Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

Πληροφορική

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Ο Αλγόριθμος Κρυπτογράφησης NTRU The NTRU Public Key Cryptosystem
Ονοματεπώνυμο Φοιτητή	Ειρήνη Χρόνη
Πατρώνυμο	Γεώργιος
Αριθμός Μητρώου	ΜΠΠΛ/ 13085
Επιβλέπων	Κωνσταντίνος Πατσάκης, Επίκουρος Καθηγητής

Ημερομηνία Παράδοσης **Οκτώβριος 2017**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής	Ευθύμιος Αλέπης Επίκουρος Καθηγητής	Γεώργιος Τσιχριντζής Καθηγητής

Ο Αλγόριθμος Κρυπτογράφησης NTRU

Περίληψη - Abstract

Περίληψη. Η συνεχής ανάπτυξη της επιστήμης των υπολογιστών έχει ως αποτέλεσμα την όλο και μεγαλύτερη ανάγκη για ασφάλεια των πληροφοριών και την προστασία της ιδιωτικότητας. Στην παρούσα μεταπτυχιακή διατριβή, ασχολούμαστε με ένα κρυπτοσύστημα δημοσίου κλειδιού, τον NTRU. Θα ασχοληθούμε με τα πλέγματα σημείων (lattices), καθώς και τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος μέσω του NTRU. Η κρυπτογραφία δημοσίου κλειδιού χαίρει παγκόσμιου ερευνητικού ενδιαφέροντος και μελέτης και αποτελεί μία ιδιαίτερα σύγχρονη και ανταγωνιστική τεχνική σε παλαιότερα είδη κρυπτογραφίας (όπως ο RSA που χρησιμοποιείται σήμερα). Έχει ως βάση κάποια δυσεπίλεπτα μαθηματικά προβλήματα που ανακύπτουν από τη χρήση των lattices, όπως το SVP (Shortest Vector Problem) και το CVP (Closest Vector Problem). Επίσης, θα παρουσιάσουμε τον πιο γνωστό αλγόριθμο αναγωγής της βάσης ενός πλέγματος σημείων, τον LLL αλγόριθμο. Τέλος, θα αναφερθούμε στην Ομομορφική Κρυπτογραφία και στις εφαρμογές που έχει το συγκεκριμένο κρυπτοσύστημα στην μετα-κβαντική κρυπτογραφία.

Λέξεις Κλειδιά: NTRU, Κρυπτογραφία Δημοσίου Κλειδιού, LLL, πλέγματα σημείων, μετα-κβαντική κρυπτογραφία

Abstract. The continuous development of computer science results to the growing need for security of the information and the protection of privacy. This thesis deals with the NTRU public key cryptosystem. We deal with integer lattices and also with the processes of message encryption and decryption through the NTRU Cryptosystem. Public Key Cryptography enjoys global research interest and study, as it is a very modern and competitive technique to older types of cryptography (such as RSA algorithm which is used today). It is also based on some hard to solve math problems arising from the use of lattices, such as the SVP (Shortest Vector Problem) and the CVP (Closest Vector Problem). We are furthermore going to present the most common lattice basis reduction algorithm, the LLL Algorithm. Finally, we will refer to Homomorphic Cryptography and the applications of the specific cryptosystem in the post-quantum cryptography.

Keywords: NTRU, Public Key Cryptosystem, LLL, latices, post-quantum cryptography

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Κωνσταντίνο Πατσάκη για την μύηση στην Κρυπτογραφία, την καθοδήγηση και την εμπιστοσύνη που μου έδειξε.

Πρέπει να αναφέρω το σεβασμό μου στον Alan Turing και φυσικά στην Alice και τον Bob.

Τέλος, να ευχαριστήσω ιδιαιτέρως τον Δημήτρη, για τη στήριξή του σε όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Περίληψη - Abstract 5

Ευχαριστίες 7

Εισαγωγή 11

Μέρος 1. Άλγεβρα-Τοπολογία 13

Κεφάλαιο 1. Άλγεβρα-Τοπολογία 15
Άλγεβρα 15
1.1 Θεωρία Αριθμών 15
1.2 Ομάδες 16
1.3 Δακτύλιοι 17
1.4 Κλάσεις υπολοίπων mod n 17
1.5 Ιδεώδη 18
1.6 Πολυώνυμα 19
1.7 Γραμμική Άλγεβρα 20
Τοπολογία 21
2.1 Μετρικοί χώροι 21

Μέρος 2. Το Κρυπτοσύστημα Δημοσίου Κλειδιού NTRU 23

Κεφάλαιο 2. Ο Αλγόριθμος Κρυπτογράφησης NTRU 25
Κρυπτογραφία 25
1.1 Τι είναι κώδικας? 25
1.2 Ιστορικά στοιχεία 25
1.3 Κρυπτογραφία 28
1.4 Κβαντική κρυπτογραφία 29
Ο αλγόριθμος κρυπτογράφησης NTRU 31
2.1 Lattices (Πλέγματα Σημείων) 31
2.2 SVP και CVP προβλήματα 32
2.2.1 NP–πλήρη και NP–δύσκολα προβλήματα 33
2.3 Ο LLL αλγόριθμος 34
2.3.1 Περιγραφή του LLL αλγορίθμου 34
2.3.2 Υλοποίηση του LLL αλγορίθμου σε Python 35
2.4 Ο αλγόριθμος NTRU 36
2.5 Παράδειγμα στον NTRU 37
2.5.1 Υπενθυμίσεις - Παραδείγματα στα modula και στους δακτυλίους 37
2.5.2 NTRU Public Key Cryptosystem Parameters 38
2.5.3 Κρυπτογράφηση 40
2.5.4 Αποκρυπτογράφηση 40
2.6 Βασικά θέματα ασφάλειας 41
2.7 Επιθέσεις στον NTRU 41
2.7.1 Επιθέσεις εξαντλητικής αναζήτησης 41
2.7.2 Επιθέσεις Meet-in-the-middle 42
2.7.3 Επιθέσεις πολλαπλής αποστολής 42
2.7.4 Επιθέσεις με πλέγματα σημείων 42
2.8 Πρακτικές εφαρμογές του $NTRU$ 44

2.8.1 Συγκεκριμένες επιλογές παραμέτρων 44
2.9 Σύγκριση με άλλα Κρυπτοσυστήματα Δημοσίου Κλειδιού 45
3 Ομομορφική Κρυπτογραφία 46
3.1 Το Πρόβλημα 46
3.2 Ορισμός και Ιδιότητες 46

Μέρος 3. Επίλογος 49

Κεφάλαιο 3. Επίλογος 51
Εφαρμογές της Ομομορφικής Κρυπτογραφίας 51
Κβαντική Κρυπτογραφία 51

Παράρτημα Α’ 53

Βιβλιογραφία 55

Εισαγωγή

> "I thought cryptography was a technique that did not require your trusting other people – that id you encrypted your files, you would have the control to make the choice as to whether you would surrender your files"
>
> *Whitfield Diffie*

> "Cryptography is the essential building block of independence for organisations on the Internet, just like armies are the essential building blocks of states, because otherwise one state just takes over another"
>
> *Julian Assange*

> "There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government"
>
> *Bruce Schneier*

> "Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve"
>
> *Edgar Allan Poe*

> "Who are you?" asked the Caterpillar.
> "I hardly know, Sir. I know who I was, but I think I must have changed"
>
> *"Alice In Wonderland", Lewis Carroll*

Η κρυπτογραφία και οι κάθε είδους εφαρμογές της παίζουν καθοριστικό ρόλο στη σύγχρονη ζωή. Όταν μιλάμε για ασφαλή επικοινωνία, ασφαλή πρόσβαση σε συστήματα και υπηρεσίες, ανάκτηση και διαχείρηση ευαίσθητων δεδομένων, ηλεκτρονικές συναλλαγές, ηλεκτρονικές ψηφοφορίες, στρατιωτικές εφαρμογές κτλ, όλα αυτά επιρρεάζονται από τις εξελίξεις στην κρυπτογραφία και την κρυπτανάλυση.

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

Η κρυπτογραφία σύμφωνα με τον Rivest, ασχολείται με την επικοινωνία παρουσία αντιπάλων, οι οποίοι, εκτός από τα φυσικά πρόσωπα που μπορεί να επιδιώκουν να παρακολουθήσουν την επικοινωνία, θεωρείται και η πιθανή αλλοίωση του περιεχομένου του μηνύματος ή η μη αντίληψη της ενδεχόμενης αλλοίωσης από τον δέκτη ή ακόμα και η παραλαβή του μηνύματος από κάποιον που υποδύεται τον πραγματικό δέκτη, αλλά δεν είναι αυτός.

Πλέον, με τους κβαντικούς υπολογιστές, η αναγκαιότητα για ύπαρξη ενός είδους κρυπτογραφίας που να μπορεί να αντισταθεί σε επιθέσεις, είναι προφανής. Παραδείγματα κρυπτογραφικών συστημάτων, που από όσα γνωρίζουμε σήμερα, είναι ασφαλή έναντι κβαντικών απειλών είναι το κρυπτοσύστημα McEliece και διάφορα κρυπτοσυστήματα βασισμένα σε πλέγματα σημείων, όπως το NTRU (που θα ασχοληθούμε σε αυτήν την εργασία) και το κρυπτοσύστημα των Goldwasser, Goldreich και Halevi (GGH). Αντίθετα, τα περισσότερα από τα συμμετρικά κρυπτογραφικά συστήματα που χρησιμοποιούνται αυτή τη στιγμή (συμμετρικοί αλγόριθμοι κρυπτογράφησης και συναρτήσεις διασποράς) δεν είναι ασφαλή από τους κβαντικούς υπολογιστές.

Στην κλασική κρυπτογραφία, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι γνωστοί σε όλους και το ίδιο κλειδί χρησιμοποιείται και για τα δύο. Δηλαδή, η αποκρυπτογράφηση είναι εύκολο αν το κλειδί κρυπτογράφησης είναι γνωστό. Αυτά τα συστήματα αναφέρονται ως συμμετρικά ή διπλής κατεύθυνσης. Αντίθετα, στην κρυπτογραφία δημοσίου κλειδιού, ο αποστολέας

και ο παραλήπτης δε μοιράζονται ένα κοινό μυστικό κλειδί, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες. Δηλαδή, το κλειδί κρυπτογράφησης μπορεί με ασφάλεια να δημοσιοποιηθεί χωρίς να αποκαλυφθεί το κλειδί αποκρυπτογράφησης. Αυτά τα σηστήματα αναφέρονται και ως μη-συμμετρικά ή ασύμμετρα ή μονής κατεύθυνσης.

Σε αυτήν την εργασία θα ασχοληθούμε με το κρυπτοσύστημα NTRU, έναν αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού ο οποίος στηρίζεται σε πλέγματα σημείων (lattices) και είναι η αρχή για την ομομορφική κρυπτογραφία. Η ομομορφική κρυπτογραφία 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.

Μέρος 1

Άλγεβρα-Τοπολογία

ΚΕΦΑΛΑΙΟ 1

Άλγεβρα-Τοπολογία

1. Άλγεβρα

1.1. Θεωρία Αριθμών

Η θεωρία αριθμών είναι ο πιο σημαντικός και πιο απαραίτητος τομέας των μαθηματικών που χρησιμοποιείται στην κρυπτογραφία μέχρι στιγμής. Επίσης, υπάρχουν μαθηματικές δομές που έχουν αναπτυχθεί όλα αυτά τα χρόνια χρησιμοποιώντας ως βάση τους φυσικούς αριθμούς και τις ιδιότητές τους.

Κάποιες από τις βασικές ιδιότητες των ακεραίων είναι:

Ορισμός 1. *Έστω $d, n \in \mathbb{Z}$. Λέμε ότι ο d διαιρεί τον n και γράφουμε $d|n$ αν υπάρχει ακέραιος c τέτοιος ώστε $n = c \cdot d$.*

Αν δεν υπάρχει τέτοιος αριθμός τότε λέμε ότι ο d δεν διαιρεί τον n και γράφουμε $d \nmid n$

Από το παραπάνω έχουμε τις εξής ιδιότητες:

(1) $\forall n \in \mathbb{Z}\ n \mid n,\ 1 \mid n$ και $n \mid 0$.
(2) $\forall n, m, d \in \mathbb{Z}$ αν $d \mid n$ και $n \mid m$ τότε $d \mid m$.
(3) $\forall n, m, d, a, b \in \mathbb{Z}$ αν $d \mid n$ και $d \mid m$ τότε $d \mid (a \cdot m + b \cdot n)$.
(4) $\forall n, d \in \mathbb{Z}$ me $n \neq 0$ αν $d \mid n$ τότε $|d| \leq |n|$.
(5) $\forall n, d \in \mathbb{Z}$ αν $d \mid n$ και $n \mid d$ τότε $d = n$.

Θεώρημα 1. *Έστω $a, b \in \mathbb{Z},\ b \neq 0$ τότε υπάρχουν δύο μοναδικοί ακέραιοι q, r τέτοιοι ώστε*

$$a = b \cdot q + r,\ \text{με } 0 \leq r < b$$

Θεώρημα 2. *Έστω $a, b \in \mathbb{Z}$, ονομάζουμε το φυσικό αριθμό d μέγιστο κοινό διαιρέτη των a, b και γράφουμε $d = MK\Delta(a, b)$ (ή $d = gcd(a, b)$[1]) αν:*

(1) $d \mid a$ *και* $d \mid b$
(2) $\forall d' \in \mathbb{N}$ *ώστε* $d' \mid a$ *και* $d' \mid b$ *ισχύει ότι* $d' \mid d$.

Ορισμός 2. *Έστω $p \in \mathbb{N},\ 1 < p$, καλούμε τον p πρώτο αριθμό αν έχει ακριβώς δύο φυσικούς διαιρέτες: το 1 και τον εαυτό του.*

Δύο αριθμοί $a, b \in \mathbb{N}$ καλούνται πρώτοι μεταξύ τους αν ο μέγιστος κοινός τους διαιρέτης είναι 1, δηλαδή $gcd(a, b) = 1$

Θεώρημα 3. *(Θεμελιώδες Θεώρημα της Θεωρίας Αριθμών)*
Κάθε φυσικός αριθμός $a \in \mathbb{N},\ a > 1$ μπορεί να αναλυθεί κατά μοναδικό τρόπο σε γινόμενο πρώτων παραγόντων, δηλ

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

όπου $n_i \in \mathbb{N},\ i = 1, 2, \ldots, k$ και p_i πρώτοι

Η εύρεση πρώτων αριθμών είναι μία δύσκολη εργασία και έως σήμερα δεν υπάρχει γνωστός γρήγορος αλγόριθμος που να το πραγματοποιεί. Παρ' όλ' αυτά, οι πρώτοι αριθμοί χρειάζονται σε πολλά κρυπτογραφικά πρωτόκολλα, συνεπώς υπάρχουν κάποιοι αλγόριθμοι που προσπαθούν να παράγουν τυχαίους πρώτους αριθμούς. Για τους περισσότερους, η αποτελεσματικότητα είναι πιο σημαντική από τη βεβαιότητα και κατ' επέκτατη οι πρακτικότεροι αλγόριθμοι από αυτούς είναι πιθανοτικοί.

[1] gcd=greater common divisor

Θεώρημα 4. *Αν P είναι ένα οποιοδήποτε πεπερασμένο σύνολο θετικών πρώτων αριθμών, τότε υπάρχει πρώτος, ο οποίος δεν ανήκει στο P. Άρα το σύνολο των πρώτων αριθμών είναι άπειρο. (βιβλίο Θ' των Στοιχείων του Ευκλείδη)*

Μία διαφορετική έκφραση του παραπάνω είναι: «Υπάρχουν άπειροι σε αριθμό πρώτοι»

Ορισμός 3. *(Συνάρτηση φ του Euler)*
Για κάθε $n \geq 1$, θεωρούμε τη συνάρτηση $\varphi(n)$ που συμβολίζει το πλήθος των ακεραίων στο διάστημα $[1, n]$ οι οποίοι είναι πρώτοι με τη n.

Ιδιότητες της συνάρτησης φ του Euler

- *Αν p πρώτος, τότε $\varphi(p) = p \cdot 1$*
- *Εάν $n, m \in \mathbb{N}$ είναι πρώτοι μεταξύ τους, τότε $\varphi(nm) = \varphi(n)\varphi(m)$*
- *Εάν $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, τότε $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$*

Δύο θεμελιώδη θεωρήματα της Θεωρίας Αριθμών που συνιστούν μέρος πολλών κρυπτοσυστημάτων, με την έννοια να παρέχουν μικρό (σχετικά) χρόνο υπολογισιμότητας για μεγάλους εκθέτες σε συγκεκριμένες αλγεβρικές μορφές είναι τα παρακάτω:

Θεώρημα 5. *(Μικρό Θεώρημα του Fermat)*
Κάθε φυσικός αριθμός $p \in \mathbb{N}$, εάν ο p είναι πρώτος αριθμός, τότε για κάθε ακέραιο a, το $a^p - a$ διαιρείται με το p

Θεώρημα 6. *(Θεώρημα του Euler)*
Για κάθε φυσικό αριθμό $n \in \mathbb{N}$, τότε για κάθε ακέραιο a, ο $a^{\varphi(n)} - 1$ διαιρείται με το n.

1.2. Ομάδες

Ένα από τα πιο θεμελιώδη μαθηματικά εργαλεία στην κρυπτογραφία είναι η έννοια της ομάδας.

Ορισμός 4. *Ένα ζεύγος $(G, *)$, όπου G είναι ένα μη κενό σύνολο και $*$ είναι μία πράξη στο G, δηλαδή*

$$* : G \times G \to G, (x, y) \to x * y$$

καλείται ομάδα εάν οι ακόλουθες προϋποθέσεις ικανοποιούνται:

- *κλειστότητα: $\forall x, y \in G$, τότε και $x * y \in G$*
- *προσεταιριστική: $(x * y) * z = x * (y * z)$, $\forall x, y, z \in G$*
- *ύπαρξη μοναδικού μοναδιαίου στοιχείου: $e \in G : \ e * x = x * e = x$, $\forall x \in G$*
- *ύπαρξη μοναδικού αντίστροφου στοιχείου: $x^{-1} \in G : \ x * x^{-1} = x^{-1} * x = e$, $\forall x \in G$*

Γενικά σε μία ομάδα $(G, *)$ δε σημαίνει απαραίτητα ότι
$\forall x, y \in G : x * y = y * x$.
Για παράδειγμα, αν πάρουμε ως ομάδα G το σύνολο των αντιστρέψιμων πινάκων στο $\mathbb{R}^{n \times n}$ και ως πράξη $*$ τον πολλαπλασιασμό πινάκων, τότε το G είναι ομάδα, αλλά γενικά ισχύει ότι $A \cdot B \neq B \cdot A$.

Αν επιπλέον η πράξη είναι αντιμεταθετική, δηλαδή $x * y = y * x$ για $x, y \in G$ τότε η ομάδα καλείται αντιμεταθετική ή αβελιανή.

Ορισμός 5. *Αν $(G, *)$ είναι μία ομάδα και $H \subseteq G$, τότε αν $(H, *)$ δημιουργεί ομάδα, λέμε ότι η $(H, *)$ είναι υποομάδα της $(G, *)$ και γράφουμε $(H, *) \leq (G, *)$.*

Ορισμός 6. *Για μία ομάδα $(G, *)$ καλούμε τάξη της ομάδας, και συμβολίζουμε $|G|$ το πλήθος των στοιχείων της ομάδας $(G, *)$.*

Ένα από τα πιο βασικά θεωρήματα της θεωρίας ομάδων είναι το θεώρημα του Lagrange:

Θεώρημα 7. *Για κάθε πεπερασμένη ομάδα G και κάθε υποομάδα H της G, ισχύει ότι $|H| \mid |G|$*

Πολύ μεγάλη σημασία παίζουν οι ομάδες που παράγονται από ένα μόνο στοιχείο της ομάδας.

Ορισμός 7. *Αν υπάρχει στοιχείο $g \in G$ τέτοιο ώστε $G =< g >= \{g, g^1, g^2, g^3, \ldots\}$, τότε η G καλείται κυκλική ομάδα και το στοιχείο g αποτελεί και γεννήτορα της ομάδας G.*
Αλλιώς, $\exists g \in G$ τέτοιο ώστε $\forall a \in G \ \exists i \in \mathbb{N} : a = g^i$

Παράδειγμα 1. *Θεωρούμε το σύνολο των ακεραίων $\mathbb{Z}$ και την πράξη $+$, τότε το $(\mathbb{Z}, +)$ είναι μία αβελιανή ομάδα άπειρης τάξης.*

1.3. Δακτύλιοι

Ορισμός 8. *Έστω R ένα σύνολο και $\diamond, \circ$ δύο τελεστές, οι οποίοι απεικονίζουν ζευγάρια στοιχείων του R σε ένα μόνο στοιχείο του R, τότε λέμε ότι η τριάδα $\{R, \diamond, \circ\}$ είναι ένας δακτύλιος αν ισχύουν οι ακόλουθες ιδιότητες:*

- *κλειστότητα: $\forall a, b \in R$, το αποτέλεσμα των πράξεων $a \diamond b$ και $a \circ b$ ανήκουν επίσης στο R.*
- *προσεταιριστική: $\forall a, b, c \in R$ ισχύει ότι $(a \diamond b) \diamond c = a \diamond (b \diamond c)$ και $(a \circ b) \circ c = a \circ (b \circ c)$*
- *ύπαρξη μοναδικού ταυτοτικού στοιχείου του $\diamond$ $\exists 0_R \in R : \forall a \in R : 0_R \diamond a = a \diamond 0_R = a$ (Η ίδια ιδιότητα δεν ισχύει γενικά για τον τελεστή $\circ$, αλλά συμβολίζουμε το ταυτοτικό στοιχείο του $\circ$ ως 1_R)*
- *ύπαρξη μοναδικού αντίστροφου στοιχείου: $\diamond \forall a \in R, \exists b \in R$ τέτοιο ώστε $a \diamond b = b \diamond a = 0_R$*
- *μεταθετική του $\diamond$ $\forall a, b \in R$ ισχύει ότι $a \diamond b = b \diamond a$*
- *επιμεριστική: $\forall a, b, c \in R$ ισχύει ότι $(a \diamond b) \circ c = a \circ c \diamond b \circ c$*
  $\forall a, b, c \in R$ ισχύει ότι $(a \circ b) \diamond c = a \diamond c \circ b \diamond c$

Αν για τον δακτύλιο $\{R, \diamond, \circ\}$ ισχύει ότι $\forall a, b \in R$, $a \circ b = b \circ a$ τότε καλούμε τον δακτύλιο μεταθετικό.

