ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΜΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΚΤΥΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΧΗΜΑΤΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΗΝ ΘΕΩΡΙΑ ΠΛΕΓΜΑΤΩΝ ΓΙΑ ΔΙΚΤΥΑ ΑΝΘΕΚΤΙΚΑ ΣΤΙΣ ΜΕΤΑ-ΚΒΑΝΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ»

ΤΖΙΑΤΖΟΣ ΓΕΩΡΓΙΟΣ

Επιβλέπουσα: Επίκουρος καθηγήτρια Βασιλική Λιάγκου

Άρτα, 2022

« LATTICE – BASED CRYPTOGRAPHE SCHEMES IN POST-QUANTUM NETWORKS »

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπουσα καθηγήτρια

Επίκουρος καθηγήτρια **Βασιλική Λιάγκου**

2. Μέλος επιτροπής

Καθηγητής **Χρυσόστομος Στύλιος**

3. Μέλος επιτροπής

Επίκουρος καθηγητής **Νικόλαος Γιαννακέας**

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εκ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Τζιάτζος, Γεώργιος

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Πρώτα από όλα θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια της παρούσας μεταπτυχιακής εργασίας Κα Βασιλική Λιάγκου που με το υψηλό επίπεδο γνώσεων της λειτούργησε επικουρικά στην προσπάθεια μου. Μέσα από την άριστη καθοδήγηση της και την συχνή επικοινωνία για την πρόοδο της εργασίας συνέβαλλε τα μέγιστα.

Ακόμη θα ήταν παράληψη μου να μην εκφράσω τις ευχαριστίες μου σε όλους τους διδάσκοντες του μεταπτυχιακού προγράμματος σπουδών που πρόσφεραν στην ολοκλήρωση του. Κατόρθωσαν να με ενισχύσουν με ζήλο και να μου προσφέρουν όλα τα απαραίτητα εφόδια έτσι ώστε να ευοδωθούν όλες οι προσπάθειες μου και να φέρω εις πέρας αυτό το εγχείρημα.

Τέλος θα ήθελα να ευχαριστήσω ιδιαίτερα την οικογένεια μου που στηρίζουν τα όνειρα και τις προσπάθειες μου χωρίς ποτέ να με αποτρέψουν από κάτι.

ΠΕΡΙΛΗΨΗ

Η κρυπτογραφία στις μέρες μας βασίζεται σε μεγάλο βαθμό σε θεωρία που μας παρέχεται από τα μαθηματικά θεωρήματα. Τα θεωρήματα αυτά εφαρμόζονται στην πληροφορική προκειμένου να αναπτυχθούν αλγόριθμοι που θα παρέχουν μεγαλύτερη ασφάλεια. Τα προβλήματα στην κρυπτογραφία κατατάσσονται σε 2 μεγάλες κατηγορίες, στα προβλήματα κλασσικής και κβαντικής κρυπτογραφίας.

Στην παρούσα εργασία θα επικεντρωθούμε στην μελέτη κρυπτογραφικών σχημάτων που είναι ανθεκτικά σε μετά-κβαντικές επιθέσεις. Για να προστατευθούμε έχουν αναπτυχθεί διάφορα κρυπτογραφικά σχήματα που βασίζονται στην θεωρία πλέγματος. Σύμφωνα με αυτά αναπτύσσουμε πολύπλοκους αλγορίθμους με χρήση ανώτερων μαθηματικών για την δημιουργία δημοσίων και ιδιωτικών κλειδιών που απαιτούνται στην κρυπτογραφία. Με την βοήθεια αυτών των αλγορίθμων υλοποιούμε σε γλώσσα προγραμματισμού MATLAB κώδικες του πολύ σημαντικού κρυπτοσυστήματος McAliece που βασίζεται στην θεωρία πλεγμάτων καθώς και του σχήματος υπογραφής Matsumoto-Imai. Τέτοιου είδους συστήματα βρίσκουν εφαρμογή σε τεχνολογίες blockchain. Όμως τα συστήματα αυτά εξαιτίας του τρόπου με τον οποίο δημιουργήθηκαν παρουσιάζουν κάποια μειονεκτήματα όπως είναι το μεγάλο μέγεθος δημόσιο και ιδιωτικό κλειδί, γεγονός που τα καθιστά μειωμένης χρήσης σε σχέση με μεταγενέστερα , έτσι στην συνέχεια περιγράφουμε το πλήρες μαθηματικό μοντέλο για την ανάπτυξη ενός νέου σχήματος υπογραφής. Στο νέο αυτό σχήμα έχει επιτευχθεί ο περιορισμός αυτών των προβλημάτων και μάλιστα σε σύγκριση με άλλα συστήματα της βιβλιογραφίας αποδεικνύεται ότι είναι περισσότερο αποδοτικά. Ακόμη μέσα από αυτή την διαδικασία γίνεται και ταυτόχρονη μελέτη των τρωτών σημείων που προκύπτουν από μετά-κβαντικές επιθέσεις.

Ως εκ τούτο με αυτήν την εργασία εμπλουτίσαμε την έρευνα πάνω στον τρόπο με τον οποίο μπορούμε να αποφύγουμε μετα-κβαντικές επιθέσεις, υλοποιήσαμε κώδικες για συστήματα βασισμένα σε τεχνολογία πλεγμάτων , καθώς επίσης και προτείναμε ένα νέο σύστημα που παρέχει μεγαλύτερη ασφάλεια και έχει καλύτερη απόδοση.

Λέξεις-κλειδιά: Μετά-κβαντική κρυπτογραφία, Ασύμμετρη κρυπτογραφία, πλέγματα, μετά-κβαντικό blockchain.

ABSTRACT

Cryptography nowadays is largely based on a theory provided to us by mathematical theorems. These theorems are applied in computer science in order to develop algorithms that will provide greater security. The problems in cryptography are classified into 2 big categories, the problems of classical and quantum cryptography.

In this thesis we will focus on the study of cryptographic schemes that are resistant to post-quantum attacks. For our protection, various cryptographic schemes based on grid theory have been developed. According to them we develop complex algorithms using higher mathematics to create public and private keys required in cryptography. With the help of these algorithms we implement codes of the very important McAliece cryptosystem based on grid theory as well as the Matsumoto-Imai signature scheme, using MATLAB programming language. Such systems find application in blockchain technologies. Because of the way these systems were created, there are some disadvantages such as the large size of public and private key, which makes them less used compared to subsequent ones, so as a result we describe the complete mathematical model for developing a new signature format. In this new scheme the reduction of these problems has been achieved and in fact in comparison with other systems of the literature it proves to be more efficient. Additionally, through this process, the vulnerabilities arising from post-quantum attacks are studied simultaneously.

Therefore, with this thesis we have augmented the research on how we can avoid post-quantum attacks, implemented codes for grid-based systems, and proposed a new system that provides greater security and better performance.

Keywords: Post- Quantum Cryptography, Asymmetric Cryptography, Lattices, Post-Quantum Blochchain

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

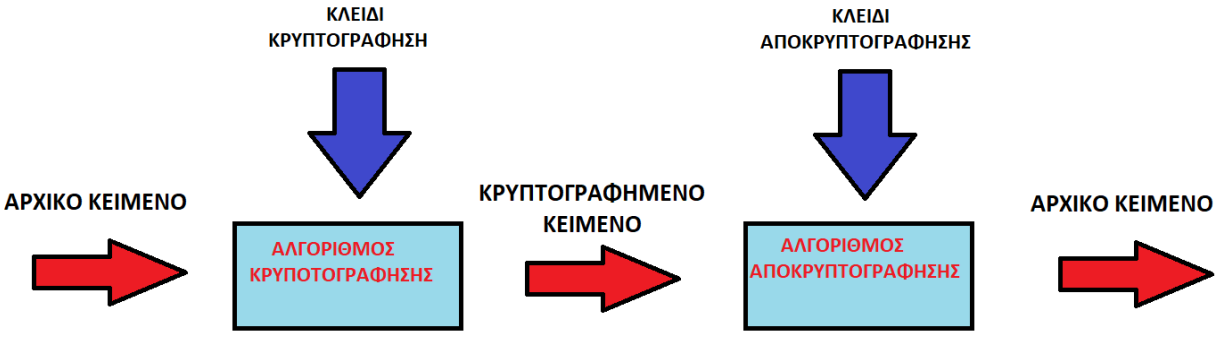
1. Εισαγωγή

1.1. Εισαγωγή στην κρυπτογραφία

Κρυπτογραφία είναι η επιστήμη που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση αλγορίθμων (ciphers) οι οποίοι μετασχηματίζουν ένα αρχικό μήνυμα (plain message), π.χ. (κείμενο, εικόνα, video, ήχος), σε ένα άλλο κρυπτογραφημένο μήνυμα το οποίο καλείται κρυπτογράφημα (cipher). Το κρυπτογράφημα είναι δυσνόητο από μη εξουσιοδοτημένα άτομα, πράκτορες (agents), παίκτες. Η κρυπτογραφία είναι σύνθετη λέξη και πήρε το όνομα της από συνθετικά "κρυπτός" + "γράφω".

Η επικοινωνία γενικά πραγματοποιείται μέσω ενός μη ασφαλούς διαύλου ή δικτύου, απόρροια αυτού είναι οι μη εξουσιοδοτημένοι χρήστες να μπορούνε να έχουν πρόσβαση στο κρυπτογραφημένο μήνυμα με απώτερο στόχο την αποκρυπτογράφηση του. [1]. Η κρυπτογραφία δύναται να παρέχει στον εκάστοτε χρήστη μια ψηφιακή υπογραφή με την βοήθεια της οποίας γίνεται η σύνδεση για παράδειγμα ενός εγγράφου με τον κάτοχο ενός κλειδιού, ώστε να εξασφαλιστεί η εμπιστοσύνη μεταξύ των εξουσιοδοτημένων χρηστών. [2] [3]

Στο σχήμα που ακολουθεί φαίνεται ένα τέτοιο τυπικό σχήμα κρυπτογράφησης – αποκρυπτογράφησης.



Σχήμα 1.1: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης

Η Κρυπτανάλυση (cryptanalysis) αξιολογεί τους αλγορίθμους κρυπτογράφησης [4], [5] και [6] .

Η διαδικασία της κρυπτογράφησης – αποκρυπτογράφησης καλείται κρυπτοσύστημα.

Ο τρόπος λειτουργίας του κρυπτοσυστήματος βασίζεται σε μια λειτουργία πέντε βημάτων. Κατά το πρώτο βήμα ο αποστολέας επιλέγει ένα κλειδί μήκους n σε ένα χώρο κλειδιών K με τυχαίο τρόπο. Στο δεύτερο βήμα με την βοήθεια ενός ασφαλούς διαύλου επικοινωνίας αποστέλλει το κλειδί στον παραλήπτη. Στην συνέχεια ο αποστολέας δημιουργεί το αρχικό μήνυμα σε ένα χώρο μηνυμάτων J. Στο βήμα που ακολουθεί το αρχικό μήνυμα μαζί με το κλειδί με την βοήθεια του μετασχηματισμού κρυπτογράφησης, παράγει το κρυπτογραφημένο μήνυμα έτοιμο για αποστολή.

1.2. Ιστορική αναδρομή

Η ιστορία της κρυπτογραφίας μπορεί να διαιρεθεί σε τρία στάδια [7]

Κατά το πρώτο στάδιο έχουμε που αφορά την περίοδο από τους αρχαίους πολιτισμούς μέχρι και τα μισά του 19^{ου} αιώνα έχουμε η διαδικασία κρυπτογράφησης να γίνεται με έντυπη απεικόνιση με χρήση μελάνι και χαρτιού. Η κρυπτογραφία σε αυτό το στάδιο κυρίως γινόταν με μορφή αντικατάστασης και αναδιάταξης των γραμμάτων της αλφαβήτου (ενδεικτικά ο κρυπτογραφικός αλγόριθμος του Καίσαρα) [8]. Στο δεύτερο στάδιο όπου κύρια περίοδος αυτού είναι ο δεύτερος παγκόσμιος πόλεμος αναφερόμαστε στη χρήση κρυπτογραφικών μμηχανών, (η Γερμανική μμηχανή Enigma). Στο Τελευταίο στάδιο που θεωρείται το σύγχρονο κρυπτογραφικό σύστημα και εκτείνεται χρονικά έως και σήμερα , λόγω της ταχείας αύξησης στις δυνατότητες των υπολογιστών ώστε να μπορούν να γίνουν επίπονοι μαθηματικοί υπολογισμοί μέσω αυτών η κρυπτογραφία στηρίζεται σε μαθηματική βάση.

Αν ανατρέξουμε επί αρχαιοτάτων χρόνων γινόταν χρήση κρυπτογραφικών συστημάτων στις ιδιωτικές επικοινωνίες , στην θρησκεία, αλλά και για διπλωματική και στρατιωτική χρήση [9] .

Ο πατέρας της μαθηματικής κρυπτογραφίας θεωρείται ο Shannon όπου κατά την διάρκεια του Δευτέρου Παγκοσμίου Πολέμου εξέλιξε την κρυπτογραφία κυρίως στον τομέα της ασφάλεια των επικοινωνιών. Ο Shannon με το άρθρο του «Θεωρία Επικοινωνίας Συστημάτων Μυστικότητας» που δημοσιεύτηκε το 1949 και λίγο αργότερα με το βιβλίο «Μαθηματική Θεωρία Επικοινωνίας» που συνέγραψε με τον Warren Weaver, ήταν αυτός που έθεσε τις στέρεες βάσεις για την κρυπτογραφία και την κρυπτανάλυση (μελέτη των μεθόδων για την ανάκτηση του νοήματος της κρυπτογραφημένης πληροφορίας). [10] [11]

Στην συνέχεια ακολούθησε ένα διάστημα μεγαλύτερο των 20 ετών, όπου η κρυπτογραφία αναπτυσσόταν σε άκρα μυστικότητα κυρίως μέσα από κρατικές υπηρεσίες μυστικών πληροφοριών. Από τα μέσα όμως της δεκαετίας του 1970 η επικρατούσα έως τότε τάση άλλαξε και άρχισαν να δημοσιοποιούνταν οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνταν χωρίς να δίνονται στην δημοσιότητα τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης.

Η σημαντικότερη ίσως δημοσίευση , που έδωσε ξανά την ώθηση για άνθιση της επιστήμης της κρυπτογραφίας που είδε το φως της δημοσιότητας ήταν η δημοσίευση του προσχέδιου του Προτύπου Κρυπτογράφησης Δεδομένων (Data Encryption Standard – DES) που υποβλήθηκε στο εθνικό γραφείο προτύπων της Αμερικής το 1975. Το DES δόθηκε στην δημοσιότητα από την IBM σε μια προσπάθεια της να εξασφαλίσει ασφάλεια στις ηλεκτρονικές επικοινωνίες επιχειρήσεων, τραπεζών και άλλων μεγάλων χρηματοπιστωτικών οργανισμών. Μετά από κάποια τροποποίηση από την υπηρεσία εθνικής ασφάλειας των Ηνωμένων Πολιτειών της Αμερικής δημοσιεύτηκε το 1977.

Άλλη μια χρονολογία ορόσημο για την κρυπτογραφία μπορεί να θεωρηθεί το 1976 , όπου οι Diffie και Hellman μέσω του άρθρου «Νέες Κατευθύνσεις στην Κρυπτογραφία» γεννήθηκε η κρυπτογραφία δημόσιου κλειδιού και κατάφερε να δημιουργήσει μια νέα μέθοδο για την ανταλλαγή κλειδιών , που βασίζεται στην δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου. [12]

Με την πάροδο δύο χρόνων , το 1978, οι Rivest, Shamir και Adleman ανακάλυψαν τον αλγόριθμο RSA, το πρώτο πρακτικό σχήμα κρυπτογράφησης και υπογραφής δημοσίου κλειδιού. [13] Το πρόβλημα της δύσκολης επίλυσης μεγάλων ακεραίων ήταν η βάση για την επίλυση αυτού του προβλήματος. Αυτή η εφαρμογή ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία έδωσε νέα προοπτική και ελπίδες στις προσπάθειες για την αναζήτηση περισσότερο αποδοτικών μεθόδων παραγοντοποίησης. Παρότι κατά την δεκαετία του ‘80 σημειώθηκε αξιοσημείωτη πρόοδος σε αυτός τον τομέα, καμία δεν καθιστούσε το σύστημα RSA ανασφαλές. Ο ElGamal το 1985 ήταν αυτός που κατάφερε να βρει μία άλλη κλάση ισχυρών και πρακτικών σχημάτων δημοσίου κλειδιού. [14]. Ένα κοινό γνώρισμα αυτών των σχημάτων με τα προηγούμενα είναι ότι βασίζονται στο πρόβλημα διακριτού λογαρίθμου .

Αξιοπρόσεκτη είναι και η ανάπτυξη νέων κρυπτογραφικών δομών και εννοιών, όπως είναι τα δένδρα Bonsai (Bonsai Trees) [15]. Τα δένδρα Bonsai στηρίζονται στο γεγονός ότι είναι μία συλλογή αρχών και τεχνικών, τέτοιες ώστε να μπορούν να χρησιμοποιηθούν με πολυάριθμους τρόπους. Η βάση της ανάπτυξης τους ήταν η επίλυση ορισμένων σημαντικών ανοικτών προβλημάτων σε αυτήν την περιοχή. Παράδειγμα τέτοιων προβλημάτων η εύρεση ενός αποδοτικού και άνευ κατάστασης, "hash–and–sign" σχήματος υπογραφής στο καθιερωμένο μοντέλο (standard model), όπως και η ανάπτυξη του πρώτου ιεραρχικού σχήματος κρυπτογράφησης που βασίζεται στην ταυτότητα (Hierarchical Identity–based Encryption), χωρίς δηλαδή την χρήση τυχαίων μαντείων (random oracles). Οι αρχές πάνω στις οποίες στηρίχτηκαν τα δέντρα Bonsai θα αναλυθούν σε επόμενη ενότητα.

1.3. Είδη κρυπτοσυστημάτων

Μια προσπάθεια κατάταξης των κρυπτοσυστημάτων έγινε από τους [16] , [17] , [18], όπου τα κατέταξαν σε δύο μεγάλες κατηγορίες: Στα Κλασσικά Κρυπτοσυστήματα και στα Μοντέρνα/Σύγχρονα Κρυπτοσυστήματα.

Κάποιες από τις περιπτώσεις κλασικής κρυπτογραφίας είναι η αντικατάσταση των συμβόλων του μηνύματος, αναδιάταξη αυτών. Μπορεί επίσης να είναι Μονοσταδιακή ή πολυσταδιακή, Μονοαλφαβητική.

Στα Μοντέρνα / Σύγχρονα κρυπτοσυστήματα έχουμε περιπτώσεις κρυπτογραφίας που βασίζεται σε επίλυση υπολογιστικών προβλημάτων. Συγκεκριμένα Συμμετρική ή κρυπτογραφία ιδιωτικού κλειδιού και ασύμμετρη ή δημόσιου κλειδιού [19]. [20].

Οι βασικές διαφορές μεταξύ των μεθόδων κρυπτογραφίας είναι ότι στα κλασικά κρυπτοσυστήματα έχουμε απευθείας επέμβαση στα γράμματα και τους χαρακτήρες, ενώ στην μοντέρνα έχουμε λειτουργία σε δυαδικές ακολουθίες bit. Στην κλασική κρυπτογραφία ή γνώση για τις τεχνικές που χρησιμοποιούνται σε κάθε κωδικοποίηση μοιράζεται μόνο στους εμπλεκόμενους στην επικοινωνία θα μπορούσαμε να πούμε ότι στηρίζεται σε κάποιο εμπιστευτικό μοτίβο, σε αντίθεση με την σύγχρονη όπου η κρυπτογράφηση των μηνυμάτων στηρίζεται σε γνωστούς μαθηματικούς αλγορίθμους. Αυτό τους καθιστά πιο ασφαλείς διότι για παράδειγμα η υπολογιστική δυσκολία αυτών των αλγορίθμων, η απουσία του μυστικού κλειδιού καθιστούν αδύνατο σε κάποιον επιτιθέμενο, ακόμη και αν γνωρίζει τον τρόπο λειτουργίας του αλγορίθμου, να αποκτήσει πρόσβαση στην πληροφορία. Τέλος κατά την κλασική κρυπτογραφία απαιτείται ολόκληρο το κρυπτογραφικό σύστημα για την

εμπιστευτική επικοινωνία (πχ στα σήματα μορς) σε αντίθεση με την σύγχρονη που η γνώση μόνο του κλειδιού μπορεί να εγγυηθεί την ασφαλή επικοινωνία. [21]

Όπως είναι εύκολα κατανοητό αντικείμενο εκτενούς μελέτης έχουν γίνει τα μοντέρνα/ σύγχρονα κρυπτοσυστήματα και κυρίως η συμμετρική και ασύμμετρη κρυπτογραφία, που καλούνται και κρυπτογραφία ιδιωτικού ή δημόσιου κλειδιού αντίστοιχα.

Πιο συγκεκριμένα η κρυπτογραφία ιδιωτικού κλειδιού χωρίζεται σε 2 κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων.

• Στους Τμηματικούς Κρυπτογραφικούς αλγορίθμους (Block Ciphers), όπου χωρίζουν το αρχικό μήνυμα σε τμήματα ίσου μήκους (blocks) συνήθως έως 128 bits έκαστο και στην συνέχεια κρυπτογραφούν έκαστο τμήμα διαδοχικά.

• Στους Κρυπτογραφικούς αλγορίθμους Ροής (Stream Ciphers), όπου κρυπτογραφούν το αρχικό μήνυμα μέσω μίας πράξης (συνήθως XOR) εκάστου όρου του μηνύματος με τον αντίστοιχο όρο μίας ακολουθίας ίσου μήκους (ροής- stream) συμβόλων η οποία παράγεται από μια γεννήτρια τυχαίων αριθμών που δέχεται ως είσοδο (seed) το κλειδί κρυπτογράφησης.

Τέλος έχουν αναπτυχθεί , ειδικά τα τελευταία χρόνια, λόγω της ραγδαίας αύξησης στις δυνατότητες των ηλεκτρονικών υπολογιστών δύο νέες μέθοδοι κρυπτογραφίας.

Η πρώτη καλείται κρυπτογραφία με χάος όπου είναι απόρροια της θεωρίας πολύπλοκων συστημάτων και η δεύτερη καλείται κβαντική κρυπτογραφία και είναι απόρροια της κβαντικής θεωρίας και της δυνατότητας επεξεργασίας σε ατομικό επίπεδο (κβαντικοί υπολογιστές). [22]

Στην παρούσα εργασία θα ασχοληθούμε με κρυπτογραφικά σχήματα που είναι ανθεκτικά σε επιθέσεις που οφείλονται στην ταχεία ανάπτυξη της κβαντικής κρυπτογραφίας.

1.4. Ασφάλεια κρυπτογραφικών συστημάτων

Η ευκολία με την οποία μπορεί να παραβιαστεί ένα κρυπτοσύστημα δεν είναι σε όλες τις περιπτώσεις η ίδια. Θεωρώντας ως δεδομένο ότι όλοι οι αλγόριθμοι, εκτός από τους one - time - pad μπορούνε θεωρητικά να παραβιαστούν με δεδομένο ότι διαθέτουμε επαρκή υπολογιστική ισχύ και αποθηκευτική χωρητικότητα , ασφαλείς θεωρείται η κρυπτογράφηση όπου ο χρόνος και οι χρηματικοί πόροι που απαιτούνται για την παραβίαση ενός αλγόριθμου

υπερβαίνουν την αξία των κρυπτογραφημένων δεδομένων. Επειδή όμως η αξία των δεδομένων πιθανότατα να μειώνεται με την πάροδο του χρόνου και ταυτόχρονα η ταχύτητα των υπολογιστών αυξάνεται, με αποτέλεσμα περισσότερων υπολογισμών στον ίδιο χρόνο, χωρίς να αυξάνεται ανάλογα η τιμή αυτών είναι σκόπιμο να εκτιμήσουμε ότι η αύξηση της ταχύτητας να μην είναι δυσανάλογη με την πτώση της αξίας των δεδομένων για να εξασφαλίσουμε και την ασφάλεια της κρυπτογράφησης σε βάθος χρόνου.

Κάποιοι αλγόριθμοι απαιτούν εκατομμύρια χρόνια να παραβιαστούν με τεράστιους υπολογιστικούς πόρους. Οι αλγόριθμοι αυτοί ενώ θεωρητικά μπορούμε να πούμε ότι παραβιάζονται, στην πράξη δεν συμβαίνει κάτι τέτοιο. Οι αλγόριθμοι αυτοί θεωρούνται ασφαλής (secure).

Ένας αλγόριθμος θεωρείται ασφαλής άνευ όρων (unconditionally secure) αν, χωρίς να λαμβάνεται υπόψη το μέγεθος του κρυπτογραφημένου μηνύματος, τους υπολογιστικούς πόρους και το χρόνο που μπορεί να διαθέτει ο κρυπταναλυτής, δεν είναι εφικτό να αποκαλυφθεί το καθαρό μήνυμα. Τα one - time -pads, δεν μπορεί να παραβιαστούν, ακόμα και δεδομένων άπειρων πόρων. Η Κρυπτογραφία ασχολείται κυρίως με κρυπτογραφικά συστήματα τα οποία δεν μπορεί να παραβιαστούν με τις δεδομένες υπολογιστικές δυνατότητες. Ένας αλγόριθμος λέγεται υπολογιστικά ασφαλής (computationally secure), ή ισχυρός (strong), αν καθίσταται ανέφικτη η παραβίασή του με τους διαθέσιμους (τωρινούς ή μελλοντικούς) πόρους.

Ο χρόνος που απαιτείται για την παραβίαση ενός αλγορίθμου δεν είναι σταθερός γιατί είναι άμεση συνέπεια της χρησιμοποιούμενης κάθε φορά υπολογιστικής ισχύς και με δεδομένο την ραγδαία αύξηση αυτής στους νέους υπολογιστές μια τέτοια εκτίμηση δεν μπορεί να είναι ακριβής.

Ως εκ τούτου συμπερασματικά θα μπορούσαμε να πούμε ότι το να ισχυριστεί κάποιος ότι ένας αλγόριθμος είναι ασφαλής γιατί δεν μπορεί να παραβιαστεί με τα σημερινά δεδομένα δεν είναι απόλυτα σωστό. Ένα κρυπτογραφικό σύστημα θεωρείται ότι είναι καλά σχεδιασμένο όταν δεν είναι δυνατό να παραβιαστεί ακόμα και με την υπολογιστική ισχύ που αναμένεται να προκύψει μετά από πολλά χρόνια.

