπτογράφησης [28].

Η κρυπτογραφία που βασίζεται σε δικτυώματα ακεραίων προσφέρει ασυμπτωτική αποτελεσματικότητα, πιθανή αντίσταση σε κβαντικούς υπολογιστές και νέες λειτουργίες. Ένα σημαντικό χαρακτηριστικό της κρυπτογραφίας που βασίζεται σε δικτυώματα ακεραίων είναι η απλότητα: οι περισσότερες κρυπτογραφικές λειτουργίες μπορεί να υλοποιηθούν χρησιμοποιώντας βασικές αριθμητικές πράξεις με μικρούς αριθμούς, και πολλές κρυπτογραφικές κατασκευές κρύβουν μία διαισθητική και ελκυστική γεωμετρική ερμηνεία όσον αφορά τα δικτυώματα σημείου. Έτσι, σε αντίθεση με άλλες περιοχές της μαθηματικής κρυπτολογίας, ακόμη και ένας αρχάριος μπορεί να αποκτήσει, με μικρή

προσπάθεια, μια καλή κατανόηση όχι μόνο των εφαρμογών, αλλά και των υποκείμενων μαθηματικών της κρυπτογραφίας αυτού του είδους.

Κατά τα τελευταία χρόνια, υπήρξε σημαντική πρόοδος στην αποδεδειγμένα ασφαλή κρυπτογράφηση που βασίζεται σε δικτυώματα ακεραίων, αλλά από πρακτικής απόψεως, πολύ λίγα σχήματα δικτυώματος μπορούν να ανταγωνιστούν, για την ώρα, τα προτυποποιημένα συστήματα που προϋπήρχαν.

Στο κεφάλαιο αυτό αναφερόμαστε αρχικά στα δυσεπίλυτα υπολογιστικά προβλήματα που ανακύπτουν από τη χρήση δικτυωμάτων, τα οποία εκμεταλλεύεται η κρυπτογραφία για να διασφαλίσει το απόρρητο των επικοινωνιών μας. Έπειτα, παρουσιάζουμε το θέμα της αναγωγής της βάσης ενός δικτυώματος, καθώς και τους πιο σημαντικούς αλγόριθμους που έχουν αναπτυχθεί για αυτόν το σκοπό.

3.1 Προβλήματα Βελτιστοποίησης σε Δικτυώματα

Όπως είναι γνωστό, κάτω από οποιοδήποτε κρυπτογραφικό σύστημα δημοσίου κλειδιού υπόκειται ένα δυσεπίλυτο –υπολογιστικά– μαθηματικό πρόβλημα, ένα πρόβλημα του οποίου η λύση απαιτεί σημαντικούς πόρους , ανεξάρτητα από τον αλγόριθμο που χρησιμοποιείται. Έτσι, στην περίπτωση του RSA αλγόριθμου το πρόβλημα είναι η παραγοντοποίηση μεγάλων ακεραίων, στο κρυπτοσύστημα McEliece το πρόβλημα είναι η εύρεση της ελάχιστης απόστασης για οποιονδήποτε γραμμικό κώδικα, ενώ στην κρυπτογράφηση ElGamal το πρόβλημα είναι η εύρεση του διακριτού λογαρίθμου μίας κυκλικής ομάδας της μορφής $(\mathbb{Z}_p)^x$. Σε δικτυώματα ακέραιων αριθμών, τα προβλήματα που υπάρχουν είναι προβλήματα βελτιστοποίησης, στοχεύουν δηλαδή στην εύρεση της καλύτερης λύσης από το σύνολο των εφικτών λύσεων.

Στη συνέχεια αυτής της υποενότητας θα περιγράψουμε αναλυτικά τα πιο θεμελιώδη από τα δυσεπίλυτα –υπολογιστικά– προβλήματα σε δικτυώματα ακεραίων, τα οποία είναι το πρόβλημα του βραχύτερου διανύσματος (Shortest Vector Problem – SVP) σε ένα δικτύωμα και το πρόβλημα του εγγύτερου διανύσματος (Closest Vector Problem – CVP) σε ένα δοθέν διάνυσμα δικτυώματος. Στη διεθνή βιβλιογραφία, υπάρχουν πολλές παραλλαγές των δύο αυτών βασικών προβλημάτων, όμως στο πλαίσιο της παρούσης εργασίας θα αναφερθούμε στην κύρια εκδοχή του καθενός από αυτά. Επίσης σημαντικά είναι και τα προβλήματα αποκωδικοποίησης μίας οριοθετημένης (Bounded Distance Decoding – BDD) ή μίας απόλυτης (Absolute Distance Decoding – ADD) απόστασης, τα

οποία θεωρούνται, όπως θα δούμε, παραλλαγές του CVP προβλήματος. Τέλος, στα προβλήματα βελτιστοποίησης σε δικτυώματα ακεραίων ανήκει και το πρόβλημα της καλύπτουσας ακτίνας (Covering Radius Problem – CRP), αλλά και το πρόβλημα εύρεσης της μικρότερης βάσης σε ένα δικτύωμα (Shortest Basis Problem – SBP).

Η εικαζόμενη δυσεπιλυσιμότητα αυτών των προβλημάτων είναι κεντρικής σημασίας για την κατασκευή ασφαλών κρυπτοσυστημάτων, βασισμένων σε δικτυώματα. Τα υπολογιστικά αυτά προβλήματα αποδεδειγμένα μειώνουν τις πιθανότητες επιτυχών επιθέσεων ενάντια σε αυτού του είδους τα κρυπτογραφικά σχήματα.

3.1.1 Το πρόβλημα του βραχύτερου διανύσματος (SVP)

Το πρόβλημα εύρεσης του βραχύτερου διανύσματος (Shortest Vector Problem – SVP) αποτελεί, μαζί με το CVP, τον πυρήνα της κρυπτογράφησης με χρήση δικτυωμάτων. Αναφέρθηκε για πρώτη φορά από τον Dirichlet το 1842 [64] και διατυπώνεται ως εξής: «Δοθείσης μιας βάσης ενός δικτυώματος L, να βρεθεί το βραχύτερο, μη μηδενικό διάνυσμα στο δικτύωμα» [36]. Με άλλα λόγια, δοθείσης μιας βάσης ενός δικτυώματος L, να βρεθεί ένα $v \in L$, τέτοιο ώστε $\|v\| = \lambda_1(L)$. Το SVP_∞ δηλώνει το ισοδύναμο του προβλήματος SVP για τη νόρμα άπειρο (infinity norm). Μπορούν να ορισθούν, επίσης και προσεγγιστικές εκδοχές του SVP. Το SVP βρίσκει εφαρμογή σε πολλούς τομείς των υπολογιστικών μαθηματικών και της επιστήμης υπολογιστών, όπως η υπολογιστική θεωρία αριθμών και η συνδυαστική βελτιστοποίηση.

Πρόβλημα βραχύτερου διανύσματος (shortest vector problem – SVP)

Ορισμός 3.1.1.1 Δοθέντος ενός δικτυώματος $L = L\,(b_1, b_2, \dots, b_n) \subseteq R^n$ ορισμένου από τα γραμμικώς ανεξάρτητα διανύσματα $b_1, b_2, \dots, b_n \in Q^n$ και ενός ρητού αριθμού $r > 0$, να βρεθεί ένα μη μηδενικό διάνυσμα $u \in L$, τέτοιο ώστε $\|u\|_2 < r$

Σύμφωνα με το πρώτο θεώρημα του H.Minkowski, κάθε δικτύωμα L τάξης (rank) n περιέχει ένα μη μηδενικό διάνυσμα με μήκος το πολύ $\sqrt{n}(\det L)^{1/n}$. Η απόδειξή του, όμως, δε μας δίνει έναν αλγόριθμο για την εύρεση ενός τέτοιου διανύσματος. Στην πραγματικότητα, δεν υπάρχει κανένας γνωστός αποτελεσματικός αλγόριθμος ο οποίος να βρίσκει τέτοια βραχέα διανύσματα.

Υπάρχουν τρεις παραλλαγές του SVP προβλήματος σε ένα δικτύωμα ακεραίων, ανάλογα με το εάν θα πρέπει στην πραγματικότητα να βρούμε το βραχύτερο διάνυσμα,

το μήκος του, ή απλά να αποφασίσουμε εάν αυτό είναι μικρότερο από κάποιο δεδομένο αριθμό. Οι παραλλαγές αυτές είναι:

1. **SVP Αναζήτησης** (Search SVP): Δοθείσης μίας βάσης δικτυώματος $\in \mathbb{Z}^{m\times n}$, να βρεθεί ένα $u \in L(B)$, τέτοιο ώστε $\|u\| = \lambda_1(L(B))$.
2. **SVP Βελτιστοποίησης** (Optimization SVP): Δοθείσης μίας βάσης δικτυώματος $\in \mathbb{Z}^{m\times n}$, να βρεθεί το $\lambda_1(L(B))$.
3. **SVP Λήψης Αποφάσεων** (Decisional SVP ή gapSVP): Δοθείσης μίας βάσης δικτυώματος $B \in \mathbb{Z}^{m\times n}$ και ενός ρητού αριθμού $r \in \mathbb{Q}$, να αποφασισθεί εάν $\lambda_1\big(L(B)\big) \leq r$ ή όχι. (NP–complete)

Παρατήρηση: Ο σκοπός του περιορισμού που υπάρχει η βάση του δικτυώματος να αποτελείται από διανύσματα με ακέραιες συντεταγμένες, είναι για να κάνει την είσοδο αναπαραστάσιμη σε πεπερασμένο πλήθος bits, ούτως ώστε να μπορούμε να θεωρήσουμε το SVP ως πρότυπο υπολογιστικό πρόβλημα. Θα μπορούσε επίσης η βάση του δικτυώματος να αποτελείται από διανύσματα με συντεταγμένες ρητούς αριθμούς. Αυτό θα οδηγούσε σε έναν ουσιαστικά ισοδύναμο ορισμό, δεδομένου ότι με στρογγυλοποίηση, μπορεί κανείς να κάνει όλες τις ρητές συντεταγμένες ακέραιες. Οι τρεις παραλλαγές του SVP είναι ισοδύναμες όσον αφορά την υπολογιστική τους δυσκολία [36, 38].

3.1.2 Το πρόβλημα του εγγύτερου διανύσματος (CVP)

Ένα άλλο θεμελιώδες υπολογιστικό πρόβλημα σε δικτυώματα σημείου είναι το πρόβλημα του εγγύτερου (ή πλησιέστερου) διανύσματος (closest vector problem – CVP). Το CVP πρόβλημα αναφέρεται στην εύρεση ενός διανύσματος εκτός του δοθέντος δικτυώματος, το οποίο να είναι το πλησιέστερο σε ένα δεδομένο διάνυσμα του δικτυώματος.

Πρόβλημα εγγύτερου διανύσματος (closest vector problem – CVP)

Ορισμός 3.1.2.1 Δοθέντος ενός δικτυώματος $L \subset \mathbb{R}^n$, ενός σημείου–στόχου $t \in \mathbb{R}^n$, και ενός φράγματος απόστασης d, το CVP ζητά ένα σημείο $v \in L$ σε απόσταση $\|t - v\| \leq d$ από το στόχο, εφόσον ένα τέτοιο σημείο υπάρχει στο δικτύωμα L [36].

Υπάρχει μία ακριβής εκδοχή του CVP και μία προσεγγιστική εκδοχή. Στην ακριβή εκδοχή, το φράγμα απόστασης είναι η απόσταση $d = \mu(t, L) = min_{v \in L} \|t - v\|$ μεταξύ του στόχου και του δικτυώματος. Στην προσεγγιστική εκδοχή του CVP, CVPγ, θέτουμε $d = \gamma \times \mu$ [36].

3.1.3 Παραλλαγές του CVP: BDD και ADD

Σύμφωνα με τον D.Micciancio, δύο ειδικές εκδόσεις του CVP που παίζουν εξέχοντα ρόλο στην κρυπτογραφία είναι:

1. Το πρόβλημα Αποκωδικοποίησης μιας Οριοθετημένης Απόστασης (Bounded Distance Decoding – BDD), όπου $d < \frac{\lambda}{2}$, και
2. το πρόβλημα Αποκωδικοποίησης μιας Απόλυτης Απόστασης (Absolute Distance Decoding – ADD), όπου $d \geq \rho$.

Αποκωδικοποίηση Οριοθετημένης Απόστασης (Bounded Distance Decoding–BDD)

Ορισμός 3.1.3.1 Δεδομένου ενός διανύσματος, έτσι ώστε η απόστασή του από το δικτύωμα να είναι το πολύ $\frac{\lambda(L)}{2}$, ο αλγόριθμος BDD πρέπει να εξάγει το εγγύτερο (σε αυτό) διάνυσμα του δικτυώματος [98].

Αποκωδικοποίηση Απόλυτης Απόστασης (Absolute Distance Decoding–ADD)

Ορισμός 3.1.3.2 Δεδομένου ενός διανύσματος, έτσι ώστε η απόστασή του από το δικτύωμα να είναι τουλάχιστον ίση με ρ, ο αλγόριθμος ADD πρέπει να εξάγει ένα διάνυσμα του δικτυώματος, όχι και τόσο μακριά από το στόχο t.

Η σημασία αυτών των συγκεκριμένων ρυθμίσεων των παραμέτρων είναι ότι, όταν $d < \frac{\lambda}{2}$, εάν υπάρχει μία λύση, τότε αυτή θα είναι και η μοναδική. Από την άλλη πλευρά, όταν $d \geq \rho$, είναι εγγυημένο ότι μία λύση θα υπάρχει (για οποιονδήποτε στόχο t) και ότι, σε γενικές γραμμές, αυτή δε θα είναι μοναδική. Μπορούν να ληφθούν ευκολότερες παραλλαγές των προβλημάτων BDD και ADD, εάν εισάγουμε έναν συντελεστή χαλαρότητας (slackness factor) $\gamma \geq 1$ και ενισχύσουμε τους περιορισμούς για το φράγμα απόστασης d σε $d < \lambda/(2\gamma)$ για το BDD_γ και $d \geq \gamma\rho$ για το ADD_γ.

Ανεπίσημα, το BDD είναι το πρόβλημα εύρεσης του διανύσματος του δικτυώματος το οποίο είναι το εγγύτερο (closest) σε έναν στόχο, όταν ο στόχος είναι

πολύ κοντά στο δικτύωμα, ενώ στο ADD αναζητούμε ένα διάνυσμα του δικτυώματος το οποίο να μην είναι και τόσο μακριά από το στόχο, όπου το «μακριά» μετράται σε σχέση με το απόλυτο όριο εντός του οποίου είναι εγγυημένο πάντα ότι θα υπάρχει μία λύση. Ως συνήθως, ο προσεγγιστικός παράγοντας γ μπορεί να είναι μία συνάρτηση της διάστασης.

Δεν είναι γνωστός κάποιος αποδοτικός αλγόριθμος για την επίλυση των προβλημάτων BDD και ADD, έστω και κατά προσέγγιση, για προσεγγιστικούς παράγοντες που είναι εκθετικοί στη διάσταση του δικτυώματος στη χειρότερη περίπτωση. Ωστόσο, η κρυπτογραφία απαιτεί δυσεπίλυτα, στη μέση περίπτωση, προβλήματα, έτσι ώστε όταν επιλέγετε το κρυπτογραφικό σας κλειδί στην τύχη , να γνωρίζετε με μεγάλη βεβαιότητα ότι το προκύπτον κρυπταναλυτικό πρόβλημα είναι πράγματι δυσεπίλυτο. Συνεπώς, πριν την ανάπτυξη οποιασδήποτε κρυπτογραφικής εφαρμογής, είναι απαραίτητο να καθορισθούν κατάλληλες κατανομές πιθανότητας (στο δικτύωμα και στο στόχο t).

3.1.4 Το πρόβλημα της καλύπτουσας ακτίνας (CRP)

Οι πρώτοι που ασχολήθηκαν με τη μελέτη της καλύπτουσας ακτίνας σε δικτυώματα από υπολογιστική άποψη, ήταν οι V.Guruswami, D.Micciancio και O.Regev στο άρθρο τους [34]. Η καλύπτουσα ακτίνα ενός δικτυώματος L σε έναν Ευκλείδειο χώρο, συμβολίζεται με $\rho(L)$ και ορίζεται ως η μικρότερη ακτίνα ρ, τέτοια ώστε οι κλειστές σφαίρες της ακτίνας ρ που είναι τοποθετημένες στο κέντρο όλων των σημείων του δικτυώματος καλύπτουν ολόκληρο το χώρο, δηλαδή, οποιοδήποτε σημείο στο $span(L)$ βρίσκεται εντός μίας απόστασης ρ από το δικτύωμα.

Πρόβλημα Καλύπτουσας Ακτίνας (Covering Radius Problem – CRP)

Ορισμός 3.1.4.1 Δεδομένης μίας βάσης για το δικτύωμα L, ο αλγόριθμος CRP πρέπει να βρει τη μεγαλύτερη απόσταση (ή σε ορισμένες εκδόσεις, την προσέγγισή της) μεταξύ οποιουδήποτε διανύσματος και του δικτυώματος [40].

Με άλλα λόγια, το πρόβλημα αυτό έγκειται στην εύρεση της $\rho(L)$ για δεδομένο δικτύωμα L. Για την επίλυση αυτού του προβλήματος πρέπει να βρούμε ένα *σημείο* στο $span(L)$ σε απόσταση $\rho(L)$ από το δικτύωμα, δηλαδή μία αποκαλούμενη *deep hole*. Μία *deep hole* είναι εκείνη της οποίας η απόσταση από το δικτύωμα είναι ένα ολικό μέγιστο. Όμως, δοθέντος ενός σημείου $t \in span(L)$, ο υπολογισμός της απόστασης από

το t στο L δεν είναι ευκολότερη από το CVP πρόβλημα, το οποίο είναι NP–πλήρες και έτσι, τότε θα πρέπει να συγκρίνουμε όλη την απόσταση, όταν το t αλλάζει μέσα στο $span(L)$ [37].

Το πρόβλημα της καλύπτουσας ακτίνας (Covering Radius Problem – CRP) σε δικτύωμα οποιασδήποτε διάστασης θεωρείται ότι δεν είναι επιλύσιμο σε μη ντετερμινιστικό (αιτιοκρατικό) πολυωνυμικό χρόνο [37].

3.1.5 Το πρόβλημα της βραχύτερης βάσης (SBP)

Πολλά προβλήματα γίνονται ευκολότερα εάν η βάση εισόδου αποτελείται από βραχέα διανύσματα. Ένας αλγόριθμος που λύνει το πρόβλημα της βραχύτερης βάσης (Shortest Basis Problem – SBP), πρέπει, δεδομένης μίας βάσης B ενός δικτυώματος, να εξάγει μία ισοδύναμη βάση B', τέτοια ώστε το μήκος του μεγαλύτερου διανύσματος στη βάση B' να είναι όσο το δυνατό μικρότερο. Το ζητούμενο, δηλαδή, είναι να βρεθεί μία βάση, η οποία να ελαχιστοποιεί το μεγαλύτερο από τα μήκη των διανυσμάτων του δικτυώματος [64]. Μία «πιο γεωμετρική» παραλλαγή του προβλήματος αυτού στοχεύει στην ελαχιστοποίηση του γινομένου των παραπάνω μηκών.

Στο SBP^p, δοθέντος ενός δικτυώματος L, ο στόχος μας είναι να βρούμε μία βάση $\{v_i\}_{i=1}^n$ του L, τέτοια ώστε το $max_i \|v_i\|_p$ να ελαχιστοποιείται. Η προσεγγιστική έκδοση SBP_γ του SBP αποτελείται από την εύρεση μίας βάσης, της οποίας το μεγαλύτερο διάνυσμα είναι το πολύ γ φορές μεγαλύτερο από το μεγαλύτερο διάνυσμα της βραχύτερης βάσης. Στο SBP_γ^p μας δίνεται ένα δικτύωμα $L \subseteq \mathbb{R}^m$, τάξης n και ο στόχος είναι να βρούμε μία βάση $\{v_i\}_{i=1}^n$ του L, τέτοια ώστε $max_i \|v_i\|_p \leq \gamma \cdot \kappa^\rho (L)$, όπου $\kappa^\rho (L)$ είναι το ελάχιστο του $max_i \|v_i\|_p$ επί όλων των βάσεων $\{v_i\}_{i=1}^n$ του L.

Το πρόβλημα της βραχύτερης βάσης έχει πολλές παραλλαγές, οι οποίες προσδιορίζονται από τον ακριβή ορισμό του όρου «βραχύτερη». Παρόλο που ο προσδιορισμός της βραχύτερης βάσης είναι πιθανώς ένα NP–πλήρες πρόβλημα, αλγόριθμοι όπως ο αλγόριθμος LLL μπορούν να βρουν μία βραχέα βάση (όχι κατ' ανάγκη τη βραχύτερη) σε πολυωνυμικό χρόνο με εγγυημένη απόδοση στη χειρότερη περίπτωση.

3.2 Αναγωγή Βάσης

Η αναγωγή της βάσης ενός δικτυώματος είναι μία διαδικασία μετασχηματισμού της, έτσι ώστε να καθίσταται εφικτή η επίλυση των προβλημάτων βελτιστοποίησης που παρουσιάσθηκαν στην προηγούμενη υποενότητα. Εκτός από τη διαδικασία της αναγωγής, στην επίλυση των παραπάνω προβλημάτων μπορούν να συμβάλλουν και κάποιες άλλες αλγοριθμικές τεχνικές, όπως η απαρίθμηση (enumeration), στην απλή μορφή της, ή σε συνδυασμό με τεχνικές «κλαδέματος» (pruning). Πειράματα έχουν δείξει ότι οι αλγόριθμοι αναγωγής της βάσης ενός δικτυώματος συμπεριφέρονται εκπληκτικά καλά και μπορούν να προσφέρουν πολύ καλύτερες προσεγγίσεις στο SVP ή στο CVP πρόβλημα από ό, τι αναμενόταν.

Από μαθηματικής άποψης, η ιστορία της αναγωγής της βάσης ενός δικτυώματος έχει τις ρίζες της στη θεωρία των τετραγωνικών μορφών που αναπτύχθηκε από τους Lagrange, Gauss, Hermite, Korkine και Zolotarev, καθώς και στη γεωμετρία αριθμών του Minkowski [41].

Όπως έχουμε ήδη αναφέρει, οποιοδήποτε δικτύωμα ακεραίων L μπορεί να περιγραφεί από πολλές, διαφορετικές βάσεις. Σε ένα διακριτό σύνολο διανυσμάτων $b_1, b_2, \dots, b_n$, όπου όλα τα διανύσματα σχηματίζουν βάσεις του L, υπάρχει κάποια κατάταξη των βάσεων B_i κι έτσι μία ή περισσότερες από τις B_i θεωρείται ότι έχουν κάποιες επιθυμητές ιδιότητες έναντι των άλλων βάσεων του δικτυώματος L. Η πλέον σημαντική από αυτές τις ιδιότητες είναι η ορθογωνιότητα των διανυσμάτων της βάσης του δικτυώματος και όπως προαναφέραμε στην υποενότητα 2.1.3.2., ορθογώνια θεωρούνται τα διανύσματα που είναι κάθετα μεταξύ τους, ή με άλλα λόγια, τα διανύσματα που έχουν εσωτερικό γινόμενο ίσο με μηδέν.

Η αναγωγή της βάσης ενός δικτυώματος συνίσταται, αρχίζοντας από μία βάση B στην προσπάθεια βελτίωσης της ποιότητάς της, η οποία παραδοσιακά μετράται με βάση την ορθογωνιότητα των διανυσμάτων της [36]. Η βάση που προκύπτει από τη διαδικασία της αναγωγής ονομάζεται *ανηγμένη*. Μία ανηγμένη βάση ενός δικτυώματος δύο διαστάσεων ορίζεται ως εξής:

Ορισμός 3.2.1 Έστω (a, b) μία βάση ενός δικτυώματος ακεραίων. Η βάση αυτή θα είναι ανηγμένη (σε σχέση με τη νόρμα $\|\cdot\|$), εάν $\|a\|,\ \|b\| \leq \|a+b\|, \|a-b\|$ [56].

Γεωμετρικά, ο ορισμός αυτός σημαίνει ότι οι διαγώνιοι του θεμελιώδους παραλληλεπιπέδου που σχετίζεται με τη βάση του δικτυώματος έχουν μήκος τουλάχιστον ίσο με το μήκος των ακμών του [56].

Υπάρχουν πολλές διαφορετικές έννοιες ανηγμένων βάσεων και για τις περισσότερες από αυτές υπάρχει και ένας αλγόριθμος για τον υπολογισμό τους, δεδομένης μίας οποιασδήποτε βάσης του δικτυώματος. Οι ανηγμένες βάσεις επιτρέπουν την επίλυση των πιο σημαντικών προβλημάτων που σχετίζονται με δικτυώματα ακεραίων, του SVP και του CVP, τα οποία όπως αναφέραμε στις υποενότητες 3.1.1 και 3.1.2, μπορούν να επιλυθούν είτε με ακρίβεια, είτε προσεγγιστικά.