Γνωστά παραδείγματα δακτυλίων είναι:

Παράδειγμα 2. *Ο δακτύλιος των ακεραίων $(\mathbb{Z}, +, \cdot)$ με τις γνωστές πράξεις, πρόσθεση και πολλαπλασιασμό των ακεραίων.*

Παράδειγμα 3. *Ο δακτύλιος $\mathbb{R}[x]$ των πολυωνύμων με συντελεστές πραγματικούς αριθμούς και πράξεις την πρόσθεση και τον πολλαπλασιασμό των πολυωνύμων.*

Παράδειγμα 4. *Ο δακτύλιος $M_n(\mathbb{R})$ των τετραγωνικών $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξεις την πρόσθεση και τον πολλαπλασιασμό πινάκων.*

Ένα άλλο παράδειγμα δακτυλίου είναι ο δακτύλιος $(\mathbb{Z}_n, +, \cdot)$ των ακεραίων $modulo\, m$ για έναν θετικό ακέραιο m, που θα δούμε παρακάτω.

Ορισμός 9. *Ένα μη κενό υποσύνολο S ενός δακτυλίου R θα λέγεται υποδακτύλιος αν είναι δακτύλιος ως προς την πρόσθεση και τον πολλαπλασιασμό του δακτυλίου R. Δηλαδή το S είναι υποομάδα ως προς την πρόσθεση και $a \cdot b \in S$ για κάθε $a, b \in S$*

Παρατήρηση 1. *Το μηδέν (το ουδέτερο στοιχείο της πρόσθεσης) ενός δακτυλίου ανήκει σε κάθε υποδακτύλιο. Για τη μονάδα (το ουδέτερο στοιχείο του πολλαπλασιασμού) δεν ισχύει κάτι ανάλογο.*

Ορισμός 10. *Ένας μεταθετικός δακτύλιος $\mathbb{F}$ με μονάδα όπου κάθε μη μηδενικό στοιχείο του έχει αντίστροφο λέγεται σώμα.*

1.4. Κλάσεις υπολοίπων mod n

Ορισμός 11. *(Ορισμός δακτυλίου $(\mathbb{Z}_m, +, \cdot)$)*
Έστω m ένας θετικός ακέραιος. Στο σύνολο των ακεραίων αριθμών ορίζουμε μία σχέση $\sim$ ως εξής:
$a \sim b$ *αν και μόνο αν ο m διαιρεί τη διαφορά $a - b$.*

Η σχέση $\sim$ είναι μία σχέση ισοδυναμίας, η οποία διαμερίζει το σύνολο των ακεραίων σε κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας ενός ακεραίου αριθμού a είναι το σύνολο

$$[a] = \{r \in \mathbb{Z} : r \sim a\} = \{r \in \mathbb{Z} : m \mid (a - r)\} = \{a + m \cdot s : s \in \mathbb{Z}\}$$

Ορισμός 12. *Έστω $n \in \mathbb{N}$. Ένας ακέραιος αριθμός $a \in \mathbb{Z}$ ονομάζεται ισότιμος με τον ακέραιο b* mod n *και γράφουμε $a \equiv b$* mod n *εάν $n \mid (a - b)$ ή ισοδύναμα $a = b + k \cdot n$ για κάποιο ακέραιο $k \in \mathbb{Z}$*

Παράδειγμα 5. 147 mod $17 =?$
Επειδή $147 = 8 \cdot 17 + 11$ έχουμε $147 = 11 mod 17$

Παρατήρηση 2.
- *Γενικά, η ισοδυναμία* $a \equiv b \mod m$ *σημαίνει ότι τα* a *και* b *αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το* m
- *Υπάρχουν τόσες κλάσεις ισοδυναμίας όσα και τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με τον* m.

Κλάση υπολοίπων του $a \mod n$: είναι το σύνολο

$$[a] = \{x \in \mathbb{Z} : x \equiv a \mod n\}$$

Σύνολο των κλάσεων υπολοίπων $\mod n$: είναι το σύνολο

$$\mathbb{Z}_n = \{[1], [2], \ldots, [n-1]\}$$

Ιδιότητες

- $a \mod m + b \mod m = a + b \mod m$
- $a \mod m \cdot b \mod m = a \cdot b \mod m$
- Αν $a \cdot b = 1 \mod m$ τότε ο b είναι αντίστροφος του $a \mod m$

Παράδειγμα 6. *Ο αντίστροφος του* $10 \mod 23$ *είναι το 7 διότι* $7 \cdot 10 = 1 \mod 23$

Παρατήρηση 3. (1) *Ο τρόπος που ορίζουμε τις πράξεις στο σύνολο των* $\mathbb{Z}_m$ *"υπαγορεύει" έναν εύκολο τρόπο να εκτελούμε τις πράξεις.*

Έστω ότι έχουμε να προσθέσουμε/πολλαπλασιάσουμε το $[a]$ *με το* $[b]$*, τότε προσθέτουμε/πολλαπλασιάζουμε το* a *με το* b *στους ακεραίους, το αποτέλεσμα που βρίσκουμε το διαιρούμε με τον* m *και το υπόλοιπο* $\mod m$ *που προκύπτει είναι το αποτέλεσμα της πρόσθεσης/πολλαπλασιασμού του* $[a]$ *με το* $[b]$.

Παράδειγμα 7. *Έστω* $[3], [5] \in \mathbb{Z}_6$.
Τότε $[3] + [5] = [8 = 6 + 2] = [2]$
και $[3] \cdot [5] = [15 = 2 \cdot 6 + 3] = [3]$

(2) *Πολλές φορές, όταν δεν υπάρχει ενδεχόμενο σύγχυσης, κάθε κλάση υπολοίπων* $\mod m$ $[a]$ *την ταυτίζουμε με τον αντίστοιχο αντιπρόσωπο* a *και γράφουμε* $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Θεώρημα 8. *Έστω* m *θετικός ακέραιος, το στοιχείο* $[a] \in \mathbb{Z}_m$ *είναι αντιστρέψιμο αν και μόνο αν ο* a *είναι πρώτος ως προς τον* m.

Θεώρημα 9. *Κάθε* $a \in \mathbb{Z}_n - \{0\}$ *αντιστρέφεται αν και μόνο αν ο* n *είναι πρώτος αριθμός.*

1.5. Ιδεώδη

Ορισμός 13. *Έστω* $(R, +, \cdot)$ *ένας δακτύλιος και* I *ένα μη κενό υποσύνολο του* R*. Το* I *θα λέγεται ιδεώδες του* R *(και θα συμβολίζεται* $I \triangleleft R$*) αν ισχύουν:*

(1) $a - b \in I$*, για όλα τα* $a, b \in I$
(2) $r \cdot a, a \cdot r \in I$ *για όλα τα* $a \in I$ *και* $r \in R$

Προφανώς το σύνολο $\{0\}$ που αποτελείται μόνο από το μηδέν είναι ιδεώδες και ονομάζεται μηδενικό ή τετριμμένο ιδεώδες. Επίσης, ολόκληρος ο δακτύλιος R είναι ιδεώδες του εαυτού του. Ένα ιδεώδες I με $\{0\} \neq I \neq R$ θα λέγεται γνήσιο ιδεώδες.

Παρατήρηση 4.
- *Έστω δύο ιδεώδη ενός δακτυλίου. Η τομή τους είναι επίσης ιδεώδες του ίδιου δακτυλίου.*
- *Η ένωση δύο ιδεωδών δεν είναι κατ' ανάγκη ιδεώδες.*

Ορισμός 14. *Αν* R *είναι ένας δακτύλιος και* $a \in R$*, τότε το ιδεώδες το παραγόμενο από το μονοσύνολο* $\{a\}$ *θα ονομάζεται κύριο και ισχύει*

$$< \{a\} > = < a > = \{r \cdot a : r \in R\}$$

Για κάθε ιδεώδες του δακτυλίου των ακεραίων υπάρχει ένας θετικός ακέραιος m έτσι ώστε $I = m\mathbb{Z} = \{m \cdot r : r \in \mathbb{Z}\}$. Δηλαδή το $I = < m >$ είναι κύριο. Άρα κάθε ιδεώδες του δακτυλίου $\mathbb{Z}$ είναι κύριο.

Έστω R ένας δακτύλιος και I ένα ιδεώδες του. Υποθέτουμε ότι το $1 \in I$, τότε προφανώς έχουμε ότι $I = R$.

Από το παραπάνω έπεται ότι $< a >= R$ αν και μόνο αν το στοιχείο $a \in R$ είναι αντιστρέψιμο.

Επίσης, από την ίδια παρατήρηση έπεται άμεσα ότι σε ένα σώμα τα μόνα ιδεώδη του είναι το μηδενικό ιδεώδες και ολόκληρο το σώμα.

Παράδειγμα 8. *Αν θεωρήσουμε το σύνολο* $\{2\mathbb{Z}\}$ *αποδεικνύεται ότι είναι ένα ιδεώδες του* $\{\mathbb{Z}, +, \cdot\}$, *δηλαδή* $\{2\mathbb{Z}, +, \cdot\} \triangleleft \{\mathbb{Z}, +, \cdot\}$. *Επίσης, το ιδεώδες* $\{2\mathbb{Z}\}$ *είναι κύριο επειδή παράγεται από το στοιχείο* 2, *δηλαδή* $\{2\mathbb{Z}\} =< 2 >$.

Έστω I ένα ιδεώδες του δακτυλίου R.
Στο δακτύλιο R ορίζουμε μία σχέση $\sim$ ως εξής:
$a \sim b$ αν και μόνο αν $a - b \in I$.
Η σχέση $\sim$ είναι σχέση ισοδυναμίας.

Ορισμός 15. *Η κλάση ισοδυναμίας του στοιχείου* a *είναι το σύνολο*
$C_a = \{r \in R : r - a \in I\} =$
$\{e \in R$ *για τα οποία υπάρχει* $h \in I$ *έτσι ώστε* $r = a + h\} =$
$\{a + h : h \in I\}$.
Την κλάση $C_a = \{a + h : h \in I\}$ *θα την ονομάζουμε σύμπλοκο ή κλάση υπολοίπων του* a *ως προς το ιδεώδες* I *και θα συμβολίζεται* $a + I$.
Το σύνολο $\{a + I : a \in R\}$ *όλων των συμπλόκων αποτελεί το σύνολο πηλίκων ως προς τη σχέση ισοδυναμίας* $\sim$ *και θα συμβολίζεται* R/I.

Επομένως, στο σύνολο R/I μπορούμε, με τη βοήθεια των πράξεων της πρόσθεσης και του πολλαπλασιασμού στο δακτύλιο R, να ορίσουμε δύο πράξης, μία πρόσθεση και έναν πολλαπλασιασμό ως εξής:

(1) $(a + I) + (b + I) = (a + b) + I$
(2) $(a + I) \cdot (b + I) = (a \cdot b) + I$

Ορισμός 16. *Το σύνολο* R/I *αποτελεί δακτύλιο και ονομάζεται δακτύλιος πηλίκων ως προς το ιδεώδες* I

Παρατήρηση 5. *Ο δακτύλιος των ακεραίων* $\mathbb{Z}_m$ *των ακεραίων* mod m *είναι ο δακτύλιος πηλίκων* $\mathbb{Z}/ < m >$

1.6. Πολυώνυμα

Ορισμός 17. *Έστω* R *ένας δακτύλιος με μονάδα, τότε υπάρχει δακτύλιος* $\mathcal{R}$ *που περιέχει τον* R *ως υποδακτύλιο και έχει τις παρακάτω ιδιότητες:*

- *Υπάρχει ένα στοιχείο* $x \in \mathcal{R}$ *τέτοιο ώστε* $\forall r \in R \; r \cdot x = x \cdot r$.
- *Κάθε στοιχείο του* $\mathcal{R}$ *μπορεί να αναπαρασταθεί στη μορφή* $r_0 + r_1 x + \ldots + r_n x^n$ *όπου* $n \in \mathbb{N}$ *και* $r_i \in R$, $\forall i \in [0, n]$.
- *Αν* $r_0 + r_1 x + \ldots + r_n x^n = s_0 + s_1 x + \ldots + s_m x^m$, *όπου* $n, m \in \mathbb{N}$, $n \leq m$ *και* $r_i \in R$, $\forall i \in [0, n]$ *και* $s_i \in R$, $\forall i \in [0, m]$, *τότε* $r_i = s_i$, $\forall i \in [0, n]$ *και* $s_i = 0_R$, $\forall i \in [n + 1, m]$.

Συμβολίζουμε αυτόν τον δακτύλιο με $\mathcal{R}[x]$ και καλούμε τα στοιχεία του πολυώνυμα, τα οποία συμβολίζουμε με $f(x), g(x), h(x), \ldots$

Καλούμε μονώνυμο κάθε στοιχείο του δακτυλίου $\mathcal{R}[x]$ που έχει τη μορφή rx^i. Ορίζουμε το βαθμό ενός πολυωνύμου $f(x)$ ως τον μεγαλύτερο εκθέτη των x, και συμβολίζουμε με $degf(x)$. Αν r είναι ο συντελεστής του όρου $x^{deg(f(x))}$, τότε λέμε ότι το r είναι ο μεγιστοβάθμιος συντελεστής. Αν ο μεγιστοβάθμιος συντελεστής σε ένα πολυώνυμο είναι το 1, τότε το πολυώνυμο ονομάζεται μονικό. Το πολυώνυμο, του οποίου όλοι οι συντελεστές είναι μηδενικοί, ονομάζεται το μηδενικό πολυώνυμο και δεν του προσάπτουμε βαθμό.

Τα πολυώνυμα μηδενικού βαθμού ονομάζονται σταθερά και ισχύει ότι ο συντελεστής του x^0 δεν είναι το 0_R, ενώ όλοι οι άλλοι συντελεστές είναι 0_R

Θεώρημα 10. *(Αλγόριθμος της διαίρεσης πολυωνύμων)*
Θεωρούμε τον δακτύλιο $\mathcal{R}[x]$, *και* $f(x), g(x) \in \mathcal{R}[x]$, $g(x) \neq 0_R$, *τότε υπάρχουν μοναδικά πολυώνυμα* $\pi(x), \upsilon(x) \in \mathcal{R}[x]$ *τέτοια ώστε*
$f(x) = \pi(x) \cdot g(x) + \upsilon(x)$ *με* $\upsilon(x) = 0$ *ή* $deg(\upsilon(x)) < deg(g(x))$.

Ορισμός 18. *Ένα πολυώνυμο $f(x) \in \mathcal{R}[x]$ θα λέγεται ανάγωγο επί του δακτυλίου R αν*

$$\forall g(x), h(x) : f(x) = g(x) \cdot h(x) \Longrightarrow (g(x) = 1_R \vee h(x) = 1_R)$$

δηλαδή ένα από τα $g(x), h(x)$ είναι σταθερό.

Πρόταση 1. *Ο δακτύλιος των πολυωνύμων $\mathcal{R}[x]$ είναι περιοχή κυρίων ιδεωδών.*

Ορισμός 19. *(Μέγιστος Κοινός Διαιρέτης)*
Έστω $f(x), g(x) \in \mathcal{R}[x]$ με τουλάχιστον ένα από αυτά διάφορο του 0_R, καλούμε το πολυώνυμο $d(x) \in \mathcal{R}[x]$ μέγιστο κοινό διαιρέτη των $f(x), g(x)$ και συμβολίζουμε με $gcd(f(x), g(x))$ αν:

(1) *$d(x) \mid f(x)$ και $d(x) \mid g(x)$, δηλαδή ο $d(x)$ είναι κοινός διαιρέτης των $f(x)$ και $g(x)$.*
(2) *$d(x)$ είναι μονικό πολυώνυμο.*
(3) *Αν $d'(x) \in \mathcal{R}[x]$ και $d'(x) \mid f(x)$ και $d'(x) \mid g(x)$ τότε $d'(x) \mid d(x)$, δηλαδή κάθε κοινός διαιρέτης των $f(x)$ και $g(x)$ είναι διαιρέτης του $d(x)$.*

Όταν για τα πολυώνυμα $f(x), g(x) \in \mathcal{R}[x]$ ισχύει ότι $gcd(f(x), g(x)) = 1_R$ τότε τα πολυώνυμα θα λέγονται σχετικά πρώτα ή πρώτα μεταξύ τους.

Θεώρημα 11. *Έστω $f(x), g(x) \in \mathcal{R}[x]$ δύο πολυώνυμα που τουλάχιστον ένα είναι διαφορετικό από το 0_R. Τότε υπάρχει πάντα πολυώνυμο $d(x) \in \mathcal{R}[x]$ το οποίο είναι ο μέγιστος κοινός διαιρέτης των $f(x), g(x)$. Επίσης, υπάρχουν $a(x), b(x) \in \mathcal{R}[x] : gcd(f(x), g(x)) = a(x) \cdot f(x) + b(x) \cdot g(x)$*

Παρατήρηση 6. *Μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη περισσοτέρων από δύο πολυωνύμων.*

1.7. Γραμμική Άλγεβρα

Ορισμός 20. *Έστω $\mathbb{F}$ ένα σώμα και V ένα μη κενό σύνολο με δύο δυαδικούς τελεστές $\diamond, \circ$. Τότε ο $\{V, \diamond, \circ\}$ είναι ένας διανυσματικός ή γραμμικός χώρος πάνω στο σώμα $\mathbb{F}$ αν ισχύουν οι ακόλουθες προϋποθέσεις:*

(1) $\diamond : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $\circ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$
(2) $\forall a, b \in V \Rightarrow a \diamond b \in V$, $l \in \mathbb{F} \Rightarrow l \diamond a \in V$
(3) $\forall a, b, c \in V \Rightarrow (a \diamond b) \diamond c = a \diamond (b \diamond c)$
(4) $\exists\, 0_V \in V \Rightarrow \forall a \in V : a \diamond 0 = 0 \diamond a = a$
(5) $\forall a \in V, \exists\, b \in V \Rightarrow a \diamond b = b \diamond a = 0_V$ *και συμβολίζουμε αυτό το b ως $-a$*
(6) $\forall a, b \in V \Rightarrow a \diamond b = b \diamond a$
(7) $\forall a, b \in V$, $l \in \mathbb{F} \Rightarrow l \circ (a \diamond b) = l \circ a \diamond l \circ b$
(8) $\exists\, 1_{\mathbb{F}} \in \mathbb{F} : \forall a \in V \Rightarrow a \circ 1_{\mathbb{F}} = 1_{\mathbb{F}} \circ a = a$
(9) $\forall k, l \in \mathbb{F}, a \in V \Rightarrow (k \diamond l) \circ a = k \circ a \diamond l \circ a$
(10) $\forall k, l \in \mathbb{F}, a \in V \Rightarrow (k \circ l) \circ a = k \circ (l \circ a)$

Ορισμός 21. *Ένα μη κενό υποσύνολο W του διανυσματικού χώρου V που είναι κλειστό ως προς τους τελεστές $\diamond$ και $\circ$ καλείται υπόχωρος του V.*

Οι υπόχωροι του V είναι κι αυτοί διανυσματικοί χώροι.

Ορισμός 22. *Έστω ένα διανυσματικός χώρος V με τις πράξεις $\diamond$ και $\circ$ πάνω στο σώμα $\mathbb{F}$. Θεωρούμε το πεπερασμένο υποσύνολο του V, $S = \{a_1, a_2, \ldots, a_n\}$. Αυτή η οικογένεια διανυσμάτων είναι γραμμικώς εξάρτημένα αν υπάρχουν $l_1, l_2, \ldots, l_n \in \mathbb{F}$ με τουλάχιστον ένα από αυτά διαφορετικό του 0_V ώστε $l_a \circ a_1 \diamond l_2 \circ a_2 \cdots l_n \circ a_n = 0_V$.*
Αν $\forall l_1, l_2, \ldots l_n \in \mathbb{F}$ τέτοια ώστε $l_1 \circ a_1 \diamond l_2 \circ a_2 \cdots l_n \circ a_n = 0_V$ ισχύει ότι $l_1 = l_2 = \ldots = l_n = 0_V$ τότε λέμε ότι τα διανύσματα $a_1, a_2, \ldots, a_n$ είναι γραμμικώς ανεξάρτητα και ο υπόχωρος S είναι ένα γραμμικά ανεξάρτητος υπόχωρος.

Εκφράσεις της μορφής $l_a \circ a_1 \diamond l_2 \circ a_2 \cdots l_n \circ a_n = a$ όπου $a \in V$, λέμε ότι το a είναι γραμμικός συνδυασμός των $\{a_1, a_2, \ldots, a_n\}$

Ορισμός 23. *Σε ένα διανυσματικό χώρο V ορισμένος όπως παραπάνω, θεωρούμε ένα σύνολο στοιχείων του V, $S = \{a_1, a_2, \ldots, a_n\}$. Λέμε ότι το S είναι μία βάση του V αν κάθε στοιχείο του V μπορεί να γραφτεί ως γραμμικός συνδυασμός των στοιχείων του S.*

Ουσιαστικά, η βάση ενός διανυσματικού χώρου είναι ένα σύνολο με γραμμικώς ανεξάρτητα διανύσματα.

Ορισμός 24. *Νόρμα είναι μια απεικόνιση* $|| \cdot || : V \to \mathbb{R}$ *με τις παρακάτω ιδιότητες:*

- $\forall a \in V, a \neq 0_V \Rightarrow ||a|| > 0$ *και αν* $a = 0_V$ *τότε* $||a|| = 0$
- $\forall a \in V, l \in \mathbb{F} \Rightarrow ||l \circ a|| = |l| \circ ||a||$
- $\forall a, b \in V \Rightarrow ||a \diamond b|| \leq ||a|| \diamond ||b||$

Αυτός ο ορισμός στην τοπολογία διαμορφώνεται όπως παρακάτω.

2. Τοπολογία

2.1. Μετρικοί χώροι

Ορισμός 25. *Έστω* X *ένα αυθαίρετο σύνολο. Μία απεικόνιση* $\rho : x \times x \to \mathbb{R}$ *καλείται μετρική στον* $\mathbb{R}$ *αν ισχύουν οι ακόλουθες προϋποθέσεις:*

- $\forall x, y \in X \Rightarrow \rho(x, y) \geq 0$
- $\forall x, y, \rho(x, y) = 0 \Leftrightarrow x = y$
- $\forall x, y \rho(x, y) = \rho(y, x)$
- $\forall x, y, z \in X \Rightarrow \rho(x, y) \leq \rho(x, z) + \rho(y, z)$

Ο χώρος (X, ρ) καλείται μετρικός χώρος.