1.5. Σκοπός της εργασίας

Στην παρούσα εργασία θα επικεντρωθούμε στην μελέτη κρυπτογραφικών σχημάτων που είναι ανθεκτικά σε μετά-κβαντικές επιθέσεις. Οι επιθέσεις αυτές πραγματοποιούνται με την βοήθεια ισχυρών ηλεκτρονικών υπολογιστών. Για να προστατευθούμε έχουν αναπτυχθεί διάφορα κρυπτογραφικά σχήματα που βασίζονται στην θεωρία πλέγματος. Σύμφωνα με αυτά αναπτύσσουμε πολύπλοκους αλγορίθμους με χρήση ανώτερων μαθηματικών για την δημιουργία δημοσίων και ιδιωτικών κλειδιών που απαιτούνται στην κρυπτογραφία ώστε να μπορέσουμε να εξασφαλίσουμε την τυχαιότητα αυτών των κλειδιών και κατ' επέκταση την όσο το δυνατόν καλύτερη προστασία τους από πιθανές επιθέσεις.

Κατά συνέπεια ο κύριος στόχος μας είναι να μπορέσουμε να αναπτύξουμε τα κατάλληλα κρυπτογραφικά σχήματα και να εξηγήσουμε πλήρως τα τρωτά σημεία που μπορούμε να συναντήσουμε σε μετά-κβαντικές επιθέσεις. Ως εκ τούτο μετά το πέρας της εργασία θα μπορέσουμε να εμπλουτίσουμε την έρευνα πάνω στον τρόπο με τον οποίο μπορούμε να αποφύγουμε αυτές τις επιθέσεις, καθώς επίσης και να παρέχουμε χρήσιμα συμπεράσματα για περαιτέρω διερεύνηση αυτού του σημαντικού προβλήματος στην κρυπτογραφία.

1.6.Δομή πτυχιακής εργασίας

Εδώ θα δώσουμε μια σύντομη αναφορά των περιεχομένων των κεφαλαίων της παρούσας εργασίας.

Συγκεκριμένα στο πρώτο κεφάλαιο έγινε μια εισαγωγή στην κρυπτογραφία, αναφέροντας τα είδη αυτής και περιγράφοντας πότε ένας κρυπτογραφικό σύστημα θεωρείται ασφαλές. Κλείνοντας το κεφάλαιο αναφέρεται ο σκοπός συγγραφής της συγκεκριμένης εργασίας.

Στο δεύτερο κεφάλαιο περιγράφονται συγκεντρωτικά οι σπουδαιότερες εκ των μαθηματικών εννοιών – ορισμών που θα γίνουν χρήση. Θεωρήθηκε σκόπιμο να γίνει μια κατάταξη αυτών σε 3 κατηγορίες: α) στις μαθηματικές έννοιες που στηρίζονται στα πλέγματα, β) σε αυτές που στηρίζονται στους κβαντικούς υπολογισμούς , περιγράφοντας και τους σχετικούς αλγορίθμους και γ) στους αλγόριθμους κρυπτογραφίας.

Στο τρίτο κεφάλαιο εστιάζουμε στην κβαντική κρυπτογραφία δίνοντας τον ορισμό της και τι είναι αυτό που την διαφοροποιεί από την κλασική. Ακόμη γίνεται περιγραφή μερικών από

τα μοντέλα για την αντιμετώπιση των επιθέσεων και ολοκληρώνουμε το κεφάλαιο παρουσιάζοντας τα σημαντικότερα προβλήματα που αντιμετωπίζουμε στην κβαντική κρυπτογραφία.

Στο τέταρτο κεφάλαιο αρχικά χρησιμοποιώντας γλώσσα προγραμματισμού MATLAB θα υλοποιήσουμε κώδικες για την δημιουργία κλειδιών στο κρυπτοσύστημα McEliece και κάνουμε εφαρμογή για κρυπτογράφηση και αποκρυπτογράφηση τυχαίου μηνύματος. Στην συνέχεια του κεφαλαίου θα ασχοληθούμε με την υλοποίηση του σχήματος υπογραφής Matsumoto-Imai, που βασίζεται στις αρχές του κρυπτοσυστήματος McEliece.

Στο πέμπτο κεφάλαιο παρουσιάζουμε την μέθοδο που θα χρησιμοποιήσουμε κάνοντας μια εισαγωγή στο πρόβλημα που έχουμε να αντιμετωπίσουμε. Επίσης γίνεται περιγραφή του blockchain και με ποιον τρόπο η κρυπτογραφία ενσωματώνεται σε αυτό. Στην συνέχεια παραθέτουμε λεπτομέρειες για την μετά–κβαντική blockchain συναλλαγή και παρουσιάζουμε τα πρωτόκολλα που χρησιμοποιούνται στα πλαίσια αυτής της εργασίας.

Στην συνέχεια στο έκτο κεφάλαιο παραθέτουμε της λεπτομέρειες του προτεινόμενου σχήματος υπογραφής, αναλύοντας και την απόδειξη της ασφάλειας του εν λόγω σχήματος και κάνουμε μια σύγκριση του προτεινόμενου σχήματος με σχήματα που έχουν ήδη αναπτυχθεί. Η σύγκριση επικεντρώνεται τόσο στο μέγεθος του δημόσιου και ιδιωτικού κλειδιού όσο και στο μέγεθος της υπογραφής σε κάθε περίπτωση.

Τέλος κλείνοντας την εργασία στο τελευταίο κεφάλαιο αναφέρουμε τα συμπεράσματα που εξήχθησαν από αυτήν την εργασία.

2. Μαθηματικές έννοιες

Σε αυτό το κεφάλαιο θα αναφερθούμε σε χρήσιμες μαθηματικές έννοιες που βρίσκουν εφαρμογή στην κρυπτογραφία.

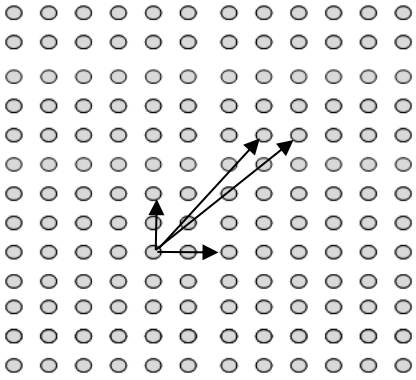
Οι μαθηματικές έννοιες που είναι εργαλεία κατά την κρυπτογραφία χωρίζονται σε 3 κατηγορίες: στα πλέγματα (δικτυωτά) , στους κβαντικούς υπολογισμούς και στους αλγόριθμους κρυπτογραφίας.

2.1.Δικτυωτά

Τα δικτυωτά είναι ένα σύνολο σημείων στον n-διάστατο χώρο με περιοδική δομή γενικά είναι γεωμετρικά αντικείμενα με πλούσια δομή. [23]. Η εμφάνιση τους έγινε από τον 19ο αιώνα και ξεκίνησε από τον Gauss, τον Hermite και τον Minkowski. Μπορούμε να πούμε βέβαια ότι ο πρώτος που ξεκίνησε να μελετάει τα δικτυωτά ήταν ο Ευκλείδης. [24] [25]

Αν θέλουμε να είμαστε περισσότερος ακριβείς ως δικτυωτά ορίζουμε οποιοσδήποτε γραμμικό συνδυασμός με ακέραιους συντελεστές μιας σειράς γραμμικώς ανεξάρτητων διανυσμάτων $\{b_i\}_{i=1}^{n}$, όπου και ονομάζουμε βάση του δικτυωτού:

$$L(b_1, \dots., b_n) = \sum_{i=1}^{n} x_i \cdot b_i \,, \qquad x_i \epsilon Z$$



Εικόνα 2.1: Δύο πιθανές βάσεις σε δικτυωτό 2 διαστάσεων

Προκειμένου να γίνουν οικεία στον αναγνώστη είναι χρήσιμο να αναφερθούμε και σε ορισμένους ορισμούς που πηγάζουν από τα δικτυωτά.

Βάση για το δικτυωτό L είναι κάθε σύνολο ανεξάρτητων διανυσμάτων που παράγουν το L. Δύο οποιαδήποτε τέτοια σύνολα έχουν τον ίδιο αριθμό διανυσμάτων ο οποίος αποτελεί

τη διάσταση του δικτυωτού L. Αν B μια βάση ενός δικτυωτού L, τότε συχνά θα γράφουμε L(B) για να δηλώνουμε και τη βάση που το παράγει.

Αν υποθέσουμε ότι $\sum_{i=1}^{n} v_i \epsilon \mathbb{R}^n$ είναι μια βάση του δικτυωτού και $\sum_{i=1}^{n} w_i$ είναι διανύσματα στο χώρο L. Τότε το κάθε w μπορεί να γραφτεί ως γραμμικός συνδυασμός των $\sum_{i=1}^{n} v_i$.

Επομένως μπορούμε να γράψουμε:

$w_1 = a_{11}v_1 + a_{12}v_2 \ldots + a_{1n}\, v_n$

$w_2 = a_{21}v_1 + a_{22}v_2 \ldots + a_{2n}\, v_n$

.

.

.

$w_n = a_{n1}v_1 + a_{n2}v_2 \ldots + a_{nn}\, v_n$, όπου τα $a_{ij} \epsilon Z$

Οι συντελεστές a_{ij} και η βάση v μπορούν να γραφτούν σε μορφή πίνακα

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \boldsymbol{V} = \begin{pmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{n1} & \cdots & v_{nn} \end{pmatrix}$$

Αν εκφραστεί το διάνυσμα w με μορφή εξίσωσης με την βοήθεια των παραπάνω πινάκων έχουμε.

W = AV

Από όπου προκύπτει

$V = A^{-1}W$.

Δηλαδή εκφράσαμε το $\sum_{i=1}^{n} w_i$ ως γραμμικό συνδυασμό ακέραιων συντελεστών που προκύπτουν από τον αντίστροφο του πίνακα A και την βάση v.

Για τον υπολογισμό επομένως του ζητούμενου διανύσματος λαμβάνοντας υπόψιν ότι

I= A A^{-1} από όπου προκύπτει det (I)= det(A)det(A^{-1}) → 1=det(A)det(A^{-1}) (1)

Δεδομένου ότι εξ' ορισμού το Α αποτελείται από ακέραια στοιχεία συνεπάγεται ότι θα έχει και ορίζουσα ακέραιο αριθμό. Αποδεικνύεται ότι και ο A^{-1} έχει ακέραια στοιχεία . Κατά συνέπεια και η ορίζουσα αυτών θα είναι ακέραιος αριθμός.

Κατά συνέπεια ο ακέραιος που ικανοποιεί την (1) για τις ορίζουσες των Α, A^{-1}είναι αριθμός 1 ή ο αριθμός -1 και για τους δύο πίνακες.

Άρα για να προκύπτει δικτύωμα απαραίτητη προϋπόθεση να ισχύει:

Det(A)=±1 (2)

Άμεση συνέπεια του ορισμού ενός μονομοδιακού πίνακα είναι ότι και αντίστροφος του θα είναι επίσης μονομοδιακός πίνακας. Ο αντίστροφος ενός τέτοιου πίνακα υπάρχει πάντα γιατί η ορίζουσα του είναι εξ ορισμού διαφορετική του μηδενός.

Από τα παραπάνω προκύπτει και η πρόταση που ακολουθεί

Αν έχουμε 2 βάσεις $B = \{b_1 . b_2, \dots, b_n .\}$ Και $V = \{v_1, v_2, \dots, v_n .\}$ Που ανήκουν σε ένα δικτύωμα L μπορούν να εκφραστούν με την βοήθεια ενός μονομοδιακού πίνακα U με ακέραια στοιχεία ως εξής:

V=BU

Προκειμένου να διευκολυνθούν οι υπολογισμοί στα δικτυωτά γίνεται συχνά χρήση διανυσμάτων με ακέραιους στις συντεταγμένες τους. Όλα τα δικτυωτά με αυτή την ιδιότητα ονομάζονται **Ακέραια δικτυωτά**.

Στη συνέχεια θα δείξω ένα παράδειγμα που προκύπτει ένα δικτυωτό $L \epsilon \mathbb{R}^3$ με χρήση 3 διανυσμάτων βάσης v_1,v_2,v_3 και τον τρόπο με τον οποίο μπορούμε να υπολογίσουμε ένα ακέραιο δικτυωτό.

Ας θεωρήσουμε τρία διανύσματα v_1=(2,1,3) , v_2=(1,2,0), v_3=(2,-3,-5) που παράγουν ένα τρισδιάστατο πλέγμα $L \epsilon \mathbb{R}^3$ Ο πίνακας Α που παράγεται από αυτά τα διανύσματα είναι :

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{pmatrix}$$

Θεωρούμε $w_1= v_1 + v_3$, $w_2= v_1 – v_2+ 2v_3$, $w_3= v_1 + 2v_2$ τρία νέα διανύσματα.

Για να προκύψουν στην ουσία αυτά τα διανύσματα έχουμε κάνει πολλαπλασιασμό του παραπάνω πίνακα A με τον πίνακα

$$U = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

Αν τώρα εκφράσουμε τα w_1, w_2, w_3 σε μορφή πίνακα θα έχουμε:

$$B = UA = \begin{pmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{pmatrix}$$

Ο πίνακας U είναι μονομοδιακός, γιατί αν υπολογίσουμε την ορίζουσα του θα βρούμε ότι detU=1. Επομένως και τα διανύσματα w_1, w_2, w_3 είναι επίσης μια βάση του L.

Εύκολα υπολογίζεται ότι ο αντίστροφος του U είναι:

$$U^{-1} = \begin{pmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{pmatrix}$$

Με τον τρόπο αυτό έχουμε καταφέρει να εκφράσουμε και τα διανύσματα v_i ως γραμμικό συνδυασμό των w_j γεγονός που προκύπτει από της γραμμές του U^{-1}. Δηλαδή έχουμε:

$v_1= 4w_1-2w_2-w_3$, $v_2 = -2w_1+w_2+w_3$ και $v_3= -3w_1+2w_2+w_3$

Τέλος θα δώσω τον ορισμό του δυϊκού ενός δικτυωτού L ως το σύνολο $\hat{L}$ των διανυσμάτων $x \in \text{span}(L)$ τέτοιο ώστε το εσωτερικό γινόμενο $\langle x,y \rangle$ να είναι ακέραιος για κάθε $y \in L$.

Το δϋικό δικτυωτό $\hat{L}$ ανήκει σε ίδιο διανυσματικό χώρο με το L , όμως τις περισσότερες φορές δεν είναι υποπλέγμα του.

2.1.1. Βασικές έννοιες στα πλέγματα

Στην ενότητα αυτή θα δώσουμε τους ορισμούς από κάποιες χρήσιμες μαθηματικές έννοιες στις αλγεβρικές δομές που βρίσκουν εφαρμογή στα πλέγματα [26]

Ως ομάδα ορίζουμε ένα ζεύγος (G, *) , όπου G είναι ένα σύνολο, και

$$* : G \times G \rightarrow G,\ *(x,y) = x*y$$

Είναι μια πράξη επί (πολλαπλασιασμού) του συνόλου G, για την οποία ικανοποιούνται τα ακόλουθα αξιώματα:

- Η πράξη * είναι **προσεταιριστική,** δηλαδή ισχύει:

  $\forall x, y \in X: \quad x*(y * z) = (x*y) * z$

- Υπάρχει ένα στοιχείο $e_{G,\ ή}\ e \in G$ αν δεν προκαλείται σύγχυση, το οποίο καλείται **ουδέτερο ή ταυτοτικό στοιχείο** της G, τέτοιο ώστε να ισχύει:

  $\forall x \in X: \quad x*e = x = e*x$

- Για κάθε $x \in G$, υπάρχει ένα στοιχείο $x' \in G$, το οποίο καλείται **αντίστροφο ή αντίθετο στοιχείο** του x, έτσι ώστε να ισχύει :

  $\forall x \in G,\ \exists\, x' \in G: \quad x * x' = e = x' * x$

Μια ομάδα (G, *) θα λέμε ότι είναι **αβελιανή ή μεταθετική** αν ισχύει:

- Η πράξη * να είναι **μεταθετική,** δηλαδή:

  $\forall x, y \in X: \quad x * y = y * x$

Άλλη μια σημαντική έννοια είναι αυτή του δακτυλίου, όπου αν θέλαμε να δώσουμε τον ορισμό αυτού θα λέγαμε ότι **δακτύλιος** , στην σύγχρονη αλγεβρική θεωρία αριθμών, είναι η αλγεβρική δομή που αποτελείται από ένα σύνολο R με δύο διμελής πράξεις συμβολικά + (πρόσθεση) και X(πολλαπλασιασμός) στο R. Οι δακτύλιοι έχουν τις παρακάτω ιδιότητες:

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

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

- Υπάρχει πολλαπλασιαστικό ουδέτερο στοιχείο, που συμβολίζεται με το 1, με $1 \neq 0$, τέτοιο ώστε $1 \times a = a \times 1 = a$ για κάθε a R.
- Η πράξη × είναι επιμεριστική ως προς την +. Δηλαδή:

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

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

Οι πιο γνωστοί δακτύλιοι είναι αυτοί των ακεραίων Z_n . Έκανα την εμφάνιση τους ουσιαστικά το 1801 στο περίφημο έργο « Disquitiones Arithmeticae" του gauss. Οι δακτύλιοι αυτοί αποτελούν ένα σημαντικό εργαλείο για την μελέτη διοφαντικών και γενικότερά ιδιοτήτων των ακεραίων.

Ακόμα **σώμα** (αλγεβρικό) ονομάζεται ένας αντιμεταθετικός δακτύλιος διαίρεσης, δηλαδή ένας αντιμεταθετικός δακτύλιος του οποίου κάθε μη μηδενικό στοιχείο έχει πολλαπλασιαστικό αντίστροφο.

Παραδείγματα γνωστών σωμάτων είναι:

- Το σώμα των πραγματικών αριθμών $\mathbb{R}$
- Το σώμα των ρητών αριθμών $\mathbb{Q}$
- Το σώμα των μιγαδικών αριθμών $\mathbb{C}$

Έστω F το σώμα των πραγματικών ή μιγαδικών αριθμών

Με την βοήθεια και των παραπάνω είμαστε σε θέση να δώσουμε και τον ορισμό του διανυσματικού χώρου.

Διανυσματικός χώρος επί ενός σώματος F πραγματικών ή μιγαδικών αριθμών είναι ένα κενό σύνολο V (τα στοιχεία του οποίου θα ονομάζονται διανύσματα) εφοδιασμένο με δύο ακόλουθες πράξεις:

$+ : \quad V \times V \to V$

$(x , y) \longmapsto x + y$ «πρόσθεση»

$\cdot \ : F \times V \to V$

$(\lambda , x) \longmapsto \lambda \cdot x \equiv \lambda x$ «βαθμωτός πολλαπλασιασμός ή γινόμενο»

Οι πράξεις αυτές θα πρέπει να ικανοποιούν τις εξής ιδιότητες:

I. $x + y = y + x , \ \forall x, y \in V$

II. $(x + y) + z = x + (y + z) , \ \forall x, y, z \in V$

III. Υπάρχει ένα στοιχείο $0 \in V$ (μηδενικό διάνυσμα) τέτοιο ώστε $x + 0 = x$, $\forall x \in V$

IV. Για κάθε στοιχείο $x \in V$ υπάρχει ένα στοιχείο $y \in V$ τέτοιο ώστε $x + y = 0$

V. Η μονάδα αποτελεί ουδέτερο στοιχείο δηλαδή:

$1 \cdot x = x , \forall x \in V$

VI. $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x , \forall \lambda, \mu \in F, x \in V$

VII. $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x) , \forall \lambda, \mu \in F, x \in V$

VIII. $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y , \forall \lambda \in F, x, y \in V$

Έτσι για παράδειγμα το R^3 είναι διανυσματικός χώρος επί του R, όπου για παράδειγμα

$$(-3 , 4, 5) + (2, 1 , 3) = (-1 , 5 , 8)$$

και $$-2(3 , 2 , -1) = (-6 , -4 , 2)$$

Αντίστοιχα το C^2 είναι διανυσματικός χώρος επί του C όπου για παράδειγμα

$$(3 + 4i , 2) + (1 + i , 3i) = (4 +5i , 2 + 3i)$$

Και $$2i(3+i , 3) = (-2 +6i , 6i)$$

Τέλος ως **υποχώρος** του V ονομάζεται ένα υποσύνολο W ενός διανυσματικού χώρου V επί του F εάν το W είναι διανυσματικός χώρος επί του F με τις ίδιες πράξεις της πρόσθεσης και βαθμωτού παλλαπλασιασμού του V. Θα συμβολίζεται με $W < V$.

Γραμμικός συνδυασμός

Έστω V ένας διανυσματικός χώρος και $v_1, v_2,.., v_n \in V$. Ένας γραμμικός συνδυασμός είναι ένα διάνυσμα της μορφής:

$\lambda_1 v_1 + \lambda_2 v_2 + ..+ \lambda_n v_n , , \lambda_\iota \in F.$

Το σύνολο όλων των γραμμικών συνδυασμών του συνόλου $\{ v_1, v_2,.., v_n \}$συμβολίζεται ως:

$\text{span} \{ v_1, v_2,.., v_n \} = \{ \lambda_1 v_1 + \lambda_2 v_2 + ..+ \lambda_n v_n : \lambda_\iota \in F \}$ ή αλλιώς

$< v_1, v_2,.., v_n >$

Παράδειγμα: Αν θεωρήσουμε ένα διάνυσμα $V = F^3$. τότε

$$(5 , 6, 3) = 2 (2 , 1, 1) + 1 (1, 4, 1)$$

Άρα $(5 , 6, 3) \in \text{span} \{ (2 , 1, 1) , (1, 4, 1) \}$.

Γραμμικός ανεξάρτητα – εξαρτημένα

Τα διανύσματα $v_1, v_2,.., v_n$ ενός διανυσματικού χώρου V λέμε ότι είναι **γραμμικώς ανεξάρτητα** εάν ο μοναδικός τρόπος για να γραφτεί το $0 \in V$ ως $\alpha_1v_1 + \alpha_2v_2 +\ldots+ \alpha_nv_n = 0$, $\alpha_i \in F$ είναι όταν $\alpha_1= \alpha_2 =..= \alpha_n = 0 \in F$.

Διαφορετικά **γραμμικώς εξαρτημένα** είναι όταν υπάρχουν $\alpha_1, \alpha_2, \ldots, \alpha_n$ όχι όλα μηδέν τέτοια ώστε: $\alpha_1v_1 + \alpha_2v_2 +\ldots+ \alpha_nv_n = 0$

Βάση – διάσταση

Τέλος θα ορίσουμε ένα πολύ σημαντικό υποσύνολο ενός διανυσματικού χώρου, την βάση του, το οποίο θα έχει την ιδιότητα ότι κάθε στοιχείο του διανυσματικού χώρου εκφράζεται κατά μοναδικό τρόπο ως γραμμικός συνδυασμός των στοιχείων της βάσης.

Το πλήθος των στοιχείων σε μια πεπερασμένη βάση θα ονομαστεί η διάσταση του διανυσματικού χώρου και αποτελεί μια σημαντική αναλλοίωτη ποσότητα του.

Μια **βάση** ενός διανυσματικού χώρου V είναι ένα υποσύνολο B του V με τις ιδιότητες:

- Το B είναι γραμμικώς ανεξάρτητο
- Το B παράγει τον V, δηλαδή V = span (B)

Από τις ιδιότητες που πρέπει να ικανοποιεί μια βάση γίνεται άμεσα αντιληπτό ότι η βάση ενός διανύσματος δεν είναι μοναδική. Ως ένα παράδειγμα μπορούμε να πούμε ότι οι βάσεις: $B_1 = \{ (1,0) , (0,1) \}$ και $B_2 = \{ (1,2) , (-3,5) \}$ αποτελούν 2 βάσεις του διανυσματικού χώρου R^2.

Ακόμη ως κανονική βάση ορίζεται το σύνολο $B= \{ e_1, e_2,.., e_n \}$ που δημιουργείται από τα διανύσματα $e_1 = \{1, 0 , \ldots,0\}$, $e_2 = \{0, 1 , \ldots,0\}$, …, $e_n = \{0, 0 , \ldots,1\}$

Η **διάσταση** ενός διανυσματικού χώρου πεπερασμένης διάστασης είναι το πλήθος των στοιχείων μιας βάσης του. Αν ο V δεν είναι πεπερασμένης διάστασης τότε λέμε ότι είναι άπειρης διάστασης.

Ελάχιστης απόσταση (Minimum Distance): Η ελάχιστη απόσταση ενός δικτυωτού L δίνεται από $\lambda_1(L)$ και είναι η ελάχιστη απόσταση δύο διακριτών σημείων του δικτυωτού L. Είναι ίση με το μήκος του πιο μικρού μη μηδενικού διανύσματος του δικτυωτού L.

2.1.2. Κανονικοποίηση gram-schmidt

Στην ενότητα αυτή θα εξετάσουμε το πρόβλημα της κατασκευής ορθοκανονικής βάσης από μια δεδομένη βάση. [27]

Για την αντιμετώπιση αυτού του προβλήματος χρησιμοποιούμε την μέθοδο Gram- Schmidt.

Έστω V ένας διανυσματικός χώρος με εσωτερικό γινόμενο και $\beta = \{v_1, v_2 \dots, v_n\}$ μια βάση του. Από αυτήν θα κατασκευάσουμε μια νέα βάση $\beta^* = \{v_1^*, v_2^* \dots, v_n^*\}$ με την ιδιότητα τα διανύσματα να είναι μεταξύ τους κάθετα, και να είναι μοναδιαία, και τέτοια ώστε [v1,v2,…,vn]= [$v_1^*, v_2^* \dots, v_n^*$].

Η διαδικασία που ακολουθείται είναι:

1. Θέτουμε v_1^*= v_1
2. Υπολογίζουμε το u_2 ως εξής:

   $v_2^* = v_2 - \mu_{2,1} v_1^*$

3. Με όμοιο τρόπο υπολογίζουμε τα u_2 , u_3 κ.τ.λ. ως εξής:

   $v_3^* = v_3 - \mu_{3,1} v_1^* - \mu_{3,2} v_2^*$

4. Τέλος διαιρούμε κάθε διάνυσμα με την νόρμα του για να γίνει μοναδιαίο.

Όπου $\mu_{i,j}$ έχουμε το σχετικός συντελεστής προβολής . Δηλαδή $\mu_{i,j} = \frac{v_i \cdot v_j^*}{\left\| v_j^* \right\|^2}$

2.1.3. Hermite Normal Form – HNF (κανονική Ερμητιανή Μορφή πίνακα)

Για την αντιμετώπιση πολλών υπολογιστικών προβλημάτων στην θεωρία πλεγμάτων έχει εισαχθεί η κανονική Ερμητιανή Μορφή πίνακα ακεραίων ή ρητών που είναι μια ειδική βάση του πλέγματος.