Ο πρώτος αλγόριθμος που αναπτύχθηκε για την επίλυση του SVP επιτυγχάνει το επιθυμητό αποτέλεσμα σε δισδιάστατο δικτύωμα με ακρίβεια και σε τετραγωνικό χρόνο. Στη βιβλιογραφία ο αλγόριθμος αυτός αποδίδεται τόσο στον Lagrange [46] , όσο και στον Gauss. Σε αυθαίρετες διαστάσεις, υπάρχουν δύο είδη SVP αλγορίθμων:

1. **Ακριβείς αλγόριθμοι.** Αυτοί οι αλγόριθμοι αποδεδειγμένα βρίσκουν το βραχύτερο διάνυσμα του δικτυώματος, αλλά είναι ακριβοί και έχουν χρόνο εκτέλεσης τουλάχιστον εκθετικό στη διάσταση του δικτυώματος. Διαισθητικά, οι αλγόριθμοι αυτοί εκτελούν εξαντλητική αναζήτηση όλων των εξαιρετικά βραχέων διανυσμάτων του δικτυώματος, των οποίων ο αριθμός είναι στη χειρότερη περίπτωση εκθετικός στη διάσταση του δικτυώματος [60]. Οι ακριβείς αλγόριθμοι μπορούν να διακριθούν σε δύο μεγάλες κατηγορίες, πολυωνυμικού χώρου ακριβείς αλγόριθμους και εκθετικού χώρου ακριβείς αλγόριθμους.

   Α. Οι αλγόριθμοι της πρώτης κατηγορίας βασίζονται στην απαρίθμηση (enumeration), η οποία αναπτύχθηκε στις αρχές του 1980 με το έργο του Pohst [70], του Kannan [43] και των Fincke–Pohst [26]. Στην απλούστερη μορφή της η απαρίθμηση είναι απλά μία εξαντλητική αναζήτηση για τον καλύτερο ακέραιο συνδυασμό των διανυσμάτων βάσης του δικτυώματος. Ο καλύτερος ντετερμινιστικός αλγόριθμος απαρίθμησης είναι ο αλγόριθμος του Kannan με υπερ–εκθετική πολυπλοκότητα χειρότερης περίπτωσης και συγκεκριμένα, $n^{n/(2e)+o(n)}$ πράξεις πολυωνυμικού χρόνου [35], όπου το n δηλώνει τη διάσταση του δικτυώματος. Οι αλγόριθμοι απαρίθμησης που χρησιμοποιούνται στην πράξη, όπως αυτός των Schnorr και Euchner [76], έχουν ασθενέστερη προεπεξεργασία από τον αλγόριθμο του Kannan και πολυπλοκότητα χειρότερης περίπτωσης ίση με $2^{O(n^2)}$ πράξεις πολυωνυμικού χρόνου. Είναι όμως δυνατόν να επιτευχθούν σημαντικές επιταχύνσεις

χρησιμοποιώντας τεχνικές «κλαδέματος» (pruning). Το «κλάδεμα» εισήχθη από τους Schnorr–Euchner [76] και Schnorr–Hörner [77] τη δεκαετία του 1990 και πρόσφατα μελετήθηκε ξανά από τους Gama, Nguyen και Regev [27], όπου παρουσιάσθηκε ότι είναι εφικτή μία ευρετική επιτάχυνση της βασικής απαρίθμησης, της τάξης $2^{n/2}$.

Β. Οι ακριβείς αλγόριθμοι εκθετικού χώρου έχουν ασυμπτωτικά καλύτερο χρόνο εκτέλεσης, αλλά όλοι απαιτούν εκθετικό χώρο $2^{\Theta(n)}$. Ο πρώτος αλγόριθμος αυτού του είδους είναι ο τυχαιοποιημένος (randomized) αλγόριθμος κοσκινίσματος (sieving algorithm) των Ajtai, Kumar και Sivakumar, ο οποίος είναι ευρέως γνωστός ως AKS [14]. Ο αλγόριθμος AKS έχει εκθετική πολυπλοκότητα χειρότερης περίπτωσης με $2^{O(n)}$ πράξεις πολυωνυμικού χρόνου. Οι D.Micciancio και Βούλγαρης [57] παρουσίασαν πρόσφατα έναν εναλλακτικό ντετερμινιστικό αλγόριθμο, ο οποίος επιλύει τόσο το CVP, όσο και το SVP με $2^{2n+o(n)}$ πράξεις πολυωνυμικού χρόνου. Υπάρχουν αρκετές ευρετικές παραλλαγές του αλγόριθμου AKS [61, 58, 81] με χρόνο εκτέλεσης $2^{O(n)}$, όπου η σταθερά $O()$ είναι πολύ μικρότερη από ό, τι εκείνη των πιο γνωστών αποδείξιμων αλγορίθμων. Για παράδειγμα, ο πρόσφατος αλγόριθμος του Wang [82] έχει χρονική πολυπλοκότητα ίση με $2^{0.3836n}$ πράξεις πολυωνυμικού χρόνου.

2. **Προσεγγιστικοί αλγόριθμοι.** Αυτοί οι αλγόριθμοι είναι πολύ πιο γρήγοροι από ό, τι οι ακριβείς αλγόριθμοι, όμως παράγουν απλά βραχέα διανύσματα του δικτυώματος, όχι απαραίτητα το βραχύτερο από όλα: συνήθως παράγουν μία ολόκληρη ανηγμένη βάση, και ως εκ τούτου συγκαταλέγονται στους αλγόριθμους αναγωγής της βάσης ενός δικτυώματος. Ο πρώτος αλγόριθμος αυτού του είδους είναι ο περίφημος αλγόριθμος των Lenstra, Lenstra και Lovász, γνωστός ως LLL [48, 66], ο οποίος μπορεί να επιλύσει σε πολυωνυμικό χρόνο το SVP πρόβλημα κατά έναν παράγοντα $O((2/\sqrt{3})^n)$. Ο LLL αλγόριθμος μπορεί να θεωρηθεί ως μία αλγοριθμική εκδοχή της Ερμιτιανής ανισότητας. Από τότε που αναπτύχθηκε ο αλγόριθμος LLL, η έρευνα σε αυτήν την περιοχή έχει επικεντρωθεί σε δύο κυρίως θέματα, α) την παραγωγή ανηγμένων βάσεων παρόμοιας ποιότητας με αυτές από τον αλγόριθμο LLL, ενδεχομένως ελαφρώς χειρότερες, αλλά με μικρότερο χρόνο εκτέλεσης και β) την παραγωγή καλύτερων προσεγγιστικών παραγόντων από αυτόν του LLL, σε βάρος του χρόνου εκτέλεσης.

Και οι δύο κατηγορίες αλγορίθμων που αναφέραμε (ακριβείς–προσεγγιστικοί) είναι στην πραγματικότητα συμπληρωματικές· όλοι οι γνωστοί ακριβείς αλγόριθμοι πρώτα εφαρμόζουν έναν προσεγγιστικό αλγόριθμο (συνήθως τουλάχιστον τον LLL) ως

προεπεξεργασία, ενώ όλοι οι αλγόριθμοι που λειτουργούν κατά τμήματα (blockwise) καλούν σε χαμηλές διαστάσεις (στην πράξη, στις πρώτες 20 διαστάσεις) πολλές φορές έναν ακριβή αλγόριθμο ως υπορουτίνα. Οι περισσότεροι από τους SVP αλγόριθμους που αναφέραμε μπορούν να προσαρμοσθούν κατάλληλα ώστε να εφαρμοσθούν και στο CVP πρόβλημα [60].

Ο κρυπτογραφικός ρόλος των προβλημάτων βελτιστοποίησης σε δικτυώματα ακεραίων και ειδικά του SVP και του CVP είναι διττός. Κατά τα τελευταία χρόνια, αρκετά κρυπτογραφικά εργαλεία έχουν σχεδιαστεί σύμφωνα με τις αποδείξεις ασφαλείας, με την παραδοχή ότι δεν υπάρχει (τόσο πιθανολογικός, όσο και κβαντικός μερικές φορές) πολυωνυμικός αλγόριθμος για την επίλυση αυθαίρετων στιγμιοτύπων των παραλλαγών του SVP και του CVP. Η απόπειρα επίλυσης του SVP και του CVP επιτρέπει την αξιολόγηση της εγκυρότητας αυτών των παραδοχών. Από την άλλη πλευρά, ο πιο γνωστός αλγόριθμος για την παραβίαση αυτών των κρυπτογραφικών σχημάτων, καθώς επίσης και μια σειρά άλλων κρυπτογραφικών συναρτήσεων όπως κάποιες που βασίζονται στο πρόβλημα του σακιδίου [67] προσπαθούν να βρουν βραχέα ή εγγύς διανύσματα από ένα σχετικό δικτύωμα, ανάγοντας τη βάση του [36].

Στην υποενότητα αυτή, παρουσιάζουμε και αναλύουμε τις σημαντικότερες θεωρίες αναγωγής της βάσης ενός δικτυώματος ακέραιων αριθμών.

3.2.1 Αναγωγή βάσης στον R^2

Στο βιβλίο του «Διακριτή Αριθμητική», ο Γκάους περιέγραψε έναν αλγόριθμο αναγωγής μίας βάσης στις δύο διαστάσεις. Πρόκειται για μία απλή μέθοδο αναγωγής, η οποία αποτελεί, ουσιαστικά, επέκταση του Ευκλείδειου αλγόριθμου για την εύρεση του Μ.Κ.Δ. δύο ακεραίων. Στη σύγχρονη ορολογία, η έννοια της ανηγμένης κατά Gauss βάσης ορίζεται συνήθως ως εξής:

Ορισμός 3.2.1.1 Μία βάση a_1, α_2 ενός δικτυώματος είναι *ανηγμένη κατά Gauss*, εάν ικανοποιεί τις παρακάτω συνθήκες:

$$\|\alpha_1\| \leq \|\alpha_2\| \leq \|\alpha_1 - \alpha_2\| \leq \|\alpha_1 + \alpha_2\|$$

Ο Γκαουσιανός αλγόριθμος αναγωγής υπολογίζει μία ακολουθία βάσεων, οι οποίες ικανοποιούν την ακόλουθη ιδιότητα:

Ορισμός 3.2.1.2 Μία βάση a_1, a_2 ενός δικτυώματος είναι *καλώς διατεταγμένη* (well – ordered), εάν ικανοποιεί τις παρακάτω συνθήκες:

$$\|\alpha_1\| \leq \|\alpha_1 - \alpha_2\| < \|\alpha_2\|$$

Η μέθοδος αναγωγής κατά Gauss υπολογίζει τα δύο βραχύτερα διανύσματα του δικτυώματος και η αντίστοιχη ανηγμένη βάση αποτελείται από αυτά ακριβώς τα διανύσματα. Με άλλα λόγια, μία βάση $B = b_1, b_2, \dots, b_n$ ενός δικτυώματος L θεωρείται ανηγμένη κατά Gauss, εάν περιέχει τα δύο πρώτα διαδοχικά ελάχιστα του L.

Ο αλγόριθμος αναγωγής της βάσης ενός δισδιάστατου δικτυώματος L κατά Gauss δέχεται ως είσοδο ένα ζεύγος γραμμικά ανεξάρτητων διανυσμάτων (a, b) του L, τα οποία επεξεργάζεται σε τρία στάδια, την επιλογή ενός κατάλληλου ακέραιου μ έτσι ώστε να ελαχιστοποιείται η νόρμα $\|b - \mu\alpha\|$, τον έλεγχο της συνθήκης $\|a + b\| < \|a - b\|$ και τέλος, την ανταλλαγή των a και b. Η ανταλλαγή των διανυσμάτων παράγει είτε μία καλώς διατεταγμένη, είτε μία ανηγμένη βάση. Ο αλγόριθμος διασχίζει, κατά την έξοδο από το στάδιο της ανταλλαγής, μία ακολουθία καλώς διατεταγμένων βάσεων του δικτυώματος, ώσπου να παραχθεί μία ανηγμένη βάση. Ο τερματισμός αυτού του αλγόριθμου επιτυγχάνεται μετά από πεπερασμένο πλήθος βημάτων, διότι η νόρμα των διανυσμάτων της βάσης μειώνεται σε κάθε επανάληψη, εκτός από την τελευταία. Προκειμένου να έχουμε έναν καλώς ορισμένο αλγόριθμο, είναι απαραίτητο στο στάδιο 1 να επιλέξουμε το μικρότερο ακέραιο μ, ο οποίος ελαχιστοποιεί τη νόρμα $\|b - \mu\alpha\|$. [42]. Η γενική μορφή του Γκαουσιανού αλγόριθμου παρατίθεται στο Παράρτημα Α1.

Στις επόμενες υποενότητες αυτού του κεφαλαίου, περιγράφονται οι πιο σημαντικές προσπάθειες που έχουν γίνει, ώστε αυτή η ιδέα αναγωγής της βάσης και ο αντίστοιχος αλγόριθμος να γενικευθούν σε υψηλότερες διαστάσεις. Σε αυτές συγκαταλέγονται η Ερμιτιανή μέθοδος αναγωγής, η αναγωγή κατά Minkowski, κατά Korkine–Zolotarev, ο περίφημος LLL αλγόριθμος με τις διάφορες παραλλαγές του, αλλά και ο αλγόριθμος του Seysen για αναγωγή της βάσης ενός δικτυώματος με ταυτόχρονη αναγωγή και του δυϊκού του δικτυώματος.

3.2.2 Αναγωγή κατά Minkowski

Ορισμός 3.2.2.1 Μία βάση $B = b_1, b_2, \dots, b_n$ ενός δικτυώματος L θεωρείται ανηγμένη κατά Minkowski, εάν ισχύουν οι ακόλουθες παραδοχές:

- ✓ Το b_1 είναι το βραχύτερο, μη μηδενικό διάνυσμα στο L.

- ✓ Για $2 \leq i \leq n$, το b_i είναι το βραχύτερο διάνυσμα στο L, τέτοιο ώστε τα $b_1, b_2, \dots, b_i$ να μπορούν να επεκταθούν σε μία βάση του L.

Μία ανηγμένη κατά Minkowski βάση ενός δικτυώματος L θα περιέχει πάντοτε το βραχύτερο, μη μηδενικό διάνυσμα σε αυτό. Τα επόμενα διανύσματα b_i της βάσης επιλέγονται βάσει του βραχύτερου διανύσματος στο δικτύωμα L, το οποίο δεν αποτελεί γραμμικό συνδυασμό των ήδη επιλεγμένων $b_1, b_2, \dots, b_{i-1}$. Εάν $b_i = \sum_{j=1}^{i-1} z_j b_j$, $z_j \in \mathbb{Z}$, τότε θα ήταν αδύνατο να επεκταθούν τα $b_1, b_2, \dots, b_i$ ώστε να αποτελέσουν μία βάση του δικτυώματος L [47].

3.2.3 Ο αλγόριθμος LLL

Ο αλγόριθμος των Lenstra–Lenstra–Lovász, γνωστός ως LLL, είναι ένας πολυωνυμικού χρόνου αλγόριθμος αναγωγής της βάσης ενός δικτυώματος, ο οποίος εφευρέθηκε το 1982 από τους Hendrik Lenstra, Arjen Lenstra και Laszlo Lovász. Αρχικά χρησιμοποιήθηκε για την παραγοντοποίηση πολυωνύμων με ρητούς συντελεστές σε ανάγωγα πολυώνυμα, για την εύρεση τυχαίων ρητών προσεγγίσεων σε πραγματικούς αριθμούς και για την επίλυση του προβλήματος του ακέραιου γραμμικού προγραμματισμού σε σταθερές διαστάσεις.

Ορισμός 3.2.3.1 Μία βάση $B = b_1, b_2, \dots, b_n$ ενός δικτυώματος L είναι **LLL–ανηγμένη,** εάν:

- ✓ $|\mu_{i,j}| \leq \frac{1}{2}$ για $1 \leq j < i \leq n$ **(1)**
- ✓ $|b_i^*| \geq (\frac{3}{4} - \mu_{i,i-1}^2)\, |b_{i-1}^*|^2$

  για $1 \leq j < i \leq n$ **(2)**

- Στην πρώτη συνθήκη, $\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$
- Η δεύτερη συνθήκη είναι γνωστή ως **συνθήκη του Lovász**
- Η σταθερά $\frac{3}{4}$ μπορεί να πάρει οποιαδήποτε τιμή στο $[\frac{1}{4}, 1]$

Περιγραφή Αλγορίθμου LLL

Είσοδος: Μία αυθαίρετη βάση ενός δικτυώματος

Έξοδος: Μία ανηγμένη βάση του ίδιου δικτυώματος

Χρειαζόμαστε μία **ορθογώνια** βάση για να ελέγξουμε τις ιδιότητες της LLL–ανηγμένης βάσης. Έτσι, αρχικά εφαρμόζουμε ορθογωνιοποίηση Gram–Schmidt στην αυθαίρετη βάση και στη συνέχεια, ο αλγόριθμος τροποποιεί κατάλληλα (αναγωγή – ανταλλαγή) τα στοιχεία της βάσης ώστε να έχουν τις επιθυμητές ιδιότητες.

Ο αλγόριθμος LLL αποτελείται, δηλαδή, από τρία στάδια:

1. Ορθογωνιοποίηση Gram–Schmidt
2. Αναγωγή της βάσης του δικτυώματος
3. Ανταλλαγή

Ορθογωνιοποίηση Gram–Schmidt

Δοθείσης μιας αυθαίρετης βάσης b_1, ..., b_n, n–διάστατου δ.χ. V, ο αλγόριθμος Gram–Schmidt κατασκευάζει μια **ορθογώνια** βάση v_1, ..., v_n, για τον V.

1. Θέτω $v_1 = b_1$

2. Θέτω $v_2 = b_2 - \frac{\langle b_2, v_1 \rangle}{\|v_1\|^2} \cdot v_1$

3. Θέτω $v_3 = b_3 - \frac{\langle b_3, v_1 \rangle}{\|v_1\|^2} \cdot v_1 - \frac{\langle b_3, v_2 \rangle}{\|v_2\|^2} \cdot v_2$

……

n. Θέτω $v_n = b_n - \frac{\langle b_n, v_1 \rangle}{\|v_1\|^2} \cdot v_1 - \ldots - \frac{\langle b_n, v_{n-1} \rangle}{\|v_{n-1}\|^2} \cdot v_{n-1}$

Αναγωγή της βάσης του δικτυώματος

Η αναγωγή της βάσης (reduction) γίνεται σύμφωνα με τον τύπο: $b_i = b_i - \mathbf{r}\, b_{i-1}$ όπου **r** ο πλησιέστερος ακέραιος στο $\mu_{i,\, i-1}$.

Ανταλλαγή

Η ανταλλαγή (swap) γίνεται ανταλλάσσοντας τη στήλη b_i με την προηγούμενη, δηλαδή swap $b_{i-1} \leftrightarrow b_i$.

Χρόνος Εκτέλεσης του αλγορίθμου LLL

Δοθείσης μίας βάσης με n–διαστάσεων ακέραιες συντεταγμένες, για ένα δικτύωμα L στον $\mathbb{R}^{\boldsymbol{n}}$, ο αλγόριθμος LLL εξάγει μια LLL–ανηγμένη (σχεδόν ορθογώνια) βάση του L σε χρόνο $O(d^5 n \log^3$ B), όπου B είναι το μεγαλύτερο μήκος των b_i στην Ευκλείδεια νόρμα.

Παράδειγμα

Έστω μία βάση B = b_1, b_2, b_3 στον $\mathbb{R}^3$, η οποία δίνεται από τις στήλες του πίνακα

$$\begin{matrix} 1 & -1 & 3 \\ 1 & 0 & 5 \\ 1 & 2 & 6 \end{matrix}$$

Αρχικά, εφαρμόζουμε ορθογωνιοποίηση Gram–Schmidt.

Θα είναι: $b_1{}^* = b_1 = (1,1,1)$ και $B_1 = \|b_1{}^*\|^2 = (b_1{}^*, b_1{}^*) = 3.$

Από τον τύπο $\mu_{i,j} = \frac{\langle b_i, b_j{}^* \rangle}{\|b_j{}^*\|^2}$, θα έχουμε: $\mu_{2,1} = \frac{\langle b_2, b_1{}^* \rangle}{\|b_1{}^*\|^2} = \frac{(-1,0,2)(1,1,1)}{(1,1,1)(1,1,1)} = \frac{1}{3}$

$b_2{}^* = b_2 - \mu_{2,1} \cdot b_1{}^* = (-1,\ 0,\ 2) - \frac{1}{3} \cdot (1,\ 1,\ 1) = (-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3})$

Έτσι: $B_2 = (b_2{}^*, b_2{}^*) = (-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3})(-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3}) = \frac{14}{3}$

Στη συνέχεια:

- $b_3{}^* = b_3 - \mu_{3,1} \cdot b_1{}^* - \mu_{3,2} \cdot b_2{}^*$
- $\mu_{3,1} = \frac{\langle b_3, b_1{}^* \rangle}{\|b_1{}^*\|^2} = \frac{(3,5,6)(1,1,1)}{(1,1,1)(1,1,1)} = \frac{14}{3}$
- $\mu_{3,2} = \frac{\langle b_3, b_2{}^* \rangle}{\|b_2{}^*\|^2} = \frac{(3,5,6)(-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3})}{(-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3})(-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3})} = \frac{13}{14}$
- $b_3{}^* = (3,5,6) - \frac{14}{3} \cdot (1,\ 1,\ 1) - \frac{13}{14} \cdot (-\frac{4}{3}, -\frac{1}{3}, \frac{5}{3}) = (-\frac{18}{42},\ \frac{27}{42}, -\frac{9}{42})$
- Έτσι: $B_3 = (b_3{}^*, b_3{}^*) = \frac{9}{14}$

Ακολουθεί η αναγωγή της βάσης, όπου μειώνεται το b_3, επειδή τα $\mu_{3,1}$ και $\mu_{3,2}$ δεν ικανοποιούν τη συνθήκη του Lovász, $|\mu_{i,j}| \leq \frac{1}{2}$.

Έτσι έχουμε: $\mu_{3,2} = \frac{13}{14}$, άρα r = $\lceil \mu_{3,2} \rceil = \left\lceil \frac{13}{14} \right\rceil = 1$ και

$$b_3 = b_3 - \mathbf{1} \cdot b_2 = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix} - \mathbf{1} \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix}$$

Άρα, ο αρχικός πίνακας γίνεται → $\begin{matrix} 1 & -1 & 4 \\ 1 & 0 & 5 \\ 1 & 2 & 4 \end{matrix}$

Τέλος, στο βήμα της ανταλλαγής, αντιμεταθέτουμε τις στήλες 2 και 3 (εάν δουλεύαμε στον $\mathbb{R}^4$ θα αλλάζαμε τις στήλες 3–4 κ.ο.κ, πάντα όμως με βάση τις δύο συνθήκες της lll–ανηγμένης βάσης)

Έτσι, ο πίνακας τώρα γίνεται → $\begin{matrix} 1 & 4 & -1 \\ 1 & 5 & 0 \\ 1 & 4 & 2 \end{matrix}$

Μπορούμε εύκολα να διαπιστώσουμε ότι η βάση που προέκυψε με την πρώτη εκτέλεση του αλγορίθμου δεν είναι ανηγμένη. Συνεπώς, εφαρμόζουμε από την αρχή τα βήματα του αλγορίθμου και καταλήγουμε τελικά στην **ανηγμένη βάση** → $\begin{matrix} 0 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{matrix}$

Στην επόμενη υποενότητα, παρουσιάζονται δύο παραλλαγές του LLL αλγορίθμου. Μία απλή υλοποίηση αυτού του αλγόριθμου σε ψευδογλώσσα υπάρχει στο Παράρτημα Α2.

3.2.4 Παραλλαγές του LLL: modified LLL και Fincke–Pohst

Στην υποενότητα αυτή περιγράφονται δύο σημαντικές παραλλαγές του αλγόριθμου LLL, ο τροποποιημένος LLL αλγόριθμος του M.Pohst – 1987 [10] και ο αλγόριθμος των Fincke–Pohst [26] για τον υπολογισμό διανυσμάτων μικρού μήκους σε ένα δικτύωμα.

Τροποποιημένος LLL αλγόριθμος (modified LLL algorithm) του M.Pohst (1987)

Δοθέντος ενός m × n πίνακα W πραγματικών αριθμών, του οποίου οι στήλες (όχι απαραίτητα γραμμικά ανεξάρτητες) παράγουν ένα δικτύωμα $L \subset \mathbb{R}^m$, ο αλγόριθμος αυτός βρίσκει –σε πολυωνυμικό χρόνο– μία ανηγμένη βάση για το L και μία (ανηγμένη) βάση για τον πυρήνα της απεικόνισης (kernel of a –linear– map) $W: \mathbb{Z}^n \rightarrow \mathbb{Z}^m$. Με τον όρο «πυρήνα της αντιστοίχισης» εννοούμε το σύνολο όλων των διανυσμάτων που αντιστοιχούν στο μηδενικό διάνυσμα.

Εναλλακτικά μπορούμε να πούμε ότι, δοθέντος του θετικού ημιορισμένου Gram πίνακα ενός συνόλου διανυσμάτων $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ που παράγει ένα δικτύωμα L, ο αλγόριθμος αυτός βρίσκει μία ανηγμένη βάση για το L (η οποία εκφράζεται ως γραμμικοί συνδυασμοί των διανυσμάτων b_i) και μία ανηγμένη βάση για το δικτύωμα των σχέσεων $\{(r_1, r_2, \dots, r_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} r_i\, b_i = 0\}$. Για τον αλγόριθμο αυτόν υπάρχει και μία καθαρή έκδοση για ακέραιους αριθμούς.