Μέρος 2

Το Κρυπτοσύστημα Δημοσίου Κλειδιού NTRU

ΚΕΦΑΛΑΙΟ 2

Ο Αλγόριθμος Κρυπτογράφησης NTRU

1. Κρυπτογραφία

1.1. Τι είναι κώδικας?

Όλοι έχουμε ακούσει για κώδικες, για κωδικοποιημένα μηνύματα, για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων και άλλα σχετικά. Λίγοι όμως έχουν συνειδητοποιήσει ότι δεν υπάρχει άνθρωπος που να μη χρησιμοποιεί ανά πάσα στιγμή κώδικες.

Κώδικας είναι, όσο περίεργο κι αν ακούγεται, η γλώσσα που χρησιμοποιούμε για να επικοινωνούμε. Πράγματι κάθε τι που θέλουμε να εκφράσουμε προφορικώς ή γραπτώς το κωδικοποιούμε σε μία ακολουθία λέξεων χρησιμοποιώντας γράμματα από ένα αλφάβητο. Το σύνολο αυτών των λέξεων αποτελεί ένα μήνυμα το οποίο μεταδίδουμε προφορικώς, γραπτώς ή με άλλο τρόπο.

Σε μια γλώσσα που έχει ένα αλφάβητο μπορούμε να σχηματίσουμε πάρα πολλές “λέξεις”, θεωρητικά άπειρες. Από αυτές όμως λίγες έχουν νόημα, δηλαδή αποτελούν στοιχεία του γλωσσικού κώδικα επικοινωνίας. Για το σχηματισμό των λέξεων που έχουν νόημα χρησιμοποιούνται κανόνες, όπως ορθογραφικοί, γραμματικοί, συντακτικοί κλπ.[**2**]

Κατά τη μετάδοση ενός μηνύματος με κάποιο τρόπο ενδέχεται (μερικώς) να αλλοιωθεί. Η αλλοίωση μπορεί να επέλθει αν η μετάδοση γίνεται προφορικά και ο ομιλητής (ο αποστολέας του μηνύματος) δεν έχει καλή άρθρωση ή εάν ο παραλήπτης δεν έχει καλή ακοή ή ακόμα κι αν υπάρχουν θόρυβοι που παρεμβάλονται. Τότε, ο παραλήπτης είναι αναγκασμένος να συνάγει τι μήνυμα εστάλει από το μήνυμα που έλαβε (δηλαδή να αποκωδικοποιήσει το μήνυμα). Για βοήθεια έχει τον κώδικα γλωσσικής επικοινωνίας. Πολλές φορές είναι αναγκασμένος να εικάσει για το μήνυμα στηριζόμενος “στα συμφραζόμενα” ή ακόμα, αναλαμβάνοντας τον κίνδυνο για λανθασμένη απόδοση, να αποδόσει μέρος του μηνύματος τυχαία.

Οι “ανάγκες” πολλές φορές επιβάλλουν να επινοήσουμε άλλους τρόπους (κώδικες) επικοινωνίας. Για παράδειγμα οι Ινδιάνοι χρησιμοποιούσαν σήματα καπνού. Αργότερα με τη στοιχειώδη χρήση του ηλεκτρικού ρεύματος, επινοήθηκε ο κώδικας Morse. Σήμερα διαθέτουμε σύγχρονα ηλεκτρομαγνητικά μέσα εγγραφής, αποθήκευσης και μετάδοσης των μηνυμάτων.

1.2. Ιστορικά στοιχεία

Η κρυπτογραφία εμφανίζεται με τη μορφή τέχνης από τα πρώτα χρόνια που ο άνθρωπος άρχισε να γράφει. Χαρακτηριστικό παράδειγμα ο δίσκος της Φαιστού που θεωρείται το αρχαιότερο έντυπο στην ιστορία του ανθρώπου. Για το κείμενο του δίσκου, που χρονολογείται γύρω στον 17^o π.Χ. αιώνα έχουν δοθεί πολλές ερμηνείες, παρ’ όλα αυτά καμία δε θεωρείται αξιόπιστη και η αποκρυπτογράφησή του παραμένει άλυτο πρόβλημα.

Τα πρώτα στοιχεία εμφανίζονται στην Αίγυπτο με τα ιερογλυφικά που κοσμούσαν τους τάφους των εκλιπόντων βασιλέων. Σκοπός δεν ήταν η απόκρυψη κάποιου κειμένου αλλά η απόδοση τιμής στον κυβερνώντα με εντυπωσιακό τρόπο, καθώς με τα ιερογλυφικά εξυμνούσαν τα κατορθώματα και τις σπουδαίες πράξεις του. Στην Ινδία εμφανίζονται οι πρώτοι μυστικοί κώδικες κατά την επικοινωνία της κυβέρνησης με ένα δίκτυο κατασκόπων στη χώρα. Οι κώδικες αφορούσαν απλές αντικαταστάσεις με φωνήεντα. Το αρχαιότερο κρυπτογραφημένο κείμενο κατά τον Kahn[**37**] θεωρείται μια επιγραφή του 1500 π.χ. που βρέθηκε στη Μεσοποταμία και περιγράφει μια μέθοδο κατασκευής σμάλτων για αγγειοπλαστική. Το αρχαιότερο βιβλίο κρυπτοκωδίκων θεωρείται μια σφηνοειδής γραφή στη Σούσα της Περσίας που περιλαμβάνει αριθμούς από το 1 έως το 8 και από το 32 έως το 35 τοποθετημένους τον ένα κάτω από τον άλλο, ενώ δίπλα τους βρίσκονται διάφορα σφηνοειδή σύμβολα.

Οι Εβραίοι συγγραφείς πολλές φορές "έκρυβαν" τα γραπτά τους αντιστρέφοντας το αλφάβητο, χρησιμοποιώντας δηλαδή το τελευταίο γράμμα της αλφαβήτου στη θέση του πρώτου, το προτελευταίο στη θέση του δεύτερου κοκ. Αυτό το σύστημα είναι γνωστό ως Atbash.

Στην αρχία Ελλάδα, οι Σπαρτιάτες επικοινωνούσαν με τους στρατηγούς τους στη μάχη, γράφοντας το μήνυμα σε μία κορδέλα που ήταν τυλιγμένη σε μία ράβδο, τη σκυτάλη. Όταν ξετύλιγαν στη συνέχεια την κορδέλα, φαινόταν ένα ακατανόητο κείμενο λόγω της ανάμειξης των γραμμάτων. Το μήνυμα μπορούσε να διαβαστεί μόνο αν ξανατυλιγόταν σε παρόμοια σκυτάλη, ίσης διαμέτρου και μήκους.

Ο Έλληνας συγγραφέας Πολύβιος, τον 2 αιώνα π.Χ. εφηύρε το τετράγωνο του Πολύβιου, κατά το οποίο κάθε γράμμα της αλφαβήτου αντικαθίσταται με ένα πίνακα 5×5, το οποίο χρησιμοποιήθηκε σε διάφορα κρυπτογραφικά συστήματα.

Ο Ιούλιος Καίσαρας όταν έστελνε μηνύματα στους αξιωματικούς του, καθώς δεν εμπιστευόταν τους αγγελιοφόρους του, άλλαζε κάθε Α με το D, το Β με το Ε κοκ. Μόνο κάποιος που ήξερε τον κανόνα "μετατόπισε κατά 3", τον κανόνα δηλαδή με τον οποίον άλλαζαν τα γράμματα, μπορούσε να αποκρυπτογραφήσει τα μηνύματα.

Η εξέλιξη της κρυπτογραφίας συνεχίζεται στον Αραβικό κόσμο και στην Ινδία. Οι Άραβες ήταν οι πρωτοπόροι στις μεθόδους κρυπτανάλυσης με σημαντικότερη αυτή του κρυπτολόγου Al Kindi τον 9 αιώνα μ.Χ. που βασίζεται στη συχνότητα εμφάνισης των χαρακτήρων της κάθε γλώσσας.

Ένα από τα πρώτα έγγραφα με οδηγίες για την κρυπτογράφηση εγγράφων, χρονολογείται γύρω στο 1379 και είναι ένας συνδυασμός κρυπτοσυστημάτων από τον Gabriele de Lavinde της Πάρμας, που υπηρετούσε τον Πάπα Κλεμέντιο τον 7ο. Αυτό το έγγραφο, που τώρα βρίσκεται στα αρχεία του Βατικανού, περιέχει ένα σύνολο κλειδιών για 24 παραλήπτες και χρησιμοποιεί σύμβολα όπως γράμματα, αριθμούς και μερικές κώδικες δύο γραμμάτων που συμβόλιζαν λέξεις και ονόματα.

Λόγω των στρατιωτικών εξελίξεων η κρυπτογραφία γνώρισε άνθηση τους επόμενους αιώνες. Ο Ιταλός συγγραφέας και αρχιτέκτονας Leon Battista Alberti (1404-1472) ανέπτυξε ένα πολυαλφαβητικό σύστημα αντικατάστασης, όπου το ίδιο σύμβολο κρυπτογραφείται από πλήθος διαφορετικών συμβόλων ώστε να αλλοιώνεται η συχνότητα εμφάνισης των κρυπτογραφημένων χαρακτήρων, οπότε η κρυπτανάλυση του Al Kindi γίνεται πλέον ανεφάρμοστη. Για να υλοποιηθεί το σύστημα αυτό επινοήθηκε η πρώτη μηχανή κρυπτογράφησης μετά τη σκυτάλη, που ονομάστηκε δίσκοι του Alberti. Επίσης, σημαντικός εκπρόσωπος της πολυαλφαβητικής αντικατάστασης είναι ο Γάλλος Blaise de Vigenere. Το σύστημα του Vigenere μπορεί να θεωρηθεί ένα σύστημα του Καίσαρα στο οποίο το κλειδί αλλάζει από βήμα σε βήμα.

Το 1518 ο Johannes Trithemios έγραψε την πρώτη εκδιδόμενη εργασία κρυπτογραφίας που την ονόμασε *"Polygraphia"* και περιείχε τα πρώτα συστήματα κυκλικών μεταθέσεων.[**37**] Για πρώτη φορά παρουσίασε την ιδέα ενός τετραγώνου στο οποίο η αλφαβήτα, μεταφερόταν σε ένα προκαθορισμένο αριθμό διαστημάτων. Κάθε σειρά στην αλφαβήτα στη συνέχεια, χρησιμοποιούταν για να κρυπτογραφήσει ένα προκαθορισμένο αριθμό διαστημάτων. Για παράδειγμα, το πρώτο γράμμα κρυπτογραφούνταν με το πρώτο αλφάβητο, το δεύτερο γράμμα με το δεύτερο κοκ. Επομένως η λέξη CRYPTO θα γινόταν (C+0)=C, (R+1)=S, (Y+2)=A, (P+3)=S, (T+4)=X, (O+5)=T, δηλαδή CSASXT.

Αργότερα, το 1605, ο Francis Bacon, παρουσιάζει το κρυπτοσύστημά του, το οποίο βασιζόταν στη δημιουργία συνδυασμών των γραμμάτων a και b ανά 5 που ο καθένας τους σήμαινε ένα γράμμα της αλφαβήτου. Ο συγκεκριμένος κώδικας, παρουσιάζει για πρώτη φορά την αρχή ότι ο κώδικας με δύο σύμβολα μπορεί να χρησιμοποιηθεί για τη μεταφορά πληροφοριών.

Μέχρι το 1860 είχαν αρχίσει να εφαρμόζονται μεγάλοι κώδικες για τις διπλωματικές αποστολές ενώ η εφεύρεση του τηλέγραφου και του ραδιοφώνου οδήγησε στην ανάπτυξη της προστασίας των τηλεπικοινωνιών, δίνοντας άλλη διάσταση στην κρυπτολογία. Στην πρώιμη ιστορία των Ηνωμένων Πολιτειών, οι κώδικες ήταν δημοφιλείς. Κατά τη διάρκεια του Εμφυλίου, ο στρατός των Βορείων πρώτος χρησιμοποίησε κρυπτοσυστήματα στα οποία μία λέξη κλειδί έδειχνε τον τρόπο με τον οποίο θα έπρεπε να διαβαστούν οι στήλες στο κείμενο ή άλλα κρυπτοσυστήματα στα οποία υπήρχε αντικατάσταση κειμένου από άλλες λέξεις ή κώδικα. Από την άλλη πλευρά ο στρατός των Νοτίων χρησιμοποιούσε το κρυπτοσύστημα Vigenere και κατά περίπτωση αντικαταστάσεις μόνο γραμμάτων.

20ος αιώνας

Τον 20ο αιώνα, διάφοροι εμπορικοί κωδικοί αναπτύχθηκαν. Ένα τέτοιο σύστημα ήταν και ο κώδικας Baudot, μέσω του οποίου κρυπτογραφούνταν ολόκληρες προτάσεις σε απλές λέξεις των πέντε γραμμάτων για τη χρήση σε τηλέγραφο. Αυτό το είδος κώδικα δεν ήταν αρκετό βέβαια για το ραδιόφωνο ή για άλλες μορφές πιο εξελιγμένης επικοινωνίας.

Το 1918 εκδόθηκε μία από τις πιο σημαντικές εργασίες του 20ου αιώνα πάνω στην κρυπτανάλυση. Το “Index of Coincidence and its Applications in Cryptography” του Willian F. Friedman, παρουσίασε τα αποτελέσματα έρευνας στα ιδιωτικά εργαστήρια του Riverbank. Την ίδια χρονιά ο Edward H. Hebern στο Oakland της California, δημιούργησε την πρώτη συσκευή κρυπτογραφίας, η οποία χρησιμοποιήθηκε σε μεγάλο βαθμό σε πολεμικές επιχειρήσεις τα επόμενα 50 χρόνια.

Μετά τον Α’ Παγκόσμιο Πόλεμο, τα πράγματα άρχισαν να αλλάζουν. Ο στρατός και το ναυτικό των Η.Π.Α. εν πλήρη μυστικότητα, άρχισαν να κάνουν θεμελιώδης αλλαγές στην κρυπτογραφία, χωρίς όμως αυτές να ανακοινώνονται στο κοινό. Στις δεκαετίες του ’30 και του ’40, μερικές βασικές εργασίες εκδόθηκαν για το κοινό, αλλά οι περισσότερες ήταν ασήμαντες.

Εξαίρεση ήταν η εργασία του Claude Shannon “The communication Theory of Secret Systems” που εκδόθηκε το 1949 στο περιοδικό “Bell System Technical Journal”. Ήταν συνέχεια της εργασίας του Friedman του 1918.

Με την εξάπλωση του ραδιοφώνου δόθηκε μία νέα πλευρά στην κρυπτογραφία, αφού οποιοσδήποτε μπορούσε πολύ εύκολα να παρακολουθήσει τις διάφορες συχνότητες σε μεγάλη απόσταση. Η έκβαση του Β’ Παγκοσμίου Πολέμου επηρεάστηκε αρκετά από τη χρήση και το “σπάσιμο” κρυπτοσυστημάτων μέσω ραδιοφώνου.

Η Μηχανή Enigma που χρησιμοποιήθηκε από τους Γερμανούς κατά το Β’ Παγκόσμιο Πόλεμο για κρυπτογράφηση ραδιοτηλεπικοινωνιών ήταν ίσως το πλέον εξελιγμένο κρυπτοσύστημα της εποχής. Ο κώδικας Enigma θυμίζει έναν κώδικα τύπου Vigenere, αλλά είναι πολύ πιο πολύπλοκος.

Οι Βρετανοί συγκέντρωσαν μία ομάδα κρυπταναλυτών και μαθηματικών με επικεφαλής των Alan Turing, σε μία βικτωριανή έπαυλη στο Buckinghamshire που ονομαζόταν Bletchley Park. Η ομάδα βάσισε τις προσπάθειές της στη λεγόμενη μέθοδο πιθανής λέξης, η οποία βασίζεται στο γεγονός ότι σε κάποιες περιπτώσεις μία συγκεκριμένη ακολουθία συμβόλων σχεδόν σίγουρα αντιπροσωπεύει μία γνωστή λέξη. Μαντεύοντας σωστά μερικές από τις κρυπτογραφημένες λέξεις του κρυπτοκειμένου, μπορούσαν να καθορίζουν τη συνδεσμολογία της μηχανής δοκιμάζοντας όλες τις πιθανές συνδεσμολογίες και προσδιορίζοντας ποια είχε ως αποτελέσμα τα υποτιθέμενα ζευγάρια κρυπτογραφημένων-αποκρυπτογραφημένων λέξεων. Ο Turing αντιλήφθηκε ότι μόνο μία αυτόματη και σχετικά γρήγορη μηχανή θα μπορούσε να τα βγάλει πέρα με τις δοκιμές οπότε και οδηγήθηκε στην κατασκευή ενός εξομοιωτή της μηχανής Enigma με το όνομα Bombe.

Είναι σημαντικό να αναφέρουμε ότι οι υπολογιστικές συσκευές που δημιουργήθηκαν από τους Βρετανούς, για την κρυπτανάλυση του Γερμανικού συστήματος Enigma, από πολλούς θεωρείται ο πρώτος πραγματικός υπολογιστής. (Μηχανές Turing)

Από το 1949 μέχρι το 1967 οι περιορισμοί στις εκδόσεις απέκλεισαν κάθε έκδοση περί κρυπτογραφίας. Το βιβλίο του David Kahn “The Codebreakers” του 1963, δεν περιείχε νέες τεχνικές ιδέες, αλλά περιείχε μία ολοκληρωμένη ιστορία για την κρυπτογραφία, αρχίζοντας από τις αρχαίες Αιγυπτιακές μεθόδους 4000 χρόνια πριν και φτάνοντας στην κρυπτογραφία της σύγχρονης εποχής. Το βιβλίο “The Codebreakers”, εκτός από λογοτεχνική του αξία, καθώς παρουσίαζε την ιστορία από μία εκπληκτική ματιά και με γλαφυρό ύφος, έχει πολύ μεγάλη σημασία στην ιστορία, καθώς κατάφερε να πουλήσει δεκάδες χιλιάδες αντίτυπα και μετέφερε στους αναγνώστες που δεν είχαν ιδέα για το τι συμβαίνει, μία ιδέα για τις συνθήκες στο χώρο της κρυπτογραφίας. Με αυτόν τον τρόπο δόθηκε νέα πνοή στην κρυπτογραφία, αναπτύχθηκε ξανά το ενδιαφέρον και εργασίες άρχισαν ξανά να εμφανίζονται στο κοινό.

Στις αρχές της δεκαετίας του 1970 ο Horst Feistel, επιστήμονας της IBM, ανέπτυξε τον $Lucifer$, ένα κρυπτοσύστημα για ηλεκτρονικούς υπολογιστές πλέον, που χρησιμοποιούσε και αντικατάσταση και μεταφορά. Το 1977, το “United States National Bureau of Standards” (γνωστό σήμερα ως “National Institute of Standards and Technology-NIST”) ανέπτυξε μία κρυπτογραφική τεχνική γνωστή και ως “Data Encryption Standard (DES)”.

Ο DES βασιζόταν στον αλγόριθμο Lucifer και χρησιμοποιούσε τον δυαδικό κώδικα του υπολογιστή και μετέτρεπε το απλό κείμενο σε δυαδικά ψηφία 0 ή 1. Ο DES μετέτρεπε $64 - bit$ κομμάτια πληροφορίας σε $64 - bit$ κομμάτια κρυπτογραφημένου κειμένου, χρησιμοποιώντας ένα κλειδί που ήταν $56 - bit$ σε μέγεθος. Κάθε χρήστης επέλεγε ένα τυχαίο κλειδί και το αποκάλυπτε μόνο σε

αυτούς που θα είχαν το δικαίωμα να δουν τις προστατευμένες πληροφορίες. Ο DES ”έσπασε” το 1998 μέσα σε 56 ώρες.

Το 1976 ήρθε μία από τις πιο αξιοσημείωτες εξελίξεις στην ιστορία της κρυπτογραφίας, όταν οι Diffie και Hellman δημοσίευσαν το άρθρο “New Directions in Cryptography”. Με αυτήν την εργασία εισήγαγαν την επαναστατική ιδέα της κρυπτογραφίας δημοσίου κλειδιού και επίσης παρείχε μια νέα και ευφυή μέθοδο για την ανταλλαγή κλειδιών, η ασφάλεια της οποίας βασίζεται στη δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου.

Το 1978 τρεις Αμερικάνοι επιστήμονες, οι Ronald L. Rivest, Adi Shamir και Leonard Aldeman δημιούργησαν το σύστημα RSA (από τα αρχικά τους).[**15**] Το σύστημα RSA χρησιμοποιεί δύο μεγάλους πρώτους αριθμούς τους p και q, οι οποίοι πολλαπλασιάζονται για να δώσουν τον σύνθετο n. Αυτός ο σύνθετος n , είναι πολύ δύσκολο να παραγοντοποιηθεί και κατά συνέπεια να διαβληθεί το σύστημα.

Με τον RSA έγινε και η πρώτη ουσιαστική εισήγηση ενός αλγόριθμου κρυπτογράφησης δημοσίου κλειδιού. Τα κλειδιά (για την ακρίβεια μέρος τους) πλέον θα έπαυαν να είναι μυστικά και μία νέα εποχή στην Κρυπτογράφηση και τις εφαρμογές της θα άρχιζε από αυτό το σημείο.

Κατά τη διάρκεια της δεκαετίας του ’80, η πίεση δόθηκε περισσότερο στην πρακτική παρά στη μελέτη της κρυπτογραφίας. Με την παγκοσμιοποίηση όμως της αγοράς και καθώς και άλλες αγορές στον κόσμο αναπτύσσονταν η πίεση για ένα κοινό κρυπτογραφικό σύστημα και στο εσωτερικό και στο εξωτερικό των Η.Π.Α. μεγάλωνε. Η κρυπτογράφηση πλέον είχε αρχίσει να αποκτά έδαφος και σε άλλες εφαρμογές σε παγκόσμιο επίπεδο.

Καθώς όλο και περισσότερες πληροφορίες μεταφέρονται σε δίκτυα υπολογιστών, οι ανάγκες για πιο ασφαλείς και περίπλοκους αλγόριθμους γίνονται μεγαλύτερες. Το 1997 οι επιστήμονες της NIST, αντικατέστησαν τον DES με τον “Advanced Encryption Standard (AES)”. Ο AES χρησιμοποιεί πλέον ένα πιο περίπλοκο αλγόριθμο, βασισμένο σε κρυπτογράφηση 128-bits αντί για τα 64-bits του DES.

