Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

Μετακβαντικοί Κρυπτογραφικοί Αλγόριθμοι

(Post-Quantum Cryptography)

Μονογιός Κωνσταντίνος

Επιβλέπων Καθηγητής

Δρ. Νικόλαος

Κολοκοτρώνης

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μετακβαντικοί Κρυπτογραφικοί Αλγόριθμοι
(Post-Quantum Cryptography)

Μονογιός Κωνσταντίνος

Επιβλέπων Καθηγητής
Δρ. Νικόλαος
Κολοκοτρώνης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων (ΑΥΔ) από τη Σχολή Θετικών Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η κρυπτογραφία μελετά τεχνικές με τις οποίες ένα μήνυμα μπορεί να μετασχηματιστεί σε ακατάληπτη μορφή. Η διαδικασία μετατροπής ενός μηνύματος σε ακατάληπτη μορφή ονομάζεται κρυπτογράφηση ενώ η αντίστροφη διαδικασία ονομάζεται αποκρυπτογράφηση. Η κβαντική κρυπτογραφία ορίζεται ως η «επιστήμη της εκμετάλλευσης των κβαντικών μηχανικών ιδιοτήτων για την εκτέλεση κρυπτογραφικών εργασιών» και ο ορισμός του απλού ανθρώπου είναι ότι οι πολλαπλές καταστάσεις του κβαντικού σε συνδυασμό με τη θεωρία της χωρίς αλλαγές σημαίνουν ότι δεν μπορεί να διακοπεί εν αγνοία τους. Η μετακβαντική κρυπτογραφία είναι κρυπτογραφία υπό την προϋπόθεση ότι ο εισβολέας έχει έναν μεγάλο κβαντικό υπολογιστή. Η ανάπτυξη προτύπων για τη μετακβαντική κρυπτογραφία θα απαιτήσει σημαντικούς πόρους για την ανάλυση υποψήφιων κβάντων ανθεκτικών συστημάτων και θα απαιτήσει σημαντική δημόσια εμπλοκή για να εξασφαλίσει την εμπιστοσύνη στους αλγορίθμους που επιλέγει ο NIST για τυποποίηση. Η μετακβαντική Κρυπτογραφία εστιάζει σε 5 κύριους τύπους κρυπτογραφικών συστημάτων. Η κύρια διαφορά μεταξύ αυτών είναι ότι βασίζονται σε διαφορετικές μαθηματικές δομές.

1. Κώδικες διόρθωσης σφαλμάτων με κύρια έμφαση στο κρυπτοσύστημα MC Eliece
2. Πλέγματα
3. Συναρτήσεις κατακερματισμού
4. Συναρτήσεις πολλών μεταβλητών
5. Ισομορφισμός πάνω σε ελλειπτικές καμπύλες.

Ο NIST το 2016 ξεκίνησε μια διαδικασία για την ανάπτυξη νέων προτύπων κρυπτογραφίας. Ο στόχος αυτής της έρευνας είναι να αναπτυχθούν κρυπτογραφικοί αλγόριθμοι που είναι ασφαλείς τόσο έναντι κβαντικών όσο και κλασικών υπολογιστών. Από τους αρχικά 69 αλγόριθμους που προτάθηκαν μετά από διάφορα Comments και θέσεις των αναγνωστών αλλά και αξιολογήσεις των ερευνητών και συνεργατών του NIST προχώρησαν στον δεύτερο γύρο μόλις 26 από τις 69 προτάσεις. Επιπλέον ο NIST πιστεύει ότι η διαδικασία ανάπτυξης των μετακβαντικών προτύπων δεν πρέπει να αντιμετωπίζεται ως ανταγωνισμός αλλά ως κοινός σκοπός.

Summary

Cryptography studies techniques by which a message can be transformed into an incomprehensible form. The process of converting a message into an incomprehensible form is called encryption, while the inverse process is called decryption. Quantum cryptography is defined as the "science of the exploitation of quantum mechanical properties for the execution of cryptographic work," and the definition of a simple human being is that the multiple states of the quantum in combination with its unchanged theory mean that it cannot be unintentionally interrupted. The transcending cryptography is cryptography provided that the intruder has a large quantum computer. The development of standards for transcending cryptography will require considerable resources for the analysis of candidate quantum resilient systems and will require significant public engagement to ensure confidence in NIST's algorithms for standardization. The transcendent Cryptography focuses on 5 main types of cryptographic systems. The main difference between them is that they are based on different mathematical structures.

1. Code-based cryptography with main emphasis on MC Eliece cryptosystem
2. Lattice-based cryptography
3. Hash-based cryptography
4. Multivariate cryptography
5. Isomorphism on elliptical curves.

NIST in 2016 launched a process to develop new cryptography standards. The aim of this research is to develop cryptographic algorithms that are safe against both quantum and classical computers. Of the original 69 algorithms proposed after several Comments and Reader Posts, as well as evaluations of NIST researchers and collaborators, only 26 out of the 69 proposals went into the second round. In addition, NIST believes that the process of developing post quantum standards should not be seen as a competition but as a common goal.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς τον επιβλέποντα καθηγητή κ. Νικόλαο Κολοκοτρώνη που συνέβαλε τα μέγιστα για την ορθή ολοκλήρωση της διατριβής παρόλες τις δυσκολίες που προέκυψαν κατά την διάρκεια της εκπόνησης της.

Τους δικούς μου ανθρώπους.

Περιεχόμενα

Πίνακας εικόνων:

Κεφάλαιο 1
Εισαγωγή

Η κρυπτογραφία μελετά τεχνικές με τις οποίες ένα μήνυμα μπορεί να μετασχηματιστεί σε ακατάληπτη μορφή. Η διαδικασία μετατροπής ενός μηνύματος σε ακατάληπτη μορφή ονομάζεται κρυπτογράφηση ενώ η αντίστροφη διαδικασία ονομάζεται αποκρυπτογράφηση. Κύριος στόχος της κρυπτογραφίας είναι η εμπιστευτικότητα του μηνύματος.

Στην εποχή μας ο όρος κρυπτογραφία είναι πολύ πιο ευρύς: συγκεκριμένα, αναφερόμαστε στη μελέτη μαθηματικών τεχνικών που έχουν σαν στόχους την διασφάλιση διαφόρων ζητημάτων που άπτονται της ασφάλειας της πληροφορίας όπως είναι η εμπιστευτικότητα, γνησιότητα χρηστών και πληροφοριών, ακεραιότητα των δεδομένων καθώς και η μη αποποίηση γεγονότων που έχουν συμβεί. Διάφοροι κρυπτογραφικοί αλγόριθμοι ή κρυπτογραφικές τεχνικές αναπτύχθηκαν για την διασφάλιση των παραπάνω ζητημάτων.

Η κρυπτανάλυση αποτελεί τον κλάδο της κρυπτογραφίας, ο οποίος ως κύριο αντικείμενο της μελέτης του έχει την ανεύρεση προβλημάτων στους κρυπτογραφικούς αλγόριθμους που χρησιμοποιούνται. Μέσω της κρυπτανάλυσης ενός αλγορίθμου κρυπτογράφησης, προσπαθεί κανείς να βρει το κλειδί αποκρυπτογράφησης ή μέρος του ή απλά να καταφέρει να έχει πρόσβαση σε κάποια αποκρυπτογραφημένα μηνύματα. Αυτό το οποίο θα πρέπει να τονίσουμε, είναι ότι η κρυπτανάλυση δεν αφορά μόνο τους αλγορίθμους κρυπτογράφησης, αφορά το σύνολο των μηχανισμών της κρυπτογραφίας, όπως για παράδειγμα τις συναρτήσεις κατακερματισμού, και τις ψηφιακές υπογραφές.

Ένα κρυπτοσύστημα αποτελείται από δύο αλγόριθμους, έναν αλγόριθμο κρυπτογράφησης (encryption algorithm) E και έναν αλγόριθμο αποκρυπτογράφησης (decryption algorithm) D. Το αρχικό κείμενο (plain text) είναι το κείμενο προς κρυπτογράφηση. Χρησιμοποιώντας το αρχικό κείμενο για είσοδο του αλγόριθμου κρυπτογράφησης, παίρνουμε στην έξοδο το κρυπτοκείμενο (cipher text). Ο αλγόριθμος αποκρυπτογράφησης χρησιμοποιεί για είσοδο το κρυπτοκείμενο και εξάγει το αντίστοιχο αρχικό κείμενο. Γενικά τα κρυπτοσυστήματα μπορούν να ταξινομηθούν με βάση τον αριθμό κλειδιών που χρησιμοποιούνται.

- Κανένα κλειδί : Όλο το κρυπτοσύστημα βασίζεται στον αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης. Ο χρησιμοποιούμενος αλγόριθμος θα πρέπει να κρατείται μυστικός,δηλαδή να είναιγνωστόςμόνο στους ιδιοκτήτες του κρυπτοσυστήματος.

- Ένακλειδί: ΟιαλγόριθμοικρυπτογράφησηςΕ καιαποκρυπτογράφησηςD χρειάζονται μια παράμετρο Κ, η οποία ουσιαστικά είναι το μυστικό κλειδί (κρυπτογράφησης – αποκρυπτογράφησης). Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να κοινοποιηθούν αλλά η παράμετρος Κ (μυστικό κλειδί) θα πρέπει να παραμείνειμυστικό.

- Δύο κλειδιά : Οι αλγόριθμοι κρυπτογράφησης – αποκρυπτογράφησης χρησιμοποιούν διαφορετικές παραμέτρους (κλειδιά). Ο αλγόριθμος κρυπτογράφησης χρησιμοποιεί το κλειδί κρυπτογράφησης Κ, το οποίο είναι δημόσιο, και ο αλγόριθμος αποκρυπτογράφησης χρησιμοποιεί το κλειδί αποκρυπτογράφησης Κ΄ που θα πρέπει να είναι διωτικό.

1.1 Ιστορική αναδρομή

Η κρυπτογραφία χρησιμοποιείται πάνω από 2500 χρόνια από τον άνθρωπο. Στην αρχαία Ελλάδα οι έφοροι στην Σπάρτη επικοινωνούσαν με τους στρατηγούς χρησιμοποιώντας μακριές, στενές κορδέλες οι οποίες τυλίγονταν γύρω από έναν κύλινδρο (σκυτάλη) και στην συνέχεια έγραφαν το μήνυμα κατά μήκους του κυλίνδρου. Για να διαβάσει κανείς το μήνυμα, έπρεπε να έχει μια παρόμοια σκυτάλη που είχε χρησιμοποιηθεί έτσι ώστε να τυλίξει την σκυτάλη με τον ίδιο τρόπο. Ο Ιούλιος Καίσαρας χρησιμοποιούσε ένα κρυπτοσύστημα για να επικοινωνήσει με τους συμμάχους του, με το οποίο το κρυπτογραφημένο κείμενο προέκυπτε με την αντικατάσταση του κάθε γράμματος με ένα άλλο σύμφωνα με ολίσθηση των γραμμάτων κατά βήμα στο αλφάβητο . Το παραπάνω κρυπτοσύστημα είναι από τα πιο απλά και ανασφαλή κρυπτοσυστήματα που έχουν προταθεί. [1]

Ο Edgar Allan Poe (1809-1849) στο κλασικό διήγημα "Το χρυσό έντομο" ("The Gold Bug") που δημοσίευσε το 1843, εξηγεί τις βασικές αρχές παραβίασης των κωδίκων και υποστηρίζει την άποψη ότι ο ανθρώπινος νους μπορεί να σπάσει οποιοδήποτε κρυπτογραφημένο κείμενο που η ανθρώπινη ευρηματικότητα μπορεί να επινοήσει. Ακόμη περιγράφει ένα σύστημα με το οποίο κάθε κρυπτογραφημένο κείμενο που προέρχεται από μια ευρωπαϊκή γλώσσα μπορεί να αποκρυπτογραφηθεί, αν έχει

κρυπτογραφηθεί με αντικατάσταση, μετρώντας τη συχνότητα των γραμμάτων της γλώσσας, τεχνική που πρώτοι συνέλαβαν οι Άραβες.

Αρκετά αργότερα ο Γκιλμπερτ Βέρναμ , μηχανικός της AT&T ανέπτυξε το πρώτο πραγματικά άθραυστο κώδικα που ονομάστηκε κρυπτογράφηση Βέρναμ . Μια ιδιότητα αυτού του κώδικα είναι η απαίτηση για κλειδί με μήκος όσο και το μήνυμα που πρέπει να μεταδοθεί και το οποίο δεν ξαναχρησιμοποιείται για την αποστολή άλλου μηνύματος. Η ανακάλυψη του συστήματος αυτού δεν εκτιμήθηκε ιδιαίτερα εκείνη την εποχή, γιατί δεν είχε αποδειχθεί ότι είναι άθραυστος καθώς επίσης και η απαίτηση για ένα κλειδί όσο και το μήκος του μηνύματος τον έκαναν πρακτικά μη χρήσιμο.[3]

Η περίφημη μηχανή Enigma που χρησιμοποιήθηκε από τους Γερμανούς κατά το δεύτερο παγκόσμιο πόλεμο για κρυπτογράφηση ραδιοτηλεπικοινωνιών ήταν ίσως το πλέον εξελιγμένο κρυπτοσύστημα της εποχής και πυροδότησε μια από τις πιο έντονες προσπάθειες αποκρυπτογράφησης στην ιστορία. Ο κώδικας Αίνιγμα θυμίζει έναν παλιότερο κώδικα (τύπου Vigenére) αλλά είναι πολύ πιο πολύπλοκος. Μια βασική ιδιότητα της μηχανής αυτής ήταν η αυτο-αντιστροφή δηλαδή εάν το κωδικοποιημένο κείμενο δινόταν ως είσοδος στη μηχανή, τότε η έξοδος θα ήταν το αρχικό μήνυμα.

Η σημερινή μορφή των κρυπτογραφικών συστημάτων έχει καθοριστεί σε πολύ μεγάλο βαθμό από δύο επιστημονικές εργασίες του Kerchoff (1883) και του Shannon (1949). Ο Auguste Kerchoff έθεσε την βασική σχεδιαστική αρχή που έκτοτε διέπει κάθε κρυπτογραφικό σύστημα, σύμφωνα με την οποία η ασφάλεια ενός συστήματος πρέπει να έγκειται μόνο στην μυστικότητα του κλειδιού και να μην εξαρτάται από την μυστικότητα του αλγόριθμου κρυπτογράφησης. Η δεύτερη εργασία ανήκει στον Claude Shannon με την οποία η κρυπτογραφία μετατρέπεται σε αυστηρό επιστημονικό πεδίο , όπου ορίζεται η έννοια του κρυπτοσυστήματος και η απόλυτη ασφάλεια. Η εργασία του Shannon αποτέλεσε το έναυσμα για την ταχεία εξέλιξη της έρευνας στο χώρο της κρυπτογραφίας και η οποία συνεχίζεται μέχρι σήμερα. Όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται με βάση τις έννοιες που εισήγαγε ο Shannon.

1.2 Σύγχρονοι αλγόριθμοι κρυπτογράφησης

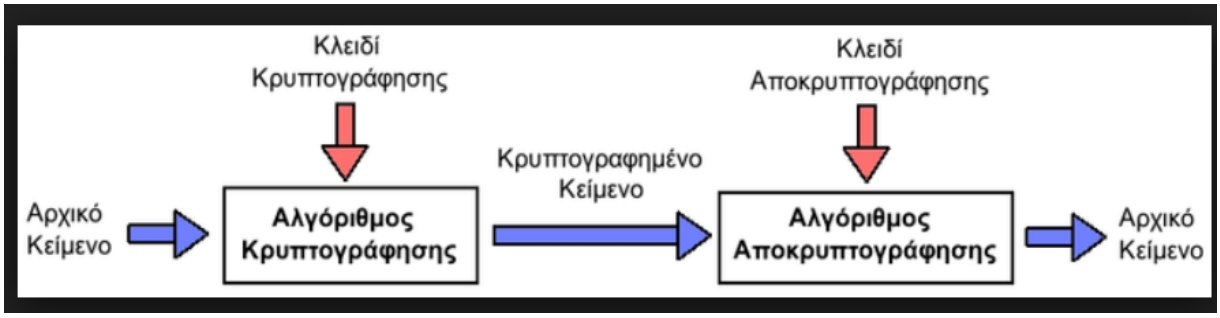
Η κρυπτογραφία είναι παρούσα σε μια πληθώρα εφαρμογών και τις οποίες συναντούμε καθημερινά. Κρυπτογραφία εφαρμόζεται στις ασφαλείς συναλλαγές με τις τράπεζες (ATM), στην κινητή τηλεφωνία (3G, 4G), ασύρματα δίκτυα (802.1X, Bluetooth), ηλεκτρονικό ταχυδρομείο, τηλεφωνία μέσω διαδικτύου

(VoIP), ηλεκτρονικό εμπόριο (πληρωμές μέσω πιστωτικών καρτών) , εφαρμογές IoT αλλά και πολλές άλλες.

Οι κρυπτογραφικοί αλγόριθμοι χωρίζονται σε δύο μεγάλες βασικές κατηγορίες: τους συμμετρικούς (symmetric) και τους ασύμμετρους (asymmetric) ή γνωστούς και ως δημοσίου κλειδιού (publickey). [2]

1.3 Συμμετρικοί αλγόριθμοι κρυπτογράφησης

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης ταυτίζεται με το κλειδί της αποκρυπτογράφησης. Ως εκ τούτου, αυτοί οι αλγόριθμοι χρειάζονται την εκ των προτέρων συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό [5]. Μπορούμε να δούμε στη εικόνα 1.1 τη διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης.



Εικόνα 1.1: Λειτουργία συμμετρικού αλγόριθμου κρυπτογράφησης

Οι συμμετρικοί αλγόριθμοι μπορούν να ταξινομηθούν σε δύο υποκατηγορίες :

Α. Αλγόριθμοι ροής (Stream ciphers)

Β.Αλγόριθμοι τμήματος (blockciphers)

1.4 Ασύμμετροι αλγόριθμοι κρυπτογράφησης

Οι ασύμμετροι αλγόριθμοι είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιούν για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί για την αποκρυπτογράφηση. Οι αλγόριθμοι αυτοί ονομάζονται και δημοσίου κλειδιού γιατί το κλειδί της κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να

κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί του παραλήπτη αλλά μόνο ο κάτοχος του ιδιωτικού κλειδιού – δηλαδή, ο παραλήπτης - μπορεί να το αποκρυπτογραφήσει. Παραδείγματα ασύμμετρων αλγορίθμων κρυπτογράφησης είναι ο RSA, αλγόριθμοι ελλειπτικών καμπυλών, ElGamal και άλλοι.[6]

Οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι εφαρμοσμένοι είτε σε υλικό ή λογισμικό από τους ασύμμετρους. Γι' αυτό το λόγο οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση του κυρίως μέρους των δεδομένων του μηνύματος, ενώ οι αλγόριθμοι δημοσίου κλειδιού προτιμώνται σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.

1.5 Εμφάνιση Μετακβαντικής Κρυπτογραφίας

Ας υπάρξει ο συλλογισμός ότι σε δεκαπέντε χρόνια από τώρα κάποιος ανακοινώνει την επιτυχή κατασκευή ενός μεγάλου κβαντικού υπολογιστή. Αυτό αυτόματα θα σήμαινε ότι έφτασε το τέλος των προσωρινά «απόρθητων» κβαντικών κρυπταλγορίθμων. Οι χρήστες των υπολογιστών θα πανικοβάλλονταν καθώς η πρώτη τους σκέψη θα ήταν ότι και πάλι τα προσωπικά τους δεδομένα δεν είναι ασφαλή. Όσοι ασχολούνται με την κρυπτογραφία θα πίστευαν πως και πάλι οι κβαντικοί κρυπτογραφικοί αλγόριθμοι θα έσπαζαν όπως τους προκατόχους τους. Δηλαδή τους RSA,DSA και ECDSA από τους κβαντικούς υπολογιστές.

Από τους πιο ισχυρούς αυτή την εποχή αλγόριθμους που θα έσπαζαν, είναι τα συστήματα υπογραφής δημόσιου κλειδιού. Οι κβαντικοί υπολογιστές φαίνεται να έχουν πολύ μικρή επίδραση πάνω στην κρυπτογραφία που αφορούν τα μυστικά κλειδιά και τις λειτουργίες κατακερματισμού. Ακόμα υπάρχει και ο αλγόριθμος του Grover ο οποίος αναγκάζει κάπως τα μεγαλύτερα μεγέθη κρυπταλγορίθμων για την εύρεση κρυπτογραφημένων μυστικών κλειδιών, αλλά αυτό το αποτέλεσμα είναι ουσιαστικά ομοιόμορφο πέρα από τους κρυφούς χαρακτήρες. Όσο αφορά τα συστήματα υπογραφής δημόσιου κλειδιού με βάση το hash, απαιτούν μια τυπική κρυπτογραφική λειτουργία κατακερματισμού. Για Η παράγει 2 bits κατά την έξοδο. Για b = 128 κάποιος θα μπορούσε να επιλέξει το Η ως SHA256 και την λειτουργία hash. Τα τελευταία χρόνια έχουν δημιουργηθεί πολλές ανησυχίες όσον αφορά την ασφάλεια της δημοφιλούς λειτουργίας κατακερματισμού και για αυτό το λόγο ο NIST διεξάγει διαγωνισμό για αντικατάσταση του SHA-256.[4]

Άλλα κρυπτογραφικά συστήματα, όπως είναι ο RSA με ένα ισχυρό κλειδί, πιστεύεται ότι αντιστέκεται σε επιθέσεις μεγάλων κλασσικών τεχνικών , όμως ,δεν αντιστέκεται σε

επιθέσεις από μεγάλους κβαντικούς υπολογιστές. Ως εναλλακτική λύση, του αλγόριθμου αυτού προβάλλεται η κρυπτογράφηση McEliece με κλειδί τεσσάρων εκατομμυρίων δυαδικών ψηφίων μέσα από τα οποία θα αντισταθούν σε επιθέσεις από μεγάλους κλασσικούς υπολογιστές και επιθέσεις μεγάλων κβαντικών υπολογιστών. Από αυτό τον τρόπο δημιουργείται λοιπόν και το ερώτημα γιατί πρέπει τώρα να υπάρχει ανησυχία για απειλή των κβαντικών υπολογιστών από την στιγμή που μπορεί να υπάρχει συνέχεια στην εστίαση του RSA αλλά και του ECDSA με την βοήθεια του McEliece;[30]

Κύρια χαρακτηριστικά της κρυπτογραφίας αυτής μέλλεται να είναι τα εξής: [7]

1. Αποδοτικότητα

2. Εμπιστοσύνη

3. Ευχρηστία

1.6 Σκοπός έρευνας και βασικά ερευνητικά ερωτήματα

Η παρούσα έρευνα αποσκοπεί στο να ορίσει αποτελεσματικά τον ορισμό και να προβεί στην ορθή ανάλυση των πτυχών της μετακβαντικής κρυπτογραφίας. Αφού ορίσει τι είναι η μετακβαντική κρυπτογραφία και ποιοι οι στόχοι της θα αναφερθούν και θα αναλύσει τους κρυπτογραφικούς αλγόριθμους που εμπίπτουν στην κατηγορία αυτή. Οι αλγόριθμοι δηλαδή οι οποίοι είναι ασφαλείς έναντι των κρυπταναλυτικών επιθέσεων με Κβαντικούς υπολογιστές[8]. Οι κύριες κατηγορίες οι οποίες χωρίζονται οι αλγόριθμοι αυτοί βασίζονται σε :

1. Κώδικες διόρθωσης σφαλμάτων
2. Πλέγματα
3. Συναρτήσεις κατακερματισμού
4. Συναρτήσεις πολλών μεταβλητών
5. Ισομορφισμούς πάνω σε ελλειπτικές καμπύλες

Ανάλυση θα γίνει ακόμα και στην κατηγορία του μετακβαντικού RSA παρόλο που δεν είναι κύριας μορφής κατηγορία ωστόσο λόγο της πολυχρησημότητας του σήμερα θα γίνει αναφορά της δυνατής λειτουργίας του στο μέλλον.

Επίσης στην παρούσα εργασία θα γίνει επιδίωξη να μελετηθεί το όλο γενικό πλαίσιο της ανάλυσης της ασφάλειας των κρυπταλγορίθμων καθώς και η μελέτη και η αναζήτηση των κρυπταναλυτικών επιθέσεων στους νέους αυτούς κρυπταλγορίθμους οι οποίοι αν προκύψουν κάποια ικανοποιητικά αποτελέσματα τότε θα προταθούν στα πλαίσια της διαδικασίας- προκήρυξης που υλοποιεί ο NIST. Ο αρμόδιος δηλαδή διεθνής οργανισμός ο οποίος αφορά τεχνολογικά επιτεύγματα.

Μέσω της παρούσας Διατριβής προκύπτουν διάφορα ερευνητικά ερωτήματα τα οποία και θα γίνει η επιδίωξη για την επίλυση τους.
Ερωτήματα όπως:

- Σε τι διαφέρουν οι προηγούμενες σύγχρονες κρυπτογραφικές μέθοδοι από τη μετακβαντική κρυπτογραφία και σε τί διαφέρει από την κβαντική κρυπτογραφία;
- Υπάρχουν οι δυνατότητες στους κβαντικούς υπολογιστές να προβούν σε επιθέσεις για την κρυπτανάλυση των μετακβαντικών αλγορίθμων;
- Το κόστος υιοθέτησης και χρήσης αυτής της κρυπτογραφίας είναι εφικτό σε διάφορα περιβάλλοντα λειτουργίας (π.χ. σε συσκευές IoT);

1.7 Δομή Μεταπτυχιακής Διατριβής

Η δομή της μεταπτυχιακή διατριβής διαμορφώνεται όπως φαίνεται παρακάτω με τα εξής κεφάλαια:

1ο Κεφάλαιο: Εισαγωγή

Στοκεφάλαιοαυτό γίνεται αναφορά των δομικώνστοιχείωντηςκρυπτογραφίαςκαθώςεπίσης διατυπώνεται οσκοπός της έρευνας καθώς επίσης και τα βασικάερευνητικάερωτήματα.

2ο Κεφάλαιο: Εισαγωγή στον κόσμο της Μετακβαντικής Κρυπτογραφίας
Στο κεφάλαιο αυτό θα γίνει μια αναλυτική εισαγωγή και επεξήγηση του κόσμου της Μετακβαντικής Κρυπτογραφίας καθώς θα αναλυθούν και θα επεξηγηθούν αρκετά θέματα γύρω από τον ορισμό ,τον σκοπό της καθώς και στις πτυχές από τις οποίες αποτελείται η Μετακβαντική Κρυπτογραφία

3ο Κεφάλαιο: Κύριες Κατηγορίες-Υποδιαιρέσεις Μετακβαντικής Κρυπτογραφίας

Σε αυτό το κεφάλαιο θα μελετήσουμε τις κατηγορίες, οι οποίες απαρτίζουν την Μετακβαντική Κρυπτογραφία μία προς μία και στην συνέχεια για κατηγορίες όπως είναι οι Κώδικες διόρθωσης Σφαλμάτων θα γίνει μια ακόμα πιό εξειδικευμένη περιγραφή σε κρυπτοσυστήματα που μέλετε να χρησιμοποιηθούν στο μέλλον όπως για παράδειγμα το κρυπτοσυστήμα Mc Eliece

4ο Κεφάλαιο: Ο NIST και η προκύρηξη των Μετακβαντικών Αλγορίθμων

Στο κεφάλαιο αυτό θα γίνει μια εκτενής αναφορά για το NIST . Ποιός είναι ο οργανισμός αυτός, από τι αποτελείται και που αποσκοπεί. Επιπλέον θα γίνει αναφορά στον διαγωνισμό που τρέχει το δεδομένο χρονικό διάστημα ο οργανισμός σχετικά με τον σχεδιασμό και δημιουργία μεταβαντικώς κρυπτοσυστημάτων που θα είναι ανθεκτικά από επιθέσεις κβαντικών υπολογιστών.

5ο Κεφάλαιο:Επίλογος

Σε αυτό το κεφάλαιο θα διατυπωθούν τα συμπεράσματα της διατριβής.