Δίνοντας τον ορισμό της HNF θα μπορούσαμε να ισχυριστούμε ότι κάθε τετραγωνικός αντιστρέψιμος πίνακας $B = [b_1, b_2, .., b_n] \in R^{nxn}$ είναι HNF αν και μόνο αν:

- Ο B είναι άνω τριγωνικός
- Οι διαγώνιες τιμές είναι μεγαλύτερες του μηδενός

  Για όλα τα $1 \leq i < j \leq n$ ισχύει $O \leq B_{ij} \leq B_{ii}$

Επιπλέον μπορεί πολύ εύκολα να αποδειχθεί ότι η HNF είναι μοναδική. Δηλαδή αν 2 πίνακες B και B' είναι σε HNF και παράγουν το ίδιο πλέγμα L(B) = L(B') τότε θα ισχύει και B=B' .

Μοναδική εξαίρεση μπορεί να υπάρχει στον αριθμό των μηδενικών στηλών στο τέλος του πίνακα.

Συνοψίζοντας μπορούμε να πούμε ότι ο πίνακας H είναι η HNF ενός πίνακα B αν L(H) = L(B) τότε ο H δεν περιέχει μηδενικές στήλες.

Το πρόβλημα του υπολογισμού της HNF ενός πίνακα ρητών αριθμών $B \in Q^{mxn}$ γίνεται αναγωγή σε πρόβλημα υπολογισμού HNF ενός ακέραιου πίνακα ως εξής:

- Θεωρούμε με M το ελάχιστο κοινό πολλαπλάσιο όλων των παρονομαστών των στοιχείων του πίνακα B.
- Υπολογίζουμε την HNF ενός νέου πίνακα ακεραίων $M \cdot B \in Z^{mxn}$
- Και τελικά παράγεται ο πίνακας $M^{-1} \cdot B$

Όταν ο πίνακας B είναι πίνακας με στοιχεία ακέραιους αριθμούς τότε για τον υπολογισμό του HNF εξετάζουμε απευθείας έναν αλγόριθμο υπολογισμού της HNF πινάκων πλήρους τάξης γραμμών και εν συνεχεία κάνουμε προσαρμογή του αλγορίθμου σε τυχαίους πίνακες. [28]

2.2. Κβαντικοί υπολογισμοί

Στην ενότητα αυτή θα αναφερθούμε σε μεθόδους κβαντικών υπολογισμών και συμβολισμών, όπως είναι για παράδειγμα οι πίνακες πυκνότητας. Επίσης θα δώσουμε έμφαση σε αλγορίθμους που χρησιμοποιούνται στην κβαντική επιστήμη και κατ' επέκταση στην κβαντική κρυπτογραφία.

2.2.1. Πίνακες πυκνοτήτων

Αν θεωρήσουμε μια διακριτή μεταβλητή X, όπου οι τιμές τις αντλούνται από ένα συγκεκριμένο αλφάβητο K μεγέθους n. Τότε με τον συμβολισμό |X| θα ορίσουμε το μέγεθος του αλφαβήτου και ως $P_X(\cdot)$ την κατανομή αυτής της μεταβλητής. Ακόμη με P_X θα συμβολίζουμε την πιθανότητα η τυχαία μεταβλητή να πάρει ένα τυχαίο σύμβολο $\chi \in K$. Σε πολλές περιπτώσεις η παραπάνω πιθανότητα γράφεται και ως $p_x = p(x) = P(X = x) = P_X(x)$.

Επίσης είναι εφικτό να έχουμε και συσχέτιση της μεταβλητής X με μια άλλη μεταβλητή Y. Οπότε πλέον θα έχουμε μια νέα τυχαία κατανομή $P_{XY}(\chi,y)$. Σε αυτή την περίπτωση οδηγούμαστε στην δεσμευμένη πιθανότητα με συμβολισμό $P_{X|Y}(\chi|y)$, όπου είναι η πιθανότητα η τυχαία μεταβλητή να πάρει την τιμή x δεδομένου ότι η Y θα πάρει την τιμή y.

Ένα πρόβλημα που συναντάμε στην περίπτωση που έχουμε 2 κβαντικά συστήματα A, B και θέλουμε να αναπαραστήσουμε την κατάσταση ενός qubit μέσα από πολλά θα παρουσιάζουν μια αρθρωτή κατάσταση $|\Psi >_{AB}$. Με δεδομένο ότι δεν είμαστε σε θέση να γνωρίζουμε αν η κατάσταση αυτή έχει προέλθει από τανιστικό γινόμενο των 2 επιμέρους καταστάσεων $|\Psi>_A$, $|\Psi >_B$ δεν μπορούμε να απομονώσουμε κάποιο από τα 2 qubits που πιθανόν μας ενδιαφέρει. Ακόμη άλλο ένα πρόβλημα που μπορεί να βρεθούμε αντιμέτωποί είναι ότι στην περίπτωση που κάνουμε μια μέτρηση, που είναι μια πιθανοκρατική διαδικασία, προετοιμάζουμε τις διάφορες καταστάσεις με κάποια πιθανότητα. Οπότε αν θέλουμε να απομονώσουμε μια κατάσταση θα πρέπει να λάβουμε υπόψιν και την αντίστοιχη πιθανότητα της, κάτι που σε ορισμένες περιπτώσεις δεν είναι εύκολο.

Έτσι για την επίλυση αυτών των προβλημάτων έχει εισαχθεί η έννοια του πίνακα πυκνοτήτων $\rho = |\Psi >< \Psi|$ ο οποίος έχει τάξη 1 και ακριβώς μια μη-μηδενική ιδιοτιμή με αντίστοιχη ιδιοκατάσταση $|\Psi >$.

Παράδειγμα εφαρμογής: Θεωρούμε 2 ενεργειακές καταστάσεις $|\Psi >_1$ και $|\Psi >_2$ με πιθανότητες $p_1=p_2=1/2$. Δεν μπορούμε με βεβαιότητα να περιγράψουμε το σύστημα με την

υπέρθεση των 2 καταστάσεων διότι δεν γνωρίζουμε αν είναι οι μοναδικές καταστάσεις που μπορεί να λάβει. Οπότε ο πλέον σωστός τρόπος για την περιγραφή του είναι μέσω της μίξης αυτών των καταστάσεων. Η περιγραφή του μπορεί να γίνει επομένως μέσω του πίνακα πυκνοτήτων ρ με την βοήθεια του τύπου.

$$\rho = \frac{1}{2}|\Psi_1 > \langle \Psi_1 \left| + \frac{1}{2}\Psi_2 \right| \rangle < \Psi_2|$$

Γενικεύοντας τον παραπάνω τύπο σε κατάσταση $|\Psi_X >$ με πιθανότητα p_x το τελικό σύστημα θα είναι σε κατάσταση :

$$\rho = \sum_x p_x |\Psi_X > < \Psi_X|$$

Στην περίπτωση που θέλουμε να μετρήσουμε το σύστημα με την τυπική βάση και το σύστημα βρίσκεται σε κατάσταση $|\Psi_j >$ με πιθανότητα p_j τότε οι πιθανότητες των αποτελεσμάτων είναι:

$$q_0 = \sum_j p_j q_{0|j}$$

Και

$$q_1 = \sum_j p_j q_{1|j}$$

Αν επεκτείνουμε τον παραπάνω τύπο με βάση τον φορμαλισμό του πίνακα των πυκνοτήτων έχουμε:

$$q_0 = \sum_j p_j q_{0|j} = \sum_j p_j < 0 \| \Psi_j > < \Psi_j \| 0 > = \langle 0 | \left(\sum_j p_x |\Psi_X > < \Psi_X| \right) |0\rangle = \langle 0|\rho|0\rangle$$

Στην γενική περίπτωση που θέλουμε να μετρήσουμε το ρ στην βάση $\{| b_j >\}_j$ θα πάρουμε ως αποτέλεσμα το j με πιθανότητα:

$$q_j = \langle b_j|\rho|b_j\rangle$$

Για να μπορέσει ένα πίνακας πυκνοτήτων να αναπαριστά μια έγκυρη κβαντική κατάσταση θα πρέπει να είναι θετικά ημιορισμένος και το ίχνος του tr(ρ) να είναι ίσο με 1.

2.2.2. Αλγόριθμος του Groven

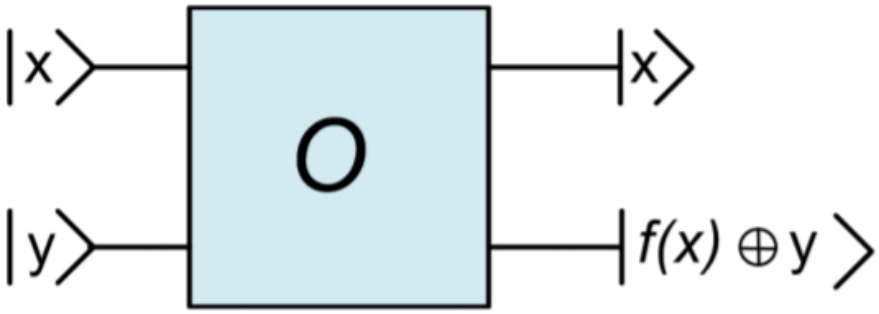
Αρχή λειτουργίας του αλγορίθμου Groven είναι ότι όταν του παρουσιάζετε ένας αριθμός, αυτός επεξεργάζεται τον αριθμό και λέει αν είναι αυτός που ψάχνετε ή όχι [29]. Το σύστημα αυτό σε έναν κλασικό υπολογιστή μπορεί να είναι ένας καταχωρητής όπου έχουμε αποθηκεύσει τον αριθμό που ψάχνουμε να βρούμε και ένα κύκλωμα λογικών πυλών, που συγκρίνει κάθε αριθμό που έρχεται στην είσοδο με τον αποθηκευμένο αριθμό. Το σύστημα αυτό, που το θεωρούμε ως ένα μαύρο κουτί, ονομάζεται στη διεθνή βιβλιογραφία oracle. [30]

Ας περιγράψουμε τώρα το πρόβλημα της έρευνας μίας μη δομημένης βάσης δεδομένων από έναν κλασικό υπολογιστή με έναν απλό μαθηματικό τρόπο [29]. Θεωρούμε ότι έχουμε N στοιχεία τα οποία αποτελούν τη βάση και ότι έχουμε αντιστοιχίσει σε κάθε στοιχείο έναν αριθμό από 0 έως N-1. Το στοιχείο που αντιστοιχεί στον αριθμό k συμβολίζεται με x_k. Το oracle είναι μία συνάρτηση f(x) η οποία παίρνει μόνο τις τιμές 0 και 1. Αν το στοιχείο που ψάχνουμε είναι το x_i, τότε:

$$f(x)=\begin{cases} 1 & \text{αν } x = x_i \\ 0 & \text{αν } x \neq x_i \end{cases}$$

Δηλαδή, παρουσιάζουμε ένα στοιχείο στο oracle και αν είναι αυτό που ψάχνουμε τότε το oracle αποκρίνεται με 1, αν όχι με 0

Αντιστοιχίζουμε κάθε ένα από τα στοιχεία με μία από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή που περιλαμβάνει n qubits. Δηλαδή, το στοιχείο που αντιστοιχεί στη βασική κατάσταση |00⋯0101> που στη δεκαδική αναπαράσταση είναι η |5> συμβολίζεται με $|x_5>$. Το κβαντικό oracle, δηλαδή το σύστημα που διακρίνει αν ένα στοιχείο είναι αυτό που ψάχνουμε ή όχι, είναι το κβαντικό κύκλωμα που συμβολίζεται με O και φαίνεται στο παρακάτω σχήμα .



Σχήμα 2.2: Το κβαντικό oracle

Δεν χρειάζεται να γνωρίζουμε τις κβαντικές πύλες από τις οποίες αποτελείται το κβαντικό oracle. Αυτό που χρειάζεται να γνωρίζουμε είναι η δράση του στον κβαντικό καταχωρητή. Αν δηλαδή το κβαντικό oracle δράσει στον κβαντικό καταχωρητή που βρίσκεται στην κατάσταση |yx> τότε:

$$|x\,y\rangle = |x\rangle\,|y\rangle \xrightarrow{o} |x\rangle\,|f(x)\oplus y\rangle$$

όπου, με $\oplus$ συμβολίζεται η πρόσθεση με βάση το 2 (mod2). Το qubit |y> ονομάζεται qubit του oracle. Όπως και στο κλασικό oracle, η f(x) παίρνει τιμή |1> αν το x είναι το στοιχείο που ψάχνουμε, αλλιώς παίρνει τιμή |0> .

Τι κάνει λοιπόν το κβαντικό oracle; Το κβαντικό oracle δρα στις βασικές καταστάσεις |x> που αντιστοιχούν σε στοιχεία της μη δομημένης βάσης δεδομένων. Αν η βασική κατάσταση δεν αντιστοιχεί στο στοιχείο που ψάχνουμε, την αφήνει όπως ήταν, αν όμως αντιστοιχεί, τότε τη «σημαδεύει» αλλάζοντας το πρόσημο της.

Τα βήματα του αλγορίθμου του Grover είναι:

Αρχικά θέτουμε έναν κβαντικό καταχωρητή που περιλαμβάνει n qubits σε υπέρθεση βασικών καταστάσεων. Το πλάτος πιθανότητας να είναι ίδιο για κάθε βασική κατάσταση. Για να το πετύχουμε αυτό, ξεκινάμε με τον κβαντικό καταχωρητή στην κατάσταση όπου όλα τα qubits είναι |0> , δηλαδή στην κατάσταση |000⋯000> . Στη συνέχεια δρούμε στο κάθε qubit με μία κβαντική πύλη Hadamard (H). Η κατάσταση του κβαντικού καταχωρητή είναι:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{J=0}^{N-1} |x_j\rangle$$

Η |S> είναι η υπέρθεση των N βασικών καταστάσεων, όπου N= $2^n - 1$. Αντιστοιχίζουμε κάθε βασική κατάσταση με ένα στοιχείο της μη δομημένης βάσης δεδομένων. Έστω ότι ψάχνουμε για το στοιχείο που αντιστοιχεί στην $|x_i>$.

Βήμα 1ο. Θέτουμε b=1, όπου b είναι ο αριθμός των επαναλήψεων εκτέλεσης των βημάτων που ακολουθούν.

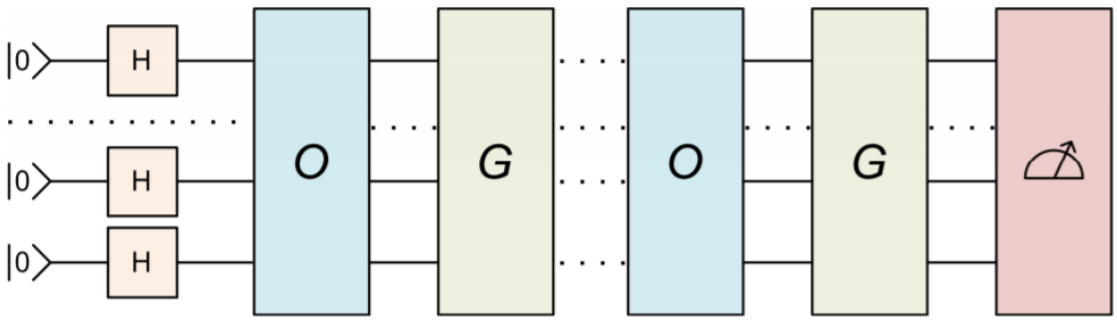
Βήμα 2ο Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i|$

Βήμα 3ο Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{G} = 2|s\rangle\langle s| - \hat{I}$

Εάν ο αριθμός επαναλήψεων b είναι μεγαλύτερος από ή περίπου ίσος με $\left((\pi/4)\sqrt{N}\right)-0{,}5$

προχωράμε στο 4ο Βήμα, αν ΟΧΙ αυξάνουμε το b κατά ένα (b= b+1)

Βήμα 4ο Μετράμε την κατάσταση του κβαντικού καταχωρητή. Είναι πρακτικώς βέβαιο ότι θα βρίσκεται στην κατάσταση $|x_i>$ που αντιστοιχεί στο στοιχείο που ψάχνουμε



Σχήμα 2.3: Το κβαντικό κύκλωμα του αλγορίθμου του Grover

2.2.3. Αλγόριθμος του Shor

Ο κβαντικός αλγόριθμος του Shor μπορεί να χρησιμοποιηθεί για την εύρεση της περιόδου περιοδικών συναρτήσεων και για την ανάλυση ενός αριθμού σε γινόμενο πρώτων παραγόντων. [31] Για να το επιτύχουμε αυτό, θα υπολογίσουμε την περίοδο της συνάρτησης $f_{n,a}(x)=\alpha^x \pmod n$.

Τα βήματα του κβαντικού αλγορίθμου του Shor είναι:

Βήμα 1ο. Επιλέγεται ένας ακέραιος αριθμός q τέτοιος ώστε $2n^2 \leq q \leq 3n^2$.

Βήμα 2ο. Επιλέγεται τυχαία ένας ακέραιος αριθμός α που είναι πρώτος ως προς τον n

Βήμα 3ο. Ένας κβαντικός καταχωρητής, ο Reg, αποτελείται από δύο καταχωρητές, που ονομάζονται Reg1 και Reg2, οι οποίοι βρίσκονται στην κατάσταση |0> . Η κατάσταση του Reg, η |ψ> , είναι:

|ψ> =|0,0>

Βήμα 4ο. Φέρνουμε τον Reg1 σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως q-1. Δεν δρούμε στον Reg2. Μετά από αυτό, η κατάσταση του Reg δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, 0\rangle$$

Βήμα 5ο. Στη συνέχεια, με χρήση της κβαντικής παραλληλίας υπολογίζεται η τιμή της $f_{n,a}(x)$ για κάθε x και τα αποτελέσματα καταγράφονται στον Reg2 ο οποίος κρατά πλέον την υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Τώρα η κατάσταση του Reg δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, a^x \pmod n\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, f_{n,a}(x)\rangle$$

Οι καταχωρητές Reg1 και Reg2 βρίσκονται πλέον σε κβαντική διεμπλοκή.

Βήμα 6ο. Μετράται η κατάσταση του Reg2. Ο Reg2 βρίσκεται σε υπέρθεση όλων των τιμών της $f_{n,a}(x)$, όμως το αποτέλεσμα της μέτρησης θα δώσει μόνο μία τιμή της συνάρτησης, ας πούμε την k. Δηλαδή, μετά τη μέτρηση ο Reg2 βρίσκεται στην κατάσταση |κ>. Η μέτρηση της κατάστασης του Reg2 καθορίζει την κατάσταση του Reg1. Δηλαδή, εξαιτίας της κβαντικής διεμπλοκής στον Reg1 θα βρίσκονται πια μόνο οι αριθμοί x για τους οποίους ισχύει: $f_{n,a}(x)=\alpha^x \pmod n=k$. Οι αριθμοί αυτοί συμβολίζονται με x' και αποτελούν ένα σύνολο A που περιγράφεται ως εξής:

$$A = \{x' : a^{x'} (\mathrm{mod} n) = k\}$$

Έστω ότι ||A|| είναι ο αριθμός των στοιχείων του συνόλου A. Μετά τη μέτρηση η κατάσταση του Reg δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} |x', k\rangle$$

Δηλαδή, αθροίζονται οι καταστάσεις που ανήκουν στο σύνολο Α.

Βήμα 7ο. Ο κβαντικός μετασχηματισμός Fourier δρα στον Reg1, ενώ το περιεχόμενο του Reg2 παραμένει αμετάβλητο. Ο κβαντικός μετασχηματισμός Fourier μετασχηματίζει κάθε κατάσταση |x'> σε μία υπέρθεση καταστάσεων που δίνεται από:

$$|x'\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x' c}{q}} |c\rangle$$

Μετά την εφαρμογή του κβαντικού μετασχηματισμού Fourier η κατάσταση του Reg είναι:

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x' c}{q}} |c, k\rangle$$

Βήμα 8ο. Μετράται η κατάσταση του Reg1. Το αποτέλεσμα της μέτρησης δίνει μία μόνο τιμή, την c' , η οποία είναι κάποιο ακέραιο πολλαπλάσιο λ του q/r, όπου r είναι η περίοδος που πρέπει να προσδιοριστεί, δηλαδή:

$$c' = \lambda \frac{q}{r}$$

Βήμα 9ο. Τα βήματα 3 έως και 8 επαναλαμβάνονται περίπου log(q) φορές. Η επανάληψη αυτή δίνει αρκετά δείγματα πολλαπλασίων του 1/r, δηλαδή, δίνει τιμές λ_1/r, λ_2/r, λ_3/r, … όπου λ_i είναι διάφοροι ακέραιοι, ώστε να είναι δυνατός ο υπολογισμός της r.

Αφού προσδιοριστεί η r, οι δύο πρώτοι αριθμοί που το γινόμενό τους δίνει τον n προσδιορίζονται υπολογίζοντας τον ΜΚΔ του n και του ($\alpha^{r/2}$ - 1), και τον ΜΚΔ του n και του ($\alpha^{r/2}$ + 1).

2.3. Αλγόριθμοι κρυπτογραφίας

Τέλος θα παρουσιάσουμε τους αλγόριθμους που βρίσκουν εφαρμογή ειδικότερα στην κρυπτογραφία. Συγκεκριμένα θα αναφερθούμε σε εκείνους τους αλγόριθμους που χρησιμοποιούνται κατά την πραγματοποίηση αυτής της εργασίας

2.3.1. Αλγόριθμος Δέντρων bonsai

Σε αυτήν την ενότητα περιγράφουμε το πλαίσιο και τις κύριες τεχνικές για την ανάπτυξη δέντρων μπονσάι. Υπάρχουν τέσσερις βασικές αρχές: μη κατευθυνόμενη ανάπτυξη,

ελεγχόμενη ανάπτυξη, επέκταση του ελέγχου της αυθαίρετης νέας ανάπτυξης και έλεγχος τυχαιοποίησης.

Μη κατευθυνόμενη ανάπτυξη

Η άμεση ανάπτυξη είναι χρήσιμη κυρίως για να επιτρέψει σε έναν προσομοιωτή να ενσωματώσει ένα υποκείμενο πρόβλημα πρόκλησης (δηλαδή, SIS ή LWE) σε ένα δέντρο. Αυτό γίνεται απλά σχεδιάζοντας νέα ομοιόμορφα τυχαία και ανεξάρτητα δείγματα $a_i \epsilon z_q^n$ από τα προβλήματα κατανομής και την ομαδοποίησή τους (ή την προσάρτησή τους) σε έναν έλεγχο ισοτιμίας μήτρας Α.

Συγκεκριμένα παίρνουμε κάποιον αυθαίρετο πίνακα $\boldsymbol{A} \epsilon z_q^{nxm}$ για m ≥ 0 και $\boldsymbol{A'}$ μια τυχαία επέκταση του **A** τέτοια ώστε $\boldsymbol{A'} = \boldsymbol{A}||\overline{\boldsymbol{A}}\ \epsilon\ z_q^{nxm'}$ για $m' > m$.

Από την παραπάνω συνθήκη γίνεται εύκολα ορατό ότι το $\Lambda^{\perp}(\boldsymbol{A'}) \subseteq Z^{m'}$ είναι μιας υψηλότερης διάστασης υπερπλέγμα σε σχέση με το $\Lambda^{\perp}(\boldsymbol{A}) \subseteq Z^{m}$ όταν το τελευταίο υψώνεται στο $Z^{m'}$.

Έχουμε ότι για κάθε $v \epsilon \Lambda^{\perp}(A)$ το διάνυσμα $v' = v||\boldsymbol{0} \epsilon\ Z^{m'}$ είναι εντός της βάσης $\Lambda^{\perp}(A')$ επειδή ισχύει $\boldsymbol{A'}v' = \boldsymbol{A}v = \boldsymbol{0}\ \epsilon\ z_q^n$.

Επιπλέον έχουμε τις στήλες των διανυσμάτων $\boldsymbol{A'}$ να μπορούν να ταξινομηθούν αυθαίρετα που μας βοηθάει να μπορεί να γίνει η καταχώρηση των διανυσμάτων στην βάση που μεταβάλλεται με αντίστοιχο τρόπο. Σύμφωνα με το παρακάτω:

$\Lambda^{\perp}(A' \cdot P) = P \cdot \Lambda^{\perp}(A')$

Για κάθε μήτρα μετάθεσης

$\boldsymbol{A'}P \epsilon \{0,1\}^{m' X m'}$ επειδή $(\boldsymbol{A'P})x = \boldsymbol{A'}(\boldsymbol{P}x)\ \epsilon\ z_q^n$ για όλα τα $x = z^{m'}$

Ελεγχόμενη ανάπτυξη

Είμαστε σε θέση να ισχυριστούμε ότι έχουμε γνώση του πλέγματος αν έχουμε βρει μια σχετικά καλή (δηλαδή σύντομη) βάση για το πλέγμα.

Η παρακάτω πρόταση αναφέρεται στον τρόπο με τον οποίο μπορούμε να δημιουργήσουμε ένα τυχαίο πλέγμα πλήρως ελεγχόμενο.

Υπάρχει μια προκαθορισμένη σταθερά C > 1 και ένας πιθανοτικός αλγόριθμος πολυωνιμικού χρόνου GenBasis(1^n,1^m,q) ο οποίος για «poly(n)-bounded» m≥Cn lgq δίνει ως έξοδο $\boldsymbol{A}\epsilon z_q^{nxm}$ και $\boldsymbol{S}\epsilon z^{mxm}$ τέτοια ώστε να ισχύουν τα κάτωθι:

- η κατανομή του A βρίσκεται εντός της negl(n) statistical distance of uniform.
- S είναι μια βάση του $\Lambda^{\perp}(\boldsymbol{A})$ και
- $\|\tilde{S}\| \leq \tilde{L} = O(\sqrt{nlogq})$

Επέκταση του ελέγχου της αυθαίρετης νέας ανάπτυξης

Στο σημείο αυτό θα περιγράψουμε τον τρόπο που μπορούμε να επεκτείνουμε τον έλεγχο ενός δικτυωτού πλέγματος σε ένα άλλο υψηλότερης διάστασης χωρίς βέβαια αυτό να έχει αντίκτυπο στην ποιότητα της προκύπτουσας βάσης.

Βασική προϋπόθεση για να συμβαίνει αυτό είναι η ισχύς του παρακάτω λήμματος.

Λήμμα 1 : Υπάρχει ένας ντετερμινιστικός αλγόριθμος πολυώνυμου χρόνου ExtBasis με τις ακόλουθες ιδιότητες:

Δοθέντος ενός αυθαίρετου $\mathbf{A}\epsilon z_q^{nxm}$,του οποίου οι στήλες δημιουργούνται από την ομάδα z_q^n, μιας αυθαίρετης βάσης $\mathbf{S}\epsilon z^{mxm}$ του $\Lambda^{\perp}(\mathbf{A})$ και ενός αυθαίρετου $\overline{\mathbf{A}} \epsilon z_q^{nxm}$ ο αλγόριθμος ExtBasis$(S, \mathbf{A}' = \mathbf{A}||\overline{\mathbf{A}})$ δίνει ως έξοδο μια βάση $\mathbf{S}'$ του $\Lambda^{\perp}(\mathbf{A}') \subseteq Z^{m+\bar{m}}$ τέτοιο ώστε $\|\tilde{S}'\| = \|\tilde{S}\|$

Επιπλέον το ίδιο ισχύει και για κάθε δεδομένη μετάθεση των στηλών του A′.