Ένα άλλο κρυπτοσύστημα βασίστηκε επίσης σε $128 - bit$ κομμάτια πληροφορίας και ονομάστηκε “International Data Encryption Algorithm (IDEA)”. Αναπτύχθηκε από το Ελβετικό Ινστιτούτο Τεχνολογίας τη δεκαετία του 1990.

Αναπτύχθηκαν επίσης πολλές τεχνικές που να καλύπτουν την κρυπτογράφηση πολλών ειδών επικοινωνίας. Για την κρυπτογράφηση τηλεφωνικών συνομιλιών, για παράδειγμα, το τσιπ clipper χρησιμοποιεί τεχνολογία Skipjack σε συνδυασμό με έναν αλγόριθμο αναταλλαγής κλειδιών “(Key Exchange Algorithm - KEA)”.[**31, 32**] Αυτά ενσωματώνονται σε μία κάρτα υπολογιστή μαζί με άλλους δύο αλγόριθμους, τον “Digital Signature Algorithm (DSA)” και τον “Secure Hash Algorithm (SHA)” και το τσιπ που προκύπτει με την ονομασία Tessera, μπορεί να κωδικοποιήσει κάθε είδους επικοινωνία.

Σήμερα, καθώς το διαδίκτυο έχει κεντρικό ρόλο στην καθημερινότητα του ανεπτυγμένου κόσμου, χρησιμοποιούνται ευρέως πρωτόκολλα που επιτρέπουν την αποστολή και λήψη κρυπτογραφημένων δεδομένων, χωρίς να μεσολαβεί ο χρήστης. Τα πρωτόκολλα “TLS (Transport Layer Security)” και “SSL (Secure Sockets Layer)” μπορούν να παρέχουν ασφάλεια στην ανταλλαγή ψηφιακών δεδομένων σε εφαρμογές όπως η περιήγηση διαδικτύου, το ηλεκτρονικό ταχυδρομείο, εφαρμογές VoIP κτλ και κάνουν χρήση ασύμμετρων αλγορίθμων κρυπτογράφησης.

Τέλος, πρόοδος έχει σημειωθεί και σε άλλες μεθόδους κρυπτογράφησης όπως η κβαντική κρυπτογραφία, όπως επίσης και στην κρυπτογράφηση και υδατογράφηση δεδομένων με τέτοιο τρόπο (σε επίπεδο λογισμικού ή και υλικού) ώστε να είναι αδύνατη η αντιγραφή τους για την προστασία πνευματικών δικαιωμάτων.

1.3. Κρυπτογραφία

Από την αμοιβαία αλληλεπίδραση των μαθηματικών που πρόσφεραν το σχεδιασμό και των υπολογιστών που επέπτρεψαν τη χρήση περιπλοκότερων αλγορίθμων κρυπτογράφησης, εξελίχθηκε η επιστήμη της κρυπτογραφίας. Η μελέτη της άπτεται των μαθηματικών (θεωρία αριθμών και αλγεβρικές δομές) και της υπολογιστικής θεωρίας πολυπλοκότητας. [**26, 27**]

Στόχος είναι η ασφάλεια της επικοινωνίας δια μέσου ενός επισφαλούς μέσου επικοινωνίας,[**28**], (παράδειγμα το Internet) μιας και δεν υπάρχει ιδεατό μέσο επικοινωνίας, ένα δίαυλο δηλαδή που κανείς πέρα από τους μετέχοντες στην επικοινωνία δεν δίναται να αντιληφθεί το περιεχόμενο της

επικοινωνίας. Οι αξιόπιστοι τρόποι μετάδοσης δεδομένων μέσα από επισφαλή κανάλια επικοινωνίας, είναι το κομμάτι της επιστήμης των υπολογιστών και των μαθηματικών με το οποίο ασχολείται η θεωρία κωδίκων. Η πληροφορία εκπέμπεται από μία πηγή (πομπός), αλλάζει μορφή (κωδικοποιείται), μεταφέρεται μέσω κάποιου δικτύου και αποκωδικοοιείται ώστε να γίνει αναγνωρίσιμη από τον παραλήπτη (δέκτη). [**2**]

Η θεωρία κωδίκων εφαρμόζεται συνήθως όταν:

- Το μήνυμα αλλοιώνεται από ανεπιθύμητες παρεμβολές κατά τη μεταφορά του. Σε αυτήν την περίπτωση η θεωρία κωδίκων προσπαθεί να ελαχιστοποιήσει τα λάθη ώστε το μήνυμα να φτάσει στο δέκτη με τη μικρότερη πιθανότητα λάθους.
- Σκοπός είναι η ασφαλής μετάδοση της πληροφορίας, εκόμα και σε περίπτωση επέμβασης στη διαδικασία μετάδοσής της. Το κομμάτι αυτό της θεωρίας κωδίκων ονομάζεται κρυπτολογία.

'Οπως έχουμε αναφέρει και στην αρχή, η κρυπτολογία χωρίζεται σε δύο κλάδους, την κρυπτογραφία και την κρυπτανάλυση. Η κρυπτογραφία μελετά τις μαθηματικές μεθόδους και τεχνικές που εξασφαλίζουν την ασφαλή μετάδοσης της πληροφορίας από ένα μη αξιόπιστο δίαυλο επικοινωνίας. Η ασφάλεια αφορά τα εξής:

- Εμπιστευτικότητα (να μη γίνεται γνωστό το περιεχόμενο της πληροφορίας που ανταλλάσεται ανάμεσα στον πομπό και το δέκτη)
- Ακεραιότητα (να μην υπάρχει δυνατότητα τροποποίησης της πληροφορίας από μη εξουσιοδοτημένο άτομο)
- Αυθεντικότητα (να υπάρχει σιγουριά για την ταυτότητα του πομπού και του δέκτη, την ημερομηνία, την προέλευση της πληροφορίας κτλ)
- Αδυναμία αποκήρυξης (πομπός και δέκτης να μην αρνηθούν την αποστολή ή υπογραφή κάποιας παλαιότερης συνδιαλλαγής)

Η Κρυπτογραφία αφορά την κατασκευή και την ανάλυση των πρωτοκόλλων ασφαλείας.[**29, 30**]. Το πρωτόκολλο, στην πραγματικότητα, μας δίνει τους κανόνες λειτουργίας και συμπεριφοράς για το κάθε συμβαλλόμενο μέρος. Είναι δηλαδή ένα πρόγραμμα, ένα σχέδιο (scheme).

Η κρυπτογραφία έχει κάποιους κανόνες. Ο πρώτος κανόνας είναι ότι μπορούμε να προσπαθήσουμε να υπερνικήσουμε τον αντίπαλο με τη βοήθεια πρωτοκόλλων. Ο δεύτερος κανόνας είναι ότι τα πρωτόκολλα πρέπει να είναι δημοσίως γνωστά. Αυτά που πρέπει να παραμένουν μυστικά, πρέπει να ενσωματόνονται στα κλειδιά (που είναι στην πραγματικότητα δεδομένα και όχι ο αλγόριθμος).

1.4. Κβαντική κρυπτογραφία

Η κβαντική κρυπτογραφία χρησιμοποιεί τις τεχνολογίες της Κβαντικής Υπολογιστικής, μία υπολογιστική επιστήμη συνεχώς ανερχόμενη, αν και ακόμα δεν είναι εφαρμόσιμη. Ένας κβαντικός υπολογιστής βασίζεται στην ιδέα των κβαντικών bits ή αλλιώς qubits. Στους κλασσικούς υπολογιστές, το bit μπορεί να βρεθεί στις καταστάσεις 0 ή 1. Ένα qubit όμως, μπορεί να βρεθεί σε υπερκατάσταση αυτών των δύο τιμών. Ένας quantum καταχωρητής αποτελείται από qubits. Λόγω αυτών των ιδιοτήτων ένα κβαντικός υπολογιστής είναι σε θεση να κάνει έναν εκθετικά αυξανόμενο αριθμό πράξεων παράλληλα και να αυξήσει τις ταχύτητες υπολογισμών.

Έχει αποδειχθεί ότι ένας κβαντικός υπολογιστής μπορεί να παραγοντοποιεί και να υπολογίζει διακριτούς λογαρίθμους σε πολυωνυμικό χρόνο. [**38, 39, 40, 41, 42**] Δυστυχώς όμως η ανάπτυξη ενός τέτοιου υπολογιστή φαντάζει πολύ δύσκολη λόγω των διαφόρων φαινομένων που έχουν σχέση με την επίδραση του περιβάλλοντος σε έναν τέτοιο υπολογιστή.

Η κβαντική κρυπτογραφία είναι μία μέθοδος αποστολής μυστικών κλειδιών μέσω ενός μη-ασφαλούς καναλιού. Για την επίτευξη αυτού γίνεται χρήση ορισμένων ιδιοτήτων των φωτονίων. Τα φωτόνια χαρακτηρίζονται από την πολικότητά τους, η οποία μπορεί να μετρηθεί από οποιαδήποτε βάση, η οποία βάση αποτελείται από δύο διευθύνσεις ορθογώνιες η μία στην άλλη.

Αν η πολικότητα ενός φωτονίου διαβαστεί μέσω της ίδιας βάσης δύο φορές, θα έχει διαβαστεί σωστά και θα παραμείνει σταθερή. Αν διαβαστεί από δύο διαφορετικές βάσεις, θα προκύψει μία τυχαία απάντηση στη δεύτερη βάση, ενώ η πολικότητα στην αρχική βάση θα αλλάξει τυχαία.

Η πιο γνωστή εφαρμογή κβαντικής κρυπτογραφίας είναι η δημιουργία κβαντικών κλειδιών (Quantum Key Distribution - QKD). Έστω ότι η Alice και ο Bob επιθυμούν να ανταλλάξουν κλειδιά μεταξύ τους. Χρησιμοποιείται το ακόλουθο πρωτόκολλο γι' αυτή τη διαδικασία:

- Η Alice στέλνει στο Bob μία σειρά από φωτόνια, το καθένα με τυχαία πολικότητα σε τυχαία βάση. Καταγράφει τις πολικότητες.
- Ο Bob μετράει κάθε φωτόνια σε τυχαία βάση και καταγράφει τα αποτελέσματα.
- Ο Bob ανακοινώνει (όχι απαραίτητα σε ιδιωτικό κανάλι, πχ ένα τηλέφωνο), ποια βάση χρησιμοποίησε για κάθε φωτόνιο.
- Η Alice του λέει ποιες βάσεις που χρησιμοποίησε είναι σωστές.
- Δημιουργείται το κλειδί από τις πολικότητες των φωτονίων που διαβάστηκαν με τη σωστή βάση.

Αν κάποιος τρίτος προσπαθεί να παρεισφρήσει κατά τη διάρκεια της μετάδοσης φωτονίων, θα χρησιμοποιήσει λάθος βάσεις, τουλάχιστον τις μισές φορές και κατά συνέπεια θα αλλάξει και κάποιες πολικότητες. Αν η Alice και ο Bob στο τέλος έχουν διαφορετικές τιμές για το κλειδί, σημαίνει ότι υπήρξε κάποιος εισβολέας στη μετάδοση.

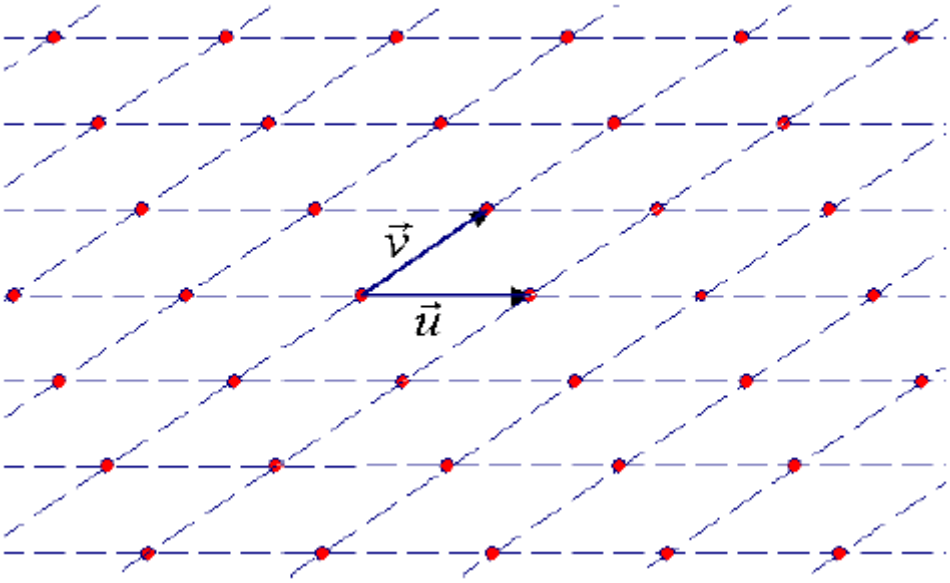
2. Ο αλγόριθμος κρυπτογράφησης NTRU

2.1. Lattices (Πλέγματα Σημείων)

Ορισμός 26. *Αν $a_1, a_2, \ldots, a_n$ είναι n ανεξάρτητα διανύσματα στον $\mathbb{R}^m$ με $n \leq m$, τότε το ακέραιο πλέγμα σημείων με αυτά τα διανύσματα ως βάση είναι το σύνολο*

$$\mathcal{L} = \{\sum_{i=1}^{n} x_i a_i : x_i \in \mathbb{Z}\}$$

Το πλέγμα σημείων είναι δηλαδή, το σύνολο των γραμμικών συνδυασμών των $a_1, a_2, \ldots, a_n$ με συντελεστές ακεραίους. Το πλέγμα σημείων παράγεται από τα παραπάνω διανύσματα.



Σχήμα 1. Πλέγμα Σημείων στον R^2

Ως βάση επομένως του πλέγματος σημείων ορίζουμε τον $n \times m$ πίνακα που περιέχει τα $a_1, a_2, \ldots, a_n$ ως γραμμές. Τα στοιχεία του πλέγματος σημείων είναι τα διανύσματα της μορφής $v^T A$ όπου v ένα διάνυσμα του πλέγματος σημείων και A η αναπαράσταση του πλέγματος σημείων με γραμμές τα διανύσματα της βάσης $a_1, a_2, \ldots, a_n$.

Ο ακέραιος n λέγεται διάσταση του πλέγματος σημείων και ο m τάξη του. Αν $n = m$ τότε το $\mathcal{L}$ λέγται πλέγμα σημείων πλήρους τάξης.

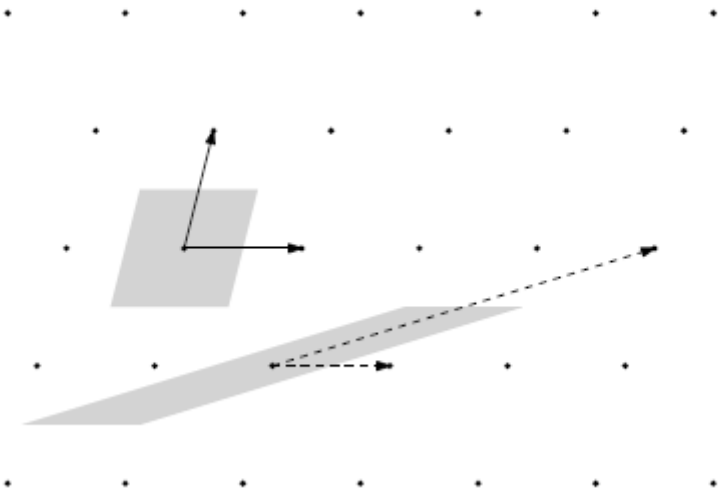
Υπάρχει αρκετή ομοιότητα στον ορισμό του πλέγματος σημείων και τον ορισμό του διανυσματικού χώρου παραγόμενου από τα διανύσματα $= \{a_1, a_2, \ldots, a_n\}$. Η διαφορά είναι ότι στον παραγόμενο χώρο μπορούμε να συνδυάσουμε τις στήλες του A με τυχαίους πραγματικούς αριθμούς, ενώ στο πλέγμα σημείων παίρνουμε μόνο ακεραίους και με αυτόν τον τρόπο καταλήγουμε σε ένα διακριτό σύνολο σημείων

Παράδειγμα 9. *Το $\mathbb{Z}^n$ είναι το πλέγμα σημείων που αποτελείται από όλα τα διανύσματα με ακέραιες συντεταγμένες.*

Ισοδύναμα, ένα ακέραιο πλέγμα σημείων είναι μια προσθετική υποομάδα του $\mathbb{Z}^m$ για κάποιο $m \geq 1$.

Έστω μία βάση $v_1, v_2, \ldots, v_n$ του $\mathcal{L}$ και έστω $w_1, w_2, \ldots, w_n \in \mathcal{L}$ μία άλλη συλλογή διανυσμάτων στο $\mathcal{L}$. Μπορούμε να αναπαραστήσουμε το κάθε w_j σα γραμμικό συνδυασμό των διανυσμάτων της βάσης ως εξής:

$$w_1 = a_{11}v_1 + a_{12}v_2 + \ldots + a_{1n}v_n$$
$$w_2 = a_{21}v_1 + a_{22}v_2 + \ldots + a_{2n}v_n$$
$$\ldots$$
$$w_n = a_{n1}v_1 + a_{n2}v_2 + \ldots + a_{nn}v_n$$



Σχήμα 2. Πλέγμα Σημείων με 2 πιθανές βάσεις

όπου οι συντελεστές a_{ij} είναι όλοι ακέραιοι. Με αυτόν τον τρόπο μπορούμε να δημιουργήσουμε τον πίνακα των συντελεστών:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Από τα παραπάνω, αποδεικνύεται ότι:

Πρόταση 2. *Οποιεσδήποτε δύο βάσεις ενός πλέγματος σημείων $\mathcal{L}$ σχετίζονται με έναν πίνακα που έχει ακέραια στοιχεία και ορίζουσα ίση με ± 1.*

Παράδειγμα 10. *Το $\mathbb{Q}^n$ είναι μία υποομάδα του $\mathbb{R}^n$ αλλά δεν είναι πλέγμα σημείων γιατί δεν είναι διακριτή.*

Παράδειγμα 11. *Το σύνολο $\mathbb{Z}^n$ είναι ένα πλέγμα σημείων γιατί ακέραια διανύσματα μπορούν να προστεθούν και να αφαιρεθούν και προφανώς η απόσταση ανάμεσα σε δύο οποιαδήποτε ακέραια διανύσματα είναι τουλάχιστον 1.*

Όπως αναφέρεται παραπάνω,η απόσταση μεταξύ δύο σημείων ορίζεται ως η νόρμα της διαφοράς τους $d(x, y) = ||x - y||$, όπου μία νόρμα είναι μία συνάρτηση $|| \cdot || : \mathbb{R}^n \to \mathbb{R}$ για την οποία ισχύουν:

- $||x|| > 0 \forall x \in \mathbb{R}^n \setminus \{0\}$
- $||a \cdot x|| = |a| \cdot ||x|| \, \forall x \in \mathbb{R}^n, a \in \mathbb{R}$
- $||x + y|| \leq ||x|| + ||y|| \forall x, y \in \mathbb{R}^n$

Το κυριότερο παράδειγμα είναι η Ευκλείδια νόρμα. Για κάποιο διάνυσμα v του πλέγματος σημείων, η ευκλείδια νόρμα είναι η: $||v||_2 = \sqrt{\sum_{i=1}^{N} v_i^2}$. Στην πραγματικότητα, ο αριθμός που βγαίνει αντιπροσωπεύει την απόσταση του διανύσματος v από την αρχή των αξόνων. Αντίστοιχα, μια παράσταση της μορφής $||x - y||$ είναι ένα μέτρο της απόστασης των διανυσμάτων x και y.

Ομοίως, έχουμε την άπειρη νόρμα: $||v||_\infty = max\{|v_1|, |v_2|, \ldots, |v_n|\}$. Γενικά, οποιαδήποτε συνάρτηση επαληθεύει τις παραπάνω ιδιότητες είναι νόρμα.

2.2. SVP και CVP προβλήματα

Τα δύο βασικά προβλήματα στην θεωρία των ακέραιων πλεγμάτων σημείων είναι το Πρόβλημα του Βραχύτερου Διανύσματος –“Shortest Vector Problem (SVP)” και το πιο γενικό Πρόβλημα του

Εγγύτερου Διανύσματος –"Closest Vector Problem (CVP)". Και τα δύο αυτά προβλήματα αφορούν την εύρεση της πιο αποτελεσματικής βάσης για το πλέγμα σημείων, μία βάση που περιέχει διανύσματα που είναι όσο μικρά και όσο ορθογώνια γίνεται.

Δεδομένου μιας βάσης A για ένα πλέγμα σημείων $\mathcal{L}$ το SVP είναι η εύρεση ενός μη-μηδενικού διανύσματος στο πλέγμα σημείων με την ελάχιστη νόρμα, δηλαδή με το μικρότερο μήκος ανάμεσα στο σύνολο των διανυσμάτων, ξεκινώντας από το στοιχείο μηδέν και εξετάζοντας όλα τα μη μηδενικά στοιχεία v sto $\mathcal{L}$.

SVP : Δεδομένου μίας βάσης πλέγματος σημείων A, πρέπει να βρεθεί το μικρότερο μη-μηδενικό διάνυσμα στο $\mathcal{L}(A)$
Input μία βάση του πλέγματος σημείων, A
Output $v \in \mathcal{L} : ||v|| \leq ||x|| \; \forall x \in \mathcal{L}$

Δεδομένου ενός τυχαίου διανύσματος v στον $\mathbb{Z}^n$ το CVP είναι το πρόβλημα της εύρεσης ενός σημείου του πλέγματος σημείων $x^T A$ που είναι το πιο κοντινό από άποψη νόρμας στο v, είναι δηλαδή το πλησιέστερο στο v. [1]

CVP : Δεδομένου μίας βάσης του πλέγματος σημείων $\in \mathbb{Z}^n$ και ενός διανύσματος $t \in \mathbb{Z}^n$, πρέπει να βρεθεί το στοιχείο του πλέγματος σημείων που είναι το πλησιέστερο στο t.
Input μία βάση πλέγματος σημείων A, ένα διάνυσμα $t \in \mathbb{Z}^n$
Output $v \in \mathcal{L} : ||v - t|| \leq ||x - t|| \; \forall x \in \mathcal{L}$

Για κανένα από αυτά τα προβλήματα, δεν υπάρχει αλγόριθμος που τελειώνει σε πολυωνυμικό χρόνο και να τα λύνει, αν και έχουν ερευνηθεί πολύ θεωρητικά και πειραματικά. Επίσης, για το SVP η λύση μπορεί να μην είναι μοναδική. Για παράδειγμα, στον $\mathbb{Z}^2$ και τα τέσσερα διανύσματα $(0, \pm 1)$, $(\pm 1, 0)$ είναι λύσεις του προβλήματος. Ομοίως και για το CVP, το σημείο που βρίσκουμε μπορεί να είναι μοναδικό, μπορεί και όχι.