Κεφάλαιο 2
Εισαγωγή στον κόσμο της Μετακβαντικής Κρυπτογραφίας

2.1 Εισαγωγή στον Κβαντισμό Υπολογισμό

Ο κβαντικός υπολογισμός διαφέρει πολύ από τον κλασικό υπολογισμό των δυαδικών ψηφίων και έτσι τα μαθηματικά για τον κβαντικό υπολογισμό είναι διαφορετικά. Η μικρότερη μονάδα πληροφοριών ενός κβαντικού υπολογιστή είναι ένα qubit που μπορεί να είναι σε κατάσταση βάσης, 1 ή 0, ή κάπου μεταξύ αυτών των καταστάσεων βάσης, η οποία είναι υπερβολή αυτών των καταστάσεων[9]. Ένα κβαντικό σύστημα με περισσότερα από ένα qubit καλείται κβαντικό μητρώο. Οι κλασικές μνήμες με n bits έχουν μια κρατική διάσταση του n, αλλά ένα σύστημα n-qubit έχει κρατική διάσταση 2n[14]. Οι κβαντικοί υπολογιστές μπορούν να σχεδιαστούν για να εκτελέσουν τις ίδιες εργασίες με τους ίδιους αλγόριθμους με τους κλασικούς υπολογιστές, αλλά ο χρόνος εκτέλεσης είναι σχεδόν ο ίδιος. Αν οι αλγόριθμοι χρησιμοποιούν τις συγκεκριμένες ιδιότητες της κβαντικής μηχανικής, τα κβαντικά συστήματα μπορούν να ξεπεράσουν τους κλασικούς υπολογιστές[10]. Ο κβαντικός υπολογισμός μπορεί να "βλέπει" όλες τις καταστάσεις 2n και να εφαρμόζει ταυτόχρονα τις πράξεις τους. Αυτή η δυνατότητα ονομάζεται κβαντικός παραλληλισμός[11]. Δεν μπορεί κανείς να έχει πρόσβαση σε όλες τις καταστάσεις 2n αλλά πρέπει να μετρήσει το κβαντικό σύστημα, όπως για παράδειγμα, κάποιος παίρνει μια τυχαία κατάσταση βάσης από την υπέρθεση. Ο στόχος των κβαντικών αλγορίθμων είναι η αύξηση της πιθανότητας μιας επιθυμητής βασικής κατάστασης η οποία είναι η λύση σε ένα συγκεκριμένο πρόβλημα.[13,12]

Και εδώ λοιπόν στους κβαντικούς υπολογιστές και μέσω των κβαντικών αλγορίθμων κάνει την εμφάνιση της η κβαντική κρυπτογραφία (Quantum Cryptography). Η κβαντική κρυπτογραφία, που ονομάζεται επίσης κβαντική κρυπτογράφηση, εφαρμόζει

τις αρχές της κβαντικής μηχανικής για την κρυπτογράφηση των μηνυμάτων με τρόπο που να μην διαβάζεται ποτέ από οποιονδήποτε εκτός του επιδιωκόμενου αποδέκτη. Επωφελείται από τις πολλαπλές καταστάσεις του κβαντικού, σε συνδυασμό με την "θεωρία της αλλαγής", που σημαίνει ότι δεν μπορεί να διακοπεί εν αγνοία του.[14,15,16]

2.2 Κβαντική Κρυπτογραφία

Η κβαντική κρυπτογραφία ορίζεται ως η «επιστήμη της εκμετάλλευσης των κβαντικών μηχανικών ιδιοτήτων για την εκτέλεση κρυπτογραφικών εργασιών» και ο ορισμός του απλού ανθρώπου είναι ότι οι πολλαπλές καταστάσεις του κβαντικού σε συνδυασμό με τη θεωρία της χωρίς αλλαγές σημαίνουν ότι δεν μπορεί να διακοπεί εν αγνοία τους.[20]

Η λειτουργία της κρυπτογράφησης αυτής στηρίζεται σε "παραδοσιακούς" υπολογιστές. Δηλαδή δυαδικά ψηφία 0 και 1 αποστέλλονται συστηματικά από το ένα μέρος στο άλλο και στη συνέχεια αποκωδικοποιούνται με ένα συμμετρικό (ιδιωτικό) ή ασύμμετρο (δημόσιο) κλειδί. Τα συμμετρικά πλήκτρα κρυπτογράφησης όπως το Advanced Encryption Standard (AES) χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση ενός μηνύματος ή αρχείου, ενώ ασύμμετρα κρυπτογράφηση όπως το RSA χρησιμοποιούν δύο συνδεδεμένα κλειδιά - ιδιωτικά και δημόσια. Το δημόσιο κλειδί μοιράζεται, αλλά το ιδιωτικό κλειδί κρατείται μυστικό για να αποκρυπτογραφήσει τις πληροφορίες.[17]

Ωστόσο, τα πρωτόκολλα κρυπτογραφίας δημόσιου κλειδιού, όπως η κρυπτογράφηση Diffie-Hellman, RSA και κρυπτογράφηση ελλειπτικής καμπύλης (ECC), τα οποία επιβιώνουν με βάση το ότι βασίζονται σε μεγάλους πρωταρχικούς αριθμούς που είναι δύσκολο να παραγάγουν, απειλούνται όλο και περισσότερο. Πολλοί πιστεύουν ότι μπορούν να καταστρατηγηθούν από επιθέσεις τελικού ή πλευρικού καναλιού, όπως το άτομο στο μέσον, οι κρυπτογραφικές επιθέσεις και τα backdoors. Ως παραδείγματα αυτής της ευπάθειας, το RSA-1024 δεν θεωρείται πλέον ασφαλές από το NIST, ενώ οι επιθέσεις με πλάγια κανάλια έχουν αποδειχθεί αποτελεσματικές μέχρι το RSA-40963.

Επιπλέον, η ανησυχία είναι ότι αυτή η κατάσταση θα επιδεινωθεί μόνο με τους κβαντικούς υπολογιστές. Πιστεύεται ότι οι κβαντικοί υπολογιστές βρίσκονται από πέντε έως 20 χρόνια μακριά, και θα είναι πιθανόν να είναι σε θέση να παράγουν

γρήγορους αριθμούς. Όταν συμβεί αυτό, κάθε κρυπτογραφημένη επικοινωνία που εξαρτάται από την κρυπτογράφηση δημόσιου κλειδιού (χρησιμοποιώντας ασύμμετρα κλειδιά) θα σπάσει[18].

"Οι κβαντικοί υπολογιστές είναι απίθανο να σπάσουν συμμετρικές μεθόδους (AES, 3DES κ.λπ.), αλλά είναι πιθανό να σπάσουν τις δημόσιες μεθόδους, όπως το ECC και το RSA", λέει ο Bill Buchanan, καθηγητής στη Σχολή Πληροφορικής του Πανεπιστημίου Napier του Εδιμβούργου στη Σκωτία[19].

Ακόμα η κβαντική κρυπτογραφία μπορεί να επιτρέψει να κρυπτογραφήσουμε ένα μήνυμα με τέτοιο τρόπο ώστε να μην διαβάζεται ποτέ από οποιονδήποτε εκτός του αποδέκτη.

Ο Buchanan βλέπει πολλές ευκαιρίες στην αγορά. "Η εφαρμογή της κβαντικής κρυπτογράφησης παρέχει την ευκαιρία να αντικατασταθούν οι υπάρχουσες μέθοδοι σήραγγας, όπως με την κρυπτογράφηση SSL και wifi, για να δημιουργηθεί μια ολοκληρωμένη κρυπτογράφηση από άκρο σε άκρο σε δίκτυα οπτικών ινών. Αν το καλώδιο ινών χρησιμοποιείται καθ 'όλη τη σύνδεση, δεν θα υπήρχε ανάγκη να εφαρμοστεί κρυπτογράφηση σε οποιοδήποτε άλλο στρώμα, καθώς η επικοινωνία θα ήταν ασφαλής στο φυσικό στρώμα. "[20]

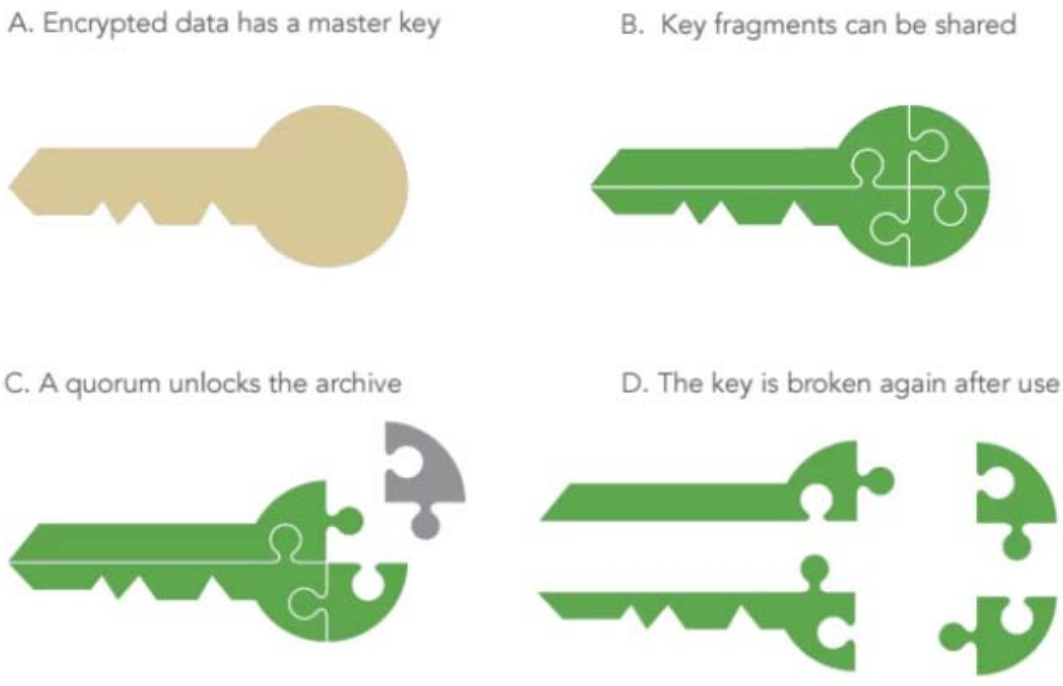
Η κβαντική κρυπτογράφηση είναι και η κατανομή κβαντικών κλειδιών καθώς εννοούν τη διανομή κβαντικού κλειδιού (QKD), μια "θεωρητικά ασφαλή λύση στο βασικό πρόβλημα ανταλλαγής". Με το QKD , τα φωτόνια που διανέμονται στην μικροσκοπική κβαντική κλίμακα μπορούν να είναι οριζόντια ή κάθετα πολωμένα, αλλά «παρατηρώντας ή μετρώντας διαταράσσουν την κβαντική κατάσταση». Αυτό λέει ο Woodward, βασίζεται στην κβαντική φυσική. Στην συνέχεια μόλις πέρνει το κλειδί ο παραλήπτης, επανέρχεται αυτόματα στη συμμετρική κρυπτογράφηση κλειδιού. Στη συνέχεια, το QKD πρόκειται να αντικαταστήσει την υποδομή δημόσιου κλειδιού (PKI). Μέσω του QKD μπορούν ακόμα να διατηρηθούν ασφαλείς οι επικοινωνίες, επικαλύπτοντας λοιπόν άλλες μεθόδους σήραγγας στις επικοινωνίες, όπως με με VPN ή με SSL.[21]

Ωστόσο, η κβαντική κρυπτογράφηση δεν είναι απαραίτητα μια ασημένια σφαίρα για την ασφάλεια των πληροφοριών. Παρουσιάζονται σφάλματα σχετικά με την αξιοπιστία,

καθώς και τεχνικές δυσκολίες στην παραγωγή μόνο φωτονίων που απαιτούνται για QKD. Επιπλέον, το QKD με βάση τις ίνες μπορεί να ταξιδέψει μόνο σε κάποια απόσταση, οπότε πρέπει να υπάρχουν αναμεταδότες, οι οποίοι αντιπροσωπεύουν έτσι "αδύναμα σημεία" [23]. Ακόμα το πρόβλημα της υποδομής χρειάζεται ευρυζωνικές ίνες από άκρο σε άκρο αφού ακόμα δεν έχουν σχεδιαστεί και κατασκευαστεί ολοκληρωμένα συστήματα οπτικών ινών αφού το τελευταίο μίλι του καναλιού επικοινωνίας είναι συχνά ακόμη χάλκινο.

Αντίθετα, η κρυπτογραφία του μετα-κβαντικού δημόσιου κλειδιού φαίνεται να προσφέρει πολύ πιο αποτελεσματικά μέτρα μετριασμού για συστήματα επικοινωνιών πραγματικού κόσμου από την απειλή μελλοντικών κβαντικών υπολογιστών . Πρόκειται για την κρυπτογραφία η οποία θα επιφέρει τις πιό ριζικές αλλαγές στον κόσμο της κρυπτογραφίας και θα πραγματοποιήσει και τα μεγαλύτερα άλματα. Μια κρυπτογραφία η οποία με την εμφάνιση της αναμένεται να πρωταγονιστίσει σε όλα τα επίπεδα της πληροφορικής. Αναλυτική περιγραφή της θα γίνει στο επόμενο υποκεφάλαιο.

2.3 Μετακβαντική Κρυπτογραφία



Εικόνα 2.1: Πιθανή Λειτουργία με μετακβαντικό συμμετρικό κλειδί

Τα τελευταία χρόνια, πραγματοποιήθηκε σημαντική έρευνα σε κβαντικούς υπολογιστές - μηχανές που εκμεταλλεύονται κβαντομηχανικά φαινόμενα για την επίλυση μαθηματικών προβλημάτων που είναι δύσκολα ή δύσκολα για συμβατικούς υπολογιστές. Εάν κατασκευαστούν κβαντικοί υπολογιστές μεγάλης κλίμακας, θα είναι σε θέση να σπάσουν πολλά από τα κρυπτοσυστήματα δημόσιου κλειδιού που χρησιμοποιούνται σήμερα.[24] Αυτό θα έθετε σε σοβαρό κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των ψηφιακών επικοινωνιών στο Διαδίκτυο και αλλού. Ο σκοπός της μετα-κβαντικής κρυπτογράφησης (που ονομάζεται επίσης κβαντική αντοχή στην κρυπτογραφία) είναι η ανάπτυξη κρυπτογραφικών συστημάτων που είναι ασφαλή τόσο έναντι κβαντικών όσο και κλασσικών υπολογιστών και μπορούν να αλληλεπιδρούν με τα υπάρχοντα πρωτόκολλα και δίκτυα επικοινωνιών. Αυτή η Εσωτερική Έκθεση μοιράζεται την τρέχουσα αντίληψη του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST)[25] σχετικά με την κατάσταση της κβαντικής πληροφορικής και της κβαντικής κρυπτογράφησης και περιγράφει το αρχικό σχέδιο του NIST για να προχωρήσουμε σε αυτό το διάστημα. Η έκθεση αναγνωρίζει επίσης τη πρόκληση της μετάβασης σε νέες κρυπτογραφικές υποδομές και ως εκ τούτου τονίζει την ανάγκη να επικεντρωθούν οι υπηρεσίες στην κρυπτοσυχνότητα.[22]

Μια μεγάλη διεθνής κοινότητα έχει αναδειχθεί για να αντιμετωπίσει το ζήτημα της ασφάλειας των πληροφοριών σε ένα μέλλον με κβαντική υπολογιστική, με την ελπίδα ότι η υποδομή δημόσιου κλειδιού μπορεί να παραμείνει άθικτη χρησιμοποιώντας νέα κβαντο-ανθεκτικά πρωτόγονα. Στον ακαδημαϊκό κόσμο, αυτή η νέα επιστήμη φέρει το όνομα "Μετα-Κβαντική Κρυπτογραφία". Πρόκειται για ένα ενεργό ερευνητικό πεδίο με τη δική του σειρά συνεδρίων PQCrypto που ξεκίνησε το 2006. Έχει λάβει σημαντική υποστήριξη από εθνικούς οργανισμούς χρηματοδότησης, κυρίως στην Ευρώπη και την Ιαπωνία, μέσω της Ευρωπαϊκής Ένωσης (ΕΕ) PQCrypto και SAFEcrypto, καθώς και το έργο CREST Crypto-Math στην Ιαπωνία.[23]

Είναι γνωστό ότι τα ευρέως χρησιμοποιούμενα κρυπτοσυστήματα δημόσιου κλειδιού, όπως η κρυπτογράφηση RSA και ελλειπτικής καμπύλης, μπορούν να σπάσουν χρησιμοποιώντας έναν ειδικό υπολογισμό σε κβαντικούς υπολογιστές. Επί του παρόντος, δεδομένου ότι οι κβαντικοί υπολογιστές που μπορούν να αντιμετωπίσουν το πρακτικό μήκος των παραμέτρων δεν υλοποιούνται ακόμη, μπορούμε ακόμα να χρησιμοποιήσουμε τους διάσημους κρυπτογραφικούς αλγορίθμους.[26] Ωστόσο, πρέπει να προετοιμάσουμε και να μελετήσουμε βαθιά τις εναλλακτικές λύσεις αυτών των

αλγορίθμων πριν την υλοποίηση των πρακτικών κβαντικών υπολογιστών.

Η μετάκβαντική κρυπτογραφία είναι κρυπτογραφία υπό την προϋπόθεση ότι ο εισβολέας έχει έναν μεγάλο κβαντικό υπολογιστή. Τα μετακβανικά κρυπτοσυστήματα προσπαθούν να παραμείνουν ασφαλή ακόμη και σε αυτό το σενάριο. Αυτός ο σχετικά νέος ερευνητικός χώρος έχει σημειώσει κάποιες επιτυχίες στον προσδιορισμό μαθηματικών πράξεων για τις οποίες οι κβαντικοί αλγόριθμοι προσφέρουν ελάχιστα πλεονεκτήματα στην ταχύτητα και στη συνέχεια κτίζουν κρυπτογραφικά συστήματα γύρω από αυτά. Η κεντρική πρόκληση στη μετακβαντική κρυπτογραφία είναι η ικανοποίηση των απαιτήσεων κρυπτογραφικής χρηστικότητας και ευελιξίας χωρίς να θυσιάζεται η εμπιστοσύνη.

Αυτές οι προσπάθειες έχουν οδηγήσει στην πρόοδο της θεμελιώδους έρευνας, ανοίγοντας το δρόμο για την ανάπτυξη των μετακβανικών κρυπτοσυστημάτων στον πραγματικό κόσμο. Τα τελευταία χρόνια, οι βιομηχανίες και οι οργανισμοί τυποποίησης άρχισαν τις δικές τους δραστηριότητες στον τομέα αυτό: από το 2013, το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) έχει πραγματοποιήσει τρεις "κβαντο-ασφαλείς κρυπτογραφήσεις" εργαστήρια και το 2015 διοργάνωσε σεμινάριο με θέμα "Cybersecurity in a Post-Quantum World", στο οποίο συμμετείχαν περισσότεροι από 140 άνθρωποι από την κυβέρνηση, τη βιομηχανία και τον ακαδημαϊκό κόσμο.

Ο NIST διαδραματίζει έναν μοναδικό ρόλο στην τυποποίηση της μετακβαντικής κρυπτογραφίας, ως μέρος της ευρύτερης της ευθύνης για την ανάπτυξη προτύπων και κατευθυντήριων γραμμών για την προστασία των ομοσπονδιακών συστημάτων πληροφοριών μη εθνικής ασφάλειας. Πολλά πρότυπα NIST, όπως το προηγμένο πρότυπο κρυπτογράφησης (Advanced Encryption Standard, AES), έχουν αναπτυχθεί με ευρεία συμμετοχή από ακαδημαϊκούς και βιομηχανικούς φορείς και έχουν υιοθετηθεί ευρέως επειδή είναι αποτελεσματικές λύσεις, βοηθώντας έτσι στην προστασία των ΗΠΑ. πληροφοριών και πληροφοριών[28]. Η τυποποίηση NIST της μετά-κβαντικής κρυπτογράφησης πιθανόν να προσφέρει παρόμοια οφέλη.

Η ανάγκη για ισχυρότερη κρυπτογραφία οδηγείται από τις προόδους τόσο στις κλασσικές όσο και στις κβαντικές υπολογιστικές τεχνολογίες. Για να διατηρηθεί η ασφάλεια κατά των κλασικών επιθέσεων, ο NIST έχει ήδη συνιστώμενες μεταβάσεις από μεγέθη κλειδιών και αλγόριθμους που παρέχουν 80 bit ασφάλεια, σε μεγέθη

κλειδιών και αλγόριθμους που παρέχουν ασφάλεια 112 ή 128 bits. Προκειμένου να εξασφαλιστεί η ασφάλεια κατά των κβαντικών επιθέσεων, η NIST θα πρέπει να αντιμετωπίσει μια πιο δύσκολη μετάβαση στα νέα μετακβαντοσυστήματα.

Δεν είναι σαφές όταν θα είναι διαθέσιμοι κλιμακωτοί κβαντικοί υπολογιστές. Ωστόσο, κατά το παρελθόν έτος περίπου, οι ερευνητές που εργάζονται για την κατασκευή ενός κβαντικού υπολογιστή εκτιμούν ότι είναι πιθανό ένας κβαντικός υπολογιστής ικανός να σπάσει RSA 2000-bit σε λίγες ώρες θα μπορούσε να κατασκευαστεί μέχρι το 2030 για έναν προϋπολογισμό περίπου ενός δισεκατομμυρίου δολάρια. Πρόκειται για σοβαρή μακροπρόθεσμη απειλή για τα κρυπτοσυστήματα που επί του παρόντος τυποποιούνται από τον NIST.

Είναι χρήσιμο να συγκρίνουμε τις παραπάνω προβλέψεις με το κόστος διάσπασης αυτών των κρυπτοσυστημάτων χρησιμοποιώντας κλασσικούς υπολογιστές. Τα κρυπτοσυστήματα που προσφέρουν 80 μονάδες ασφαλείας ή λιγότερα, τα οποία καταργήθηκαν σταδιακά το 2011-2013, διατρέχουν τον μεγαλύτερο κίνδυνο: μπορούν να σπάσουν τώρα με κόστος που κυμαίνεται από δεκάδες χιλιάδες έως εκατοντάδες εκατομμύρια δολάρια. Τα κρυπτοσυστήματα που προσφέρουν ασφάλεια 112 bits είναι πιθανό να παραμείνουν ασφαλή για κάποιο χρονικό διάστημα: μπορεί να είναι θραύσιμα για έναν προϋπολογισμό ενός δισεκατομμυρίου δολαρίων σε 30 έως 40 χρόνια (χρησιμοποιώντας κλασικούς υπολογιστές).[28]

Έτσι, η μετάβαση από τα 112 σε 128 (ή υψηλότερα) bits της ασφάλειας είναι ίσως λιγότερο επείγουσα από τη μετάβαση από τα υπάρχοντα κρυπτοσυστήματα σε μετα-κβαντικά κρυπτοσυστήματα. Αυτή η μετά-κβαντική μετάβαση εγείρει πολλές θεμελιώδεις προκλήσεις.

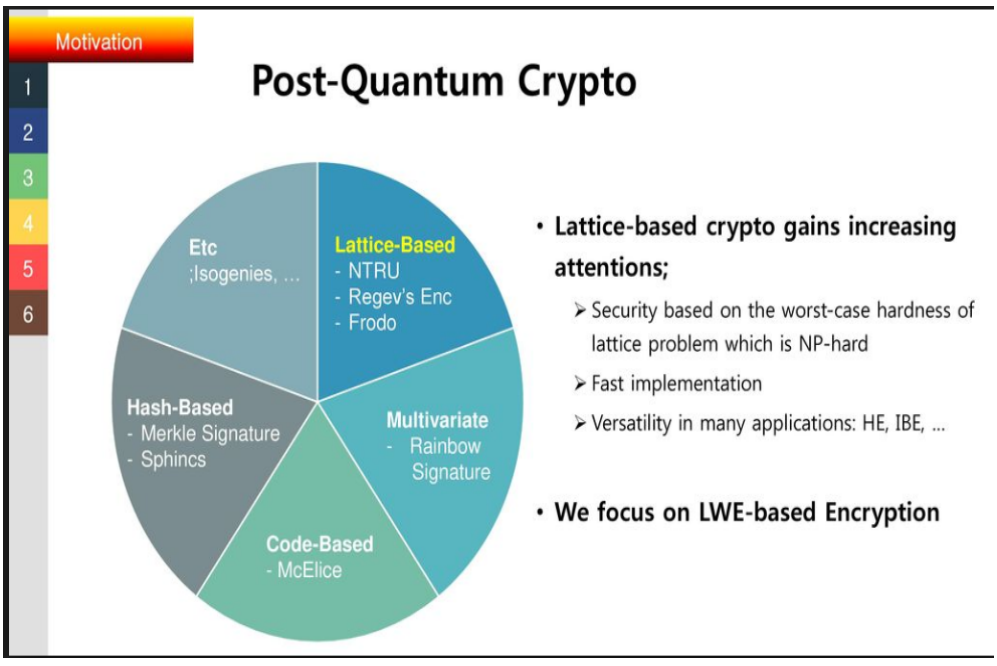
Λαμβάνοντας υπόψη όλες αυτές τις πηγές, είναι σαφές ότι η προσπάθεια να αναπτυχθούν τεχνολογίες ανθεκτικές στις κβάντες εντείνεται. Εξίσου σαφές είναι ο επείγων χαρακτήρας των επενδύσεων αυτών για την ανάγκη τυποποίησης της νέας κρυπτογραφίας μετά το κβαντικό δημόσιο κλειδί. Είναι κρίσιμο να συνεργαστούμε με την κοινότητα για τα κρυπτογραφικά πρότυπα NIST που πρέπει να υιοθετηθούν από τη βιομηχανία και άλλους οργανισμούς τυποποίησης σε όλο τον κόσμο.

Η ανάπτυξη προτύπων για τη μετακβαντική κρυπτογραφία θα απαιτήσει σημαντικούς πόρους για την ανάλυση υποψήφιων κβάντων ανθεκτικών συστημάτων και θα απαιτήσει σημαντική δημόσια εμπλοκή για να εξασφαλίσει την εμπιστοσύνη στους αλγορίθμους που επιλέγει η NIST για τυποποίηση. Το ενδιαφέρον για τους τομείς της κβαντικής πληροφορικής και της κβαντο-ανθεκτικής κρυπτογράφησης έχει πρόσφατα αυξηθεί, λόγω των ορόσημων στην ανάπτυξη του κβαντικού υπολογιστικού υλικού και των πρόσφατων αλλαγών που παρουσίασε η National Security Agency (NSA). Αυτό παρέχει μια ευκαιρία για συμμετοχή στην ερευνητική κοινότητα που ίσως να μην ξανασυμβεί προτού η πραγματική κβαντική πληροφορική γίνει πραγματικότητα. Κατά συνέπεια, ο NIST αρχίζει να προετοιμάζεται για τη μετάβαση στην κβαντο-ανθεκτική κρυπτογράφηση.

ΚΕΦΑΛΑΙΟ 3

Κύριες Κατηγορίες-Υποδιαιρέσεις Μετακβαντικής Κρυπτογραφίας

3.1 Εισαγωγή



Εικόνα 3.1: Πολυμορφηκότητα- Διακλάδωση Μετακβαντικής Κρυπτογράφησης

Αφού προηγουμένως ορίσαμε την έννοια της μετακβαντικής κρυπτογραφίας καθώς και τον σκοπό αλλά και τις πτυχές που προδιαθέτει αυτό το είδος της κρυπτογραφίας στην συνέχεια αυτού του κεφαλαίου θα γίνει μια εκτενής μελέτη στις κατηγορίες, οι οποίες απαρτίζουν την Μετακβαντική Κρυπτογραφία μία προς μία. Όπως και στην κβαντική κρυπτογραφία αλλά και στην κρυπτογραφία που χρησιμοποιείται σήμερα στις μέρες μας υπάρχουν διάφορες κατηγορίες καθώς και υποδιαιρέσεις αυτών των κατηγοριών που όλες μαζί αποτελούν την μετακβαντική

κρυπτογραφία.

Η μετακβαντική Κρυπτογραφία εστιάζει σε 5 κύριους τύπους κρυπτογραφικών συστημάτων καθώς και κάποια άλλα μικρότερα αυτόνομα υποσυστήματα τα οποία δεν αποτελούν κύρια κατηγορία τα οποία το καθένα ξεχωριστά μπορεί να είναι σε θέση να αποκρούσει επιθέσεις από κβαντικούς υπολογιστές. Η κύρια διαφορά μεταξύ αυτών είναι ότι βασίζονται σε διαφορετικές μαθηματικές δομές. Συγκεκριμένα οι κύριοι τύποι που θα αναληθούν στην συνέχεια του κεφαλαίου είναι οι ακόλουθοι.

1. Κώδικες διόρθωσης σφαλμάτων με κύρια έμφαση στο κρυπτοσύστημα MC Eliece
2. Πλέγματα
3. Συναρτήσεις κατακερματισμού
4. Συναρτήσεις πολλών μεταβλητών
5. Ισομορφισμός πάνω σε ελλειπτικές καμπύλες.

Στην συνέχεια θα γίνει αναφορά και ανάλυση και στο κρυπτογραφικό σύστημα του μετακβαντικού RSA καθώς παρουσιάζει ιδιαίτερο ενδιαφέρον.

3.2 Κώδικες Διόρθωσης Σφαλμάτων-Mc Eliece

Οι κώδικες διόρθωσης σφαλμάτων πρόκειται για μια από τις κύριες κατηγορίες μετακβαντικής κρυπτογράφησης. Με τον όρο αυτό, εννοούμε τα κρυπτοσυστήματα στα οποία το αλγοριθμικό πρωτόγονο δηλαδή η υποκείμενη λειτουργία μονής κατεύθυνσης χρησιμοποιεί έναν κώδικα διόρθωσης σφάλματος C. Αυτό το πρωτόγονο μπορεί να συνίσταται στην προσθήκη σφάλματος σε μια λέξη του C ή σε υπολογισμό ενός συνδρόμου σε σχέση με μια μήτρα ελέγχου ισοτιμίας του C. [27] Το ιδιωτικό κλειδί είναι ένας τυχαίος δυαδικός μη αναγωγικός κώδικας Goppa και το δημόσιο κλειδί είναι ένας τυχαίος πίνακας γεννήτριας μιας τυχαία μετατρεπόμενης έκδοσης αυτού του κώδικα. Το κρυπτογράφημα είναι μια λέξη κώδικα με τα οποία έχουν προστεθεί ορισμένα σφάλματα, και μόνο ο κάτοχος του ιδιωτικού κλειδιού δηλαδή του Goppa κώδικα μπορεί να αφαιρέσει αυτά τα σφάλματα. Όπως και για οποιαδήποτε κατηγορία κρυπτοσυστημάτων, η πρακτική της κρυπτογραφίας με βάση τον κώδικα αποτελεί συμβιβασμό μεταξύ ασφάλειας και αποτελεσματικότητας. Παρόλο που δεν είναι γνωστή η πρακτική εφαρμογή κρυπτογραφίας με βάση τον κώδικα ίσως επειδή μπορεί εν μέρει να οφείλεται στο μεγάλο μέγεθος του δημόσιου κλειδιού της τάξεως των 100 kilobytes σε αρκετά megabytes, αλλά ίσως και σε μια έλλειψη της δημοσιότητας σε ένα

πλαίσιο που δεν ήταν επειγόντως απαραίτητη η εναλλακτική λύση.
Μερικά παραδείγματα αυτού του είδους κρυπτογράφησης είναι το κρυπτογραφικό σύστημα McEliece όπου θα το δούμε αναλυτικά στην συνέχεια,το Niederreiter και το σχετικό σύστημα Courtois, το Finiasz καθώς και το Sendrier Signature.

Mc Eliece

Ήταν το πρώτο κρυπτοσύστημα δημόσιου κλειδιού που βασίστηκε στον κώδικα και εισήχθη το 1978 από τον McEliece. Το δημόσιο κλειδί ορίζει έναν τυχαίο δυαδικό κώδικα Goppa. Ένα κρυπτογράφημα είναι μια λέξη κώδικα συν τυχαία σφάλματα. Το ιδιωτικό κλειδί επιτρέπει την αποτελεσματική αποκωδικοποίηση: εξαγωγή της κωδικής λέξης από το κρυπτογραφικό κείμενο, τον εντοπισμό και την αφαίρεση των σφαλμάτων.

Μετά την κβαντική κρυπτογραφία, μια νέα έκδοση του κρυπτοσυστήματος McEliece που βασίζεται σε πολικούς κώδικες και οι οποίοι προτείνουν πρόσφατα ελπιδοφόρους κώδικες διόρθωσης σφαλμάτων σε πολλές εφαρμογές.