Αλγόριθμος Fincke–Pohst (1985)

Ο αλγόριθμος των Fincke–Pohst (1985) αποτελεί μία σημαντική παραλλαγή του αρχικού LLL αλγόριθμου και έχει ως εξής: Δοθέντος ενός δικτυώματος $L = (\mathbb{Z}^n,\ Q)$ και μίας σταθεράς $C > 0$, ο αλγόριθμος βρίσκει –σε εκθετικό χρόνο– όλα τα $x \in \mathbb{Z}^n$, τέτοια ώστε $Q(x) < C$. Παρά την εκθετική πολυπλοκότητα χρόνου που έχει αυτός ο αλγόριθμος, λειτουργεί καλά σε πολλές πρακτικές καταστάσεις.

Ο καλύτερος τρόπος για να προσδιοριστούν με βεβαιότητα τα βραχύτερα, μη μηδενικά διανύσματα σε ένα δικτύωμα L είναι, χρησιμοποιώντας τον αλγόριθμο LLL να βρούμε τη νόρμα C του βραχύτερου διανύσματος βάσης σε μία ανηγμένη βάση και έπειτα, να χρησιμοποιήσουμε τον αλγόριθμο–παραλλαγή των Fincke–Pohst για να αναζητήσουμε βραχύτερα διανύσματα στο δικτύωμα L, εάν υπάρχουν.

3.2.5 Αναγωγή κατά Hermite και Korkin–Zolotarev

Ορισμός 3.2.5.1 Μία βάση $B = b_1, b_2, \dots, b_n$ ενός δικτυώματος L θεωρείται ανηγμένη κατά *Hermite* (ή size–reduced), εάν η Gram–Schmidt ορθογωνιοποίησή της ικανοποιεί τη συνθήκη $v_{i,j} \leq \frac{1}{2}$, για $1 \leq i < j \leq n$ ή με άλλα λόγια, εάν η QR παραγοντοποίησή της ικανοποιεί τη συνθήκη $|r_{i,i}| \geq 2|r_{i,j}|$ για $1 \leq j < i \leq n$. [49]. Η QR παραγοντοποίηση είναι ουσιαστικά η διαδικασία Gram–Schmidt με το αποτέλεσμά της σε μορφή πίνακα.

Η αναγωγή της βάσης ενός δικτυώματος κατά Korkin–Zolotarev, γνωστή και ως KZ – αναγωγή [45] αποτελεί μία παραλλαγή της αναγωγής κατά Minkowski. Οι δύο μέθοδοι ομοιάζουν διότι απαιτούν, δεδομένης μίας βάσης του δικτυώματος $B = b_1, \dots, b_n$, όπου τα διανύσματα έχουν ταξινομηθεί κατά αύξουσα σειρά των Ευκλείδειων μηκών τους, το πρώτο διάνυσμα (b_1) να είναι το βραχύτερο, μη μηδενικό διάνυσμα της βάσης. Η διαφορά αυτών των δύο μεθόδων έγκειται στο γεγονός ότι, δεδομένης μίας βάσης του δικτυώματος $B = b_1, \dots, b_n$, η ανηγμένη κατά Minkowski βάση απαιτεί το b_i να είναι το βραχύτερο, μη μηδενικό, γραμμικά ανεξάρτητο από τα $b_1, \dots, b_{i-1}$ διάνυσμα της βάσης. Η προϋπόθεση αυτή δεν μπορεί πάντοτε να ισχύει, καθώς ενδέχεται τα πρώτα i βραχύτερα διανύσματα του δικτυώματος να είναι γραμμικά εξαρτημένα και συνεπώς να μην μπορούν να σχηματίσουν μία βάση του δικτυώματος. Έτσι, ενώ στην αναγωγή

κατά Minkowski τα διαδοχικά διανύσματα b_i της βάσης προστίθενται στη βάση του δικτυώματος μόνο εάν το b_i είναι το βραχύτερο, μη μηδενικό διάνυσμα το οποίο επιτρέπει την επέκταση της βάσης, στην αναγωγή κατά Korbin–Zolotarev τα διαδοχικά διανύσματα b_i της βάσης επιλέγονται βάσει του μήκους τους στο ορθογώνιο συμπλήρωμα του χώρου που παράγεται από τα προηγούμενα $b_1, \dots, b_{i-1}$ διανύσματα της βάσης [47].

Ο απαιτούμενος αριθμός των ελάχιστων διανυσμάτων τα οποία μπορούν να σχηματίσουν μία βάση του δικτυώματος είναι άγνωστος. Σύμφωνα με τον ορισμό των Korkin–Zolotarev, μία βάση $B = b_1, \dots, b_n$ ενός δικτυώματος L θεωρείται ότι είναι ανηγμένη κατά Korkin–Zolotarev, εάν ικανοποιεί τις εξής συνθήκες:

1. Στο δικτύωμα που παράγεται από τη βάση $B = b_1, \dots, b_n$, το b_1 είναι το βραχύτερο, μη μηδενικό διάνυσμά του.

   Το b_i^* είναι το βραχύτερο, μη μηδενικό διάνυσμα στο δικτύωμα που παράγεται από τη βάση $B = b_1^*, \dots, b_n^*$, όπου τα $b_1^*, \dots, b_n^*$ είναι οι προβολές των διανυσμάτων $b_1, \dots, b_n$ στον κάθετο υπόχωρο των $b_1, \dots, b_{i-1}$.

3.2.6 Ο αλγόριθμος του Seysen

Το 1990, ο Martin Seysen [98] επιχειρώντας να βρει έναν καλύτερο τρόπο για ταυτόχρονη αναγωγή της βάσης ενός δικτυώματος και του δυϊκού του δικτυώματος, ανακάλυψε μία νέα μέθοδο αναγωγής, η οποία διαφέρει από αυτές που παρουσιάστηκαν στις προηγούμενες υποενότητες. Ο σκοπός της αναγωγής μίας βάσης ενός δικτυώματος ακεραίων κατά Seysen είναι να αναχθεί ταυτόχρονα η βάση τόσο του απλού δικτυώματος όσο και του δυϊκού του. Ο αλγόριθμος αυτός λαμβάνει υπ’ όψιν όλα τα διανύσματα ενός δικτυώματος ταυτόχρονα και εκτελεί (αριθμητικές) πράξεις σε εκείνα τα διανύσματα, τα οποία θα ανάγουν τη βάση του δικτυώματος σύμφωνα με κάποιο μέτρο. Υπενθυμίζουμε ότι ο αλγόριθμος LLL λειτουργεί τοπικά στο δικτύωμα τη βάση του οποίου επιχειρεί να ανάγει, πράγμα που σημαίνει ότι θα εκτελεί μόνο μία πράξη ανάμεσα σε δύο διανύσματα, γειτονικά το ένα στο άλλο στην ταξινομημένη βάση του δικτυώματος.

Στο σημείο αυτό ολοκληρώθηκε η παρουσίαση των πιο σημαντικών αλγορίθμων για αναγωγή της βάσης ενός δικτυώματος.

Κεφάλαιο 4
Κρυπτογραφικά Συστήματα Βασισμένα σε Δικτυώματα Ακεραίων

Τα κρυπτογραφικά συστήματα που βασίζονται σε δικτυώματα ακέραιων αριθμών άρχισαν να μελετούνται από το 1996 περίπου, με το πρωτοποριακό εύρημα του Miklos Ajtai σχετικά με μία μονόδρομη συνάρτηση, η οποία βασίζεται στη δυσκολία της χειρότερης περίπτωσης διαφόρων προβλημάτων που υπάρχουν σε δικτυώματα ακεραίων.

Στο κεφάλαιο αυτό παρουσιάζονται κάποια σημαντικά κρυπτοσυστήματα δημοσίου κλειδιού βασισμένα σε δικτυώματα ακεραίων, τα οποία στηρίχθηκαν στο αποτέλεσμα στο οποίο κατέληξε ο Ajtai, σχετικά με την ισοδυναμία της μέσης και της χειρότερης περίπτωσης σε ορισμένα προβλήματα δικτυωμάτων [11]. Αρχικά, γίνεται μία αναφορά στο κρυπτοσύστημα Ajtai – Dwork (AD), το πρώτο κρυπτοσύστημα της κρυπτογραφίας δημοσίου κλειδιού το οποίο βασίστηκε στο προαναφερθέν αποτέλεσμα ισοδυναμίας. Στη συνέχεια, αναφερόμαστε εκτενέστερα στο κρυπτοσύστημα Goldreich – Goldwasser – Halevi (GGH) και τέλος, στο NTRU, ένα διαφορετικό, όμως ιδιαίτερα ενδιαφέρον κρυπτοσύστημα δημοσίου κλειδιού. Εκτός από το AD κρυπτοσύστημα , στο οποίο υπάρχει μία αποδεδειγμένα άμεση σχέση μεταξύ αποκρυπτογράφησης του κρυπτογραφήματος και τον προσδιορισμό του βραχύτερου διανύσματος σε μία κατηγορία δικτυωμάτων, τα επιχειρήματα ότι αυτά τα κρυπτοσυστήματα είναι ασφαλή είναι κατά κύριο λόγο ευρετικά.

4.1 Το κρυπτοσύστημα AD

Το κρυπτοσύστημα Ajtai–Dwork είναι ένα πιθανολογικό κρυπτογραφικό σύστημα δημοσίου κλειδιού, το οποίο είναι ασφαλές, εκτός εάν η χειρότερη περίπτωση μίας ειδικής παραλλαγής του SVP προβλήματος (unique SVP) μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Πριν από μερικά χρόνια, στις πρωτοποριακές εργασίες του [11, 12], ο Miklos Ajtai έδειξε ότι το πρόβλημα SVP ήταν NP–hard πολυπλοκότητας και ανακάλυψε μία συναρπαστική σχέση μεταξύ της πολυπλοκότητας χειρότερης περίπτωσης και της

πολυπλοκότητας μέσης περίπτωσης ορισμένων ιδιαίτερα γνωστών προβλημάτων σε δικτυώματα και συγκεκριμένα του SVP προβλήματος.

Αυτό που έκανε ουσιαστικά ο M.Ajtai ήταν να εγκαθιδρύσει μία αναγωγή από το πρόβλημα της εύρεσης του βραχύτερου, μη μηδενικού διανύσματος–στοιχείου u σε ένα δικτύωμα, δεδομένου ότι αυτό είναι «μοναδικό», στο πρόβλημα της προσέγγισης του SVP, για τυχαία επιλεγμένα στιγμιότυπα συγκεκριμένης κλάσης δικτυωμάτων. Αυτή η αναγωγή βελτιώθηκε στο [13].

Με βάση αυτά τα αποτελέσματα, οι Ajtai και Dwork [13] δημιούργησαν ένα κρυπτοσύστημα δημοσίου κλειδιού η ασφάλεια του οποίου θα μπορούσε να αποδειχθεί χρησιμοποιώντας μόνο τη δυσκολία της χειρότερης περίπτωσης μιας συγκεκριμένης έκδοσης του SVP, καθιστώντας το με αυτόν τον τρόπο το πρώτο [20] αποτέλεσμα που έχει χρησιμοποιήσει τη δυσκολία της χειρότερης περίπτωσης για τη δημιουργία ασφαλών συστημάτων.

Στη συνέχεια, εμπνευσμένοι από το εύρημα του Ajtai, εκείνος και η C.Dwork πρότειναν, το 1997, ένα κρυπτοσύστημα αποδεδειγμένα ασφαλές, με την παραδοχή ότι το πρόβλημα του «μοναδικού» βραχύτερου διανύσματος στο δικτύωμα είναι υπολογιστικά δύσκολο στη χειρότερη περίπτωση. Το κρυπτοσύστημα Ajtai–Dwork είναι αποδεδειγμένα ασφαλές, εάν ένα πρόβλημα συγκεκριμένου δικτυώματος είναι δύσκολο στη χειρότερη περίπτωση.

Από θεωρητικής άποψης, το επίτευγμα των Ajtai – Dwork είναι ιδιαίτερα σημαντικό. Ωστόσο, η πρακτική σημασία του είναι ασαφής. Αυτό οφείλεται εν μέρει στο γεγονός, το οποίο έγινε φανερό από τον αλγόριθμο RSA, ότι η επιτυχία ενός κρυπτοσυστήματος δεν εξαρτάται μόνο από την υπολογιστική δυσκολία του προβλήματος επί του οποίου βασίζεται, αλλά και από τις επιδόσεις που εμφανίζει όσον αφορά την ταχύτητα, το μέγεθος του κλειδιού, το ρυθμό επέκτασης (expansion rate) και άλλα χαρακτηριστικά. Η μη πρακτικότητα του κρυπτοσυστήματος Ajtai–Dwork σχετίζεται επίσης με το γεγονός ότι, μέχρι σήμερα, η χρήση των δικτυωμάτων στην κρυπτογραφία έχει κατευθυνθεί σε σχήματα επιτυχώς κρυπταναλυτικά [98].

Οι P.Nguyen και J.Stern, το 1998, κρυπτανέλυσαν το διάσημο αυτό κρυπτοσύστημα, παρουσιάζοντας μία ευρετική επίθεση για την ανάκτηση του ιδιωτικού κλειδιού. Πληθώρα πειραμάτων με αυτήν την επίθεση έχει έκτοτε διεξαχθεί, από τα οποία έχουν εξαχθεί πολύτιμα συμπεράσματα. Μερικά από αυτά είναι ότι, προκειμένου να εξασφαλιστεί η ασφάλεια του κρυπτοσυστήματος Ajtai–Dwork, οι υλοποιήσεις του

απαιτούν πολύ μεγάλο μήκος κλειδιών, καθιστώντας το έτσι μη πρακτικό/μη λειτουργικό σε ένα πραγματικό περιβάλλον.

Μία εκτενέστερη ανάλυση της επίθεσης αυτής είναι εκτός του σκοπού της παρούσης εργασίας.

4.2 Το κρυπτοσύστημα GGH

Το κρυπτοσύστημα αυτό δημιουργήθηκε το 1996 από τους Oded Goldreich, Shafi Goldwasser και Shai Halevi και παρουσιάστηκε στο [31] το 1997. Το κρυπτοσύστημα Goldreich–Goldwasser–Halevi, το οποίο είναι γνωστό ως GGH, είναι ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού, το οποίο στηρίζεται σε προβλήματα δικτυωμάτων ακέραιων αριθμών. Συγκεκριμένα, το GGH είναι βασισμένο στη δυσκολία του προβλήματος εύρεσης του εγγύτερου εξωτερικού διανύσματος σε ένα εσωτερικό διάνυσμα ενός δικτυώματος ακέραιων αριθμών.

Η γενική αρχή λειτουργίας του κρυπτοσυστήματος GGH έχει ως εξής: το δημόσιο κλειδί είναι μια «κακή» βάση ενός δικτυώματος (δηλαδή μια βάση με μεγάλα διανύσματα), ενώ το ιδιωτικό κλειδί είναι η ανηγμένη βάση του ίδιου δικτυώματος (δηλαδή μια βάση με μικρά, σχεδόν ορθογώνια μεταξύ τους διανύσματα), η οποία και καθιστά εφικτή την αποδοτική επίλυση συγκεκριμένων στιγμιοτύπων του CVP προβλήματος.

Για την κρυπτογράφηση του μηνύματος, σε γενικές γραμμές, παίρνουμε ένα σημείο του δικτυώματος που ανταποκρίνεται στο απλό κείμενο και εφαρμόζουμε επάνω του μια μικρή τυχαία διαταραχή, έτσι ώστε να πάρουμε ένα σημείο εκτός του δικτυώματος, του οποίου το πλησιέστερο σημείο στο δικτύωμα να είναι το σημείο του απλού κειμένου. Άρα τα κρυπτοκείμενα είναι στιγμιότυπα του CVP και η ασφάλεια του ιδιωτικού κλειδιού εξαρτάται από τη δυσκολία της εύρεσης μιας αρκετά ανηγμένης βάσης του δικτυώματος. Το GGH χρησιμοποιεί μια μονόδρομη συνάρτηση κερκόπορτας που στηρίζεται στην δυσκολία αναγωγής της βάσης του δικτυώματος. Η ιδέα που περιλαμβάνεται σε αυτήν τη συνάρτηση κερκόπορτας είναι ότι, δεδομένης οποιασδήποτε βάσης για ένα δικτύωμα , είναι εύκολο να παραχθεί ένα διάνυσμα το οποίο να είναι κοντά σε ένα σημείο του δικτυώματος, για παράδειγμα, παίρνοντας ένα σημείο του δικτυώματος και προσθέτοντας ένα μικρό διάνυσμα σφάλματος. Αλλά για την επιστροφή

από αυτό το εσφαλμένο διάνυσμα στο αρχικό σημείο του δικτυώματος είναι απαραίτητη μια ειδική βάση [98].

Λειτουργία του κρυπτοσυστήματος GGH

Όπως έχουμε δει, το GGH περιλαμβάνει ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Το ιδιωτικό κλειδί είναι μία βάση B ενός δικτυώματος με καλές ιδιότητες (όπως μικρά, σχεδόν ορθογώνια διανύσματα) και έναν πίνακα U με ορίζουσα ίση με τη μονάδα. Το δημόσιο κλειδί είναι μια άλλη βάση του δικτυώματος της μορφής $B' = U \times B$. Για κάποιο επιλεγμένο μήνυμα M, ο χώρος μηνυμάτων αποτελείται από το διάνυσμα $\lambda_1, \lambda_2, \dots, \lambda_n$ εντός του εύρους $-M \leq \lambda_i \leq M$.

Κρυπτογράφηση του κρυπτοσυστήματος GGH

Δοθέντος ενός μηνύματος $m = (\lambda_1, \lambda_2, \dots, \lambda_n)$, ενός σφάλματος e και ενός δημόσιου κλειδιού B', υπολογίζουμε το $v = \sum \lambda_i \; b_i'$. Με σημειολογία πινάκων, αυτό είναι $v = m \times B'$. Υπενθυμίζουμε ότι το m αποτελείται από ακέραιες τιμές και ότι το b' είναι ένα σημείο του δικτυώματος, συνεπώς και το v θα είναι ένα σημείο δικτυώματος. Το κρυπτογράφημα c είναι τότε $c = v + e = m \times B' + e$.

Αποκρυπτογράφηση του κρυπτοσυστήματος GGH

Για την αποκρυπτογράφηση του κρυπτοκειμένου, αρκεί να υπολογίσουμε το εξής:

$$c \times B^{-1} = (m \times B' + e) \times B^{-1} = m \times B' \times B^{-1} + e \times B^{-1} =$$

$$m \times U \times B \times B^{-1} + e \times B^{-1} = m \times U + e \times B^{-1} .$$

Στο σημείο αυτό χρησιμοποιούμε μία τεχνική στρογγυλοποίησης, την τεχνική Babai (Babai's rounding technique) για την απομάκρυνση του όρου $e \times B^{-1}$, εφόσον βέβαια ο όρος αυτός είναι αρκετά μικρός. Ουσιαστικά, απλά αντικαθιστούμε τις ρητές συντεταγμένες του διανύσματος με τους πλησιέστερους σε αυτές ακέραιους αριθμούς. Τέλος, υπολογίζουμε το $m = m \times U \times U^{-1}$ για να ανακτήσουμε το αρχικό μήνυμα.

Παράδειγμα

Έστω ότι έχουμε ένα δικτύωμα δύο διαστάσεων $L \subseteq \mathbb{R}^2$.

Η βάση B του δικτυώματος L είναι $B = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$ και $B^{-1} = \begin{pmatrix} 1/3 & 0 \\ 0 & 1/5 \end{pmatrix}$.

Επιλέγουμε έναν πίνακα U με ορίζουσα ίση με ± 1, έστω τον $U = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$.

Άρα, $U^{-1} = \begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix}$. Στη συνέχεια, υπολογίζουμε τη $B' = U \times B = \begin{pmatrix} 6 & 5 \\ 15 & 15 \end{pmatrix}$.

Έστω ότι το μήνυμα είναι $m = (-1, 6)$ και το διάνυσμα λάθους είναι $e = (-1, 1)$.

Τότε, το κρυπτοκείμενο θα είναι $c = m \times B' + e = (84, 85) + (-1, 1) = (83, 86)$.

Για την αποκρυπτογράφηση του μηνύματος θα πρέπει να υπολογίσουμε το $c \times B^{-1}$.

$c \times B^{-1} = (\frac{83}{3}, \frac{86}{5})$. Το διάνυσμα αυτό, αφού στρογγυλοποιηθεί, γίνεται $(28, 17)$ και τελικά, ανακτάται το μήνυμα ως εξής: $m = (28, 17)U^{-1} = (-1, 6)$.

Το σύστημα κρυπτογράφησης GGH κρυπταναλύθηκε το 1999 από τον Phong Q. Nguyen, όμως η υποκείμενη μαθηματική ιδέα μπορεί να παράγει καινούρια κρυπτοσυστήματα.

4.3 Το κρυπτοσύστημα NTRU

Το κρυπτοσύστημα NTRU [39] είναι ένα σχετικά νέο σύστημα, το οποίο δημιουργήθηκε το 1998 από τρεις μαθηματικούς, τους J. Hoffstein, J. Pipher και J.H.Silverman. Η ονομασία του προέρχεται από τις λέξεις «**N**th Degree **T**runcated Polynomial **R**ing **U**nits», δηλαδή «μονάδες περικομμένου πολυωνυμικού δακτυλίου n–οστού βαθμού». Κάποιες εναλλακτικές ονομασίες που έχουν αποδοθεί στο σύστημα NTRU είναι: «**N**umber **T**heorist **R**esearch **U**nit» ή «**N**umber **T**heorists a**R**e **U**s». Το κρυπτοσύστημα NTRU είναι στην πραγματικότητα μία παραμετροποιημένη οικογένεια κρυπτοσυστημάτων δημοσίου κλειδιού, κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας από την εταιρεία NTRU Cryptosystems, η οποία πρόσφατα έχει γίνει μέρος της Security Innovations, κορυφαίας εταιρείας στην παροχή λύσεων σχετικών με την ασφάλεια ενός συστήματος.

Το NTRU είναι ένα πιθανοτικό κρυπτοσύστημα. Η διαδικασία κρυπτογράφησης περιλαμβάνει ένα τυχαίο στοιχείο και ως εκ τούτου ένα μήνυμα έχει πολλές πιθανές κρυπτογραφήσεις. Αρχικά, το κρυπτοσύστημα αυτό ορίστηκε από την άποψη των πολυωνυμικών δακτυλίων. Ωστόσο, το NTRU μπορεί να περιγραφεί χρησιμοποιώντας

και κάποιους ειδικούς τύπους δικτυωμάτων ακέραιων αριθμών. Το κρυπτοσύστημα NTRU αποτελείται από δύο αλγορίθμους:

1. τον NTRUEncrypt αλγόριθμο, ο οποίος χρησιμοποιείται για τη διαδικασία της κρυπτογράφησης, και
2. τον NTRUSign αλγόριθμο, ο οποίος χρησιμοποιείται για τις ψηφιακές υπογραφές.

Οι αλγόριθμοι αυτοί έχουν αξιοσημείωτη ταχύτητα λειτουργίας και μέγεθος κλειδιού και βασίζονται σε δύσκολα προβλήματα που είναι φαινομενικά δυσεπίλυτα. Σε αντίθεση με άλλα δημοφιλή κρυπτοσυστήματα δημοσίου κλειδιού, το NTRU ανθίσταται σε επιθέσεις που χρησιμοποιούν τον αλγόριθμο του Shor και έχει δειχθεί ότι η απόδοσή του είναι σημαντικά καλύτερη. Για το λόγο αυτό, αποτελεί μία κορυφαία εναλλακτική λύση των αλγορίθμων RSA και ελλειπτικών καμπυλών (ECC). Η ασφάλεια του κρυπτοσυστήματος NTRU βασίζεται στη δυσκολία της εξεύρεσης μικρών διανυσμάτων σε ένα συγκεκριμένο δικτύωμα. Όσο μεγαλύτερη είναι η παράμετρος N (βαθμός των πολυωνύμων του δακτυλίου), τόσο πιο ασφαλές είναι το σύστημα.

Το πλεονέκτημα του NTRU έναντι άλλων κρυπτοσυστημάτων είναι ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι πολύ γρήγορη και τα μεγέθη του κλειδιού είναι σχετικά μικρά. Επίσης, η δημιουργία του κλειδιού είναι γρήγορη και εύκολη [39]. Υπάρχουν διάφορες διαθέσιμες υλοποιήσεις του κρυπτοσυστήματος NTRU, τόσο ιδιόκτητες όσο και εφαρμογές ανοιχτού κώδικα.