Και τα δύο προβλήματα είναι πολύ δύσκολα και η δυσκολία τους αυξάνει καθώς η διάσταση των πλεγμάτων σημείων μεγαλώνει.

Πρακτικά το CVP θεωρείται λίγο πιο δύσκολο από το SVP, εφόσον το πρώτο μπορεί συχνά να αναχθεί στο δεύτερο με ελαφρώς υψηλότερη διάσταση. Στην πιο γενική περίπτωση και τα δύο προβλήματα θεωρούνται εξαιρετικά δύσκολα, πρακτικά όμως αυτή η γενικότητα δεν επιτυγχάνεται. Στην πραγματικότητα, τα κρυπτοσυστήματα που είναι βασισμένα σε προβλήματα NP-πλήρη ($NP - complete$) ή NP-δύσκολα ($NP - hard$) τείνουν να βασίζονται σε συγκεκριμένη υποκατηγορία προβλημάτων, είτε για να επιτύχουν την αποδοτικότητα είτε για να επιτρέψουν τη δημιουργία καταπακτών. [**4**]

Αφού γίνει αυτό υπάρχει η πιθανότητα πως κάποια ειδική κατηγορία της επιλεγμένης υποκατηγορίας προβλημάτων να κάνει ευκολότερη την επίλυση από ότι η γενική περίπτωση. Για παράδειγμα το γενικό πρόβλημα του σακιδίου είναι NP-πλήρης, αλλά το μεταμφιεσμένο υπεραυξημένο πρόβλημα του σακιδίου που προτάθηκε να χρησιμοποιηθεί στην κρυπτογραφία είναι πολύ πιο εύκολο στην επίλυσή του.[**4**]

2.2.1. NP–πλήρη και NP–δύσκολα προβλήματα

Γενικός στόχος είναι η κατηγοριοποίηση των προβλημάτων ανάλογα με το αν μπορούν να λυθούν σε πολυωνυμικό χρόνο ή όχι. Δυστυχώς, μία τεράστια συλλογή από βασικά προβλήματα δεν έχουν κατηγοριοποιηθεί με αυτόν τον τρόπο, παρά τις μεγάλες προσπάθειες που έχουν γίνει.

Προβλήματα για τα οποία υπάρχει πολυωνυμικός αλγόριθμος ανήκουν στο σύνολο προβλημάτων απόφασης P.

Προβλήματα που δεν γνωρίζουμε αλγόριθμους ποκυωνυμικού χρόνου και ταυτόχρονα δεν μπορούμε να αποδείξουμε ότι δεν υπάρχουν αλγόριθμοι πολυωνυμικού χρόνου ανήκουν στα NP-πλήρη προβλήματα. Από αυτά, μία μεγάλη κλάση προβλημάτων έχει αποδειχθεί ότι είναι ισοδύναμα με την ακόλουθη έννοια:[**43**]

[1] x^T είναι ο ανάστροφος πίνακας του x, δηλαδή αν $x = [x_{ij}] \, \forall i, j \in \mathbb{N}$ τότε $x^T = [x_{ji}] \, \forall i, j \in \mathbb{N}$

Για τα NP-πλήρη προβλήματα γνωρίζουμε ότι ένας αλγόριθμος πολυωνυμικού χρόνου για οποιοδήποτε από αυτά θα σήμαινε την ύπαρξη ενός αλγορίθμου πολυωνυμικού χρόνου για όλα. Έτσι μπορούν να διατυπωθούν με τυπικό τρόπο προτάσεις όπως:

Το πρόβλημα Χ είναι τουλάχιστον εξίσου δύσκολο με το πρόβλημα Υ.

2.3. Ο LLL αλγόριθμος

Συχνά, από τις άπειρες βάσεις ενός δεδομένου πλέγματος σημείων, ξεχωρίζουν κάποιες με "καλές" ιδιότητες. Κανείς ορίζει αρχικά μια τέτοια ιδιότητα και στη συνέχεια προσπαθεί να βρει μια βάση που την ικανοποιεί. Η διαδικασία μετάβασης απο την αρχική βάση στη βάση που ικανοποιεί την ιδιότητα ονομάζεται αναγωγή της βάσης. [**11**]

Το 1982, οι Lenstra, Lenstra και Lovasz όρισαν μια τέτοια ιδιότητα και έδωσαν έναν αλγόριθμο πολυωνυμικού χρόνου για την εύρεση της ανηγμένης βάσης. Η ιδιότητα αυτή ονομάζεται LLL–ιδιότητα και η τελικά βάση LLL–ανηγμένη. Ο αλγόριθμος είναι γνωστός ως LLL.

Ο LLL βρίσκει ένα κατά προσέγγιση μικρό διάνυσμα και είναι εγγυημένο να είναι ανάμεσα σε ένα παράγοντα $(2/\sqrt{3})^n$ από το πραγματικό μικρότερο διάνυσμα, σε πολυωνυμικό χρόνο. Ο αλγόριθμος αυτός παράγει μία "ανηγμένη" βάση ενός πλέγματος σημείων και παράγει το κατά προσέγγιση μικρότερο διάνυσμα ως αποτέλεσμα.[**6**]

2.3.1. Περιγραφή του LLL αλγορίθμου

Σκοπός είναι να βρεθεί μία καλύτερη βάση του πλέγματος σημείων από αυτήν που υπάρχει ήδη. Για να γίνει εφικτό αυτό, χρησιμοποιούμε τον LLL αλγόριθμο. Πριν όμως εξηγήσουμε πως λειτουργεί, θα πρέπει να περιγράψουμε τη διαδικασία Gram–Schmidt ορθοκανονικοποίησης βάσης, η οποία είναι ένας αποτελεσματικός (αποδοτικός) αλγόριθμος που παράγει μία ορθοκανονική βάση ξεκινώντας από μία τυχαία.

Ορίζουμε ως προβολή ενός στοιχείου a πάνω στο χώρο που εκτείνεται τα διανύσματα $S = \{a_1, a_2, \ldots, a_k\}$ με $proj_S(a) = \sum_{i=1}^{k} \frac{< a, a_i >}{< a_i, a_i >} \cdot a_i$

Αλγόριθμος 1. *(Gram–Schmidt Ορθοκανονικοποίησης Βάσης)*
Input: Μία τυχαία βάση $B = \{b_1, b_2, \ldots, b_n\}$ *του υποχώρου* $\mathbb{R}^n$
Output: Μία ορθοκανονική βάση του ίδου υποχώρου

(1) *Υπολογίζουμε* $v_1 = b_1$ *και* $u_1 = \frac{v_1}{||v_1||}$

(2) *Υπολογίζουμε* $v_i = b_i - \sum_{j=1}^{i-1} proj_{b_i}(v_i)$ *και* $u_i = \frac{v_i}{||v_i||}$

(3) *Επιστρέφει* $\{u_1, u_2, \ldots, u_n\}$

Ο παραπάνω αλγόριθμος είναι αποτελεσματικός μόνο στις 2 διαστάσεις. Γενικά όταν η διάσταση είναι μεγαλύτερη του 2 τότε η ορθογωνοποίηση δεν είναι καθόλου εύκολη και μέχρι σήμερα όλοι οι γνωστοί αλγόριθμοι καθυστερούν.

Ο αλγόριθμος LLL παράγει σχεδόν ορθογώνιες βάσεις σε μεγαλύτερες διαστάσεις.[**11, 10**]

Για απλοποίηση του ορισμού, συμβολίζουμε με μ_{ij} τον όρο $\frac{<v_i, b_j>}{<b_j, b_j>}$ που προκύπτει από τον παραπάνω αλγόριθμο ορθογωνοποίησης των Gram–Schmidt.

Ορισμός 27. *(Ανηγμένη βάση LLL).*
Έστω $\mathcal{L}$ *ένα πλέγμα σημείων και* B *μία βάση του. Υποδηλώνουμε με το* b_i *την* $i-$*οστή στήλη του πίνακα* B*. Ο* B *λέγεται LLL ανηγμένος με παράμετρο* δ, $1/4 \leq \delta \leq 1$ *αν οι παρακάτω συνθήκες ικανοποιούνται:*

- $|\mu_{ij} \leq 1/2, \forall\, i > j$
- *Για κάθε ζευγάρι διαδοχικών διανυσμάτων* b_i, b_{i+1} *με* $i < n$ *έχουμε*

$$\delta ||proj_{a_j}(b_i)||^2 \leq ||proj_{a_j}(b_{i+1})||^2$$

Αλγόριθμος 2. *(**Ο LLL αλγόριθμος**[**7**])*
Input: Μία βάση πλέγματος σημείων $B = \{b_1, b_2, \cdots, b_n\} \in \mathbb{Z}^n$

Output: Μία $\delta - LLL-$ανηγμένη βάση για το ίδιο πλέγμα σημείων.

(1) *Υπολογίζουμε τη βάση* $b_1^*, b_2^*, \cdots, b_n^*$ *την οποία παράγει ο αλγόριθμος Gram–Schmidt.*

(2) *Θέτουμε* $b_i \leftarrow b_i - \frac{<b_i, b_j^*>}{<b_j^*, b_j^*>}$, $i \in [2, n]$ *και* $j \in [1, i-1]$

(3) *Αν υπάρχει* i *τέτοιο ώστε* $||b_{i+}^* + \mu_{i+1,i} \cdot b_i^*||^2 < \delta||b_i^*||^2$ *τότε*

(α΄) *Ανταλλάσουμε το* b_i *με το* b_{i+1}

(β΄) *Τρέχουμε τον LLL αλγόριθμο με εισοδο τα* $\{b_1, b_2 \cdots, b_n\}$

(4) *Επιστρέφουμε το* $\{b_1, b_2 \cdots, b_n\}$

Υποθέτουμε ότι έχουμε μία τυχαία βάση B του πλέγματος σημείων $\mathcal{L}$, τότε μπορούμε να εκμεταλλευτούμε τον παραπάνω αλγόριθμο και να παράξουμε μία ανηγμένη βάση B' που επίσης περιγράφει το πλέγμα σημείων $\mathcal{L}$ αλλά δίνει μία καλύτερη απεικόνιση του πλέγματος σημείων από ότι η αρχική βάση.[**7**]

2.3.2. Υλοποίηση του LLL αλγορίθμου σε Python

Ο πρώτος αλγόριθμος υπολογίζει την ορθογωνοποίηση κατά Gram–Schmidt και ελέγχει αν ο πίνακας B είναι μειωμένος κατά c ή όχι.

```
def LLL_reduced(B,c=2)
  n=B.mrows()
  m=B.ncols()
  U=matrix(RR,m,m)
  V=matrix(RR,n,m)
  for i in range(0,m) :
        U[i,i]=1
        V.set_column(i,B.column(i))
        for j in range(0,i) :
                U[j,i]=(B.column(i)*V.column(j))/ \
                        (V.column(j)*V.column(j))
  for i in range(0,m-1) :
        if V.column(i)*V.column(i)>c*V.column(i+1)*V.column(i+1) :
                return False
  return True
```

Ο κώδικας για τον LLL αλγόριθμο σε Python είναι ο ακόλουθος:

```
def reduce(i,B,U)
        j=i-1
        while j>=0:
                B.set_column(i,B.column(i)-round(U[j,i])*B.column(j))
                U.set_column(i,U.column(i)-round(U[j,i])*U.column(j))
                j=j-1

def LLL(B,c=2)
        n=B.nrows()
        m=B.ncols()
        U=matrix(RR,m,m)
        V=matrix(RR,n,m)
        for i in range(0,m) :
                U[i,i]=1
                V.set_column(i,B.column(i))
                for j in range(0,i) :
                        U[j,i]=(B.column(i)*V.column(j))/ \
                                (V.column(j)*V.column(j))
                        V.set_column(i,V.column(i)-U[j,i]*V.column(j))
```

```
                    reduce(i,B,U)

    i=0
    while i<m-1:
    if V.column(i)*V.column(i)<=c*V.column(i+1)*V.column(i+1) :
            i=i+1
    else :
            V.set_column(i+1),V.column(i+1)+U[i,i+1]*V.column(i))
            U[i,i]=(B.column(i)*V.column(i+1)/ \
                    (V.column(i+1)*V.column(i+1))
            U[i+1,i]=1
            U[i,i+1]=1
            U[i+1,i+1]=0
            V.set_column(i,V.column(i)-U[i,i]*V.column(i+1))
            U.swap_columns(i,i+1)
            V.swap_columns(i,i+1)
            B.swap_columns(i,i+1)
            for k in range(i+2,m) :
                    U[i,k]=(B.column(k)*V.column(i))/ \
                            (V.column(i)*V.column(i))
                    U[i+1,k]=(B.column(k)*V.column(i+1))/ \
                            (V.column(i+1)*V.column(i+))
            if abs(U[i,i+1])>0.5 : reduce(i+1,B,U)
                    i=max(i-1,0)
    return B
```

2.4. Ο αλγόριθμος NTRU

Η ασφάλεια του κρυπτοσυστήματος δημοσίου κλειδιού NTRU έγγυται στην αδυναμία του LLL και οποιουδήποτε άλλου αλγορίθμου μεταβλητών, να παράγει ιδιαιτέρως καλά μικρά διανύσματα μέσα σε ένα λογικό διάστημα χρόνου. Ενώ ο LLL συχνά λειτουργεί καλύτερα στην πράξη, φαίνεται ότι ο εστιμώμενος χρόνος που τρέχει ο αλγόριθμος μεγαλώνει εκθετικά καθώς μεγαλώνει η διάσταση.[**6**]

Δημόσιες παράμετροι. Η επιλογή του N καθορίζει το πολυωνυμικό δακτύλιο $(Z)[X]/(X^N - 1)$. Δύο $moduli\ p$ και q επιλέγονται έτσι ώστε $gcd(p, q) = 1$. Επιπλέον δημόσιες παράμετροι είναι αριθμοί, τους οποίους θα ονομάσουμε d_f, d_g, , d_m και d_r. Αυτοί καθορίζουν το διάστημα των επιτρεπόμενων ιδιωτικών κλειδιών f και g, τα επιτραπτά μηνύματα και τη μορφή του τυχαίου πολυωνύμου r που χρησιμοποιείται στην κρυπτογράφηση.

Εδώ, το q μπορεί να είναι τυπικά μία δύναμη του 2 και το p πολύ μικρό. Ένα παράδειγμα είναι $(N, p, q) = (251, 3, 128)$.

Δημιουργία Κλειδιού. Επιλέγουμε τυχαία "μικρά" πολυώνυμα f και g, όπου το f έχει d_f μονάδες (1) και $d_f - 1$ αρνητικές μονάδες (-1) και τα υπόλοιπα μηδενικά. Το g θα είναι παρόμοιο, αλλά θα έχει το ίδιο πλήθος (d_g) από 1 και (-1). Από κατασκευής, $f(1) = 1$ αλλά επίσης, το πολυώνυμο f πρέπει να είναι αντιστρέψιμο στον $(Z)[X]/(X_N - 1)\ modulo\ p$ και q. Αυτό προκύπτει με μεγάλη πιθανότητα, ενώ αν αποτύχει ένα νέο τυχαίο πολυώνυμο f παράγεται. Υπολογίζουμε το αντίστροφο $f_q^{-1}\ mod\, q$ και το πολυώνυμο

$$h = f_q^{-1} g\ (mod\, q)$$

δημοσιεύεται.

Εδώ το h είναι το δημόσιο κλειδί ενώ τα f και g είναι και τα δύο ιδιωτικά.

Κρυπτογράφηση. Διαλέγουμε ένα τυχαίο πολυώνυμο r με d_r μονάδες (1) και $d_r - 1$ αρνητικές μονάδες (-1) και τα υπόλοιπα μηδενικά. Έστω ότι το m είναι το μήνυμα, με d_m μονάδες και αρνητικές μονάδες. Υπολογίζουμε το κρυπτογραφημένο μήνυμα

$$e = m + pr * h\ (mod\, q)$$

Αναγωγή mod q εδώ σημαίνει αναγωγή των συντελεστών στο διάστημα $(-q/2,\, q/2]$. (Αυτή είναι η φυσική επιλογή αφού αυτά τα πολυώνυμα έχουν συντελεστές κεντραρισμένους γύρω από το μηδέν.

Αποκρυπτογράφηση. Πολλαπλασιάζουμε το e με το ιδιωτικό κλειδί f και λαμβάνουμε το

$$f * e = f * m + pr * f * h \,(mod\, q) = f * m + pr * g \,(mod\, q)$$

όπου η τελευταία ισότητα χρησιμοποιεί τον ορισμό του h. Με την κατάλληλη επιλογή των παραμέτρων που καθορίζει το μέγεθος των ιδιωτικών κλειδιών, μηνύματα, και το πολυώνυμο r, καταλλήγουμε ότι οι συντελεστές του $f * m + pr * g$ φυσικά θα παρευρίσκονται στο διάστημα $(-q/2,\, q/2]$. Επομένως, έχοντας λάβει ακριβώς το $f*m+pr*g$, μπορούμε τώρα να μειώσουμε αυτό με το $mod\, p$ για να ανακτίσουμε το $f * m$, και το m ανακτάται αφού πολλαπλασιάσουμε με το αντίστροφο f_p^{-1} του $f \,mod\, p$. Σημειώνουμε ότι το m είναι ένα mod p πολυώνυμο και τότε το ανακτάμε ακριβώς.

Η βασική ιδέα πίσω από την αποκρυτογράφηση είναι η παρακάτω παρατήρηση για τον περίπλοκο πολλαπλασιασμό μικρών πολυωνύμων. Ένας συντελεστής, παράδειγμα του $f * m$, είναι το άθροισμα των γινομένων της μορφής $f_i m_j$, καθένα από τα οποία παίρνει τις τιμές 0, 1, και -1 με κάποια πιθανότητα. Ας σκεφτούμε έναν συντελεστή σαν μία τυχαία μεταβλητή και αναλογιζόμαστε την κατανομή που πιθανών να κατέχει. Ενώ είναι εύλογο να υποθέσουμε ότι αυτή η τυχαία μεταβλητή έχει κανονική κατανομή γύρω από το μηδέν, φαίνεται ότι η υπεργεωμετρική κατανομή (ίδιος μέσος, μικρότερη τυπική αποκλιση) είναι πιο ακριβής. Επομένως, οι συντελεστές των γινομένων των μικρών κεντραρισμένων γύρω από το μηδέν πολυωνύμων, όπως το $f * m$, παραμένουν πολύ σφιχτά ομαδοποιημένα γύρω από το μηδέν. (Φυσικά, το f δεν είναι ακριβώς κεντραρισμένο εδώ.) Κατ' επέκταση είναι εύκολο να καθορίσουμε (πειραματικά) επιλογές παραμέτρων για τις οποίες η αποκρυπτογράφηση συμβαίνει με συντριπτική πιθανότητα.[**6**]

Για παράδειγμα, για να δουλέψει η αποκρυπτογράφηση, είναι απαραίτητο να ισχύει ότι

$$||f * m + pr * g||_\infty < q$$

Έχει βρεθεί ότι αυτό θα είναι ουσιαστικά πάντα αληθές αν έχουμε διαλέξει παραμέτρους ώστε

$$||f * m||_\infty \leq q/4 \text{ και } ||pr * g||_\infty \leq q/4$$

Παρ'όλα αυτά, η επιλογή κάποιων παραμέτρων μπορεί να καταλήξει σε περιστασιακή αποτυχία αποκρυπτογράφησης, άρα σίγουρα κάποιος θα πρέπει να εισάγει κάποια σημεία ελέγχου σε κάθε μέρος του μηνύματος. Όταν η αποκρυπτογράφηση αποτυχαίνει, υπάρχουν 2 πιθανοί λόγοι. Αν δε βρίσκονται όλοι οι συντελεστές του $b = f * m + pr * g$ στο διάστημα $(-q/2,\, q/2]$ αλλά επίσης ικανοποιούν το $max b_i - min b_i \leq q$, τότε ένα λάθος "αναδίπλωσης" (wrap failure) έχει προκύψει. Αν η απόσταση ανάμεσα στο μέγιστο και το ελάχιστο είναι μεγαλύτερη από q, δηλαδή δεν είναι όλοι οι συντελεστές σωστά κεντραρισμένοι, τότε ένα λάθος "κενού" (gap failure) προκύπτει. Στην πραγματικότητα, μία συνετή επιλογή των παραμέτρων, κάνει τέτοια λάθη υπερβολικά απίθανο να συμβούν και μπορούν να αγνοηθούν στην πράξη.[**3**]

2.5. Παράδειγμα στον NTRU

2.5.1. Υπενθυμίσεις - Παραδείγματα στα modula και στους δακτυλίους

Διαίρεση με modulo και κρατάμε το υπόλοιπο:

Παράδειγμα 12. $147(\mod 17) =?$ *Επειδή* $147 = 8 * 17 + 11$ *έχουμε ότι* $147 = 11(\mod 17)$

Γενικά, $a = b(\mod m)$ σημαίνει ότι τα a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το m

Αν $a * b = 1(\mod m)$ τότε το b είναι το αντίστροφο του $a(\mod m)$

Παράδειγμα 13. *Το αντίστροφο του* $10(\mod 23)$ *είναι το 7 διότι* $7 * 10 = 1(\mod 23)$

Ο ευκλείδιος αλγόριθμος μπορεί να χρησιμοποιηθεί για να ελεγχθεί αν τα a και m έχουν κοινούς παράγοντες και να υπολογίσει το αντίστροφο του $a(\mod m)$ αν έχουν κοινούς παράγοντες.

Ένας δακτύλιος βαθμού $N - 1$ είναι ο

$$a = a_0 + a_1 X + a_2 X^2 + a_3 x^3 + \cdots + a_{N-2} X^{X-2} + a_{N-1} X^{N-1}$$

Γνωρίζουμε ότι $X^N = 1(\mod X^N - 1)$.