Η κρυπτογραφία δημόσιου κλειδιού είναι μία από τις βασικές τεχνολογίες για την εξακρίβωση της γνησιότητας και την ηλεκτρονική πληρωμή του ηλεκτρονικού εμπορίου στο Διαδίκτυο. Ωστόσο, είναι γνωστό ότι τα ευρέως χρησιμοποιούμενα κρυπτοσυστήματα δημόσιου κλειδιού όπως ο αλγόριθμος RSA και η κρυπτογραφία ελλειπτικής καμπύλης μπορούν να σπάσουν με τον αλγόριθμο Shor, ο οποίος μπορεί να λειτουργήσει μόνο σε κβαντικούς υπολογιστές. Ευτυχώς, οι κβαντικοί υπολογιστές που μπορούν να εκτελέσουν τον κβαντικό υπολογισμό με πρακτικό μήκος παραμέτρων δεν έχουν ακόμη πραγματοποιηθεί, μπορούμε ακόμα να χρησιμοποιήσουμε τα συμβατικά συστήματα δημόσιου κλειδιού. Ωστόσο, αναμένεται ότι η υλοποίηση των πρακτικών κβαντικών υπολογιστών θα γίνει πραγματικότητα στο εγγύς μέλλον.[29] Ως εκ τούτου, απαιτείται η προετοιμασία των αντικαταστάσεων για τους συμβατικούς κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού, οι οποίοι θα είναι άχρηστοι μετά από πρακτικούς κβαντικούς υπολογιστές. Οι υποψήφιοι και η ερευνητική σειρά τους καλούνται ως μετα-κβαντική κρυπτογραφία (PQC) και ένας από τους πολλά υποσχόμενους αλγόριθμους PQC είναι η κρυπτογραφία McEliece που βασίζεται σε κώδικες διόρθωσης σφαλμάτων.

Ο McEliece πρότεινε ένα κρυπτοσύστημα δημόσιου κλειδιού βασισμένο σε κώδικες διόρθωσης σφαλμάτων το 1978. Βασίζεται στον δυαδικό κώδικα Goppa για την κατασκευή κρυπτοσυστήματος και δεν υπάρχει επιτυχής επίθεση για την αποκωδικοποίηση των τυχαίων κωδίκων Goppa για να σπάσει το δημόσιο McEliece κλειδί κρυπτογράφηση μέχρι τώρα. Μετά από την πρόταση της αρχικής ιδέας, υπήρχαν διαμάχες που βασίζονταν σε διάφορους κωδικούς, όπως κώδικες Reed-Solomon, κώδικες Reed-Muller, κώδικες LDPC, συνελικτικοί κώδικες. Ωστόσο, οι παραλλαγές των κρυπτοσυστημάτων McEliece σπάνε ή έβρισκαν την αδυναμία τους, εκτός από την αρχική πρόταση του McEliece με βάση τους κώδικες Goppa. Επομένως, είναι σημαντικό να αναθεωρήσετε την αρχική πρόταση του McEliece.[31]

Έστω C ο δυαδικός κώδικας Goppa με μήκος κώδικα N, διάσταση K και ελάχιστη απόσταση 2t + 1 όπου t = (N-K) / log2 n. Στην αρχική πρόταση, ο McEliece χρησιμοποίησε παραμέτρους N = 1,024, K = 524 και t = 50. Με αυτές τις παραμέτρους, το μέγεθος του δημόσιου κλειδιού είναι 67,072 bytes και ο ρυθμός μετάδοσης είναι 0,512. Σε αυτό το σύστημα, το ιδιωτικό κλειδί αποτελείται από τη μήτρα γεννήτριας G του δυαδικού κώδικα Goppa, ένα αποτελεσματικό σχήμα αποκαταστάσεως που μπορεί να διορθωθεί με t-σφάλμα και το N × N matrix μεταθέσεως P και K x K μηδενικό matrix S.

Είναι δύσκολο να προσδιοριστεί η ακριβής θέση των σφαλμάτων t που προστίθενται τυχαία στη λέξη κώδικα. Τα σφάλματα προστίθενται σε τυχαίες θέσεις και λόγω αυτού, η κρυπτογράφηση του κρυπτοσυστήματος McEliece ονομάζεται στοχαστική κρυπτογράφηση.[32] Ακόμα και το ίδιο μήνυμα είναι κρυπτογραφημένο, η θέση των σφαλμάτων στο κείμενο του ciper δεν είναι ίδια με την προηγούμενη. Δεν είναι εφικτό να προσδιοριστούν τυχαίες θέσεις σφαλμάτων σε μεγάλο μήκος μπλοκ από τον εισβολέα. Δεδομένου του μήκους Gpub δημόσιου κλειδιού, ο επιτιθέμενος δεν μπορεί να υπολογίσει ή να διακρίνει αποτελεσματικά τα στοιχεία ιδιωτικού κλειδιού που είναι ενσωματωμένα στο δημόσιο κλειδί Gpub. Για την κρυπτογράφηση δημόσιου κλειδιού McEliece, εκτός από την εξαίρεση μερικών αδύναμων κλειδιών, οι δομικές επιθέσεις είναι αναποτελεσματικές λόγω της μεγάλης καρδιανότητας πιθανών μεταθέσεων, των γεννήτριων matrix και των πινάκων κρυπτογράφησης. Χρησιμοποιήθηκαν διάφορες μέθοδοι κρυπτοανάλυσης για τα διάφορα κρυπτοσύστηματα McEliece. Για το κρυπτοσύστημα McEliece, η επίθεση με τα λάθη. Σε αυτόν τον αλγόριθμο, λαμβάνοντας υπόψη το κρυπτογραφικό κείμενο C, καθορίζεται διάνυσμα σφάλματος που είναι η

ελάχιστη κωδική λέξη βάρους Hamming. Αυτή η μέθοδος αποκωδικοποίησης είναι γνωστή ως "επίθεση αποκωδικοποίησης" επειδή είναι ισοδύναμη με την αποκωδικοποίηση γραμμικού κώδικα.

Το νέο κρυπτοσύστημα McEliece που προτείνεται πιο πάνω βασίζεται σε πολικούς κώδικες, οι οποίοι προτείνονται από τον Arikan και έχουν αποδειχτεί ότι επιτυγχάνουν ασυμπτωτικά το όριο Shannon. Αυτός ο κώδικας διακρίνεται από τους προηγούμενους κώδικες διόρθωσης σφαλμάτων με την έννοια της χρήσης της κατάστασης καναλιού εισάγοντας την πόλωση του καναλιού. Στην πόλωση του καναλιού, με γραμμική επεξεργασία, τα N ισοδύναμα κανάλια μπορούν να χωριστούν ασυμπτωτικά σε δύο τύπους, σφάλματα και κακά κανάλια που δεν μπορούν να χρησιμοποιηθούν για τη μετάδοση πληροφοριών. Επομένως, για τα κακά κανάλια, χρησιμοποιούνται τα προκαθορισμένα bits (κατεψυγμένα bits) και χρησιμοποιούνται μόνο καλά κανάλια για τη μετάδοση πληροφοριών. Χρησιμοποιώντας την διαδοχική αποκωδικοποίηση ακύρωσης, μπορούμε να αποκωδικοποιήσουμε τις πληροφορίες που μεταδίδονται στα καλά κανάλια.

Μια Προτεινόμενη μέθοδος

Α. Κατασκευή

Δείχνεται ότι η μυστικότητα μπορεί να επιτευχθεί με τη χρήση πολικών κωδικών στην θεωρητική ασφάλεια πληροφοριών. Οι πολικοί κώδικες έχουν αποδειχθεί ότι λειτουργούν καλύτερα καθώς το μήκος των κωδικών λέξεων αυξάνεται ασυμπτωτικά. Προτείνεται ένας άλλος τρόπος χρήσης πολικών κωδικών για κρυπτογραφική ασφάλεια, αντί για θεωρητική ασφάλεια πληροφοριών. Αφού δημιουργηθεί ο matrix γεννήτριας πολικών κωδικών, επιλέγονται μόνο οι σειρές που αντιστοιχούν σε καλά κανάλια για δεδομένη κατάσταση καναλιού και οι άλλες σειρές απορρίπτονται. Επομένως, από αυτή την επιλογή, μπορούμε να πάρουμε το matrix γεννήτριας GN (A) μεγέθους K × N. Αυτός ο matrix γεννήτριας είναι τυχαίας κατανομής με matrix μοναδιαίου κρούσματος K × K και matrix μεταλλαγής N × N. Στη συνέχεια, ο δημόσιος πίνακας γίνεται Gpub = SGN (A) P.

Για αξιόπιστη αποκωδικοποίηση και εξασφάλιση επαρκούς επιπέδου ασφαλείας, θα ορίσουμε το μήκος κώδικα N = 2.048 και τον κωδικό συντελεστή 0.3. Η διάσταση του

matrix γεννήτριας είναι (614 × 2048). Για να επιλέξετε σειρές αντίστοιχων καλών καναλιών μετά την πόλωση του καναλιού, επιτυγχάνεται η χωρητικότητα του καναλιού πολωμένου καναλιού και επιλέγονται τα καλύτερα κανάλια από αυτά. Αφού δημιουργηθεί ο matrix της γεννήτριας, πρέπει να γίνει αόρατη με πολλαπλασιασμό με τους μιστυκούς matrix «S» και «P» που περιλαμβάνονται στο ιδιωτικό κλειδί. Αυτό κάνει την δομή του να εμφανίζεται τυχαία καθιστώντας έτσι απλή αποκωδικοποίηση άχρηστη. Δηλαδή, το δημόσιο κλειδί είναι ένας τυχαίος πίνακας γεννήτριας ο οποίος είναι ο κωδικοποιημένος και τροποποιημένος πίνακας γεννήτριας για την κωδικοποίηση δεδομένων.

Β. Ιδιωτικό κλειδί

Το ιδιωτικό κλειδί περιλαμβάνει ένα matrix κρυπτογράφησης S και το πλέγμα μεταλλαγής P. Για την κατασκευή του invertible matrix S, χρησιμοποιούμε την παραγωγή τυχαίων αριθμών στην περιοχή [0,1] και τη διάσταση K × K. Προκειμένου να ελέγξουμε την ανυπαρξία του, μπορούμε να εφαρμόσουμε τη μέθοδο Gaussian elimination. Για την περίπτωση του πίνακα μετασχηματισμού, ο matrix έχει διάσταση N × N. Αυτός ο matrix σχηματίζεται από την τυχαία στήλη, η οποία μετρά την ταυτότητα matrix N × N. Αφού ο δέκτης λάβει ένα κρυπτογράφημα, αντιστρέφεται με πολλαπλασιασμό του αντιστρόφου matrix μετάθεσης. Για να ληφθεί το αντίστροφο του matrix μετάθεσης, αρκεί η μεταφορά του matrix μεταστοιχείωσης.

Γ. Δημόσιο κλειδί

Το δημόσιο κλειδί δίνεται ως ο matrix Gpub = SGN (A) P. Δεδομένου ότι το δημόσιο κλειδί είναι «δημόσιες» πληροφορίες, ο καθένας όχι μόνο για τον αποστολέα «Alice» έχει τη γνώση του Gpub αλλά δεν έχει καμία γνώση για τους παράγοντες S και P του Gpub. Επομένως, παρόλο που οι άλλοι γνωρίζουν το δημόσιο κλειδί, δεν μπορούν να αποκρυπτογραφήσουν σωστά το κρυπτογραφικό κείμενο. Υπάρχουν διαφορετικές κατασκευές του matrix γεννήτριας πολικών κωδικών. Θα χρησιμοποιήσουμε τον πίνακα F. Ο Korada έχει δώσει μια εξήγηση για την τάξη του πίνακα που μπορεί να πολώσει τα κανάλια. Για την πόλωση, ο matrix της γεννήτριας πρέπει να είναι κατασκευασμένη από κάτω με τριγωνικό matrix . Ο matrix F = [1 0 1 1] ικανοποιεί αυτή την κατάσταση.

Δ. Κρυπτογράφηση του Προτεινόμενου Σχεδίου

Το μήνυμα K-bit κωδικοποιείται ως εξής:

Υ = mSGN (A) P + e ,όπου ο τελευταίος όρος e είναι ένα διάνυσμα σφάλματος το οποίο εμφανίζεται κυρίως σε κακά κανάλια λόγω μετασχηματισμού καναλιού.

Ε. Αποκρυπτογράφηση του Προτεινόμενου Σχεδίου: Διορθώστε την αποκρυπτογράφηση

Σε αυτό το σημείο, θα ήθελα να σχολιαστέι η αποκρυπτογράφηση από τον πραγματικό παραλήπτη. Πρώτον, ο πίνακας μεταλλαγής P που περιλαμβάνεται στο ιδιωτικό κλειδί χρησιμοποιείται για να εντοπίσει την αντίστροφη μετάθεση P-1. Αυτή η αντίστροφη μετάθεση πολλαπλασιάζεται με το λαμβανόμενο κρυπτογραφικό κείμενο Υ και μπορούμε να λάβουμε τα ενδιάμεσα δεδομένα ως εξής: $Υ' = ΥP^{-1}$

Μετά την αφαίρεση του matrix μεταλλαγής στο λαμβανόμενο κρυπτοκείμενο κείμενο, μπορούμε τώρα να αποκωδικοποιήσουμε τα δυαδικά ψηφία του Υ 'με τη χρήση της διαδοχικής αποκωδικοποίησης ακύρωσης. Με τον υπολογισμό των αναλογιών πιθανότητας, μπορούμε να αποκτήσουμε τον λόγο πιθανότητας οποιουδήποτε bit i εάν είναι γνωστά προηγούμενα (i-1) bits. Χρησιμοποιώντας τον κανόνα απόφασης των δυαδικών ψηφίων βάσει του λόγου πιθανοτήτων, λαμβάνεται η εκτίμηση του πρώτου δυαδικού ψηφίου. Στη συνέχεια, το πρόσφατα αποκωδικοποιημένο κομμάτι μαζί με όλο το άλλο προηγουμένως αποκωδικοποιημένο δυαδικό ψηφίο χρησιμοποιείται για την αποκωδικοποίηση του μελλοντικού δυαδικού ψηφίου μέχρι να ολοκληρωθεί αυτή η διαδικασία για όλο το μήκος του μπλοκ. Κατά τη διαδικασία αποκωδικοποίησης, η απόφαση πρέπει να ληφθεί μόνο με βάση το σύνολο πληροφοριών. Στο παγωμένο σύνολο, εισάγονται τα προκαθορισμένα bits. Στην περίπτωσή μας, τα προκαθορισμένα bits ρυθμίζονται σε όλους τους 0 φορείς. Μετά την αποκωδικοποίηση, επιλέγονται μόνο εκείνα τα δυαδικά ψηφία που βρίσκονται στο ευρετήριο του συνόλου πληροφοριών. Ακόμα και μετά τη λήψη των δυαδικών ψηφίων από το σύνολο πληροφοριών, δεν έχουμε ακόμα σωστό μήνυμα. Ο προφανής λόγος για αυτό είναι ότι πρέπει να καταργήσουμε τους αναδιπλούμενοι κώδικες από τις αποκωδικοποιημένες πληροφορίες.

Δηλαδή, οι πληροφορίες που αποκτώνται από τον αποκωδικοποιητή διαδοχικής ακύρωσης δίδονται ως m'

m' = mS.

Προκειμένου να ληφθούν οι σωστές πληροφορίες m, πρέπει να χρησιμοποιήσουμε μια άλλη γνώση του matrix S που περιλαμβάνεται στο ιδιωτικό κλειδί. Από το S, το αντίστροφο υπολογίζεται με τη μέθοδο Gaussian elimination. Ο αντίστροφος πίνακας S-1 πολλαπλασιάζεται επί m 'και τελικά μπορούμε να ανασυνθέσουμε το επιθυμητό αρχικό μήνυμα m ως εξής :

$m = m'S^{-1} = (mS)S^{-1}$

Ε. Ανάλυση Ασφάλειας

Σε αυτό το σημείο, θα αναφερθώ στην ασφάλεια του προτεινούμενου συστήματος.

TABLE I. THE AVERAGE NUMBER OF ERRORS ACCORDING TO THE CODE RATE AND ERASURE PROBABILITY e FOR $L = 1,024$

rate \e	0.2	0.3	0.4	0.5	0.6	0.7
0.3	154.3	153.5	153	154.1	152	152
0.5	257	256.4	256.5	244	-	-
0.6	308.3	308	304.8	-	-	-
0.7	359	357.5	-	-	-	-
0.8	412.1	-	-	-	-	-

TABLE II. THE AVERAGE NUMBER OF ERRORS ACCORDING TO THE CODE RATE AND ERASURE PROBABILITY e FOR $L = 2,048$

rate \e	0.2	0.3	0.4	0.5	0.6	0.7
0.3	303.8	311	306.8	305.4	306	303
0.5	508	511.7	507.9	508.3	-	-
0.6	613.1	617	614	-	-	-
0.7	714	714.2	-	-	-	-
0.8	821	-	-	-	-	-

Α. Αποκωδικοποιήση από Attacker

Σε αυτό το υποκεφάλαιο, πρώτα θα αναλύσουμε την ισχύ του προτεινόμενου σχεδίου ενάντια στην εξαντλητική αποκωδικοποίηση μονοπατιών. Ο μη εξουσιοδοτημένος αποκωδικοποιητής (ή εισβολέας) προσπαθεί να αποκωδικοποιήσει τις σωστές πληροφορίες χωρίς τη γνώση του ιδιωτικού κλειδιού. Για να αποκωδικοποιήσει το κρυπτογραφικό κείμενο, ο εισβολέας αναλαμβάνει έναν τυχαίο πίνακα μετασχηματισμού P και έναν πίνακα scramble S. Επειδή είναι δυνατόν να αποκαλυφθεί η αρχική πληροφορία ακόμη και με την τυχαίο matrix μετασχηματισμού P και τον matrix scramble S, πρώτα ελέγξουμε τη δυνατότητα χρησιμοποιώντας αριθμητικά προσομοίωση. Δηλαδή, πρώτον, ο εισβολέας μαντέψει τυχαία τις μήτρες μετατόπισης και ανατροπής P 'και S' για το δεδομένο δημόσιο κλειδί Gpub και, στη συνέχεια, εφαρμόζει την διαδοχική αποκωδικοποίηση ακύρωσης για να πάρει σωστές πληροφορίες.

Η αριθμητική προσομοίωση εκτελέστηκε για τα μήκη μπλοκ N = 1,024, 2,048 και 4,096 όπου N = 2n και n = 10,11 και 12 με ρυθμούς πληροφόρησης ξεκινώντας από 0,3 έως 0,8 και πάνω από το δυαδικό κανάλι διαγραφής (BEC) με πιθανότητες διαγραφής 0,2 έως 0,7 . Τα αποτελέσματα προσομοίωσης παρουσιάζονται στους Πίνακες I-III. Οι τιμές σε αυτούς τους πίνακες επιτυγχάνονται επαναλαμβάνοντας την επεξεργασία τυχαίων εικασιών 10.000 φορές και υπολογίζοντας κατά μέσο όρο τα αποτελέσματα. Όπως μπορείτε να δείτε στους πίνακες, η αριθμητική προσομοίωση δείχνει ότι οι ρυθμοί σφάλματος είναι περίπου 0,5 για τους διάφορους ρυθμούς κώδικα και τα διάφορα κανάλια με διαφορετικές πιθανότητες διαγραφής όταν χρησιμοποιούνται τυχαία εικασμένες μεταστοιχείες και μήτρες ανατροπής. Επίσης, μπορούμε να προσδιορίσουμε την τοποθεσία των σφαλμάτων είναι επίσης τυχαία για κάθε επεξεργασία. Επομένως, μπορούμε να σκεφτούμε ότι ο επιτιθέμενος δεν μπορεί να έχει κανένα πλεονέκτημα από την τυχαία μαντεία για το ιδιωτικό κλειδί.[32]

Β. Επίθεση βίαιης δύναμης

Σε αυτήν την υποενότητα, θα υπολογίσουμε την πολυπλοκότητα τυχαίων εικασιών για το ιδιωτικό κλειδί. Για μη μοναδική μήτρα scramble S της διάστασης K × K, η καρδιανότητα του S δίνεται ως

$$\begin{aligned}\sharp S &= (2^K - 1)(2^K - 2)(2^K - 2^2) \cdots (2^K - 2^{K-1}) \\ &= 2^{0+1+2+\cdots+(K-1)}(2^K - 1)(2^{K-1} - 1) \cdots (2^2 - 1) \cdot 1 \\ &= 2^{\binom{K}{2}}[K]!\end{aligned}$$

όπου [K] = $2^{K-1} + 2^{K-2} + \cdot + 2 + 1 = 2^K - 1$ και [K]! = [K] [K-1] [K -2] ⋯ [2] [1].

Για μεγαλύτερη απλόποίηση,

TABLE III. THE AVERAGE NUMBER OF ERRORS ACCORDING TO THE CODE RATE AND ERASURE PROBABILITY e FOR $L = 4,096$

rate \e	0.2	0.3	0.4	0.5	0.6	0.7
0.3	612.3	614.9	613.4	610.9	614.1	619.5
0.5	1,017	1,014	1,007	1,035	-	-
0.6	1,176	1,219	1,225	-	-	-

μπορούμε να χρησιμοποιήσουμε την ακόλουθη ανισότητα:

$$\begin{aligned}\sharp S &= 2^{\binom{K}{2}}(2^K - 1)(2^{K-1} - 1) \cdots 2 \cdot 1 \\ &\leq 2^{\binom{K}{2}} 2^K \cdot 2^{K-1} \cdots 2^2 = 2^{2\binom{K}{2}-1} = 2^{K(K+1)-1}\end{aligned}$$

Επίσης, είναι σαφές ότι υπάρχουν N! πιθανοί πίνακες μεταστοιχείωσης. Με αυτούς τους μεγάλους αριθμούς πιθανών μεταβλητών πινάκων και πινάκων μεταλλαγής, δεν είναι εφικτό να εντοπιστούν τα σωστά S και P με τη μέθοδο hit και trial, καθώς ο αριθμός των απαιτούμενων δοκιμών θα ήταν κατά μέσο όρο (♯S) (N!).

Για παράδειγμα, όταν το μπλοκ φτάσει αυτό το 1,024, η καρδιανότητα των αντιστρεπτών πινάκων είναι

$\sharp S \leq {}^{2512\times513-1} = 2^{262,655}$

Και όταν το μήκος του μπλοκ είναι 2.048, η καρδιαλότητα των μετατρέψιμων πινάκων είναι

$\sharp S \leq 2^{1024\times1025-1} = 2^{1,049,599}$

Επιπλέον, η καρδιαλότητα των πινάκων μεταθέσεως για το μήκος μπλοκ 1,024 ή 2,048 δίνεται ως (1024!) ή (2048!). Με την προσέγγιση του Stirling για την παραγοντική

συνάρτηση, έχουμε $x! \approx x^x e^{-x}\sqrt{2\pi x}$. Ως εκ τούτου, έχουμε

$$1,024! \approx 2^{10,240} e^{-1,024} \sqrt{2,048\pi} \approx 2^{8,769.6}$$

και

$$2,048! \approx 2^{22,528} e^{-2,048} \sqrt{4,096\pi} \approx 2^{19,581.4}$$

Επομένως, ο μέγιστος αριθμός δοκιμών για επιτυχημένη τυχαία εικασία P και S δίνεται ως $(\sharp S)\,(N!) \leq 2^{271,424.6}$ ή $2^{1,069,180.4}$ για N = 1,024 ή N = 2,048, αντίστοιχα.

Γ. Επίθεση Sidelnikov

Είναι γνωστό ότι η κατασκευή των πολικών κωδικών και του κώδικα Reed-Muller (RM) είναι πολύ παρόμοια. Ωστόσο, με την εξελιγμένη ανάλυση μεταξύ αυτών των κατασκευών, μπορούμε να διαπιστώσουμε ότι υπάρχουν σημαντικές διαφορές. Σε αυτή την υποενότητα θα επικεντρωθούμε στη διαφορά μεταξύ των πολικών κωδικών και των κωδικών RM, διότι πρόκειται να δείξουμε ότι δεν μπορεί να εφαρμοστεί η σημαντική κρυπτοανάλυση κατά του κρυπτοσυστήματος McEliece που βασίζεται σε κώδικες RM γνωστού ως κρυπτοσύστημα Sidennikov στο προτεινόμενο σχήμα που βασίζεται σε πολικούς κωδικούς.

Πρώτα απ 'όλα, ο N × N σούπερ πίνακας για τις μήτρες των γεννητριών και των δύο πολικών κωδικών και των κωδικών RM μπορεί να κατασκευαστεί λαμβάνοντας τη δύναμη mth Kroenecker της μήτρας F = [1 0 1 1] όπου N = 2m. Εάν m = 3, έχουμε τον ακόλουθο πίνακα γεννήτριας

$$F^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Στον κώδικα R (r, m), μόνο σειρές που έχουν μέγιστο βάρος επιλέγονται από Ftinum για

την κατασκευή της μήτρας γεννήτριας. Μετά τη διαλογή των επιλεγμένων σειρών σύμφωνα με το βάρος Hamming από το υψηλότερο στο χαμηλότερο βάρος και την ομαδοποίηση σειρών με ίσο βάρος Hamming, μπορούμε να πάρουμε τη μήτρα γεννήτριας ενός κώδικα RM. Ο αριθμός των κωδικών λέξεων με το ίδιο βάρος Hamming είναι ίσο με Ci = (m i) όπου 0 ≤ i ≤ m. Προσθέτοντας όλα τα Ciare ίσα με τον αριθμό των γραμμών στο R (r, m). Το βάρος Hamming των κωδικών λέξεων στο C 'είναι ίσο με 2m-i.

Οι κωδικοί λέξεις βαθμού 2 του R (r, m) είναι ίσες με το προϊόν των 2 κωδικών λέξεων του R (1, m). Αυτό ισχύει για όλους τους δυνατούς συνδυασμούς (m 2). Όταν 3 μεταβλητές του βαθμού 1 πολλαπλασιάζονται, τότε η προκύπτουσα λέξη κώδικα έχει βαθμό 3. Επομένως, υπάρχουν όλες μαζί (m 3) τέτοιες λέξεις-κλειδιά και το βάρος κάθε μιας από αυτές είναι 2m-3. Όταν αυτές οι λέξεις-κλειδιά είναι διαδοχικές με R (2, m), ο νέος κώδικας μπορεί να γραφεί ως R (3, m). Από αυτό μπορούμε να πούμε ότι το R (0, m) είναι ένα υποσύνολο του R (1, m) που είναι ένα υποσύνολο του R (2, m) και ούτω καθεξής. Τέλος, το R (m-1, m) είναι ένα υποσύνολο του R (m, m). Έπειτα, έχουμε την ακόλουθη ιδιότητα των κωδικών RM

$$R(0,m) \subset R(1,m) \subset \cdots \subset R(m-1,m) \subset R(m,m).$$

Η επίθεση κατά του κρυπτοσυστήματος Sidelnikov χρησιμοποιεί αυτή την ιδιότητα για να εντοπίσει τη μυστική μεταλλαγή P του δημόσιου κλειδιού Gpub. Χρησιμοποιώντας τον αλγόριθμο, προσδιορίζεται η κωδική λέξη που ανήκει στο R (r-1, m). Αν και ο αλγόριθμος μεταβάλλεται με δύο τρόπους, και οι δύο παίρνουν το παρόμοιο έργο, δηλ., Φθάνουν οι συντελεστές R (r, m) που ανήκουν στο R (r - 1, m). Πρέπει να σημειώσουμε ότι αυτές οι κωδικές λέξεις είναι μεταβλητές και κωδικοποιημένες. Όταν συναντάμε επαρκείς συντελεστές του R (r, m) τότε γνωρίζουμε ότι αυτοί οι παράγοντες ανήκουν στο R (r - 1, m) επειδή R (r - 1, m) είναι ένας υποκώδικας R (r, m). Στη συνέχεια επαναλαμβάνεται η ίδια διαδικασία στις λέξεις-κλειδιά του R (r - 1, m) για την εύρεση των κωδικών λέξεων που ανήκουν στο R (r - 2, m). Αυτή η διαδικασία συνεχίζεται με μείωση του r σε κάθε επανάληψη μέχρι να βρεθούν αρκετοί παράγοντες για να κατασκευαστεί τελικά η βάση των Rm (1, m). Αφού εντοπιστούν κωδικοποιημένες λέξεις-κλειδιά του R (1, m), το επόμενο βήμα είναι να εντοπιστεί η μετάθεση η οποία αναδιατάσσει τις στήλες της μήτρας γεννήτριας σε κανονική μορφή. Η λέξη κώδικα που περιέχει όλα τα 1 απορρίπτεται και λαμβάνονται μόνο μεταβλητές m.
Οι κωδικές λέξεις χαμηλού βαθμού είναι ένας παράγοντας κωδικών λέξεων υψηλότερου

βαθμού. Ως εκ τούτου, η επίθεση Sidelnikov εντοπίζει τους παράγοντες που βρίσκονται στον υποκώδικα κωδικών λέξεων υψηλής τάξης. Μετά την ανίχνευση του κώδικα R (1, m) p, μπορεί να βρεθεί η αντίστοιχη μετάθεση q η οποία είναι αντίστροφη του p όπως (R (1, m) ρ) q = R (1, m). Για δεδομένο r και m, η μήτρα γεννήτριας των κωδικών RM αποτελείται μόνο από εκείνες τις σειρές που έχουν υψηλότερο βάρος Hamming και όλες οι άλλες κωδικές λέξεις που έχουν λιγότερες κωδικές λέξεις Hamming απορρίπτονται.

Στην περίπτωση πολικών κωδικών, αυτή η προσέγγιση δεν μπορεί να χρησιμοποιηθεί. Από την περιγραφή του Arikan, οι σειρές επιλέγονται σύμφωνα με την χωρητικότητα του καναλιού τους για δεδομένη κατάσταση καναλιού. Για δεδομένο ρυθμό, μόνο οι σειρές που έχουν πολύ υψηλή χωρητικότητα ή πολύ χαμηλή παράμετρο z θεωρούνται σειρές μήτρας γεννήτριας.[33] Λόγω αυτού, κατά τη διάρκεια της επιλογής των σειρών, είναι πολύ συνηθισμένο να απορρίπτεται κάποια υψηλή κωδική λέξη βάρους Hamming και να επιλεγούν ορισμένες χαμηλές κωδικές λέξεις βάρους Hamming. Έτσι μπορούμε να πούμε ότι σε δεδομένη διάσταση των πολικών κωδικών, όλες οι βάσεις που έχουν μικρό βάρος δεν περιέχουν απαραιτήτως τους παράγοντες τους. Και αυτή η επιλογή είναι πολύ διαφορετική από τους κώδικες Reed-Muller. Για μικρότερο μήκος κώδικα, η μήτρα γεννήτριας για πολικούς και RM κώδικες συμβαίνει να είναι η ίδια, αλλά για πολύ μεγαλύτερα μήκη κώδικα που συνήθως χρησιμοποιούνται για πραγματικές εφαρμογές, η μήτρα γεννήτριας πολικών κωδικών συνήθως δεν είναι ίδια με αυτή των κωδικών RM. Επομένως, ο αλγόριθμος παράγοντα που εφαρμόζεται σε πολικούς κωδικούς δεν θα δώσει παράγοντες αυτών των κωδικών λέξεων που ανήκουν στη μήτρα γεννήτριας κάτω διάστασης ως εξής

$$f/= f1 \cdot f2 \cdots f_{r-1} \cdot fr$$

Εξαιτίας αυτού, η μετάθεση των πολικών κωδικών δεν μπορεί να αντιστραφεί, όπως γίνεται στην κρυπτογράφηση Sidelnikov. Ως εκ τούτου, η επίθεση Sidelnikov δεν μπορεί να είναι επιτυχής για την επίθεση στο προτεινόμενο σχήμα βάσει πολικών κωδικών.