4.3.1 Ο αλγόριθμος NTRUEncrypt

Ο αλγόριθμος κρυπτογράφησης του NTRU, επίσης γνωστός και ως κρυπτοσύστημα NTRUEncrypt, είναι μία βασισμένη σε δικτύωμα εναλλακτική σε σχέση με τους αλγορίθμους RSA και ECC. Όπως προαναφέρθηκε, το κρυπτοσύστημα αυτό ορίστηκε αρχικά από την άποψη των πολυωνυμικών δακτυλίων και με αυτόν τον τρόπο θα το περιγράψουμε σε αυτήν την υποενότητα. Συγκεκριμένα, το NTRUEncrypt λειτουργεί στον περικομμένο δακτύλιο πολυωνύμων που δίνεται από τον τύπο $R = \frac{\mathbb{Z}[x]}{x^N-1}$., όπου ο N είναι πρώτος (prime) αριθμός. Ένα στοιχείο $F \in R$ θα γραφεί ως πολυώνυμο ή ως διάνυσμα: $F = \sum_{i=0}^{N-1} f_i x^i = [F_0, F_1, \dots, F_{N-1}]$

Οι αριθμητικές πράξεις που γίνονται στον προαναφεθέντα πολυωνυμικό δακτύλιο R είναι η πρόσθεση (addition) και ο πολλαπλασιασμός συνέλιξης (convolution multiplication). Τόσο οι παραπάνω πράξεις, όσο και όλα τα πολυώνυμα του δακτυλίου έχουν ακέραιους συντελεστές και βαθμό το πολύ $N-1$:

$$\mathrm{a} = \alpha_0 + \alpha_1 X + a_2 X^2 + \cdots + a_{N-2} X^{N-2} + a_{N-1} X^{N-1}$$

Έστω ότι έχουμε έναν ακέραιο $N \geq 1$, δύο μοδιακά (moduli) p και q και τους πολυωνυμικούς δακτυλίους $R = \frac{\mathbb{Z}[x]}{x^N-1}$, $R_p = \frac{\mathbb{Z}_p[x]}{x^N-1}$ και $R_q = \frac{\mathbb{Z}_q[x]}{x^N-1}$.

Ορίζουμε: $T\ (d_1, d_2) = \begin{cases} & d_1\ \textit{συντελεστές ίσοι με } 1 \\ a\ (x) \in R: & d_2\ \textit{συντελεστές ίσοι με } -1 \\ & \textit{όλοι οι άλλοι συντελεστές ίσοι με } 0 \end{cases}$

Μπορούμε τώρα να περιγράψουμε το κρυπτοσύστημα NTRUEncrypt ως εξής:

Παράμετροι

Επιλέγουμε τα (N, p, q, d), έτσι ώστε τα N και p να είναι πρώτοι αριθμοί (prime numbers) και να ισχύουν επίσης οι ακόλουθες συνθήκες:

1. $M.K.\Delta\ (p, q) = M.K.\Delta\ (N, q) = 1$ και
2. $q > (6d+1)p$

Δημιουργία κλειδιών

Αρχικά, επιλέγουμε τυχαία δύο «μικρά» πολυώνυμα f και g, τα οποία διατηρούμε ιδιωτικά. Για τα πολυώνυμα αυτά θα πρέπει να ισχύει $f(x) \in T\ (d+1, d)$ και $g(x) \in T\ (d, d)$. Με τον όρο «τυχαία», εννοούμε ότι οι συντελεστές τους θα πρέπει να είναι τυχαία κατανεμημένοι στο σύνολο p ή στο q και με τον όρο «μικρά», ότι θα πρέπει να είναι πολύ μικρότεροι από το p ή το q. Έστω ότι:

- $F_q(x)$ είναι η αντίστροφη της $f(x)$ στο δακτύλιο R_q και
- $F_p(x)$ είναι η αντίστροφη της $f(x)$ στο δακτύλιο R_p.

Τότε, το ιδιωτικό κλειδί θα είναι η $f(x)$, ενώ το δημόσιο κλειδί θα υπολογίζεται από τον τύπο $h(x) = F_q(x) \cdot g(x)$.

Κρυπτογράφηση

Κωδικοποιούμε το απλό κείμενο m ως $m(x) \in R_p$ και επιλέγουμε ένα τυχαίο, εφήμερο (ephemeral) κλειδί $r(x)$, τέτοιο ώστε $r(x) \in T\ (d, d)$. Τότε, το κρυπτοκείμενο (ciphertext) θα δίνεται από τον τύπο: $e(x) = p \cdot r(x) \cdot h(x) + m(x)\ (mod\ q)$

Αποκρυπτογράφηση

Για την αποκρυπτογράφηση του κρυπτοκειμένου, εκτελούμε τις παρακάτω πράξεις:

- $a(x) \equiv f(x) \cdot e(x)\ (mod\ q) \in R_q$
- $m(x) \equiv F_p(x) \cdot a(x)\ (mod\ p)$–αφού προηγηθεί center–lift $a(x)(mod\ q) \in R$

Στη συνέχεια, ακολουθεί ένα αριθμητικό παράδειγμα για τον κρυπταλγόριθμο NTRUEncrypt, προκειμένου να καταστεί πιο κατανοητή η λειτουργία του. Έστω ότι $N = 11,\ p = 3$ και $q = 32$, οπότε τα πολυώνυμα f και g έχουν βαθμό το πολύ 10. Οι παράμετροι του συστήματος (N, p, q) είναι δημόσια γνωστές. Τα πολυώνυμα επιλέγονται τυχαία, οπότε ας υποθέσουμε ότι εκπροσωπούνται από τα

$$f = -1 + X + X^2 - X^4 + X^6 + X^9 - X^{10} \text{ και}$$

$$\mathrm{g} = -1 + X^2 + X^3 + X^5 - X^8 - X^{10}$$

Υπενθυμίζουμε ότι τα πολυώνυμα f και g πρέπει να διατηρούνται ιδιωτικά, καθώς το f αποτελεί το ιδιωτικό κλειδί του κρυπτοσυστήματος NTRUEncrypt. Για τον υπολογισμό του δημόσιου κλειδιού, πρέπει αρχικά να υπολογιστεί η αντίστροφη της f(x) $(mod\ q)$ και η αντίστροφη της f(x) $(mod\ p)$. Δηλαδή,

$$F_q(x) = f^{-1}(\mathrm{x})\ (mod\ q) \text{ και } F_p(x) = f^{-1}(\mathrm{x})\ (mod\ p).$$

Χρησιμοποιώντας το Διευρυμένο Ευκλείδειο Αλγόριθμο μπορούμε να υπολογίσουμε την αντίστροφη της f(x) στα μοδιακά p και q, η οποία, αντίστοιχα, θα είναι: $F_p(x) = 1 + 2X + 2X^3 + 2X^4 + X^5 + 2X^7 + X^8 + 2X^9\ (mod\ 3)$ και

$$F_q(x) = 5 + 9X + 6X^2 + 16X^3 + 4X^4 + 15X^5 + 16X^6 + 22X^7 + 20X^8 + 18X^9 + 30X^{10}\ (mod\ 32)$$

Στο σημείο αυτό, μπορούμε να υπολογίσουμε το δημόσιο κλειδί από τον τύπο:

$$h(x) = F_q(x) \cdot g(x)$$

Άρα, $$h(x) = (5 + 9X + 6X^2 + 16X^3 + 4X^4 + 15X^5 + 16X^6 + 22X^7 + 20X^8 + 18X^9 + 30X^{10}) \cdot (-1 + X^2 + X^3 + X^5 - X^8 - X^{10})(mod\ 32)$$

Εκτελώντας τη συνέλιξη (convolution), προκύπτει ότι το δημόσιο κλειδί είναι:

$$h(x) = 24 + 51X + 18X^2 - 4X^3 + 4X^4 - 24X^5 - 27X^6 - 47X^7 + 4X^8 - 15X^9 + 16X^{10}\ (mod\ 32)$$

Δουλεύουμε όμως στο μοδιακό 32, οπότε έχουμε:

$$h(x) = 24 + 19X + 18X^2 + 28X^3 + 4X^4 + 8X^5 + 5X^6 + 17X^7 + 4X^8 + 17X^9 + 16X^{10}\ (mod\ 32)$$

Ας υποθέσουμε τώρα ότι η Άλις (αποστολέας) θέλει να στείλει ένα μυστικό μήνυμα στον Μπομπ (παραλήπτης). Βάζει το μήνυμά της με τη μορφή ενός πολυωνύμου $m(x)$ με συντελεστές $\{-1, 0, 1\}$. Στις σύγχρονες κρυπτογραφικές εφαρμογές, το πολυώνυμο του μηνύματος μπορεί να μεταφραστεί σε δυαδική (binary) ή τριαδική (ternary) αναπαράσταση. Μετά τη δημιουργία του πολυωνύμου του μηνύματος, η Άλις επιλέγει τυχαία ένα πολυώνυμο $r(x)$ με μικρούς συντελεστές (όχι απαραίτητα από το σύνολο $\{-1, 0, 1\}$ που έχει ως στόχο να συσκοτίσει το μήνυμα). Μπορεί τώρα να υπολογίσει το κρυπτογραφημένο μήνυμα $e(x)$ με τη βοήθεια του δημόσιου κλειδιού $h(x)$ του Μπομπ ως εξής: $e(x) = p \cdot r(x) \cdot h(x) + m(x)$. Έτσι το κρυπτοκείμενο αποκρύπτει τα μηνύματα της Άλις και μπορούν να αποσταλούν στον Μπομπ με ασφάλεια. Έστω ότι, στο παράδειγμά μας, η Άλις θέλει να στείλει ένα μήνυμα το οποίο μπορεί να γραφεί ως πολυώνυμο ως εξής:

$$m(x) = -1 + X^3 - X^4 - X^8 + X^9 + X^{10} \ (mod\ 32)$$

Επίσης, έστω ότι το τυχαία επιλεγμένο πολυώνυμο $r(x)$ μπορεί να εκφρασθεί ως:

$$r(x) = -1 + X^2 + X^3 + X^4 - X^5 - X^7 (mod\ 32)$$

Τότε, το κρυπτοκείμενο $e(x)$ που αναπαριστά το κρυπτογραφημένο μήνυμα της Άλις θα είναι: $e(x) = 3 \cdot (-1 + X^2 + X^3 + X^4 - X^5 - X^7) \cdot (24 + 19X + 18X^2 + 28X^3 + 4X^4 + 8X^5 + 5X^6 + 17X^7 + 4X^8 + 17X^9 + 16X^{10}) + (-1 + X^3 - X^4 - X^8 + X^9 + X^{10})\ (mod\ 32)$

Εάν στην αναπαράσταση του κρυπτοκειμένου συμπεριλάβουμε μόνο τους συντελεστές των όρων του πολυωνύμου, τότε αυτό θα είναι:

$$e(x) = 3 \cdot (-1, 0, 1, 1, 1, -1, 0, -1, 0, 0, 0) \cdot (24, 19, 18, 28, 4, 8, 5, 17, 4, 17, 16) + (-1, 0,0, 1, -1, 0, 0, 0, -1,1,1)(mod\ 32)$$

Εκτελούμε αρχικά τη συνέλιξη, έπειτα τον πολλαπλασιασμό με το 3 και τέλος, την πρόσθεση με τους συντελεστές του αρχικού μηνύματος $m(x)$. Έτσι έχουμε:

$$e(x) = 3 \cdot (5, -7, 30, -3, 37, 16, 10, -19, -34, -9, -26) + (-1, 0,0, 1, -1, 0, 0, 0, -1,1,1)(mod\ 32)$$

$$e(x) = (15, -21, 90, -9, 111, 48, 30, -57, -102, -27, -78) + (-1, 0,0, 1, -1, 0, 0, 0, -1,1,1)(mod\ 32)$$

$$e(x) = (14, -21, 90, -8, 110, 48, 30, -57, -103, -26, -77)(mod\ 32)$$

Δουλεύουμε όμως στο μοδιακό 32, οπότε έχουμε:

$$e(x) = (14, 11, 26, 24, 14, 16, 30, 7, 25, 6, 19)$$

Έτσι, το κρυπτοκείμενο $e(x)$ που αναπαριστά το κρυπτογραφημένο μήνυμα της Άλις θα είναι: $e(x) = 14 + 11X + 26X^2 + 24X^3 + 14X^4 + 16X^5 + 30X^6 + 7X^7 + 25X^8 + 6X^9 + 19X^{10}$

Οποιοσδήποτε γνωρίζει το τυχαίο πολυώνυμο $r(x)$ μπορεί να υπολογίσει το αρχικό μήνυμα $m(x)$. Συνεπώς, η Άλις (αποστολέας) δεν πρέπει να αποκαλύψει το $r(x)$ σε κανέναν. Όσον αφορά τον Μπομπ (παραλήπτης), εκείνος εκτός από τις δημόσια διαθέσιμες πληροφορίες γνωρίζει και το ιδιωτικό του κλειδί, οπότε μπορεί να ανακτήσει το αρχικό μήνυμα. Για να είναι αποδοτική η αποκρυπτογράφηση, ο Μπομπ θα πρέπει να έχει υπολογίσει από πριν την αντίστροφη συνάρτηση της $f(\mathrm{x})\ (mod\ p)$, $F_p(x)$.

Η διαδικασία αποκρυπτογράφησης του κρυπτογραφήματος έχει ως εξής:

- $a(x) \equiv f(x) \cdot e(x)\ (mod\ q) \in R_q$, όπου οι συντελεστές του $a(x)$ επιλέγονται να είναι στο διάστημα $\left[-\frac{q}{2}, \frac{q}{2}\right]$.
- Τώρα, ο Μπομπ μπορεί να ανακτήσει το αρχικό μήνυμα υπολογίζοντας

$$m(x) \equiv F_p(x) \cdot a(x)\ (mod\ p)$$

Η επιτυχής αποκρυπτογράφηση, δηλαδή η ορθή ανάκτηση του αρχικού μηνύματος δεν είναι απόλυτα εφικτή σε κάθε περίπτωση. Κάποιες επιλογές των παραμέτρων ενδέχεται να προκαλέσουν περιστασιακή αποτυχία στην αποκρυπτογράφηση. Ο συνηθέστερος λόγος για μία τέτοια αποτυχία είναι η λανθασμένη προσαρμογή του μηνύματος. Στην περίπτωση αυτή, ο Μπομπ θα πρέπει να επιλέξει τους συντελεστές του $a(x)$ σε ένα διάστημα, ελάχιστα διαφορετικό από το αρχικό κατά μία ποσότητα x. Δηλαδή, $\left[-\frac{q}{2} + x, \frac{q}{2} + x\right]$. Εάν και αυτή η τεχνική δεν καταλήξει στο σωστό μήνυμα, λέμε ότι έχουμε αποτυχία κενού (gap failure), πράγμα που σημαίνει ότι το μήνυμα δεν μπορεί να επανακτηθεί τόσο εύκολα. Εάν, όμως, έχει γίνει κατάλληλη επιλογή των παραμέτρων, υπάρχει μία εξαιρετικά μεγάλη πιθανότητα ότι η διαδικασία της αποκρυπτογράφησης θα ανακτήσει το πρωτότυπο μήνυμα. Στην περίπτωση αυτή, όπου έχουν επιλεχθεί σωστά οι παράμετροι του συστήματος, το ενδεχόμενο αποτυχίας είναι πάρα πολύ μικρό, τόσο που στην πράξη μπορεί να αγνοηθεί.

4.3.2 Το NTRU δικτύωμα

Όπως προαναφέρθηκε, το κρυπτοσύστημα NTRU (NTRUEncrypt – NTRUSign) μπορεί να περιγραφεί χρησιμοποιώντας και κάποιους ειδικούς τύπους δικτυωμάτων

ακέραιων αριθμών. Από την άποψη των δικτυωμάτων, το NTRU βασίζεται σε μία ιδιαίτερα αποτελεσματική κλάση συνελικτικών (convolution), μοδιακών (modular) δικτυωμάτων, τα οποία θα τα αναφέρουμε ως NTRU δικτυώματα [3]. Πιο συγκεκριμένα, ο αλγόριθμος NTRUEncrypt βασίζεται στο πρόβλημα εύρεσης του βραχύτερου διανύσματος (SVP) σε ένα δικτύωμα, το οποίο από όσο γνωρίζουμε, ακόμα και χρησιμοποιώντας κβαντικούς υπολογιστές, δεν είναι εύθραυστο. Η διαδικασία ανάκτησης του δημόσιου κλειδιού στο κρυπτοσύστημα NTRU μπορεί να διαμορφωθεί ως ένα πρόβλημα (SVP) εύρεσης του βραχύτερου διανύσματος σε ένα συγκεκριμένο είδος δικτυώματος και η διαδικασία ανάκτησης του αρχικού κειμένου (plaintext) μπορεί να περιγραφεί ως ένα πρόβλημα (CVP) εύρεσης ενός διανύσματος σε ένα συγκεκριμένο είδος δικτυώματος, το οποίο να είναι το πλησιέστερο σε ένα δεδομένο διάνυσμα εκτός του δικτυώματος.

Έστω $h(x) = h_0 + h_1 x + \cdots + h_{N-1} x^{N-1}$ ένα NTRU δημόσιο κλειδί. Το NTRU δικτύωμα L_h^{NTRU} που σχετίζεται με το $h(x)$ είναι ένα δισδιάστατο δικτύωμα που παράγεται από τις γραμμές του παρακάτω πίνακα, M_h^{NTRU}:

$$M_h^{NTRU} = \begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & 1 & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & q \end{pmatrix}$$

Παρατηρούμε ότι ο πίνακας M_h^{NTRU} συντίθενται από τέσσερα $N \times N$ τμήματα:

1. Άνω αριστερό τμήμα = μοναδιαίος πίνακας (identity matrix)
2. Κάτω αριστερό τμήμα = μηδενικός πίνακας (zero matrix)
3. Κάτω δεξιό τμήμα = q φορές το μοναδιαίο πίνακα I
4. Άνω δεξιό τμήμα = κυκλικές μεταθέσεις των συντεταγμένων του $h(x)$

Συντομογραφικά, ο πίνακας M_h^{NTRU} μπορεί να γραφεί ως εξής: $M_h^{NTRU} = \begin{pmatrix} I & h \\ 0 & qI \end{pmatrix}$.

Μπορούμε να θεωρήσουμε, δηλαδή, τον πίνακα M_h^{NTRU} ως έναν 2×2 πίνακα που έχει συντεταγμένες στο R.

4.3.3 Επιθέσεις στο κρυπτοσύστημα NTRU

Από τότε που προτάθηκε το κρυπτοσύστημα NTRU, έχουν παρουσιασθεί πολλές επιθέσεις σε αυτό. Οι περισσότερες επιθέσεις επικεντρώνονται στη συνολική παραβίαση του συστήματος με την εύρεση του ιδιωτικού κλειδιού f και όχι μόνο στην ανάκτηση του μηνύματος m. Εάν το ιδιωτικό κλειδί f φέρεται να έχει ελάχιστους, μη μηδενικούς συντελεστές, ο επιτιθέμενος μπορεί να εξαπολύσει με επιτυχία μία επίθεση ωμής βίας (brute–force attack), δοκιμάζοντας όλες τις τιμές για το ιδιωτικό κλειδί f. Όταν ο επιτιθέμενος θέλει να ξέρει εάν το f' είναι το ιδιωτικό κλειδί, τότε υπολογίζει απλά το $f' \cdot h \ (mod\ q)$. Εάν το αποτέλεσμα έχει μικρούς συντελεστές, πιθανόν να είναι αυτό το ιδιωτικό κλειδί και τότε ο επιτιθέμενος μπορεί να ελέγξει ένα το κλειδί f' είναι το ιδιωτικό, χρησιμοποιώντας το για να αποκρυπτογραφήσει ένα μήνυμα που έχει κρυπτογραφήσει ο ίδιος του. Ο επιτιθέμενος θα μπορούσε, επίσης, να δοκιμάσει τις τιμές της συνάρτησης g και να ελέγξει εάν το γινόμενο $g' \cdot h^{-1} \ (mod\ q)$ έχει μικρές τιμές.

4.3.4 Σύγκριση του NTRU με άλλα κρυπτοσυστήματα

Δεδομένου ότι τόσο η κρυπτογράφηση, όσο και η αποκρυπτογράφηση στο NTRU χρησιμοποιούν μόνο απλό πολλαπλασιασμό πολυωνύμου, οι πράξεις αυτές εκτελούνται πολύ γρήγορα σε σύγκριση με άλλα συστήματα ασύμμετρης κρυπτογράφησης, όπως το κρυπτοσύστημα RSA, το κρυπτοσύστημα ElGamal και η ελλειπτική κρυπτογραφία. Ωστόσο, το NTRUEncrypt δεν έχει υποστεί ακόμη ένα αντίστοιχο ποσό κρυπτογραφικής ανάλυσης και η ασφάλειά του δεν έχει αποδειχθεί για όλες τις περιπτώσεις.

Το σύστημα NTRU έχει ορισμένα κοινά χαρακτηριστικά με το σύστημα McEliece, μεταξύ των οποίων είναι και το γεγονός ότι η πράξη του πολλαπλασιασμού στο δακτύλιο R μπορεί να διαμορφωθεί ως πολλαπλασιασμός πινάκων (μίας ειδικής κατηγορίας πινάκων), και επίσης, η διαδικασία της κρυπτογράφησης και στα δύο συστήματα μπορεί να γραφτεί ως πολλαπλασιασμός πινάκων E = AX + Y, όπου το A είναι το δημόσιο κλειδί. Μια μικρή διαφορά μεταξύ των δύο συστημάτων είναι ότι για την κρυπτογράφηση NTRU, το Y είναι το μήνυμα και το X είναι ένα τυχαίο διάνυσμα, ενώ στο σύστημα McEliece οι αντιστοιχίσεις αυτές είναι αντίστροφες. Αλλά η πραγματική διαφορά είναι η υποκείμενη συνάρτηση κερκόπορτας (trap–door function)

που επιτρέπει την αποκρυπτογράφηση. Για το σύστημα McEliece, ο πίνακας A συνδέεται με έναν κώδικα διόρθωσης σφαλμάτων (Goppa code), και η αποκρυπτογράφηση λειτουργεί επειδή η τυχαία συνεισφορά είναι αρκετά μικρή για να "διορθωθεί" από τον κώδικα Goppa. Για το NTRU, ο πίνακας A είναι ένας κυκλικός (circulant) πίνακας και η αποκρυπτογράφηση εξαρτάται από την παραγοντοποίηση του A σε ένα γινόμενο δύο πινάκων που έχουν ειδική μορφή, μαζί με μια άρση από το mod q στο mod p [39].

Από όσο μπορούμε να πούμε, το σύστημα NTRU έχει ελάχιστα κοινά με το σύστημα RSA. Παρομοίως, παρόλο που το NTRU σύστημα πρέπει να ρυθμιστεί με τέτοιο τρόπο, ώστε να αποτρέπει και να προλαμβάνει επιθέσεις βασισμένες στην αναγωγή της βάσης ενός δικτυώματος, η υποκείμενη μέθοδος αποκρυπτογράφησης είναι πολύ διαφορετική από αυτήν στο σύστημα GGH, στο οποίο η αποκρυπτογράφηση βασίζεται στη γνώση μικρών βάσεων του δικτυώματος. Από αυτήν την άποψη, το GGH μοιάζει στην πραγματικότητα με το σύστημα McEliece, αφού και στις δύο περιπτώσεις η αποκρυπτογράφηση πραγματοποιείται με την αναγνώριση και την εξάλειψη μια μικρής τυχαίας συμβολής. Εν αντιθέσει, το NTRU εξαλείφει μία πολύ μεγαλύτερη τυχαία συνεισφορά [39].

Στο επόμενο κεφάλαιο παρουσιάζεται, μεταξύ άλλων, και ο αντίστοιχος αλγόριθμος NTRU για δημιουργία ψηφιακής υπογραφής, ο NTRUSign.

4.4 Άλλα Κρυπτοσυστήματα

Τα κρυπτοσυστήματα που παρουσιάσθηκαν μέχρι τώρα σε αυτό το κεφάλαιο θεωρούνται κλασσικά πλέον σε αυτήν την κατηγορία κρυπτοσυστημάτων. Εκτός από αυτά, υπάρχει πλήθος σύγχρονων κρυπτοσυστημάτων τα οποία προσφέρουν παρόμοιες επιδόσεις με αυστηρές εγγυήσεις ασφάλειας.

Μεταξύ των σύγχρονων κρυπτοσυστημάτων που βασίζονται σε δικτυώματα ακέραιων αριθμών είναι και κάποιες συνδυαστικές προτάσεις, που χρησιμοποιούν μαζί με τα δικτυώματα και σακίδια (knapsacks). Τα πιο γνωστά παραδείγματα τέτοιων προσεγγίσεων έγιναν από τους Cai και Cusick [21], οι οποίοι συνδύασαν το κρυπτοσύστημα των Ajtai–Dwork με ένα σακίδιο, καθώς και από τους Pan και Deng [68], οι οποίοι αφού κρυπτανέλυσαν το σύστημα των πρώτων, πρότειναν ένα καινούριο

συνδυαστικό κρυπτοσύστημα, με δικτυώματα ακεραίων και σακίδια. Το κρυπτοσύστημα των Pan και Deng επίσης κρυπταναλύθηκε από τους J.Xu et.al [85] στο CANS 2012.

Επίσης, στα σύγχρονα κρυπτοσυστήματα με δικτυώματα ακεραίων συγκαταλέγονται πολλές παραλλαγές και βελτιστοποιήσεις του κρυπτοσυστήματος NTRU, καθώς αυτό θεωρείται ότι είναι ουσιαστικά το μόνο πρακτικό κρυπτοσύστημα, βασισμένο σε δικτυώματα ακεραίων. Το NTRU θεωρείται επίσης και ασφαλές κρυπτοσύστημα (αν και η ασφάλειά του δεν έχει αποδειχθεί), αλλά για την επίτευξη της ασφάλειας απαιτείται πολύ μεγάλο μήκος κλειδιού.