Επίπεδο ασφάλειας (σε bits)	N	q	p
128	439	2048	3
192	593	2048	3
256	743	2048	3

Πίνακας 1. Ασφάλεια του NTRU σύμφωνα με [**24**].

Επίπεδο ασφάλειας (σε bits)	NTRU	ECC	RSA
128	4829	256	3072
192	6523	384	7680
256	8173	521	15360

Πίνακας 2. Αντιστοιχία ασφάλειας αλγορίθμων δημοσίου κλειδιού σύμφωνα με [**25**].

Επίσης έχουμε ότι

$$a * b = c_0 + c_1X + c_2X^2 + \cdots + c_{N-2}X^{N-2} + c_{N-1}X^{N-1}$$

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 + a_{k+1}b_{N-1} + a_{k+2}b_{N-2} + \cdots + a_{N-1}b_{k+1}$$

$$c_k = \sum_{i=0}^{k} a_ib_{k-i} + \sum_{i=k+1}^{N-1} a_ib_{N+k-i} = \sum_{i+j\equiv k \mod N} a_ib_j$$

Αυτός είναι ένας δακτύλιος πολυωνύμων και είναι ισομορφικός με το δακτύλιο πηλίκο $Z[X]/(X^N - 1)$.

Το πολυώνυμο $a(\mod q)$ σημαίνει ότι μειώνουμε τους συντελεστές του a κατά $\mod q$ και αντίστοιχα $a = b(\mod q)$ σημαίνει ότι κάθε συντελεστής της διαφοράς $a - b$ είναι πολλαπλάσιο του q.

Το $a = a_0 + a_1X + a_2X^2 + a_3x^3 + \cdots + a_{N-2}X^{X-2} + a_{N-1}X^{N-1}$ μπορεί να γραφτεί ως μία λίστα από N αριθμούς ως εξής: $a = (a_0, a_1, a_2, \cdots, a_{N-2}, a_{N-1})$

Παράδειγμα 14. *Για $= 7$, το πολυώνυμο $a = 3 + 2X_2 - 3X^4 + X^6$ μπορεί να αποθηκευτεί και ως* $(3, 0, 2, 0, -3, 0, 1)$

Αντίστροφο modulo$q$ του πολυωνύμου a είναι ένα πολυώνυμο A με την ιδιότητα $a * A = 1(\mod q)$.

Δεν έχει κάθε πολυώνυμο αντίστροφο, αλλά είναι εύκολο να διευκρινιστεί αν το a έχει αντίστροφο και να βρεθεί αν υπάρχει.

Παράδειγμα 15. *Για $= 7$, $q = 11$ το πολυώνυμο $a = 3 + 2X^2 - 3X^4 + X^6$ έχει αντίστροφο modulo 11 και είναι το*
$A = -2 + 4X + 2X^2 + 4X^3 - 4X^4 + 2X^5 - 2X^6$ *διότι*

$$(3 + 2X^2 - 3X^4 + X^6) * (-2 + 4X + 2X^2 + 4X^3 - 4X^4 + 2X^5 - 2X^6)$$

$$= -10 + 22 + 22^3 - 22^6 = 1(\mod 11)$$

υπενθύμιση ότι είμαστε στο δακτύλιο όπου $N = 7$ και επομένως $X^7 = X^0$, $X^8 = X^1 = X$, $X^0 = X^2$ κοκ. Επίσης, είναι προφανές ότι $22 = 0 \mod 11$ *και* $-10 = 1 \mod 11$.

2.5.2. NTRU Public Key Cryptosystem Parameters

Ένας δακτύλιος R που αποτελείται από όλα τα πολυώνυμα βαθμού $N - 1$ με ακέραιους συντελεστές:

$$a = a_0 + a_1X + a_2X^2 + a_3x^3 + \cdots + a_{N-2}X^{X-2} + a_{N-1}X^{N-1}$$

όπου N είναι το πλήθος των πολυωνύμων στον δακτύλιο με βαθμό $N-1$, q ένας μεγάλος αριθμός με τον οποίο θα αναχθούν κατά $\mod q$ οι συντελεστές των πολυωνύμων, p ένας μικρός αριθμός με τον οποίο, στο τελευταίο βήμα της αποκρυπτογράφησης, θα αναχθούν οι συντελεστές του μηνύματος.

Θέτουμε σε αυτό το παράδειγμα ότι $N = 11$, $q = 32$, $p = 3$.[**13**]

Διαλέγουμε τυχαία δύο "μικρά" πολυώνυμα f και g και τα κρατάμε κρυφά.

Τυχαία σημαίνει ότι οι συντελεστές είναι τυχαία διανεμειμένοι στο p ή στο q, μικρά σημαίνει ότι οι συντελεστές πρέπει να είναι πολύ μικρότεροι από το p ή το q.

Υπολογίζουμε το αντίστροφο του $f \mod q$ και το αντίστροφο του $f \mod p$ ($f * f_q = 1 \mod q$ και $f * f_p = 1 \mod p$)

Το δημόσιο κλειδί είναι $h = pf_q * g \mod q$

Μία μέθοδος για να παράξουμε τα f και g είναι:

- Διαλέγουμε d_f το οποίο μας δείχνει πόσοι συντελεστές του f είναι ίσοι με +1, $d_f - 1$ είναι οι συντελεστές που είναι ίσοι με -1 και οι υπόλοιποι είναι 0.
- Διαλέγουμε d_g το οποίο δείχνει ότι ότι το πολυώνυμο g έχει d_g συντελεστές ίσους με +1, d_g συντελεστές ίσους με -1 και οι υπόλοιποι είναι 0.
- Ο λόγος για τον οποίο πρέπει τα f και g να είναι "μικρά" πολυώνυμα είναι ότι το f πρέπει να είναι αντιστρέψιμο, ενώ το g όχι.

Έστω $d_f = 4$, $d_g = 3$ και

$$f = -1 + X + X^2 - X^4 + X^6 + X^9 - X^{10}$$
$$g = -1 + X^2 + X^3 + X^5 - X^8 - X^{10}$$

Τότε

$$f_p = 1 + 2X + 2x^3 + 2X^4 + X^5 + 2X^7 + X^8 + 2X^9$$
$$f_q = 5 + 9X + 6X^2 + 16X^3 + 4X^4 + 15X^6 + 22X^7 + 20X^8 + 18X^9 + 30X^{10}$$

Και για $H = pf_q * g \mod q$, $q = 32$, $p = 3$ έχουμε

$$H = 8 + 25X + 22X^2 + 20X^3 + 12X^4 + 24X^5 + 15X^6 + 19X^7 + 12X^8 + 19X^9 + 16X^{10}$$

όπου για να υπολογίσουμε το H χρησιμοποιούμε τα Low Hamming Weight Polynomials[2]

Παράδειγμα 16.

$$(4,5,7) * (5,3,2) = 4 * (5,3,2) + 5 * (2,5,3) + 7 * (3,2,5) =$$
$$(20,12,8) + (10,25,15) + (21,14,35) =$$
$$(20 + 10 + 21, 12 + 25 + 14, 8 + 15 + 35) = (51,51,56)$$

Με τον ίδιο τρόπο βγαίνει το h και στη δική μας περίπτωση όπου

$$f_q = 5 + 9X + 6X^2 + 16X^3 + 4X^4 + 15X^6 + 22X^7 + 20X^8 + 18X^9 + 30X^{10}$$
$$g = -1 + X^2 + X^3 + X^5 - X^8 - X^{10}$$

και επομένως

$$(-1,0,1,1,0,1,0,0,-1,0,-1) * (5,9,6,16,4,15,16,22,20,18,30) =$$
$$(\underline{-5}, -9, -6, -16, -4, -15 - 16, -22, -20, -18, -30) +$$
$$(\underline{18}, 30, 5, 9, 6, 16, 4, 15, 16, 22, 20) +$$
$$(\underline{20}, 18, 30, 5, 9, 6, 16, 4, 15, 16, 22) +$$
$$(\underline{16}, 22, 20, 18, 30, 5, 9, 6, 116, 4, 15) +$$
$$(\underline{-16}, -4, -15, -16, -22, -20, -18, -30, -5, -9) +$$
$$(\underline{-9}, -6, -16, -4, 0, -115, -16, -22, -20, -18, -30, -5) =$$
$$(24, 51, \cdots)$$

διότι

$$-5 + 18 + 20 + 16 - 16 - 9 = 24 \text{ και } 24 * 3 = 72 \ \ 72 = 8 \mod 32$$

για τον πρώτο όρο του h και ομοίως και για τους υπόλοιπους.

[2]Reference: Hoffstein J. Silverman J., "Random Small Hamming Weight Products with Applications to Cryptography"

2.5.3. Κρυπτογράφηση

Έστω m το κείμενο σε μορφή πολυωνύμου όπου οι συντελεστές είναι μικροί mod q. Τυχαία διαλέγουμε ένα άλλο μικρό πολυώνυμο r. Τότε $e = r * h + m($ mod $q)$ όπου e είναι το κρυπτογραφημένο μήνυμα και h το δημόσιο κλειδί.

Το r έχει d_r συντελεστές ίσους με +1, $d_r - 1$ συντελεστές ίσους με -1 και όλους τους υπόλοιπους 0.

Για $d_r = 3$, έχουμε $r = -1+X^2+X^3+X^4-X^5-X^7$ και έστω $m = -1+x^3-X^4-X^8+X^9+X^10$ και $h = 8 + 25X + 22X^2 + 20X^3 + 12X^4 + 24X^5 + 15X^6 + 19X^7 + 12X^8 + 19X^9 + 16X^{10}$. Τότε

$$e = r * h + m \mod q =$$
$$(-1, 0, 1, 1, 1, -1, 0, -1, 0, 0, 0) * (8, 25, 22, 20, 12, 24, 15, 19, 12, 19, 16) +$$
$$+(-1, 0, 0, 1, -1, 0, 0, 0, -1, 1, 1)$$
$$= 14 + 11X + 26X^2 + 24X^3 + 14X^4 + 16X^5 + 30X^6 + 7X^7 + 25X^8 + 6X^9 + 19X^{10}$$

2.5.4. Αποκρυπτογράφηση

Έχουμε τα a, b και c για τα οποία ισχύει:

$a = f * e \mod q$ και πρέπει να επιλεχθούν συντελεστές μεταξύ του $-q/2$ και $q/2$ για παράδειγμα αν $q = 32$, οι συντελεστες πρέπει να είναι ανάμεσα στα $[-15, 16]$

$b = a \mod p$ και πρέπει να επιλεχθούν συντελεστές ανάμεσα στο $-p/2$ και $p/2$, άρα για $p = 3$ το εύρος θα είναι $[-1, 1]$

$c = f_p * b \mod p$ και πρέπει να επιλεχθούν συντελεστές ανάμεσα στο $-p/2$ και $p/2$

Παράδειγμα 17. *Για* $e = 14 + 11X + 26X^2 + 24X^3 + 14X^4 + 16X^5 + 30X^6 + 7X^7 + 25X^8 + 6X^9 + 19X^{10}$ *και* $f = -1 + X + X^2 - X^4 + X^6 + X^9 - X^{10}$ *έχουμε*

$$a = f * e \mod 32$$

όπου το $modulo32$ *αλλάζει τους συντελεστές στο διάστημα* $[-15, 16]$

$$a = 3 - 7X - 10X^2 - 11X^3 + 10X^4 + 7X^5 + 6X^6 + 7X^7 + 5X^8 - 3X^9 - 7X^{10}$$

που σημειώνεται και ως $(3, -7, -10, -11, 10, 7, 6, 7, 5, -3, -7)$

$$b = a \mod 3$$

όπου το $modulo3$ *αλλάζει τους συντελεστές στο διάστημα* $[-1, 1]$

$$b = -X - X^2 + X^3 + X^4 + X^5 + X^7 - X^8 - X^{10}(\mod 3)$$

και σημειώνεται ως $(0, -1, -1, 1, 1, 1, 0, 1, -1, 0, -1)$

Και επομένως επειδή $f_p = 1+2X+2X^3+2X^4+X^5+2X^7+X^8+2X^9$ *ή ως* $(1, 2, 0, 2, 2, 1, 0, 2, 1, 2, 0)$ *και* $b = -X - X^2 + X^3 + X^4 + X^5 + X^7 - X^8 - X^{10}$ *έχουμε*

$$c = f_p * b \mod p$$
$$(0, -1, -1, 1, 1, 1, 0, 1, -1, 0, -1) * (1, 2, 0, 2, 2, 1, 0, 2, 1, 2, 0) =$$
$$\cdots = (-2, 0, -2, -2, -1, 0, -2, -1, -2, 0, -1)$$

όπου το $modulo3$ *αλλάζει τους συντελεστές στο διάστημα* $[-1, 1]$*:*
$c = (-1, 0, 0, 1, -1, 0, 0, 0, -1, 1, 1)$ *το οποίο είναι ίσο με το μήνυμα* m *που είχαμε αρχικά.*

Συνοπτικά, δουλεύει

$$e = r * h + m(\mod q)(1)$$
$$h = pf_q * g(\mod q)(2)$$
$$f * f_q = 1(\mod q)(3)$$

Επομένως

$$a = f * e(\mod q) \overset{(1)}{=}$$
$$= f * (r * h + m)(\mod q) \overset{(2)}{=}$$
$$= f * (r * pf_q * g + m)(\mod q) \overset{(3)}{=}$$

$$= pr * g + f * m(\mod q)$$

Τα πολυώνυμα r, g, f, m *όλα έχουν συντελεστές που είναι σχετικά μικροί, ώστε οι συντελεστές των* $r*g$ *και* $f*m$ *είναι επίσης αρκετά μικροί, τουλάχιστον σε σχέση με το* q*. Αφού ο πρώτος* p *είναι επίσης μικρός σε σύγκριση με το* q*, αυτό σημαίνει ότι το πολυώνυμο* $pr * g + f * m$ *βρίσκεται ανάμεσα στο* $-q/2$ *και το* $q/2$*, επομένως το να μειώσουμε τους συντελεστές με* $modulo\, q$ *δεν έχει καμία συνέπεια.*

$$b = a = f * m(\mod p)$$

$$c = f_p * b \overset{f_p * f = 1(\mod p)}{=} m(\mod p)$$

2.6. Βασικά θέματα ασφάλειας

Υπάρχουν διαφορετικοί τύποι για θέματα ασφαλείας: στοιχειώδης (γιατί το N πρέπει να είναι πρώτος), κανονικές (meet–in–the–middle επιθέσεις), εξεζητημένες (lattice reduction attacks) και εκτελεστικές (διαλεγμένες επιθέσεις κρυπτογραφήματος, θέματα πλήρωσης και κατακερματισμού). [**6**]

Το δύσκολο πρόβλημα που υποβόσκει με τον NTRU είναι το CVP (closest vector problem) πρόβλημα σε κάποια πολύπλοκα πλέγματα σημείων. Το ζευγάρι των ιδιωτικών κλειδιών (f, g) θα είναι ένα ισότιμο μικρό διάνυσμα στο ακέραιο πλέγμα σημείων $\mathcal{L}_h$ που αναπαρισταται από τον πίνακα

$$\left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

ο οποίο εν συντομία θα είναι ο

$$M = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}$$

Αν k είναι το ακέραιο πολυώνυμο τέτοιο ώστε $f * h = g + qk$, τότε το διάνυσμα (f, k) είναι π γραμμικός συνδυασμός των γραμμών αυτού του πίνακα που παράγει το ιδιωτικό κλειδί (f, g). Τα παραπάνω $h-$διανύσματα έχουν συντελεστές που είναι ισότημα ομοιόμορφα κατανεμημένα σε ένα $q-$διάστημα. Ο πίνακας έχει διάσταση $2N$ και ορίζουσα q^N ενώ το δημόσιο κλειδί έχει μήκος $N \log q$. Η ικανότητα να διατηρήσουμε το μήκος του κλειδιού σχετικά μικρό συγκρινόμενο με τη διάσταση του πλέγματος σημείων στο οποίο το ιδιωτικό κλειδί είναι ένα μικρό διάνυσμα, διαχωρίζει τον NTRU από τα υπόλοιπα κρυπτοσυστήματα που στηρίζονται σε πλέγματα σημείων, όπως τα knapsack ή το GGH σύστημα.[**22**]

Επομένως το μήκος του κλειδιού είναι σε ένα πρακτικό μέγεθος, ενώ η διάσταση του πλέγματος σημείων είναι έξω από το εύρος των υπάρχοντων τεχνολογιών απλοποίησης πλέγματος σημείων. Στην πράξη, οι παράμετροι ενός NTRU σχήματος θα διαλεχθούν για να ισορροπήσουν ένα πλήθος από συναγωνιστικές σκέψεις: ελάττωση του σφάλματος αποκρυπτογράφησης, εξάλειψη της πιθανότητας των επιθέσεων εξαντλητικής αναζήτησης (brute force attacks), διατήρηση της ταχύτητας και της αποτελεσματικότητας, και την απαίτηση ενός ανέφικτα μεγάλου εκτιμώμενου χρόνου για τον LLL αλγόριθμο να επιστρέψει ένα μικρό διάνυσμα.

2.7. Επιθέσεις στον NTRU

2.7.1. Επιθέσεις εξαντλητικής αναζήτησης

Ένας επιτιθέμενος μπορεί να ανακτύσει το ιδιωτικό κλειδί αν προσπαθήσει όλα τα πιθανά $f \in \mathcal{L}_f$ και δοκιμάζοντας εάν το $f * h(\mod q)$ έχει μικρές καταχωρήσεις ή προσπαθώντας όλα

τα $g \in \mathcal{L}_g$ και δοκιμάζοντας εάν τα $g * h^{-1} (\mod q)$ έχει μικρές καταχωρήσεις. Ομοίως, ένας επιτιθέμενος μπορεί να ανακτύσει το μήνυμα δοκιμάζοντας όλα τα πιθανά $\phi \in \mathcal{L}_\phi$ και ελέγχοντας εάν $e - \phi * h (\mod q)$ έχει μικρές καταχωρήσεις (όπου $\phi = pr$)

Στη πράξη, $\mathcal{L}_g$ θα είναι μικρότερο από $\mathcal{L}_f$, επομένως η ασφάλεια του κλειδιού καθορίζεται από το $\#\mathcal{L}_g$, και η ασφάλεια του ανεξάρτητου μηνύματος καθορίζεται από $\#\mathcal{L}_\phi$.

Παρ' όλα αυτά, όπως περιγράφεται παρακάτω, υπάρχει η επίθεση "meet in the middle" η οποία (θεωρώντας ότι υπάρχει αρκετός χώρος μνήμης) μειώνει το χρόνο της αναζήτησης στην κλασική τετραγωνική ρίζα. Επομένως το επίπεδο ασφάλειας δίνεται από

$$\big(Key\ Security\big) = \sqrt{\#\mathcal{L}_g} = \frac{1}{d_g!}\sqrt{\frac{N!}{(N-2d_g)!}}$$

$$\big(Message\ Security\big) = \sqrt{\#\mathcal{L}_\phi} = \frac{1}{d!}\sqrt{\frac{N!}{(N-2d)!}}$$

2.7.2. Επιθέσεις Meet-in-the-middle

Υπενθυμίζουμε ότι το κρυπτογραφημένο μήνυμα είναι $e = \phi * h + m (\mod q)$. Ο Andrew Odlyzko έχει υποδείξει ότι υπάρχει μία meet–in–the–middle επίθεση η οποία μπορεί να χρησιμοποιηθεί εναντίον του ϕ και παρατηρούμε ότι μία παρόμοια επίθεση εφαρμόζεται επίσης και στο ιδιωτικό κλειδί f. Για να μπορέσουμε να διατηρήσουμε ένα επίπεδο ασφαλείας περίπου 2^{80} πρέπει κάποιος να διαλέξει d_f και d_g ώστε το διάστημα των επιτρεπόμενων ζευγαριών να περιέχει περίπου 2^{160} στοιχεία.

2.7.3. Επιθέσεις πολλαπλής αποστολής

Αν ένας επιτιθέμενος στείλει το ίδιο μήνυμα m πολλαπλές φορές χρησιμοποιώντας το ίδιο δημόσιο κλειδί αλλά χρησιμοποιώντας διαφορετικά τυχαία ϕ, τότε ο επιτιθέμενος θα μπορέσει να ανακτύσει ένα μεγάλο μέρος του μηνύματος. Συνοπτικά, αν υποθέσουμε ότι ο επιτιθέμενος μεταδώσει $e_i = \phi_i * h + m (\mod q)$ για $i = 1, 2, \cdots, r$, τότε ο επιτιθέμενος θα μπορέσει να υπολογίσει το $(e_i - e_1) * h^{-1} (\mod q)$ και κατ' αυτόν τον τρόπο να ανακτύσει το $\phi_i - \phi_1 (\mod q)$. Ωστόσο, οι συντελεστές των ϕ είναι τόσο μικροί ώστε θα καταφέρει να ανακτύσει ακριβώς το $\phi_i - \phi_1$ και από αυτό θα ανακτύσει πολλούς από τους συντελεστές του ϕ_1. Εάν το r έχει ένα μέτριο μέγεθος, τότε ο επιτιθέμενος θα ανακτύσει αρκετούς συντελεστές από το ϕ_1 ώστε να είναι σε θέση να ελέγξει όλες τς πιθανότητες για τους υπολειπόμενους συντελεστές με "ωμή βία" (brute force) και κατ' επέκταση να ανακτύσει το μήνυμα m.

Επομένως, πολλαπλές μεταδόσεις δεν συννίστανται χωρίς περεταίρω κωδικοποιήσεις του υποκείμενου μηνύματος. Είναι μία επισήμανση αυτό ότι ακόμα κι αν ο επιτιθέμενος κατεφέρει να αποκρυπτογραφήσει το μήνυμα κατ' αυτόν τον τρόπο, αυτή η πληροφορία δε θα τον βοηθήσει να αποκρυπτογραφήσει το πραγματικό μήνυμα.

2.7.4. Επιθέσεις με πλέγματα σημείων

Υπενθύμιση: Ο σκοπός της αναγωγής των πλεγμάτων σημείων είναι να βρεθεί ένα ή περισσότερα "μικρά" διανύσματα για ένα συγκεκριμένο πλέγμα σημείων. Στη θεωρία, το μικρότερο διάνυσμα μπορεί να βρεθεί με μία εκτενή έρευνα, αλλά στην πρακτική αυτό είναι αδύνατο αν η διάσταση είναι μεγάλη. Ο LLL αλγόριθμος, με πολλές βελτιώσεις από τον Schnorr και άλλους, θα βρει σχετικά μικρά διανύσματα σε πολυωνυμικό χρόνο, αλλά ακόμα και αυτός ο αλγόριθμος θα πάρει πολύ χρόνο για να βρει το μικρότερο διάνυσμα.