Συνοψίζοντας, μελετήσαμε έναν υποψήφιο μετα-κβαντικό κρυπτογράφημα, μια νέα έκδοση του κρυπτο-συστήματος McEliece που βασίζεται σε πολικούς κώδικες, η οποία προτείνεται πρόσφατα ελπιδοφόρες κώδικες διόρθωσης σφαλμάτων σε πολλές εφαρμογές. Μετά την κατασκευή του κρυπτοσυστήματος McEliece χρησιμοποιώντας πολικούς κωδικούς, παρέχουμε κάποιες αναλύσεις ασφαλείας και διαπιστώσαμε ότι η

νέα πρόταση μπορεί να αντισταθεί σε ορισμένες γνωστές επιθέσεις σε κρυπτοσυστήματα McEliece.

3.3 Πλέγματα

Η κατηγορία αυτή αφορά τα πλέγματα και το πώς η κρυπτογράφηση μέσω των πλεγμάτων μπορεί να λειτουργήσει και στην οικογένεια της μετακβαντικής κρυπτογράφησης. Συγκεκριμένα όπως αναφέρθηκε και στα πιο πάνω κεφάλαια, η κρυπτογραφία που είναι βασισμένη σε πλέγμα είναι ο γενικός όρος για κατασκευές κρυπτογραφικών αρχέγονων που εμπλέκουν πλέγματα, είτε στην ίδια την κατασκευή είτε στην απόδειξη ασφαλείας.[34] Οι κατασκευές που βασίζονται σε πλέγματα είναι επί του παρόντος σημαντικοί υποψήφιοι για την μετάκβαντική κρυπτογραφία. Σε αντίθεση με τα ευρύτερα χρησιμοποιούμενα και γνωστά συστήματα δημόσιου κλειδιού, όπως τα cryptosystems RSA, Diffie-Hellman ή Elliptic-Curve (Ελλειπτικές καμπύλες), τα οποία δέχονται εύκολα επίθεση από έναν κβαντικό υπολογιστή, ορισμένα κρυπτοσυστήματα που είναι βασισμένα σε πλέγμα φαίνεται να είναι ανθεκτικά σε επίθεση τόσο από κλασσικούς όσο και από κβαντικούς υπολογιστές . Επιπλέον, πολλές δομές βασισμένες σε πλέγματα είναι γνωστό ότι είναι ασφαλείς υπό την προϋπόθεση ότι ορισμένα καλά μελετημένα προβλήματα υπολογιστικού πλέγματος δεν μπορούν να επιλυθούν αποτελεσματικά.

Οι κρυπτογραφικές κατασκευές βασιζόμενες σε πλέγματα μερικοί θεωρούν πως είναι οι κορυφαίοι υποψήφιοι για την μετάκβαντική κρυπτογραφία δημόσιου κλειδιού. Πράγματι, οι κύριες εναλλακτικές μορφές κρυπτογραφίας δημόσιου κλειδιού είναι τα συστήματα που βασίζονται στη σκληρότητα του factoring και σε συναφή προβλήματα και σχήματα που βασίζονται στη σκληρότητα του διακριτού λογαρίθμου και σε συναφή προβλήματα. Ωστόσο, τόσο ο factoring όσο και ο διακριτός λογάριθμος είναι γνωστό ότι είναι επιλύσιμοι σε πολυωνυμικό χρόνο σε έναν κβαντικό υπολογιστή. Επιπλέον, οι αλγόριθμοι για την παραγοντοποίηση τείνουν να παράγουν αλγόριθμους για διακριτό λογάριθμο και αντίστροφα. Αυτό υποκινεί περαιτέρω τη μελέτη των κατασκευών με βάση εναλλακτικές υποθέσεις, όπως η σκληρότητα των προβλημάτων πλέγματος.[35]
Πολλά κρυπτογραφικά σχήματα βασισμένα σε πλέγμα είναι γνωστό ότι είναι ασφαλή, υποθέτοντας τη σκληρότητα της χειρότερης περίπτωσης τους σε ορισμένα προβλημάτα πλέγματος. Δηλαδή, εάν υπάρχει ένας αλγόριθμος που μπορεί να σπάσει

αποτελεσματικά το κρυπτογραφικό σχήμα με μη αμελητέες πιθανότητες, τότε πρόκυτε για ένα αποτελεσματικό αλγόριθμο που λύει ένα συγκεκριμένο πρόβλημα πλέγματος σε οποιαδήποτε είσοδο. Αντίθετα, τα κρυπτογραφικά συστήματα που βασίζονται,σε μεθόδους όπως το factoring, θα ήταν σπασμένα εάν ο συντελεστής τους ήταν σκληρός ακόμη και αν οι συντελεστές ήταν στην πραγματικότητα σκληροί στη χειρότερη περίπτωση.Ωστόσο, για τις αποδοτικότερες και πρακτικότερες κατασκευές με βάση το πλέγμα όπως τα συστήματα που βασίζονται σε NTRU και ακόμη και τα συστήματα που βασίζονται σε LWE με πιο επιθετικές παραμέτρους, δεν είναι γνωστά τα αποτελέσματα της σκληρότητας της χειρότερης περίπτωσης. Ακόμα με την μετακβαντική κρυπτογραφηση βάσει πλέγματος ο σχεδιασμός τους είναι αρκετά υποσχόμενος. Πολλοί από αυτούς είναι αρκετά αποδοτικοί και κάποιοι ανταγωνίζονται ακόμη και με τις πιο γνωστές εναλλακτικές λύσεις όμως είναι συνήθως και αρκετά απλοί στην εφαρμογή τους. Φυσικά, όλες οι μεθόδοι θεωρούντε ότι είναι ασφαλείς ενάντια στους κβαντικούς υπολογιστές ή τουλάχιστον αυτό υποστηρίζουν με βάση τις προδιαγραφές τους.

Από την άποψη της ασφάλειας, οι κρυπτογραφικές κατασκευές με βάση το πλέγμα μπορούν να διαχωριστούν σε δύο τύπους:

- Το πρώτο περιλαμβάνει πρακτικές προτάσεις, οι οποίες είναι συνήθως πολύ αποτελεσματικές, αλλά συχνά δεν διαθέτουν αποδεικτικά στοιχεία ασφαλείας
- Ο δεύτερος τύπος προσπαθεί να αναγνωρίσει ισχυρές εγγυημένες εγγυήσεις ασφάλειας βασισμένες στη σκληρότητα της χειρότερης περίπτωσης των προβλημάτων πλέγματος.

Όμως μόνο μερικά από αυτά είναι αρκετά αποτελεσματικά για να χρησιμοποιηθούν στην πράξη.

Στην συνέχεια γίνεται μια επεξεργασία που αφορά κυρίως τις ισχυρές εγγυήσεις ασφαλείας που δίνεται από τους τελευταίους σχεδιασμούς του τύπου και αφορούν μη παροχή εγγυημένης σκληρότητας. Αυτό σημαίνει ότι το σπάσιμο της κρυπτογραφικής κατασκευής ακόμη και με κάποια μικρή μη αμελητέα πιθανότητα είναι προφανώς τουλάχιστον τόσο σκληρή, ως επίλυση αρκετών προβλημάτων πλέγματος δηλαδή περίπου, εντός πολυωνυμικών παραγόντων στη χειρότερη περίπτωση. Με άλλα λόγια, το σπάσιμο της κρυπτογραφικής κατασκευής συνεπάγεται ως ένας αποτελεσματικός αλγόριθμος για την επίλυση οποιουδήποτε περιστατικού και κάποιου υποκείμενου πλέγματος.[36]

Στις περισσότερες περιπτώσεις, το υποκείμενο πρόβλημα είναι αυτό της προσέγγισης του πλέγματος όπως τα SVP μέσα στους πολυωνυμικούς παράγοντες, τα οποία αναφέρθηκαν παραπάνω και θεωρούνται ότι είναι ένα δύσκολο πρόβλημα.

Μια τέτοια ισχυρή εγγύηση ασφάλειας είναι ένα από τα χαρακτηριστικά γνωρίσματα της Κρυπτογραφίας που είναι βασισμένη σε πλέγματα. Σχεδόν όλα τα άλλα κρυπτογραφικά συστήματα είναι με βάση τη σκληρότητα κατά μέσο όρο. Για παράδειγμα, το σπάσιμο ενός κρυπτοσυστήματος βασίζεται στο factoring και μπορεί να συνεπάγεται την ικανότητα να παράγουν ορισμένους αριθμούς που επιλέγονται σύμφωνα με μια ορισμένη κατανομή, αλλά όχι στην ικανότητα να παράγουν όλους τους αριθμούς.

Η σημασία της μή εγγύησης ασφάλειας είναι διττή για τους εξής λόγους:

- Πρώτον, αυτό μας διαβεβαιώνει ότι οι επιθέσεις στην κρυπτογραφική κατασκευή είναι πιθανό να είναι αποτελεσματικές μόνο για μικρές επιλογές παραμέτρων και όχι ασυμπτωτικές.Μας διαβεβαιώνει ακόμα ότι δεν υπάρχουν ουσιαστικές ατέλειες στο σχεδιασμό τους. Στην πραγματικότητα, σε ορισμένες περιπτώσεις, η χειρότερη περίπτωση ασφάλειας μπορεί να μας οδηγήσει ακόμη και στη λήψη αποφάσεων σχεδιασμού.
- Δεύτερον,η χειρότερη περίπτωση εγγύησης ασφάλειας μπορεί να μας βοηθήσει στην επιλογή συγκεκριμένων παραμέτρων για το κρυπτοσύστημα, αν και στην πράξη αυτό οδηγεί σε αυτό που φαίνεται υπερβολικά συντηρητικό, και όπως θα δούμε αργότερα, κάποιος συχνά θέτει τις παραμέτρους με βάση τις πιο γνωστές επιθέσεις.

Τα κρυπτοσυστήματα που βασίζονται σε προβλήματα πλέγματος έλαβαν ανανεωμένο ενδιαφέρον, για λίγους λόγους. Συναρπαστικές νέες εφαρμογές όπως η πλήρως ομοιομορφική κρυπτογράφηση, η κωδικοποίηση κώδικα και η κρυπτογράφηση βάση χαρακτηριστικών έχουν καταστεί δυνατές χρησιμοποιώντας κρυπτογράφηση βάση πλέγματος. Οι περισσότεροι αλγόριθμοι δημιουργίας κλειδιών που είναι βασισμένοι σε πλέγμα είναι σχετικά απλοί, αποδοτικοί και εξαιρετικά παράλληλοι. Επίσης, η ασφάλεια ορισμένων συστημάτων που βασίζονται σε πλέγματα είναι αποδεδειγμένα ασφαλής κάτω από μια χειρότερη υπόθεση σκλήρηνσης, και όχι στη μέση περίπτωση. Από την άλλη πλευρά, έχει αποδειχθεί δύσκολο να δοθούν ακριβείς εκτιμήσεις της ασφάλειας

των σχημάτων πλέγματος με ακόμη γνωστές τεχνικές κρυπτοανάλυσης.

Όπως γνωρίζουμε η κρυπτογραφία βασιζόμενη σε πλέγματα εισήχθη σε δύο μορφές ανεξάρτητα σε δύο διαφορετικές πτυχές τα μαθηματικά και την επιστήμη των υπολογιστών περίπου πρίν από δύο δεκαετίες. Σήμερα, παίρνει νέα προσοχή και από τις δύο κοινότητες καθώς είναι υποψήφια για την πιό ασφαλή λύση μετά την ολοκλήρωση της κρυπτογράφησης στον μετακβαντικό τομέα.

Κάνοντας μια μικρή παρένθεση στον τομέα την πληροφορικής αναφέρουμε το εξής.Η κοινότητα των μαθηματικών το 1996, με τους Jeffrey Hoffstein, Jill Pipher και Joseph Silverman εισήγαγαν την έννοια NTRU[37], η οποία μπορεί να ερμηνευτεί ως ένα σύστημα βασισμένο σε πλέγματα το οποίο είναι ιδιαίτερα αποτελεσματικό λόγω της περιγραφής του σε ένα ειδικό είδος δακτυλίου αριθμών. Στην επιστήμη των υπολογιστών περίπου την ίδια εποχή ο, Miklós Ajtai και Cynthia Dwork εισήγαγε μια λύση για κρυπτογράφηση με δημόσιο κλειδί σχετικά με τη σκληρότητα ορισμένων γνωστών προβλημάτων πλέγματος SVP .2 Ένα πλέγμα πιο συγκεκριμένα είναι ένας γραμμικός χώρος που δημιουργείται από μια επιλογή φορέων βάσης. Κάποιος μπορεί να το φανταστεί στον Ευκλείδειο χώρο, όπου είναι τυχαίο ορίζεται ως το σύνολο των γραμμικά ανεξάρτητων διανυσμάτων. Το πλέγμα αποτελείται από όλα τα σημεία που είναι γραμμικοί συνδυασμοί σε αυτούς τους φορείς.

Δεδομένης μιας αυθαίρετης βάσης με πολύ μεγάλα διανύσματα σε πολύ μεγάλες διαστάσεις, για εύρεση του συντομότερου φορέα το πλέγμα είναι ένα δύσκολο πρόβλημα. Οι πιο γνωστοί αλγόριθμοι για την επίλυση του SVP εκτελούνται σε εκθετικό χρόνο σε n, με τη διάσταση του πλέγματος. Πολύ γνωστοί αλγόριθμοι πολυωνυμικού χρόνου μπορεί να βρούν κατά προσέγγιση λύσεις, σχετικά με τον λόγο του μήκους του κατά προσέγγιση φορέα και με το μήκος του μικρότερου διανύσματος να είναι εκθετικά κακό.

Σύμφωνα με το άρθρο με όνομα "Cryptography Based Lattice" των Daniele Micciancio τον Oded Regev σχετικά με την κρυπτογραφία βάσει πλέγματος, που καλύπτει την ιστορία και θεωρία της,παρέχεται μια συνοπτική περιγραφή σχετικά με πρόσφατες, και πολλές εξελίξεις που αφορούν την κρυπτογραφία που βασιζεται στα πλέγματα ως την πρώτη γραμμή τους. Συγκεκριμένα:

- Πρώτον,αναφέρει ότι η έλευση των κβαντικών υπολογιστών έχει ωθήσει την

κρυπτογραφική κοινότητα να ασχολείται με postquantum κρυπτογραφία καθώς πλέον οι υπολογιστές αυτοί μπορούν να καταρρίψουν κάθε προηγούμενο αλγόριθμο που ως τώρα θεωρείτο ασφαλείς. Μέχρι τώρα, οι λύσεις που βασίζονται σε πλέγματα δεν είναι γνωστό ότι είναι ευάλωτες σε κβαντικές επιθέσεις πολυώνυμου χρόνου, ωστόσο,ανάλογα με την υποκείμενη ασφάλεια,οι κβαντικές επιθέσεις σε συστήματα που βασίζονται σε πλέγματα μπορεί να είναι δυνατές.

- Δεύτερον, λύσεις στην ομομορφική κρυπτογράφηση με βάση τα πλέγματα μπορεί να έχουν σημαντικές πρακτικές εφαρμογές για την εξωτερική ανάθεση ιδιωτικών υπολογισμών στο σύννεφο.
- Τέλος, ενσωματώνονται αποτελεσματικά συστήματα βασισμένα σε πλέγματα αριθμητικών θεωρητικών κατασκευών, όπως οι αριθμητικοί δακτύλιοι, που έχουν αποδειχθεί ότι είναι αποδεδειγμένα ασφαλείς με την έννοια που υιοθετήθηκε από την κρυπτογραφική κοινότητα.

Δηλαδή, μία μπορούν να αποδείξουν μειώσεις ασφαλείας για να μειώσουν το πιθανό «σπάσιμο» τους σε συστήματα για την επίλυση προβλημάτων σκληρού πλέγματος που σχετίζονται με το SVP ή το πρόβλημα κοντινότερου διανύσματος.

Η ιδέα πίσω από τα σκληρά προβλήματα για την οποία χρησιμοποιήθηκε η κρυπτογραφία βασισμένη σε πλέγμα είναι αυτή που προσθέτει αρκετό θόρυβο σε ένα διάνυσμα εσωτερικών προϊόντων ενός τυχαίου μυστικού φορέα.

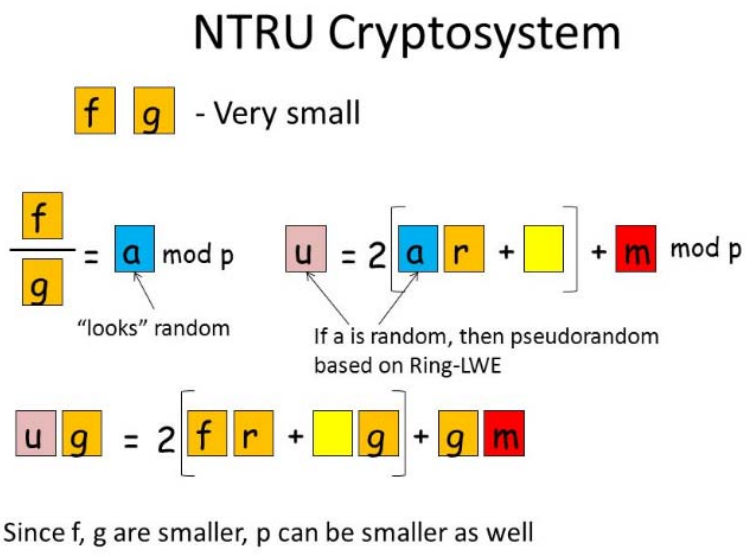
Οι φορείς αυτοί δημιουργούν ένα πρόβλημα αποκωδικοποίησης το οποίο από μόνο του είναι ένα δύσκολο γεγονός. Για να κρυπτογραφήσει ένα μήνυμα, ο αποστολέας το κωδικοποιεί ως διανυσματικός χώρος στο χώρο του πλανήτη, και στην συνέχεια ουσιαστικά το τυφλώνει με την προσθήκη ενός φορέα τυχαίων εσωτερικών προϊόντων με το μυστικό του vector. Στη συνέχεια προσθέτει ένα μικρό διάνυσμα σφάλματος.

Το τυχαίο με τα εσωτερικά προϊόντα με το μυστικό διάνυσμα του αποστολέα είναι μια μορφή τυχαίας τυφλοποίησης για το μήνυμα όπου δηλαδή,η τύφλωση είναι διαφορετική κάθε φορά που ο αποστολέας κρυπτογραφεί. Το προστιθέμενο σφάλμα καθιστά το πρόβλημα ασαφές έτσι ένας εισβολέας δεν μπορεί να χρησιμοποιήσει γραμμική άλγεβρα και πολλά δείγματα κρυπτογράφησης για να ανακαλύψει το μυστικό κλειδί. Αυτή η ασφάλεια του συστήματος κρυπτογράφησης βασίζεται στη σκληρότητα της μάθησης με λάθη LWE, που παρουσιάστηκε από τον Regev.7 Είναι

σχετικό με το πρόβλημα αποκωδικοποίησης που χρησιμοποιείται ως βάση για τον κώδικα κρυπτογράφησης[38,39]. Στην πραγματικότητα, οι μειώσεις ασφαλείας περιλαμβάνουν μειώσεις στο πρόβλημα οριοθετημένης απόστασης αποκωδικοποίησης. Πολλές παραλλαγές αυτής της βασικής ιδέας επιτρέπουν την κρυπτογράφηση, με υπογραφές και άλλα κρυπτογραφικά δομικά στοιχεία όπου ο υποκείμενος χώρος διανύσματος μπορεί να αλλάξει και να δομηθεί προσθέτοντας, για παράδειγμα, τη χρήση ενός διανυσματικού χώρου που έρχεται από έναν πολυωνυμικό δακτύλιο στη θεωρία αριθμών του RLWE8.

Η κατανομή σφαλμάτων που χρησιμοποιείται για τα τυχαία σφάλματα που προστίθενται είναι επίσης εξαιρετικά σημαντική για την ασφάλεια του συστήματος. Το βασικό σημείο είναι η αναλογία του μεγέθους του θορύβου προς το μέγεθος του συνολικού προβλήματος. Η αποκρυπτογράφηση είναι δυνατή εάν υπάρχει μία σχετική γνώση αυτού του μυστικού συνδυασμού, επειδή τα τυχαία εσωτερικά προϊόντα μπορεί να αφαιρεθούν από το κρυπτογράφημα και τα σφάλματα στρογγυλοποιήθηκαν για να ληφθεί το αρχικό μήνυμα.

Σχετική τυποποίηση της κρυπτογράφησης πλέγματος με βάση το NIST:
Παρόλο που το NTRU έχει τυποποιηθεί, πιο πρόσφατα από κρυπτοσυστήματα που βασίζονται σε πλέγματα δεν έχει ακόμη προταθεί κάποια συγκεκριμένη τυποποίηση. Πιθανότατα να εξεταστεί το γεγονός αυτό σε κάποιο επερχόμενο διαγωνισμό του NIST αφού αποτελεί και ο σχετικά αρμόδιος φορέας. Από όσο γνωρίζουμε στον NIST έχουν υποβληθεί κάποιες υποβολές που σχετίζονται με την τυποποίηση αυτή τον Νοέμβριο του 2017. Ως μέρος αυτής της διαδικασίας, ο υποκείμενος μηχανισμός κρυπτογράφησης για ομομορφική κρυπτογράφηση θα πρέπει να είναι τυποποιημένος,[40] καθώς θα αποτελεί ένα πολύ σημαντικό βήμα προς την υποστήριξη της κοινότητας των εφαρμογών.



Εικόνα 3.2 : Κρυπτοσύστημα NTRU (Γενικός Ορισμός)

Το κρυπτοσύστημα δημόσιου κλειδιού NTRU Encrypt έχει καλά χαρακτηριστικά απόδοσης όσον αφορά την ταχύτητα και την χαμηλή δεύσμευση μνήμης, έτσι ώστε να μπορεί να χρησιμοποιηθεί σε εφαρμογές σε κινητές συσκευές και έξυπνες κάρτες. Το 2008,το NTRU τυποποιήθηκε στο IEEE P1363.1 (doi: 10.1109/IEEESTD.2009.4800404), και το 2011, το NTRUEncrypt τυποποιήθηκε στο X9.98 για πιο εύκολη χρήση στις οικονομικές βιομηχανίες των υπηρεσιών. Η έρευνα κβαντικού αλγορίθμου είναι ένα εξαιρετικά τεχνικό θέμα στο οποίο προσφέρει σημαντικές νέες αλγοριθμικές τεχνικές που έχουν αναπτυχθεί μόνο μία ή δύο φορές ανά δεκαετία. Κάποιες από τις πιο πρόσφατες εξελίξεις είναι ένας κβαντικός αλγόριθμος για το βασικό ιδανικό πρόβλημα, το οποίο έχει εφαρμογές σε κρυπτογραφία βασισμένη σε πλέγματα.[42] Κάποιες νέες μέθοδοι που προέκυψαν μα βάση αυτό το κρυπτοσύστημα είναι για την επίλυση διακριτών προβλημάτων βελτιστοποίησης στους κβαντικούς υπολογιστές και ονομάζεται Quantum Approximate, δηλαδή Αλγόριθμος βελτιστοποίησης (QAOA) αλλά και για την λύση εκθετικά μεγάλων συστήματων γραμμικών εξισώσεων υπό ορισμένες συνθήκες που ονομάζονται Harrow-Hassidim δηλαδή Αλγόριθμος Lloyd (HHL). [41]

Παρόλα αυτά δεν είναι ακόμη σαφές αν υπάρχουν, βέβαια συνέπειες αυτών των πρωτόγονων κρυπτοσυστημάτων σε επίπεδο μετακβαντικής κρυπτανλάλυσης.

Έχουν γίνει πολλές προσπάθειες για την ανάπτυξη κβαντικών αλγορίθμων για την

εύρεση βραχέων διανυσμάτων μεγάλης διαστάσεως σε πλέγματα. Από νωρίς, οι ερευνητές σημείωσαν μια σειρά από εντυπωσιακές συνδέσεις μεταξύ των μαθηματικών μεθόδων που χρησιμοποιούνται στην κρυπτογραφία με βάση πλέγματα και εκείνες που χρησιμοποιούνται στην κρυπτογράφηση των κβαντικών αλγορίθμων. Συγκεκριμένα, υπάρχουν πολλές αποδείξεις ότι παρέχουν ασφάλεια τα κρυπτοσυστήματα που είναι βασισμένα σε πλέγματα και κάνουν χρήση τυχαίων δειγμάτων από ορισμένες περιοδικές κατανομές n-διαστάσεων Euclidean στον χώρο καθώς ακόμα και το Fourier μετασχηματίζει αυτές τις περιοδικές κατανομές. Θα μπορούσε να υπάρξει ένας τρόπος χρήσης του μετασχηματισμού του κβαντικού Fourier για να προετοιμάσει έτσι τις αντίστοιχες καταστάσεις κβαντικής υπέρθεσης σε αυτές τις διανομές; Αυτές οι καταστάσεις υπέρθεσης,που μερικές φορές ονομάζονται "κβαντικά δείγματα", περιέχουν περισσότερες πληροφορίες από τα κλασσικά τυχαία δείγματα και θα μπορούσαν να χρησιμοποιηθούν για την επίλυση προβλημάτων πλέγματος.

Στην πραγματικότητα, αυτή η γραμμή σκέψης δεν οδήγησε στους κβαντικούς αλγορίθμους για προβλήματα πλέγματος, Αλλά αντ 'αυτού, αυτή η ιδέα ήταν που χρησιμοποίησε ο Oded Regev για να αποδείξει μία από τις ισχυρότερες εγγυήσεις για την κρυπτογραφία που είναι βασισμένη σε πλέγματα.

Συγκεκριμένα,ο Regev έδειξε ότι σπάζοντας ένα ορισμένο δημόσιο κλειδί τότε το σύστημα κρυπτογράφησης είναι τουλάχιστον τόσο δύσκολο όσο η επίλυση ενός αδύνατου προβλήματος πλέγματος σε έναν κβαντικό υπολογιστή.

Και έτσι σε αυτή την περίπτωση, μια τεχνική που είχε αρχικά προβλεφθεί στην κβαντική κρυπτανάλυση χρησιμοποιήθηκε τελικά για την παροχή απόδειξης σε ένα κρυπτοσύστημα που είναι πραγματικά ασφαλές.

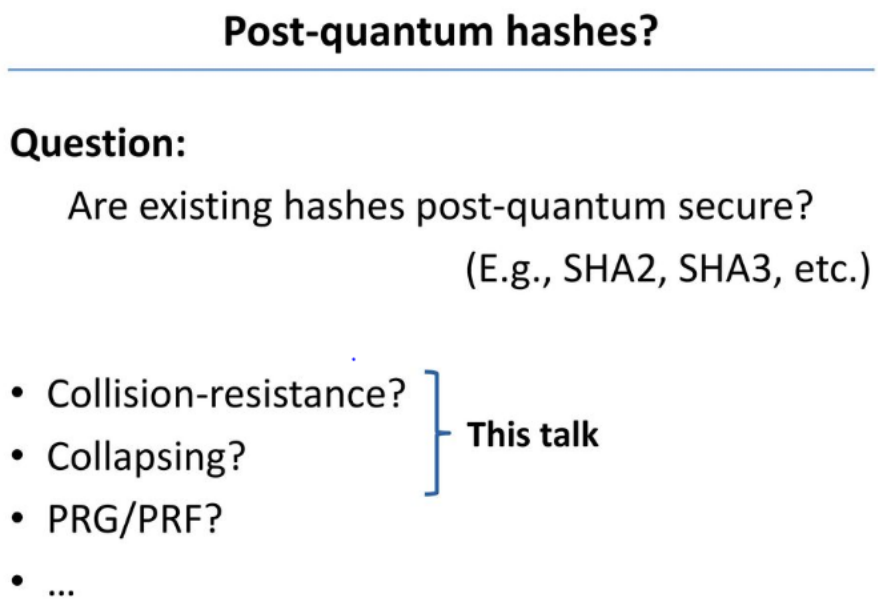
Πιο πρόσφατα, ωστόσο, σημειώθηκε μεγαλύτερη πρόοδος από την πλευρά της κβαντικής κρυπτανάλυση αφού έχει σημειωθεί πρόοδος στην ανάπτυξη κβαντικών αλγορίθμων για την επίλυση προβλημάτων που εμπλέκονται σε πλέγματα που έχουν αλγεβρική δομή. Δηλαδή σχάρες με αλγεβρική δομή χρησιμοποιούνται συχνά στην κρυπτογραφία, καθώς έχουν πιο συμπαγή περιγραφές από τα γενικά πλέγματα. Αυτό κάνει τα πιο αποτελεσματικά κρυπτοσυστήματα. Πρόσφατα, οι ερευνητές έχουν ανακαλύψει αποτελεσματικούς κβαντικους αλγόριθμους για την εύρεση βραχέων γεννητριών ορισμένων από τα κυριότερα ιδανικά σε κυκλωτοσωματικούς δακτυλίους.

Αυτοί οι κβαντικοί αλγόριθμοι επιδεικνύουν μια εκθετική επιτάχυνση των ταχύτερων κλασσικών αλγορίθμων καθώς και μια αδυναμία ασφάλειας ορισμένων αλγεβρικά δομημένων πλεγμάτων σε σύγκριση με τα γενικά σύνολα. Συγκεκριμένα, αυτοί οι κβαντικοί αλγόριθμοι διασπούν ορισμένα κρυπτοσυστήματα που χρησιμοποιούν τα κύρια ιδεατά πλέγματα με ασυνήθιστα μικρές γεννήτριες όπως είναι για παράδειγμα το SOLILOQUY, αλλά και ορισμένοι υποψήφιοι κατασκευαστές πολυεθνικών χάρτων. [40]

Άλλα κρυπτοσυστήματα με βάση τα ιδανικά πλέγματα είναι το NTRU Encrypt και το ring-LWE δηλαδή την μάθηση με σφάλματα, που δεν είναι ότι διασπάται από οποιονδήποτε σήμερα γνωστό κβαντικό αλγόριθμο.Η υποκείμενη τεχνική που χρησιμοποιείται σε αυτούς τους μετακβαντικούς αλγόριθμους αφορά την εύρεση περιόδου σε μια συνεχή και όχι διακριτή. Για συνεχείς λειτουργίκούς τομείς, όπως οι πραγματικοί αριθμοί, το πρόβλημα της εύρεσης κατά προσέγγιση περιοδικοτήτων γίνεται πιο λεπτό. Παρ 'όλα αυτά, οι κβαντικοί αλγόριθμοι έχουν ανακαλυφθεί ότι επιτυγχάνουν εκθετική επιτάχυνση σε κλασικούς αλγορίθμους για αυτό το έργο. Αυτό με τη σειρά του οδηγεί σε αλγόριθμους κβαντικού πολυωνυμικού χρόνου για διάφορους αριθμούς σε θεωρητικά προβλήματα, όπως η επίλυση της εξίσωσης Pell, ή τον εντοπισμό γεννητριών σε βασικούς ιδεώδεις υπολογιστές σε ομάδες τάξεων και σε ομάδες μονάδων αλγεβρικού αριθμού των πεδίων, αλλά και του χρόνου πολυώνυμων του βαθμού των αριθμών.