Όπως είναι για παράδειγμα αν οι στήλες του $\overline{A}$ προσαρτώνται και προστίθενται στο A.

Για να αποδείξουμε αυτό το λήμμα εργαζόμαστε ως εξής.

Λαμβάνουμε ένα $m' = m + \bar{m}$. Ο αλγόριθμος ExtBasis(S, A') δίνει ως έξοδο την βάση S'σύμφωνα με τον παρακάτω τύπο:

$$S' = \begin{pmatrix} S & W \\ 0 & I \end{pmatrix} \in Z^{m' x\, m'}$$

Όπου $I \in Z^{\bar{m}\, x\, \bar{m}}$ είναι η μοναδιαία βάση και W είναι μια αυθαίρετη λύση την εξίσωσης

$$AW = -\overline{A} \in Z_q^{nx\bar{m}}$$

Σημειώνουμε ότι το W υπάρχει από την υπόθεση ότι το A αναπαράγει την Z_q^n, και μπορεί να υπολογιστεί χρησιμοποιώντας αποτελεσματικά, π.χ., την Gauss elimination.

Στην συνέχεια θα αναλύσουμε την S′ ως εξής:

Ισχύει ότι $\mathrm{A'S'} = \mathrm{AS}\,||(\mathrm{AW} + \bar{\mathrm{A}}) = 0 \in Z^{n\,x\,m'}$, με βάση την παραδοχή που έχουμε κάνει για το S και τον τρόπο κατασκευής του W, έτσι το $\mathrm{S'} \subset \Lambda^{\perp}(\mathrm{A'})$. Εξάλλου το $\mathrm{S'}$ είναι στην πραγματικότητα μια βάση $\Lambda^{\perp}(\mathrm{A'})$.

Ακολούθως λαμβάνουμε αυθαίρετα ένα $v' = v\,||\,\bar{v} \in \Lambda^{\perp}(\mathrm{A'})$ με το $\mathrm{v} \in Z^{m}$ και το $\bar{v} \in Z^{\bar{m}}$ και παίρνουμε:

$$0 = \mathrm{A'v'} = \mathrm{Av} + \bar{\mathrm{A}}\bar{\mathrm{v}} = \mathrm{Av} - (\mathrm{AW})\bar{\mathrm{v}} = \mathrm{A}(\mathrm{v} - \mathrm{W}\bar{\mathrm{v}}) \in \mathrm{Z_q^n}$$

Έτσι $(\mathrm{v} - \mathrm{W}\bar{\mathrm{v}}) \in \Lambda^{\perp}(\mathrm{A'})$, οπότε με βάση την παραδοχή ότι στην βάση S υπάρχει κάποιο $\mathrm{z} \in Z^{m}$ τέτοιο ώστε $\mathrm{Sz} = \mathrm{v} - \mathrm{W}\bar{\mathrm{v}}$ λαμβάνουμε ένα $z' = z\,||\,\bar{v} \in Z^{m+\bar{m}}$. Με βάση την κατασκευή της βάσης έχουμε:

$\mathrm{S'z'} = (\mathrm{Sz} + \mathrm{W}\bar{\mathrm{v}})\,||\,\bar{\mathrm{v}} = \mathrm{v}\,||\,\bar{\mathrm{v}} = \mathrm{v'}$

Άρα επειδή το $\mathrm{v'} \in \Lambda^{\perp}(\mathrm{A'})$ συνεπάγεται ότι και το $\mathrm{S'}$ είναι μια βάση του $\Lambda^{\perp}(\mathrm{A'})$.

Έπειτα επιβεβαιώνουμε ότι $\|\widetilde{S'}\| = \|\widetilde{S}\|$. Πράγματι από τον τρόπο που έχει σχεδιαστεί η $\mathrm{S'}$και από τον ορισμό την ορθογωνιοποιησης Gram-Schmidt είναι εύκολο να ελέγξουμε ότι: $\widetilde{S'} = \begin{pmatrix} \tilde{S} & 0 \\ 0 & \mathrm{I} \end{pmatrix}$, επειδή το S είναι full rank (δηλαδή το lattice rank είναι ίσο με lattice dimension).

Για το τελευταίο μέρος του λήμματος υπολογίζουμε την $\mathrm{S'}$για $\mathrm{A'} = \mathrm{A}\,||\,\bar{\mathrm{A}}$ με τον τρόπο που υπολογίσαμε παραπάνω και βγάζει ως έξοδο $\mathrm{S''} = \mathrm{PS'}$ ως βάση για $\Lambda^{\perp}(\mathrm{A'} \cdot \mathrm{P})$, όπου P είναι δοθέν πλέγμα μετάθεσης.

Το μήκος με βάση την ορθογωνιοποιηση Gram-Schmidt και σε αυτή την περίπτωση παραμένει αμετάβλητο, δηλαδή $\widetilde{s_i''} = \widetilde{s_i'}$, επειδή το P είναι ορθογώνιο προκύπτει ως εκ τούτου ότι και οι ορθογώνιες μήτρες της QR παραγοντοποίησης στα $\mathrm{S'}$ και $\mathrm{PS'}$είναι ακριβώς οι ίδιες.

Βελτιστοποίηση με την βοήθεια δειγματοληψίας από Gaussian κατανομή μέσω έμμεσης επέκτασης.

Σε πολλές από τις κρυπτογραφικές εφαρμογές μας, ένα μοτίβο σχεδίασης είναι να επεκτείνουμε μια βάση S διάστασης m του πλέγματος $\Lambda^{\perp}(\boldsymbol{A})$ σε μια άλλη βάση $\boldsymbol{S'}$ διάστασης m' του υπερπλέγματος $\Lambda^{\perp}(\boldsymbol{A'})$ και στη συνέχεια αμέσως το δείγμα μετατρέπεται από μια διακριτή γκαουσιανή πάνω στο υπερπλέγμα. Για την κατασκευή και ανάλυση των σχημάτων μας είναι πιο βολικό και αρθρωτό να αντιμετωπίζετε αυτές τις λειτουργίες ξεχωριστά. Ωστόσο, μια naive εφαρμογή θα ήταν μάλλον αναποτελεσματική, απαιτώντας

τουλάχιστον $(m')^2$ διάστημα και χρόνο (όπου το m' μπορεί να είναι σημαντικά μεγαλύτερο από το m). Ευτυχώς η ειδική δομή της εκτεταμένης βάσης S'σε συνδυασμό με την αναδρομική μορφή του «nearest-plane» στην λειτουργία του αλγορίθμου SampleD μπορούν να αξιοποιηθούν για να αποφευχθεί κάθε αναλυτικός υπολογισμός του S'.Με αυτόν τον τρόπο εξοικονομούμε σημαντικό χρονικό διάστημα και χώρο κατά την naive προσέγγιση.

Για να το πετύχουμε αυτό αρχικά ορίζουμε μια βάση $\boldsymbol{S}\epsilon z^{mxm}$ του πλέγματος $\Lambda^{\perp}(\boldsymbol{A})$ και μια μήτρα $\boldsymbol{A'} = \boldsymbol{A}||\overline{\boldsymbol{A}}$ για κάποιο $\overline{\boldsymbol{A}}\ \epsilon\ z_q^{nxm}$, όπου $m' = m + \overline{m}$. Για να γίνει περισσότερο κατανοητό εξετάζουμε μια υποθετική εκτέλεση του αλγορίθμου $SampleD(S', y', s)$, όπου το $S' = \begin{pmatrix} S & W \\ 0 & I \end{pmatrix}$ είναι η εκτεταμένη βάση όπως περιγράφεται παραπάνω και $\tilde{S}' = \begin{pmatrix} \tilde{S} & 0 \\ 0 & I \end{pmatrix}$. Μπορεί να αποδειχθεί ότι είναι μια αναδρομική εκτέλεση του αλγορίθμου $v' \leftarrow SampleD(S', y', s)$ αν απλά επιλέξεις όλες τις καταχωρήσεις του $\bar{v}\epsilon z^{\overline{m}}$ανεξάρτητα από το $D_{Z,s}$. Οπότε τότε επιλέγεις $v \leftarrow SampleD(S, y' - \overline{\boldsymbol{A}}\bar{v}, s)$ και παίρνεις ως έξοδο $v' = v||\bar{v}$. Επομένως, ο βελτιστοποιημένος αλγόριθμος μπορεί να εκτελέσει ακριβώς τα ίδια βήματα, αποφεύγοντας έτσι την ανάγκη υπολογισμού και αποθήκευσης του. Μια παρόμοια βελτιστοποίηση λειτουργεί επίσης για οποιαδήποτε παραλλαγή των στηλών του $\boldsymbol{A'}$. [32]

Τυχαιοποίηση ελέγχου

Τέλος στην τελευταία αρχή της ανάπτυξης των δέντρων θα παρουσιαστεί ο τρόπος με τον οποίο μπορεί κάποιος να τυχαιοποιήσει την βάση του πλέγματος, έχοντας βέβαια ως κόστος μια πολύ μικρή απώλεια ποιότητας. Αυτή η λειτουργία είναι χρήσιμη για την ασφαλή ανάθεση ελέγχου σε άλλη οντότητα, επειδή η βάση που προκύπτει είναι ακόμα μικρή, αλλά είναι (ουσιαστικά) στατιστικά ανεξάρτητη από την αρχική βάση.

Ο πιθανοτικός αλγόριθμος πολυωνιμικού χρόνου RandBasis (S, s) παίρνει τη βάση S ενός αδιάστατου ακέραιου αριθμού πλέγματος και μια παράμετρος $s \geq \left\|\tilde{S}\right\| \cdot \omega(\sqrt{logn})$ και δίνει ως έξοδο την βάση S'στο Λ.

Τα βήματα του αλγορίθμου φαίνονται παρακάτω.

1) Λαμβάνουμε ένα i=0 εώς I < m

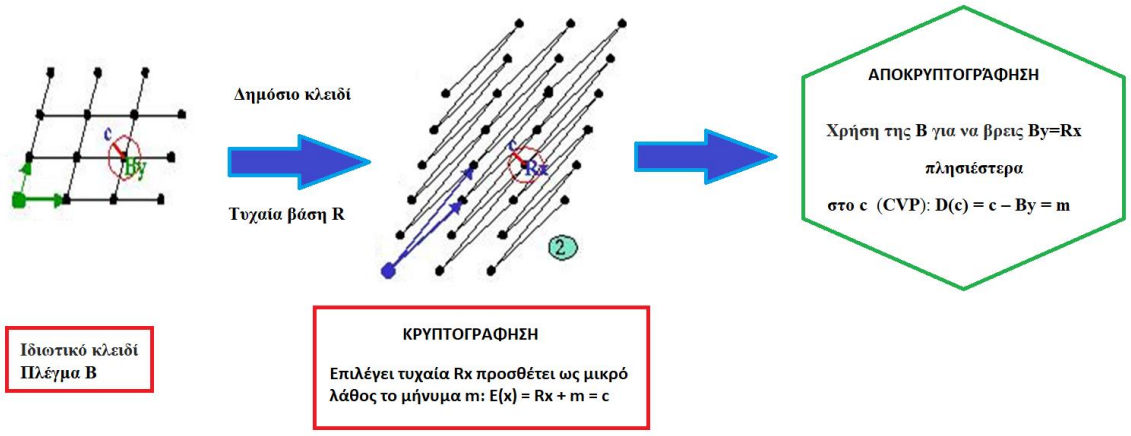
   Από την SampleD(S,s) βρίσκουμε ένα v. Αν το v είναι γραμμικά ανεξάρτητο του $\{v_1, v_2, .., v_i\}$ τότε θέτουμε i=i+1 και αντικαθιστούμε το v με το v_i .

2) Από την ToBasic (V,HNF(S)) παίρνουμε ως έξοδο την ζητούμενη S'.

Θα πρέπει να αναφερθεί ότι γίνεται HNF (κανονική ερμητιανή μορφής) για να διασφαλίσουμε όσο τον δυνατόν καλύτερη ασφάλεια στην μεταφορά των πληροφοριών κατά την έξοδο σε S'. Παρόλα αυτά οποιαδήποτε άλλη δημόσια διαθέσιμη (ή αποτελεσματικά υπολογιστική) βάση του πλέγματος που θα εξασφάλιζε αυτή την προστασία θα μπορούσε να χρησιμοποιηθεί αντί της HNF.

Στο σημείο αυτό είναι χρήσιμο να αναφερθεί και το παρακάτω λήμμα.

Η πιθανότητα να συμβεί ένα συμβάν να είναι $1 - 2^{\Omega(v^{\varepsilon})}$ με ε μια σταθερά μεγαλύτερη του μηδενός όταν το S' παράγεται από την RandBasis (S, s) επαναλαμβάνοντας το πρώτο βήμα του παραπάνω αλγορίθμου για μέγιστη πολυπλοκότητα $O(m^2)$ θα προκύπτει τελικά για $\|\tilde{S}\| \leq s.\sqrt{m}$. Ακόμη για οποιεσδήποτε δύο βάσεις S_0 και S_1 του ίδιου δικτυωτού πλέγματος και για κάθε $s \geq max\{\|\tilde{S}_0\|, \|\tilde{S}_1\|\} \cdot \omega(\sqrt{logn})$ η έξοδος που λαμβάνουμε με χρήση της RandBasis των 2 βάσεων είναι σε negl(n) statistical distance



Σχήμα 2.4: Κρυπτογράφηση με πλέγμα- κρυπτοσύστημα HNF

2.3.2. Αλγόριθμος LLL

Ο αλγόριθμος αυτός αναπτύχθηκε το 1982 από τους Arjen Lenstra, Hendrik Lenstra, László Lovász , [33] από τα αρχικά των επωνύμων των δημιουργών του πήρε και το όνομα του. Αποτελεί πιθανότατα τον πλέον χρησιμοποιούμενο αλγόριθμο για την αναγωγή της βάσης ενός δικτυωτού. [34]

Με τον αλγόριθμο αυτό πετυχαίνουμε την εύρεση μια καλύτερης βάσης από μια δοθείσα αρχική βάση $\{v_1, v_2 \dots, v_n\}$ ενός δικτυωτού L. Με τον όρο καλύτερη βάση εννοούμε κάποια

βάση που το διάνυσμα της να είναι όσο το δυνατόν μικρότερο. Με τον αλγόριθμο αυτό ξεκινάμε από το μικρότερο διάνυσμα που δύναται να βρούμε και κινούμαστε σταδιακά μέχρι να καταλήξουμε στο τελικό διάνυσμα της καλύτερης βάσης. Μια άλλη προσέγγιση αυτού λέει ότι στόχος είναι να καταλήξουμε στο τελικό σημείο όπου τα διανύσματα της καλύτερης βάσης είναι όσο το δυνατόν περισσότερο ορθογώνια μεταξύ τους. Δηλαδή το γινόμενο $v_i \cdot v_j$ να προσεγγίζει περισσότερο την τιμή μηδέν.

Για την επίλυση αυτού του αλγορίθμου γίνεται χρήση της ανισότητας του Hadamard που λέει ότι:

$$\det L = vol(F) \leq \|v_1\| \cdot \|v_2\| \cdot \ldots \cdot \|v_n\|$$

όπου vol(F) είναι ο όγκος του θεμελιώδους χωρίου του δικτυωτού L.

Όσο τα διανύσματα είναι ορθογώνια μεταξύ τους τόσο η παραπάνω ανισότητα προσεγγίζει την ισότητα.

Άμεση συνέπεια αυτού είναι η παρακάτω πρόταση.

Για μια βάση $B = \{v_1, v_2 \ldots, v_n\}$ του δικτυωτού L και αν θεωρήσουμε με B^* την ορθογώνια βάση κατά Gram – Schmidt ισχύει ότι :

$$\det L = \|v_1^*\| \cdot \|v_2^*\| \cdot \ldots \cdot \|v_n^*\|$$

Γενικεύοντας τα αποτελέσματα των Lenstra – Lenstra – Lovász μπορούμε να πούμε ότι μία ανηγμένη βάση LLL είναι «καλή» βάση και ότι είναι δυνατόν να υπολογιστεί μια ανηγμένη βάση LLL σε πολυωνυμικό χρόνο.

Τα βήματα που εκτελεί ο LLL αλγόριθμος είναι:

1. Λαμβάνει ως είσοδο μια οποιαδήποτε βάση $B = \{v_1, v_2 \ldots, v_n\}$του δικτυωτού L
2. Πραγματοποιούμε ορθογωνιοποίηση Gram – Schmidt της βάσης. Σύμφωνα με τα γνωστά θα έχουμε:

$$v_1^* = v_1$$

$$v_2^* = v_2 - \mu_{2,1} v_1^*$$

$v_3^* = v_3 - \mu_{3,1} v_1^* - \mu_{3,2} v_2^*$

.

.

.

$v_n^* = v_n - \mu_{n,1} v_1^* - \cdots - \mu_{n,n-1} v_{n-1}^*$, όπου $\mu_{i,j}$ ο σχετικός συντελεστής προβολής . Δηλαδή $\mu_{i,j} = \frac{v_i \cdot v_j^*}{\|v_j^*\|^2}$

3. Κάνουμε αναγωγή της βάσης του δικτυωτού σύμφωνα με τον τύπο:
   $v_i = vi - r \cdot v_{i-1}$, όπου r ο πλησιέστερος ακέραιος στο $\mu_{i,i-1}$
   a. Αν ικανοποιείται η συνθήκη Lovasz προχωράει στο επόμενο βήμα
   b. Αν όχι Ανταλλάσσουμε την στήλη v_i με την v_{i-1}
4. Λαμβάνουμε ως έξοδο την ανηγμένη βάση του δικτυωτού L.

Ο Παραπάνω αλγόριθμος έχει πεπερασμένο αριθμό βημάτων και δίνει μια ανηγμένη βάση L για το δικτυωτό. Αν θεωρήσουμε B=max$\|v_i\|$ μπορεί να αποδειχθεί ότι εκτελεί τις επαναλήψεις για χρόνο όχι περισσότερο από $\boldsymbol{O}$ ($\boldsymbol{n2}$ $\mathbf{log}$ $\boldsymbol{n}$ + $\boldsymbol{n}$2 $\mathbf{log}$ $\boldsymbol{B}$) φορές. Δηλαδή ο αλγόριθμος είναι πολυωνυμικού χρόνου.

Από τον τρόπο με τον οποίο αναπτύχθηκε και εκτελείται ο αλγόριθμος LLL εξάγονται κάποια χρήσιμα συμπεράσματα. Πρώτα από όλα αν κάποιος επιχειρήσει να εκτελέσει τον αλγόριθμο με χρήση υπολογισμών σε ακριβείς τιμές, τότε οι ενδιάμεσοι υπολογισμοί θα περιέχουν τεράστιους αριθμούς. Για τον λόγο αυτό αν εργαζόμαστε σε δικτυωτά μεγάλης διάστασης, είναι απαραίτητο να χρησιμοποιηθούν προσεγγίσεις κινητής υποδιαστολής, γεγονός που θα οδηγήσει σε προβλήματα με σφάλματα στρογγυλοποίησης. Έχουν αναπτυχθεί διάφορες τεχνικές για την αντιμετώπιση αυτού του προβλήματος, που δεν θεωρείται σκόπιμο να συζητηθούν στα πλαίσια αυτής της εργασίας.

Ακόμη τον υπολογισμό των κύκλων που εκτελεί ο κύριος βρόχος του αλγορίθμου είμαστε σε θέση να τον βρούμε μετρώντας μόνο τον αριθμό των βασικών πράξεων που κάνει ο αλγόριθμος LLL. Κάτι τέτοιο συνεπάγεται ότι στην ουσία μετράμε μόνο τις φορές που εκτελείται ο εσωτερικός βρόχος j καθώς και τις εκτελούμενες πράξεις στις συντεταγμένες του διανύσματος. Έτσι για παράδειγμα αν προσθέσουμε δύο διανύσματα ή αν εκτελέσουμε την πράξη του πολλαπλασιασμού αυτού με μια σταθερά οι βασικές πράξεις που εκτελούνται

είναι n. . Έτσι καταφέραμε να αποδείξουμε ότι ο αλγόριθμος LLL [33] τερματίζει όχι σε περισσότερα από $O\,(n^{6}(\log B)^{3})$ βασικές πράξεις.

3. Κβαντική Κρυπτογραφία

3.1. Εισαγωγή στην Κβαντική Κρυπτογραφία

Κατά τη δεκαετία του 1930 εμβληματικές μορφές της επιστημονικής κοινότητας, όπως ο Alan Turing, επιχείρησαν να θεμελιώσουν τη θεωρητική πληροφορικής. Με τις θεωρίες τους θέτουν κάποια όρια για τους αλγορίθμους που εκτελούνται σε πρότυπες υπολογιστικές μηχανές. Αυτό που είναι άξιο επισήμανσης είναι ότι οι θεωρίες τους αποτελούν τη βάση για την κατασκευή μιας "σύγχρονης" υπολογιστικής μηχανής (προσομοιάζει στη λειτουργία με τους σημερινούς υπολογιστές) που πρωτοεμφανίστηκε τη δεκαετία του '50. Από τότε οι εξελίξεις που ακολούθησαν στον τομέα της κατασκευής υπολογιστών υπήρξαν ραγδαίες. Έτσι, περνώντας από τεχνολογία λυχνιών και DLSI κυκλώματα έχουμε κατορθώσει σήμερα να φτάσουμε σε ένα σημείο που τα δομικά στοιχεία των υπολογιστών είναι τόσο μικρά ώστε να επηρεάζονται ήδη από τους νόμους της κβαντομηχανικής. Η εξέλιξη αυτή έφερε στο προσκήνιο νέα γενιά επιστημόνων που οραματίζονταν ότι ίσως αυτές οι επιδράσεις θα ήταν δυνατό να βρουν πρακτική εφαρμογή για να γίνουν οι υπολογισμοί ταχύτατα. [35] [36]

Καινοτόμος πρωτεργάτης μίας ιδέας για το πώς ένα κβαντικό σύστημα θα μπορούσε θεωρητικά να χρησιμοποιηθεί για την υλοποίηση υπολογισμών υπήρξε ο Richard Feynman. Το 1985 μέσω μιας ρηξικέλευθης δημοσίευσης, όπου περιέγραφε το πώς κάθε φυσική διαδικασία θα μπορούσε να μοντελοποιηθεί θεωρητικά με τέλειο τρόπο με χρήση ενός κβαντικού υπολογιστικού συστήματος. Ένα τέτοιο κβαντικό υπολογιστικό σύστημα μπορεί, όπως επισημαίνει, να πραγματοποιήσει διαδικασίες αδύνατες για έναν "κλασσικό" υπολογιστή, π.χ. παραγωγή πραγματικά τυχαίων ακεραίων. Το βασικότερο χαρακτηριστικό του είναι η ικανότητα να χρησιμοποιεί το φαινόμενο του κβαντικού παραλληλισμού, για να πραγματώνει κάποιους υπολογισμούς σε χρόνο πολύ μικρότερο από τον "κλασσικό" υπολογιστή. Ας επισημάνουμε όμως εμφατικά τις βασικές αρχές αυτού του κβαντικού υπολογιστή.

Όπως είναι γνωστό, ένα bit σε ένα «κλασσικό» μοντέλο υπολογιστή είναι δυνατόν να βρίσκεται σε καταστάσεις 0 και 1. Στον αντίποδα ένα κβαντικό bit (qubit) μπορεί να βρίσκεται όχι μόνο σε μία από αυτές τις δύο καταστάσεις, αλλά και σε μία υπέρθεσή τους!

Σ’ αυτή τη σύμφωνη κατάσταση, το qubit, υπάρχει σαν 0 και 1 ταυτόχρονα! Υποθέτουμε για παράδειγμα έναν καταχωρητή από 3 bit. Αυτός είναι δυνατό να χρησιμοποιηθεί για αναπαράσταση ενός εκ των αριθμών από το 0 ως το 7 σε κάθε χρονική στιγμή. Αν τώρα θεωρήσουμε έναν καταχωρητή από τρία qubit, παρατηρούμε ότι αν κάθε qubit είναι σε υπέρθεση, ο καταχωρητής μπορεί να αναπαριστά όλους τους αριθμούς από το 0 μέχρι το 7 ταυτόχρονα. Γενικότερα είναι θεωρητικά εφικτό ένα κβαντικός υπολογιστής n qubit, να βρίσκεται την ίδια στιγμή σε 2n καταστάσεις. Αυτό θα σηματοδοτούσε επί παραδείγματι ότι θα μπορούσαν να αναπαραστήσει ταυτόχρονα όλα τα κλειδιά ενός κρυπτοσυστήματος.

Δεν πρέπει εντούτοις να θεωρήσουμε ότι ο κβαντικός υπολογιστής θα “εκτελεί” -δωρεάν - τους σημερινούς αλγορίθμους σε λιγότερο χρόνο. Ακόμα και αν καταφέρουμε και κατασκευάσουμε την υπέρθεσή 2n καταστάσεων - από το οποίο βρισκόμαστε αρκετά μακριά, είναι απαραίτητο να βρεθεί ένας τρόπος να διεξαχθεί ένας υπολογισμός με αυτές. Δημιουργείται η σταθερή εντύπωση ότι με τον υπολογισμό αυτό, δεν θα μπορούν να λυθούν NP πλήρη προβλήματα.

3.2. Κβαντικά ανθεκτικά κρυπτοσυστήματα

Η μετα-κβαντική κρυπτογραφία (μερικές φορές αναφέρεται ως quantum-proof, quantum-safe ή quantum-resistant) αναφέρεται σε κρυπτογραφικούς αλγόριθμους (συνήθως αλγόριθμους δημόσιου κλειδιού) που πιστεύεται ότι είναι ασφαλείς έναντι μιας επίθεσης από έναν κβαντικό υπολογιστή. Από το 2020, αυτό δεν ισχύει για τους πιο δημοφιλείς αλγόριθμους δημόσιου κλειδιού, οι οποίοι μπορούν να διαλυθούν αποτελεσματικά από έναν αρκετά ισχυρό κβαντικό υπολογιστή. Το πρόβλημα με τους επί του παρόντος δημοφιλείς αλγόριθμους είναι ότι η ασφάλειά τους βασίζεται σε ένα από τα τρία δύσκολα μαθηματικά προβλήματα:

- Το πρόβλημα ακέραιας παραγοντοποίησης.
- Το διακριτό πρόβλημα λογάριθμου.
- Το πρόβλημα διακριτού λογάριθμου ελλειπτικής καμπύλης

Όλα αυτά όμως τα προβλήματα μπορούν να επιλυθούν εύκολα σε έναν αρκετά ισχυρό κβαντικό υπολογιστή και με χρήση του αλγορίθμου Shor.