Επίθεση πλέγματος σημείων σε ιδιωτικό κλειδί του NTRU

Θεωρούμε έναν $2N \times 2N$ πίνακα που αποτελείται από 4 $N \times N$ blocks:

$$\left(\begin{array}{cccc|cccc} a & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & a & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

Διαλέγουμε το a ως εξής:

Έστω $\mathcal{L}$ το πλέγμα σημείων που παράγεται από τις γραμμές του παραπάνω πίνακα. Η ορίζουσα του $\mathcal{L}$ είναι $q^N a^N$.

Αφού το δημόσιο κλειδί είναι $h = g * f_q^{-1} \mod q$, το πλέγμα σημείων $\mathcal{L}$ θα περιέχει το διάνυσμα $\tau = (af, g)$, το οποίο σημαίνει ότι το διάνυσμα θα αποτελείται από N συντελεστές του f πολλαπλασιασμένοι με το a, ακολουθούμενους από N συντελεστές του g. Το αναμενόμενο μέγεθος του μικρότερου διανύσματος σε ένα τυχαίο πλέγμα σημείων διάστασης n και ορίζουσας D βρίσκεται ανάμεσα στα

$$D^{1/n}\sqrt{\frac{n}{2\pi e}} \text{ και } D^{1/n}\sqrt{\frac{n}{\pi e}}$$

Σε αυτήν την περίπτωση, $n = 2N$ και $D = q^N a^N$ επομένως το αναμενόμενο μικρότερο μήκος είναι μεγαλύτερο (αν και όχι πολύ μεγαλύτερο) από

$$s = \sqrt{\frac{Naq}{\pi e}}$$

Μία εφαρμογή του αλγορίθμου αναγωγής πλέγματος σημείων θα έχει καλύτερες πιθανότητες να εντοπίσει το τ, ή κάποιο άλλο διάνυσμα που το μήκος του είναι κοντά στο τ, εάν ο επιτιθέμενος διαλέξει a να μεγιστοποιεί το λόγο $s/||\tau||_2$. Τετραγωνίζοντας αυτό το λόγο, φαίνεται ότι ο επιτιθέμενος πρέπει να διαλέξει a τέτοιο ώστε να μεγιστοποιεί

$$\frac{a}{a^2||f||_2^2 + ||g||_2^2} = (a||f||_2^2 + a^{-1}||g||_2^2)^{-1}$$

Αυτό γίνεται διαλέγοντας $a = ||g||_2/||f||_2$.

Όταν το a διαλέγεται με αυτόν τον τρόπο, καθορίζουμε μία σταθερά c_h θέτοντας $||\tau||_2 = c_h s$. Συνεπώς c_h είναι ο λόγος του μήκους του διανύσματος που έχουμε ως στόχο προς το μήκος του αναμενόμενου μικρότερου διανύσματος. Όσο μικρότερη η τιμή του c_h, τόσο πιο εύκολο θα είναι να βρεθεί το στοχευμένο διάνυσμα. Αντικαθιστώντας παραπάνω, καταλήγουμε

$$c_h = \sqrt{\frac{2\pi e||f||_2||g||_2}{Nq}}$$

Για δεδομένο ζευγάρι (f, g) που χρησιμοποιείται για να στηθεί το κρυπτοσύστημα, το c_h μπορεί να θεωρηθεί ως ένα μέτρο του πόσο κοντά το συσχετισμένο πλέγμα σημείων παρεκλίνει από ένα τυχαίο πλέγμα σημείων. Εάν το c_h είναι κοντά στο 1, τότε το $\mathcal{L}$ θα μοιάζει με τυχαίο πλέγμα σημείων και οι μέθοδοι αναγωγής πλέγματος σημείων θα είναι πολύ δύσκολο να βρουν το μικρότερο διάνυσμα γενικά, και ιδιαίτερα η εύρεση του τ. Όσο το c_h μειώνεται, οι αλγόριθμοι αναγωγής πλέγματος σημείων θα είναι πιο εύκολο να βρουν το τ.

Επίθεση Πλέγματος σημείων σε ένα μήνυμα

Μία επίθεση πλέγματος σημείων μπορεί να κατευθυνθεί εναντίον του μηνύματος m. Εδώ, το συσχετισμένο πρόβλημα πλέγματος σημείων είναι πολύ κοντά σε αυτό με το h και το διάνυσμα που είναι στόχος θα έχει τη μορφή (am, ϕ). Όπως και πριν, ο επιτιθέμενος θα πρέπει να εξισορροπήσει το πλέγμα σημείων χρησιμοποιώντας $a = ||\phi||_2/||m||_2$, που οδηγεί στην τιμή

$$c_m = \sqrt{\frac{2\pi e||m||_2||\phi||_2}{Nq}}$$

Αυτή η σταθερά c_m δίνει το μέγεθος της ευαισθησίας του ανεξάρτητου μηνύματος σε μία επίθεση πλέγματος σημείων, όμοια με το c_h σε μία επίθεση πλέγματος σημείων στο h. Ένα κρυπτογραφημένο μήνυμα είναι πιο ευαίσθητο αν το c_m είναι μικρό και γίνεται λιγότερο όσο το c_m πλησιάζει το 1.

Για να γίνουν οι επιθέσεις στο h και στο m εξίσου δύσκολες, θέλουμε να πάρουμε $c_m \approx c_h$ ή ισοδύναμα $||f||_2||g||_2 \approx ||m||_2||\phi||_2$. Έστω ότι $p = 3$ (οι υπόλοιπες τιμές μπορούν να αναλυθούν με τον ίδιο τρόπο).Για αυτό το p, το μέσο μήνυμα m θα αποτελείται από $N/3$ 1,0 και -1, ώστε $||m||_2 \approx \sqrt{2N/3}$. Ομοίως, το ϕ θα αποτελείται από d 1 και -1 και τα υπόλοιπα είναι 0, ώστε $||\phi||_2 = \sqrt{2d}$, διότι, θέλουμε να εφαρμόσουμε $||f||_2||g||_2 \approx \sqrt{4Nd/3}$

Επίθεση πλέγματος σημείων σε ένα ψεύτικο κλειδί

Αντί να προσπαθούμε να βρούμε το ιδιωτικό κλειδί f, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τα πλέγματα σημείων όπως περιγράφονται παραπάνω και να προσπαθήσει να βρει ένα άλλο μικρό διάνυσμα στο πλέγμα σημείων, έστω της μορφής $\tau' = (af', g')$. Αν αυτό το διάνυσμα είναι αρκετά μικρό, τότε f' θα λειτουργήσει ως κλειδί αποκρυπτογράφησης. Πιο συγκεκριμένα, εάν καταλήξει με μεγάλη πιθανότητα ότι

$$f' * e \equiv p\phi * g' + m * f'(\mod q)$$

ικανοποιεί την

$$||p\phi * g' + m * f'||_\infty < q$$

τότε η αποκρυπτογράφηση θα πετύχει. Και ακόμα και εάν αυτό το μέγεθος είναι $2q$ ή $3q$ είναι πιθανό το μήνυμα να ανακτηθεί μέσω τεχνικές διόρθωσης λαθών, ιδιαίτερα εάν αρκετά τέτοια τ' μπορούν να βρεθούν. Παρ' όλα αυτά, πειραματικές αποδείξεις υποδεικνύουν ότι η ύπαρξη ψεύτικων κλειδιών δεν αποτελεί απειλή ασφαλείας.

2.8. Πρακτικές εφαρμογές του $NTRU$

2.8.1. Συγκεκριμένες επιλογές παραμέτρων

Θα παρουσιάσουμε τρία ξένα σύνολα παραμέτρων που καταλήγουν σε διαφορετικά επίπεδα ασφάλειας. Οι νόρμες του f και του g έχουν διαλεχθεί με τέτοιο τρόπο ώστε η αποτυχία της αποκρυπτογράφησης να προκύπτει με πιθανότητα μικρότερη της $5 \cdot 10^{-5}$ (βάση εκτεταμένων υπολογιστικών πειραμάτων)

Περίπτωση Α: Μία Μεσσαία Ασφάλεια

Μία μεσσαία ασφάλεια είναι κατάλληλη για καταστάσεις όπου η εγγενής τιμή του ανεξάρτητου μηνύματος είναι μικρή, και όπου τα κλειδιά θα αλλάζουν με σχετική συχνότητα. Παραδείγματα μπορεί να περιλαμβάνει κρυπτογράφηση της τηλεόρασης, των pagers και των μεταδόσεων των κινητών τηλεφώνων.

Όταν έχουμε $(N, p, q) = (107, 3, 64)$ τότε

$$\mathcal{L}_f = \mathcal{L}(15, 14)\ \mathcal{L}_g = \mathcal{L}(12, 12)\ \mathcal{L}_\phi = \mathcal{L}(5, 5)$$

όπως για παράδειγμα όταν $d = 5$.

Με άλλα λόγια, το f διαλέγεται με 15 συντελεστές να είναι ίσοι με +1 και 14 ίσοι με -1, το g διαλέγεται με 12 συντελεστες ίσοι με +1 και 12 ίσοι με -1 και το ϕ με 5 συντελεστές ίσοι με +1 και 5 ίσοι με -1. Αυτά δίνουν κλειδιά μεγέθους:

$$Private\,Key = 340\,bits \text{ και } Public\,Key = 642\,bits$$

και τα επίπεδα ασφαλείας (meet–in–the–middle):

$$Key\,Security = 2^{50} \text{ και } Message\,Security = 2^{26.5}$$

Σημειώνουμε ότι οι meet–in–the–middle επιθέσεις, χρειάζονται μεγάλους αποθηκευτικούς χώρους στους υπολογιστές, για ευθεία αναζήτηση με brute force επίθεση, αυτά τα επίπεδα ασφάλειας θα πρέπει να τετραφωνιστούν. Υποκαθιστώντας τις παραπάνω τιμές με τις κατάλληλες φόρμουλες δίνουν τις παρακάτω τιμές για τα πλέγματα σημείων

$$c_h = 0.257,\ c_m = 0.258, \text{ και } s = 0.422q$$

Περίπτωση Β: Υψηλή Ασφάλεια

Όταν έχουμε $(N, p, q) = (167, 3, 128)$ τότε

$$\mathcal{L}_f = \mathcal{L}(61, 60)\ \mathcal{L}_g = \mathcal{L}(20, 20)\ \mathcal{L}_\phi = \mathcal{L}(18, 18)$$

όπως για παράδειγμα όταν $d = 18$.

Αυτά δίνουν κλειδιά μεγέθους:

$$Private\,Key = 530\,bits \text{ και } Public\,Key = 1169\,bits$$

και τα επίπεδα ασφαλείας:

$$Key\,Security = 2^{82.9} \text{ και } Message\,Security = 2^{77.5}$$

Ενώ για τα πλέγματα σημείων έχουμε:

$$c_h = 0.236,\ c_m = 0.225,\ \text{και } s = 0.296q$$

Περίπτωση Γ: Υψηλότερη Ασφάλεια

Όταν έχουμε $(N, p, q) = (503, 3, 256)$ τότε

$$\mathcal{L}_f = \mathcal{L}(216, 215)\ \mathcal{L}_g = \mathcal{L}(72, 72)\ \mathcal{L}_\phi = \mathcal{L}(55, 55)$$

όπως για παράδειγμα όταν $d = 55$.

Αυτά δίνουν κλειδιά μεγέθους:

$$Private\,Key = 1595\,bits \text{ και } Public\,Key = 4024\,bits$$

και τα επίπεδα ασφαλείας:

$$Key\,Security = 2^{285} \text{ και } Message\,Security = 2^{170}$$

Ενώ για τα πλέγματα σημείων έχουμε:

$$c_h = 0.182,\ c_m = 0.160,\ \text{και } s = 0.0365q$$

2.9. Σύγκριση με άλλα Κρυπτοσυστήματα Δημοσίου Κλειδιού

Αυτή τη στιγμή υπάρχουν διάφορα κρυπτοσυστήματα δημοσίου κλειδιού, κάποια εκ των οποίων είναι ο RSA ο οποίος στηρίζεται στη δυσκολία της παραγοντοποίησης, ο McEliece που στηρίζεται σε κώδικες διόρθωσης λαθών και ο GGH (Goldreich, Goldwassser και Haveli)[**22**] που στηρίζεται στη δυσκολία να βρεθεί μικρή σχεδόν ορθογωνοποιημένη βάση ενός πλέγματος σημείων.

Ο NTRU έχει κάποια κοινά χαρακτηριστικά με το σύστημα McEliece, ένα από αυτά είναι ότι ο πολλαπλασιασμός * στο δακτύλιο R μπορεί να σχηματιστεί ως πολλαπλασιασμός πινάκων (ενός συγκεκριμένου είδους) και η κρυπτογράφηση και στα δύο συστήματα μπορεί να γραφτεί ως πολλαπλασιασμός πινάκων $E = AX + Y$, όπου A είναι το δημόσιο κλειδί. Μία μικρή διαφορά ανάμεσα στα δύο συστήματα είναι ότι στην κρυπτογράφηση με τον NTRU, το Y είναι το μήνυμα και X είναι ένας τυχαίος παράγοντας, ενώ στο σύστημα McEliece το ακριβώς αντίθετο. Αλλά η βασική διαφορά είναι ο τρόπος που γίνεται η αποκρυπτογράφηση. Στο σύστημα McEliece, ο πίνακας A σχετίζεται με κώδικα διόρθωσης λαθών (Goppa) και η αποκρυπτογράφηση πετυχαίνει επειδή η τυχαία συνεισφορά είναι αρκετά μικρή για να διορθωθεί από τον κώδικα Goppa. Για τον NTRU, ο πίνακας A είναι ένας κυκλικός πίνακας, και η αποκρυπτογράφηση στηρίζεται στην παραγοντοποίηση του A σε γινόμενο δύο πινάκων με συγκεκριμένη μορφή, σε συνδυασμό με άρση από το mod q στο mod p. [**3**]

3. Ομομορφική Κρυπτογραφία

3.1. Το Πρόβλημα

Ας θεωρήσουμε ότι αντιμετωπίζουμε την εξής κατάσταση. Έχουμε μία τεράστια ποσότητα από ηλεκτρονικά δεδομένα και επίσης έναν προσωπικό υπολογιστή με πολύ μικρότερη χωρητικότητα από ότι το μέγεθος των δεδομένων μας. Ας υποθέσουμε ακόμα, ότι υπάρχει ένας server στον οποίο εμείς, μεταξύ άλλων, μπορούμε να συνδεθούμε. Αυτός ο server μπορεί να αποθηκεύσει προσωπικά δεδομένα και να μας επιστρέψει ανά πάσα στιγμή όποιο μέρος των δεδομένων χρειαζόμαστε. Αποφασίζουμε να στείλουμε εκεί τα δεδομένα μας αλλά δεν εμπιστευόμαστε τον server και αποφασίζουμε να τα κρυπτογραφήσουμε ώστε να είναι ανέφικτο σε έναν αντίπαλο να διαβάσει κάτι από αυτά. Μετά, αφού ο server έχει τα κρυπτογραφημένα μας δεδομένα, χρειαζόμαστε να μας επιστρέχει ένα μέρος από αυτά. Και εδώ είναι το δίλημμα. Πως μπορεί να επιτευχθεί αυτό; Η πρώτη επιλογή είναι, ο server να μας στέλνει πίσω τα δεδομένα σε πακέτα, εμείς τα αποκρυπτογραφούμε ένα προς ένα και κρατάμε όσα χρειαζόμαστε. Μία άλλη επιλογή είναι να εμπιστευτούμε το server και να δώσουμε το ιδιωτικό μας κλειδί για την κρυπτογράφηση έτσι ώστε να αποφύγουμε να χάσουμε πολύτιμο χρόνο και μνήμη.

Καμία από τις δύο λύσεις δεν είναι πειστική αφού ούτε θέλουμε να χάσουμε τόσο χρόνο για να κατεβάζουμε τα δεδομένα που χρειαζόμαστε, ούτε θέλουμε ένας άγνωστος server να χειριστεί τα δεδομένα μας δίνοντάς του το ιδιωτικό κλειδί.

Τι θα γινόταν αν κάποιος μπορούσε να κάνει ερωτήσεις (queries) πάνω στα κρυπτογραφημένα δεδομένα που έχει ο server και να πάρει πίσω μόνο τα κρυπτογραφημένα δεδομένα που χρειάζεται; Αυτή είναι και η κεντρική ιδέα πίσω από την ομομορφική κρυπτογραφία. Το παραπάνω ερώτημα πρώτα προέκυψε μετά την δημοσιοποίηση του κρυπτοσυστήματος RSA που είναι ένα πολλαπλασιαστικό ομομορφικό σύστημα. Για την κρυπτογραφία, το παραπάνω ήταν ένα από τα πιο μπερδεμένα ζητήματα αφού το πρόβλημα να κατασκευαστεί ή ακόμα και να αποδειχθεί η ύπαρξη ενός τέτοιου συστήματος ήταν σε εκκρεμότητα για πάνω από 30 χρόνια. Αλλά το 2009 ο Graig Gentry κατασκεύασε ένα πλήρως ομομορφικό σύστημα. [**16**] Αμέσως μετά την πρώτη αυτή κατασκευή, που χρησιμοποιεί τα πλέγματα σημείων ως μαθηματικές δομές, έγινε απλούστευση του πρώτου συστήματος χρησιμοποιώντας μόνο ακεραίους.[**17**]

3.2. Ορισμός και Ιδιότητες

Ας θεωρήσουμε ένα κρυπτοσύστημα δημοσίου κλειδιού $\mathcal{E}$ που αποτελείται από τέσσερις αλγορίθμους: $KeyGen_{\mathcal{E}}$, $Encrypt_{\mathcal{E}}$, $Decrypt_{\mathcal{E}}$, $Evaluate_{\mathcal{E}}$.

- Ο αλγόριθμος $KeyGen_{\mathcal{E}}$ παίρνει μία παράμετρο ως μεταβλητή, που καλείται παράμετρος ασφαλείας του συστήματος και υποδηλώνεται με το λ. Αυτός ο αλγόριθμος παράγει ένα ζευγάρι (sk, pk) που είναι το ιδιωτικό και το δημόσιο κλειδί αντίστοιχα. Βασιζόμενοι στο pk καθορίζουμε το χώρο των απλών κειμένων $\mathcal{P}$ και το χώρο των κρυπτογραφημένων κειμένων $\mathcal{C}$ για το σύστημα $\mathcal{E}$
- Ο δεύτερος αλγόριθμος, πρώτ' απ' όλα παραμετροποιείται από το δημόσιο κλειδί του $\mathcal{E}$, η εισοδός του είναι το απλό κείμενο $\pi \in \mathcal{P}$ και η έξοδος το σχετικό κρυπτογραφημένο κείμενο $\psi \in \mathcal{C}$
- Ο αλγόριθμος $Decrypt_{\mathcal{E}}$ παραμετροποιείται από το ιδιωτικό κλειδί του $\mathcal{E}$, παίρνει το κρυπτογράφημα ψ και παράγει το αντίστοιχα απλό κείμενο π
- Τέλος, κάθε ομομορφικό κρυπτογραφικό σύστημα πρέπει να είναι εφοδιασμένο με έναν ακόμη αλγόριθμο το οποίο θα παραμετροποιηθεί από το δημόσιο κλειδί του συστήματος . Η είσοδός του είναι ένα κύκλωμα $C \in \mathcal{C}_{\mathcal{E}}$ - όπου με $\mathcal{C}_{\mathcal{E}}$ συμβολίζουμε ένα σύνολο από κυκλώματα για τα οποία το $\mathcal{E}$ είναι ομομορφικός, και μία πλειάδα από κρυπτογραφήματα $\Psi =< \psi_1, \psi_2, \cdots, \psi_t >$ όου κάθε στοιχείο του Ψ είναι μία είσοδος στο ανάλογο νήμα του κυκλώματος. Αυτό που ζητείται από τον $Evaluate_{\mathcal{E}}$, είναι, εάν $Encrypt_{\mathcal{E}}(pk, \pi_i) = \psi_i$ για $1 \leq i \leq t$ και $C(\pi_1, \pi_2, \cdots, \pi_t) = w$, τότε εάν $Encrypt_{\mathcal{E}}(pk, X, \Psi) = c$ τότε $Decrypt_{\mathcal{E}}(sk, c) = w$

Παρατηρείται ότι ένα ομομορφικό σύστημα είναι ακριβώς όπως ένα κλασικό σύστημα δημοσίου κλειδιού με έναν παραπάνω αλγόριθμο. Οι απαραίτητες προϋποθέσεις του $Evaluate_{\mathcal{E}}$ είναι

να μπορεί να υπολογιστεί χωρίς το ιδιωτικό κλειδί, το μόνο που χρειαζόμαστε με κάποιο τρόπο, είναι να μας επιστρέψει τα κρυπτογραφημένα δεδομένα που ζητήσαμε.

Για να κατανοήσουμε καλύτερα τον τρόπο λειτουργίας των διαφόρων σχημάτων ομομορφικής κρυπτογραφίας, πρέπει να αλλάξουμε λίγο την οπτική που έχουμε για τα διάφορα κρυπτοσυστήματα, χρησιμοποιώντας έννοιες από τη Θεωρία Πληροφορίας.

Συγκεκριμένα, μπορούμε να φανταστούμε τη διαδικασία κρυπτογράφησης ως την προσθήκη θορύβου στο αρχικό μήνυμα. Ο θόρυβος αυτός είναι "ελεγχόμενος" και μπορεί να διορθωθεί με την αποκρυπτογράφηση (από τον κάτοχο του αντίστοιχου κλειδιού) με τρόπο ανάλογο με έναν κώδικα διόρθωσης λαθών. Αν βέβαια ο θόρυβος μεγαλώσει, τότε κανένας δε μπορεί να προχωρήσει στην απικρυπτογράφηση. Το πρόβλημα στην ομομορφική κρυπτογραφία, είναι ότι η αποτίμηση διαφόρων συναρτήσεων πάνω στα κρυπτοκείμενα αυξάνει το θόρυβο. Έτσι υπάρχει ένα όριο στο πλήθος των συναρτήσεων που μπορούμε να αποτιμήσουμε ή στο βάθος του κυκλώματος που τις αναπαριστά, καθιστώντας μερικών και όχι πλήρως ομομορφικό ένα τέτοιο κρυπτοσύστημα.