Μελετώντας την υποκατηγορία των πλεγμάτων είναι εύλογο να αντιληφθεί κάποιος ότι ουσιαστικά τα πλέγματα πρόκειται για μια πολύ νέο εμφανιζόμενη κατηγορία στην οποία όμως θα πρέπει να δωθεί ιδιαίτερη έμφαση τόσο από φυσικομαθηματικής άποψης αλλά και υπολογιστικής-τεχονολογικής μορφής. Οι δυνατότητες οι οποίες προσφέρονται στον τομέα της μετακβαντικής κρυπτογράφησης από τα πλέγματα είναι πραγματικά πολύ μεγάλες κάνοντας την κατηγορία αυτή πολύ υποσχομένη για τον σχεδιασμό ή ακόμα και την εξέλιξη κρυπτοσυστημάτων που θα είναι αρκετά ισχυρά έναντι σε επιθέσεις κβαντικών υπολογιστών.

3.4 Συναρτήσεις Κατακερματισμού



Εικόνα 3.3: Υπάρχουν συναρτήσεις Κατακερματισμού με αντοχές στην εμφάνιση του Μετακβαντικού Κόσμου

Από μόνης της η πιο πάνω εικόνα τέθει ένα πολύ σημαντικό ερώτημα. Ένα ερώτημα που αν γινόταν κάτω από τις υπάρχουσες συνθήκες έως σήμερα και φυσικά θα καταρριπτόταν αμέσως. Μέχρι σήμερα οι συναρτήσεις κατακερματισμού αποτελούν ένα πολύ σημαντικό και αξιόλογο μέτρο γενικής ασφάλισης σε όλους τους τομείς ανάμεσα τους βέβαια και η οικογένεια της κρυπτογραφίας. Τί γίνεται όμως όταν στον κόσμο μας τεθεί για τα καλά η χρήση των κβαντικών υπολογιστών; Υπάρχει ζωή και για μετά την έλευση των κβαντικών υπολογιστών;

Τα πιο πάνω βέβαια ερωτήματα αναλύονται και απαντώνται στην συνέχεια του υποκεφαλαίου αυτού που αφορά τις συναρτήσεις κατακερματισμού στον μετακβαντικό κόσμο.

Η συνάρτηση κατακερματισμού που είναι γνωστή και ως συνάρτηση διασποράς αλλά και κατατεμαχισμού ορίζεται ως μια μαθηματική συνάρτηση που λειτουργεί εισάγοντας μια ομάδα δεδομένων και εξάγοντας μια στοιχειο σειρά η οποία έχει μέγεθος πολύ

μικρότερο από την είσοδο. Συνήθως από την συνάρτηση αυτή εξάγεται ένας ακέραιος αριθμός και μπορεί να χρησιμοποιηθεί ακόμα και ως δείκτης σε κάποιο πίνακα. [44]

Η συνάρτηση κατακερματισμού μπορεί να αντιστοιχίζει δύο και περισσότερες εισόδους στο Hash Value.

Η κρυπτογραφία με βάση το Hash (Συναρτήσεις Κατακερματισμού) είναι ο γενικός όρος για τις κατασκευές κρυπτογραφικών πρωτόγονων που βασίζονται στην ασφάλεια των λειτουργιών κατακερματισμού. Είναι ενδιαφέρον ως ένας τύπος μετάκβαντικής κρυπτογράφησης αφού με τις κατάλληλες μετατροπές μπορεί να λειτουργήσει ιδιαίτερα αποτελεσματικά.

Οι υπογραφές που βασίζονται στο Hash είναι ψηφιακές υπογραφές που κατασκευάζονται με λειτουργίες κατακερματισμού. Η ασφάλεια τους, ακόμη και εναντίον κβαντικών επιθέσεων, είναι κατανοητή. Πολλά από τα πιο αποδοτικά συστήματα υπογραφής που βασίζονται σε κατακερματισμό έχουν το μειονέκτημα ότι ο υπογράφων πρέπει να τηρεί αρχείο με τον ακριβή αριθμό μηνυμάτων που έχουν υπογραφεί προηγουμένως και κάθε λάθος σε αυτό το αρχείο θα έχει ως αποτέλεσμα την ανασφάλεια. Ένα άλλο μειονέκτημα είναι ότι μπορούν να παράγουν μόνο έναν περιορισμένο αριθμό υπογραφών. Ο αριθμός των υπογραφών μπορεί να αυξηθεί, ακόμη και στο σημείο να είναι πραγματικά απεριόριστος, αλλά αυτό αυξάνει και το μέγεθος της υπογραφής.[45]

Μέχρι στιγμής, η κρυπτογραφία με την χρήση συναρτήσεων κατακερματισμού περιορίζεται σε συστήματα ψηφιακών υπογραφών, όπως η συνάρτηση ψηφιακής υπογραφής Merkle.Οι ψηφιακές υπογραφές που είναι βασισμένες στο Hash συνδυάζουν ένα σχήμα υπογραφής ενός χρόνου με μια δομή του συστήματος Merkle. Δεδομένου ότι ένα κλειδί ενός χρόνου υπογραφής μπορεί να υπογράψει με ασφάλεια μόνο ένα μήνυμα, είναι πρακτικό να γίνει συνδυασμός πολλών τέτοιων κλειδιών μέσα σε μια ενιαία, μεγαλύτερη δομή. Μια δομή του σχεδιασμού του Merkle χρησιμοποιείται για το σκοπό αυτό. Σε αυτήν την ιεραρχική δομή δεδομένων, μια συνάρτηση κατακερματισμού και ο τρόπος που προσκολλάται χρησιμοποιούνται επανειλημμένα για τον υπολογισμό κόμβων δέντρων. Οι υπογραφές Lamport είναι ένα παράδειγμα ενός συστήματος υπογραφής ενός χρόνου που μπορεί να συνδυαστεί με μια δομή τύπου Merkle.

Αναφορά στην συνέχεια του υποκεφαλαίου αξίζει να γίνει κυρίως στον Ralph Merkle που εφηύρε υπογραφές που βασίζονται σε συναρτήσεις κατακερματισμού το 1979. Τα συστήματα υπογραφής XMSS (eXtended Merkle Signature Scheme) και SPHINCS εισήχθησαν το 2011 και το 2015 αντίστοιχα. Το XMSS βασίζεται τόσο στο σπερματικό σχήμα του Merkle όσο και στο γενικό πρόγραμμα υπογραφής Merkle GMSS του 2007 . Μια παραλλαγή πολλαπλών δέντρων του XMSS, XMSSMT, περιγράφηκε το 2013.[47]

Οι ψηφιακές υπογραφές έχουν γίνει μια βασική τεχνολογία για την κατασκευή τόσο του Διαδικτύου αλλά και άλλων υποδομών πληροφορικής ασφάλειας. Οι ψηφιακές υπογραφές παρέχουν αυθεντικότητα, ακεραιότητα και τη μη άρνηση των δεδομένων. Οι ψηφιακές υπογραφές χρησιμοποιούνται ευρέως στα πρωτόκολλα ταυτοποίησης και ελέγχου ταυτότητας. Ως εκ τούτου, η ύπαρξη ασφαλών αλγορίθμων ψηφιακής υπογραφής είναι κρίσιμοι για τη διατήρηση της ασφάλειας των ΤΠ.

Οι αλγόριθμοι ψηφιακής υπογραφής που χρησιμοποιούνται στην πράξη σήμερα είναι ο RSA, ο DSA και ο ECDSA. Δεν είναι κβαντική ανοσία που από τώρα χωρίς να τεθούν σε εφαρμογή οι κβαντικοί υπολογιστές η ασφάλεια τους βασίζεται στη δυσκολία του factoring μεγάλων σύνθετων ακεραίων και υπολογιστών σεδιακριτό λογάριθμο. Αλλά αποτελούν αρκετά καινοτόμοι σχεδιασμοί με ένα λαμπρό μέλλον.

Μελλοντικοί όμως σχεδιασμοί ψηφιακών υπογραφών που παρουσιάζονται σε αυτό το κεφάλαιο προσφέρουν μια πολύ ενδιαφέρουσα εναλλακτική λύση. Όπως κάθε άλλος σχέδιασμός ψηφιακής υπογραφής,τα συστήματα υπολογισμού ψηφιακής υπογραφής που βασίζονται σε κατακερματισμό χρησιμοποιούν κρυπτογραφική λειτουργία κατακερματισμού. Η ασφάλεια τους βασίζεται στην αντίσταση σύγκρουσης αυτής της συνάρτησης κατακερματισμού. Στην πραγματικότητα,τα σημερινά συστήματα ψηφιακής υπογραφής που βασίζονται σε κατακερματισμούς είναι ασφαλή εάν και μόνο εάν η υποκείμενη λειτουργία κατακερματισμού είναι ανθεκτική στη σύγκρουση. Η ύπαρξη ανθεκτικών σε σύγκρουση λειτουργίών κατακερματισμού μπορούν να θεωρηθούν ως μια ελάχιστη απαίτηση για την ύπαρξη ενός σχεδίου ψηφιακής υπογραφής που μπορεί να υπογράψει πολλά έγγραφα με ένα ιδιωτικό κλειδί. Αυτό το σύστημα υπογραφής χαρτώνει έγγραφα που είναι αυθαίρετα σε χορδές μεγάλου αριθμού δυαδικών ψηφίων στις ψηφιακές υπογραφές σταθερού μήκους. Αυτό δείχνει ότι η ψηφιακή υπογραφή των αλγόριθμων είναι στην πραγματικότητα λειτουργίες κατακερματισμού.

Όσο αφορά την ανθεκτικότητα των λογαρίθμων αυτών εάν ήταν δυνατή η κατασκευή δύο εγγράφων με την ίδια ψηφιακή υπογραφή,τότε το σύστημα υπογραφής δεν θα μπορούσε πλέον να θεωρηθεί ασφαλές. Αυτό το επιχείρημα δείχνει ότι υπάρχουν χάρτες ψηφιακής υπογραφής που βασίζονται σε κατακερματισμό καθώς υπάρχει κάποιο σχέδιο ψηφιακής υπογραφής που μπορεί να υπογράψει πολλά έγγραφα χρησιμοποιώντας ένα ιδιωτικό κλειδί. Κατά συνέπεια, τα συστήματα υπογραφής βάση κατακερματισμού είναι οι σημαντικότεροι υποψήφιοι υπογράφοντες στις ίδιες τις υπογραφές τους. Αν και δεν υπάρχει απόδειξη της αντοχής των κβαντικών υπολογιστών τους, οι απαιτήσεις ασφαλείας τους είναι ελάχιστες. Επίσης, κάθε νέα κρυπτογραφική συνάρτηση κατακερματισμού αποδίδει μια νέα hash-based υπογραφή. Επομένως, η κατασκευή ασφαλών συστημάτων υπογραφής αποτελεί ανεξάρτητο γεγονός από τα σκληρά αλγοριθμικά προβλήματα της θεωρίας αριθμών ή της άλγεβρας. Αυτό οδηγεί σε ένα άλλο μεγάλο πλεονέκτημα των υπογραφών που βασίζονται σε κατακερματισμό. Η υποκείμενη λειτουργία κατακερματισμού μπορεί να επιλεγεί λόγω των διαθέσιμων πόρων υλικού και λογισμικού.

Ένα παράδειγμα είναι όταν το σύστημα υπογραφής πρόκειται να εφαρμοστεί σε ένα τσιπ που ήδη υλοποιείται σε AES, μπορεί να χρησιμοποιηθεί μια λειτουργία κατακερματισμού βάσει AES, μειώνοντας έτσι τον κώδικα του μέγεθους του σχήματος υπογραφής και βελτιστοποίησης του χρόνου λειτουργίας του.

Τα σχέδια υπογραφής βασισμένα στο Hash επινοήθηκαν από τον Ralph Merkle όπως και προαναφέραμε στην αρχή της ενότητας.[46]
Επομένως, τα συστήματα υπογραφής ενός χρόνου είναι πραγματικά τα περισσότερα των βασικών τύπων των συστημάτων ψηφιακής υπογραφής. Ωστόσο, έχουν ένα μεγάλο μειονέκτημα. Ένα ζευγάρι κλειδιών που αποτελείται από ένα κλειστό κλειδί υπογραφής και ένα κοινό κλειδί επαλήθευσης μπορεί να χρησιμοποιηθεί μόνο για υπογραφή και επαλήθευση ενός μόνο εγγράφου. Αυτό είναι ανεπαρκής για τις περισσότερες εφαρμογές. Ήταν η ιδέα του Merkle να χρησιμοποιεί ένα hash δέντρο που μειώνει την εγκυρότητα πολλών πλήκτρων επαλήθευσης μιας ώρας με βάση τα φύλλα του κατακερματισμού στην εγκυρότητα ενός δημόσιου κλειδιού της ρίζας του δένδρου κατακερματισμού.

Η αρχική κατασκευή του Merkle δεν ήταν αρκετά αποτελεσματική, ειδικότερα σε σύγκριση με το σχήμα υπογραφής RSA. Ωστόσο, στο μεταξύ, έχουν βρεθεί πολλές

βελτιώσεις. Τώρα οι υπογραφές που βασίζονται στο hash είναι περισσότερο υποσχόμενες ως εναλλακτική λύση στα σχήματα υπογραφής RSA και ελλειπτικής καμπύλης.

Συνάρτηση κατακερματισμού Lamport-Diffie και ανάλυση Ασφάλειας της.

Όπως προαναφέρθηκε στην αρχή της ενότητας αυτής ένα από τα συστήματα που μπορούν αντεπεξέλθουν επάξια στην εποχή της έλευσης των κβαντικών υπολογιστών είναι αυτό του Lamport-Diffie που αφορά την υπογραφή με βάση τον χρόνο.

Έστω ότι n είναι θετικός ακέραιος, η παράμετρος ασφαλείας του LD-OTS. Το LD-OTS χρησιμοποιεί μια λειτουργία μονής κατεύθυνσης και μια κρυπτογραφημένη συνάρτηση κατακερματισμού, για την δημιουργία ζευγών κλειδιών LD-OTS. Το κλειδί υπογραφής X του LD-OTS αποτελείται από 2n bit χορδές μήκους η που επιλέγονται ομοιόμορφα τυχαία. Στην συνέχεια ταυτοποιείται το LD-OTS κλειδί Υ

$$(\Upsilon = yn{-}1^{[0]}, yn{-}1^{[1]}, \ldots, y1^{[0]}, y1^{[1]}, y0^{[0]}, y0^{[1]}) \in \{0, 1\}^{(n,2n)},)$$

Επομένως, η παραγωγή κλειδιών LD-OTS απαιτεί 2η αξιολογήσεις της f. Η υπογραφή και τα κλειδιά επαλήθευσης είναι σειρές 2n bit μήκους n.
Ένα έγγραφο M ∈ {0, 1} * υπογράφεται με χρήση LD-OTS με ένα κλειδί υπογραφής X όπως στην Εξίσωση. Αυτή η υπογραφή είναι μια ακολουθία από χορδές δυαδικών ψηφίων n, κάθε μια από το μήκος n. Επιλέγονται ως συνάρτηση του μηνύματος digest d. Η συμβολοσειρά bit στην υπογραφή αυτή είναι xi [0] αν το i-bit στο d είναι 0 και xi [1], αλλιώς. Η υπογραφή δεν απαιτεί αξιολογήσεις του f. Το μήκος της υπογραφής είναι n2.
Επαλήθευση LD-OTS. Για να επαληθεύσουμε μια υπογραφή σ = (σn-1, ..., σ0) του M, ο επαληθευτής υπολογίζει το μήνυμα digest d = (dn-1, ..., d0). Τότε αυτή ελέγχει αν η εν λόγω υπογραφή επαληθεύεται απαιτώντας n αξιολογήσεις της f και υπολογίζει το αντίστοιχο κλειδί επαλήθευσης.[48]

Στην συνέχεια γίνεται επιλογή μιας παράμετρου ασφαλείας n ∈ N. Και K = K (n) να είναι α ως πεπερασμένο σύνολο παραμέτρων. Αφήνουμε το F ούτως ώστε

$$F = \{fk: \{0, 1\}^{n} \rightarrow \{0, 1\}^{n} \mid k \in K$$

να είναι μια οικογένεια λειτουργιών μονής κατεύθυνσης. Η γενιά κλειδιών του τροποποιημένου LD-OTS λειτουργεί ως εξής με βάση την είσοδο 1^n για μια παράμετρο ασφαλείας n ένα κλειδί k ∈ K (n) όπου επιλέγεται τυχαία με την ομοιόμορφη κατανομή. Στη συνέχεια χρησιμοποιείται LD-OTS με τη λειτουργία μονής κατεύθυνσης fk. Το κλειδί k περιλαμβάνεται στο δημόσιο κλειδί.

Μερικά Ψηφιακά υπογραφικά συστήματα με βάση το Hash 85 λειτουργούν με το M, όπου υπάρχει τουλάχιστον ένας δείκτης c έτσι ώστε m'c = 1-mc. Το AdvPre είναι επιτυχές εάν c = a, η οποία συμβαίνει με πιθανότητα τουλάχιστον 1 / 2n. Ως εκ τούτου, η πιθανότητα επιτυχίας για την εύρεση προκαταρκτικής εικόνας στο χρόνο

$$tow = t + tSig + tGen$$

είναι σε τουλάχιστον ε / 4n.

Ασφάλεια της Ψηφιακής Υπογραφής Merkle

Όπως ήδη γνωρίζουμε το σχήμα υπογραφής ενός χρόνου Lamport-Diffie είναι υπαρξιακά ανυπέρβλητο κάτω από μια επιθετική επιλεγμένη επίθεση μηνύματος CMA-secure στον χρόνο καθώς η χρησιμοποιούμενη λειτουργία μονής κατεύθυνσης είναι ανθεκτική στην πρόληψη. Τότε δείχνουμε ότι το στυλ υπογραφής του Merkle είναι ασφαλές με CMA, όσο χρησιμοποιείται η λειτουργία hash τότε είναι ανθεκτική στη σύγκρουση και το υποκείμενο σχέδιο υπογραφής ενός χρόνου είναι CMAsecure. Τέλος, υπολογίζουμε το επίπεδο ασφάλειας του συστήματος υπογραφής Merkle για ένα δεδομένο μήκος εξόδου n της συνάρτησης κατακερματισμού.

Στην συνέχεια πραγματοποιείται μια μικρή αλλαγή της ψηφιακής υπογραφής του Merkle προκυμένου να τροποποιηθεί η ασφάλεια η οποία παρέχεται.Συγκεκριμένα γίνεται μια επιλογή μιας παράμετρου ασφαλείας n ∈ N. Αφήνουμε το K = K (n) να είναι ένα πεπερασμένο σύνολο παραμέτρων. Και το

$$G = gk: \{0, 1\}^* \rightarrow \{0, 1\}^n \mid k \in K$$

είναι μια οικογένεια λειτουργιών κατακερματισμού. Η δημιουργία κλειδιών του τροποποιημένου MSS λειτουργεί ως εξής. Στην είσοδο 1n για μια παράμετρο ασφαλείας n επιλέγεται ένα κλειδί k ∈ K (n) τυχαία με την ομοιόμορφη κατανομή. Στη συνέχεια, το σχέδιο υπογραφής Merkle χρησιμοποιείται με τη συνάρτηση κατακερματισμού gk και

με κάποιο σχήμα υπογραφής ενός χρόνου. Η παράμετρος k περιλαμβάνεται στο δημόσιο κλειδί. Δείχνουμε ότι η υπαρξιακή αδυναμία αυτής της παραλλαγής MSS υπό μια επιθετική επιλεγμένη επίθεση μηνύματος μπορεί να μειωθεί στην αντοχή και στην σύγκρουση της οικογένειας G καθώς και στην υπαρξιακή αδυναμία του υποκείμενου με καθεστώς υπογραφής ενός χρόνου.[46]

Εξηγούμε στην συνέχεια πώς ένας υπαρξιακός πλαστογράφος για το σχέδιο υπογραφής Merkle μπορεί να χρησιμοποιηθεί για την κατασκευή ενός αντιπάλου που είναι είτε ένας υπαρξιακός πλαστογράφος για το ένα υποκείμενο σύστημα υπογραφής ενός χρόνου ή ένας ανιχνευτής σύγκρουσης για μια λειτουργία κατακερματισμού στο G. Η είσοδος του αντιπάλου είναι ένα σχήμα υπογραφής ενός χρόνου, ένα κλειδί k ∈ K που επιλέγονται τυχαία με την ομοιόμορφη κατανομή και το ύψος του δέντρου Merkle. Η είσοδος είναι επίσης ένα κλειδί επαλήθευσης YOTS και ένα υπογεγραμμένο OOTS όπου είναι ένα ζευγάρι κλειδιών του σχήματος μιας στιγμής υπογραφής.

Ο αντίπαλος επιτρέπεται να υποβάλλει μία ερώτηση στο OOTS του μαντείου (XOTS). Στόχος μας είναι να προκαλέσει μια σύγκρουση για τη συνάρτηση κατακερματισμού gk ή ένα υπαρκτό πλαστό (M ', σ') για το καθεστώς υπογραφής ενός χρόνου που μπορεί να επαληθευτεί χρησιμοποιώντας την επαλήθευση ως κλειδί YOTS. Έχει πρόσβαση σε ένα προσαρμοσμένο επιλεγμένο μήνυμα forger ForO για το MSS με συνάρτηση κατακερματισμού gk και ύψος δέντρου H. Επιτρέπεται ο πλαστογράφος να ζητήσει ερωτήματα 2H στην υπογραφή του μαντείου. Ο αντίπαλος υποτίθεται ότι υποδύεται αυτό το μαντείο.

Ο αντίπαλος επιλέγει τυχαία με την ομοιόμορφη κατανομή ένα δείκτη c στο σύνολο {0,. . . , 2H-1}. Δημιουργεί ένα ζευγάρι κλειδιών Merkle με τον συνήθη τρόπο με την μόνη εξαίρεση ότι, όπως το κλειδί επαλήθευσης ενός έτους, το κλειδί επαλήθευσης μιας ώρας YOTS από την είσοδο χρησιμοποιείται. Τότε ο αντίπαλος επικαλείται το προσαρμοστικό επιλεγμένο παραχαραγμένο μήνυμα για το σχέδιο Merkle με τη συνάρτηση κατακερματισμού gk και το δημόσιο Merkle κλειδί που δημιούργησε πριν. Χωρίς απώλεια , υποθέτουμε ότι ο πλαστογράφος αμφισβητεί το μαντείο 2 φορές. Οι απαντήσεις δίνονται από τον αντίπαλο. Όταν ο πλαστογράφος ζητήσει την υπογραφή i = c, τότε ο αντίπαλος παράγει αυτές τις υπογραφές χρησιμοποιώντας τα κλειδιά υπογραφής.

Ωστόσο, όταν ο πλαστογράφος ζητά την υπογραφή, όπου ο αντίπαλος διερωτάται το μαντείο OOTS . Ας υποθέσουμε ότι ο πλαστογράφος είναι (M ', (s, σ', Y ', A')) όπου το s είναι ο δείκτης του ζεύγους κλειδιών μιας χρήσης που χρησιμοποιείται για αυτήν την υπογραφή, σ 'είναι η μία φορά υπογραφή, Y 'είναι το κλειδί επαλήθευσης και το A' είναι η διαδρομή επαλήθευσης ταυτότητας. Εάν s = c και (Y, A) = (Y ', A') τότε ο αντίπαλος επιστρέφει (M ', σ'). και στην συνέχεια δείχνουμε ότι πρόκειται για υπαρξιακή πλαστογραφία του καθεστώτος υπογραφής ενός χρόνου με κλειδί επαλήθευσης YOTS. Δεδομένου ότι s = c έχουμε Y = Y '= YOTS. Έτσι, η επαλήθευση με το κλειδί στο μήνυμα που επιστρέφει ο πλαστογράφος είναι το ίδιο με το κλειδί επαλήθευσης που επιστρέφεται από το μαντείο όταν ερωτάται για τον πέμπτο χρόνο. Το ίδιο ισχύει για τη διαδρομή αυθεντικοποίησης. Αυτό σημαίνει ότι το μήνυμα M στο ερώτημα είναι διαφορετικό από το M '. Έτσι (M ', σ') είναι μια υπαρξιακή πλαστογραφία.

Αν (Y, A) A = (Y ', A') τότε ο αντίπαλος μπορεί να κατασκευάσει μια σύγκρουση για το hash function gk.

Αρχικά εξατάζουμε τη διαδρομή B = (B0 = gk (Y), B1, ..., BH) από το Y στο δέντρο Merkle μέχρι τη ρίζα του που κατασκευάστηκε χρησιμοποιώντας τη συνάρτηση κατακερματισμού gk και η διαδρομή αυθεντικοποίησης A = (A0, ..., AH-1). Συγκρίνουμε τη διαδρομή B '= (B'0 = gk (Y'), B'1, ..., B'H) από το Y 'στο δέντρο Merkle στη ρίζα του που κατασκευάστηκε χρησιμοποιώντας τη διαδρομή επαλήθευσης A '= (A'0, ..., A'H-1). Δεδομένου ότι το BH = B'H είναι το δημόσιο κλειδί MSS, υπάρχει ένας δείκτης 0 ≤ i <H με Bi + 1 = B'i + 1 και Bi2 = B'i. Με το Bi + 1 να είναι η τιμή κατακερματισμού της συνένωσης του Bi και Ai με την κατάλληλη σειρά, και δεδομένου ότι B'i + 1 είναι η τιμή κατακερματισμού του με τη σύζευξη του B'i και του A'i με την κατάλληλη σειρά, συναντάται μια σύγκρουση του gk.

Στη συνέχεια, υποθέτουμε ότι τα B και B 'είναι ίσα. Επομένως,

$$gk (Y) = B0 = B'0 = gk(Y ')$$

Ας υποθέσουμε ότι Ai = A'i για κάποιο δείκτη i <H. Δεδομένου ότι Bi + 1 είναι η τιμή κατακερματισμού της σύζευξης των Bï και Aï (με την κατάλληλη σειρά) και από το B'i + 1 είναι η τιμή κατακερματισμού της σύζευξης των B'i και A'i με την κατάλληλη σειρά ξανά μια σύγκρουση. Η σύγκρουση αυτή επιστρέφεται από τον αντίπαλο. Σε όλες τις

άλλες περιπτώσεις ο αντίπαλος επιστρέφει με αποτυχία.
Τώρα υπολογίζουμε την πιθανότητα επιτυχίας του αντιπάλου AdvCR, OTS.Επίσης, tGen, tSig και tVer υποδηλώνουν τους χρόνους που απαιτεί το MSS για το κλειδί με παραγωγή και δημιουργία υπογραφών για επαλήθευση και αντίστοιχα.
Αν (Y β ^{2}, Αβ ^{2}) = (Y, A), τότε ο αντίπαλος επιστρέφει μια σύγκρουση.Η πιθανότητα Η για την επιστροφή μιας σύγκρουσης στο χρόνο είναι :

$$tcr = t + 2H\,B \cdot tSig + tVer + tGen$$

Η πιθανότητα υπό όρους για την εξεύρεση υπαρξιακής πλαστογραφίας στο χρόνο είναι:

$$tots = t + 2H\,B \cdot tSig + tVer + tGen$$

Και από τις δύο περιπτώσεις, ένας από αυτούς συμβαίνει με πιθανότητα τουλάχιστον 1/2. **Έτσι έχουμε αποδείξει το θεώρημα ασφάλειας Merkle** με μικρές μετατροπές.
Αυτό το θεώρημα μας λέει ότι δεν υπάρχει κανένας αντίπαλος που να σπάει τη σύγκρουση με αντοχή της οικογένειας G σε χρόνο το πολύ tcr με πιθανότητα μεγαλύτερη από Η και δεν υπάρχει κανένας αντίπαλος που να είναι σε θέση να παράγει μια υπαρξιακή πλαστογραφία για το ένα σύστημα υπογραφής υπογραφής που χρησιμοποιείται σε MSS εγκαίρως σε περισσότερες περιπτώσεις με πιθανότητα μεγαλύτερη από το Η .[46]

Το 2019, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α. NIST ανακοίνωσε την πρόθεσή του να δημοσιεύσει πρότυπα για την κρατική κρυπτογράφηση με βάση το hash με βάση το XMSS και τις υπογραφές Leighton-Micali (LMS) που εφαρμόζονται σε διαφορετικές περιστάσεις. Περεταίρω ανάλυση σχετικά με το NIST και την μετακβαντική Κρυπτογραφία θα γίνει στο επόμενο κεφάλαιο.

3.5 Συναρτήσεις πολλών Μεταβλητών

Το 1994 ο Peter Shor έδειξε ότι οι κβαντικοί υπολογιστές μπορούν να λύσουν διάφορα προβλήματα σε πολυωνυμικό χρόνο. Επομένως, μόλις γίνουν μεγάλοι κβαντικοί υπολογιστές, όλα τα κρυπτοσυστήματα που βασίζονται σε τέτοιες υποθέσεις θα είναι ανασφαλής.

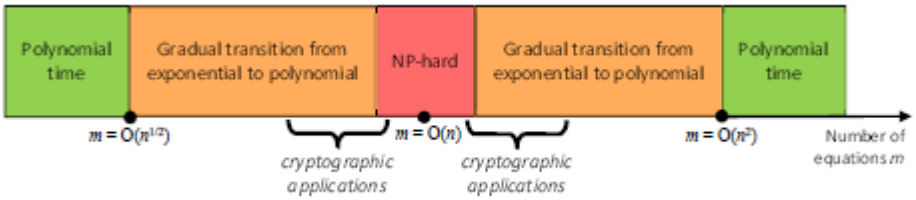
Ώς αντίμετρο της ένταξης της πληροφοριακής κοινωνίας στην εποχή των κβαντικών υπολογιστών δεν θα είναι βέβαια η παρεμπόδιση ένταξης της κβαντικής εποχής της κοινωνίας μας αλλά θα είναι η ελπίδα ότι η υποδομή μας δημόσιων κλειδιών μπορεί να παραμείνει άθικτη με τη χρήση νέων κβαντοανθεκτικών πρωτόγονων. Στον ακαδημαϊκό κόσμο, αυτό το νέο πεδίο έρευνας καλείται μετά την κρυπτογραφία.