Παρόλο που οι τρέχοντες, ευρέως γνωστοί, πειραματικοί κβαντικοί υπολογιστές δεν διαθέτουν επαρκή επεξεργαστική ισχύ για να σπάσουν οποιονδήποτε πραγματικό κρυπτογραφικό αλγόριθμο, πολλοί κρυπτογράφοι για να το παρακάμψουν αυτό σχεδιάζουν νέους αλγόριθμους για να προετοιμαστούν για μια στιγμή που ο κβαντικός υπολογιστής θα γίνει απειλή.

Σε αντίθεση με την απειλή του κβαντικού υπολογισμού για τους τρέχοντες αλγόριθμους δημόσιου κλειδιού, οι περισσότεροι τρέχοντες συμμετρικοί κρυπτογραφικοί αλγόριθμοι και οι λειτουργίες κατακερματισμού θεωρούνται σχετικά ασφαλείς έναντι επιθέσεων από κβαντικούς υπολογιστές. Ενώ ο αλγόριθμος του κβαντικού Grover επιταχύνει τις επιθέσεις εναντίον συμμετρικών κρυπτογράφων, ο διπλασιασμός του μεγέθους του κλειδιού μπορεί αποτελεσματικά να αποκλείσει αυτές τις επιθέσεις. Επομένως, η μετά-κβαντική συμμετρική κρυπτογραφία δεν χρειάζεται να διαφέρει σημαντικά από την τρέχουσα συμμετρική κρυπτογραφία.

3.3. Μοντέλα Αντιμετώπισης Επιθέσεων

Όπως γίνεται άμεσα εμφανές αυτή η ραγδαία αύξηση στην τεχνολογία είχε αντίκτυπο και στην ασφάλεια των κρυπτοσυστημάτων.

Η αντιμετώπιση αυτών των επιθέσεων είναι κάτι που έχει απασχολήσει την ερευνητική κοινότητα και για αυτό τον λόγο έχουν αναπτυχθεί πληθώρα μοντέλων που κινούνται προς αυτήν την κατεύθυνση. Θα αναφερθούμε στα σημαντικότερα εξ αυτών.

3.3.1. Quantum-resistant cryptography

Η **Quantum-resistant cryptography** περιλαμβάνει κάποιους κλασικούς αλγόριθμους που μπορούν να μετριάσουν την επίθεση από τον κβαντικό υπολογιστή. Ορισμένοι ψηφιακοί αλγόριθμοι υπογραφής βασίζονται σε πρωταρχική παραγοντοποίηση μεγάλων αριθμών και διακριτών λογαρίθμων που μπορούν εύκολα να επιλυθούν με τον αλγόριθμο του Shor με την βοήθεια κβαντικών υπολογιστών. Η μέθοδος αυτή χρησιμοποιεί hash μεθόδους και εργαλεία ανθεκτικά σε κβαντικές επιθέσεις. [37] [38].

3.3.2. Μετά-Κβαντικό blockchain (PQB)

Το μετά-κβαντικό blockchain (PQB) είναι ένα κλασσικό σύστημα blockchain εφοδιασμένο με τις αρχές της μετά-κβαντικής κρυπτογραφίας ή την κλασσική δομή αποθήκευσης blockchain με κβαντική επικοινωνία.

Στο PQB, υπάρχουν κάποιες αναφορές [39] [40] οι οποίες έχουν προσθέσει κβαντικά χαρακτηριστικά στο κλασικό blockchain στην αντιμετώπιση των κβαντικών επιθέσεων. Μάλιστα στην αναφορά [41] γίνεται προσθήκη ενός επιπέδου δικτύου QKD στο τρέχον σύστημα blockchain για προστασία στον σχετικό υπο-αλγόριθμο κατά των κβαντικών επιθέσεων. Ωστόσο, ο αριθμός των επαληθευμένων επικοινωνιών QKD για τη διαδικασία δημιουργίας μπλοκ στο σχήμα κλίμακας είναι O(n2). Είναι πιθανό να μην είναι βιώσιμο για την εξασφάλιση πλήρους κρυπτογράφησης, αλλά μπορεί να είναι χρήσιμο για την εξασφάλιση μικρότερων κατανεμημένων βάσεων δεδομένων. Το QKD είναι μια ασφαλής μέθοδος επικοινωνίας που εφαρμόζει ένα κρυπτογραφικό πρωτόκολλο που περιλαμβάνει στοιχεία της κβαντικής μηχανικής.

Υπάρχουν πολλά πρωτόκολλα που κωδικοποιούν και αποθηκεύουν πληροφορίες σε ένα κβαντικό σύστημα τα οποία καθιστούν την πληροφορία tamper-proof. Ειδικά, υπάρχει μια πρόταση για "Quantum Bitcoin" [42], το οποίο όχι μόνο χρησιμοποιεί ένα κλασικό blockchain για την αποθήκευση δεδομένων συναλλαγών, αλλά και κβαντικές μεθόδους για την δημιουργία του μπλοκ και για την επαλήθευση των συναλλαγών. Υπάρχουν επίσης μερικά πρωτόκολλα δέσμευσης κβαντικών bit που μπορούν να ληφθούν υπόψη ως ένας τύπος εναλλακτικού σε σχέση με τα σχήματα ψηφιακής υπογραφής.

Για να είναι αποτελεσματικό, ένα μετα-κβαντικό κρυπτοσύστημα θα χρειαστεί να παράσχει blockchain με τα παρακάτω πλεονεκτήματα[43].

Μικρά μεγέθη κλειδιών. Οι συσκευές που αλληλεπιδρούν με ένα blockchain πρέπει ιδανικά να κάνουν χρήση μικρά σε μέγεθος δημόσια και ιδιωτικά κλειδιά για τη μείωση του απαιτούμενου χώρου αποθήκευσης. Επιπλέον, τα μικρά κλειδιά περιλαμβάνουν λιγότερο περίπλοκες υπολογιστικές λειτουργίες κατά τη διαχείριση τους. Αυτό είναι ιδιαίτερα σημαντικό για blockchain που απαιτούν η αλληλεπίδραση των τελικών συσκευών του Internet of Things (IoT), που συνήθως περιορίζονται από την άποψη της αποθήκευσης και της υπολογιστικής ισχύς. Αξίζει να σημειωθεί ότι το IoT, γνώρισε σημαντική ανάπτυξη τα τελευταία χρόνια, αλλά οι συσκευές IoT εξακολουθούν να αντιμετωπίζουν ορισμένες σημαντικές προκλήσεις, κυρίως όσον αφορά την ασφάλεια.

Μικρή υπογραφή και συνάρτηση κατακερματισμού. Ένα blockchain ουσιαστικά αποθηκεύει συναλλαγές δεδομένων, συμπεριλαμβανομένων υπογραφών χρηστών και

κατακερματισμού δεδομένων. Επομένως, εάν αυξηθεί το μήκος της υπογραφής και του κατακερματισμού τότε θα αυξηθεί και το μέγεθος blockchain.

Γρήγορη εκτέλεση. Τα μετα-κβαντικά σχήματα πρέπει να είναι τόσο γρήγορα όσο το δυνατόν περισσότερο για να επιτρέψει σε ένα blockchain να επεξεργαστεί ένα μεγάλο ποσό συναλλαγών ανά δευτερόλεπτο. Επιπλέον, μια γρήγορη εκτέλεση συνήθως περιλαμβάνει χαμηλή υπολογιστική πολυπλοκότητα, η οποία είναι απαραίτητη για να μην εξαιρούνται συσκευές με περιορισμούς πόρων από συναλλαγές blockchain.

Χαμηλή υπολογιστική πολυπλοκότητα. Αυτή η δυνατότητα σχετίζεται με την γρήγορη εκτέλεση, αλλά είναι σημαντικό να σημειωθεί ότι μια γρήγορη εκτέλεση με συγκεκριμένο υλικό δεν σημαίνει ότι το μετα-κβαντικό κρυπτοσύστημα είναι υπολογιστικά απλό. Επομένως, είναι απαραίτητο για να αναζητήσετε μια βελτιστοποίηση μεταξύ υπολογιστικής πολυπλοκότητας, χρόνου εκτέλεσης και υποστηριζόμενων συσκευών υλικού.

Χαμηλή κατανάλωση ενέργειας. Ορισμένα blockchain όπως το Bitcoin θεωρούνται άπληστα ως προς τις απαιτήσεις κυρίως λόγω της ενέργειας που απαιτείται για την εκτέλεση του πρωτοκόλλου συναίνεσης. Εκεί είναι άλλοι παράγοντες που επηρεάζουν την κατανάλωση ενέργειας, όπως το χρησιμοποιημένο υλικό, το ποσό των συναλλαγών που πραγματοποιήθηκαν και, προφανώς, την υλοποίηση του συστήματος ασφαλείας, τα οποία μπορούν να αντλήσουν σχετικό ποσό ρεύμα λόγω της πολυπλοκότητας των εκτελούμενων λειτουργιών.

3.3.3. Κβαντικός κατακερματισμός

Μελετήθηκε ότι ο κβαντικός κατακερματισμός είναι ένα πιο ισχυρό σύστημα έναντι διαφόρων άλλων που βασίζονται σε δυαδικές διακριτές συναρτήσεις. Η κβαντική διαδικασία είναι «κλασική-κβαντική», δηλαδή, χρειάζεται μια κλασική συμβολοσειρά bit ως είσοδος και παράγει μια κβαντική κατάσταση. Η συνάρτηση που προκύπτει έχει την ιδιότητα μιας συνάρτησης oneway (pre-image resistance), επιπλέον έχει τις ιδιότητες ανάλογες με την κλασική κρυπτογραφική αντίσταση (pre-image resistance) και collision resistance. Αυτή η συνάρτηση μπορεί να χρησιμοποιηθεί σε ένα πρωτόκολλο κβαντικής ψηφιακής υπογραφής. [44]

3.3.4. Quantum networked time machine

Στο μοντέλο αυτό έχουμε ένα εννοιολογικό σχέδιο για ένα κβαντικό blockchain. Η μέθοδος περιλαμβάνει την κωδικοποίηση του blockchain σε μια χρονική κατάσταση GHZ (Greenberger – Horne – Zeilinger) των φωτονίων που δεν συνυπάρχουν ταυτόχρονα. Αποδεικνύεται ότι η εμπλοκή στο χρόνο, σε αντίθεση με την εμπλοκή στο χώρο, παρέχει το κρίσιμο κβαντικό πλεονέκτημα ί. Επιπλέον, η διαδικασία κωδικοποίησης μπορεί να ερμηνευθεί ως μη κλασική επηρεάζοντας τις προγενέστερες. [45]

3.4. Προβλήματα στην κβαντική κρυπτογραφία.

Τα σημαντικότερα προβλήματα των δικτυωτών του χρησιμοποιούνται προκειμένου η κρυπτογραφία βασισμένη στα δικτυωτά , και κατ' επέκταση στην κβαντική κρυπτογραφία, να έχει μεγαλύτερη ασφάλεια είναι το πρόβλημα του μικρότερου διανύσματος (Shortest Vector Problem – SVP) και η προσεγγιστική παραλλαγή του καθώς επίσης και το πρόβλημα του κοντινότερου διανύσματος (Closest Vector Problem – CVP) με την προσεγγιστική παραλλαγή αυτού σε ένα δοθέν διάνυσμα του δικτυωτού.

Ακόμη επειδή τα πλέγματα έχουν την ιδιότητα ότι αν «σπάσει το κρυπτοσύστημα» τότε μπορεί να επιλυθεί οποιοδήποτε στιγμιότυπο του δύσκολου προβλήματος μπορούμε να πούμε ότι τα κρυπτοσυστήματα με πλέγματα βασίζονται και σε δύο άλλα προβλήματα:

Το πρόβλημα των Σύντομων Ακέραιων Λύσεων (Short Integer Solutions - SIS) και το πρόβλημα της Μάθησης Με Λάθη (Learning with Errors - LWE)

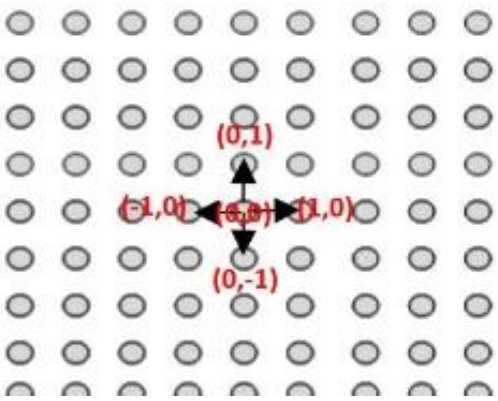
3.4.1. Το πρόβλημα του μικρότερου διανύσματος

Το πρόβλημα του μικρότερου διανύσματος αναφέρεται στην εύρεση ενός μη μηδενικού διανύσματος $v \epsilon L$, όπου το μέτρο με την ευκλείδεια νόρμα του είναι μικρότερο ή ίσο από το μέτρο άλλου μη μηδενικού διανύσματος του L, δηλαδή:

$$\|x\| = min\{\|v\| : v \epsilon L, v \neq 0\}$$

Όπως μπορεί πολύ εύκολα να αποδειχθεί το μικρότερο διάνυσμα (SVP) δεν είναι πάντοτε μοναδικό. Αν για παράδειγμα αναφερόμαστε στον χώρο Z^2 τότε και τα τέσσερα διανύσματα $(0,1), (0,-1), (1,0)$ και $(-1,0)$ είναι λύσεις του προβλήματος του μικρότερου διανύσματος

σε ένα δικτυωτό (SVP) (εικόνα 4). Γι‘ αυτό και αναζητούμε ένα από τα μικρότερα διανύσματα.



Εικόνα 3.1: Τέσσερα Ισοδύναμα διανύσματα που αποτελούν λύση του SVP προβλήματος στον Z^2

Ο P.van Embe-Boas με μια εργασία που δημοσίευσε το 1981 [46] έδειξε ότι η επίλυση του παραπάνω προβλήματος είναι NP-hard με χρήση της L∞ νόρμας. Παρόλα αυτά δεν έδωσε απάντηση τι γίνεται όταν έχουμε L2 νόρμα που βασίζονται και οι περισσότερες εφαρμογές. Απάντηση σε αυτό έδωσε ο Ajtai το 1998 [47] που κατάφερε να αποδείξει ότι το πρόβλημα του μικρότερου διανύσματος (SVP) με χρήση της L2 νόρμας είναι επίσης NP-hard.

Το 2010 ο Daniele Micciancio και ο Παναγιώτης Βούλγαρης [48] παρουσίασαν ένα ντετερμινιστικό αλγόριθμο για την επίλυση του SVP σε ένα n-διάστατο δικτυωτό.

3.4.2. Προσεγγιστικό πρόβλημα του μικρότερου διανύσματος

Σε πολλές περιπτώσεις δεν είναι απαραίτητο η εύρεση του ακριβές διανύσματος. Προκειμένου κατά κύριο λόγο να κερδίσουμε σε πολυπλοκότητά στον αλγόριθμο αναπτύχθηκε κάποια προσέγγιση αυτού.

Για τον υπολογισμό αυτής της προσέγγισης θα θεωρήσουμε κάποια συνάρτηση f(n) και θα αναζητήσουμε κάποιο μη μηδενικό διάνυσμα του δικτυωτού L της διάστασης n, το οποίο δεν είναι μεγαλύτερο από f(n) φορές το μικρότερο μη μηδενικό διάνυσμα.

Αν θεωρήσουμε επομένως V_{min} το μικρότερο μη μηδενικό διάνυσμα στο δικτυωτό L θα αναζητήσουμε κάποιο v∈L τέτοιο ώστε: $\|v\| \leq f(n)\|v_{min}\|$

Όπως είναι εύκολο αντιληπτό οι προσεγγίσεις μπορεί να είναι περισσότερες από μια καθώς κάθε διαφορετική επιλογή συνάρτησης που f(n) που ικανοποιεί την συνθήκη δίνει και διαφορετική προσέγγιση.

Ο πιο γνωστός αλγόριθμος που αναπτύχθηκε για την προσέγγιση του μικρότερου διανύσματος σε κάποιο δικτυωτό είναι ο αλγόριθμος LLL.

3.4.3. Το πρόβλημα κοντινότερου διανύσματος

Άλλο ένα εξίσου σημαντικό πρόβλημα που συναντάμε στα δικτυωτά είναι αυτό του κοντινότερου διανύσματος (CVP) σε ένα δοθέν διάνυσμα του χώρου.

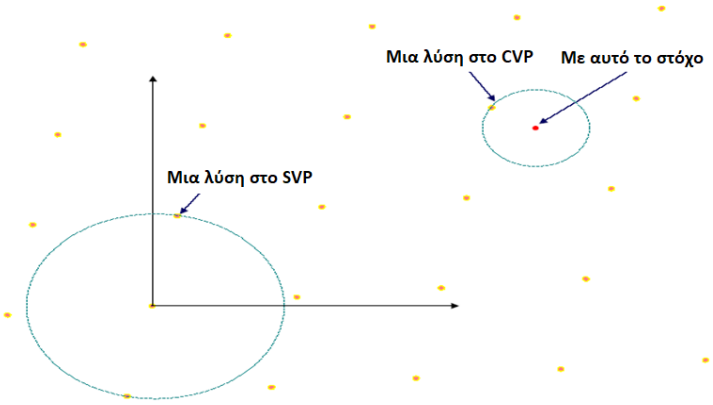
Το CVP πρόβλημα αναφέρεται στην εύρεση ενός διανύσματος εκτός του δοθέντος δικτυώματος, το οποίο να είναι το πλησιέστερο σε ένα δεδομένο διάνυσμα του δικτυώματος

Αν θέλαμε να εκφράσουμε και με μαθηματικές εκφράσεις τον παραπάνω ορισμό θα μπορούσαμε να πούμε ότι :

Παίρνοντας ως δεδομένο ένα διάνυσμα w ∈ $\mathbb{R}^n$ τέτοιο ώστε να μην ανήκει στο δικτυωτό L στόχος μας είναι να βρούμε ένα διάνυσμα v∈L που έχει την ιδιότητα να είναι το κοντινότερο στο w, δηλαδή απώτερος σκοπός είναι να βρούμε ένα διάνυσμα v ∈ L για να ελαχιστοποιήσουμε την Ευκλείδεια νόρμα $\|w - \bar{v}\|$, $\bar{v} \epsilon L$ Οπότε έχουμε:

$$\|w - \bar{v}\| = min\{\|w - \bar{v}\| \ : \ \bar{v} \epsilon L \}.$$

Όπως στην περίπτωση του SVP έτσι και σε αυτή του CVP τα διανύσματα που ικανοποιούν τις συνθήκη μπορεί να είναι περισσότερα από ένα. Η αναζήτηση μας αρκείται σε ένα από το πλήθος αυτών ων ισοδύναμων διανυσμάτων.



Σχήμα 3.2: Παράδειγμα SVP και CVP .

3.4.4. Προσεγγιστικό Πρόβλημα Κοντινότερου Διανύσματος

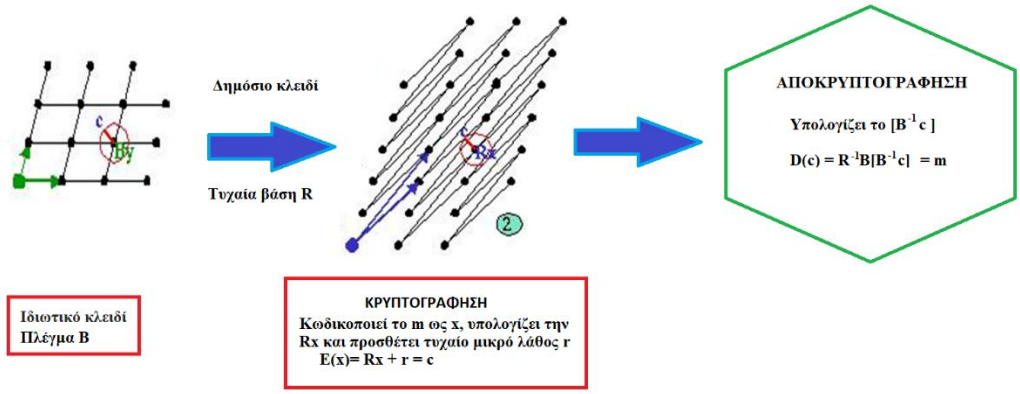
Κατ' αναλογία με το προσεγγιστικό SVP αναπτύχθηκε και το προσεγγιστικό CVP όπου το πρόβλημα παύει να είναι NP-hard.

Σε αυτήν την περίπτωση η επίλυση του γίνεται με την αναζήτηση ενός διανύσματος που είναι κατά προσέγγιση λύση του CVP. Δηλαδή έστω $L \subset \mathbb{R}n$ δικτυωτό και $w \in \mathbb{R}n$, βρίσκουμε ένα διάνυσμα $v \in L$ τέτοιο ώστε:

$$\|w - \bar{v}\| < f(n) min\{\|w - \bar{v}\| \ : \ \bar{v} \epsilon L\}.$$

Όπως και στην περίπτωση του SVP προβλήματος οι προσεγγίσεις δύναται να είναι περισσότερες από μια και εξαρτώνται από την συνάρτηση f(n) .

Το 1986 ο Babai [49] [50] παρουσίασε δύο αλγόριθμους για την προσέγγιση του CVP σε πολυωνυμικό χρόνο. Παρότι οι αλγόριθμοι αυτοί δεν πραγματοποιούν την επίλυση του προβλήματος του κοντινότερου διανύσματος (CVP) του δικτυωτού σε ένα δοθέν διάνυσμα του χώρου σε κάθε περίπτωση, θεωρούνται ιδιαίτερα χρήσιμοι σε πολλά κρυπτοσυστήματα και επιθέσεις. Χρήση αυτών έχουμε στο GGH (Goldreich – Goldwaser – Halevi) κρυπτοσύστημα, στο κρυπτοσύστημα του Micciancio και σε μερικές ακόμη επιθέσεις.



Σχήμα 3.3: Κρυπτογράφηση με πλέγμα σχήμα GGH

3.4.5. Το πρόβλημα των Σύντομων Ακέραιων Λύσεων

Για να γίνει σαφές το SIS πρόβλημα θα αναφερθούμε στον τρόπο με τον οποίο διατυπώνεται στο πόρισμα που εξάγεται από αυτόν τον ορισμό καθώς και στην απόδειξη του.

Εάν δώσουμε m τυχαία διανύσματα $a_i \in \mathrm{Z}_q^n$ στις στήλες ενός πίνακα $A \in \mathrm{Z}_q^{nxm}$, ζητάμε να βρούμε ένα μη-μηδενικό διάνυσμα $z \in \mathrm{Z}^m$, $z \leq \beta < q$ τέτοιο ώστε

$$f_A(z) = \boldsymbol{A}z = \sum_{i=1}^{m} a_i \cdot z_i = 0 \ \in \mathrm{Z}_q^n$$

Οι παράμετροι n, q, m είναι θετικοί ακέραιοι, με q πρώτο αριθμό μεγαλύτερο του 2.

Η σταθερά $\beta \in \mathbb{R}$ καθορίζει το πόσο «μικρός» είναι ο μη-τετριμμένος συνδυασμός με μηδενικό άθροισμα.

Πόρισμα: Έστω $m = n \log q$ με $m \geq \bar{m}$ και $\beta \geq \sqrt{\bar{m}}$. Τότε υπάρχει τουλάχιστον ένα $z \in \mathbb{Z}^m$ που ικανοποιεί τον περιορισμό του προβλήματος SIS.

Παρακάτω παραθέτω την απόδειξη

θεωρώ $m = \bar{m} = \lceil n\, logq \rceil$. Από το οποίο προκύπτει ότι υπάρχουν περισσότερα από q^n διανύσματα $x \in \{0,1\}^m$ με $q^n < 2^n$ τέτοια ώστε **Ax** = **Ay**$\in \mathrm{Z}_q^n$. Αρα υπάρχει διάνυσμα **z** = **x**− **y** $\in \{0,\pm 1\}$ του οποίου η νόρμα είναι μικρότερη ή ίση της σταθεράς β.

<u>Αναγωγή του sis προβλήματος ως πρόβλημα πλεγμάτων</u>

Θα ξεκινήσουμε την ενότητα δίνοντας αρχικά έναν ορισμό του q-ary lattice

Για έναν πρώτο αριθμό q, ένα $A \in \mathrm{Z}_q^{nxm}$ και $y \in \mathrm{Z}_q^n$ μπορούμε να ορίσουμε:

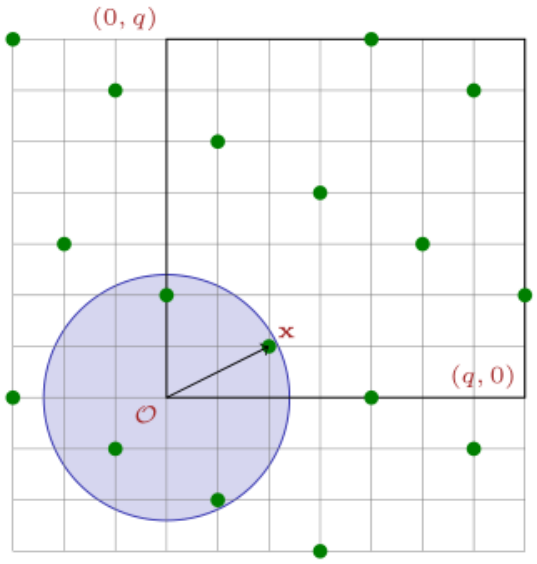
$$\mathcal{L}_q(A) = \{y \in \mathrm{Z}^m : y = A^T s (mod q), για\ κάποιο\ s \in \mathrm{Z}^n\}$$

Και

$$\mathcal{L}_q^{\perp}(A) = \{y \in \mathrm{Z}^m : Ay = 0 (mod q)\}$$

Στις παραπάνω εκφράσεις το πρώτο πλέγμα είναι αυτό που παράγεται από τις γραμμές του πίνακα Α και το δεύτερο περιέχει όλα τα διανύσματα που είναι ορθογώνια στις γραμμές του πίνακα Α.

Γενικά μπορούμε να πούμε ότι το SIS πρόβλημα ισοδυναμεί με το πρόβλημα εύρεσης ικανοποιητικά μικρών μη-μηδενικών διανυσμάτων στο πλέγμα $\mathcal{L}_q^{\perp}(A)$ για κάποιον τυχαίο πίνακα A.



Εικόνα 3.4 : σχηματική αναπαράσταση του sis προβλήματος

Θεώρημα (SIS hardness)

Για κάθε $m = poly(n)$, $\beta > 0$ και ικανοποιητικά μεγάλο $q \geq \beta \cdot poly\ n$ η επίλυση του προβλήματος $SIS_{n,q,\beta,m}$ είναι τουλάχιστον ισοδύναμη με την επίλυση του $GapSVP_\gamma$ και του $SIVP_\gamma$ σε τυχαία n-διάστατα πλέγματα για $\gamma = \beta \cdot poly(n)$

Το 1996 ο Ajtai με την εύρεση συναρτήσεων κατακερματισμού κατάφερε να αποδείξει ότι η ύπαρξη συγκρούσεων σε αυτές τις συναρτήσεις είναι ισοδύναμη με την επίλυση των δύσκολων προβλημάτων $GapSVP_\gamma$ και $GapSIVP_\gamma$.