Η λύση που έδωσε ο Gentry στο πρόβλημα αυτό βασίζεται στην παρατήρηση πως και η ίδια η αποκρυπτογράφηση είναι μία υπολογίσιμη συνάρτηση. [**20**]

Κάποιες ιδιότητες που πρέπει το ομομορφικό σύστημα να έχει είναι οι παρακάτω:

Ορισμός 28. *(Ορθότητα του ομομορφικού συστήματος κρυπτογράφησης)*
Λέμε ότι το $\mathcal{E}$ είναι ορθό για κυκλώματα στο $C \in \mathcal{C}_{\mathcal{E}}$ εάν:

$$Encrypt_{\mathcal{E}}(pk, \pi_i) = \psi_i, \textit{ gia } 1 \leq i \leq t \textit{ και } C(\pi_1, \pi_2, \cdots, \pi_t) = w$$

συνεπάγεται

$$\textit{εάν } Evaluate_{\mathcal{E}}(pk, C, \Psi) = c \Rightarrow Decrypt_{\mathcal{E}}(sk, c) = w$$

Ορισμός 29. *(Συμπάγεια για ομομορφικό σύστημα κρυπτογραφίας)*
Καλούμε το κρυπτοσύστημα $\mathcal{E}$ συμπαγές εάν υπάρχει πολυώνυμο f ώστε το μέγεθος του κυκλώματος κρυπτογράφησης $D_{\mathcal{E}}$ παραμένει μικρότερο από το $f(\lambda)$ για κάθε τιμή της παραμέτρου ασφαλείας λ

Λέμε ότι το ομομορφικό σύστημα κρυπτογράφησης συμπαγώς αξιολογεί κυκλώματα στο $\mathcal{C}_{\mathcal{E}}$ εάν είναι συμπαγής και επίσης ορθό για τα κυκλώματα στο $\mathcal{C}_{\mathcal{E}}$.

Οι δύο παραπάνω ορισμοί μας παρέχουν μία αίσθηση του προβλήματος που πρέπει να λυθεί. Η πρώτη απαραίτητη προϋπόθεση (ορθότητα) αναμένεται πλήρως αφού ζητάει την προφανή ιδιότητα του σωστού υπολογισμού στα κρυπτογραφημένα δεδομένα έτσι ώστε η αποκρυπτογράφηση να προχωρήσει με το επιθυμητό αποτέλεσμα. Η δεύτερη απαραίτητη προϋπόθεση μπορεί να μην είναι εμφανής στην αρχή, αλλά επειδή δε χρειαζόμαστε ένα σύστημα το οποίο να στέλνει όλα τα δεδομένα πίσω για αποκρυπτογράφηση και μετά να εφαρμόζει το κύκλωμα σε αυτά, διότι βασικά αυτό είναι που θέλουμε να αποφύγουμε, αυτό γίνεται με τη συμπάγεια. Έτσι αποκλύουμε την προφανή λύση $Evaluate_{\mathcal{E}}(pk, C, \Psi) = (C, \Psi)$.

Συμβολίζουμε με $\mathcal{E}^i$ το κρυπτοσύστημα $\mathcal{E}$ ένα κρυπτοσύστημα που ορθώς εκτιμά κυκλώματα σε βάθος το πολύ για $i, i \in \mathbb{Z}$

Ορισμός 30. *(Μερικώς ομομορφική κρυπτογραφία)*
Έστω $\{\mathcal{E}^{(d)} : d \in \mathbb{N}\}$ μία οικογένεια από ομομορφικά συστήματα κρυπτογραφίας. Λέμε ότι το $\mathcal{E}^{(d)}$ είναι μερικώς ομομορφική αν για κάθε $d \in \mathbb{N}$ κάθε πιθανή αποκρυπτογράφηση υπολογίζεται από το ίδιο κύκλωμα αποκρυπτογράφησης και επίσης $\mathcal{E}^{(d)}$ συμπαγώς υπολογίζει κάθε κύκλωμα σε βάθος το πολύ d, και επιπλέον η πολυπλοκότητα του κάθε αλγορίθμου που περιέχει το $\mathcal{E}^{(d)}$ είναι πολυώνυμο σύμφωνα με τα λ, d και το μέγεθος του κυκλώματος C.

Ορισμός 31. *(Πλήρως ομομορφικό κρυπτογραφικό σύστημα)*
Καλούμε ένα σύστημα $\mathcal{E}$ πλήρως ομομορφικό αν συμπαγώς υπολογίζει κάθε δυνατό κύκλωμα.

Μέρος 3

Επίλογος

ΚΕΦΑΛΑΙΟ 3

Επίλογος

1. Εφαρμογές της Ομομορφικής Κρυπτογραφίας

Αρκετά κρυπτοσυστήματα έχουν τη δυνατότητα να επιτρέπουν σε ένα (περιορισμένο) σύνολο λειτουργιών πάνω σε κρυπτοκείμενα χωρίς βέβαια πρόσβαση στο κλειδί αποκρυπτογράφησης. Κάτι τέτοιο έγινε αντιληπτό από την αρχή των κρυπτοσυστημάτων δημοσίου κλειδιού, ίσως με την παρατήρηση ότι το RSA είναι πολλαπλασιαστικά ομομορφικό.[**18**] Το συγκεκριμένο είδος ομομορφικής κρυπτογραφίας έχει αρκετούς περιορισμούς καθώς τα διάφορα ”παραδοσιακά” κρυπτοσυστήματα επιτρέπουν ένα μόνο είδος επεξεργασίας πάνω στα κρυπτογραφημένα δεδομένα (πρόσθεση ή πολλαπλασιασμός).[**12**]

Η δυνατότητα πραγματοποίησης οποιουδήποτε υπολογισμού πάνω σε κρυπτογραφημένα δεδομένα είναι φυσικό να έχει πληθώρα εφαρμογών. Οι Rivest, Adleman και Dertouzos[**18**] πρότειναν την υλοποίηση αναζήτησης πάνω σε κρυπτογραφημένα δεδομένα τα οποία είναι αποθηκευμενα σε ένα server. Ο χρήστης κωδικοποιεί το ερώτημα αναζήτησης με τέτοιο τρόπο ώστε όταν ο εξυπηρετητής το αποτιμήσει, θα λάβει ως απάντηση ένα κρυπτογραφημένο αποτέλεσμα.

Τέτοιες εφαρμογές έχουν τεράστια σημασία στη σύγχρονη εποχή με τη δυνατότητα υπολογισμού στο νέφος (cloud computing), όπου διάφοροι πάροχοι υπηρεσιών έχουν συγκεντρώσει τεράστια υπολογιστική ισχύ (επεξεργαστική ή αποθηκευτική), την οποία νοικιάζουν στους διάφορους χρήστες. Τυπικά τα διάφορα δεδομένα διατηρούνται κρυπτογραφημένα, αποκρυπτογραοφύνται όμως όταν οι χρήστες θέλουν να τα επεξεργαστούν. Αυτό θέτει τεράστια προβλήματα ιδιωτικότητα, καθώς ο πάροχος μπορεί να είναι κακόβουλος ή να χρειαστεί να παρέχει τα διάφορα δεδομένα σε κυβερνητικούς φορείς. Αυτό που θα θέλαμε ιδανικά, θα ήταν να εκμεταλλευτούμε την υπολογιστική ισχύ του νέφους, χωρίς όμως να θυσιάσουμε την ιδιωτικότητα των δεδομένων μας. Με άλλα λόγια, θέλουμς να επιτρέψουμε την πλήρη επεξεργασία των δεδομένων, δηλαδή να πραγματοποιήσουμε οποιεσδήποτε λειτουργίες σε αυτά, χωρίς όμως να δώσουμε πρόσβαση σε αυτά, ώστε για παράδειγμα, να μπορούμε να ελέγξουμε ένα email αν είναι ανεπιθύμητο (Spam) χωρίς όμως να εξετάσουμε τα περιεχόμενά του. Κάτι τέτοιο, αν και φαίνεται οξύμωρο, είναι θεωρητικά δυνατό με την Πλήρως Ομομορφική Κρυπτογραφία. Το πρώτο τέτοιο κρυπτοσύστημα προτάθηκε από τον Graig Gentry στα “Computing arbitrary functions of encrypted data”[**19**] και “A fully homomorphic encryption scheme” [**20**]

Μία ακόμα χρήσιμη εφαρμογή του ομοιομορφισμού, είναι ότι ανοίγει το δρόμο για να στηθούν συστήματα για ηλεκτρονικές ψηφοφορίες. Στην περίπτωση που ένα πλήρως ομομορφικό σύστημα είναι διαθέσιμο, ο καθένας θα μπορούσε να καταθέσει την ψήφο του αφού την πρυπτογραφούσε. Τότε το σύστημα θα είχε τη δυνατότητα της καταμέτρησης όλων των ψήφων και της έκδοσης του αποτελέσματος χωρίς να γνωρίζει της επιμέρους μεμονωμένες ψήφους. Μία επέκταση της ηλεκτρονικής ψηφοφορίας είναι η στατιστική ανάλυση που θα μπορούσε να γίνει σε ένα σύστημα το οποίο δίνει ερωτηματολόγια σε μία συγκεκριμένη μορφή ώστε να συλλέξει μόνο ανώνυμα και κρυπτογραφημένα δεδομένα τα οποία επεξεργάζονται μόνο από το ίδιο το σύστημα.

Ερωτήματα μέσω internet επίσης, θα είναι πιο “ασφαλή” με την ύπαρξη ενός τέτοιου συστήματος. Αφού είναι δυνατό να κρυπτογραφηθεί κάθε ερώτημα, ο κατάλληλος server μπορεί να στείλει τα αποτελέσματα της εκάστοτε ερώτησης χωρίς να ξέρει ποιο ήταν το πραγματικό ερώτημα.

2. Κβαντική Κρυπτογραφία

Κατά τη δεκαετία του 1930 μεγάλες μορφές της επιστημονικής κοινότητας, όπως ο Alan Turing έθεσαν τις βάσεις της θεωρητικής πληροφορικής. Αυτές οι θεωρίες θέτουν κάποια όρια για τους αλγορίθμους που εκτελούνται σε πρότυπες υπολογιστικές μηχανές. Το συγκλονιστικό είναι ότι στις

θεωρίες αυτές βασίστηκε η κατασκευή μιας “σύγχρονης” υπολογιστικής μηχανής (παρόμοια στη λειτουργία με τους σημερινούς υπολογιστές) που πρωτοεμφανίστηκε τη δεκαερία του ’50. Από τότε οι εξελίξεις στον τομέα της κατασκευής υπολογιστών υπήρξαν ραγδαίες. Έτσι περνώντας από τεχνολογία λυχνιών και DLSI κυκλώματα έχουμε σήμερα φτάσει σε ένα σημείο που τα δομικά στοιχεία των υπολογιστών είναι τόσο μικρά ώστε να επηρεάζονται ήδη από τους νόμους της κβαντομηχανικής. Η εξέλιξη αυτή γέννησε μία νέα γενιά επιστημόνων που οραματίζονταν ότι ίσως αυτές οι επιδράσεις θα μπορούσαν να χρησιμοποιηθούν για να επιταχύνουν τους υπολογισμούς.

Ο Richard Feynman ήταν εκείνος που πρώτος παρουσίασε μία ιδέα για το πως ένα κβαντικό σύστημα θα μπορούσε θεωρητικά να χρησιμοποιηθεί για την πραγματοποίηση υπολογισμών. Στη συνέχεια ο David Deutsch το 1985 έκανε μία ριζοσπαστική δημοσίευση όπου περιέγραφε το πως κάθε φυσική διαδικασία θα μπορούσε να μοντελοποιηθεί θεωρητικά με τέλειο τρόπο με χρήση ενός κβαντικού υπολογιστικού συστήματος. Ένα τέτοιο κβαντικό υπολογιστικό σύστημα μπορεί, όπως αναφέρει, να πραγματοποιήσει διαδικασίες αδύνατες για έναν “κλασικό” υπολογιστή, παράδειγμα η παραγωγή πραγματικά τυχαίων ακεραίων. Η βασικότερη ιδιότητά του είναι η ικανότητα να χρησιμοποιεί το φαινόμενο του κβαντικού παραλληλησμού για να πραγματοποιεί κάποιους υπολογισμούς σε χρόνο πολύ μικρότερο από τον “κλασικό” υπολογιστή.

Όπως έχουμε ήδη αναφέρει σε προηγούμενη υποπαράγραφο για την κβαντική κρυπτογραφία, είναι θεωρητικά δυνατό ένας κβαντικός υπολογιστής n qubit να βρίσκεται ταυτόχρονα σε 2^n καταστάσεις. Αυτό θα σήμαινε ότι θα μπορούσε να αναπαραστήσει ταυτόχρονα όλα τα κλειδια ενός κρυπτοσυστήματος.[**12**] Κατ’ επέκταση, μπορεί να δημιουργηθούν νέοι αλγόριθμοι για την επίλυση προβλημάτων που να εκμεταλλεύονται τις νέες ιδιότητες μιας τέτοιας κβαντικής υπολογιστικής μηχανής και να λύνουν (ίσως και NP–πλήρη) προβλήματα με καινούργιους τρόπους, όπως ο αλγόριθμος του Shor (που δημιουργήθηκε το 1994!) και ο οποίος με κάποιες τροποποιήσεις μπορεί να επιλύσει με εκθετική βελτίωση το πρόβλημα Διακριτού Λογαρίθμου σε ομάδες πρώτων και σε ελλειπτικές καμπύλες. Επίσης, στη συμμετρική κρυπτογραφία υπάρχει ο αλγόριθμος του Grover που επιφέρει πολυωνυμική βελτίωση τον AES.

Γενικά, η κρυπτογραφία που βασίζεται σε Πλέγματα Σημείων είναι ένας σχετικά καινούργιος κλάδος της κρυπτογραφίας που έχει ήδη δώσει αρκετά σημαντικά κρυπτοσυστήματα και σχήματα ψηφιακών υπογραφών. Το πιο σημαντικό πλεονέκτημα αυτών των συστημάτων, είναι η μετακβαντική τους ασφάλεια, διότι τα προβλήματα με πλέγματα σημείων είναι δυσεπίλυτα, που σημαίνει ότι είναι ασφαλή για όσο διάστημα δε μπορεί κανείς να βρει έναν αλγόριθμο πολυωνυμικού χρόνου για να προσεγγίσει τα βραχύτερα διανύσματα σε κάθε πλέγμα σημείων (SVP-CVP).

Παράρτημα Α'

Το Πρόβλημα του Διακριτού Λογαρίθμου

Είναι εύκολο για κάποιον να υπολογίσει το b^x για κάποιο μεγάλο x σε σχετικά μικρό χρόνο. Αν μας δώσουν έναν αριθμό y, ο οποίος είναι της μορφής b^x (όπου το b θεωρείται γνωστό) είναι επίσης εύκολο να υπολογίσουμε το μοναδικό x τέτοιο ώστε $y = b^x$ δηλαδή το $x = \log_b y$.

Η επίλυση της παραπάνω εξίσωσης στο $\mathbb{Z}_p$, για p πρώτο, είναι το Πρόβλημα Διακριτού Λογαρίθμου (Discrete Logarithm Problem –DLOG)

Ορισμός 32. *Έστω G μία πεπερασμένη κυκλική ομάδα τάξης n, a ένας γεννήτορας της G και $\beta \in G$. Ο Διακριτός Λογάριθμος του β στη βάση a, συμβολίζεται με $\log_a \beta$ και είναι ο μοναδικός ακέραιος x με $0 \leq x \leq n-1$ τέτοιος ώστε $b = a^x$.*

Ορισμός 33. *Το Πρόβλημα του Διακριτού Λογαρίθμου $DLOG$ είναι το παρακάτω:*
Input: p πρώτος αριθμός, a γεννήτορας του $\mathbb{Z}_p^*$, $\beta \in \mathbb{Z}_p^*$
Output: x με $0 \leq x \leq q-2$ τέτοιος ώστε

$$a^x = \beta(\mod p)$$

Πρόταση 3. *Η δυσκολία του DLOG είναι ανεξάρτητη από την επιλογή του γεννήτορα a του $\mathbb{Z}_p^*$.*

Το διακριτό Πρόβλημα Σακιδίου

- Υπάρχουν n διαφορετικά αντικείμενα με αξία c_i και βάρος a_i
- Διαθέτουμε έναν σάκο που αντέχει συνολικό μέγιστο φορτίο b
- Σκοπός μας είναι να βρούμε ποια αντικείμενα θα τοποθετήσουμε στο σάκο χωρίς να υπερβούμε το μέγιστο συνολικό φορτίο και μεγιστοποιώντας την συνολική αξία

Βιβλιογραφία

[1] Βάρσος Δ., Δεριζιώτης Δ., Εμμανουήλ Γ., Μαλιάκας Μ., Ταλέλλη Ολ., "Μία εισαγωγή στην Άλγεβρα", Εκδ Σοφία, 2005

[2] Βάρσος Δ. "Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων"

[3] Hoffstein J., Pipher J. and Silverman J.H., "NTRU: a ring based public key cryptosystem" In Proc of ANTS III, vol 1423 of LNCS, Springer-Verlag, 1998, pp.267-288

[4] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "An Introduction to Mathematical Cryptography", 2008 Springer Science & Business Media, LLC

[5] Ron Steinfeld, "NTRU Cryptosystem: Recent Developments", RICAM, 2013

[6] J.Pipher, "Lectures on the NTRU encryption algorithm and digital signature scheme", Grenoble 2002

[7] "The LLL Algorithm, Survey and Applications", Springer 2010 Editors Nguyen Phong Q., Vallee Brigitte

[8] Shai Halevi, Tal Malkin, "Ideal Lattices and NTRU", 2013

[9] Bremner M.R., "Lattice Basis Reduction: An introduction to the LLL Algorithm and its Applications", CRC PRess 2012

[10] Micciancio Daniele, "Introduction to Lattices, Lattice Algorithms and Applications", 2010

[11] Thijs Laarhoven, Joop can de Polt, Benne de Weger, "Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems", 2012

[12] Menezes A.J., PC van Oorschot, Vanstone S.A., "Handbook of Applied Cryptography", CRC Press, 2001

[13] Wei Ren, "Ntru Cryptography: A tutorial", UNLV 2006

[14] D. Coppersmith, A. Shamir, "Lattice attacks on NTRU", 1997

[15] W.Diffie, M.E.Hellman, "New Directions in cryptography", IEEE, 1976

[16] Graig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices", STOC 2009

[17] van Dijk, Marten and Gentry, Craig and Halevi, Shai and Vaikintanathan, Vinod, "Fully Homomorphic Encryption over the Integers", Cryptology ePrint Archive, Report, 2009

[18] Ronald L. Rivest, Len Adleman and Michael L. Derouzos "On data banks and privacy homomorphisms", 1978

[19] Graig Gentry, "Computing arbitrary functions of encrypted data", Communications of the ACM, 2010

[20] Graig Gentry, “A fully homomorphic encryption scheme”, PhD thesis, Stanford University, 2009 http://crypto.stanford.edu/craig

[21] Hoffstein J., Pipher J. and Silverman J., “NTRU: A new high speed public key cryptosystem”, 1996

[22] Goldreich O., Goldwasser S., Haveli S., “Public-Key cryptosystems from lattice reduction problems” MIT Laboratory for Computer Science, Springer-Verlag, 1997

[23] R.J. McEliece, “A public-key cryptosystem based on algebraic coding theory”, Pasadena, DSN Progress Reports, 1978

[24] Constantinos Patsakis, Jeroen var Rest, Michal Choras and Melanie Bouroche, “Privacy-Preserving Biometric Authentication and Matching via Lattice-Based Encryption”

[25] Constantinos Patsakis, Panayiotis Kotzanikolaou and Melanie Buoroche, “Private Proximity Testing on Steroids: An NTRU-based Protocol”

[26] Bell T., Thimbleby H., Fellows M., Witten I., Koblitz N., Powel M.,“Explaining cryptographic systems”, Computers & education, 2003

[27] Blake-Wilson S., “Information Security, Mathematics and Public-Key Cryptography”, Designs, Codes and Cryptography, 2000

[28] Pieprzyk J. Hardjono T., Seberry J., “Fundamentals of Computer Security”, Springer, 2003

[29] Schneier B., “Applied Cryptography, Protocols, Algorithms and Source Code in C”, Wiley, 1996

[30] Goldreich O., “Foundations of Cryptography, basic tools”, Cambridge University Press, 2001

[31] Ford W. “Computer Communications Security Principles”, Standard Protocols and Techniques, Prentice-Hall, New Jersey, 1994

[32] Kalinski B.S. Jr., “A survey of encryption standards”, IEEE Micro(6), 1993

[33] Abbas Acar, Hidayer Aksu and Selcuk Uluagac, Mauro Conti, “A Survey on Homomorphic Encryption Schemes: Theory and Implementation”, 2017

[34] Guillaume Bonnoron, Caroline Fontaine, Guy Gogniat, Vincent Herbert, Vianney Lapotre, Vincent Migliore and Adeline Roux-Langlois, “Somewhat/Fully Homomorphic Encryption: Implementation pregresses and challenges”

[35] Hao Chen, Kim Laine, Rachel Player and Yuhou Xia, “ High-Precision Arithmetic in Homomorphic Encryption”

[36] Wei Dai, Yarkin Doroz, Berk Sunar, “Accelerating NTRU based Homomorphic Encryption using GPU’s”, IEEE, 2014

[37] David Kahn, “The Codebreakers”, 1973, New American Library

[38] Bennett C., Bessette F., Brassard G., Savail L., Smolin J., “Experimental quantum cryptography”, Journal of Cryptology (1) 5, 1992

[39] Brassard G., “Cryptography column - Quantum cryptography: A bibliography”, Sigast News (3) 24, 1993

[40] Brassard G., “The computer in the 21sr Century”, Scientific American, 1995

[41] Brassard G., “The impending demise of RSA?” Cryptobytes(1), 1995

[42] Brassard G., “A quantum jump in computer science”, Current Trends in Computer Science, Springer-Verlag, 1995

[43] Μιχαήλ Δ., “Αλγόριθμοι και Πολυπλοκότητα, NP και υπολογιστική Δυσεπιλυσιμότητα”, Χαροκόπειο Πανεπιστήμιο

[44] https://github.com/NTRUOpenSourceProject/ntru-crypto