Στην συνέχεια της ενότητας αυτής γίνεται εστίαση στην καλύτερη υπάρχουσα πολυπαραγοντική λειτουργία του κρυπτοσυστήματος δημόσιου κλειδιού (MPKC) για υπογραφές και κρυπτογράφηση. Αφού δωθεί μια γενική εικόνα της ασφάλειας των πολυπαραγοντικών συστημάτων και τονιστούν κάποια πλεονεκτήματα και μειονεκτήματα, θα γίνει και μια αναλυτικότερη ανάλυση κάποιων πολυπαραγοντικών συστημάτων και πιο συγκεκριμένα του συστήματος Rainbow.[53]

Τα πολυμεταβλητά κρυπτοσυστήματα βασίζονται στην σκληρότητα της επίλυσης ενός μη γραμμικού συστήματος που είναι πολυωνυμικό και πολυδιάστατο. Το πρόβλημα αυτό είναι γνωστό ότι είναι NP-Hard και παραμένει έτσι ακόμα και αν περιορίζεται σε ένα σύστημα πολλαπλών μεταβλητών με τετραγωνικές (MQ) εξισώσεις.

Η σκληρότητα του MQ εξαρτάται από την αναλογία μεταξύ του αριθμού των μεταβλητών n και του αριθμού των εξισώσεων m. Για ένα τυχαίο σύστημα εξισώσεων, το MQ είναι εκθετικό όταν m = O(n) ,αλλά γίνεται πολυωνυμικό όταν το όταν m = 0 (n2) ή πολύ ανεπαρκώς προσδιορισμένο δηλαδή όταν η = 0 (m2). Στο μεταξύ, μια σταδιακή μετάβαση συμβαίνει από την εκθετική πολυωνυμική πολυπλοκότητα.Για παράδειγμα, η πολυπλοκότητα της επίλυσης ενός συστήματος τετραγωνικών εξισώσεων πάνω από το GF(2) είναι υποεκθετική όταν το m / n τείνει στο άπειρο και το m / n2 τείνει στο μηδέν. Γενικά, τα σχήματα κρυπτογράφησης MQ χρησιμοποιούν ένα υπερπροσδιορισμένο

σύστημα εξισώσεων, έτσι n <m <n2, ενώ τα σχήματα υπογραφής MQ χρησιμοποιούν ένα υποδηέστερο σύστημα, έτσι m <n <m2.



Εικόνα 3.4 Πολυπλοκότητα του πολυμεταβλητού τετραγωνικού προβλήματος

Σχεδόν δεν υπάρχουν πολλά συστήματα πολλαπλών μεταβλητών, τα οποία έχουν τις χειρότερες περιπτώσεις μείωσης κατά μέσο όρο και πολύ λίγοι έχουν πλήρη ασφάλεια λόγω του γενικού προβλήματος NP-hard. Συνηθέστερα, υπάρχουν μειώσεις από το πρόβλημα της επίλυσης του προβλήματος με συγκεκριμένο τύπο μη τυχαίου συστήματος παγίδας που χρησιμοποιείται στο δημόσιο κλειδί ή υπό περιορισμένα μοντέλα επίθεσης. Συνεπώς, η ασφάλεια των περισσότερων συστημάτων πολλαπλών μεταβλητών εξαρτάται από εκτιμήσεις της υπολογιστικής δυσκολίας της επίλυσης των δημόσιων συστημάτων χρησιμοποιώντας τις πιο γνωστές πρακτικές επιθέσεις.

Μετά από τον αλγόριθμο Diffie-Hellman, οι κρυπτογράφοι πρότειναν πολλές λειτουργίες κρυπτογράφησης. Τα περισσότερα από αυτά ξεχάστηκαν και το RSA έγινε κυρίαρχο στην εποχή με τις απαιτήσεις που χρειάζονται έως τώρα. Οι πρώτες προτάσεις που δημοσιεύτηκαν σχετικά με το σύστημα των MPKCs των Shigeo Tsujii και Hideki Imai, φάνηκαν να έχουν προκύψει πρόσφατα στις εποχές που ζούμε. Όμως είναι ανεξάρτητα γνωστό ότι έχουν εργαστεί σχετικά με το θέμα αυτό στις αρχές της δεκαετίας του '80. Σίγουρα διαλέξεις δίνονται σε αυτό το θέμα όχι αργότερα από το 1983. Ωστόσο, για πολλά χρόνια, οι εργασίες τους δεν δημοσιεύθηκαν το 2004 οτιδήποτε άλλο εκτός από την Ιαπωνία, και παρέμεινε σε μεγάλο βαθμό άγνωστο έξω από την Ιαπωνία.[54]

Η κρυπτογραφία πολλαπλών μεταβλητών (Public Key) είναι η μελέτη των PKC όπου παρομοιάζεται με την λειτουργία ενός δρόμου με διασταύρωση που λαμβάνει τη μορφή ενός πολυμεταβλητού τετραγωνικού πολυωνύμου χάρτη πάνω από ένα πεπερασμένο πεδίο. Δηλαδή το δημόσιο κλειδί γενικά δίνεται από το a ενός συνόλου τετραγωνικών πολυωνύμων:

$$P = (p1\ (w1, ..., wn), ..., pm\ (w1, ..., wn)),$$

όπου κάθε pi είναι ένα μη γραμμικό πολυώνυμο **(w)** = (w1, ..., wn). Η αξιολόγηση αυτών των πολυωνύμων σε οποιαδήποτε δεδομένη τιμή αντιστοιχεί είτε στην διαδικασία κρυπτογράφησης ή τη διαδικασία επαλήθευσης. Αυτά τα PKC καλούνται πολυπαραγοντικά κρυπτοσυστήματα ενός δημόσιου κλειδιού εφεξής MPKC. Ανατρέποντας ένα πολυμεταβλητό τετραγωνικό χάρτη που ισοδυναμεί με την επίλυση ενός συνόλου τετραγωνικών εξισώσεων σε ένα πεπερασμένο πεδίο ή το ακόλουθο πρόβλημαMQ:
Επίλυση του συστήματος p1 (x) = p2 (x) = · · · = pm (x) = 0, όπου κάθε pi είναι τετραγωνικό σε x = (x1, ..., xn).
Όλοι οι συντελεστές και μεταβλητές είναι σε K = Fq, το πεδίο με q στοιχεία.
Το MQ είναι γενικά πρόβλημα NP-hard. Τέτοια προβλήματα πιστεύεται ότι είναι μια σκληρή εκτός αν η τάξη P ισούται με NP. Φυσικά, ένα τυχαίο σύνολο τετραγωνικών
οι εξισώσεις δεν θα είχαν διακλαδώσεις και επομένως δεν θα μπορούσαν να χρησιμοποιηθούν σε ένα MPKC.

Η αντίστοιχη μαθηματική δομή σε ένα σύστημα πολυώνυμων εξισώσεων,που δεν είναι απαραίτητα γενική, είναι το ιδανικό που παράγεται από αυτά τα πολυώνυμα.Έτσι, φιλοσοφικά, η πολυπαραγοντική κρυπτογραφία σχετίζεται με τα μαθηματικά που χειρίζεται πολυώνυμα ιδανικά, δηλαδή την αλγεβρική γεωμετρία.

Τα μαθηματικά που χρησιμοποιούν τα MPKC, αναπτύχθηκαν τον 20ό αιώνα.
Δεδομένου ότι δεν ασχολούμαστε πλέον πλέον με "τυχαία" ή "γενικά" συστήματα, αλλά όπου υπάρχουν συγκεκριμένοι trapdoors, η ασφάλεια των MPKC δεν είναι τότε εγγυημένη από την πυκνότητα NP του MQ, και μπορεί να υπάρχουν αποτελεσματικές επιθέσεις για οποιοδήποτε επιλεγμένο διαχωριστικό. Επομένως, η ιστορία των MPKC εξελίσσεται όπως καταλαβαίνουμε όλο και περισσότερο για το πώς να γίνει σχεδιασμός μια ασφαλών πολυπαραγοντικών καταπακτών.[54]

Η κατασκευή και οι συμβολισμοί των τυποποιημένων διπολικών

Ακόμα κι αν περιοριστούμε σε κρυπτοσυστήματα για τα οποία το δημόσιο κλειδί είναι ένα
σύνολο πολυώνυμων P = (p1, ..., pm) σε μεταβλητές w = (w1, ..., wn) όπου όλες οι

μεταβλητές και οι συντελεστές είναι σε K = Fq, και ο τρόπος απόκρυψης της θύρας δεν είναι μοναδικός ωστόσο, τα υπάρχοντα MPKC σχεδόν πάντα κρύβουν τον ιδιωτικό χάρτη Q μέσω σύνθεσης δύο συγγενικών χάρτων S, T.

$$P = T \circ Q \circ S: K^n \rightarrow K^m, \quad \text{ή}$$

$$P: w = (w1, ..., wn) \xrightarrow{S} x = M_S w + c_S \rightarrow \xrightarrow{Q} y \rightarrow \xrightarrow{T} z = M_T y + c_T = (z1, zm)$$

Σε κάθε δεδομένο σχήμα, ο κεντρικός χάρτης Q ανήκει σε μια συγκεκριμένη κατηγορία όπου οι τετραγωνικοί χάρτες των οποίων το αντίστροφο μπορεί να υπολογιστεί σχετικά εύκολα. Τα S, T είναι συγγενικά μερικές φορές ακόμα και γραμμικά μεταξύ τους ή και πλήρης. Τα xj ονομάζονται κεντρικές μεταβλητές. Τα πολυώνυμα που δίνουν yi στο x ονομάζονται κεντρικά πολυώνυμα. Οταν είναι απαραίτητο να γίνει διάκριση μεταξύ της μεταβλητής και της τιμής, θα το κάνουμε γράφοντας το yi = qi (x). Το κλειδί ενός MPKC είναι ο σχεδιασμός του κεντρικού χάρτη. Ακόμα το δημόσιο κλειδί αποτελείται από τα πολυώνυμα στην P. Στην πράξη, αυτό είναι πάντα μια συλλογή των συντελεστών των pi, που καταρτίζονται με κάποια τάξη ευνοϊκά σε εύκολο όμως υπολογισμό. Δεδομένου ότι κάνουμε κρυπτογράφηση δημόσιου κλειδιού, το P (0) θεωρείται πάντα ότι είναι μηδέν, επομένως τα δημόσια πολυώνυμα δεν έχουν σταθερούς όρους και το μυστικό κλειδί αποτελείται από τις πληροφορίες σε S, T, και Q. Δηλαδή, εμείς συλλέγουμε τα (M^{-1}_S, c_S), (M^{-1}_T, c_T) και οποιεσδήποτε παράμετρους υπάρχουν στο Q. Η θεωρία ενός c_S και c_T είναι ξένη αλλά το διατηρούμε ούτως ή άλλως. Για να επαληθεύσουμε μια υπογραφή ή για να κρυπτογραφήσουμε ένα μπλοκ, υπολογίζουμε απλώς το z = P (w). Στην συνέχεια για να υπογράψουμε ή να αποκρυπτογραφήσουμε ένα μπλοκ, υπολογίζουμε το $y = T^{-1}$ (z), το $x = Q^{-1}$ (y) και το w = S^{-1} (x) με τη σειρά του. Παρατηρούμε ότι αυτά μπορεί να είναι μόνο πολλά προγνωστικά, όχι απαραίτητα μια αντίστροφη λειτουργία με την αυστηρή έννοια της λέξης και συνοψίζουμε με διάφορες λειτουργικές λεπτομέρειες παρακάτω, ώστε ο αναγνώστης να έχει κάποια βασική αίσθηση περίπου πώς αυτά τα συστήματα μπορούν να εφαρμοστούν πρακτικά.

Ένα μεγάλο μειονέκτημα των MPKC είναι ότι τα κλειδιά τους είναι πολύ μεγάλο σε σύγκριση με τα παραδοσιακά συστήματα όπως το RSA ή το ECC. Για παράδειγμα, το μέγεθος του δημόσιου κλειδιού του RSA-2048 δεν είναι πολύ περισσότερο από 2048

bits, αλλά ένα ρεύμα έκδοσης του σχεδίου υπογραφής Rainbow έχει n = 42, m = 24, q = 256, δηλ. το μέγεθος του δημόσιου κλειδιού είναι 22680 bytes, πάνω από τα 16kB μνήμης flash που κάποια μικρά smartcards έχουν. Τα ιδιωτικά κλειδιά είναι μικρότερα, αλλά εξακολουθούν να είναι εντυπωσιακά με μικρές ενσωματωμένες συσκευές που έχουν περιορισμούς μνήμης. Όμως λειτουργούσε μονάδες με εκατοντάδες bits μακριά που είναι απαγορευτικά ακριβό για ενσωματωμένες συσκευές χωρίς συνεπεξεργαστή. Έτσι τα MPKC έχουν κάποια πλεονεκτήματα αντιστάθμισης και εξακολουθούν να έχουν πιθανότητες σε αυτά οι διάφορες συσκευές που τα χρησιμοποιούν.

Κβαντική ασφάλεια

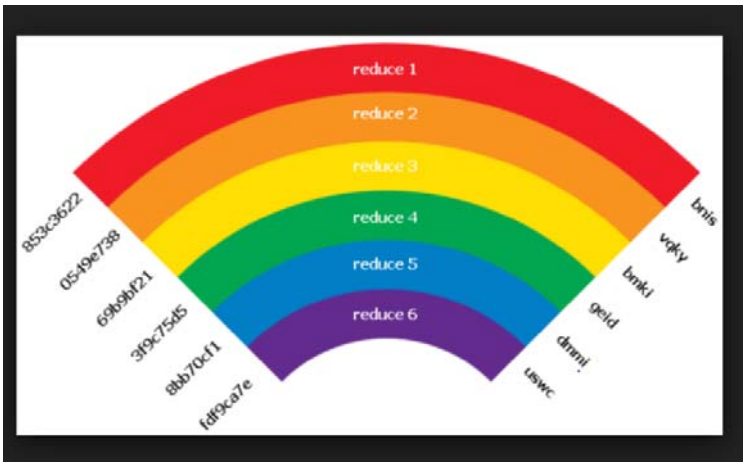
Η κλάση των προβλημάτων απόφασης που μπορούν να λυθούν οριστικά σε πολυωνυμικό χρόνο από έναν κβαντικό υπολογιστή με πιθανότητα τουλάχιστον 1/3 καλείται BQP. Υπάρχει υποψία ότι δεν υπάρχουν NP-complete προβλήματα στο BQP που σημαίνει ότι δεν υπάρχουν κβαντικοί αλγόριθμοι πολυωνυμικού χρόνου για την επίλυση προβλημάτων MQ. Πράγματι, φαίνεται ότι δεν υπάρχει κανένας προφανής τρόπος για την εφαρμογή του αλγόριθμο Shor και η γενική ανάλυση υποδηλώνει ότι ο αλγόριθμος του Grover είναι ουσιαστικά βέλτιστος για τυχαία συστήματα MQ με m= O(n).

Γενικά, δεν φαίνεται να υπάρχει ένας καλός κανόνας για τα συστήματα πολλαπλών μεταβλητών. Η εφαρμογή του αλγόριθμου Grover γίνεται άμεσα για την αναστροφή στο δημόσιο σύστημα και σημαίνει ότι τα πρωτόγονα που χρησιμοποιούν μικρά συστήματα, όπως το σύστημα κρυπτογράφησης HFE και το HFEv-signature θα πρέπει να διπλασιάσει τον αριθμό των πολυωνύμων και των μεταβλητών. Αυτό που διπλασιάζει τη διάρκεια του κρυπτογραφημένο κείμενο είναι ή υπογραφή, αλλά αυξάνει το μέγεθος των δημόσιων κλειδιών κατά συντελεστή 8 .Η κατάσταση των πολυμεταβλητών πρωτόγονων που χρησιμοποιούν μεγάλα συστήματα είναι λιγότερο ξεκάθαρη. Είναι δυνατό να χρησιμοποιηθεί ο Grover για να αποκτήθεί ταχύτητα τετραγωνικής ρίζας για μερικές επιθέσεις όπως το MinRank. Ωστόσο, η ασφάλεια τουλάχιστον του UOV και του Rainbow με τις υπογραφές καθορίζονται από το κόστος εύρεσης σύγκρουσης στη συνάρτηση κατακερματισμού ή επίθεσης στο σύστημα με χρήση του Gröbner και των βασικών τεχνικών του όπου καμία από τις οποίες δεν φαίνεται να βελτιώνεται με κβαντικούς αλγορίθμους. Απαιτείται έτσι περισσότερη έρευνα και στο πλαίσιο της συντηρητικής προσέγγισης είναι να γίνει η υπόθεση ότι μπορεί να επιτευχθεί μια ταχύτητα τετραγωνικής ρίζας. Και για το UOV και το Rainbow

σημαίνει διπλασιασμό του μήκους της υπογραφής και αύξηση του μεγέθους των δημόσιων κλειδιών κατά 8 φορές. [56]

Rainbow

Ένα από τα συστήματα ψηφιακών υπογραφών όπου θα πρωταγωνιστίσουν στο μέλλον της μετακβαντικής κρυπτογραφίας είναι και αυτό του Rainbow.



Εικόνα 3.5: Rainbow Cryptographic Multivariate Hash

Το Rainbow είναι μια πολυεπίπεδη έκδοση της υπογραφής UOV για ταχύτερη δημιουργία της υπογραφής .Αποτελείται από μια κυκλική παραλλαγή για μικρότερα μεγέθη δημόσιου κλειδιού. Δεν υπάρχει επίσημη μείωση της ασφάλειας για μια σειρά επιθέσεων που έχουν εκμεταλλευτεί την πρόσθετη δομή που παρέχουν τα στρώματα. Συγκεκριμένα, φαίνεται να μειώνει την ασφάλεια εκτιμήσεων για τις παραμέτρους μεγαλύτερου πεδίου και μπορεί επίσης να ισχύσει και για ορισμένες από τις πιο πρόσφατες παραμέτρους που προτείνονται.[50]

Χαρακτηρίζουμε ένα PKC τύπου Rainbow] με εξής στάδια:

• Η δομή του τμήματος δίνεται από μια ακολουθία 0 <v1 <v2 <· · · <vu + 1 =n.

• Για το l = 1,. . . , u + 1, σύνολο S_l: = {1, 2,. . . , v_l} έτσι ώστε | S_l | = v_l και $S_0 \subset S_1 \subset \cdot \cdot \subset S_u$ + 1 = S. Σημειώστε με o_l: = v_l + 1 - v_l και O_l: = S_l + 1 \ S_l για l = 1 · · u.

• Ο κεντρικός χάρτης Q έχει πολυώνυμα συνιστωσών y_{v1} + 1= q_{v1} + $1^{(x)}$, y_{v1} + 2=q_{v1} +$2^{(x)}$,. . . , y_n = q_n (x) .

Σε κάθε qk, όπου k ∈ O_l, δεν υπάρχει διαχρονική xixj όπου και τα i και j είναι στο O_l. Έτσι δίνεται όλα τα y_i με v_l <i ≤ v_l + 1, και όλα τα x_j με j ≤ v_l, μπορούμε να υπολογίσουμε x_{vl} + 1,. . . , x_{vl} + 1.

• Για να επιταχυνθούν οι υπολογισμοί, ορισμένοι συντελεστές ($\alpha_{ij}^{(k)}$) μπορεί να σταθεροποιηθούν (π.χ.έως το μηδέν), που επιλέγονται τυχαία (και συμπεριλαμβάνονται στο ιδιωτικό κλειδί ή αλληλένδετα με προκαθορισμένο τρόπο.
• Για την αντιστροφή του Q, προσδιορίζεται τυχαία $x_1,. . .x_{v1}$, δηλαδή, όλα τα x_k, $k \in S_1$. Από τα συστατικά του y που αντιστοιχούν στα πολυώνυμα $p'_{v1} + 1,. . .p'_{v2}$, λαμβάνουμε ένα σύνολο o_1 εξισώσεων στις μεταβλητές x_k, ($k \in O_1$). Μπορούμε να επαναλάβουμε τη διαδικασία για να βρούμε όλες τις υπόλοιπες μεταβλητές.
Ενα σχέδιο υπογραφής τύπου Rainbow λέγεται ότι είναι TTS εάν οι συντελεστές του Q είναι αραιωμένοι.

Τον Αύγουστο του 2015, η NSA δημοσίευσε μια ιστοσελίδα ανακοίνωντας προκαταρκτικά σχέδια για τη μετάβαση κβαντοανθεκτικών αλγόριθμων (www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm). Τον Δεκεμβριο του 2016, ο NIST ανακοίνωσε πρόσκληση υποβολής προτάσεων για κβαντικούς ανθεκτικούς αλγορίθμους (www.nist.gov/ pqcrypto). Επιπλέον, κυβερνητικές οργανώσεις όπως η Ευρωπαϊκή Επιτροπή και η Ιαπωνική Εταιρεία για την προώθηση της έρευνας για τη χρηματοδότηση της επιστήμης και προγραμμάτων όπως το PQCRYPTO, το SAFECRYPTO και το CryptoMathCrest ,επιδιώκουν την ενίσχυση της κρυπτογραφίας. Λόγω αυτών των πρωτοβουλιών, ενισχύεται η προσπάθεια για να αναπτυχθουν κβαντικές ανθεκτικές τεχνολογίες ιδιαίτερα για μετακβαντικά κρυπτοσυστήματα όπου γίνεται κεντρικά στον τομέα της ασφάλειας των πληροφοριών. [52,55]

Έτσι και με την ανάλυση του πιο πάνω συστήματος Rainbow αλλά και άλλων πολλών που υπάρχουν αποδεικνύεται ότι περίτρανα μπορούν τα συστήματα πολλαπλών μεταβλητών να αντεπεξέλθουν και αυτά σίγουρα στον ίδιο βαθμό ή ακόμα και περισσότερο προκυμένου να καταστίσουν ασφαλείς τους υπολογιστές που θα τα χρησιμοποιούν και τα διάφορα συστήματα-λογισμικά με την έλευση της κβαντικής εποχής των υπολογιστών.

3.6 Ισομορφισμός πάνω σε Ελλειπτικές Καμπύλες

Η κρυπτογράφηση ελλειπτικής καμπύλης (ECC) είναι μια τεχνική κρυπτογράφησης δημόσιου κλειδιού βασισμένη στην θεωρία ελλειπτικής καμπύλης που μπορεί να χρησιμοποιηθεί για τη δημιουργία ταχύτερων, μικρότερων και αποδοτικότερων κρυπτογραφικών κλειδιών. Αυτή η κρυπτογράφηση παράγει κλειδιά μέσω των ιδιοτήτων της εξίσωσης ελλειπτικής καμπύλης αντί της παραδοσιακής μεθόδου παραγωγής ως προϊόντος πολύ μεγάλων πρώτων αριθμών.[57] Η τεχνολογία μπορεί να χρησιμοποιηθεί σε συνδυασμό με τις περισσότερες μεθόδους κρυπτογράφησης δημόσιων κλειδιών, όπως RSA και Diffie-Hellman. Σύμφωνα με ορισμένους ερευνητές, η κρυπτογράφηση ελλειπτικής καμπύλης μέχρι τώρα μπορεί να αποδώσει ένα επίπεδο ασφάλειας με ένα κλειδί 164-bit, το οποίο άλλα συστήματα απαιτούν ένα κλειδί 1,024-bit για να επιτευχθεί. Επειδή, συμβάλλει στην καθιέρωση ισοδύναμης ασφάλειας με χαμηλότερη υπολογιστική ισχύ και χρήση πόρων μπαταρίας, χρησιμοποιείται ευρέως για κινητές εφαρμογές. Οι ελλειπτικές καμπύλες αναπτύχθηκαν από την Certicom,που είναι φορέας παροχής κινητών υπηρεσιών, και πρόσφατα χορηγήθηκε άδεια από την Hifn, κατασκευαστή ολοκληρωμένων κυκλωμάτων (IC) και προϊόντων ασφάλειας δικτύων. Η RSA έχει αναπτύξει τη δική της έκδοση κρυπτογράφησης όπως θα δούμε στην συνέχεια . Πολλοί κατασκευαστές, συμπεριλαμβανομένων των 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW και VeriFone, συμπεριέλαβαν υποστήριξη για κρυπτογράφηση ελλειπτικής καμπύλης στα προϊόντα τους.[58]

Οι ιδιότητες και οι λειτουργίες των ελλειπτικών καμπυλών έχουν μελετηθεί στα μαθηματικά για 150 χρόνια. Η χρήση τους στην κρυπτογραφία προτάθηκε για πρώτη φορά το 1985 από τον Neal Koblitz από το Πανεπιστήμιο της Ουάσιγκτον και τον Victor Miller από την IBM. Μια ελλειπτική καμπύλη δεν είναι μια ελλειπτική ωοειδής μορφή, αλλά αντιπροσωπεύεται ως μια γραμμή βρόχου που τέμνει δύο άξονες δηλαδή γραμμές σε ένα γράφημα που χρησιμοποιείται για την ένδειξη της θέσης ενός σημείου. Το ECC βασίζεται σε ιδιότητες ενός συγκεκριμένου τύπου εξίσωσης που δημιουργείται από τη μαθηματική ομάδα με ένα σύνολο τιμών για τις οποίες μπορούν να εκτελεστούν πράξεις σε οποιαδήποτε δύο μέλη της ομάδας για την παραγωγή ενός τρίτου μέλους που προέρχεται από σημεία όπου η γραμμή τέμνει τους άξονες. Ο πολλαπλασιασμός ενός σημείου στην καμπύλη με έναν αριθμό θα παράγει ένα άλλο σημείο στην καμπύλη, αλλά

είναι πολύ δύσκολο να βρεθεί ποιος αριθμός χρησιμοποιήθηκε, ακόμα κι αν γνωρίζουμε το αρχικό σημείο και το αποτέλεσμα. Οι εξισώσεις που βασίζονται στις ελλειπτικές καμπύλες έχουν ένα χαρακτηριστικό που είναι πολύτιμο για λόγους κρυπτογράφησης και είναι σχετικά εύκολο να εκτελεστούν αλλά είναι εξαιρετικά δύσκολο να αντιστραφούν.[59]

Η βιομηχανία εξακολουθεί να έχει κάποιες επιφυλάξεις σχετικά με τη χρήση ελλειπτικών καμπυλών. Ο Nigel Smart, ερευνητής της Hewlett Packard, ανακάλυψε ένα ελάττωμα στο οποίο ορισμένες καμπύλες είναι εξαιρετικά ευάλωτες. Ωστόσο, ο Philip Deck της Certicom λέει ότι, ενώ υπάρχουν καμπύλες που είναι ευάλωτες, εκείνοι που εφαρμόζουν το ECC θα πρέπει να γνωρίζουν ποιες καμπύλες δεν μπορούσαν να χρησιμοποιηθούν. Πιστεύει ότι το ECC προσφέρει ένα μοναδικό δυναμικό ως τεχνολογία που θα μπορούσε να εφαρμοστεί παγκοσμίως και σε όλες τις συσκευές. Σύμφωνα με το Deck (που αναφέρεται στην ενσύρματη), "ο μόνος τρόπος για να επιτευχθεί αυτό είναι με την ελλειπτική καμπύλη.

Η κρυπτογραφία υποστηρίζει τα σχέδια ψηφιακής υπογραφής των κρυπτοσυχνοτήτων και αποτελεί τη βάση για την ασφαλή επαλήθευση των συναλλαγών μεταξύ δύο μερών σε ένα αποκεντρωμένο δίκτυο. Υπάρχουν πολλές κρυπτογραφικές μέθοδοι που χρησιμοποιούνται σήμερα από διαφορετικές κρυπτοσυχνότητες, εστιάζοντας στην παροχή αποτελεσματικών και ασφαλών μοντέλων συναλλαγών.

Η κρυπτογράφηση ελλειπτικής καμπύλης (ECC) είναι μία από τις πιο ευρέως χρησιμοποιούμενες μεθόδους για συστήματα ψηφιακής υπογραφής σε κρυπτοσυχνότητες με ένα ειδικό σχήμα,με τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA) που εφαρμόζεται τόσο σε Bitcoin όσο και σε Ethereum για την υπογραφή συναλλαγών. Το ECC είναι μια σημαντική ανακάλυψη στην κρυπτογραφία, παρόλο που δεν χρησιμοποιήθηκε ευρέως μέχρι τις αρχές της δεκαετίας του 2000, κατά την εμφάνιση του Διαδικτύου, όπου οι κυβερνήσεις και οι πάροχοι του διαδικτύου άρχισαν να το χρησιμοποιούν ως μέθοδο κρυπτογράφησης. [61]

Σε σύγκριση με την κρυπτογράφηση RSA, το ECC προσφέρει ένα σημαντικό πλεονέκτημα. Το μέγεθος κλειδιού που χρησιμοποιείται για το ECC είναι πολύ μικρότερο από αυτό που απαιτείται για την κρυπτογράφηση RSA, παρέχοντας

ταυτόχρονα το ίδιο επίπεδο ασφάλειας. Αν και η κρυπτογράφηση RSA χρησιμοποιείται ευρύτερα σήμερα στο διαδίκτυο μέχρι στιγμής από τους συνηθισμένους εώς τώρα υπολογιστές, το ECC είναι ουσιαστικά μια πιο αποτελεσματική μορφή RSA, που είναι ένας από τους κύριους λόγους που χρησιμοποιείται σε κρυπτοσυχνότητες.
Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) υποστηρίζει το ECC ως τους συνιστώμενους αλγόριθμους "Suite B" και η NSA υποστηρίζει επισήμως την ταξινόμηση των άκρως απόρρητων πληροφοριών με κλειδιά 384-bit. Ως παράδειγμα της αποτελεσματικότητας του ECC σε σύγκριση με το RSA, το ίδιο κλειδί 384-bit που χρησιμοποιείται στην κρυπτογράφηση διαβαθμισμένων πληροφοριών θα απαιτούσε ένα κλειδί 7680-bit χρησιμοποιώντας κρυπτογράφηση RSA. Επομένως, η αποδοτικότητα που παρέχεται από το ECC είναι εξαιρετικά χρήσιμη για την παρεμπόδιση δικτύων, καθώς μειώνει το μέγεθος των συναλλαγών.
Ωστόσο, παρά τα οφέλη του ECC, αυτή τη στιγμή χρησιμοποιείται μόνο από μικρό αριθμό τοποθεσιών. Τα πρόσφατα δεδομένα δείχνουν ότι το RSA εξακολουθεί να χρησιμοποιείται ευρύτατα από ένα ευρύ περιθώριο - πάνω από το 90% των πιστοποιητικών SSL χρησιμοποιούν κλειδιά RSA (μόνο το 4% των πιστοποιητικών χρησιμοποίησαν κλειδιά ECC). Το RSA υπήρξε το κρυπτοσύστημα από την αρχή του SSL, καθιστώντας την την πιο ευρέως υποστηριζόμενη επιλογή εκεί έξω. Οι περισσότεροι ιστότοποι δεν χρησιμοποιούν το ECC, ωστόσο, επειδή οι servers και client software είναι αργοί για να το υποστηρίξουν και δεν είναι δυνατή η παροχή πιστοποιητικών SSL που χρησιμοποιούν τα κλειδιά ECC.