Με μια σειρά υπολογισμών κατάφερε να αποδείξει ότι οι συναρτήσεις αυτές δεν αντιστρέφονται εύκολα με αποτέλεσμα να μπορέσει να δημιουργήσει μια οικογένεια από μονόδρομες και ανθεκτικές σε συγκρούσεις συναρτήσεις κατακερματισμού.

Μια σημαντική παρατήρηση είναι ότι αύξηση της τιμής της παραμέτρου m μπορεί να προκαλέσει αύξηση και στη συμπίεση που μπορεί να πραγματοποιήσει ο αλγόριθμος αλλά

την ίδια στιγμή η επίλυση του προβλήματος SIS γίνεται ευκολότερη, επομένως στην επιλογή της m δύναται να γίνει ένας συμβιβασμός.

Σε αντιδιαστολή με την απλότητά του, το γεγονός ότι το κλειδί έχει μεγάλο μέγεθος κάνει τον αλγόριθμο όχι τόσο αποδοτικό για πρακτικές εφαρμογές.

3.4.6. Το πρόβλημα της Μάθησης Με Λάθη

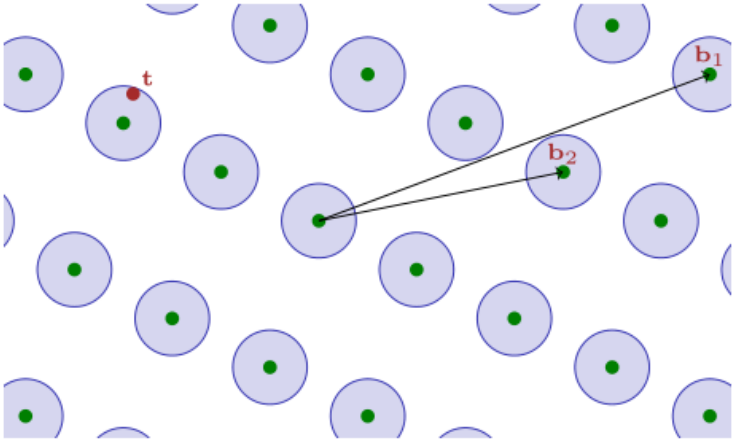
Στα προβλήματα μάθησης με λάθη αναπτύχθηκαν 2 προβλήματα αποφάσεων για την επίλυση τους. Το πρώτο είναι το Bounded Distance Decoding Problem (BDDγ) και το δεύτερο το Decisional Approximate SVP (GapSVPγ)

Bounded Distance Decoding Problem

Σύμφωνα με το πρόβλημα αυτό αν δώσουμε μια βάση B ενός n-διάστατου πλέγματος $\mathcal{L} = \mathcal{L}(B)$ και ένα σημείο στόχος $t \in \mathbb{R}^n$ για το οποίο ισχύει ότι:

$$dist\big(t, \mathcal{L}(B)\big) < d = \frac{\lambda_1 \mathcal{L}}{2\gamma(v)}$$

Αναζητούμε να βρούμε ένα μοναδικό διάνυσμα του πλέγματος $v \in \mathcal{L}(B)$ για το οποίο να ισχύει: $\|t - v\| < d$



Εικόνα 3.5: σχηματική αναπαράσταση του BDDγ

Decisional Approximate SVP

Σύμφωνα με το πρόβλημα αυτό αν δώσουμε μια βάση B ενός n-διάστατου πλέγματος $\mathcal{L} = \mathcal{L}(B)$ για το οποίο να ισχύει:$\lambda_1(\mathcal{L}) \leq 1$ ή $\lambda_1(\mathcal{L}) \leq \gamma(n)$

Ζητάμε να βρούμε ποια από τις 2 από τις παραπάνω συνθήκες ισχύει προκειμένου να μπορέσουμε να επιλύσουμε το LWE πρόβλημα.

4. Εφαρμογή της MATLAB σε συστήματα μετά-κβαντικής κρυπτογραφίας

Σε αυτό το κεφάλαιο με την βοήθεια της γλώσσας προγραμματισμού MATLAB θα παρουσιάσουμε τον τρόπο με τον οποίο μπορούμε να κατασκευάσουμε έναν κώδικα για τον υπολογισμό του ζεύγους κλειδιών σε ένα κρυπτοσύστημα McEliece [51]. Ακόμη θα γίνει εφαρμογή των κλειδιών για κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος.

Το κρυπτοσύστημα McEliece είναι ένα cipher κρυπτοσύστημα που στηρίζεται στην δημιουργία πλέγματος. Η περιγραφή του τρόπου λειτουργίας του κρυπτοσυστήματος θα γίνει στις επόμενες ενότητες.

Στην συνέχεια του κεφαλαίου θα υλοποιήσουμε το σχήμα υπογραφής των Matsumoto-Imai. [52] Ο τρόπος με τον οποίο θα γίνει η κατασκευή του στηρίζεται στην γνώση που έχει αποκτηθεί από το κρυπτοσύστημα McEliece. Οι κώδικες που υλοποιήθηκαν βρίσκονται και στο παράρτημα της παρούσας εργασίας

4.1. Εισαγωγή

Στην κρυπτογραφία, το κρυπτοσύστημα McEliece είναι ένας αλγόριθμος ασύμμετρης κρυπτογράφησης που αναπτύχθηκε το 1978 από τον Robert McEliece[51]. Ήταν το πρώτο σχήμα που χρησιμοποίησε την τυχαιοποίηση στη διαδικασία κρυπτογράφησης. Ο αλγόριθμος χρησιμοποιείται για μετακβαντική κρυπτογραφία, καθώς είναι απρόσβλητος σε επιθέσεις χρησιμοποιώντας τον αλγόριθμο του Shor και – γενικότερα – τη μέτρηση καταστάσεων συνόλου .

Στο κρυπτοσύστημα McEliece για την εύρεση του ιδιωτικού κλειδιού λαμβάνεται υπόψιν ένας κώδικας διόρθωσης σφαλμάτων για τον οποίο είναι γνωστός ένας αποτελεσματικός αλγόριθμος αποκωδικοποίησης που μπορεί να διορθώσει t σφάλματα.

Ο αρχικός αλγόριθμος του συστήματος χρησιμοποιεί δυαδικούς κώδικες Goppa.Οι κώδικες αυτοί μπορούν να αποκωδικοποιηθούν αποτελεσματικά χάρη σε έναν αλγόριθμο που οφείλεται στον Patterson [53].

Η βασική ιδέα για την δημιουργία των κλειδιών είναι η εφαρμογή 2 τυχαίων πινάκων S,P πάνω στον γεννήτορα πίνακα G.

Ο McEliece με κωδικούς Goppa έχει αντισταθεί στην κρυπτανάλυση μέχρι στιγμής. Οι πιο αποτελεσματικές γνωστές επιθέσεις χρησιμοποιούν αλγόριθμους αποκωδικοποίησης συνόλου πληροφοριών. Ένα paper του 2008 περιγράφει τόσο μια επίθεση όσο και μια επιδιόρθωση.[54]

Το κρυπτοσύστημα McEliece έχει ορισμένα πλεονεκτήματα έναντι, για παράδειγμα, του RSA. Η κρυπτογράφηση και η αποκρυπτογράφηση είναι ταχύτερες[55] . Για πολύ καιρό, πιστευόταν ότι ο McEliece δεν μπορούσε να χρησιμοποιηθεί για την παραγωγή υπογραφών. Ωστόσο, ένα σχήμα υπογραφής μπορεί να κατασκευαστεί με βάση το σχήμα Niederreiter, τη διπλή παραλλαγή του σχήματος McEliece. Ένα από τα κύρια μειονεκτήματα του McEliece είναι ότι το ιδιωτικό και το δημόσιο κλειδί είναι μεγάλοι πίνακες. Για μια τυπική επιλογή παραμέτρων, το δημόσιο κλειδί έχει μήκος 512 kilobit.

4.2. Το κρυπτοσύστημα McEliece

Δημιουργία κλειδιών

Στο παράδειγμα που θα παρουσιάσουμε θα ορίσουμε έναν γεννήτορα πίνακα G που θα προκύπτει σε συμφωνία με το μαθηματικό μοντέλο που περιγράφεται από τον Valentijn [56] θεωρώντας τις παραμέτρους n=15 και k=5 για τις γραμμές και τις στήλες αντίστοιχα. Ο αριθμός διόρθωσης σφαλμάτων t στο παράδειγμα μας θεωρείτε ίσος με 3.

Ο πίνακας G που προκύπτει είναι :

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Στην συνέχεια δημιουργούμε μια τυχαία μετάθεση R για n=15.

Έστω η τυχαία μετάθεση R είναι :

$$R = [3 \;\; 4 \;\; 14 \;\; 5 \;\; 13 \;\; 8 \;\; 6 \;\; 12 \;\; 15 \;\; 2 \;\; 7 \;\; 1 \;\; 10 \;\; 9 \;\; 11]$$

Ακόμη με εφαρμογή του R στις στήλες του πίνακα ταυτότητας προκύπτει ο πίνακας P. Για παράδειγμα βλέπουμε ότι στον πίνακα R ο αριθμός 1 βρίσκεται στην δωδέκατη θέση. Οπότε

με εφαρμογή του R στις στήλες του πίνακα ταυτότητας η πρώτη στήλη του γίνεται δωδέκατη. Με ανάλογο τρόπο προκύπτουν και οι υπόλοιπες στήλες.

Ως εκ τούτου με βάση τα παραπάνω ο πίνακας P είναι:

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Από τον πίνακα R υπολογίζεται ο Ri. Συγκεκριμένα ο υπολογισμός του Ri γίνεται από τον τύπο Ri(R(j)) = j για όλα τα j στο [1 .. n].

$$Ri = [12 \quad 10 \quad 1 \quad 2 \quad 4 \quad 7 \quad 11 \quad 6 \quad 14 \quad 13 \quad 15 \quad 8 \quad 5 \quad 3 \quad 9]$$

Ο πίνακας Ri αποτελεί μια από τις παραμέτρους για την εύρεση των ιδιωτικών κλειδιών

Για την εύρεση όμως τόσο των ιδιωτικών όσο και των δημόσιων κλειδιών απαιτείται και η χρήση ενός δεύτερου τυχαίου kxk πίνακα S.

Έστω ο πίνακας S

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Ο τελικός πίνακας E που θα αποτελεί επίσης παράμετρο αυτών των κλειδιών προκύπτει από τον συνδυασμό των πινάκων S,P και G.

Συγκεκριμένα ο πίνακας E υπολογίζεται με βάση τους γνωστούς πίνακες S,G και P από την σχέση:

$$E = S \cdot G \cdot P$$

Στο παράδειγμα ο πίνακας E είναι ο :

$$E = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Τελικά το δημόσιο κλειδί θα προκύπτει από τα (E,t) και το ιδιωτικό από τα (Si,G,Ri), όπου Si ο αντίστροφος του πίνακα S.

Διαδικασία κρυπτογράφησης

Αρχικά θα θεωρήσουμε ένα τυχαίο μήνυμα m που έχει προκύψει με την μορφή k-διάστατου διανύσματος.

Έστω m = [1 0 0 0 0] το μήνυμα σε μορφή πίνακα κ διαστάσεων

Το κρυπτογραφημένο μήνυμα θα προκύψει από την σχέση:

$$c = m \cdot E + z$$

όπου z ένα τυχαίο n-διάστατο διάνυσμα.

Έστω z = [0 0 0 1 0 0 0 0 0 1 0 0 0 0 0]

Άρα το κρυπτογραφημένο μήνυμα θα είναι:

c = [1 1 0 0 0 0 0 1 1 1 0 1 1 0 0]

Διαδικασία αποκρυπτογράφησης

Αρχικά υπολογίζουμε το n-διάστατο διάνυσμα u με την εφαρμογή της μετάθεσης Ri στο διάνυσμα κρυπτογραφημένου κειμένου c

u = [1 1 1 1 0 0 0 0 0 1 0 1 0 0 1]

Στην συνέχεια βρίσκουμε ένα δεύτερο διάνυσμα v ως αποτέλεσμα της αποκωδικοποίησης του διανύσματος u.

v = [0 1 0 0 0]

Τελικά η αποκρυπτογράφηση του μηνύματος προκύπτει από τον πολλαπλασιασμό του διανύσματος v με το διάνυσμα S^{-1} και αποδίδεται με την μορφή ενός διανύσματος d.

d = [1 0 0 0 0]

Αν η αποκρυπτογράφηση έγινε σωστά το αποτέλεσμα d θα είναι ίσο με το m.

Κατά την εφαρμογή του κώδικα το διάνυσμα k διαστάσεων που θα αναπαριστά το μήνυμα προήλθε από γεννήτρια τυχαίων αριθμών. Έτσι μπορούμε να εξάγουμε το συμπέρασμα ότι ο παραπάνω κώδικας γενικεύεται για την κρυπτογράφηση και την αποκρυπτογράφηση οποιουδήποτε μηνύματος.

4.3. Το Matsumoto-Imai σχήμα υπογραφής

Οι Matsumoto-Imai χρησιμοποιώντας τις αρχές του κρυπτοσύστηματος McEliece προχώρησαν στην δημιουργία ενός σχήματος υπογραφής [52]

Η κεντρική απεικόνιση που χρησιμοποιείται στο κρυπτοσύστημα Matsumoto-Imai είναι μια απεικόνιση μεταξύ n-διάστατων διανυσμάτων που εφαρμόζεται πάνω σε ένα πεπερασμένο πεδίο (Galois Field ή GF)[57].

Τα δεδομένα μπορούν να αναπαρασταθούν ως διάνυσμα Galois και στη συνέχεια να εφαρμοστούν για την κρυπτογράφηση. Αν και αυτός ο χειρισμός από μόνος του δεν είναι ασφαλής στα κρυπτογραφικά πρότυπα, μπορεί όμως να συνδυαστεί με άλλες τεχνικές shuffling bit, με αποτέλεσμα ισχυρούς συμμετρικούς αλγόριθμους όπως ο AES.

Το extension field $GF(q^n)$ κατασκευάζεται με χρήση κάποιου μη αναγώγιμου n-βαθμού πολυωνύμου g(z) πάνω στο πεπερασμένο σώμα q.

Ως εκ τούτου και κάθε στοιχείο του πεπερασμένου σώματος q^n είναι ένα πολυώνυμο με συντελεστές στο πεπερασμένο σώμα q και βαθμό μικρότερο του n. Η απεικόνιση w , η οποία είναι μια διχοτόμηση μεταξύ διανυσμάτων n διαστάσεων του πεπερασμένου σώματος q και q^n , ορίζεται ως :

$$W: (V, V, \dots, V_{n-1}) \rightarrow V_{n-1} \cdot Z^{n-1} + \cdots + V_1 \cdot Z + V_0$$

Οι απεικονίσεις m και m^{-1} που μετασχηματίζουν τα στοιχεία του πεπερασμένου σώματος q^n μπορούν να περιγραφούν ως εξής:

$m: \varepsilon \rightarrow \varepsilon^{1+q^a}$,

$m^{-1}: \varepsilon \rightarrow \varepsilon^{b}$

Όπου a και b είναι θετικοί ακέραιοι τέτοιοι ώστε να ισχύει :

$$(1 + q^a) \cdot b \bmod (q^n - 1) = 1 \quad (1)$$

Η απεικόνιση F και ο αντίστροφος του ορίζονται από τις σχέσεις:

$F = W^{-1} \circ m \circ W$,

$F^{-1} = W^{-1} \circ m^{-1} \circ W$

Στην παρούσα υλοποίηση και σε συμφωνία με την (1) θεωρούμε τις παραμέτρους n=6, q=2 , a=4 , b=26.

Ο απεικόνιση F περιγράφεται ως:

$$F: (V_0, \dots, V_{n-1}) \rightarrow (U_0, \dots, U_{n-1}) \quad (2)$$

Η αντιστοίχιση αυτή παρέχει το δημόσιο κλειδί με παραμέτρους

$$(p_0(x_0, \dots, x_{n-1}), \dots p_{n-1}(x_0, \dots, x_{n-1}))$$

Με γνώση των παραπάνω τιμών για τα n,q,a,b και της σχέσης (2) οι παράμετροι v_i και u_i περιγράφονται από τις παρακάτω εξισώσεις αν εφαρμοστούν στο GF(2):

$$U_5 = V_5 \cdot V_4 + V_5 \cdot V_2 + V_3^2 + V_5^2 + V_2^2 + V_4^2 + V_1^2 + V_3 \cdot V_2 + V_4 \cdot V_1 + V_5 \cdot V_1$$

$$U_4 = V_4 \cdot V_2 + V_4 \cdot V_0 + V_5^2 + V_0 \cdot V_1 + V_3 \cdot V_2 + V_5 \cdot V_1 + V_5 \cdot V_2 + V_5 \cdot V_3 + V_2 \cdot V_1 + V_5 \cdot V_4 + V_4 \cdot V_1$$

$$U_3 = V_3 \cdot V_2 + V_2 \cdot V_0 + V_4 \cdot V_2 + V_3^2 + V_2 \cdot V_1 + V_4 \cdot V_1 + V_5 \cdot V_4$$

$$U_2 = V_2^2 + V_2 \cdot V_0 + V_5 \cdot V_1 + V_4 \cdot V_2 + V_5^2 + V_3 \cdot V_0 + V_4 \cdot V_3 + V_5 \cdot V_0 + V_3 \cdot V_2 + V_2 \cdot V_1 + V_5 \cdot V_3 + V_1^2 + V_3 \cdot V_1$$

$$U_1 = V_4 \cdot V_0 + V_5 \cdot V_0 + V_3^2 + V_1^2 + V_5 \cdot V_3 + V_4 \cdot V_2 + V_5 \cdot V_2 + V_3 \cdot V_2$$

$$U_0 = V_3^2 + V_0 \cdot V_1 + V_4 \cdot V_3 + V_0^2 + V_5^2 + V_2 \cdot V_0 + V_3 \cdot V_0 + V_2 \cdot V_1 + V_3 \cdot V_2$$

Διαδικασία υπογραφής μηνύματος

Αρχικά γίνεται κατακερματισμός του μηνύματος και μετατροπή των ψηφίων του σε n-διάστατο διάνυσμα (h) πάνω στο πεπερασμένο σώμα q. Στην συνέχεια εφαρμόζουμε τον αντίστροφο του αρχικού πίνακα πάνω στην h .

Στο επόμενο βήμα γίνεται εφαρμογή της F^{-1} στον πίνακα που προκύπτει από το προηγούμενο στάδιο. Για το στάδιο αυτό απαιτείται να γίνει απεικόνιση του πολυωνύμου g(z) σε ακέραιη μορφή. Τελικά με εφαρμογή του S^{-1} προκύπτει η υπογραφή του μηνύματος E.

Επαλήθευση της ψηφιακής υπογραφής

Για την επαλήθευση της υπογραφής γίνεται εφαρμογή του P στο E. Το αποτέλεσμα που προκύπτει θα πρέπει να είναι ίδιο με την τιμή h , που προήλθε από τον κατακερματισμό του μηνύματος. Αν ισχύει αυτή η συνθήκη τότε η αποκρυπτογράφηση του μηνύματος έγινε σωστά.

Ένα από τα σημαντικότερα προβλήματα του σχήματος είναι ότι παρέχει μεγάλου μεγέθους δημόσιο κλειδί κάτι που καθιστά επίπονη την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης [58]. Επίσης το σχήμα αυτό έχει το μειονέκτημα ότι λόγο του τρόπου τυχαιοποίησης η ασφάλεια του είναι περιορισμένη σε σχέση με σχήματα που αναπτύχθηκαν μεταγενέστερα.

Εξαιτίας αυτών των προβλημάτων δημιουργήθηκε η ανάγκη για την ανάπτυξη πιο αποτελεσματικών σχημάτων . Στην συνέχεια θα αναφερθούμε στην προτεινόμενη μέθοδο βοηθάει στο να περιοριστούν τα παραπάνω προβλήματα.

5. Η Προτεινόμενη μέθοδος

Προτείνετε το P-QBN που παρουσιάστηκε στο κεφάλαιο 3.3.2 που είναι ένα νέο lattice-based σχήμα υπογραφής. Στο σχήμα αυτό τα δημόσια και ιδιωτικά κλειδιά δημιουργούνται από την τεχνολογία Bonsai Trees όπως αναλύθηκε στο εδάφιο 2.3.1 για την δημιουργία κλειδιών. Η μέθοδος που χρησιμοποιείται παράγει σύνολο κλειδιών με την χρήση αλγορίθμου για την δημιουργία τυχαίας βάσης αλγορίθμου RandBasis και ενός αλγόριθμου ExtBasis, οι οποίοι όχι μόνο μπορούν να δημιουργήσουν ένα απλό μη-ντετερμινιστικό σύνολο κλειδιών, αλλά εξασφαλίζουν την τυχαιότητα των δευτερευόντων κλειδιών. Το σχήμα αυτό μπορεί να προσφέρει ασφάλεια έναντι κβαντικών επιθέσεων στο P-QBN.

5.1. Εισαγωγή στο πρόβλημα

Όσον αφορά τον μετά-κβαντικό μετριασμό, η κρυπτογραφία πλέγματος είναι κατάλληλη για τον σχεδιασμό του quantum resisting signature σχήματος στο P-QBN. Το 2008, στην αναφορά [59] παρουσιάζεται το πρώτο αποδεδειγμένο ασφαλές πλέγματος-βάσης σχήμα υπογραφής στο οποίο ένα novel cryptographic primitive που ονομάζεται συνάρτηση δείγματος προ-εικόνας (preimage sample function -PSF) και χρησιμοποιείται για την δημιουργία ενός τυχαίου oracle το οποίο ανάγεται στο πρόβλημα της σύντομης ακέραιας λύσης (SIS) [23] .

Στις παραπομπές [15] και [32] σχεδιάστηκαν δύο νέα σχέδια υπογραφής στο πρότυπο μοντέλο, με χρήση αλγορίθμου δέντρων μπονσάι . Η χρήση αυτού μπορεί να επεκτείνει την συνάρτηση αποκρυπτογράφησης από χαμηλότερη σε υψηλότερη διάσταση. Ωστόσο, το μέγεθος του δημόσιου κλειδιού και του ιδιωτικού κλειδιού στα δύο παραπάνω σχήματα είναι μεγάλο, επειδή τα κλειδιά ελέγχου ταυτότητας πρέπει να αποτελούνται από μια ομάδα πινάκων που έχουν ως αποτέλεσμα το μεγάλο μέγεθος χώρου του ελέγχου ταυτότητας κλειδιών. Στη συνέχεια, [60] πρότεινε ένα πιο αποτελεσματικό πλέγμα βάσης υπογραφής σχήματος, αυτό το σχήμα ήταν ασφαλές ενάντια σε επιθέσεις επιλεγόμενου μηνύματος για υπογραφή. Οι [61], [62]. παρουσίασαν τα αντι-κβαντικά κρυπτογραφικά σχήματα με βάση την κρυπτογραφία πλέγματος για την ενίσχυση της συναλλαγής διαδικασία ελέγχου ταυτότητας σε P-QBN.

Στην εργασία των [61] πήραν την τεχνολογία Bonsai Tree για να κατασκευάσουν ένα λιτό μη καθορισμένο πορτοφολιού και πρότειναν μια νέα αντικβαντική μέθοδο ελέγχου ταυτότητας για το blockchain. Οι [62] έδωσαν έναν απλό ορισμό του PQB και παρουσίασαν μια ασφαλή δομή κρυπτονομίσματος που βασίζεται στο PQB. Αν και τα προηγούμενα αναφερόμενα κρυπτογραφικά σχήματα μπορούν να παρέχουν το θεωρητική υπόβαθρο της εφαρμογής του blockchain στην μετακβαντική περίοδο, δεν είναι όμως αποτελεσματικά και πρακτικά στο P-QBN

Η τεχνολογία Blockchain έχει αποκτήσει σημαντική προβολή τα τελευταία χρόνια λόγω του δημόσιου χαρακτήρα της διανομής τους και των αποκεντρωμένων χαρακτηριστικών, τα οποία εφαρμόστηκαν ευρέως σε όλους τους τομείς της ζωής. Ωστόσο, στα περισσότερα κρυπτογραφικά πρωτόκολλα που χρησιμοποιούνται στο τρέχον blockchain, τα δίκτυα είναι ευαίσθητα στην κβαντική επίθεση με την ταχεία ανάπτυξη ενός επαρκώς μεγάλου κβαντικού υπολογιστή.

Θα ακολουθήσει μια περιγραφή του blockchain και θα επιχειρήσω να δώσω μια επισκόπηση των τρωτών σημείων των σύγχρονων δικτύων blockchain σε έναν κβαντικό αντίπαλο και μερικές πιθανές μετά-κβαντικές μεθόδους μετριασμού. Στην συνέχεια της εργασίας θα γίνει περιγραφή ενός νέου δικτυωτού πλέγματος υπογραφής σχήματος, που έχει προταθεί και μπορεί να χρησιμοποιηθεί για την διασφάλιση του δικτύου blockchain από το υπάρχον κλασικά κανάλια. Επιπλέον, δίνουμε λεπτομερή περιγραφή της μετα-κβαντικής συναλλαγής blockchain.

5.2. Τι είναι το blockchain

Το blockchain είναι επί της ουσίας μία σειρά καταχωρίσεων που λαμβάνουν χώρα σε συναλλαγές, σε ένα δημόσιο κατάστιχο (ledger). Κάθε καινούρια ομάδα καταχωρήσεων - ένα «block»- συνδέεται με τα προηγούμενα, δημιουργώντας μία «αλυσίδα» καταχωρίσεων, δηλαδή ένα «blockchain».

Τα blocks αυτά συνδέονται μονοσήμαντα μεταξύ τους. Αναδύονται δε μέσα από μια διαδικασία που ονομάζουμε «proof of work», κατά την οποία επιτυγχάνεται η αλγοριθμική επίλυση ενός «δύσκολου» υπολογιστικού προβλήματος. Κατ' αυτό τον τρόπο, το blockchain

λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες, μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του. Απώτερος στόχος αυτού είναι η εξασφάλιση της ασφάλειας και η διαφάνεια των συναλλαγών. Η ειδοποιός διαφορά αναφορικά με την προστασία έγκειται στο γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής (πχ. μιας τράπεζας), ενώ η εκατέρωθεν εμπιστοσύνη των συναλλασσόμενων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

Η δημόσια πρόσβαση στο blockchain διευκολύνει τη διαφάνεια στις συναλλαγές και τη διάχυση της πληροφορίας. Υπό το πρίσμα αυτών των συνθηκών , διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων, ακριβώς εξαιτίας της δημόσιας φύσης των δεδομένων. Ταυτόχρονα, τείνει να μη θεωρείται απαραίτητη και η ανάγκη για ενδιάμεσα μέρη που αυξάνουν τα κόστη, αφού όλες οι πληροφορίες που αφορούν στη συναλλαγή βρίσκονται κρυπτογραφημένες μέσα στο blockchain. Χρησιμοποιώντας το παράδειγμα των τραπεζών βλέπουμε ότι οι τράπεζες μπορούν να κατορθώσουν να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με την ελαχιστοποίηση του χρόνου διακανονισμού αλλά και την κατάργηση μίας σειράς διαδικασιών που κοστίζουν σε χρόνο και χρήμα. [63] [64]

Βέβαια δεν εστιάζουμε μόνο σε αυτό. Θα παρατηρηθούν μία σειρά από υπηρεσίες και λύσεις στον χρηματοπιστωτικό κλάδο που θα παρουσιάζουν τάσεις βελτίωσης , πιο ασφαλείς και θα απαιτούν λιγότερο χρόνο υλοποίησης με τη χρήση του blockchain. Διευρύνοντας το πλαίσιο, υπάρχουν και αρκετές ακόμη ιδέες που θα μπορούσαν να αξιοποιήσουν τη συγκεκριμένη τεχνολογία και να εμφανίσουν πολλά νέα προϊόντα και λύσεις για τον χρηματοπιστωτικό κλάδο.