Από την πληθώρα των παραλλαγών που υπάρχουν για το NTRU, κρίναμε σκόπιμο να αναφερθούμε σε ένα σύστημα, το οποίο περιλαμβάνει στοιχεία από την πολυμεταβλητή πολυωνυμική άλγεβρα και χρησιμοποιεί δύο μεταβλητές αντί για μία. Το κρυπτοσύστημα αυτό δημιουργήθηκε το 2008 από τους M. Caboara, F.Caruso and C. Traverso και ονομάστηκε NTWO, τόσο διότι αποτελεί μία δεύτερη εκδοχή του NTRU, όσο και για το λόγο ότι χρησιμοποιεί, όπως προαναφέρθηκε, δύο μεταβλητές αντί για μία [98].

Η υποκείμενη ιδέα του NTWO κρυπτοσυστήματος είναι ίδια με αυτή του NTRU, αλλά στο NTWO η ιδέα αυτή τροποποιείται με ορισμένες πτυχές της πολυμεταβλητής πολυωνυμικής άλγεβρας. Οι διαφορές στον ορισμό των δύο αυτών κρυπτοσυστημάτων είναι ελάχιστες, αλλά μεταβάλλουν ουσιαστικά τις πιθανές επιθέσεις κατά του ιδιωτικού κλειδιού.

Όσον αφορά το δημόσιο τμήμα των δύο κρυπτοσυστημάτων, δεν παρατηρούνται σημαντικές διαφορές μεταξύ τους. Τόσο το NTRU, όσο και το NTWO λειτουργούν σε έναν περικομμένο πολυωνυμικό δακτύλιο $R = \frac{\mathbb{Z}[x]}{x^N - 1}$, οι υπολογισμοί για την κρυπτογράφηση γίνονται στο μοδιακό q, ενώ οι υπολογισμοί για την αποκρυπτογράφηση γίνονται σε ένα βοηθητικό (auxiliary) μοδιακό p. Ακόμη, και στα δύο αυτά συστήματα, το δημόσιο κλειδί είναι ένα πολυώνυμο $h \in R$, τα μηνύματα είναι «μικρά» πολυώνυμα (συντελεστές των πολυωνύμων πολύ μικρότεροι από το p ή το q) και η διαδικασία της κρυπτογράφησης προκύπτει από τον τύπο $e(x) = p \cdot r(x) \cdot h(x) + m(x) \ (mod\ q)$, όπου το $r(x)$ είναι ένα τυχαίο, μικρό πολυώνυμο.

Η θεμελιώδης διαφορά τους έγκειται στο ιδιωτικό τμήμα τους. Πιο συγκεκριμένα, ενώ στο NTRU η αντίστροφη της συνάρτησης $f(x)$ (που αποτελεί το ιδιωτικό κλειδί) υπολογίζεται στο μοδιακό q, στο NTWO ο υπολογισμός αυτός γίνεται στο μοδιακό Q. Το Q είναι ένα ιδεώδες (ideal) του δακτυλίου R, το οποίο περιέχει το q

και αποτελεί μέρος του ιδιωτικού κλειδιού. Με τον όρο «ιδεώδες» ενός δακτυλίου R, αναφερόμαστε σε ένα ειδικό υποσύνολο του R, έστω I, το οποίο αποτελεί μία προσθετική υποομάδα του R και πληροί τις ακόλουθες συνθήκες:

- $\forall x \in I, \forall r \in R: x \cdot r \in I$
- $\forall x \in I, \forall r \in R: r \cdot x \in I$

Ένα ακόμη σημαντικό σημείο διαφορετικότητας μεταξύ του NTRU και του NTWO είναι το δύσκολο πρόβλημα που προστατεύει το ιδιωτικό κλειδί. Στην περίπτωση του NTWO, το πρόβλημα αυτό είναι αρκετά δυσκολότερο. Περαιτέρω ανάλυση του κρυπτοσυστήματος NTWO ή των προσεγγίσεων με τα σακίδια θεωρείται εκτός των σκοπών αυτής της εργασίας.

Κεφάλαιο 5
Συναρτήσεις Διασποράς και Ψηφιακές Υπογραφές

Η συνάρτηση διασποράς, γνωστή και ως συνάρτηση κατατεμαχισμού ή κατακερματισμού, είναι μία μαθηματική συνάρτηση που έχοντας ως είσοδο μία αυθαίρετου μεγέθους ομάδα δεδομένων δίνει έξοδο μία καθορισμένου μεγέθους στοιχειοσειρά (string) πολύ μικρότερη από την είσοδο. Η έξοδος της συνάρτησης είναι συνήθως ένας ακέραιος αριθμός και μπορεί να χρησιμοποιηθεί ως δείκτης σε κάποιο πίνακα. Οι τιμές που επιστρέφει η συνάρτηση διασποράς ονομάζονται τιμές διασποράς (hash values), κώδικες διασποράς (hash codes), αθροίσματα διασποράς (hash sums) ή απλά hashes.

Οι συναρτήσεις διασποράς χρησιμοποιούνται συνήθως για να επιταχυνθεί η αναζήτηση σε κάποιο πίνακα ή σε εργασίες σύγκρισης δεδομένων (π.χ. εύρεση στοιχείων σε μια βάση δεδομένων, εύρεση παρόμοιων εγγραφών σε ένα μεγάλο αρχείο βάσης κλπ).

Μία συνάρτηση διασποράς μπορεί να αντιστοιχίζει δύο ή περισσότερες εισόδους στην ίδια τιμή διασποράς. Πιο συγκεκριμένα, μία συνάρτηση διασποράς, έστω h, αντιστοιχίζει συμβολοσειρές δυαδικών ψηφίων αυθαίρετου πεπερασμένου μήκους σε συμβολοσειρές σταθερού μήκους, ας πούμε των n bits. Εάν πεδίο ορισμού (domain) D και σύνολο τιμών (range) R με $h : D \longrightarrow R$ και $|D| > |R|$, η συνάρτηση είναι πολλά–προς–ένα, πράγμα που σημαίνει ότι η ύπαρξη συγκρούσεων (ζεύγη εισόδων με πανομοιότυπη έξοδο) είναι αναπόφευκτη. Στις περισσότερες εφαρμογές είναι επιθυμητή η ελαχιστοποίηση αυτών των συγκρούσεων. Αυτό σημαίνει ότι η συνάρτηση διασποράς θα πρέπει να αντιστοιχίζει κάθε είσοδο σε διαφορετική τιμή διασποράς. Ανάλογα με την εφαρμογή στην οποία επρόκειται να χρησιμοποιηθεί, η συνάρτηση διασποράς σχεδιάζεται με διαφορετικές προδιαγραφές. Η ιδέα αυτών των συναρτήσεων εμφανίστηκε το 1950 αλλά ακόμη και σήμερα ο σχεδιασμός μιας καλής συνάρτησης διασποράς εξακολουθεί να είναι αντικείμενο ενεργού έρευνας.

Οι συναρτήσεις διασποράς συσχετίζονται (αν και πολλές φορές συγχέονται ως έννοιες) με τις συναρτήσεις αθροίσματος ελέγχου (π.χ. τον κυκλικό έλεγχο πλεονασμού–

Cyclic Redundancy Check, CRC) τον υπολογισμό ψηφίου ελέγχου (check digit), τα δακτυλικά αποτυπώματα (fingerprints), τους κώδικες ελέγχου λαθών (error correcting codes) και την κρυπτογραφική συνάρτηση διασποράς [98].

Στο κεφάλαιο αυτό θα ασχοληθούμε με συναρτήσεις διασποράς που χρησιμοποιούνται για κρυπτογραφικούς σκοπούς και πιο συγκεκριμένα, κρυπτογραφικές συναρτήσεις διασποράς που είναι βασισμένες σε δικτυώματα ακέραιων αριθμών. Επίσης, στη δεύτερη ενότητα του κεφαλαίου, αναφερόμαστε στην έννοια της ψηφιακής υπογραφής, παρουσιάζοντας τις πιο σημαντικές προσπάθειες που έχουν γίνει και οι οποίες βασίζονται σε διάφορα είδη δικτυωμάτων.

5.1 Κρυπτογραφικές Συναρτήσεις Διασποράς

Η βασική ιδέα των κρυπτογραφικών συναρτήσεων διασποράς είναι ότι μία τιμή διασποράς (hash value) χρησιμεύει ως μία συμπαγής αντιπροσωπευτική εικόνα (μερικές φορές ονομάζεται αποτύπωμα, ψηφιακό αποτύπωμα , ή σύνοψη μηνύματος (message digest)) μιας συμβολοσειράς εισόδου και η τιμή αυτή μπορεί να χρησιμοποιηθεί σαν να ήταν μοναδικά αναγνωρίσιμη με την εν λόγω συμβολοσειρά.

Οι κρυπτογραφικές συναρτήσεις διασποράς έχουν διαδραματίσει θεμελιώδη ρόλο στη σύγχρονη κρυπτογραφία. Παρόλο που είναι σχετικές με τις συμβατικές συναρτήσεις διασποράς που χρησιμοποιούνται συνήθως σε μη κρυπτογραφικές εφαρμογές υπολογιστών, καθώς και στις δύο περιπτώσεις οι μεγαλύτερες περιοχές αντιστοιχίζονται σε μικρότερες κλίμακες, οι κρυπτογραφικές συναρτήσεις διασποράς διαφέρουν σε αρκετές σημαντικές πτυχές. Στην ενότητα αυτή εστιάζουμε σε κρυπτογραφικές συναρτήσεις διασποράς και πιο συγκεκριμένα στη χρήση τους για την ακεραιότητα των δεδομένων και την αυθεντικοποίηση των μηνυμάτων [1].

Οι πρώτες κρυπτογραφικές συναρτήσεις διασποράς (εφεξής, απλά συναρτήσεις διασποράς) άρχισαν να σχεδιάζονται στα τέλη της δεκαετίας του 1970, ενώ στη δεκαετία του 1980 υπήρξαν αρκετές προσπάθειες και προτάσεις όσον αφορά αυτό το θέμα. Κατά τη διάρκεια της δεκαετίας του 1990, παρουσιάστηκε εκθετική αύξηση στον αριθμό των συναρτήσεων διασποράς, αλλά για αρκετές από αυτές εντοπίστηκαν κενά ασφαλείας.

Οι συναρτήσεις MD5 (message digest) και SHA–1 (secure hash algorithm) αναπτύχθηκαν και συμπεριλήφθησαν σε πλήθος εφαρμογών με αποτέλεσμα να χαρακτηριστούν ως «Swiss army knifes» της κρυπτογραφίας, ονομασία εμπνευσμένη

από τα θρυλικά ελβετικά μαχαίρια στρατού που δημιούργησε ο Καρλ Έλσενερ ο 3ος . Παρά τη μεγάλη σημασία των συναρτήσεων διασποράς, λίγες σχετικά προσπάθειες καταβλήθηκαν για την εγκαθίδρυση ορισμών εννοιών που εμπεριέχονται σε αυτές, αλλά και των γενικών αρχών λειτουργίας τους.

Το 2004, ο Wang και οι συνεργάτες του [80, 82] συνέβαλλαν σημαντικά στην τελειοποίηση της διαφορικής κρυπτανάλυσης (differential cryptanalysis) και κατά συνέπεια, η εύρεση συγκρούσεων για τη συνάρτηση MD5 έγινε ένα εύκολο ζήτημα. Επίσης, για τη συνάρτηση SHA–1 υπήρξε μία σημαντική μείωση του ορίου ασφαλείας. Αυτή η σπουδαία ανακάλυψη πυροδότησε μία έκρηξη ερευνητικής δραστηριότητας, που κατέληξε σε νέες κατασκευές συναρτήσεων διασποράς και σε ένα διαρκώς αυξανόμενο σώμα θεμελιώδους έρευνας.

Οι συναρτήσεις διασποράς χρησιμοποιούνται για την ακεραιότητα των δεδομένων, σε συνδυασμό με τα σχήματα ψηφιακών υπογραφών, όπου για διάφορους λόγους ένα μήνυμα τυπικά πρώτα διασπείρεται και στη συνέχεια υπογράφεται η τιμή διασποράς (hash–value), ως εκπρόσωπος του μηνύματος, στη θέση του αρχικού [1].

Μία ξεχωριστή κατηγορία συναρτήσεων διασποράς, που ονομάζονται κώδικες αυθεντικοποίησης μηνυμάτων (Message Authentication Codes – MAC), επιτρέπουν τον έλεγχο αυθεντικοποίησης μηνυμάτων με συμμετρικές τεχνικές. Οι MAC αλγόριθμοι μπορούν να θεωρηθούν ως συναρτήσεις διασποράς που λαμβάνουν δύο συναρτησιακά διακριτές εισόδους, ένα μήνυμα και ένα μυστικό κλειδί, και παράγουν μία σταθερού μεγέθους (ας πούμε n –bit) έξοδο. Οι αλγόριθμοι MAC μπορούν να χρησιμοποιηθούν για να παρέχουν ακεραιότητα των δεδομένων και αυθεντικοποίηση της προέλευσης συμμετρικών δεδομένων, καθώς και αναγνώρισης σε σχήματα συμμετρικού κλειδιού.

Η ιδανική κρυπτογραφική συνάρτηση διασποράς έχει τέσσερις βασικές ιδιότητες :

- είναι εύκολο να υπολογίσει την τιμή διασποράς για κάθε δεδομένο μήνυμα
- είναι ανέφικτο να δημιουργήσει ένα μήνυμα που έχει μία δεδομένη σύνοψη
- είναι ανέφικτο να τροποποιήσει ένα μήνυμα χωρίς να αλλάζει η σύνοψη
- είναι ανέφικτο να βρεθούν δύο διαφορετικά μηνύματα με την ίδια σύνοψη

Οι κρυπτογραφικές συναρτήσεις διασποράς έχουν πολλές εφαρμογές στην ασφάλεια των πληροφοριών, ιδίως στις ψηφιακές υπογραφές, στους κώδικες αυθεντικοποίησης μηνύματος (MAC) και σε άλλες μορφές αυθεντικοποίησης. Μπορούν επίσης να χρησιμοποιηθούν ως απλές συναρτήσεις διασποράς, δηλαδή για να λειτουργήσουν ως δείκτης των δεδομένων σε έναν πίνακα διασποράς, για λήψη

δακτυλικών αποτυπωμάτων, για τον εντοπισμό διπλών δεδομένων ή για να προσδιορίσουν μοναδικά τα διάφορα αρχεία, και ως αθροίσματα ελέγχου για την ανίχνευση κάποιας τυχαίας καταστροφής των δεδομένων. Πράγματι , στο πλαίσιο της ασφάλειας των πληροφοριών, οι κρυπτογραφικές τιμές σύνοψης μερικές φορές ονομάζονται (ψηφιακά) δακτυλικά αποτυπώματα, αθροίσματα ελέγχου, ή απλά hash τιμές σύνοψης, ακόμη και εάν όλοι αυτοί οι όροι ισχύουν για γενικότερες συναρτήσεις με αρκετά διαφορετικές ιδιότητες και σκοπούς [98].

5.1.1 Βασικές Έννοιες

Στο υψηλότερο επίπεδο, οι συναρτήσεις διασποράς μπορούν να χωριστούν σε δύο κατηγορίες: στις συναρτήσεις διασποράς χωρίς κλειδί (unkeyed), οι προδιαγραφές των οποίων υπαγορεύουν μία μόνο παράμετρο εισόδου και στις συναρτήσεις διασποράς με κλειδί (keyed), οι προδιαγραφές των οποίων υπαγορεύουν δύο ξεχωριστές εισόδους, ένα μήνυμα και ένα μυστικό κλειδί. Μία συνάρτηση διασποράς ανεπίσημα ορίζεται ως εξής:

Ορισμός 5.1.1.1 Μία συνάρτηση διασποράς (κατά τη γενική έννοια) είναι μία συνάρτηση h που έχει τουλάχιστον, τις ακόλουθες δύο ιδιότητες:

1. Συμπίεση – η h απεικονίζει μία είσοδο πεπερασμένου μήκους x αυθαίρετων δυαδικών ψηφίων (bits) σε μια έξοδο $h(x)$ σταθερού μήκους n δυαδικών ψηφίων.
2. Ευκολία υπολογισμού – Με δεδομένη την h και μία είσοδο x, η $h(x)$ είναι εύκολο να υπολογιστεί [7].

Κάποιες ακόμη ιδιότητες που συνδέονται συχνά με τις κρυπτογραφικές συναρτήσεις διασποράς είναι:

- Αποδοτικότητα (Efficiency). Λαμβάνοντας υπόψη οποιαδήποτε είσοδο x, το hash αποτέλεσμα $h\,(x)$ μπορεί να υπολογιστεί αποτελεσματικά και με αμελητέα ποσότητα μνήμης.
- Αντίσταση Προεικόνας (Preimage Resistance). Λαμβάνοντας υπόψη μία έξοδο y, είναι υπολογιστικά δύσκολο να βρεθεί οποιαδήποτε είσοδος x που ικανοποιεί $h\,(x) = y$.
- Δεύτερη αντίσταση προεικόνας (Second Preimage Resistance). Δεδομένου του x, είναι υπολογιστικά δύσκολο να βρεθεί το x' που ικανοποιεί $h\,(x) = h\,(x')$ με $x \neq x'$.

- Αντοχή σύγκρουσης (Collision Resistance). Είναι υπολογιστικά δύσκολο να βρεθούν x και x', με $x \neq x'$, που ικανοποιούν $h(x) = h(x')$. Η αντοχή σύγκρουσης συνεπάγεται τη δεύτερη αντίσταση προεικόνας [34], αλλά δεν εγγυάται την αντίσταση προεικόνας.
- Ψευδοτυχαιότητα (Pseudorandomness). Μία συνάρτηση διασποράς πρέπει να προσομοιάζει αρκετά με μια τυχαία συνάρτηση.

Οι παραπάνω ιδιότητες συντελούν και στον ορισμό της επιτυχούς κρυπτανάλυσης μίας συνάρτησης διασποράς, δηλαδή καθορίζουν τα κριτήρια με τα οποία θεωρούμε ότι μία συνάρτηση διασποράς έχει παραβιασθεί.

Οι περισσότερες συναρτήσεις διασποράς που χρησιμοποιούνται σήμερα στην πράξη είναι επαναληπτικές (iterative), πράγμα που σημαίνει ότι η είσοδος διασπάται σε μικρότερα τμήματα τα οποία υποβάλλονται σε επεξεργασία επαναληπτικά χρησιμοποιώντας μία συνάρτηση συμπίεσης (ουσιαστικά, μία συνάρτηση διασποράς) με σταθερά μεγέθη εισόδου και εξόδου.

Οι παρακάτω πρόσθετοι μετασχηματισμοί μπορούν να χρησιμοποιηθούν στην κατασκευή επαναληπτικών συναρτήσεων διασποράς:

- **«Παραγέμισμα»(padding) και εκ νέου κωδικοποίηση**

  Η είσοδος του μηνύματος μπορεί να τροποποιηθεί κατά κάποιο τρόπο για τη συνάρτηση συμπίεσης. Τυπικές μετατροπές της εκ νέου κωδικοποίησης περιλαμβάνουν το «παραγέμισμα» (με το μήκος του μηνύματος) και διάφορους μετασχηματισμούς του κλειδιού.
- **Τελικός μετασχηματισμός**

  Δε χρειάζεται να επιστραφούν ως αποτέλεσμα της συνάρτησης διασποράς όλες οι πληροφορίες εσωτερικής κατάστασης της συνάρτησης. Ο τελικός μετασχηματισμός μπορεί να χρησιμοποιήσει το συνολικό μήκος του μηνύματος σαν παράμετρο.

Η αντίσταση προεικόνας που αναφέρθηκε παραπάνω ως έννοια συνάδει με τη διαισθητική αντίληψη της μη αντιστρεψιμότητας (non reversibility) μίας συνάρτησης διασποράς. Είναι σαφές ότι η αντίσταση προεικόνας είναι εξαιρετικά δύσκολο (εάν όχι αδύνατο) να αποδειχθεί σε μία γενική ρύθμιση. Ωστόσο, οι συναρτήσεις διασποράς παραβιάζονται τακτικά και ως εκ τούτου, είναι σύνηθες φαινόμενο οι αποδείξεις ότι συγκεκριμένες συναρτήσεις διασποράς δεν είναι ανθιστάμενες σην προεικόνα (no preimage resistant). Η δεύτερη αντίσταση προεικόνας είναι μία ελαφρώς ισχυρότερη

έννοια από την αντίσταση προεικόνας. Όπως προαναφέραμε, αυτό σημαίνει ότι είναι δύσκολο να βρεθεί ένα μήνυμα που παράγει την ίδια σύνοψη, με ένα άλλο, γνωστό μήνυμα. Διαισθητικά, η δεύτερη αντίσταση προεικόνας είναι πολύ στενά συνδεδεμένη με την αντίσταση προεικόνας, εκτός από το ότι υπάρχει και ένα άλλο μήνυμα για να βοηθήσει την αναζήτηση προεικόνας. Η πρώτη αντίσταση προεικόνας δεν συνεπάγεται τη δεύτερη. Αυτές οι ιδιότητες δεν απαιτούνται κατ' ανάγκη σε μη κρυπτογραφικές εφαρμογές των συναρτήσεων διασποράς, όπως είναι η ταξινόμηση και η αναζήτηση [74].

Οι περισσότερες σύγχρονες συναρτήσεις διασποράς επεξεργάζονται τα μηνύματα σε μπλοκ σταθερού μήκους. Όλες, εκτός από τις πρώτες που αναπτύχθηκαν, περιλαμβάνουν κάποιο είδος «παραγεμίσματος» (padding). Είναι κρίσιμης σημασίας για τις συναρτήσεις διασποράς να περιέχουν κάποιο σχήμα τερματισμού, που εμποδίζει μία τέτοια συνάρτηση από το να είναι ευάλωτη σε επιθέσεις επέκτασης μήκους (length extension attacks). Οι επιθέσεις επέκτασης μήκους είναι ένα είδος επίθεσης σε συγκεκριμένους τύπους συναρτήσεων διασποράς, οι οποίοι επιτρέπουν την ενσωμάτωση επιπρόσθετων πληροφοριών [98].

5.1.2 Η συνάρτηση LASH–x

Η συνάρτηση LASH–x είναι μία κρυπτογραφική συνάρτηση διασποράς, βασισμένη σε δικτυώματα ακέραιων αριθμών, η οποία προτάθηκε στο δεύτερο συνέδριο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST) από τους K.Bentahar, Page, J.H. Silverman, M.J.O. Saarinen και N.Smart [75].

Όσον αφορά την ονομασία της, αυτή μπορεί να συσχετιστεί με διάφορα πιθανά ακρωνύμια:

- **L**inear **A**lgebra based **S**ecure **H**ash, δηλαδή ασφαλής σύνοψη βασισμένη στη γραμμική άλγεβρα, αφού το κύριο συστατικό της είναι απλά ένα γινόμενο πίνακα–διανύσματος.
- **LA**ttice based **S**ecure **H**ash, δηλαδή ασφαλής σύνοψη βασισμένη σε δικτύωμα, επειδή η αντιστροφή του γραμμικού στοιχείου της και συνεπώς, η εξεύρεση συγκρούσεων, είναι στενά συνδεδεμένη με τα δυσεπίλυτα προβλήματα SVP και CVP σε δικτυώματα.

- **L**ight–weight **A**rithmetical **S**ecure **H**ash, δηλαδή «ελαφριά», αριθμητική, ασφαλής σύνοψη, επειδή ο σχεδιασμός της είναι πολύ μικρός σε έκταση και συνεπώς, ευκολομνημόνευτος [75].

Ο σχεδιασμός της συνάρτησης LASH–x βασίζεται σε μία απλή υποκείμενη αρχή, και ένα μέρος της ασφάλειάς της μπορεί να αποδειχθεί ότι σχετίζεται με προβλήματα δικτυώματος [75].

Η LASH–x είναι μία πρακτική κρυπτογραφική συνάρτηση διασποράς, βασισμένη στην κατασκευή των Miyaguchi – Preneel [98], η οποία αντί να χρησιμοποιεί ένα μπλοκ κρυπτογράφησης, ως κύριο συστατικό, χρησιμοποιεί μοδιακό (modular) πολλαπλασιασμό πινάκων.

Έτσι, ως κύριο συστατικό χρησιμοποιεί μία συνάρτηση συμπίεσης, η οποία είναι στενά συνδεδεμένη με τη θεωρητική συνάρτηση διασποράς των Goldreich, Goldwasser και Halevi. Με κατάλληλες επιλογές των παραμέτρων μπορούμε να παράγουμε μία συνάρτηση διασποράς, η οποία να είναι συγκρίσιμη σε απόδοση με τις υφιστάμενες συναρτήσεις διασποράς, όπως οι SHA–1, και SHA–2.

Περιγραφή της συνάρτησης LASH–x

Οι συναρτήσεις της σειράς LASH–x υπολογίζουν μία τιμή διασποράς (hash value) μήκους x–bit από μία ακολουθία bit εισόδου αυθαίρετου μήκους. Υπάρχουν τέσσερις συγκεκριμένες προτάσεις, όπου n είναι το μέγεθος της εισόδου στη συνάρτηση συμπίεσης (εκφρασμένο σε bits) και το m είναι το μέγεθος της μεταβλητής αλυσοποίησης (chaining variable) σε 8–bit byte. Για όλες τις εκδόσεις της συνάρτησης LASH–x, ισχύει ότι m = n/16 και q = 256 [35].