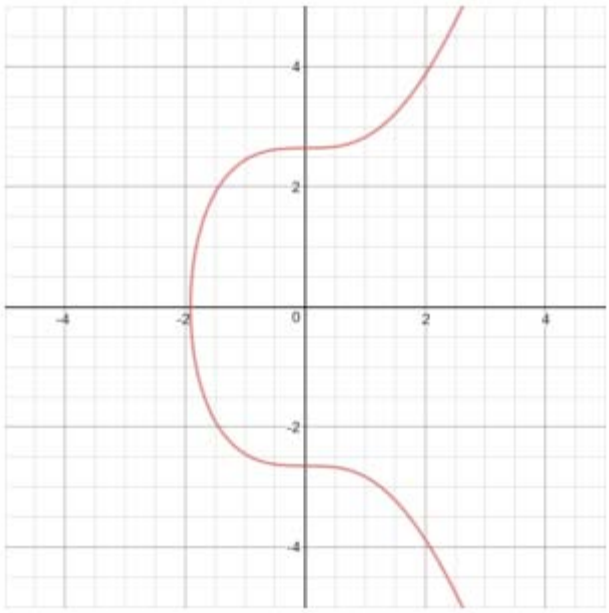
Η κρυπτογραφία ελλειπτικής καμπύλης είναι μια μέθοδος κρυπτογράφησης δημόσιου κλειδιού που βασίζεται στην αλγεβρική λειτουργία και τη δομή μιας καμπύλης πάνω σε ένα πεπερασμένο γράφημα όπως προαναφέραμε. Χρησιμοποιεί ακόμα, μια λειτουργία τσαμπιού που βασίζεται στην αδυναμία προσδιορισμού του διακριτού λογαρίθμου ενός τυχαίου στοιχείου ελλειπτικής καμπύλης που έχει ένα γνωστό σημείο βάσης.[62,64]

Οι λειτουργίες του Trapdoor χρησιμοποιούνται στην κρυπτογραφία δημόσιου κλειδιού για να το κάνουν, πηγαίνοντας από το A -> B είναι ασήμαντο, αλλά η μετάβαση από το B -> A δεν είναι εφικτό, εκμεταλλευόμενος ένα συγκεκριμένο μαθηματικό πρόβλημα. Για παράδειγμα, η κρυπτογράφηση RSA βασίζεται στην έννοια του Prime Factorization και το ECC βασίζεται στην έννοια του πολλαπλασιασμού σημείων, όπου ο πολλαπλασιαστής αντιπροσωπεύει το ιδιωτικό κλειδί και είναι αδύνατο να υπολογιστεί από τα δεδομένα σημεία εκκίνησης.

Η ελλειπτική καμπύλη πρέπει να αποτελείται από σημεία που ικανοποιούν την εξίσωση:

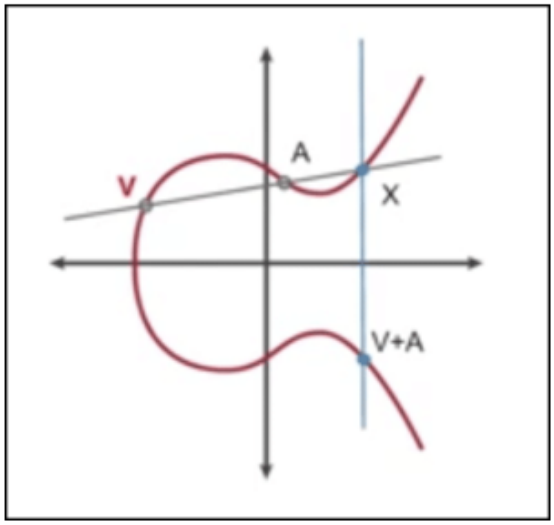
$$y^2 = ax^3 + b$$

(x, y) στην καμπύλη αντιπροσωπεύουν ένα σημείο, ενώ και οι δύο a και b είναι σταθερές. Θεωρητικά, υπάρχουν άπειρες καμπύλες που θα μπορούσαν να δημιουργηθούν, αλλά εφαρμοσμένες ειδικά σε κρυπτοσυχνότητες (στην περίπτωση των Bitcoin και Ethereum), χρησιμοποιείται μια συγκεκριμένη ελλειπτική καμπύλη που ονομάζεται secp256k1. Παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 3.6: Ελλειπτική Καμπύλη τύπου secp256k1

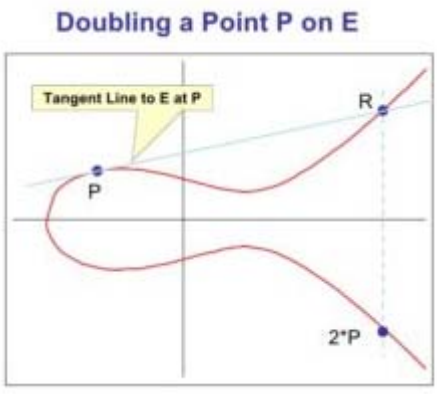
Όπως μπορείτε να δείτε, οι ελλειπτικές καμπύλες είναι συμμετρικές ως προς τον άξονα x. Λόγω αυτού, αν σχεδιάσετε μια ευθεία γραμμή ξεκινώντας από ένα τυχαίο σημείο στην καμπύλη, η γραμμή τέμνει την καμπύλη σε όχι περισσότερο από 3 σημεία. Μπορείτε να σχεδιάσετε μια γραμμή μέσα από τα πρώτα δύο σημεία και να καθορίσετε πού η γραμμή θα τέμνει με το τρίτο σημείο. Στη συνέχεια, θα αντικατοπτρίσετε αυτό το τρίτο σημείο στον άξονα x (είναι συμμετρικό) και αυτό το σημείο είναι το αποτέλεσμα της προσθήκης των δύο πρώτων σημείων μαζί. Αυτό φαίνεται στην παρακάτω εικόνα.



Εικόνα 3.7: Παράδειγμα σχεδιασμού Ελλειπτικής Καμπύλης

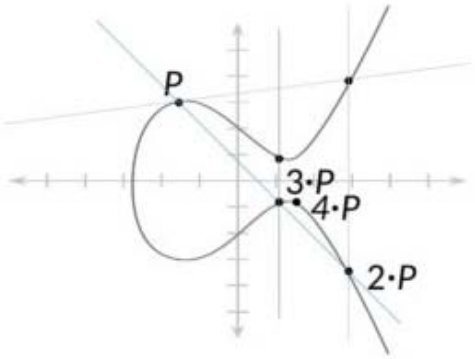
Στο παραπάνω γράφημα, τα V και A αντιπροσωπεύουν τα σημεία εκκίνησης, το X αντιπροσωπεύει το τρίτο σημείο και το τελικό σημείο (όπως το αποκαλούμε Z) αντιπροσωπεύει την προσθήκη V και A μαζί. Όταν χρησιμοποιείται σε σχήμα ψηφιακής υπογραφής, το βασικό σημείο όπως γραμμής είναι συνήθως προκαθορισμένο.

Προκειμένου το ECC να δημιουργήσει μια λειτουργία trapdoor, η κρυπτογραφία ελλειπτικής καμπύλης χρησιμοποιεί πολλαπλασιασμό σημείων, όπου το γνωστό σημείο βάσης προστίθεται επανειλημμένα στον εαυτό του. Σε μια τέτοια περίπτωση, όπως χρησιμοποιήσουμε ένα σημείο βάσης P, όπου ο στόχος είναι να βρούμε 2P, όπως περιγράφεται παρακάτω.



Εικόνα 3.8: Σημείο Βάσης P, 2P

Πάνω, μια εφαπτομένη τρέχει από το σημείο P στο σημείο R, το οποίο είναι το σημείο τομής. Η αντανάκλαση αυτού του σημείου είναι 2P. Ας υποθέσουμε ότι θέλουμε να συνεχίσουμε αυτό και να βρούμε 3P, 4P, και ούτω καθεξής. Στη συνέχεια, θα ενώσουμε τα P και 2P και στη συνέχεια θα αντικατοπτρίσουμε αυτό το σημείο στη διασταύρωση και θα συνεχίσουμε να το κάνουμε αυτό για το 4P. Εικονογραφημένο παρακάτω:



Εικόνα 3.9: Ευρεση 3P, 4P

Αυτή είναι η πολλαπλασιαστική ιδιότητα του γραφήματος, επειδή βρίσκουμε σημεία που είναι ένας πολλαπλασιασμός ενός ακέραιου αριθμού με το ίδιο το σημείο. Το αποτέλεσμα είναι αυτό που δίδει στη λειτουργία το σύστημα καταπακτών, γνωστό ως πρόβλημα διακριτού λογαρίθμου. Αν αντιπροσωπεύσουμε μια μεταβλητή x ως ακέραιο 384-bit και πολλαπλασιάσουμε το με το σημείο βάσης P, το αποτέλεσμα είναι ένα σημείο της καμπύλης, που ονομάζεται Z. Εφαρμόζεται σε cryptocurrencies, το Z είναι δημόσιο, αλλά η αρχική μεταβλητή x είναι μυστική δηλαδή είναι ιδιωτικό κλειδί. Για να προσδιορίσουμε το x από το Z και το P, θα πρέπει να καθορίσουμε πόσες φορές το P προστέθηκε στον εαυτό του για να πάρει το σημείο Z στην καμπύλη. Αυτό το πρόβλημα είναι μια μορφή αριθμητικής αριθμητικής που είναι μαθηματικά ανέφικτη και είναι ο λόγος για τον οποίο το ECC είναι τόσο ασφαλές.

Κατά την ανάλυση της ανάγκης για συστήματα ψηφιακών υπογραφών σε κρυπτοσυχνότητες, υπάρχουν 4 πρωταρχικές απαιτήσεις οποιουδήποτε σχεδίου που πρέπει να πληρούνται για να είναι το σχήμα υπογραφής αποδεδειγμένα αυθεντικό και επαληθεύσιμο. Αυτά περιλαμβάνουν:

1. Πρέπει να είναι αποδεδειγμένα επαληθεύσιμο ότι ο υπογράφων μιας συναλλαγής είναι ο υπογράφων.
2. Η υπογραφή δεν πρέπει να είναι πλαστή.

3. Η υπογραφή πρέπει να είναι αξιόπιστη, δηλαδή οι υπογραφές είναι τελικές και δεν μπορούν να συνδεθούν με άλλη ταυτότητα.
4. Θα πρέπει να είναι υπολογιστικά ανέφικτο να εξαχθεί το ιδιωτικό κλειδί από ένα αντίστοιχο δημόσιο κλειδί.

Η κρυπτογραφία ελλειπτικής καμπύλης ικανοποιεί και τις 4 συνθήκες και είναι επίσης ιδιαίτερα αποτελεσματική. Χρησιμοποιώντας το ECC, οι συντεταγμένες (x, y) ενός σημείου στο γράφημα θα είναι το δημόσιο κλειδί και ο τυχαίος ακέραιος 384-bit θα είναι το ιδιωτικό σας κλειδί.Είναι επίσης δυνατό να αποδείξουμε σε κάποιον ότι γνωρίζουμε την τιμή του x, χωρίς στην πραγματικότητα να αποκαλύπτουμε τι είναι το x. Αυτή η ιδιότητα συμβάλλει περαιτέρω στην ικανοποίηση των απαραίτητων προϋποθέσεων για βιώσιμη χρήση σε ένα σχήμα συναλλαγής ψηφιακής υπογραφής.[65]

Η χρήση του ECC σε συστήματα ψηφιακής υπογραφής κρυπτοσυχνοτήτων είναι εξαιρετικά ασφαλής. Ωστόσο, έχουν ανακύψει πρόσφατα ανησυχίες σχετικά με τις μελλοντικές δυνατότητες των κβαντικών υπολογιστών και της ουσιαστικής ισχύος τους που έχουν τη δυνατότητα να σπάσουν το ECC. Αν και η πιθανότητά του θεωρείται χρόνια μακριά, ο αλγόριθμος Shor θεωρητικά θα μπορούσε να υπολογίσει διακεκριμένους λογαρίθμους σε έναν υποθετικό κβαντικό υπολογιστή με επαρκή ισχύ.

Διάφορες κρυπτοσυχνότητες έχουν υιοθετήσει μια προσέγγιση προς τα εμπρός για την πιθανή απειλή που προκαλούν οι κβαντικοί υπολογιστές, εφαρμόζοντας αλγόριθμους ανθεκτικούς στην κβάντα ως θεμέλιο των σχεδίων ψηφιακής υπογραφής τους. Ακόμη και η NSA το 2015 ανακοίνωσε την προγραμματισμένη μελλοντική μετάβαση της μακριά από το ECC, και σε μια διαφορετική σειρά από αλγόριθμους κρυπτογράφησης για τις κρυπτογράφικές της ανάγκες, λόγω της διαφαινόμενα αναπόφευκτης κβαντικής υπολογιστικής ισχύος.

Οι ανησυχίες αυτές είναι κατά κύριο λόγο η κερδοσκοπία σε αυτό το σημείο, όπως η κβαντική υπολογιστική ισχύ που απαιτείται για τον αλγόριθμο του Shor και για τον υπολογισμό διακριτών λογαρίθμων πουείναι σημαντικά υψηλότερο από ό, τι ακόμη και τα πιο ισχυρό πρώιμο σταδίο των κβαντικών υπολογιστών που υπάρχουν σήμερα.

Κοιτάζοντας μπροστά, οι διαδοχικές γενιές κρυπτοσυχνοτήτων μπορεί τελικά να μεταβαίνουν σε πιο προηγμένες μεθόδους κρυπτογράφησης για την εξασφάλιση των

συναλλαγών τους και ενδεχομένως τα Bitcoin και Ethereum ίσως να χρειαστούν να κάνουν την ίδια μετάβαση.Προς το παρόν, τα συστήματα ECC και άλλα είδη ψηφιακών υπογραφών που χρησιμοποιούν λειτουργίες με κρυπτογράφηση παραμένουν μερικές από τις πιο ασφαλείς μεθόδους κρυπτογράφησης στον κόσμο και θα πρέπει να παραμείνουν έτσι για αρκετό καιρό.

Πρακτικές κβαντικές τεχνολογίες, που θα επέτρεπαν την οικοδόμηση ενός κβαντικού υπολογιστή μεγάλης κλίμακας, αναδύθηκαν ενεργά. Σύμφωνα με ορισμένους ειδικούς, ίσως χρειαστούν άλλα 15-20 χρόνια για να μπορέσουν να χτίσουν ένα. Οι κβαντικοί υπολογιστές θα ανοίξουν νέες δυνατότητες για τον κόσμο. Ο κατάλογος των ωφελειών είναι εντυπωσιακός. Ωστόσο, στα χέρια των κακόβουλων αντιπάλων, ο κβαντικός υπολογιστής θα μπορούσε να γίνει πραγματική απειλή. Όλες οι σημερινές τυποποιημένες κρυπτογραφήσεις δημόσιου κλειδιού θα μπορούσαν να διαρρηγυριστούν από μεγάλης κλίμακας κβαντικούς υπολογιστές. Είναι ζωτικής σημασίας να αναπτύξουμε προστασία από αυτήν την απειλή τώρα ή στο εγγύς μέλλον. Οι κβαντοανθεκτικοί κρυπτογραφικοί αλγόριθμοι θα πρέπει να αναπτυχθούν και να υλοποιηθούν πολύ πριν την άφιξη του κβαντικού υπολογιστή, διαφορετικά θα είναι πολύ αργά για πολλούς τομείς σε ασφαλή προστασία δεδομένων και επικοινωνία. Δεδομένου ότι δεν είναι ακόμη εφικτή η χρήση τεχνητών τεχνικών, η λύση είναι η μετάκβαντική κρυπτογραφία, κλασσικά κρυπτογραφικά σχήματα που θα ήταν ανθεκτικά στον κβαντικό τρόπο δράσης των υπολογιστών αυτών.

Τα συστήματα που βασίζονται σε ισογονίδια μπορούν να θεωρηθούν ως συνέχεια της κρυπτογράφησης της ελλειπτικής καμπύλης, αλλά ως μετάκβαντική συνέχιση. Το υποκείμενο σκληρό πρόβλημα για την κρυπτογραφία με βάση την ισογονικότητα λαμβάνει δύο ισογενείς υπερκείμενες ελλειπτικές καμπύλες, οι οποίες βρίσκονται μεταξύ τους. Επί του παρόντος δεν είναι γνωστός κανένας κβαντικός αλγόριθμος για την επίλυση αυτού του προβλήματος γενικά σε λιγότερο από εκθετικό χρόνο. Ένας από τους κύριους λόγους για τους οποίους αυτό το πρόβλημα φαίνεται ανυπόφορο για τους κβαντικούς υπολογιστές είναι ότι ο δακτύλιος ενδομορφισμού για την ελλειπτική καμπύλη είναι μη μεταλλαξιογόνος, πράγμα που προστατεύει το πρόβλημα από επιθέσεις όπως ο αλγόριθμος Shor. Σε σύγκριση με άλλες μετακβαντικές προτάσεις, αυτή η προσέγγιση θα ήταν μια από τις πιο απλές αντικαταστάσεις για την τρέχουσα κρυπτογραφική υποδομή. Έχει επίσης το μικρότερο μέγεθος κλειδιού. Εκτός αυτού, βασίζεται σε ελλειπτικές καμπύλες, επομένως είναι κάτι που ο κρυπτογραφικός

βιομηχανικός κόσμος έχει ήδη δει μερικώς και μπορεί να επαναχρησιμοποιηθεί πολύς κώδικας.

Ο κωδικευτής έχει ιδανικά τα ακόλουθα τρία βασικά στοιχεία:

1. Βασική συμφωνία
2. Κρυπτογράφηση δημόσιου κλειδιού
3. Ψηφιακή υπογραφή

Τα πρώτα δύο συστατικά ήταν τα πρώτα κρυπτογραφικά σχήματα που βασίζονται σε ισογονίδια που αναπτύχθηκαν πριν από μερικά χρόνια. Έχουν αναπτυχθεί αρκετά πρωτόκολλα που σχετίζονται με την επαλήθευση της ταυτότητας. Πρόσφατα, η ψηφιακή υπογραφή προέκυψε και αποδείχθηκε ασφαλής στο κβαντικό random oracle model.

Η δυνητική απειλή μελλοντικών κβαντικών επιθέσεων σε κρυπτοσυστήματα δημόσιου κλειδιού οδήγησε την NIST να εκδώσει επίσημη Αίτηση για Πρόταση που ζητούσε "μετακβαντικούς κρυπτογραφικούς αλγορίθμους" τον Δεκέμβριο του 2016. Μέχρι την προθεσμία του Δεκεμβρίου του 2017 για την υποβολή στρογγυλής υποβολής, έλαβαν 69 προτάσεις. Τα περισσότερα από αυτά βασίζονται σε προβλήματα θεωρίας πλέγματος ή κωδικοποίησης που δεν πιστεύεται ότι είναι επιρρεπή σε κβαντικές επιθέσεις.

Μια πρόταση από αυτές όμως και συγκεκριμένα η SIKE χρησιμοποιεί όμως και ελλειπτικές καμπύλες. Αντί να δουλεύει στην ομάδα των ορθολογικών σημείων σε μια ενιαία ελλειπτική καμπύλη, λειτουργεί με γραφήματα ισογονισμού των υπερηχητικών ελλειπτικών καμπυλών σε ένα και μόνο πεπερασμένο πεδίο.

Έκτοτε έχουν προταθεί άλλα πρωτόκολλα που βασίζονται σε ισογονίδια, συγκεκριμένα τα CSIDH. Το κύριο πλεονέκτημα των πρωτοκόλλων που βασίζονται σε ισογονίδια είναι ότι είναι καλά κατανοητά, προσφέρουν μια εύκολη στην εφαρμογή αντικατάσταση drop-in για το ECDHE και έχουν μικρότερα μεγέθη κλειδιών από τις προσεγγίσεις που βασίζονται σε πλέγματα.

Το πλήρες σύνολο κρυπτογραφικών σχημάτων δείχνει ότι οι ελλειπτικές καμπύλες μπορούν να χρησιμοποιηθούν ως προστασία έναντι κβαντικών υπολογιστών. Η εμφάνιση κβαντικών υπολογιστών θα αποφέρει πολλά οφέλη στην κοινωνία. Ωστόσο, στα χέρια του αντιπάλου θα αποτελέσουν απειλή για την ασφάλεια. Έτσι, προκειμένου να αποφευχθεί αυτή η απειλή, πρέπει να αρχίσουμε τη μετάβαση σε κβαντοανθεκτικά κρυπτογραφικά πρωτόκολλα το συντομότερο δυνατό. Στην πραγματικότητα, η μετάβαση είναι μια μακρά και περίπλοκη διαδικασία. Τα σχέδια με βάση την ισόρροπη καμπύλη της ελλειπτικής καμπύλης έχουν τις ιδιότητες, οι οποίες θα επιτρέψουν την ομαλότερη μετάβαση, σε σύγκριση με όλους τους άλλους μετακβανικούς υποψηφίους.

Για πολλές εφαρμογές υψηλής αξιοπιστίας όπως η κυκλοφορία TLS, οι ιατρικές βάσεις δεδομένων και τα μπλοκ αλυσίδων,αλλά και η μυστικότητα για τα εμπρός είναι απολύτως απαραίτητη. Δεν αρκεί να εμποδίσουμε έναν εισβολέα να αποκρυπτογραφήσει αμέσως ευαίσθητες πληροφορίες. Εδώ το μοντέλο απειλής περιλαμβάνει καταστάσεις όπου ο αντίπαλος μπορεί να αφιερώσει πολλά χρόνια στην αποκρυπτογράφηση κρυπτογραφημάτων μετά τη συλλογή τους. Μια πιθανή μελλοντική μυστικότητα μπορεί να σπάσει είναι ότι ένας συνδυασμός αυξημένης υπολογιστικής ισχύος και αριθμητικών θεωρητικών ανακαλύψεων καθιστά την επίθεση της τρέχουσας κρυπτογραφίας εφικτή. Ωστόσο, αν κάποιος δεν βρει έναν αλγόριθμο πολυωνυμικού χρόνου για την παραγώγιση μεγάλων ακεραίων, αυτός ο κίνδυνος είναι ελάχιστος για τις τρέχουσες βέλτιστες πρακτικές. Πρέπει να ανησυχούμε περισσότερο για την επιτυχή ανάπτυξη ενός κβαντικού υπολογιστή, καθώς μια τέτοια ανακάλυψη θα καθιστούσε το μεγαλύτερο μέρος της κρυπτογραφίας που χρησιμοποιούμε σήμερα επισφαλής.[65]

Συνοψίζουμε συνοπτικά τις ιδέες αυτές που είναι εγγενείς σε κάθε τύπο κρυπτοσυστήματος και με συγκρίσεις με την τρέχουσα όχι δηλαδή την μετακβαντική ελλειπτική καμπύλη κρυπτογραφία. Σημειώνεται επίσης ότι ότι οι κώδικες και τα ισογονίδια είναι ικανά να παράγουν ψηφιακές υπογραφές, αλλά δεν έχουν υποβληθεί τέτοια προγράμματα στο NIST.

	Signatures	Key Exchange	Fast?
Elliptic Curves	64 bytes	32 bytes	✓
Lattices	2.7kb	1 kb	✓
Isogenies	✗	330 bytes	✗
Codes	✗	1 mb	✓
Hash functions	41 kb	✗	✓

Εικόνα 3.10: Καταχωρημένος Πίνακας στο NIST

Όσον αφορά τις αποδείξεις ασφάλειας, κανένα από τα παραπάνω κρυπτοσυστήματα δεν μειώνει τα προβλήματα NP-hard ή NP-complete. Στην περίπτωση του πλέγματος και των κωδίκων, αυτά τα κρυπτοσυστήματα βασίζονται σε ελαφρές τροποποιήσεις των προβλημάτων των σκληρών NP. Τα κρυπτοσυστήματα με βάση το Hash βασίζονται στην ύπαρξη καλών λειτουργιών κατακερματισμού και δεν κάνουν άλλες κρυπτογραφικές υποθέσεις. Τέλος, η κρυπτογραφία βασισμένη σε ισογονίδια βασίζεται σε ένα πρόβλημα που θεωρείται ισχυρή, αλλά δεν είναι παρόμοια με ένα πρόβλημα NP-hard ή προηγούμενη κρυπτογραφική παραδοχή. Αξίζει να σημειωθεί όμως ότι, όπως δεν μπορούμε να αποδείξουμε ότι ένας κλασικός αλγόριθμος δεν είναι ευάλωτος σε πολυωνυμικό χρόνο δεδομένου ότι το P μπορεί να είναι NP, θα μπορούσε να είναι τα προβλήματα που θεωρούνται δύσκολα για τους κβαντικούς υπολογιστές. Επιπλέον, ένα κρυπτοσύστημα που δεν μειώνει σε κάποιο NP-σκληρό ή πλήρες πρόβλημα δεν πρέπει να είναι ένα σημάδι εναντίον του, per se, αφού ο ακέραιος συντελεστής και το διακριτό log πρόβλημα δεν πιστεύεται ότι είναι NP-πλήρης.

Το πεδίο της κρυπτογραφίας ελλειπτικής καμπύλης είναι κάπως περιβόητο για τη χρήση και αρκετά κομψό μαθηματικά. Οι ισογονιαίες το παίρνουν σε ένα εντελώς νέο επίπεδο. Στην κρυπτογραφία ελλειπτικής καμπύλης χρησιμοποιούμε ένα πρωτόκολλο τύπου Diffie-Hellman για να αποκτήσουμε ένα κοινό μυστικό, αλλά αντί να αυξήσουμε τα στοιχεία της ομάδας σε μια ορισμένη δύναμη, περπατάμε μέσω σημείων σε μια ελλειπτική καμπύλη. Σε κρυπτογραφία βασισμένη σε ισογονίδια, χρησιμοποιούμε και πάλι ένα πρωτόκολλο τύπου Diffie-Hellman, αλλά αντί να περπατάμε μέσω σημείων στην ελλειπτική καμπύλη, περνάμε μέσα από μια σειρά ελλειπτικών καμπυλών.

	DH	ECDH	SIDH
Elements	integers g modulo prime	points P in curve group	curves E in isogeny class
Secrets	exponents x	scalars k	isogenies ϕ
computations	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $E, \phi(E)$ find ϕ

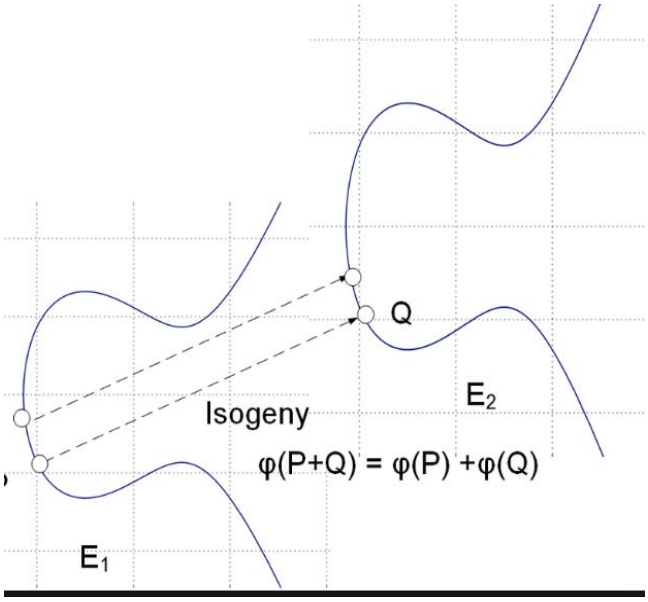
Εικόνα 3.11: Supersingular Ισογενεί Κρυπτογραφικά Συστήματα

Μια ισογονικότητα είναι μια συνάρτηση που μετατρέπει μια ελλειπτική καμπύλη στην άλλη με τέτοιο τρόπο ώστε η δομή της ομάδας της πρώτης καμπύλης να αντανακλάται στο δεύτερο. Για όσους είναι εξοικειωμένοι με τη θεωρία των ομάδων, πρόκειται για ομοιομορφισμό ομάδας με κάποια προστιθέμενη δομή που ασχολείται με τη γεωμετρία κάθε καμπύλης. Όταν περιορίζουμε την προσοχή μας στις υπερηχητικές ελλειπτικές καμπύλες που δεν θα καθορίσαμε ακόμα, κάθε καμπύλη εγγυάται ότι έχει σταθερό αριθμό ισογενών από αυτήν σε άλλες υπερηχητικές καμπύλες.