5.3.Κρυπτογραφία blockchain

Οι Blockchains χρησιμοποιούν δύο τύπους κρυπτογραφικών αλγορίθμων, τους αλγόριθμους ασύμμετρου-κλειδιού και τις συναρτήσεις κατακερματισμού. Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται για να παρέχουν τη λειτουργικότητα μιας μοναδικής προβολής του blockchain σε κάθε συμμετέχοντα. Οι Blockchains χρησιμοποιούν γενικά τον αλγόριθμο κατακερματισμού SHA-256 ως λειτουργία κατακερματισμού.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού παρέχουν τα ακόλουθα οφέλη για το blockchain:

Avalanche effect: Μια μικρή αλλαγή στα δεδομένα μπορεί να έχει ως αποτέλεσμα μια σημαντικά διαφορετική έξοδο.

Uniqueness: Κάθε είσοδος έχει μοναδική έξοδο.

Deterministic: Κάθε είσοδος θα έχει πάντα την ίδια έξοδο εάν περάσει από τη συνάρτηση κατακερματισμού.

Quickness: Η έξοδος μπορεί να δημιουργηθεί σε πολύ μικρό χρονικό διάστημα.

Η αντίστροφη μηχανική δεν είναι δυνατή, δηλαδή δεν μπορούμε να δημιουργήσουμε την είσοδο έχοντας την έξοδο και τη συνάρτηση κατακερματισμού.

Οι συναρτήσεις κατακερματισμού διαδραματίζουν σημαντικό ρόλο στη σύνδεση των μπλοκ μεταξύ τους και επίσης στη διατήρηση της ακεραιότητας των δεδομένων που είναι αποθηκευμένα μέσα σε κάθε μπλοκ. Οποιαδήποτε αλλαγή στα δεδομένα μπλοκ μπορεί να οδηγήσει σε ασυνέπεια και να σπάσει το blockchain, καθιστώντας το άκυρο. Αυτή η απαίτηση επιτυγχάνεται με την ιδιότητα των λειτουργιών κατακερματισμού, που ονομάζεται «φαινόμενο χιονοστιβάδας» (Avalanche effect) .

Σύμφωνα με αυτό, εάν κάνουμε ακόμη και μια μικρή αλλαγή στην είσοδο στη συνάρτηση κατακερματισμού, θα καταλήξουμε να έχουμε μια εντελώς άσχετη έξοδο σε σύγκριση με την αρχική έξοδο.

Είναι απαραίτητο να διασφαλιστεί η ασφάλεια του ασύμμετρου αλγορίθμου κρυπτογράφησης κατά τη μετάδοση δεδομένων στο blockchain. Η επιβεβαίωση και επικύρωση των δεδομένων στο blockchain γίνονται με την βοήθεια των ψηφιακών υπογραφών.

Συμπερασματικά μπορούμε να πούμε ότι ο κατακερματισμός, τα ζεύγη κλειδιών δημόσιου-ιδιωτικού και οι ψηφιακές υπογραφές αποτελούν το θεμέλιο για το blockchain. Αυτές οι κρυπτογραφικές δυνατότητες καθιστούν δυνατή την ασφαλή σύνδεση των μπλοκ με άλλα μπλοκ και επίσης διασφαλίζουν την αξιοπιστία και την αμετάβλητη των δεδομένων που είναι αποθηκευμένα στο blockchain.

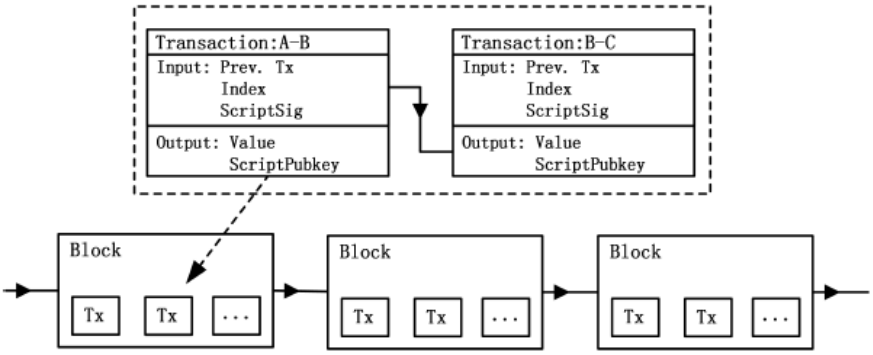
Υπάρχει ένας τεράστιος αριθμός εφαρμογών τεχνολογίας blockchain που η κρυπτογραφία τις καθιστά δυνατές. Μία από τις σημαντικότερες εφαρμογές κρυπτογραφίας πραγματικού κόσμου στο blockchain είναι τα κρυπτονομίσματα.

5.4. Η Μετά - Κβαντική blockchain συναλλαγή

Σύμφωνα με ότι γνωρίζουμε έως σήμερα για την προτεινόμενη κβαντική ανθεκτική υπογραφή Σχήματος (quantum-resistant signature scheme) , τα τρέχοντα συστήματα με δυνατότητα blockchain μπορούν αντισταθούν στις κβαντικές επιθέσεις, οι οποίες μπορούν να θεωρηθούν ως PQB (Post Quantum Blockchain) [65]. Η μετα-κβαντική συναλλαγή blockchain θα προστατεύεται από το μετα-κβαντικό κρυπτογραφικό σχήμα. Η διαδικασία αυτή είναι διαδικασία τριών σταδίων . Κατά το πρώτο στάδιο έχουμε την προετοιμασία της συναλλαγής. Στο δεύτερο έχουμε την υλοποίηση αυτής και στο τρίτο έχουμε την επιβεβαίωση της συναλλαγής.

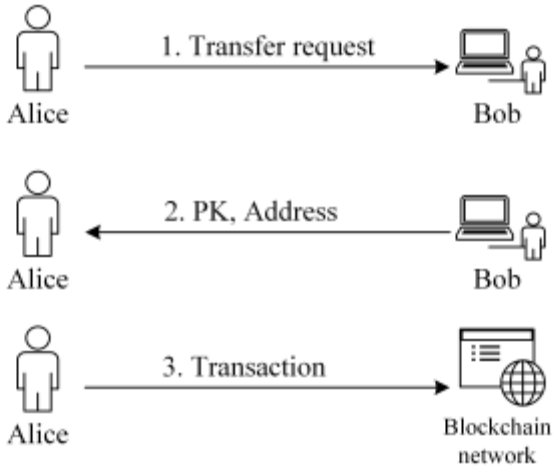
Αναλυτικότερα στο πρώτο στάδιο, που είναι η προετοιμασία της συναλλαγής είτε ο γενικός χρήστη ή ο miner, λειτουργούν ως διαφορετικοί, ανεξάρτητες οντότητες για την κατασκευή του κατανεμημένου δικτύου blockchain. Η διεύθυνση συναλλαγής είναι το πιο σημαντικό για την εκτέλεση της συναλλαγής. Εδώ, η διεύθυνση δημιουργείται από το δημόσιο κλειδί. Προκειμένου να αντισταθεί στη στατιστική επίθεση, μια νέα διεύθυνση θα δημιουργηθεί από ένα διαφορετικό δημόσιο κλειδί για μια νέα συναλλαγή. Επομένως, κάθε χρήστης στο blockchain δίκτυο πρέπει να αποθηκεύει πολύ περισσότερα ζευγάρια από δημόσια και ιδιωτικά κλειδιά για νέες συναλλαγές και το wallet θα γίνει περισσότερο διογκωμένο. Ωστόσο, το lightweight wallet που έχει σχεδιαστεί στο πρώτο προτεινόμενο σύστημα υπογραφής μπορεί να λύσει αυτό το πρόβλημα, το οποίο χρειάζεται μόνο για να αποθηκεύει το αρχικό κλειδί. Μειώνοντας τον πλεονασμό του wallet, είναι πιο κατάλληλο για την υλοποίηση της συναλλαγής στο blockchain.

Στο δεύτερο στάδιο, που είναι η υλοποίηση της συναλλαγής, όπου στην πραγματικότητα , μια συναλλαγή είναι μια δομή δεδομένων που περιλαμβάνει είσοδο και έξοδο. Ως είσοδος έχουμε το Προηγούμενο tx, index και ScriptSig, εδώ το Προηγούμενο tx είναι η τιμή Hash της προηγούμενης συναλλαγής. index είναι ο δείκτης τιμών της προηγούμενης παραγωγής tx και το ScriptSig είναι η υπογραφή του κατόχου της συναλλαγής. Κατά την έξοδο με το Value και ScriptPubkey, που είναι η αξία της συναλλαγής και το δημόσιο κλειδί του δέκτη, αντίστοιχα (εικόνα 4.1).



Εικόνα 4.1: σχηματική απεικόνιση της συναλλαγής επαλήθευσης. Πηγή: [65]

Εάν ο χρήστης Α θέλει να στείλει μερικά bitcoin μέσω μιας συναλλαγής στον χρήστη Β, θα εκτελέσουν τα ακόλουθα τρία βήματα για την ολοκλήρωση αυτής της συναλλαγής (Εικόνα 4.2). Πρώτον, ο χρήστης Α ξεκινά ένα αίτημα μεταφοράς. Δεύτερον, ο χρήστης Β επιλέγει ένα ζεύγος δημόσιων και ιδιωτικών κλειδιών, δημιουργεί μια διεύθυνση και την αποστέλλει στο χρήστη Α για την εκτέλεση της συναλλαγή . Τέλος, ο χρήστης Α δημιουργεί αυτήν τη συναλλαγή και την μεταδίδει σε ολόκληρο το δίκτυο. Επιπλέον, είναι σημαντικό να τονιστεί ότι το συνολικό ποσό εισόδου της συναλλαγής πρέπει να ισούται με το συνολικό ποσό εξόδου. Αν για τον χρήστης Α το ποσό εξόδου είναι μεγαλύτερο από το απαιτούμενο ποσό, θα έπρεπε δημιουργήστε μια νέα διεύθυνση για να ληφθεί το πλεόνασμα bitcoin. Για τον miner, η ανταμοιβή για τη δημιουργία ενός νέου μπλοκ έχει επίσης καταγραφεί ως συναλλαγή στο blockchain. Στη διαδικασία εξόρυξης, κάθε miner θα δημιουργήσει μια ειδική ανταμοιβή συναλλαγής στο προσωρινό μπλοκ που περιέχει επίσης τις συναλλαγές που μεταδίδονται σε ολόκληρο το blockchain δίκτυο την τελευταία χρονική περίοδο. Μόλις ένας miner αποκτήσει τα δικαιώματα δημιουργίας του νέου μπλοκ, η συναλλαγή ανταλλαγής που πρόσθεσε θα γίνει αναλώσιμη για την κύρια συναλλαγή.



Εικόνα 4.2: Σχηματική απεικόνιση της υλοποίησης της συναλλαγής. Πηγή: Li, Chen, Chen, Hou, & Li, 2019)

Τέλος κατά το τρίτο στάδιο που έχουμε την επιβεβαίωση της συναλλαγής, οι συναλλαγές που μεταδόθηκαν στο δίκτυο και επαληθεύτηκαν από τον miner, θα συλλεχθούν και θα μεταφερθούν στο προσωρινό μπλοκ. Όταν δημιουργηθεί το μπλοκ για την τελευταία χρονική περίοδο, το προσωρινό μπλοκ θα γίνει το νέο μπλοκ. Όλες οι συναλλαγές σε αυτό το μπλοκ έχουν επαληθευτεί για μια φορά συνδέοντας το νέο μπλοκ στη μακρύτερη αλυσίδα. Από εκείνη την χρονική στιγμή και έπειτα οι συναλλαγές σε αυτό το μπλοκ θα επαληθευτούν πολλές φορές μαζί με τα ακόλουθα νέα μπλοκ που δημιουργήθηκαν. Κάθε φορά το νέο μπλοκ δημιουργείται με βάση το προηγούμενο. Γενικά, μετά από έξι μπλοκ, αυτές οι συναλλαγές δεν μπορούν να τροποποιηθούν λόγω του τεράστιου υπολογισμού για την ανοικοδόμηση έξι μπλοκ. Σε αυτό το σημείο, μια συναλλαγή έχει αποθηκευτεί ως αναλλοίωτη εγγραφή στο blockchain.

5.5. Πρωτόκολλο proof-of-work (pow) και proof-of-stake(pos)

Το πρωτόκολλο pow χρησιμοποιείται για να βρεθεί η μορφή του timestamp. Τα συστήματα αυτά βασίζονται κυρίως στην επίλυση ενός προβλήματος αναζήτησης Το pow δημιουργεί ένα μπλοκ που έχει την τιμή της hash function της προηγούμενης συναλλαγής (προηγούμενου μπλοκ), έναν δείκτη που αντιστοιχεί στην προηγούμενη συναλλαγή και υπογράφει κάθε συναλλαγή με διαφορετικό ScriptSig. Στην πραγματικότητα για να δημιουργηθεί ένα νέο μπλοκ ο αλγόριθμος Grover που χρησιμοποιείται κάνει επιβεβαίωση

των hashes όλων των προηγούμενων με έναν τυχαίο αριθμό και ελέγχει αν έχουμε N zeros στο νέο μπλοκ. Αν δεν υπάρχουν ξαναφτιάχνει το μπλοκ. Το N zeros είναι αυτό που δείχνει πόσα nonce έχω και μου δείχνει το σημείο της αλυσίδας που βρίσκομαι. [66]

Ένας τρόπος με τον οποίο μπορούμε να κάνουμε επίθεση είναι με την δημιουργία μιας άλλης συνάρτησης κατακερματισμού, που θα δίνει το ίδιο αποτέλεσμα. Αυτό μπορεί να επιτευχθεί διότι η sha που χρησιμοποιούμε δεν είναι collision free, δηλαδή 2 διαφορετικοί αριθμοί μπορούνε να δώσουν ίδιο αποτέλεσμα. Έτσι δημιουργούμε ένα νέο μπλοκ πριν γίνει ο έλεγχος από τον miner. Για να αποφευχθεί αυτού του είδους η επίθεση αναπτύχθηκε το pos [67]. Το πρωτόκολλο αυτό είναι πιο γρήγορο από το προηγούμενο του , με αποτέλεσμα να δυσκολεύει την αντικατάσταση της sha συνάρτησης πριν δοθεί απάντηση από τον miner. Παρά το πλεονέκτημα του δεν αποφεύγεται ούτε με αυτό τον τρόπο η πιθανότητα της επίθεσης διότι το πρωτόκολλο αυτό είναι ευάλωτο στην shor επίθεση που βασίζεται στον shor αλγόριθμο.

6. Προτεινόμενο σχέδιο υπογραφής

6.1. Υπολογιστικές λεπτομέρειες

Στην ενότητα αυτή θα αναφερθούμε στις συνθήκες που απαιτούνται για το προτεινόμενο σχέδιο υπογραφής καθώς και στον τρόπο με τον οποίο μπορεί να υλοποιηθεί με την βοήθεια λημμάτων που έχουν αναλυθεί παραπάνω.

Αρχικά λαμβάνουμε 3 παραμέτρου n,m και q που πρέπει να ακολουθούν τις παρακάτω συνθήκες:

- Ο αριθμός n πρέπει να είναι πρώτος αριθμός
- Ο αριθμός m θα προκύπτει από τον n σύμφωνα με την σχέση m=2nlogq
- Ο αριθμός q είναι ένας αριθμός που προκύπτει ως poly(n) .

Σημείωση: Για να μπορέσει ο αριθμός n να εκφραστεί ως poly(n) και να τον αντιστοιχήσουμε στον q θα πρέπει να είναι ένας αρκετά μεγάλος αριθμός.

Επίσης κάνουμε χρήση μιας συνάρτησης κατακερματισμού H για την οποία ισχύει:

$\{0,1\}^* = \{0,1\}^*$

Τέλος για το πλέγμα L και για την γκαουσιανή παράμετρο s ισχύουν :

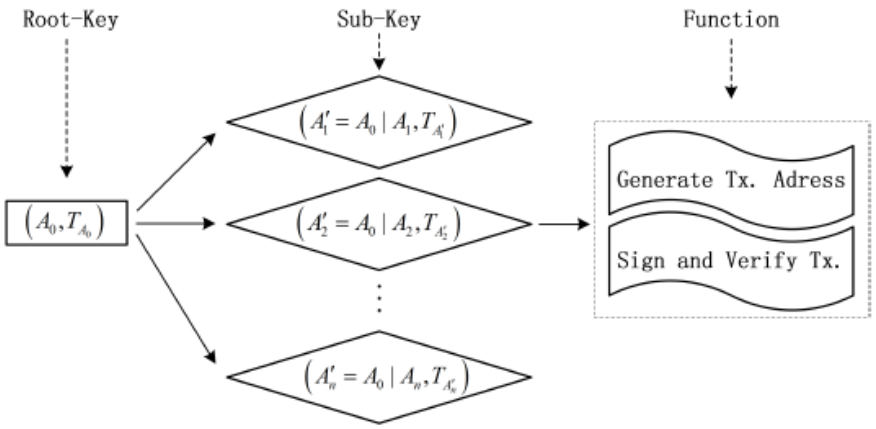
$$\tilde{L} \geq O(\sqrt{nlogq})$$

Και

$$s = \tilde{L}\omega(\sqrt{logn})$$

Στην συνέχεια για την εύρεση της βάσης T_{A_0} θα κάνουμε χρήση ενός PPT (probabilistic polynomial-time) αλγόριθμου Trapgen. Ο αλγόριθμος αυτός δέχεται ως είσοδο τις παραμέτρους n,q και λαμβάνονται υπόψιν τους περιορισμούς και τις συνθήκες του λήμματος που σχετίζονται με αυτές τις παραμέτρους δίνει ως έξοδο έναν ομοιόμορφο τυχαίο πίνακα n x m $A_0 \in Z_q^{nxm}$ και μια βάση T_{A_0} τέτοια ώστε: $\|\tilde{T}_{A_0}\| \leq O(\sqrt{nlogq})$.

Τα A_0 , T_{A_0} αποθηκεύονται ως κύρια βάση του δικτυωτού (root lattice basis) και από τον αλγόριθμο bonsai tree παράγονται τα sub-public και private κλειδιά (εικόνα 5.1)



Εικόνα 5.1: Η δημιουργία κλειδιών με βάση το δικτυωτό πλέγμα Bonsai. Πηγή: : [65]

Συγκεκριμένα για την δημιουργία των κλειδιών και την εξασφάλιση της ανωνυμίας των χρηστών αρχικά διαλέγουμε 2 ομοιόμορφους πίνακες n x m

$A_i = \{A_1, A_2, \dots, A_n\}$, όπου i=1,2,3,…,n και $B_j = \{B_1, B_2, \dots, B_n\}$ όπου j= 1,2,3,…,l .

Στην συνέχεια υπολογίζουμε τα εκάστοτε A_i' σύμφωνα με την σχέση $A_i' = A_0 + A_i$. Το A_i' χρησιμοποιείται προκειμένου να παραχθούν τα δημόσια κλειδιά για την επαλήθευση της υπογραφής. Ο αλγόριθμος **ExtBasis** σε συνδυασμό με τον **RandBasis** παράγουν την αντιστοίχιση των κλειδιών ως εξής:

$$T_{A_i'} \leftarrow \mathbf{RandBasis}\left(\mathbf{ExtBasis}\left(T_{A_0}, A_i' = A_0 \mid A_i, s\right), s\right)$$

Τα παραχθέντα δημόσια κλειδιά χρησιμοποιούνται στην συναλλαγή για την δημιουργία διευθύνσεων (Tx) και για την επαλήθευση της υπογραφής όπως έχει ήδη αναφερθεί, σε συνδυασμό βέβαια με τα ιδιωτικά κλειδιά, με μορφή ζευγών ($A_i', T_{A_i'}$). Τέλος για να εξασφαλίσουμε την ανωνυμία των χρηστών θα πρέπει κάθε ζεύγος να γίνεται χρήση μία φορά.

Πως γίνεται η διαδικασία υπογραφής

Έστω ότι δίνουμε ένα μήνυμα m για κρυπτογράφηση. Με την βοήθεια μιας συνάρτησης κατακερματισμού H της μορφής H(m) = (m[1], m[2],…, m[n]) και ενός μυστικού ιδιωτικού κλειδιού $T_{A_i'}$ ως είσοδο στον αλγόριθμο ο υπογράφων πραγματοποιεί τα παρακάτω βήματα:

I. Αν m[j] =1 , τότε επιλέγουμε τον πίνακα B_j που έχουμε ήδη ορίσει , διαφορετικά θέτουμε το m[j] =0 και δεν επιλέγουμε τίποτα. Αν ισχύει η συνθήκη τότε το l* είναι το Hamming weight του μηνύματος και ορίζουμε:
$B_m = (A_\iota \| B_{j1} \| \dots . \| B_{ji^*})$

II. Στην συνέχεια συνδυάζοντας τον αλγόριθμο **SampleD** με γνωστό λήμμα που αναφέρεται στο τρόπο που λειτουργεί η ExtBasis δημιουργούμε την υπογραφή $v \in Z_q^{(l^*+l)m}$ της συναλλαγής του μηνύματος ως εξής:

$$v \leftarrow \mathbf{SampleD}(\mathbf{ExtBasis}\left(T_{A_i'}, B_m, s\right), s)$$

<u>Για την επιβεβαίωση</u>

Δίνουμε ως είσοδο το μήνυμα m και την υπογραφή v, αν ισχύει:

$B_m v = 0(\mathrm{mod} q)$ υπό την προϋπόθεση $\|v\| \leq s\sqrt{(l^* + l)m}$ τότε η κρυπτογράφηση έγινε σωστά σε αντίθετη περίπτωση όχι.

6.2. Απόδειξη ασφάλειας του σχήματος.

Στην ενότητα αυτή θα δώσουμε μια λεπτομερή απόδειξη της ασφάλειας του προτεινόμενου σχήματος υπογραφής.
Είναι χρήσιμο για την καλύτερη κατανόηση του να αναφερθούμε σε 2 βασικά θεωρήματα
<u>Θεώρημα 1:</u>
Το προτεινόμενο σχήμα υπογραφής στο P-QBN είναι ισχυρά ασήμαντο κάτω από την προσαρμοσμένη επίθεση μηνυμάτων υπό την πιθανότητα $\frac{\varepsilon}{lq2}$.

Άμεση απόρροια του θεωρήματος αυτού είναι και το παρακάτω θεώρημα (θεώρημα 2) για την ασφάλεια του σχήματος.
<u>Θεώρημα 2:</u>
Ένα challenger R μπορεί να λύση το SIS instance με την πιθανότητα $\frac{\varepsilon}{lq2}$ (όπου l είναι το μήκος του μηνύματος m της συναλλαγής) αν ένας αντίπαλος G μπορεί να σπάσει το

προτεινόμενο σχήμα με μια πιθανότητα ε κάτω από την προσαρμοσμένη επίθεση των επιλεγμένων μηνυμάτων με q2 φορές signing queries.

Η απόδειξη αυτού του θεωρήματος έχει ως εξής.

Αρχικά υποθέτουμε ότι ένας challenger R λαμβάνει ένα SIS instance ως εξής:

$$SIS_{n,(l+2)m,q,2s\sqrt{(l+1)m}} = (\bar{B}, n, m, l, q, s)$$

Όπου $\bar{B} = (\bar{B}_0, \dots, \bar{B}_k)$ και το $\bar{B}_\iota \in Z_q^{(l^*+1)m}$.

Τότε στόχος είναι να βρεθεί ένα σύντομο διάνυσμα που να ικανοποιεί την :

$\bar{B}v = 0\ (modq), \|v\| \leq s\sqrt{(l+1)m}$

Η διαδικασία που θα ακολουθήσουμε για το πετύχουμε είναι:

Ο challenger R εκτελεί της ενέργειες του G για να λάβει q2 μηνύματα $m^{(1)}$, $m^{(2)}$,…, $m^{(q2)}$

Στην συνέχεια υπολογίζει το σύνολο $P = \{p|p\ \in \{0,1\}^{\leq k}\}$

Όπου η μικρότερη συμβολοσειρά bit του p δεν είναι το σύνολο των $m^{(i)}$. Σύμφωνα με την αναφορά [15] αυτό το είδος των συνόλων μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο και ο αριθμός p είναι το πολύ lq2.

Ακολούθως ο R επιλέγει τυχαία ένα $p \in P$ και ορίζει τα σύνολα του hamming weight και το μήκος του p να είναι t και |p| αντίστοιχα. Η δημιουργία του δημόσιου κλειδιού από τον R γίνεται ως εξής:

- Αρχικά επιλέγουμε τυχαία ένα |p| -t trapdoor του πλέγματος $\Lambda_q^{\perp}C(j)$και της trapdoor βάσης $T_j \in Z_q^{mxm}$, όπου το $C(j) \in\ Z_q^{nxm}$ και το $j \neq t_i\ , i = 1,2, \dots, t$ και ορίζουμε B =$\bar{B}_0$
- Όταν το i< |p| λαμβάνουμε κάθε $B_{t_i} = \bar{B}_{t_i}$ για κάθε t_i< |p| και $p_{t_i} = 1.$ Σε οποιαδήποτε άλλη περίπτωση ορίζουμε $A_j = B_j$
- Όταν το i> |p| τότε το $B_i = \bar{B}_i$

Έτσι δημιουργούνται τα δημόσια κλειδιά $(B_i, C_1, \dots, C_k)$ και ο challenger R τα αποστέλλει στον χρήστη G μαζί με τις παραμέτρους (n,m,q,s,k) και ξεκινάει το query-respond game. Το C φυλάσσει για λίστα L για να αποθηκεύσει τις απαντήσεις των Sign ερωτημάτων.