Η οικογένεια LASH–x είναι ένα σύνολο συναρτήσεων διασποράς, οι οποίες παράγουν x bit σύνοψης (digest), με τις συνηθέστερες τιμές του x να είναι οι 160, 256, 384, 512. Η παράμετρος του κλειδιού είναι n = 640, 1024, 1536, 2048. Ουσιαστικά, n = 4 επί x. Στη συνέχεια, ορίζουμε m = n/16.

Ο αλγόριθμος LASH–x μπορεί να διαιρεθεί σε τρία μέρη, τα οποία έχουν ως εξής:

- **«Παραγέμισμα» (padding) του μηνύματος**: το αρχικό μήνυμα M, με $|M| = l$ «παραγεμίζεται» από ένα και μοναδικό δυαδικό ψηφίο (bit) με τιμή 1 και αρκετά bits με τιμή 0, έως ότου να ληφθεί το συνολικό μήκος ίσο με ένα πολλαπλάσιο

του $8 \cdot m$ bits. Το «παραγεμισμένο» μήνυμα χωρίζεται σε $k = \lceil l/8m \rceil$ μπλοκ. Επισυνάπτεται ένα επιπλέον μπλοκ που περιέχει το αρχικό μήκος του μηνύματος. Τα μπλοκ τροφοδοτούνται στη συνάρτηση συμπίεσης ένα προς ένα.

- **Επανάληψη της συνάρτησης συμπίεσης**: Τα τμήματα (μπλοκ) του μηνύματος $M_1, M_2, \dots, M_k, M_{k+1}$ υποβάλλονται σε επεξεργασία ως εξής:

$$r_0 \leftarrow [0, 0, \dots, 0]$$

$$r_i \leftarrow f\,(r_{i-1}, M_i) \text{ για } i = 1, \dots,\ k+1$$

- **Τελικός μετασχηματισμός**: Έστω ότι $r, s \in \mathbb{Z}_{256}^m$ είναι δύο διανύσματα από bytes. Ορίζουμε: $rep\,(\cdot) : \mathbb{Z}_{256}^m \rightarrow \mathbb{Z}_{256}^{8m}$ ως τη συνάρτηση που επιστρέφει τη δυαδική αναπαράσταση, δηλαδή την ακολουθία από 0 και 1 των bytes που δίνονται ως όρισμα. Για παράδειγμα,

$$rep\,([255, 1, 128]) = [1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$$ [75]

Στον πίνακα που ακολουθεί παρατίθενται οι προτεινόμενες παράμετροι για τις διάφορες παραλλαγές της συνάρτησης LASH–x.

Πίνακας 5.1.21. Προτεινόμενη επιλογή παραμέτρων για τις παραλλαγές της LASH–x

Παραλλαγή	**N**	**m**
LASH–x–160	640	40
LASH–x–256	1024	64
LASH–x–384	1536	96
LASH–x–512	2048	128

5.1.3 Θεωρήσεις ασφαλείας της συνάρτησης LASH–x

Η γενική δομή της συνάρτησης LASH–x, έχοντας μόνο γραμμικά συστατικά στοιχεία, εύκολα οδηγεί στην υποψία ότι είναι άμεσα ευάλωτη σε διαφορική και γραμμική κρυπτανάλυση. Η συνάρτηση αυτή έχει περάσει από διάφορα στάδια εξέλιξης από τότε που η ιδέα μίας συνάρτησης διασποράς, βασισμένης σε δικτυώματα ακεραίων, εξετάστηκε για πρώτη φορά. Η τρέχουσα έκδοση της LASH–x είναι αποτέλεσμα

συνδυασμού των παραδόσεων της θεωρητικής ασφάλειας –με αποδεδειγμένη πολυπλοκότητα– και της συμμετρικής κρυπτανάλυσης.

Κατά τον καθορισμό της ασφάλειας της LASH–x ενάντια σε αυτές τις επιθέσεις, οφείλουμε να παρατηρήσουμε ότι ως πλήρως παραμετροποιήσιμη συνάρτηση διασποράς που είναι (ευέλικτη επιλογή μεγέθους του μπλοκ μηνύματος, του μεγέθους κατάστασης και του μεγέθους του αποτελέσματος διασποράς), η προσομοίωση επιθέσεων εναντίον της είναι απλή και με νόημα. Εάν μία επίθεση μπορεί να ολοκληρωθεί με επιτυχία και να προσομοιωθεί σε μειωμένες παραλλαγές της LASH–x και να εγκαθιδρυθεί η ασυμπτωτική συμπεριφορά της ασφάλειας ως συνάρτηση διαφόρων παραμέτρων, τότε μπορούν να ληφθούν συγκεκριμένα στοιχεία σχετικά με την ασφάλεια των παραλλαγών πλήρους μεγέθους. Αυτή η ευελιξία καθιστά επίσης εύκολη τη δημιουργία μεγαλύτερων εκδόσεων της LASH–x, σε περίπτωση που βρεθούν αδυναμίες στις τρέχουσες εκδόσεις. Αυτό είναι ένα σαφές πλεονέκτημα της LASH–x απέναντι σε πολλά σχέδια συνάρτησης διασποράς με πιο άκαμπτες δομές (π.χ. με μπλοκ κρυπτογράφησης).

Η συνάρτηση LASH–x είναι ευάλωτη σε επιθέσεις σύγκρουσης (collision attacks) και σε επιθέσεις στην προεικόνα. Κρυπταναλύθηκε από μία ομάδα επτά κορυφαίων δημιουργών (S.Contini, K. Matusiewicz, J.Pieprzyk, R.Steinfeld, J.Guo, S.Ling και H.Wang) και η κρυπτανάλυσή της κατατέθηκε στο FSE 2008.

5.1.4 Οι συναρτήσεις SWIFFT και SWIFFTX

Η SWIFFT είναι μία συλλογή από συναρτήσεις συμπίεσης, υψηλά παραλληλοποιήσιμες, οι οποίες υλοποιούνται ιδιαίτερα αποδοτικά στους σύγχρονους μικροεπεξεργαστές. Βασίζονται, κυρίως, στην έννοια του γρήγορου μετασχηματισμού Fourier (Fast Fourier Transform – FFT) για να επιτύχουν τη «διάχυση»(diffusion) και χρησιμοποιούν συνδυαστικά με τον FFT και έναν γραμμικό συνδυασμό για να επιτύχουν τη συμπίεση και τη «σύγχυση» (confusion) [51].

Από την παραδοσιακή άποψη για το σχεδιασμό συναρτήσεων διασποράς, η SWIFFT αποτελεί μία πολύ ελκυστική και διαισθητική, θα λέγαμε, πρόταση, η οποία ταυτόχρονα επιτυγχάνει τα οφέλη στιβαρότητας και αξιοπιστίας της αποδείξιμης ασυμπτωτικής ασφάλειας σύμφωνα με μία ήπια υπόθεση [51]. Οι συναρτήσεις αντιστοιχούν σε μία απλή αλγεβρική έκφραση πάνω σε έναν συγκεκριμένο πολυωνυμικό δακτύλιο, όπως θα περιγραφεί παρακάτω.

Αρχικά, θα περιγράψουμε έναν αλγόριθμο υψηλού επιπέδου για ταχεία εκτίμηση της συνάρτησης συμπίεσης SWIFFT. Ο αλγόριθμος δέχεται ως είσοδο μία δυαδική συμβολοσειρά μήκους mn (για κατάλληλες παραμέτρους m, n), η οποία μπορεί να θεωρηθεί και ως ένας $n \times m$ δυαδικός πίνακας $(x_{i,j}) \in \{0,1\}^{n \times m}$. Στη συνέχεια εκτελούνται τα δύο παρακάτω βήματα, όπου όλες οι πράξεις εκτελούνται στο $\mathbb{Z}_p$ για ένα κατάλληλο μοδιακό p:

1. Ο πίνακας εισόδου $(x_{i,j})$ αρχικά μεταποιείται, πολλαπλασιάζοντας την i–οστή γραμμή κατά w^{i-1} για $i = 1, \dots, n$ (όπου το $w \in \mathbb{Z}_p$ είναι ένα κατάλληλο, σταθερό στοιχείο). Έπειτα, υπολογίζεται ο FFT στο $\mathbb{Z}_p$ για κάθε στήλη $j = 1, \dots, m$: $\left(y_{1,j}, \dots, y_{n,j}\right) = FFT\,(w^0 \cdot x_{1,j}, \dots, w^{n-1} \cdot x_{n,j})$
   Η πράξη αυτή είναι εύκολο να αντιστραφεί και εκτελείται για να επιτευχθεί η «διάχυση», δηλαδή, για να ανακατευθούν τα bits εισόδου κάθε γραμμής.
2. Έπειτα, υπολογίζεται ένας γραμμικός συνδυασμός κατά μήκος κάθε γραμμής $i = 1, \dots, n$: $z_i = a_{i,1} \cdot y_{i,1} + \dots + a_{i,m} \cdot y_{i,m} = \sum_{j=1}^{m} a_{i,j} \cdot y_{i,j}$, όπου οι συντεταγμένες $a_{i,j} \in \mathbb{Z}_p$ είναι σταθερές ως τμήμα της περιγραφής της συνάρτησης. Η πράξη αυτή συμπιέζει την είσοδο, επιτυγχάνοντας «σύγχυση». Η έξοδος είναι το διάνυσμα $(z_1, \dots, z_n) \in \mathbb{Z}_p^n$ [51].

Ας επιχειρήσουμε τώρα να αντιστρέψουμε τη συνάρτηση, δηλαδή, να βρούμε κάποια είσοδο $(x_{i,j})$, η οποία αποτιμάται σε κάποια συγκεκριμένη έξοδο $(z_1, \dots, z_n)$. Κάθε γραμμική εξίσωση $z_i = \sum_{j=1}^{m} a_{i,j} \cdot y_{i,j}$ στις γραμμές επιδέχεται ένα μεγάλο αριθμών λύσεων, εύκολα υπολογίσιμων. Παρόλα αυτά, υπάρχουν ισχυρές εξαρτήσεις μεταξύ των εξισώσεων. Συγκεκριμένα, κάθε στήλη $\left(y_{1,j}, \dots, y_{n,j}\right)$ περιορίζεται να είναι το αποτέλεσμα της εφαρμογής του βήματος 1 σε ένα n–διάστατο δυαδικό διάνυσμα $(x_{1,j}, \dots, x_{n,j}) \in \{0,1\}^n$ [51].

Ίσως απροσδόκητα, αυτοί οι περιορισμοί αποδεικνύονται να είναι επαρκείς ώστε να εγγυηθούν ασυμπτωτικά ότι οι συναρτήσεις της «οικογένειας» SWIFFT είναι αποδεδειγμένα μονόδρομες και ανθιστάμενες στις συγκρούσεις. Ακριβέστερα, οι συναρτήσεις αυτές επιδέχονται μία ισχυρή μείωση ασφαλείας: η εύρεση συγκρούσεων στη μέση περίπτωση (όταν οι συντεταγμένες $a_{i,j}$ επιλέγονται τυχαία στο $\mathbb{Z}_p$) με κάποια αξιοσημείωτη πιθανότητα είναι τουλάχιστον τόσο δύσκολη όσο και η επίλυση ενός υποκείμενου μαθηματικού προβλήματος σε συγκεκριμένα είδη δικτυωμάτων σημείου στη χειρότερη περίπτωση. Ο ισχυρισμός αυτός προκύπτει από το γεγονός ότι οι

συναρτήσεις SWIFFT αποτελούν μία ειδική περίπτωση των συναρτήσεων [54, 69, 50], οι οποίες είναι βασισμένες σε κυκλικά (cyclic) και ιδεώδη (ideal) δικτυώματα [51].

Ο απλός σχεδιασμός των συναρτήσεων SWIFFT έχει πολλά πλεονεκτήματα. Πρώτον, επιτρέπει άνευ όρων αποδείξεις για μία ευρεία ποικιλία στατιστικών ιδιοτήτων οι οποίες είναι επιθυμητές σε πολλές εφαρμογές των συναρτήσεων διασποράς, τόσο στην κρυπτογραφία, όσο και σε άλλους τομείς. Δεύτερον, η υποκείμενη μαθηματική δομή των συναρτήσεων SWIFFT είναι στενά συνδεδεμένη με καλά μελετημένα κρυπτογραφικά προβλήματα, πράγμα το οποίο επιτρέπει την εύκολη κατανόηση και ανάλυση των συγκεκριμένα συναρτήσεων. Τρίτον, οι συναρτήσεις της «οικογένειας» SWIFFT είναι εξαιρετικά παραλληλοποιήσιμες και επιδέχονται υλοποιήσεις σε λογισμικό με απόδοση συγκρίσιμη με (ή ακόμη και πάνω από) την «οικογένεια» SHA – 2 για σύγχρονους μικροεπεξεργαστές [51].

Αλγεβρική Περιγραφή των συναρτήσεων SWIFFT

Οι συναρτήσεις αντιστοιχούν σε μία απλή αλγεβρική έκφραση πάνω σε έναν συγκεκριμένο πολυωνυμικό δακτύλιο. Περιγράφονται από τρεις, κύριες παραμέτρους: n, m και p. Έστω n μία δύναμη του 2, έστω $m > 0$ ένας μικρός ακέραιος και έστω $p > 0$ ένα μοδιακό (όχι *απαραίτητα* πρώτο, παρόλο που θα δούμε στη συνέχεια ότι θα είναι βολικό συγκεκριμένο πρώτο μοδιακό p). Έστω R ένας δακτύλιος, με $R = \frac{\mathbb{Z}_p[a]}{a^n+1}$, δηλαδή, ο πολυωνυμικός δακτύλιος (στο α) έχει ακέραιες στο μοδιακό p και $\alpha^n + 1$. Οποιοδήποτε στοιχείο του R μπορεί, συνεπώς, να γραφεί ως ένα πολυώνυμο βαθμού $< n$, το οποίο έχει συντελεστές στο $\mathbb{Z}_p = \{0, \dots, p-1\}$.

Μία συγκεκριμένη συνάρτηση SWIFFT μπορεί να προσδιορισθεί από m σταθερά στοιχεία $\alpha_1, \dots, \alpha_m \in R$ του δακτυλίου R, τα οποία ονομάζονται «πολλαπλασιαστές» (multipliers). Η συνάρτηση αντιστοιχεί στην παρακάτω έκφραση πάνω στο δακτύλιο R: $\sum_{i=1}^{m}(\alpha_i \cdot x_i) \in R$, όπου $x_1, \dots, x_m \in R$ είναι πολυώνυμα που έχουν δυαδικούς συντελεστές και αντιστοιχούν στη δυαδική είσοδο μήκους mn [51].

Για τον υπολογισμό της παραπάνω έκφρασης, η κύρια επιβάρυνση προκαλείται από τον υπολογισμό των πολυωνυμικών γινομένων $\alpha_i \cdot x_i$ στο δακτύλιο R. Είναι ευρέως γνωστό ότι ο γρήγορος μετασχηματισμός Fourier (Fast Fourier Transform – FFT) παρέχει έναν αλγόριθμο με χρονική πολυπλοκότητα $O(n\, logn)$, ο οποίος μπορεί να χρησιμοποιηθεί για τον πολλαπλασιασμό πολυωνύμων βαθμού $< n$. Ο αλγόριθμος πολλαπλασιασμού ξεκινά χρησιμοποιώντας τον FFT για να υπολογίσει μεμιάς όλους

τους συντελεστές Fourier για κάθε πολυώνυμο, δηλαδή, τις τιμές σε όλες τις $2n$–οστές ρίζες του συνόλου των δύο πολυωνύμων στο σώμα $\mathbb{C}$ των μιγαδικών αριθμών. Έπειτα, πολλαπλασιάζει τους αντίστοιχους συντελεστές Fourier των δύο πολυωνύμων και τελικά, παρεμβάλλει προς τα πίσω σε ένα πολυώνυμο βαθμού $< 2n$ μέσω ενός αντίστροφου μετασχηματισμού FFT [51].

Για τις κύριες παραμέτρους n, m και p των συναρτήσεων SWIFFT προτείνεται από τους σχεδιαστές τους να επιλέγονται οι τιμές $n = 64$, $m = 16$ και $p = 257$. Οι λόγοι επιλογής αυτών των τιμών σχετίζονται με την ασφάλεια της συνάρτησης συμπίεσης και την αποδειξιμότητα αυτής της ασφάλειας, με τη βελτιστοποίηση του χρόνου εκτέλεσης και του χώρου της συνάρτησης και την αποδοτικότητα του υπολογισμού του γρήγορου μετασχηματισμού Fourier. Συγκεκριμένα, η συνάρτηση συμπίεσης αντιστοιχεί σε ένα άθροισμα υποσυνόλων (subset–sum) από mn bits σε περίπου $n\,logp$ bits. Έχουν τεθεί οι περιορισμοί $mn = 1024$ και $n\,logp \approx 512$, επειδή τέτοια προβλήματα αθροίσματος υποσυνόλων φαίνεται να είναι δυσεπίλυτα. Επίσης, για την αποδειξιμότητα της ασφάλειας της συνάρτησης συμπίεσης, είναι απαραίτητο το πολυώνυμο $\alpha^n + 1$ να είναι ανάγωγο στο $\mathbb{Z}[\alpha]$, πράγμα το οποίο αληθεύει εάν και μόνο εάν η παράμετρος n είναι μία δύναμη του 2. Εάν χρησιμοποιηθεί ένα μη ανάγωγο πολυώνυμο, είναι δυνατόν να υπάρξουν πραγματικές επιθέσεις. Ο χρόνος εκτέλεσης και ο χώρος της συνάρτησης βελτιστοποιείται, εάν επιλεγεί η παράμετρος n να είναι μεγάλη και οι παράμετροι m και p να είναι μικρές (υπόκεινται στους παραπάνω περιορισμούς). Ο γρήγορος μετασχηματισμός Fourier είναι πιο αποδοτικός και εύκολα υπολογίσιμος, όταν η παράμετρος p είναι ένας πρώτος αριθμός και το $p - 1$ είναι πολλαπλάσιο του $2n$. Η τιμή $n = 64$ είναι η μεγαλύτερη δύναμη του 2 για την οποία υπάρχει ένα τέτοιο p [51].

Η συνάρτηση SWIFFTX

Η συνάρτηση SWIFFTX αποτελεί τροποποίηση της «οικογένειας» συναρτήσεων SWIFFT και προτάθηκε ως υποψήφια συνάρτηση για τη SHA - 3 στον αντίστοιχο διαγωνισμό συνάρτησης διασποράς του NIST [51], όμως απορρίφθηκε στον πρώτο γύρο, για λόγους, οι οποίοι σε γενικές γραμμές σχετίζονται με αδυναμίες στις σχεδιαστικές συνιστώσες ή ζητήματα επίδοσης. Οι συναρτήσεις συμπίεσης SWIFFTX έχουν έναν απλό και μαθηματικά κομψό σχεδιασμό. Αυτό τις καθιστά ιδιαίτερα δεκτικές σε

ανάλυση και βελτιστοποίηση [15]. Επιπλέον, απολαμβάνουν δύο, όχι και τόσο συνηθισμένα, χαρακτηριστικά:

1. **Ασυμπτωτική απόδειξη της ασφάλειας**: μπορεί να αποδειχθεί επισήμως ότι η εξεύρεση μιας σύγκρουσης σε μία τυχαία επιλεγμένη συνάρτηση συμπίεσης από την οικογένεια SWIFFTX είναι τουλάχιστον τόσο δύσκολο όσο η εξεύρεση βραχέων διανυσμάτων σε κυκλικά και ιδεώδη πλέγματα στη χειρότερη περίπτωση [15].
2. **Υψηλή παραλληλοποίηση**: η συνάρτηση συμπίεσης επιδέχεται αποτελεσματικές υλοποιήσεις στους σύγχρονους μικροεπεξεργαστές. Αυτό μπορεί να επιτευχθεί μέσω μιας νέας κρυπτογραφικής χρήσης του Fast Fourier Transform (FFT). Το κύριο δομικό στοιχείο των συναρτήσεων SWIFFTX είναι η «οικογένεια» SWIFFT συναρτήσεων συμπίεσης, οι οποίες παρουσιάσθηκαν το 2008 στο FSE. Κατά το σχεδιασμό της SWIFFTX, δόθηκε μεγάλη προσοχή στο να διασφαλισθεί ότι αυτή δεν κληρονομεί το μεγάλο μειονέκτημα της SWIFFT, τη γραμμικότητα (linearity), διατηρώντας παράλληλα την αποδεδειγμένη της αντίσταση σε συγκρούσεις. Η συνάρτηση συμπίεσης SWIFFTX αντιστοιχίζει 2048 bits εισόδου σε 520 bits εξόδου [15]. Περισσότερες πληροφορίες για τη SWIFFTX θα βρείτε στο άρθρο [15] των Y.Arbitman, G.Dogon, V.Lyubashevsky, D.Micciancio, C.Peikert και A.Rosen.

5.2 Ψηφιακές Υπογραφές

Με τον όρο «Ψηφιακή Υπογραφή» αναφερόμαστε σε ένα μαθηματικό σύστημα, το οποίο χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου [98]. Σύμφωνα με τον Menezes [7], ψηφιακή υπογραφή είναι μία συμβολοσειρά δεδομένων η οποία συσχετίζει ένα μήνυμα (σε ψηφιακή μορφή) με κάποια δημιουργό οντότητα.

Μία έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε ή παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης διασποράς (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασύμμετρη κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και

κρυπτογράφησης με ασύμμετρη κρυπτογραφία αποδεικνύει την ακεραιότητα του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα) [98].

Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της ευρωπαϊκής ένωσης οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται και εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε η ψηφιακή υπογραφή να είναι έγκυρη, ακόμα και εάν το ιδιωτικό κλειδί υποκλαπεί. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών) [98].

Ένα σχήμα (ή μηχανισμός) ψηφιακών υπογραφών συνίσταται σε έναν αλγόριθμο παραγωγής υπογραφών και έναν αντίστοιχο αλγόριθμο επαλήθευσης. Ο πρώτος είναι μία μέθοδος παραγωγής μιας ψηφιακής υπογραφής και ο δεύτερος είναι μία μέθοδος για την επιβεβαίωση της αυθεντικότητας μιας ψηφιακής υπογραφής (αποδεικνύει, δηλαδή, ότι όντως δημιουργήθηκε από την καθορισμένη οντότητα) [7]. Άλλες βασικές έννοιες σχετικές με τις ψηφιακές υπογραφές είναι η διεργασία υπογραφής ψηφιακών υπογραφών και η διεργασία επαλήθευσης ψηφιακών υπογραφών. Μία διεργασία υπογραφής ψηφιακών υπογραφών (ή διαδικασία) συνίσταται σε έναν (μαθηματικό) αλγόριθμο παραγωγής ψηφιακών υπογραφών, μαζί με μια μέθοδο μορφοποίησης των δεδομένων σε μηνύματα τα οποία μπορούν να υπογραφούν. Μία διεργασία επαλήθευσης ψηφιακών υπογραφών (ή διαδικασία) συνίσταται σε έναν αλγόριθμο επαλήθευσης, μαζί με μια μέθοδο ανάκτησης δεδομένων από το μήνυμα [1].

Για να χρησιμοποιήσουμε στην πράξη ένα σχήμα ψηφιακών υπογραφών είναι αναγκαίο να έχουμε μία διεργασία ψηφιακών υπογραφών. Οι πιο γνωστές τέτοιες

διεργασίες, συνδεδεμένες με διάφορα σχήματα ως σχετικά εμπορικά πρότυπα είναι η ISO/IEC 9796 και η PKCS #1 [7].

5.2.1 Ιστορικά Στοιχεία

Το 1976 οι Diffie και Hellman παρουσίασαν για πρώτη φορά την ιδέα των ψηφιακών υπογραφών, αν και η κεντρική ιδέα τέτοιων συστημάτων προϋπήρχε. Λίγο αργότερα οι Rivest, Shamir και Adleman παρουσίασαν τον αλγόριθμο RSA, ο οποίος χρησιμοποιήθηκε στις πρώτες ψηφιακές υπογραφές. Οι πρώτες ψηφιακές υπογραφές με τον αλγόριθμο RSA αποδείχθηκαν ότι δεν ήταν ασφαλείς. Το πρώτο, ευρέος γνωστό στην αγορά, λογισμικό που χρησιμοποίησε τέτοιες ψηφιακές υπογραφές ήταν το Lotus Notes 1.0, το οποίο κυκλοφόρησε το 1989.

Η χρήση της συνάρτησης διασποράς στις ψηφιακές υπογραφές προστέθηκε αργότερα για λόγους ασφάλειας. Η ιδέα είναι ότι υπολογίζεται η σύνοψη (hash) του μηνύματος/εγγράφου και η ψηφιακή υπογραφή υπολογίζεται πάνω στη σύνοψη (hash) και όχι στο μήνυμα/έγγραφο. Άλλοι αλγόριθμοι που αναπτύχθηκαν μετά το RSA ήταν οι ψηφιακές υπογραφές Lamport οι ψηφιακές υπογραφές Merkle (γνωστές ως δένδρα Merkle ή απλούστερα "δένδρα συνόψεων/hash trees") και οι ψηφιακές υπογραφές Rabin.

Το 1988 ο Shafi Goldwasser, ο Silvio Micali και ο Ronald Rivest ήταν οι πρώτοι που δημοσίευσαν ολοκληρωμένη μελέτη για τις απαιτήσεις ασφάλειας των ψηφιακών υπογραφών. Παρουσίασαν με ποιους τρόπους κάποιος μπορεί να παραβιάσει τις υπάρχουσες υλοποιήσεις ψηφιακών υπογραφών καθώς και το μοντέλο ψηφιακών υπογραφών GMR.

Οι πρόσφατες υλοποιήσεις ψηφιακών υπογραφών είναι παρόμοιας τεχνικής: χρησιμοποιούν μία συνάρτηση της οποίας η έξοδος δεν είναι προβλέψιμη από την είσοδο (trapdoor function), όπως η συνάρτηση RSA. Η κύρια τεχνική είναι ότι η ψηφιακή υπογραφή είναι η σύνοψη (hash) του μηνύματος κρυπτογραφημένη με το ιδιωτικό κλειδί (χρησιμοποιώντας ασύμμετρη κρυπτογραφία). Υπάρχουν διάφοροι λόγοι που ουσιαστικά εφαρμόζεται η ψηφιακή υπογραφή στη σύνοψη του μηνύματος (hash) και όχι σε ολόκληρο το μήνυμα/έγγραφο, οι οποίοι είναι:

- Αποτελεσματικότητα (efficiency): Η ψηφιακή υπογραφή είναι πολύ μικρότερη σε μέγεθος και χρειάζεται λιγότερος χρόνος για να εφαρμοστεί (η σύνοψη (hash) έχει πολύ μικρότερο μέγεθος από ότι ολόκληρο το μήνυμα/έγγραφο).
- Συμβατότητα (compatibility): Τα μηνύματα/έγγραφα είναι ουσιαστικά μεταβλητές δέσμες bits. Ο αλγόριθμος διασποράς μπορεί να μετατρέψει μεταβλητού μεγέθους δέσμες bits σε συγκεκριμένο αριθμό bits (σύνοψη – hash).
- Ακεραιότητα (integrity): Εάν δεν εφαρμοστεί η συνάρτηση διασποράς το αρχικό μήνυμα/έγγραφο θα πρέπει να διαιρεθεί σε μικρότερα μεγέθη bits (πακέτα bits), ώστε ο αλγόριθμος ψηφιακών υπογραφών να εφαρμοστεί σε αυτά. Ο αποδέκτης των πακέτων bits δεν είναι σε θέση να αναγνωρίσει εάν όλα τα πακέτα έχουν έρθει και εάν βρίσκονται στη σωστή σειρά.

5.2.2 Το σχήμα GGH

Εκτός από το κρυπτοσύστημα GGH, οι Goldreich, Goldwasser και Halevi ανέπτυξαν το 1995 και ένα GGH σχήμα ψηφιακής υπογραφής, το οποίο δημοσιεύθηκε το 1997. Το GGH είναι ένα σχήμα ψηφιακών υπογραφών που βασίστηκε στην επίλυση του προβλήματος εγγύτερου διανύσματος (CVP) σε ένα δικτύωμα. Ο υπογράφων (signer) αποδεικνύει τη γνώση μίας καλής βάσης του δικτυώματος, χρησιμοποιώντας την για την επίλυση του CVP προβλήματος σε ένα σημείο, το οποίο αντιπροσωπεύει το μήνυμα. Ο επαληθευτής (verifier) χρησιμοποιεί μία κακή βάση για το ίδιο δικτύωμα για να επαληθεύσει ότι η υπό εξέταση υπογραφή είναι πραγματικά ένα σημείο του δικτυώματος και είναι αρκετά κοντά στο σημείο του μηνύματος.

Η ιδέα για αυτό το σχήμα ψηφιακής υπογραφής δεν αναπτύχθηκε λεπτομερώς στο αρχικό έγγραφο των Goldreich, Goldwasser και Halevi, το οποίο εστιάζει περισσότερο στον σχετικό αλγόριθμο κρυπτογράφησης [98]. Το σχήμα υπογραφής GGH δεν προσέλκυσε μεγάλο ενδιαφέρον στην ερευνητική βιβλιογραφία, έως ότου η εταιρεία NTRU Cryptosystems, inc., πρότεινε ένα σχετικά αποτελεσματικό σχήμα υπογραφής, το οποίο ονομάζεται NTRUSign. Οι GGH ψηφιακές υπογραφές αποτελούν τη βάση για τον αλγόριθμο υπογραφής NTRUSign [98].

Οι Gentry και Szydlo παρατήρησαν ότι το σχήμα υπογραφής GGH έχει μία ασυνήθιστη ιδιότητα (σε σχέση με τα παραδοσιακά σχήματα υπογραφής): κάθε

υπογραφή που κυκλοφορεί διαρρέει πληροφορίες σχετικά με το ιδιωτικό (μυστικό) κλειδί και όταν έχουν ληφθεί επαρκώς πολλές υπογραφές, τότε μπορεί να υπολογιστεί (έστω και προσεγγιστικά) ένας συγκεκριμένος Gram πίνακας που σχετίζεται με το ιδιωτικό κλειδί. Το γεγονός ότι οι υπογραφές GGH δεν είναι μηδενικής γνώσης μπορεί να εξηγηθεί διαισθητικά ως ακολούθως: για ένα δεδομένο μήνυμα, είναι δυνατόν να υπάρχουν πολλές έγκυρες υπογραφές και η μία που επιλέγεται από το ιδιωτικό κλειδί λέει κάτι για το ίδιο το κλειδί. Αυτή η διαρροή πληροφοριών δεν αποδεικνύει κατ' ανάγκη ότι τα συγκεκριμένα σχήματα είναι μη ασφαλή.

5.2.3 Το σχήμα NTRUsign

Το σχήμα NTRUSign, επίσης γνωστό και ως αλγόριθμος υπογραφής NTRU, είναι ένας αλγόριθμος ψηφιακής υπογραφής της κρυπτογράφησης δημοσίου κλειδιού, που βασίζεται στο GGH σχήμα υπογραφής, αλλά χρησιμοποιεί και συμπαγή NTRU δικτυώματα. Αρχικά, επρόκειτο για ένα σχετικά αποτελεσματικό σχήμα υπογραφής, με μήκος υπογραφής μόλις 1757 bits, το οποίο παρουσιάστηκε για πρώτη φορά το 2001 (Asiacrypt) και δημοσιεύθηκε το 2003 (RSA Conference). Κάποιες ατέλειες στο σχήμα NTRUsign επισημάνθηκαν το 2006 από τους Gentry και Szydlo. Πλέον το σχήμα αυτό έχει κρυπταναλυθεί, από τους L. Ducas και P.Q. Nguyen το 2012 , οπότε η αναφορά του εδώ γίνεται μόνο από ιστορικό ενδιαφέρον.

Η δημοσίευση του 2003 περιλαμβάνει συστάσεις παραμέτρων για ασφάλεια 80–bit. Η μεταγενέστερη έκδοση του 2005 αναθεώρησε τις συστάσεις παραμέτρων για ασφάλεια 80–bit, παρουσίασε παραμέτρους που έδωσαν επίπεδα ισχυριζόμενης ασφαλείας των 112, 128, 160, 192 και 256 δυαδικών ψηφίων (bits) και περιέγραψε έναν αλγόριθμο για τον υπολογισμό συνόλων παραμέτρων σε οποιοδήποτε επιθυμητό επίπεδο ασφάλειας.

Ο αλγόριθμος ψηφιακής υπογραφής NTRUSign είχε έναν πρόγονο, το σχήμα NSS (NTRU Signature Scheme) [62] λιγότερο σχετικό με το GGH σχεδιασμό και το οποίο είχε κρυπταναλυθεί το 2001 στο [24]. Στη συνέχεια, παρατίθεται ενδεικτικά ένας πίνακας με κάποια συγκριτικά στοιχεία σχετικά με τον αλγόριθμο NSS, τον RSA και τον ECDSA.

Πίνακας 5.2.3.1 Σύγκριση των NSS, RSA και ECDSA

	Pentium	**Palm**
NSS υπογραφή	0,35 ms	0,33 sec
RSA υπογραφή	66,56 ms	36,13 sec
ECDSA υπογραφή	1,18 ms	1,79 sec
NSS επαλήθευση	0,29 ms	0,25 sec
RSA επαλήθευση	1,23 ms	0,73 sec
ECDSA επαλήθευση	1,70 ms	3,26 sec

Ο αλγόριθμος ψηφιακής υπογραφής NTRUSign περιλαμβάνει τη χαρτογράφηση ενός μηνύματος σε ένα τυχαίο σημείο στον 2N–διαστάσεων χώρο (όπου το N είναι μία από τις παραμέτρους NTRUSign) και την επίλυση του προβλήματος CVP σε ένα δικτύωμα, στενά συνδεδεμένο με το δικτύωμα που χρησιμοποιείται στον αλγόριθμο NTRUEncrypt . Αυτό το δικτύωμα έχει την ιδιότητα ότι μία ιδιωτική βάση 2N–διαστάσεων για το δικτύωμα μπορεί να περιγραφεί με 2 διανύσματα, το καθένα με N συντελεστές και μία δημόσια βάση μπορεί να περιγραφεί με ένα μόνο N–διάστατο διάνυσμα . Αυτό επιτρέπει στα δημόσια κλειδιά να αναπαρίστανται στο O(N) χώρο, παρά στον O(N^2), όπως συμβαίνει με άλλα σχήματα υπογραφής βασισμένα σε δικτυώματα. Οι συναρτήσεις λαμβάνουν O(N^2) χρόνο για να εκτελεστούν, σε αντίθεση με την ελλειπτική κρυπτογραφία (ECC) και τις λειτουργίες του ιδιωτικού κλειδιού στον αλγόριθμο RSA, οι οποίες απαιτούν O(N^3) χρόνο. Ο NTRUSign επομένως φέρεται να είναι πιο γρήγορος από τους αλγορίθμους RSA και ECC σε χαμηλά επίπεδα ασφάλειας και πολύ πιο γρήγορος σε υψηλά επίπεδα ασφάλειας [98].

Όσον αφορά την ασφάλεια του NTRUSign, το σχήμα αυτό δεν είναι ένα σχήμα υπογραφής μηδενικής γνώσης και ένα αντίγραφο των υπογραφών διαρρέει πληροφορίες σχετικά με το ιδιωτικό κλειδί, όπως παρατηρήθηκε για πρώτη φορά από τους Gentry και Szydlo. Οι Nguyen και Regev απέδειξαν το 2006 ότι για το αρχικό αδιατάρακτο σύνολο

παραμέτρων του NTRUSign, ένας επιτιθέμενος μπορεί να ανακτήσει το ιδιωτικό κλειδί με μόνο 400 υπογραφές. Συνεπώς, ο αλγόριθμος NTRUsign χωρίς διαταραχές θα πρέπει να θεωρείται εντελώς μη ασφαλής.

Οι τρέχουσες προτάσεις χρησιμοποιούν διαταραχές (perturbations) για να αυξήσουν το απαιτούμενο μήκος του αντιγράφου για την ανάκτηση του ιδιωτικού κλειδιού: ο υπογράφων εκτοπίζει το σημείο που αντιπροσωπεύει το μήνυμα κατά ένα μικρό, μυστικό ποσό πριν από τον υπολογισμό της ίδιας της υπογραφής. Με μία και μόνο διαταραχή, το πλήθος των απαιτούμενων υπογραφών για ανάκτηση του ιδιωτικού κλειδιού αυξάνεται ραγδαία (ίσως και εκατομμύρια ή ακόμα και δισεκατομμύρια υπογραφές, σε κάποιες περιπτώσεις). Η χρήση των διαταραχών στο NTRUsign θεωρούνταν ότι εγγυάται πως ο αριθμός των υπογραφών που απαιτείται για την εξαγωγή πληροφοριών υπερβαίνει κατά πολύ οποιεσδήποτε πρακτικές απαιτήσεις. Όμως, το 2012 παρουσιάστηκε μία επίθεση στο σχήμα με τις διαταραχές, η οποία απαιτούσε μόνο μερικές χιλιάδες υπογραφές (συγκεκριμένα, 90.000 υπογραφές) για πρότυπες παραμέτρους ασφαλείας. Από τα παραπάνω συμπεραίνουμε ότι και η χρήση διαταραχής δε διασφαλίζει την αξιοπιστία του αλγόριθμου NTRUsign.

Κεφάλαιο 6
Συμπεράσματα – Μελλοντική Έρευνα

6.1 Σύνοψη και συμπεράσματα

Η μετα–κβαντική κρυπτογραφία αποτελεί μία συναρπαστική ερευνητική πρόκληση της σύγχρονης εποχής, η οποία θα διαδραματίσει καθοριστικό ρόλο όσον αφορά το μέλλον του Διαδικτύου, σε περίπτωση που η κατασκευή κβαντικών υπολογιστών για διεθνείς επικοινωνίες γίνει κάποτε μία τεχνολογική πραγματικότητα.

Η διπλωματική αυτή εργασία είχε ως αντικείμενό της το τμήμα εκείνο της μετα-κβαντικής κρυπτογραφίας που βασίζεται σε δικτυώματα ακέραιων αριθμών. Στο πλαίσιο αυτής και αφότου παρατέθηκε το απαιτούμενο μαθηματικό υπόβαθρο παρουσιάστηκαν επιμέρους ζητήματα αυτού του θέματος, όπως:

- ✓ Κάποια δυσεπίλυτα προβλήματα που ανακύπτουν από τη χρήση των δικτυωμάτων και τα οποία εκμεταλλευόμαστε για κρυπτογραφικούς σκοπούς (για ανάπτυξη είτε κρυπτοσυστημάτων, είτε σχημάτων ψηφιακών υπογραφών)
- ✓ Κάποιοι αλγόριθμοι, οι οποίοι χρησιμοποιούνται για αναγωγή της βάσης ενός δικτυώματος (χρήσιμη κυρίως στην κρυπτανάλυση με δικτυώματα)
- ✓ Κάποια κρυπτοσυστήματα που έχουν αναπτυχθεί με δικτυώματα (δημιουργία κλειδιών – κρυπτογράφηση – αποκρυπτογράφηση)
- ✓ Οι πιο βασικές συναρτήσεις διασποράς αυτού του είδους (LASH–x, SWIFFT και SWIFFTX)
- ✓ Τα πιο σημαντικά σχήματα ψηφιακών υπογραφών αυτού του είδους (GGH και NTRUSign)

Από την έρευνα σχετικά με τα παραπάνω ζητήματα καταλήξαμε στο συμπέρασμα ότι μπορεί το μαθηματικό υπόβαθρο να προϋπήρχε για τουλάχιστον πάνω από έναν αιώνα, αλλά η χρήση του για κρυπτογραφικούς σκοπούς έχει ελάχιστα (λιγότερα από 20) χρόνια που λαμβάνει χώρα. Η κρυπτογραφία που βασίζεται σε δικτυώματα ακεραίων είναι ένας σχετικά καινούριος κλάδος της κρυπτογραφίας που έχει δώσει όμως ήδη κάποια αρκετά σημαντικά κρυπτοσυστήματα και σχήματα ψηφιακών υπογραφών. Από τη μελέτη της αντίστοιχης βιβλιογραφίας, έχουμε να επισημάνουμε τα εξής:

- ✓ Πρόκειται για έναν πολλά υποσχόμενο κλάδο της κρυπτογραφίας.
- ✓ Το πιο σημαντικό πλεονέκτημα των κρυπτογραφικών προϊόντων (συστήματα, ψηφιακές υπογραφές) που περιλαμβάνουν δικτυώματα ακεραίων είναι η μετα–κβαντική τους ασφάλεια, δηλαδή η αντοχή τους σε επιθέσεις από κβαντικούς υπολογιστές.
- ✓ Επίσης σημαντικό χαρακτηριστικό τους είναι και το γεγονός ότι υποστηρίζονται από ισχυρές εγγυήσεις ασφάλειας χειρότερης περίπτωσης/μέσης περίπτωσης. Σε αποδείξεις ασφάλειας για κρυπτοσυστήματα, συνήθως υποθέτουμε ότι κάποιο πρόβλημα είναι δυσεπίλυτο, κατά μέσο όρο ή, ακριβέστερα, είναι δύσκολο να επιλυθεί για τυχαίες περιπτώσεις που προέρχονται από κάποια συγκεκριμένη διανομή. Για παράδειγμα , μπορούμε να υποθέσουμε ότι η παραγοντοποίηση ενός γινομένου δύο τυχαίων πρώτων αριθμών δεν μπορεί να γίνει με έναν πολυωνυμικό αλγόριθμο. Εάν και αυτό είναι συνήθως ασφαλές, είναι κατ 'αρχήν δυνατό κάποιος να βρει έναν αποτελεσματικό αλγόριθμο παραγοντοποίησης, ο οποίος να λειτουργεί συχνά σε τυχαίες περιπτώσεις, αλλά όχι σε όλες τις περιπτώσεις. Η κρυπτογραφία με χρήση δικτυωμάτων δεν υποφέρει από αυτό το μειονέκτημα. Τέτοια σχήματα αποδεικνύονται ασφαλή, υποθέτοντας ότι τα προβλήματα με δικτυώματα είναι δυσεπίλυτα στη χειρότερη περίπτωση, που σημαίνει ότι είναι ασφαλή για όσο διάστημα δεν μπορεί κανείς να βρει, ας πούμε, έναν αλγόριθμο πολυωνυμικού χρόνου για να προσεγγίσει τα βραχύτερα διανύσματα σε κάθε δικτύωμα, όχι απλά σε τυχαία δικτυώματα. Αυτή είναι μία τεράστια θεωρητική εξέλιξη, αλλά είναι δύσκολο να καθοριστεί πού ακριβώς θα οδηγήσει σε πρακτικό επίπεδο.
- ✓ Η κρυπτογραφία αυτή έχει αποδειχθεί να είναι πολύ ευέλικτη και αποτελεσματική, χαρακτηριστικό το οποίο οδηγεί σε μια άνευ προηγουμένου ποικιλία εφαρμογών. Συστήματα τέτοιου τύπου έχουν μία παραλληλοποιήσιμη δομή που μπορεί να τα κάνει ακόμα πιο γρήγορα σε ορισμένες περιπτώσεις. Αυτό συμβαίνει επειδή οι αλγόριθμοι που εμπλέκονται χρησιμοποιούν συνήθως απλό πολλαπλασιασμό πινάκων με σχετικά μικρό ποσοστό μοδιακής αριθμητικής.

6.2 Όρια και περιορισμοί της έρευνας

Δεδομένου του τίτλου που επιλέχθηκε για αυτήν τη διπλωματική εργασία, μπορεί κανείς να υποθέσει ότι στα πλαίσια αυτής δε θα γίνεται επεξηγηματική παρουσίαση από οτιδήποτε αφορά τον τομέα της κρυπτανάλυσης, είτε πρόκειται για κρυπταναλυτικές επιθέσεις σε διάφορους αλγόριθμους, είτε για επιθέσεις στο κανάλι επικοινωνίας, είτε για τα διάφορα είδη και τις μεθόδους κρυπτανάλυσης που χρησιμοποιήθηκαν σε παλαιότερα αλλά και σε σύγχρονα κρυπτοσυστήματα. Οτιδήποτε αφορά τον τομέα της κρυπτανάλυσης απλά αναφέρεται εδώ και δε λαμβάνει περαιτέρω επεξήγηση.

Επιπρόσθετα, όπως αναφέρθηκε και στην εισαγωγή, τα όρια της παρούσης έρευνας δεν περιλαμβάνουν πιο πρόσφατα σχετικά με την κρυπτογραφία αυτού του είδους αντικείμενα, όπως το πρόβλημα της μάθησης με σφάλματα (Learning with Errors – LWE) του Oded Regev [73] που διατυπώθηκε το 2005, το πρόβλημα της μικρής το πρόβλημα της μικρής ακέραιας λύσης (Short Integer Solution – SIS) [11], το σχήμα πλήρως ομομορφικής κρυπτογράφησης (Fully Homomorphic Encryption – FHE) του Craig Gentry [28] που διατυπώθηκε το 2009, κ.ά.

6.3 Μελλοντικές Επεκτάσεις

Η παρούσα διπλωματική εργασία, ως ένα εισαγωγικό πόνημα στην κρυπτογραφία με χρήση δικτυωμάτων ακεραίων μπορεί να επιδεχθεί πληθώρα βελτιώσεων και επεκτάσεων. Άλλωστε, υπάρχει ακόμη πολλή δουλειά να γίνει στην κρυπτογράφηση που βασίζεται σε δικτυώματα ακεραίων και ακόμη περισσότερη δουλειά χρειάζεται για να αυξηθεί η εμπιστοσύνη και η κατανόηση στον τομέα αυτό, και προκειμένου να αρχίσει η κρυπτογραφία αυτού του είδους να χρησιμοποιείται σε ευρεία κλίμακα.

Τα διάφορα ανοιχτά προβλήματα αυτής της ερευνητικής περιοχής αποτελούν στην ουσία προκλήσεις για περαιτέρω έρευνα. Καταρχάς, κάποια δικτυώματα με ειδική αλγεβρική δομή, όπως είναι τα κυκλικά και τα ιδεώδη, πρέπει να μελετηθούν με μεγαλύτερη λεπτομέρεια, καθώς διαφαίνεται ότι μπορούν να προσφέρουν σημαντική αποτελεσματικότητα, αλλά μέχρι τώρα δεν είναι γνωστά πάρα πολλά χαρακτηριστικά τους στοιχεία. Από αλγοριθμική άποψη, ελάχιστα γνωρίζουμε για την υπολογιστική πολυπλοκότητα των προβλημάτων βελτιστοποίησης σε δικτυώματα, όταν αυτά έχουν κυκλική δομή και συνεπώς, δεν είναι ξεκάθαρο το πώς μπορούμε να εκμεταλλευτούμε τη

δομή ενός κυκλικού δικτυώματος στους αλγόριθμους αναγωγής της βάσης του. Η πρόταση για τη χρήση κυκλικών δικτυωμάτων ως μία νέα πηγή υποθέσεων δυσεπιλυσιμότητας ήρθε μέσα από το έργο του D.Micciancio [54], το οποίο αποτέλεσε εφαλτήριο για μελέτη των κυκλικών δικτυωμάτων από υπολογιστική άποψη. Υπάρχουν, επίσης, κάποιες εργασίες [53] που δείχνουν πώς η διαδικασία επίλυσης συγκεκριμένων προβλημάτων σε δικτυώματα μπορεί να επιταχυνθεί κατά έναν παράγοντα n, όταν το δικτύωμα είναι κυκλικό, διάστασης n.

Οι μελλοντικές κατευθύνσεις έρευνας σχετίζονται, επίσης, με την αποδειξιμότητα της ασφάλειας των συναρτήσεων διασποράς που χρησιμοποιούνται στην κρυπτογραφία αυτού του είδους. Μετά την κρυπτανάλυση της LASH–x, έχουν προταθεί διάφορες καινούριες συναρτήσεις διασποράς (π.χ. SWIFFT με γρήγορους μετασχηματισμούς Fourier, SWIFFTX κ.ά.), οι οποίες είναι ασφαλείς μόνο σε θεωρητικό επίπεδο, έως ότου δηλαδή κάποιος εντοπίσει μία κατάλληλη ιδιότητά τους και επισημάνει μία αδυναμία.

Ένα ακόμη άλυτο πρόβλημα αυτής της περιοχής είναι η κατασκευή ενός κρυπτοσυστήματος που να είναι ταυτόχρονα ασφαλές και αποδοτικό. Υπενθυμίζουμε ότι το πιο γνωστό και πρακτικό κρυπτοσύστημα αυτού του είδους, το NTRU, είναι αρκετά αποδοτικό, αλλά εάν και έχει αντισταθεί σθεναρά σε διαφόρων ειδών επιθέσεις, η ασφάλεια του δεν έχει αποδειχθεί. Η επιστημονική κοινότητα προτείνει κατά καιρούς καινούρια κρυπτοσυστήματα ή παραλλαγές του NTRU, όμως η αποδειξιμότητα της ασφάλειάς τους παραμένει ένα μείζον ζήτημα.

Το κρυπτοσύστημα που πρότεινε ο O.Regev, το οποίο βασίζεται στο πρόβλημα μάθησης με σφάλματα (Learning with Errors–LWE) [73] είναι αρκετά αποτελεσματικό και έχει αποδεδειγμένη ασφάλεια, βασισμένη στη χειρότερη περίπτωση. Παρόλα αυτά, θα μπορούσε κανείς να ελπίζει σε μία σημαντική βελτίωση της αποτελεσματικότητάς του, και ιδίως του μεγέθους του δημόσιου κλειδιού του, χρησιμοποιώντας δομημένα δικτυώματα, όπως είναι τα κυκλικά [59].

Ακόμη, εξακολουθεί να απασχολεί τους επιστήμονες το ζήτημα της εύρεσης αποδοτικών αλγορίθμων για την επίλυση του προβλήματος SVP, έστω προσεγγιστικά, σε πολυωνυμικό χρόνο. Ιδιαίτερα σημαντική θεωρείται και η απάντηση στο ερώτημα εάν μπορεί κάποιος να παραγοντοποιήσει ακεραίους ή να υπολογίσει διακριτούς λογάριθμους, χρησιμοποιώντας ένα μαντείο (oracle) το οποίο επιλύει το SVP προσεγγιστικά. Εάν κάτι τέτοιο ισχύει, θα ήταν πολύ χρήσιμο στην απόδειξη της

«ανωτερότητας» της ασφάλειας ενός κρυπτοσυστήματος βασισμένου σε δικτυώματα ακεραίων έναντι των παραδοσιακών αριθμοθεωρητικών κρυπτοσυστημάτων [59].