Υπογραφή ερωτημάτων:

Ας υποθέσουμε ότι ο αντίπαλος R λαμβάνει q2 πραγματικές τιμές κατακερματισμού, τις $m^{(1)}$, $m^{(2)}$,…, $m^{(q2)}$/ Ο G ελέγχει την λίστα L για να σιγουρευτεί ότι είναι καινούρια, σε αντίθετη περίπτωση επιστρέφει την ίδια απάντηση. Για ένα νέο μήνυμα, ο G μπορεί να

παράξει την αντίστοιχη υπογραφή. Γνωρίζουμε ότι το p δεν είναι το πρόθεμα του $m^{(i)}$, ωστόσο δύναται να ικανοποιήσει την ψευδο-τυχαιότητα ως τιμή κατακερματισμού. Στη συνέχεια, απομακρύνει τις θέσεις $t_1,t_2,\ldots,t_t$ από τις πρότερες $|p|$ θέσεις, ενώ εξακολουθεί να υπάρχει η θέση 1 με πιθανότητα $1-(\frac{1}{2})^{|p|-t}$. Ας θεωρήσουμε αυτού του είδους η θέση να είναι το t' , και ο αντίστοιχος δημόσιος πίνακας να είναι $B_{t'}=C_{t'}$ Κατά συνέπεια, ο G μπορεί να λάβει το πλέγμα $\Lambda_q^{\perp}(B_{t'})$. Ακολούθως, ο G μπορεί να δημιουργήσει την υπογραφή v_i του μηνύματος $m^{(i)}$ βασισμένη στο trapdoor βάσης του πλέγματος $\Lambda_q^{\perp}(C_{t'})$. Εν τέλει, ο G στέλνει το v_i πίσω στον αντίπαλο R και αποθηκεύει το $(v_i ,m^{(i)})$ στο L.

Όταν ο αντίπαλος R ολοκληρώνει q_2 αναζητήσεις ερωτημάτων υπογραφής, τότε δύναται να παράξει μια νέα πλαστή υπογραφή v* ενός νέου μηνύματος $\bar{m}$, και $B_{\bar{m}}v^* = 0\ (mod q)$, $\|v^*\| \leq s\sqrt{(t+1)m}$ εδώ το j* είναι το βάρος Hamming του $\bar{m}$ και ο πίνακας $B_{\bar{m}}$ είναι ίδιος όπως ο αλγόριθμος υπογραφής. Σε διαφορετική περίπτωση, το p δεν είναι το πρόθεμα του $\bar{m}$ και ο πίνακας $B_{\bar{m}}$ είναι κατά μέρος συνένωση των πινάκων $\bar{A}_0 , \bar{B}_{t1}, \ldots , \bar{B}_{tt}, \bar{B}_{|p|}, \bar{B}_{|p|+1} , \bar{B}_k$

Σύμφωνα με την σχέση του πίνακα $B_{\bar{m}}$ και B, ο G μπορεί να τοποθετήσει πίνακες στην αντίστοιχη θέση και να αλλάξει το $B_{\bar{m}}$ σε B, ενώ μπορεί επίσης να τοποθετήσει το διάνυσμα 0 στην αντίστοιχη θέση και να τροποποιήσει το διάνυσμα v* σε $\bar{v}^*$. Στην περίπτωσή αυτή είναι $B_{\bar{v}^*} = 0\ (mod q)$ και $\|\bar{v}^*\| \leq s\sqrt{(t+1)m} \leq s\sqrt{(l+1)m}$, συνεπώς ο G μπορεί να πάρει μια αποδεκτή (έγκυρη) λύση για το SIS παράδειγμα.

Από την άλλη πλευρά, με απλούς υπολογισμούς, η υπάρχουσα πιθανότητα της θέσης t' είναι $1-(\frac{3}{4})^{|p|}$, ενώ το $(\frac{3}{4})^{|p|}$ είναι αμελητέα ποσότητα. Χωρίς απώλεια της γενικότητας, ας υποθέσουμε ότι το p είναι η μικρότερου μήκους ακολουθία bit του P, άρα οι ακολουθίες bit p||0 και p||1 δεν είναι προθέματα του $m^{(i)}$. Για παράδειγμα, εάν το p είναι το πρόθεμα της ακολουθίας bit p', τότε το p' δεν είναι το πρόθεμα οποιουδήποτε $m^{(\iota)'}$. Εδώ το πλήθος των ακολουθιών bit p' με μήκος l είναι $2^{l-|p|}$. Επειδή δεν υπάρχουν περισσότερες από lq_2 ακολουθίες bit και το p είναι η μικρότερου μήκους ακολουθία bit, συνεπώς $lq_2 2^{l-|p|}$ και $|p| \geq \log_2(lq_2)$. Επομένως, κάθε ακολουθία bit μέσα στο P ικανοποιεί την σχέση $|p| \geq \log_2(lq_2)$. Η πιθανότητα $(\frac{3}{4})^{|p|}$ είναι αμελητέα καθώς $(\frac{3}{4})^{|p|} \leq (\frac{3}{4})^{log_2(lq_2)}$. Εφόσον γνωρίζουμε ότι η ακολουθία bit p έχει επιλεγεί με τυχαίο ομοιόμορφο τρόπο, τότε η πιθανότητα του p με

πρόθεμα μηνύματος m* είναι $\frac{1}{lq_2}$. Επιπλέον, ο G μπορεί να επιλύσει το πρόβλημα SIS με πιθανότητα $\frac{l}{lq_2}(1-\left(\frac{3}{4}\right)^{log_2(lq_2)}) \approx \frac{1}{lq_2}$

6.3.Σύγκριση Απόδοσης του προτεινόμενου σχήματος

Θεωρείται σκόπιμο να γίνει μια σύγκριση του προτεινόμενου σχήματος υπογραφής με αντίστοιχα σχήματα που έχουν αναπτυχθεί στην βιβλιογραφία. Θα εστιάσουμε την σύγκριση μας στο μέγεθος του ιδιωτικού, του δημόσιου κλειδιού και στο μέγεθος της υπογραφής αυτών.

Συγκεκριμένα από τον πίνακα 5.1 και με δεδομένο ότι αναφερόμαστε σε ίδιες τιμές παραμέτρων n,m,q,l μεταξύ των σχημάτων που θέλουμε να συγκρίνουμε, παρατηρούμε ότι στο σχήμα που αναπτύχθηκε από τους ([62]) το μέγεθος του δημόσιου κλειδιού είναι μεγαλύτερο σε σχέση με το προτεινόμενο της παρούσας εργασίας. Επίσης το μέγεθος της υπογραφής είναι επίσης σημαντικά μεγαλύτερο.

Ακόμη με βάση το σχήμα υπογραφής δέντρων μπονσάι των [15] και το «identity-based signature» σχήμα των δέντρων μπονσάι των [32] βλέπουμε ότι το μέγεθος τόσο του ιδιωτικού όσο και του δημόσιου κλειδιού μειώθηκε αρκετά στο αναπτυχθέν σχήμα υπογραφής. Επιπροσθέτως το μέγεθος της υπογραφής είναι αρκετά μικρότερο σε σχέση με αυτό των [15] και άμεσα συγκρίσιμο με σχέση με τους [32].

Σχήματα	Μέγεθος Δημόσιου κλειδιού	Μέγεθος ιδιωτικού κλειδιού	Μέγεθος Υπογραφής
[62]	(l+1)mnlogq	m^2logq	2mnlogq +l
Cash, Hofheinz, Kiltz, & Peikert, 2010	(2l+1)mnlogq	$4m^2$logq	(l+1)mnlogq
Lili & Sang, 2012	3mnlogq	$5m^2$logq	2mnlogq
Προτεινόμενο σχήμα	Mnlogq	m^2logq	(l/2+1)mnlogq

Πίνακας 5.1 Σύγκριση με παρόμοιες βιβλιογραφικές μελέτες

Άρα με βάση και τα προαναφερθέντα το σχήμα υπογραφής που βασίζεται σε πλέγμα δεν μπορεί μόνο να αντισταθεί στην κβαντική επίθεση, αλλά επίσης είναι και το πλέον κατάλληλο για την υλοποίηση της συναλλαγής στο P-QBN.

7. Συμπεράσματα

Συμπερασματικά μπορούμε να πούμε ότι μέσα από αυτήν την εργασία καταφέραμε να δώσουμε μια επισκόπηση των τρωτών σημείων που αντιμετωπίζουν τα σύγχρονα δίκτυα blochchain, αλλά και κάποιοι πιθανοί τρόποι με τους οποίους μπορούν να αντιμετωπιστούν αυτά τα προβλήματα.

Η παρουσίαση βέβαια αυτών των τρωτών σημείων μπορούν να δώσουν τροφή για σκέψη και να αποτελέσουν το έναυσμα για περαιτέρω έρευνα πάνω στην ανάπτυξη κατάλληλων αντικβαντικών κρυπτογραφικών εργαλείων.

Στην συνέχεια γίνεται και μια σύνοψη σε ορισμένες μετα- κβαντικές μεθόδους μετριασμού, που είναι σε θέση να παρέχουν σημαντική μείωση της αποτελεσματικότητας των κβαντικών επιθέσεων.

Ακόμη μέσα από αυτή την εργασία παρουσιάζεται ένα νέο σχήμα υπογραφής που βασίζεται στην θεωρία πλεγμάτων όπου μπορεί να χρησιμοποιηθεί για να παρέχει μεγαλύτερη ασφάλεια στο blockchain.

Επίσης γίνεται μια πλήρη περιγραφή του σχήματος κάνοντας αναφορά τόσο στα τρωτά του σημεία, αλλά και στα πλεονεκτήματα έναντι των υπολοίπων που έχουν αναπτυχθεί περιγράφοντας και την σπουδαιότητα του αλγορίθμου bonsai.

Συγκεκριμένα το σημαντικότερο ίσως από τα πλεονεκτήματα του προτεινόμενου σχήματος είναι ότι για την παραγωγή των sub-private κλειδιών γίνεται συνδυασμός των αλγορίθμων ExtBasis με τον RandBasis όπου ο δεύτερος αλγόριθμος ουσιαστικά είναι αυτός που παρέχει την τυχαιοποίση της εξόδου του αλγορίθμου ExtBasis γεγονός που τον καθιστά περισσότερο αποτελεσματικό.

Επιπλέον μέσα από την απόδειξη της ασφάλειας βλέπουμε ότι το προτεινόμενο σύστημα υπογραφής είναι ασφαλές έναντι στην προσαρμοστική επιλεγμένη επίθεση μηνύματος σε τυχαίο oracle.

Τέλος μέσω της σύγκρισης των αποτελεσμάτων μας με παρόμοιες βιβλιογραφικές μελέτες γίνετε εμφανές ότι το σχήμα που βασίζεται στην θεωρία πλεγμάτων είναι πιο αποτελεσματικό και υπερτερεί έναντι των υπολοίπων σχημάτων. Ως εκ τούτου το σχήμα αυτό είναι το πλέον κατάλληλο για την πραγματοποίηση της συναλλαγής σε P-QBN. Επίσης η εργασία αυτή μπορεί να συνεισφέρει στο να εμπλουτιστεί η έρευνα για το μελλοντικό PQB της μετακβαντικής εποχής.

Παρόλα αυτά εξαιτίας και της ραγδαίας αύξησης στην τεχνολογία των ηλεκτρονικών υπολογιστών οι κβαντικές επιθέσεις όλο και πιο έντονα μπορούν να κάνουν διάτρητο ένα

σύστημα και κατ’ επέκταση και να το καθιστούν μειωμένης ασφάλειας. Έτσι είναι σημαντικό να διερευνηθεί περισσότερο η εύρεση ενός σχήματος που να αντιστέκεται ακόμη περισσότερο στις κβαντικές επιθέσεις.

8. Βιβλιογραφία

1. Delfs, H. and H. Knebl, *Introduction to Cryptography*

Principles and Applications. Springer-Verlag New York, 2007.
2. Trappe, W. and L. Washington, *Introduction to Cryptography with Coding Theory.* Prentice Hall, 2002.
3. Bell, T., et al., *Explaining cryptographic systems.* Computers & Education, 2003. **40**(3): p. 199-215.
4. Menezes, A.J., P.C.v. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography.* CRC Press, 1996.
5. Schneier, B., *Applied Cryptography, Second Edition.* John Wiley & Sons, 1996.
6. Talbot, J. and D. Welsh, *Complexity and Cryptography (An Introduction).* Cambridge University Press, 2006.
7. Bellare, M., *Introduction to Modern Cryptography.* Course Notes, http://www.cse.ucsd.edu/users/mihir/, 2005.
8. Luciano, D. and G. Prichett, *Cryptology: From Caesar Ciphers to Public-key Cryptosystems.* The College Mathematics Journal, 1987. **18**(1): p. 2-17.
9. Singh, S., *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Knopf Doubleday Publishing Group. , 2000.
10. Shannon, C.E., *A Mathematical Theory of Communication.* Bell System Technical Journal, 1948. **27**(3): p. 379-423.
11. Shannon, C.E., *Communication Theory of Secrecy Systems**. Bell System Technical Journal, 1949. **28**(4): p. 656-715.
12. Diffie, W. and M. Hellman, *New directions in cryptography.* IEEE Trans. Inf. Theor., 2006. **22**(6): p. 644–654.
13. Rivest, R.L., A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.* Commun. ACM, 1978. **21**(2): p. 120–126.
14. Elgamal, T., *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory, 1985. **31**(4): p. 469-472.
15. Cash, D., et al. *Bonsai Trees, or How to Delegate a Lattice Basis*. 2010. Berlin, Heidelberg: Springer Berlin Heidelberg.
16. Πουλάκης, Δ., *Η επιστήμη της ασφαλούς επικοινωνίας.* Ζήτη, 2004.
17. Κάτος, Β. and Γ. Στεφανίδης, *Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης.* Ζυγός, 2003.
18. Νάστου, Π., Π. Σπυράκης, and Γ. Σταματίου, *Σύγχρονη κρυπτογραφία: Μια ξέγνοιαστη διαδρομή στα μονοπάτια της.* ΕΛΛΗΝΙΚΑ ΓΡΑΜΜΑΤΑ, 2003.
19. Blake-Wilson, S., *Information Security, Mathematics, and Public-Key Cryptography.* Des. Codes Cryptography, 2000. **19**(2–3): p. 77–99.
20. Bruschi, D., A. Curti, and E. Rosti, *A quantitative study of Public Key Infrastructures.* Comput. Secur., 2003. **22**(1): p. 56–67.
21. Mao, W., *Modern Cryptography: Theory and Practice.* Prentice Hall, 2003.
22. Meyers, R.A., *Encyclopedia of Complexity and Systems Science.* Springer-Verlag New York, 2009.
23. Ajtai, M., *Generating hard instances of lattice problems (extended abstract)*, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*. 1996, Association for Computing Machinery: Philadelphia, Pennsylvania, USA. p. 99–108.
24. Joux, A. and J. Stern, *Lattice Reduction: A Toolbox for the Cryptanalyst.* Journal of Cryptology, 1998. **11**(3): p. 161-185.

25. Micciancio, D. and S. Goldwasser, *Complexity of Lattice Problems.* Springer-Verlag New York, 2002.
26. Μπεληγιάννης, Α., *Μια Εισαγωγή στη Βασική Άλγεβρα.* ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, 2015.
27. Meyer, C.D., *Matrix analysis and applied linear algebra.* Soc. For Industrial and Applied Math, 2000.
28. Hung, M.S. and W.O. Rom, *An application of the Hermite normal form in integer programming.* Linear Algebra and its Applications, 1990. **140**: p. 163-179.
29. Grover, L.K., *A fast quantum mechanical algorithm for database search*, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*. 1996, Association for Computing Machinery: Philadelphia, Pennsylvania, USA. p. 212–219.
30. Kwiat, P.G., et al., *Grover's search algorithm: An optical approach.* Journal of Modern Optics, 2000. **47**(2-3): p. 257-266.
31. Shor, P.W. *Algorithms for quantum computation: discrete logarithms and factoring*. in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994.
32. Lili, Z. and Y. Sang, *A Lattice-based Identity-based Proxy Signature from Bonsai Trees.* International Journal of Advancements in Computing Technology, 2012. **4**: p. 99-104.
33. Lenstra, A.K., H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients.* Mathematische Annalen, 1982. **261**(4): p. 515-534.
34. Nguyen, P.Q. and B. Vallee, *The LLL Algorithm* Springer-Verlag New York, 2010.
35. Ζάχος, Ε., Α. Παγουρτζής, and Π. Γροντάς, *Υπολογιστική Κρυπτογραφία.* ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, 2015.
36. Deutsch, D. and R. Penrose, *Quantum theory, the Church–Turing principle and the universal quantum computer.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1985. **400**(1818): p. 97-117.
37. Perlner, R.A. and D.A. Cooper, *Quantum resistant public key cryptography: a survey*, in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*. 2009, Association for Computing Machinery: Gaithersburg, Maryland, USA. p. 85–93.
38. Ablayev, F. and A. Vasiliev, *Quantum Hashing.* 2013.
39. Kalinin, K.P. and N.G. Berloff *Blockchain platform with proof-of-work based on analog Hamiltonian optimisers*. 2018. arXiv:1802.10091.
40. Tessler, L. and T. Byrnes *Bitcoin and quantum computing*. 2017. arXiv:1711.04235.
41. Kiktenko, E.O., et al., *Quantum-secured blockchain.* Quantum Science and Technology, 2018. **3**(3): p. 035004.
42. Jogenfors, J. *Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics*. in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2019.
43. Fernández-Caramès, T.M. and P. Fraga-Lamas, *Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks.* IEEE Access, 2020. **8**: p. 21091-21116.
44. Jin, M. and C.D. Yoo, *Quantum Hashing for Multimedia.* IEEE Transactions on Information Forensics and Security, 2009. **4**(4): p. 982-994.
45. Rajan, D. and M. Visser, *Quantum Blockchain Using Entanglement in Time.* Quantum Reports, 2019. **1**(1): p. 3-11.

46. van Emde Boas, P., *Another Np-complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice.* University of Amsterdam, 1981.
47. Ajtai, M., *The shortest vector problem in L₂ is NP-hard for randomized reductions (extended abstract)*, in *Proceedings of the thirtieth annual ACM symposium on Theory of computing*. 1998, Association for Computing Machinery: Dallas, Texas, USA. p. 10–19.
48. Micciancio, D. and P. Voulgaris, *Faster exponential time algorithms for the shortest vector problem*, in *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete algorithms*. 2010, Society for Industrial and Applied Mathematics: Austin, Texas. p. 1468–1480.
49. Alon, N., L. Babai, and A. Itai, *A fast and simple randomized parallel algorithm for the maximal independent set problem.* Journal of Algorithms, 1986. **7**(4): p. 567-583.
50. Babai, L., *On Lovász' lattice reduction and the nearest lattice point problem.* Combinatorica, 1986. **6**(1): p. 1-13.
51. McEliece, R.J., *A Public-Key Cryptosystem Based On Algebraic Coding Theory.* Deep Space Network Progress Report, 1978. **44**: p. 114.
52. Ding, J. *A new variant of the Matsumoto-Imai cryptosystem through perturbation*. in *International Workshop on Public Key Cryptography*. 2004. Springer.
53. Patterson, N., *The algebraic decoding of Goppa codes.* IEEE Transactions on Information Theory, 1975. **21**(2): p. 203-207.
54. Bernstein, D.J., T. Lange, and C. Peters, *Attacking and defending the McEliece cryptosystem.*
55. Bernstein, D. and T. Lange, *eBATS: ECRYPT benchmarking of asymmetric systems.* 2017.
56. Valentijn, A., *Goppa codes and their use in the McEliece cryptosystems.* 2015.
57. Benvenuto, C.J., *Galois Field in Cryptography.* 2012.
58. Ding, J., J.E. Gower, and D.S. Schmidt, *Multivariate public key cryptosystems*. Vol. 25. 2006: Springer Science & Business Media.
59. Gentry, C., C. Peikert, and V. Vaikuntanathan, *Trapdoors for hard lattices and new cryptographic constructions*, in *Proceedings of the fortieth annual ACM symposium on Theory of computing*. 2008, Association for Computing Machinery: Victoria, British Columbia, Canada. p. 197–206.
60. Ducas, L. and D. Micciancio. *Improved Short Lattice Signatures in the Standard Model*. in *Advances in Cryptology – CRYPTO 2014*. 2014. Berlin, Heidelberg: Springer Berlin Heidelberg.
61. Yin, W., et al., *An Anti-Quantum Transaction Authentication Approach in Blockchain.* IEEE Access, 2018. **6**: p. 5393-5401.
62. Gao, Y., et al., *A Secure Cryptocurrency Scheme based on Post-Quantum Blockchain.* IEEE Access, 2018. **PP**: p. 1-1.
63. Nofer, M., et al., *Blockchain.* Business & Information Systems Engineering, 2017. **59**(3): p. 183-187.
64. Zheng, Z., et al., *Blockchain challenges and opportunities: a survey.* Int. J. Web Grid Serv., 2018. **14**(4): p. 352–375.
65. Li, C., et al., *A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network.* IEEE Access, 2019. **7**: p. 2026-2033.
66. Bentov, I., A. Gabizon, and A. Mizrahi, *Cryptocurrencies Without Proof of Work.* Springer-Verlag New York, 2016.

67. Khalifa, A.M., A.M. Bahaa-Eldin, and M.A. Sobh. *Quantum Attacks and Defenses for Proof-of-Stake*. in *2019 14th International Conference on Computer Engineering and Systems (ICCES)*. 2019.

9. ΠΑΡΑΡΤΗΜΑ

9.1.Παράρτημα Α

Η υλοποίηση σε MATLAB για την παραγωγή δημόσιων και ιδιωτικών κλειδιών και η διαδικασία υπογραφής στο κρυπτοσύστημα McEliece

```
clear;clc
%----------------PUBLIC AND PRIVATE KEY----------------------------------
%Random generation of n x n permutation matrix P . Construction of P is performed by applying a random permutation R to the columns of the identity matrix.
The components of Ri are calculated in accordance with the formula Ri(R(j)) = j for all j in [1 .. n].



R = randperm(15)
I= eye(15)
P = gf(I(:, R))
Ri(R(1:15)) = [1:15]
%Random generation of a nonsingular 5 x 5 matrix S . Computing Si as inv(S).
tmp = [0 1 0 0 1;
1 1 1 0 1;
0 0 1 1 0;
0 0 1 0 0;
0 1 1 1 0]
S = gf(tmp)
Si = inv(S)
%Computation of 5 x 15 matrix E by the formula E = S · G · P
G = [1 0 1 0 0 1 1 0 1 1 1 0 0 0 0;
    1 1 1 1 0 1 0 1 1 0 0 1 0 0 0;
    0 1 1 1 1 0 1 0 0 1 0 0 1 0 0;
    1 0 0 1 1 0 1 1 1 0 0 0 0 1 0;
    0 1 0 0 1 1 0 1 1 1 0 0 0 0 1]
E = S * gf(G) * P
%The public and private keys are the tuples (E, t) and (Si, G, Ri),respectively.
% t=3
```

```
%----------Encryption----------------------------------------------------

%Representation of the message, which in this task is generated randomly, in the form of k-dimensional vector m
lin=1
col=5
kk= randi([0 1], lin,col)
m=gf(kk)
% Selection of a random n-dimensional vector z of weight t (t=3)
 z = gf([0 0 0 1 0 0 0 0 0 1 0 0 0 1 0])
%Computation of the ciphertext c by the formula c = m · E + z.
c = m * E + z
%-------------------------------------------------------------------------
%------Decryption-----------------------------------------------------------
%Calculation of the n-dimensional vector u by means of applying the permutation Ri to the ciphertext vector c
u = c(Ri)
%Obtainment of the vector v as the result of decoding of u by (n, k) linear binary code with the generator matrix G
v = decode(double(u.x), 15, 5, 'linear/binary', G)
%Computation of the decrypted message vector d by the formula d = v · Si
d = gf(v) * Si
%The result of decryption should be tested for equality to the initial message
isequal(d, m)
```

9.2.Παράρτημα Β

Υλοποίηση σε MATLAB του σχήματος υπογραφής Matsumoto-Imai

```
clear;clc
% Creation of the initial map S(x) = x · SD + SL
tmp = [1 1 0 0 1 0;
       0 1 0 1 0 0;
       0 0 0 1 0 1;
       1 0 1 0 1 0;
       1 1 0 1 0 0;
       0 0 1 1 0 1]
   Sd = gf(tmp)
   Si = inv(Sd)
   Sl = gf([1 0 0 1 1 0])
   %The final map T(x)
tmp = [1 0 0 1 0 1;
0 1 0 0 1 0;
0 0 1 0 0 0;
0 1 0 1 0 0;
0 0 0 0 1 0;
0 0 0 0 0 1]
 Td = gf(tmp)
 Ti = inv(Td)
 Tl = gf([0 1 0 0 1 1])
% Representation of the map composition P, which equals T ◦ F ◦ S
 syms x0 x1 x2 x3 x4 x5
 tmp = num2cell(mod([x0 x1 x2 x3 x4 x5] * Sd.x + Sl.x, 2))
 [v0 v1 v2 v3 v4 v5] = tmp[6]
 u5 = v3^2+v5*v4+v5*v2+v5^2+v2^2+v4^2+v1^2+v3*v2+v4*v1+v5*v1
 u4 = v4*v2+v4*v0+v0*v1+v3*v2+v5^2+v5*v1+v5*v2+v5*v3+v2*v1+v5*v4+v4*v1
 u3 = v3*v2+v2*v0+v4*v2+v3^2+v2*v1+v4*v1+v5*v4
 u2=v2^2+v2*v0+v5*v1+v4*v2+v5^2+v3*v0+v4*v3+v5*v0+v3*v2+v2*v1+v5*v3+v1^2+ v3*v1
 u1 = v4*v0+v5*v0+v5*v3+v3^2+v4*v2+v1^2+v5*v2+v3*v2
 u0 = v3^2+v0*v1+v4*v3+v2*v0+v3*v0+v2*v1+v5^2+v0^2+v3*v2
 tmp = num2cell(mod(expand([u0 u1 u2 u3 u4 u5] * Td.x + Tl.x), 2))
```

```
[p0 p1 p2 p3 p4 p5] = tmp
%--------------------signatuge-----------------------------------------------
% hashing message h

lin=1
col=6
kk= randi([0 1], lin,col)
h=gf(kk)
% Applying T^-1 to h
tmp = (h - Tl) * Ti
% Applying F^-1 to the result of the previous step with paremeters n=6,g=67,b=26
 n = 6, g = 67, b = 26
 tmp = gf(bi2de(double(tmp.x)), n, g)^b
 tmp = gf(de2bi(double(tmp.x), n))
% The signature E is computed by applying S^-1
E =(tmp - Sl) * Si
% Applying P to E and saving the result to J
 tmp = num2cell(E.x)
 [x0 x1 x2 x3 x4 x5] = tmp[1]
 J = gf(double(mod(subs([p0 p1 p2 p3 p4 p5]),2)))
% Comparison of J with the hash value of the signed message
 isequal(J, h)
```