Τέλος, η εκτενέστερη μελέτη και κατανόηση νέων κρυπτογραφικών εργαλείων, όπως τα δένδρα Bonsai (Bonsai Trees) [23], τα οποία αναπτύχθηκαν για την επίλυση ορισμένων σημαντικών ανοικτών προβλημάτων σε αυτήν την περιοχή κρίνεται, όχι μόνο επιθυμητή, αλλά απαραίτητη. Μεγάλο ενδιαφέρον προκαλεί επίσης, το γεγονός ότι, οι αφηρημένες ιδιότητες των δέντρων Bonsai δε φαίνεται να έχουν καμία γνωστή υλοποίηση στη συμβατική αριθμοθεωρητική κρυπτογραφία.

Παράρτημα

Α1. Γενικευμένος Γκαουσιανός Αλγόριθμος (generalized Gauss algorithm – gGA)

Η γενική μορφή του Γκαουσιανού αλγόριθμου αναγωγής της βάσης ενός δισδιάστατου δικτυώματος σε ψευδογλώσσα έχει ως εξής:

ΕΙΣΟΔΟΣ Μία καλώς διατεταγμένη βάση (a, b) του δικτυώματος

ΟΣΟ $\|b\| > \|a - b\|$ **ΚΑΝΕ**

$b \leftarrow b - \mu\alpha$ **όπου** ο ακέραιος μ έχει επιλεχθεί έτσι ώστε να ελαχιστοποιεί τη νόρμα $\|b - \mu\alpha\|$

ΕΑΝ $\|a + b\| < \|a - b\|$ **ΤΟΤΕ** $b \leftarrow -b$

ΑΝΤΑΛΛΑΞΕ a και b

ΤΕΛΟΣ ΟΣΟ

ΕΞΟΔΟΣ (a, b)

Α2. Γενική Μορφή LLL

Η γενική μορφή του LLL αλγόριθμου αναγωγής της βάσης ενός n–διάστατου δικτυώματος σε ψευδογλώσσα έχει ως εξής:

$k = 2$

ΟΣΟ $k \leq n$ {

ΑΝΗΓΑΓΕ-ΚΑΤΑ-ΜΕΓΕΘΟΣ $(b_1, \ldots, b_k)$;

ΕΑΝ (συνθήκη Lovász) **ΤΟΤΕ**

{

$k = k + 1$

ΑΛΛΙΩΣ

ΑΝΤΙΜΕΤΑΘΕΣΕ $b_{k-1} \leftrightarrow b_k$ **ΚΑΙ**

ΘΕΣΕ $k = max\,\{2, k-1\}$;

}

Α3. Συνάρτηση Συμπίεσης (Compression Function) της LASH – $\boldsymbol{t} = \boldsymbol{f}\ (\boldsymbol{r}, \boldsymbol{s})$

Η συνάρτηση συμπίεσης t της συνάρτησης διασποράς LASH σε ψευδογλώσσα έχει ως εξής:

ΓΙΑ i $= 0, 1, \ldots, \mathrm{m} - 1$ **ΚΑΝΕ**

$t_i \leftarrow r_i \oplus s_i$

ΤΕΛΟΣ_ΓΙΑ

ΓΙΑ $i = 0, 1, \ldots, n$ **ΚΑΝΕ**

ΑΝ $i < 8m$ **ΤΟΤΕ**

$x \leftarrow \left\lfloor 2^{-(7-(i \bmod 8))}\, r_{\lfloor i/8 \rfloor} \right\rfloor mod\ 2$

ΑΛΛΙΩΣ

$x \leftarrow \left\lfloor 2^{-(7-(i \bmod 8))}\, s_{(\lfloor i/8 \rfloor - m)} \right\rfloor mod\ 2$

ΤΕΛΟΣ_ΑΝ

ΑΝ $x = 1$ **ΤΟΤΕ**

ΓΙΑ j $= 0, 1, \ldots, \mathrm{m} - 1$ **ΚΑΝΕ**

$t_j \leftarrow t_j + a_{((n+j-i) mod\ n)}\ mod\ 256$

ΤΕΛΟΣ_ΓΙΑ

ΤΕΛΟΣ_ΑΝ

ΤΕΛΟΣ_ΓΙΑ

ΕΠΕΣΤΡΕΨΕ $\boldsymbol{t}$

Για την αποσαφήνιση των μεταβλητών που χρησιμοποιούνται και την περαιτέρω μελέτη της συνάρτησης συμπίεσης t της συνάρτησης διασποράς LASH, παραπέμπουμε τον αναγνώστη στο άρθρο «LASH» των K.Bentahar, D.Page, G.H. Silverman, M.-J.O Saarinen και N.P. Smart.

A4. Συνάρτηση διασποράς (Hash Function)LASH

Η συνάρτηση διασποράς LASH σε ψευδογλώσσα έχει ως εξής:

ΓΙΑ i $= 0, 1, \ldots, \mathrm{m} - 1$ **ΚΑΝΕ**

$r_i = 0$

ΤΕΛΟΣ_ΓΙΑ

ΓΙΑ $i = 0, 1, \ldots, \lceil l/8m \rceil - 1$ **ΚΑΝΕ**

ΓΙΑ j $= 0, 1, \ldots, \mathrm{m} - 1$ **ΚΑΝΕ**

$s_i = u_{m \times i + j}$

ΤΕΛΟΣ_ΓΙΑ

$\boldsymbol{r} \leftarrow \boldsymbol{f}\,(\boldsymbol{r}, \boldsymbol{s})$

ΤΕΛΟΣ_ΓΙΑ

ΓΙΑ i $= 0, 1, \ldots, \mathrm{m} - 1$ **ΚΑΝΕ**

$s_i \leftarrow \lfloor l/2^{8i} \rfloor \; mod \; 256$

ΤΕΛΟΣ_ΓΙΑ

$\boldsymbol{r} \leftarrow \boldsymbol{f}\,(\boldsymbol{r}, \boldsymbol{s})$

ΓΙΑ i $= 0, 1, \ldots, \mathrm{m}/2 - 1$ **ΚΑΝΕ**

$t_i = 16\,\lfloor r_{2i}/16 \rfloor + \lfloor r_{2i+1}/16 \rfloor$

ΤΕΛΟΣ_ΓΙΑ

ΕΠΕΣΤΡΕΨΕ $\boldsymbol{t}$

Για την αποσαφήνιση των μεταβλητών που χρησιμοποιούνται και την περαιτέρω μελέτη της συνάρτησης διασποράς LASH, παραπέμπουμε τον αναγνώστη στο άρθρο «LASH» των K.Bentahar, D.Page, G.H. Silverman, M.-J.O Saarinen και N.P. Smart.

Για τη μελέτη των συναρτήσεων διασποράς SWIFFT και SWIFFTX, παραπέμπουμε τον αναγνώστη στα άρθρα «SWIFFT: A Modest Proposal for FFT Hashing» των V. Lyubashevsky, D.Micciancio, C.Peikert, A.Rosen και «SWIFFTX: A Proposal for the SHA-3 Standard» των Y.Arbitman, G.Dogon, V.Lyubashevsky, D.Micciancio, C.Peikert, A.Rosen, αντίστοιχα.

Βιβλιογραφία – Αναφορές

Α.1 Βιβλία

[1] Κάτος, Β.Α., Στεφανίδης, Γ.Χ. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης, Εκδόσεις ΖΥΓΟΣ, Θεσσαλονίκη, 2003.

[2] Birkhoff, G. 1979, Lattice theory, American Mathematical Society Colloquium Publications 25 (3rd ed.), Providence, R.I.: American Mathematical Society, ISBN 978-0-8218-1025-5, MR 598630

[3] Bremner, M.R., Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications CRC Press, 2012

[4] Fraleigh, J., B., A First Course in Abstract Algebra, 1967, Addison Wesley Publishing Company, Inc., μτφρ.: Α.Γιαννόπουλος, Ν. Μαρμαρίδης, Εισαγωγή στην Άλγεβρα, 1994, Παν. Εκδόσεις Κρήτης

[5] Grätzer, G. General Lattice Theory, 2nd ed. Boston, Birkhäuser, 1998.

[6] Hoffstein, J., Pipher, J., Silverman, J.H. 2008. An Introduction to Mathematical Cryptography (1 ed.). Springer Publishing Company, Incorporated.

[7] Menezes, A.J., P.C. van Oorschot, Vanstone, S.A., Handbook of Applied Cryptography, CRC Press, (2001), μετάφραση: Γ.Χ. Στεφανίδης, Εγχειρίδιο Εφαρμοσμένης Κρυπτογραφίας, Πανεπιστήμιο Μακεδονίας, Τμήμα Εφαρμοσμένης Πληροφορικής, Πανεπιστημιακές παραδόσεις μαθήματος, Θεσσαλονίκη (2005)

[8] Meyer, C.D., Matrix Analysis and Applied Linear Algebra (Ed.). 2000. Soc. For Industrial and Applied Math., Philadelphia, PA, USA.

[9] Priestly, H. A. and Davey, B. A. Introduction to Lattices and Order. Cambridge, England: Cambridge University Press, 1990.

[10] Zhou, T., Modified LLL Algorithms, McGill University, Canada, (2006).

Α.2 Αρθρογραφία

[11] Ajtai, M. 1996. Generating hard instances of lattice problems (extended abstract). In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (STOC '96). ACM, New York, NY, USA, 99-108.

[12] Ajtai, M. 1998. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of the thirtieth annual ACM symposium on Theory of computing* (STOC '98). ACM, New York, NY, USA, 10-19.

[13] Ajtai, M., Dwork, C. 1997. A public-key cryptosystem with worst case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*(STOC '97). ACM, New York, NY, USA, 284-293.

[14] Ajtai, M., Kumar, R., Sivakumar, D. A sieve algorithm for the shortest

lattice vector problem. In Proc. 33rd STOC, pages 601–610, 2001.

[15] Arbitman, Y., Dogon, G., Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A. 2008. SWIFFTX: A Proposal for the SHA-3 Standard. NIST, SHA-3 Competition (2007 -2012), First Round Candidates.URL: http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html [Last Accessed: 31/10/2013]

[16] Bernstein, D.J., Grover vs. McEliece., in: N. Sendrier (Ed.), PQCrypto,Vol. 6061 of Lecture Notes in Computer Science, Springer, 2010, pp.73–80.

[17] Bogdanov, A, Knudsen, L.R., Leander, G. Paar, C. Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., 2007. PRESENT: An Ultra-Lightweight Block Cipher. In *Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems* (CHES '07), Pascal Paillier and Ingrid Verbauwhede (Eds.). Springer-Verlag, Berlin, Heidelberg, 450-466.

[18] Boneh, D., Franklin, M., Identity–based encryption from the Weil pairing, Springer–Verlag, 2001, pp. 213–229.

[19] Buchmann, J. Lindner, R. 2009. Secure Parameters for SWIFFT. In *Proceedings of the 10th International Conference on Cryptology in India: Progress in Cryptology* (INDOCRYPT '09), Bimal Roy and Nicolas Sendrier (Eds.). Springer-Verlag, Berlin, Heidelberg, 1-17.

[20] Cai, J.,Y. 2000. The Complexity of Some Lattice Problems. In Proceedings of the 4t*h International Symposium on Algorithmic Number Theory* (ANTS-IV), Wieb Bosma (Ed.). Springer-Verlag, London, UK, UK, 1-32.

[21] Cai, J.Y., Cusick, T.W., A lattice–based public–key cryptosystem, in: Proceedings of the Selected Areas in Cryptography, SAC ’98, Springer–Verlag, London, UK, UK, 1999, pp. 219–233.

[22] Cai, J.Y., Nerurkar, A.P., An improved worst–case to average–case connection for lattice problems (extended abstract), in: In FOCS, IEEE, 1997, pp. 468–477.

[23] Cash, D., Hofheinz, D., Kiltz, E. Peikert, C. 2010. Bonsai trees, or how to delegate a lattice basis. In *Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT'10), Henri Gilbert (Ed.). Springer-Verlag, Berlin, Heidelberg, 523-552.

[24] Ducas, L., Nguyen, P.Q. Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures, in: Advances in Cryptology – Proceedings of ASIACRYPT ’12, LNCS, Springer, 2012.

[25] Eskicioglu, A.M., Multimedia security in group communications: recent progress in key management, authentication, and watermarking, Multimedia Syst. 9 (3) (2003), pp. 239–248.

[26] Fincke, U., Pohst, M., Improved methods for calculating vectors of short

length in a lattice, including a complexity analysis, Mathematics of Computation 44 (1985), pp. 463–471.

[27] Gama, N., Nguyen, P.Q. Regev, O. Lattice enumeration using extreme pruning. In Proc. EUROCRYPT ’10, volume 6110 of Lecture Notes in Computer Science. Springer, 2010.

[28] Gentry, C. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (STOC '09). ACM, New York, NY, USA, 169-178.

[29] Gentry, C., Jonsson, J., Stern, J., Szydlo, M., Cryptanalysis of the NTRU signature scheme (NSS) from eurocrypt 2001, in: C. Boyd (Ed.), ASIACRYPT, Vol. 2248 of Lecture Notes in Computer Science, Springer, 2001, pp. 1–20.

[30] Gentry, C., Szydlo, M., Cryptanalysis of the revised NTRU signature scheme, in: Advances in Cryptology – EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 – May 2, 2002, Proceedings, Vol. 2332 of Lecture Notes in Computer Science, Springer, 2002, pp. 299–320.

[31] Goldreich, O., Goldwasser, S., Halevi, S.1997. Public-Key Cryptosystems from Lattice Reduction Problems. In *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO '97), Burton S. Kaliski, Jr. (Ed.). Springer-Verlag, London, UK, UK, 112-131.

[32] Gong, Z. Nikova, S. and Law, Y.W. 2011. KLEIN: a new family of lightweight block ciphers. In *Proceedings of the 7th international conference on RFID Security and Privacy* (RFIDSec'11), Ari Juels and Christof Paar (Eds.). Springer-Verlag, Berlin, Heidelberg, 1-18.

[33] Gottesman, D., Chuang, I.L., Quantum digital signatures, Tech.rep.(2001).

[34] Guruswami, V., Micciancio, D., Regev, O. The complexity of the covering radius problem on lattices and codes, in: Proceedings of the 19th annual IEEE conference on computational complexity – CCC ’04, IEEE, Amherst, MA, USA, 2004, pp. 161–173, journal version in Computational Complexity.

[35] Hanrot, G. and Stehle, D. Improved analysis of Kannan’s shortest lattice vector algorithm (extended abstract). In Proc. of CRYPTO ’07, volume 4622 of LNCS, pages 170–186. Springer-Verlag, 2007.

[36] Hanrot, G., Pujol, X. and Stehlé, D. (2011). Algorithms for the Shortest and Closest Lattice Vector Problems. In *Proceedings of the Third international conference on Coding and cryptology* (IWCC'11), Yeow Meng Chee, San Ling, Huaxiong Wang, Chaoping Xing, and Zhenbo Guo (Eds.). Springer-Verlag, Berlin, Heidelberg, 159-190.

[37] Haviv, I., Regev, O. Hardness of the covering radius problem on lattices, 2013 IEEE Conference on Computational Complexity 0 (2006) 145–158.

[38] Henk, M. Note on shortest and nearest lattice vectors, Information

Processing Letters 61 (1997) 183–188.

[39] Hoffstein, J., Pipher, J. and Silverman, J., H. NTRU: a ring based public key cryptosystem. In Proc. of ANTS III, volume 1423 of LNCS, pages 267–288. Springer-Verlag, 1998. First presented at the rump session of Crypto ’96.

[40] Jiang, Y., Deng, Y., Pan, Y. Covering radius of two–dimensional lattices, IACR Cryptology ePrint Archive 2009 (2009) 539.

[41] Joux, A. Stern, J., Lattice Reduction: a Toolbox for the Cryptanalyst, 1997.Journal of Cryptology,

[42] Kaib, M., Schnorr, C.P. 1996. The Generalized Gauss Reduction Algorithm, Journal of Algorithms 21, 3, 565-578.

[43] Kannan, R. Improved algorithms for integer programming and related lattice problems. In Proc. 15th ACM Symp. on Theory of Computing (STOC), pages 193–206, 1983

[44] Kerckhof, S. Durvaux, F., Hocquet, C., Bol, D., Standaert, F.X., Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint, in: CHES, Vol. 7428, Springer, 2012, pp. 390–407.

[45] Korkine, A., Zolotareff, G., Sur les formes quadratiques, Mathematische Annalen 6 (3) (1873) 366–389.

[46] Lagrange, L. Recherches d’arithm´etique. Nouv. M´em. Acad., 1773.

[47] LaMacchia. B., A. 1991. *Basis Reduction Algorithms and Subset Sum Problems*. Technical Report. Massachusetts Institute of Technology, Cambridge, MA, USA.

[48] Lenstra, A.K., Lenstra, Jr. H.W., Lovasz, L. Factoring polynomials with rational coefficients. Mathematische Ann., 261:513–534, 1982.

[49] Luk, F.T., Qiao, S., Zhand, W. A Lattice Basis Reduction Algorithm, Institute for Computational Mathematics Technical Report 10-04. Hong Kong Baptist University, Kowloon, Hong Kong, China

[50] Lyubashevsky, V., Micciancio, D. 2006. Generalized compact knapsacks are collision resistant. In *Proceedings of the 33rd international conference on Automata, Languages and Programming - Volume Part II* (ICALP'06), Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener (Eds.), Vol. Part II. Springer-Verlag, Berlin, Heidelberg, 144-155.

[51] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A. 2008. SWIFFT: A Modest Proposal for FFT Hashing. In *Fast Software Encryption*, Kaisa Nyberg (Ed.). Lecture Notes In Computer Science, Vol. 5086. Springer-Verlag, Berlin, Heidelberg 54-72.

[52] Lyubashevsky, V., Peikert, C., Regev, O. 2010. On Ideal Lattices and Learning with Errors over Rings. In Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), Henri Gilbert (Ed.). Springer-Verlag, Berlin, Heidelberg, 1-23.

[53] May, A. Silverman, J.H. 2001. Dimension Reduction Methods for

Convolution Modular Lattices. In *Revised Papers from the International Conference on Cryptography and Lattices* (CaLC '01), Joseph H. Silverman (Ed.). Springer-Verlag, London, UK, 110-125.

[54] Micciancio, D. Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions, Computational Complexity, Volume 16, Number 4, Springer, 2007, pp. 365−411.

[55] Micciancio, D. The geometry of lattice cryptography, in: FOSAD, 2011, pp. 185–210.

[56] Micciancio, D., Goldwasser, S. 2002. *Complexity of Lattice Problems*. Kluwer Academic Publishers, Norwell, MA, USA.

[57] Micciancio, D., Voulgaris, P. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In Proc. STOC ’10, pages 351–358. ACM, 2010.

[58] Micciancio, D., Voulgaris, P. Faster exponential time algorithms for the shortest vector problem. In Proc. ACM-SIAM Symp. on Discrete Algorithms (SODA), pages 1468–1480, 2010.

[59] Mihaita, A., Simion, E. New Trends in Lattice-based Cryptography, Acta Universitatis Apulensis, ISSN: 1582-5329, No. 29/2012, pp. 53-64

[60] Nguyen, P.Q. 2011. Lattice reduction algorithms: theory and practice. In Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology (EUROCRYPT'11), Kenneth G. Paterson (Ed.). Springer Verlag, Berlin, Heidelberg, 2-6.

[61] Nguyen, P.Q. Vidick, T. Sieve algorithms for the shortest vector problem are practical. J. of Mathematical Cryptology, 2(2):181–207, 2008.

[62] Nguyen, P.Q., A note on the security of NTRUSign., IACR Cryptology ePrint Archive 2006 (2006) 387.

[63] Nguyen, P.Q., Regev, O. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures, in: Advances in Cryptology – Proceedings of EUROCRYPT ’06, Vol. 4004 of LNCS, Springer, 2006, pp. 215–233.

[64] Nguyen, P.Q., Stern, J. 2000. Lattice Reduction in Cryptology: An Update. In*Proceedings of the 4th International Symposium on Algorithmic Number Theory* (ANTS-IV), Wieb Bosma (Ed.). Springer-Verlag, London, UK, UK, 85-112.

[65] Nguyen, P.Q., Stern, J., Cryptanalysis of the ajtai–dwork cryptosystem, in: Advances in Cryptology Crypto 98, LNCS 1462, Springer–Verlag, 1998, pp. 223–242.

[66] Nguyen, P.Q., Vallee, B. The LLL Algorithm: Survey and Applications. Information Security and Cryptography. Springer, 2010.

[67] Odlyzko, A.M. The rise and fall of knapsack cryptosystems. In Cryptology and Computational Number Theory, volume 42 of Proc. Of Symposia in Applied Mathematics, pages 75–88. A.M.S., 1990.

[68] Pan, Y., Deng, Y., A ciphertext–only attack against the cai–cusick lattice

based public–key cryptosystem, IEEE Trans. Inf. Theor. 57 (3) (2011) pp.1780–1785.

[69] Peikert, C., Rosen, A. 2006. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Proceedings of the Third conference on Theory of Cryptography* (TCC'06), Shai Halevi and Tal Rabin (Eds.). Springer-Verlag, Berlin, Heidelberg, 145-166.

[70] Pohst, M. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. SIGSAM Bull., 15(1):37–44, 1981.

[71] Pohst, M., A modification of the LLL reduction algorithm, J. Symb. Comput. 4 (1) (1987) 123–127.

[72] Pujol, X. and Stehlé, D., Solving the Shortest Lattice Vector Problem in Time $2^{2.465n}$, IACR Cryptology ePrint Archive 01/2009; 2009:605.

[73] Regev, O. 2005. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (STOC '05). ACM, NY, USA, 84-93.

[74] Rogaway, P., Shrimpton, T., Cryptographic Hash–Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second–Preimage Resistance, and Collision Resistance, in: Fast Software Encryption 2004 (FSE 04), 2004.

[75] Saarinen, M.-J. O., Bentahar, K., Page, D., Silverman, J. H. Smart, N.LASH. NIST: 2nd Cryptographic Hash Workshop. Online, 2006.

[76] Schnorr, C.P, Euchner, M. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Programming, 66:181–199, 1994.

[77] Schnorr, C.P., Horner, H.H. Attacking the Chor-Rivest cryptosystem by improved lattice reduction. In Proc. of Eurocrypt ’95, volume 921 of LNCS, pages 1–12. IACR, Springer-Verlag, 1995

[78] Shamir, A. Identity–based cryptosystems and signature schemes, in: Proceedings of CRYPTO 84 on Advances in cryptology, Springer–Verlag New York, Inc., New York, NY, USA, 1985, pp. 47–53.

[79] Stehlé, D., Steinfeld, R. 2011. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices

[80] Troutman, J., Rijmen, V. Green cryptography: Cleaner engineering through recycling, IEEE Security and Privacy 7 (4) (2009) 71–73.

[81] Wang, X., Lai, X., Feng, D., Chen, H., Yu, X., Cryptanalysis of the hash functions MD4 and ripeMD, in: Advances in Cryptology – EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, Proceedings, Vol. 3494 of Lecture Notes in Computer Science, Springer, 2005, pp. 1–18.

[82] Wang, X., Liu, M., Tian, C., Bi, J. Improved Nguyen-Vidick heuristic sieve algorithm for SVP. Cryptology ePrint Archive, 2010.

[83] Wang, X., Yu, H., How to break md5 and other hash functions, in: In EUROCRYPT, Springer–Verlag, 2005.

[84] Wong, C.K., Gouda, M., Lam, S.S. Secure group communications using key graphs, in: IEEE/ACM Transactions on Networking, 1998, pp. 68–79.

[85] Xu, J., Hu, L., Sun, S., Wang, P. Cryptanalysis of a lattice–knapsack mixed public key cryptosystem, in: CANS, 2012, pp. 32–42.

A.3 Ανέκδοτες Πηγές (Εργασίες / Διατριβές)

[86] Νταής, Ι.Δ., Εισαγωγή στη Θεωρία Δακτυλίων, Σημειώσεις μαθήματος, Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης, (2013).

[87] Healy, A., D., Lattice Basis Reduction and Public–Key Cryptography, BSc thesis, Harvard College, Cambridge, Massachusetts (2002).

[88] Pipher, J., Lectures on the NTRU encryption algorithm and digital signature scheme: Grenoble, 2002, Brown University, Providence, USA

[89] Saarinen, M.,-J.,O. Cryptanalysis of dedicated cryptographic hash functions, Ph.D. thesis, Information Security Group, Royal Holloway, University of London (2009).

A.4 Ιστοσελίδες

[90] http://www.ecrypt.eu.org/ [Last Accessed: 31/10/2013]

[91] http://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding [Last Accessed: 31/10/2013]

[92] http://www.cims.nyu.edu/~regev/teaching/Lattices_faLL_2004/Ln/introduction.pdf [Last Accessed: 31/10/2013]

[93] http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2–1.pdf [Last Accessed: 31/10/2013]

[94] https://web.math.princeton.edu/~svanzwam/pdf/vanzwam2005.pdf [Last Accessed: 31/10/2013]

[95] https://www.cosic.esat.kuleuven.be/ecrypt/cryptofor2020/slides/ECRYPT–PQC.pdf [Last Accessed: 31/10/2013]

[96] http://cryptanalysis.eu/blog/ [Last Accessed: 31/10/2013]

[97] http://gro.noekeon.org/ [Last Accessed: 31/10/2013]

[98] http://en.wikipedia.org/ [Last Accessed: 31/10/2013]