Τώρα, ας σκεφτούμε το γράφημα που δημιουργήθηκε εξετάζοντας όλες τις ισογονίες αυτής της φόρμας από την αρχική μας καμπύλη, τότε όλες οι ισογονίες από αυτές τις καμπύλες και ούτω καθεξής. Αυτό το γράφημα είναι πολύ δομημένο με την έννοια ότι εάν κάνουμε μια τυχαία βόλτα ξεκινώντας από την πρώτη καμπύλη μας, η πιθανότητα να χτυπήσει μια συγκεκριμένη άλλη καμπύλη είναι αμελητέα μικρή εκτός εάν λάβουμε εκθετικά πολλά βήματα. Στη γραμματική μαθηματικών, λέμε ότι το γράφημα που δημιουργήθηκε εξετάζοντας όλες αυτές τις ισογονίες είναι ένα γράφημα διαστολέα και επίσης Ramanujan. Αυτή η ιδιότητα της επέκτασης είναι ακριβώς αυτό που κάνει την κρυπτογράφηση με βάση την ισογονία ασφαλής.[63]

Για το σχήμα Supersingular Isogeny Diffie-Hellman (SIDH), τα μυστικά κλειδιά είναι μια αλυσίδα ισογενών και τα δημόσια κλειδιά είναι καμπύλες.
Η κρυπτογραφία με βάση την ισογονία έχει εξαιρετικά μικρά μεγέθη κλειδιών σε σύγκριση με άλλα μετακβαντικά σχήματα, χρησιμοποιώντας μόνο 330 byte για δημόσια κλειδιά.Η μετά-κβαντική κρυπτογραφία είναι ένας εξαιρετικά συναρπαστικός τομέας έρευνας που γνώρισε τεράστια αύξηση κατά την τελευταία δεκαετία. Ενώ οι τέσσερις

τύποι κρυπτοσυστημάτων που περιγράφονται σε αυτή τη θέση έχουν λάβει μεγάλη ακαδημαϊκή προσοχή, κανένας δεν έχει εγκριθεί από το NIST και ως εκ τούτου δεν συνιστάται για γενική χρήση ακόμα. Πολλά από τα συστήματα δεν έχουν απόδοση στην αρχική τους μορφή και έχουν υποστεί διάφορες βελτιστοποιήσεις που μπορεί να επηρεάσουν ή να μην επηρεάσουν την ασφάλεια. Πράγματι, αρκετές προσπάθειες για τη χρήση περισσότερων διαλειτουργικών κωδίκων για το σύστημα McEliece έχουν αποδειχθεί ανασφαλείς. Σήμερα, η εξασφάλιση της καλύτερης ασφάλειας από τα κβαντικά κρυπτοσυστήματα απαιτεί μια θυσία κάποιου ποσού χώρου ή χρόνου. Η κρυπτογραφία με δακτυλιοειδή πλέξη είναι η πιο ελπιδοφόρα δουλειά από την άποψη της ευελιξίας τόσο των υπογραφών όσο και της KEM, αλλά και της πλήρως ομομορφικής κρυπτογράφησης, αλλά οι υποθέσεις στις οποίες στηρίζεται έχουν μελετηθεί έντονα για αρκετά χρόνια. Αυτή τη στιγμή, το ασφαλέστερο στοίχημα είναι να χρησιμοποιήσουμε τον McEliece με τους κώδικες Goppa, δεδομένου ότι έχει αντέξει αρκετές δεκαετίες κρυπτοανάλυσης. Ωστόσο, κάθε περίπτωση χρήσης είναι μοναδική. Όλες οι σύγχρονες κρυπτογραφίες ελλειπτικής καμπύλης (ECC) απαιτούν ιδανικά έναν επιτιθέμενο να λύσει μια περίπτωση του προβλήματος διακριτού λογαρίθμου σε μια ελλειπτική καμπύλη E πάνω από ένα πεπερασμένο πεδίο Fp με στοιχεία p, όπου το p είναι ένας prime αριθμός. Συγκεκριμένα, το καθήκον του / της είναι να βρει έναν μυστικό ακέραιο n για τον οποίο P '= nP κατά την είσοδο δύο σημείων P και P' στο E, όπου ο πολλαπλασιασμός με το n γίνεται μέσω μιας επαναλαμβανόμενης εφαπτομένης και χορδής που καλεί στα σημεία του E με φαινομενικά ακανόνιστο και απρόβλεπτο τρόπο. Όταν δηλώνεται γεωμετρικά, το πρόβλημα διακριτού λογαρίθμου είναι να ξεδιπλωθεί αυτή η επανάληψη.

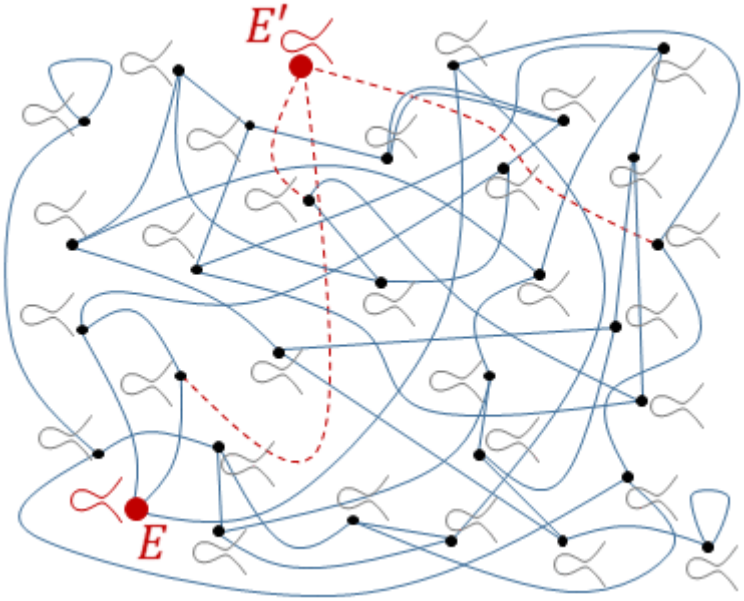


Εικόνα 3.12: Supersingular Isogeny

Με καλά επιλεγμένους Ε και ρ αυτό πιστεύεται ότι είναι εξαιρετικά δύσκολο. Για παράδειγμα, το σπάσιμο του ευρέως χρησιμοποιούμενου Curve25519 χρησιμοποιώντας τις καλύτερες διαθέσιμες επιθέσεις απαιτεί περισσότερες από 2128 λειτουργίες bit, ένα αστρονομικό ποσό που συμφωνεί με τα ισχύοντα πρότυπα ασφαλείας. Το κύριο σημείο πώλησης του ECC είναι ότι αυτό το επίπεδο ασφάλειας επιτυγχάνεται χρησιμοποιώντας πολύ σύντομες παραμέτρους του συστήματος. Σύμφωνα με τις περισσότερες συστάσεις, τα βασικά μήκη μπορούν να ληφθούν περίπου δώδεκα φορές μικρότερα από τα αντίστοιχά τους σε RSA ή με κρυπτογραφία με κλασική λογική λογαρίθμου. συγκεκριμένα, το Curve25519 λειτουργεί με πλήκτρα που αποτελούνται από περίπου 256 μπιτ, ενώ μια ισοδύναμη παράμετρος RSA θα χρειαζόταν πλήκτρα μεγέθους 3072 bits. Ωστόσο, εάν ο επιτιθέμενος μας θα είχε ένα αρκετά μεγάλο παγκόσμιο κβαντικό υπολογιστή εξοπλισμένο με εφαρμογή του αλγορίθμου Shor, τότε αυτή η ανάλυση θα καταρρεύσει δραματικά: σε αυτήν την περίπτωση θα μπορούσε εύκολα να σπάσει όλα τα προαναφερθέντα συστήματα, συμπεριλαμβανομένου του ECC. Αν και δεν είναι σαφές εάν μια τέτοια συσκευή θα είναι πράγματι τεχνικά εφικτή μια μέρα, οι μικρογραφικές εκδοχές έχουν αποδείξει την αρχή της εργασίας: για παράδειγμα, μια κβαντική αριθμομηχανή πέντε qubit επιτυχώς φέρεσε 15 σε 5 x 3 με τη μέθοδο Shor. Ως εκ τούτου, η απειλή λαμβάνεται πολύ σοβαρά, τόσο περισσότερο από την εμφάνιση ενός κβαντικού υπολογιστή μεγάλης κλίμακας θα καταστεί δυνατή η αποκρυπτογράφηση όλων των σημερινών επικοινωνιών αναδρομικά. Είναι αρκετά ειρωνικό, λόγω των μικρότερων παραμέτρων και των μεγεθών του κλειδιού. Το ECC είναι ακόμη μεγαλύτερο σε κίνδυνο από το RSA: εκτιμάται ότι 1600 qubits θα αρκούσαν

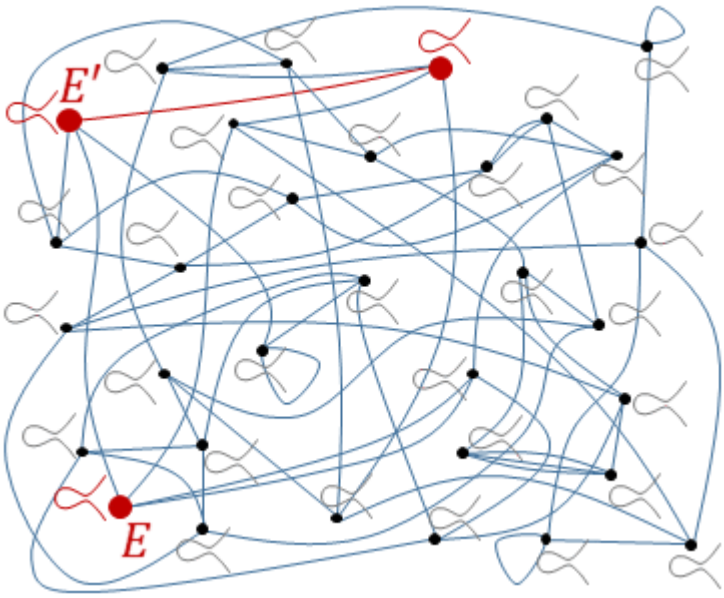
για να σπάσουν το Curve25519, ενώ χρειάζονται 6147 qubits για να σπάσουν το RSA-3072.

Επομένως σε συνέφεια με τα πιο πάνω έρχεται το παράδειγμα χρήσης των ελλειπτικών καμπύλων στον μετακβαντικό κόσμο.Το υποκείμενα σκληρό μαθηματικό πρόβλημα δεν είναι το διακριτό πρόβλημα λογαρίθμου. Αντί να ανακαλύψουμε μια κρυμμένη σχέση μεταξύ δύο σημείων P και P 'σε μία δεδομένη ελλειπτική καμπύλη E, βρίσκουμε μια σύνδεση μεταξύ δύο ελλειπτικών καμπυλών E και E' μέσα σε ένα μεγάλο δοχείο.



Εικόνα 3.13: Σύνδεση Ελλειπτικών καμπύλων Α

Πιο συγκεκριμένα, κάθε ελλειπτική καμπύλη έρχεται εφοδιασμένη με τρεις χάρτες που εκπέμπονται σε άλλες ελλειπτικές καμπύλες, που ονομάζονται δύο ισόγια, οι οποίες συνδέουν το δοχείο με έναν φαινομενικά αδόμητο τρόπο. Με την επανειλημμένη εφαρμογή ενός τυχαίου χάρτη, καταλήγουμε σε μια άλλη καμπύλη E ' και ο στόχος του επιτιθέμενου είναι να ανοικοδομήσουμε τη διαδρομή που ανέλαβε ή τουλάχιστον να βρούμε μια κατάλληλη εναλλακτική διαδρομή. Το ίδιο σύνολο ελλειπτικών καμπυλών συνδέεται επίσης μέσω τριών ισογονιδίων, τα οποία είναι ένα άλλο, αλλά πολύ παρόμοιο είδος χαρτών, από τα οποία τέσσερα εξέρχονται από κάθε καμπύλη. Το ίδιο πρόβλημα μπορεί να διατυπωθεί: το ένα παράγει μια ελλειπτική καμπύλη E 'εφαρμόζοντας μια τυχαία ακολουθία τριών ισογονιδίων ξεκινώντας από το E και πάλι ο στόχος του εισβολέα είναι να μάθει πώς να φτάσει από το E στην E'.



Εικόνα 3.14: Σύνδεση Ελλειπτικών Καμπύλων Β

Η ακριβής μαθηματική ορολογία για το δοχείο είναι μια κλάση υπερηχητικών ισογονιδιών, η οποία αποτελείται από όλες τις υπερηχητικές ελλειπτικές καμπύλες πάνω από ένα πεπερασμένο πεδίο με στοιχεία ρ^2. Εδώ το ρ είναι ένας πρωταρχικός αριθμός μιας μάλλον ειδικής μορφής, που επιλέγεται έτσι ώστε να μπορούν να περιγραφούν όλα τα δύο και τα τρία ισογονίδια με βολικό τρόπο.

Για τα κατάλληλα μεγέθη p τα προαναφερθέντα προβλήματα πιστεύεται ότι είναι εξαιρετικά δύσκολα. Ακόμη και με τη βοήθεια ενός μεγάλου παγκόσμιου κβαντικού υπολογιστή, δηλαδή. Αυτό οδήγησε τον David Jao και τον Luca De Feo να σχεδιάσουν ένα πρωτόκολλο μετά-κβαντικού ανταλλαγής κλειδιών το οποίο υπάγεται στο όνομα Supersingular Isogeny Diffie-Hellman (SIDH).

Στον σημερινό κόσμο, όπου η πληροφορία διαδραματίζει έναν ιδιαίτερα σημαντικό ρόλο, η μετάδοση και η αποθήκευση δεδομένων πρέπει να είναι απόλυτα ασφαλείς. Οι κβαντικοί υπολογιστές αποτελούν σημαντικό παράγοντα τόσο για συμβατικούς αλγορίθμους δημόσιου κλειδιού όπως ο RSA, ο ElGamal,ο ECC και ο DSA όσο και για αλγόριθμους συμμετρικού κλειδιού όπως ο 3DES και ο AES. Κάθε χρόνο φαίνεται ότι πλησιάζουμε στη δημιουργία ενός πλήρως λειτουργικού παγκόσμιου κβαντικού υπολογιστή που μπορεί να χρησιμοποιήσει ισχυρούς κβαντικούς αλγορίθμους όπως ο αλγόριθμος του Shor και ο αλγόριθμος του Grover. Η συνέπεια αυτής της τεχνολογικής πρόβλεψης είναι η απόλυτη κατάρρευση των παρόντων αλγορίθμων δημόσιου κλειδιού

που θεωρούνται ασφαλείς, όπως τα κρυπτοσυστήματα RSA αλλά και στην προκειμένη περίπτωση της υποενότητας αυτής τα κρυπτοσυστήματα Ισομορφισμού Καμπύλης. Εν κατακλείδι αξίζει να σημειωθεί ότι ώς πιθανή απάντηση σε αυτήν την απειλή θα μπορούσε να είναι η εισαγωγή κρυπτογραφικών σχημάτων τέτοιων ώστε να είναι ανθεκτικά στην κβαντική αναμετάδοση, όπως οι μέθοδοι κατανομής κβαντικού κλειδιού όπως το πρωτόκολλο BB84 ,οι μαθηματικές λύσεις αλλά και η η κρυπτογραφία με βάση το πλέγμα, και τέλος οι υπογραφές που βασίζονται σε κατακερματισμό και η κρυπτογραφία με βάση τον κώδικα διώρθωσης σφάλματος κατηγορίες δηλαδή που είδαμε πιο πάνω. Πιο κάτω παρουσιάζεται όμως και μια διαφορετική ιδέα χρήσης του RSA σε μετακβαντική μορφή.

3.7 Δευτερεύον Σημασίας Κρυπτογραφικά Συστήματα-Μετακβαντικός RSA

Γενική Θέση:

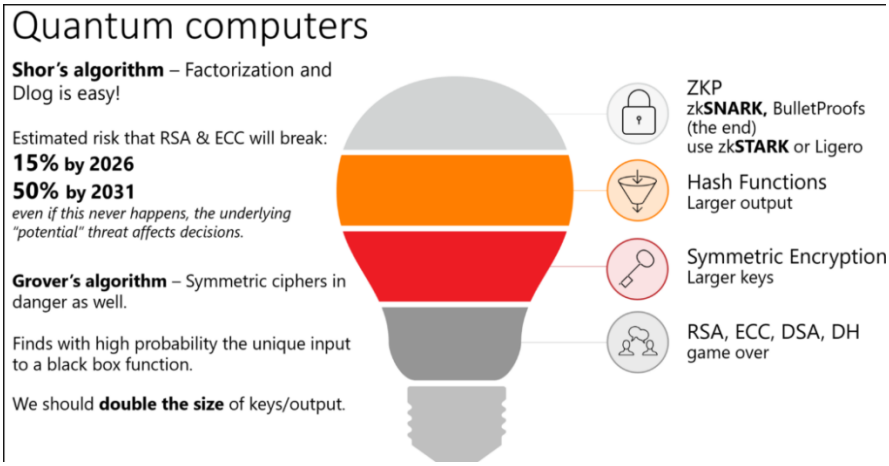
¨Δεν έχει πει κανείς μέχρις στιγμής ότι ο RSA δεν μπορεί να έχει θέση στον μετακβαντικό κόσμο της πληροφορικής.¨

Συγκεκριμένα πολλοί ερευνητές θεωρούν ότι ο RSA και ο τρόπος λειτουργίας του θα σταματήσει και θα παραμείνει απλά ιστορία όταν αρχίσει η χρήση των μετακβαντικών υπολογιστών. Είναι γεγονός ότι δεν υπάρχει μέσα στις αρχικές λύσεις και σχέδια των ερευνητών όμως παρόλα αυτά για τον RSA έχει υπάρξη πρόνοια όπου θα τον καταστήσει ισχυρό απέναντι ακόμα και στους κβαντικούς υπολογιστές. Πολλοί γνωρίζουν ότι ο RSA είναι ο πιο διάσημος αλγόριθμος κρυπτογραφησης αυτή την στιγμή στο εμπόριο. Παρόλα αυτά όμως θα συνεχήσει να είναι εμπορεύσιμος και στο μέλλον χωρίς να είναι υπολογίσιμος αυτή την στιγμή.[66]

Αρχικά η δημοσίευση του 1994 του αλγόριθμου Shor ο οποίος θα θεωρείται η αρχή της κβαντικής κρυπτογραφίας όταν αυτή ξεκινήσει και επίσημα, προκάλεσε ευρέως ισχυρισμούς ότι οι κβαντικοί υπολογιστές θα σκοτώσουν την κρυπτογραφία, ή τουλάχιστον την κρυπτογραφία δημόσιου κλειδιού. Αλλά οι ισχυρισμοί αυτοί ξεπερνούν τα όρια του αλγορίθμου Shor, η τεράστια έρευνα για την κβαντική κρυπτανάλυση δεν έχει προχωρήσει τόσο πολύ για να κλείσει για καλά την θεωρία του αλγορίθμου RSA αν

και η συνηθισμένη σοφία μεταξύ των ερευνητών στη μετακβαντική κρυπτογραφία είναι ότι οι κβαντικοί υπολογιστές θα σκοτώσουν τον RSA , αλλά δεν θα σκοτώσουν την κρυπτογράφηση με βάση το hash, την κρυπτογραφία με βάση τον κώδικα, την κρυπτογράφηση βάσει πλέγματος ή την πολυπαραγοντική κρυπτογράφηση, και κρυπτογραφία των τετραγωνικών εξισώσεων.

Ο αλγόριθμος του Shor διαλύει εύκολα τον RSA όπως χρησιμοποιείται στο Διαδίκτυο σήμερα. Το ερώτημα είναι αν μπορούν να ρυθμιστούν οι παράμετροι RSA έτσι ώστε όλοι οι γνωστοί αλγόριθμοι κβαντικής επίθεσης να είναι ασφαλείς κατά την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αλγόριθμος του Shor ουσιαστικά είναι ένα δημόσιο κλειδί RSA n. Ο αλγόριθμος Shor χρησιμοποιεί μια κβαντική εκτόνωση modulo n.



Εικόνα 3.15: Shor and Post Quantum algorithms

Οι τυποποιημένες τεχνικές για την επιτάχυνση του RSA, όταν ωθούνται στα άκρα τους, δημιουργούν ένα πολύ μεγαλύτερο χάσμα μεταξύ των νόμιμων στα έξοδα του χρήστη και τα έξοδα του εισβολέα. Συγκεκριμένα, για την έκδοση του εγγράφου RSA, το κόστος επίθεσης είναι ουσιαστικά το κόστος χρήσης επί τον εαυτό του. Στο πλαίσιο αυτής της ανάλυσης ασφάλειας, γίνεται λόγος για έναν νέο αλγόριθμο κβαντικής παραγοντοποίησης τον GEECM, που συχνά είναι πολύ πιο γρήγορος από τον Shor αλγόριθμο και όλους τους αλγόριθμους προ κβαντικής παραγοντοποίησης αποδεικνύεται ως ένας από τους κύριους περιορισμούς κατά την επιλογή παραμέτρων για τον μετακβαντικό RSA.[17]

Αυτά τα άκρα απαιτούν επίσης προσεκτική ανάλυση αλγορίθμων για τον βασικό RSA. Έτσι σχετικά με την ανάλυση επιδόσεων, δημιουργείται ένας νέος αλγόριθμος για τη δημιουργία μιας μεγάλης παρτίδας ανεξάρτητης και ομοιόμορφης τυχαίας σειράς

που εκτελείται πιο αποτελεσματικά από οποιονδήποτε γνωστό αλγόριθμο για την παραγωγή τέτοιων πρώτων κάθε φορά.

Στην συνέχεια του υποκεφαλαίου αναλύεται η επιτυχής ολοκλήρωση της πιο δαπανηρής λειτουργίας σε μετακβαντικό RSA, δηλαδή τη δημιουργία ενός δημόσιου κλειδιού ισχυρού απέναντι σε επιθέσεις από κβαντικούς υπολογιστές.

Ο postquantum RSA δεν χαρακτηρίζεται ως ασφαλές σύμφωνα με ορισμούς ασφαλείας που απαιτούν απέναντι σε μεγάλες κβαντικές επιθέσεις.Κάποιος μπορεί να σκεφτεί ότι η τετραγωνική ασφάλεια του μετακβαντικού RSA δεν είναι καλύτερη από την πολύ γνωστή τετραγωνική ασφάλεια του αρχικού συστήματος δημοσίου κλειδιού του Merkle.[67]

Ωστόσο, η γνωστή τετραγωνική ασφάλεια είναι ενάντια στους προκβαντικούς επιτιθέμενους. Οι μελέτες των Brassard, Salvail , Brassard, Hoyer , Kalach, Kaplan, Laplante και Salvail ,δείχνουν ότι οι πιο περίπλοκες παραλλαγές του αρχικού συστήματος δημοσίου κλειδιού του Merkle μπορεί να επιτύχει στους εκθέτες κοντά στο 1,5% έναντι κβαντικών υπολογιστών, αλλά αυτό είναι πολύ κάτω από τον εκθέτη 2% που επιτυγχάνεται με τον μετακβαντικό RSA. Συγκεκριμένα, $(2^{100})^{1/1,5}$ είναι περίπου 100000 φορές μεγαλύτερο από $(2^{100})^{1/2}$.Το μετακβαντικό RSA δεν είναι αυτό που θα αποκαλούσε ελαφριά-οικονομική κρυπτογραφία καθώς το κόστος κάθε νέας κρυπτογράφησης ή αποκρυπτογράφησης είναι στην κλίμακα του $ 1 το χρόνο , Ωστόσο, εάν αυτός είναι ο λιγότερο δαπανηρός τρόπος για την προστασία των πληροφοριών υψηλής ασφάλειας και με αυτό τον τρόπο δεν αποκρυπτογραφούνται από τους μελλοντικούς κβαντικούς υπολογιστές, τότε θα πρέπει να ενδιαφέρει αρκετούς χρήστες. Κάποιος μπορεί να κάνει μια αναλογία εδώ με πλήρως ομοιομορφική κρυπτογράφηση καθώς κάτι ακριβό μπορεί να είναι χρήσιμο αν είναι ο λιγότερο ακριβός τρόπος για να επιτευχθεί ο επιθυμητός στόχος ασφαλείας του χρήστη.

Η κρυπτογραφία βάσει κώδικα και η κρυπτογραφία βάσει πλέγματος έχουν μελετηθεί για πολλά χρόνια και φαίνεται να παρέχουν ασφαλή κρυπτογράφηση με πολύ μικρότερο κόστος από ότι ο μετάκβαντικός RSA. Ο RSA, για τους χρήστες που μπορούν να το αντέξουν οικονομικά, παρέχει υψηλότερο επίπεδο εμπιστοσύνης. Ο μετάκβαντικός RSA είναι επίσης αρκετά ασυνήθιστος όσον αφορά τη δυνατότητα μετακβαντικής κρυπτογράφησης, τις υπογραφές και για μια πιο προηγμένη

κρυπτογραφική λειτουργικότητα όπως οι τυφλές υπογραφές που πρέπει να παρέχονται με έναν οικείο τρόπο από ένα ενιαίο μηχανισμό, και μια πολλαπλά ομοιομορφική μετάθεση καταπακτών.

Το πιο σημαντικό, είναι ότι ο RSA έχει αρκετή ευελιξία για να επιβιώσει από την έλευση των κβαντικών υπολογιστών όμως για να γίνει η επιβίωση του εφικτή θα πρέπει να υποστεί αρκετές μεταρρυθμίσεις.

Ο αλγόριθμος πρώτης γενιάς θα πρέπει, για να συμβάλει στη μείωση της ενέργειας την κατανάλωση και την προστασία του περιβάλλοντος, όλοι οι χρήστες του RSA συμπεριλαμβανομένων των χρηστών του παραδοσιακό προ κβαντικό RSA-θα πρέπει να μεταβιβάσουν την υπολογιστική τους ισχύ σύμφωνα με τα πρότυπα της NIST ή με άλλο αξιόπιστο τρίτο μέρος. Αυτή η βελτίωση της ταχύτητας θα επιτρέψει στους χρήστες να δημιουργούν νέα κλειδιά RSA και να διαγράφουν συχνότερα τα παλιά κλειδιά RSA, περιορίζοντας τη ζημιά από κλοπή κλειδιών. Η πρόκληση εδώ είναι να αποδειχτεί ότι μπορεί να είναι ασφαλής η δημιουργία πολλαπλών χρηστών RSA κλειδιών που διεξάγεται πιο αποτελεσματικά από τη δημιουργία ενός κλειδιού RSA ενός χρήστη.

Μια άλλη φυσική κατεύθυνση είναι η ολοκλήρωση του μετακβαντικού RSA σε πρότυπα πρωτόκολλα Internet όπως το TLS. Αυτή η ολοκλήρωση είναι ήδη σχεδιασμένη και είναι απλή, αλλά απαιτεί την αντιμετώπιση πολλών προκλήσεων σε επίπεδο συστημάτων.
Για κάθε σύγχρονη παραλλαγή του RSA, συμπεριλαμβανομένων των παραλλαγών που εξετάζονται και σε αυτό το υποκεφάλαιο, οι καλύτερες επιθέσεις που είναι γνωστές είναι οι αλγόριθμοι παραγοντοποίησης. Στην συνέχεια αναλύεται η μετακβαντική πολυπλοκότητα του ακέραιου παραγοντοποίησης.

Ο αλγόριθμος Shor αντικαθιστά ολόκληρη την προηγούμενη βιβλιογραφία για τον ακέραιο παράγοντα, καθιστώντας παλιότερους όλους τους προηγούμενους αλγόριθμους παραγοντοποίησης, μελετώντας έτσι την πολυπλοκότητα της παραγοντοποίησης σε έναν μετακβαντικό κόσμο που ισοδυναμεί και με τη μελέτη της πολυπλοκότητας του αλγορίθμου Shor.

Ίσως είναι λιγότερο προφανές ότι υπάρχουν αλγόριθμοι κβαντικής παραγοντοποίησης που είναι, για πολλούς ακεραίους, πολύ γρηγορότεροι από τον αλγόριθμο του Shor και πολύ ταχύτεροι από όλους γνωστούς προ κβαντικούς αλγορίθμους. Αυτοί οι αλγόριθμοι

αποδεικνύονται σημαντικοί μετά την έλευση του κβαντικού RSA, Υπάρχουν δύο σημαντικές τάξεις αλγορίθμων παραγοντοποίησης:
Η πρώτη τάξη αποτελείται από αλγόριθμους που είναι ιδιαίτερα γρήγοροι στην εύρεση μικρών πριμοδοτήσεων όπως είναι η δοκιμαστική διαίρεση, η μέθοδος rho , η μέθοδος p-1 , η μέθοδος p + 1, και η μέθοδος ελλειπτικής καμπύλης (ECM).

Καθένας από αυτούς τους αλγορίθμους μπορεί να αναδιατυπωθεί, χωρίς σοβαρή απώλεια αποδοτικότητας, ως αλγόριθμος δακτυλίου που συνθέτει τις λειτουργίες του δακτυλίου 0,1, +, -, για την παραγωγή ενός μεγάλου ακέραιου διαιρούμενου αριθμού από πολλούς πιο μικρούς. Με την εκτέλεση της ίδιας διαδικασίας, την πλειονότητα των λειτουργιών modulo έναν ακέραιο στόχο n και τον υπολογισμό του μεγαλύτερου κοινού διαιρέτη του αποτελέσματος με n, κάποιος βλέπει εάν το n διαιρείται από οποιοδήποτε από τα ίδια πρωτεύοντα. Για παράδειγμα, η διαίρεση μέσω y έχει ουσιαστικά την ίδια απόδοση ως υπολογιστική gcd {n, 2 · 3 · 5 ···· y 2).

Η σημασία των λειτουργιών του δακτυλίου είναι ότι η εκτέλεση τους modulo n έχει το αποτέλεσμα της εκτέλεσης τους modulo κάθε διάκριση prime p $Z / n \rightarrow Z / p$ και έτσι είναι μια μορφή δακτυλίου.

Η δεύτερη τάξη αποτελείται από αλγόριθμους συνδυασμού συνάφειας όπως την μέθοδο συνεχούς κλάσματος , το τετραγωνικό sieve και το πεδίο αριθμών sieve (NFS) . Αυτοί οι αλγόριθμοι πολλαπλασιάζουν τις διάφορες συναρτήσεις modulo n με αποκτώντας μια αντιστοιχία της μορφής $\alpha^2=b^2 (\text{mod } n)$ και στη συνέχεια ελπίζουμε ότι gcd {n, α-β} είναι μη παράγων ο συντελεστής n. Αυτοί οι αλγόριθμοι δεν θεωρούνται χρήσιμοι ως δακτύλιοι algorithms αφού οι συναρτήσεις modulo n παράγονται κατά τρόπο που εξαρτάται από n και δεν είναι ιδιαίτερα γρήγοροι στην εύρεση μικρών πριμοδοτήσεων.
Για το μεγάλο n, ο καλύτερος αλγόριθμος συνδυασμού συμπίεσης φαίνεται να είναι ο NFS, που (υποθετικά) χρησιμοποιεί $2\,(\ln n)^{1/3+o(1)}$ bits. Για σύγκριση, ο ECM χρησιμοποιεί $2(\lg y)^{1/2+o(1)}$ όταν η παράμετρος ECM έχει επιλεγεί ως περιστασιακή και βρίσκουν κάθε πρωταρχικό $p \leq y$. [68]

Ο αλγόριθμος του Shor αρχίζει με ένα κύκλωμα για να υπολογίσει τη συνάρτηση $x \mapsto (x, {}^{3x} \bmod n)$, όπου το χ είναι ένας ακέραιος ο οποίος έχει περίπου 2lgn δυαδικά ψηφία.

Με μια μικρή πρόσθετη επιβάρυνση εφαρμόζοντας ένα κβαντικό μετασχηματισμό Fourier στην έξοδο, του Shor εμφανίζεται έτσι η περίοδος αυτή της συνάρτησης, δηλαδή της τάξης του 3 modulo n. Αυτή η σειρά είναι ένας διαιρέτης, τυπικά ένας μεγάλος διαιρέτης, φ (n) = # (Z / n) * , και το factoring n με αυτές τις πληροφορίες είναι μια τυπική άσκηση. Υπάρχει ένα τεράστιο χάσμα μεταξύ των λειτουργιών (lg n) $^{2+o(1)}$ qubit που χρησιμοποιούνται από τον Shor και το $2(\lg n)^{1/3+o(1)}$ bit που χρησιμοποιούνται από τον NFS. Για τις λειτουργίες qubit moment φαίνεται απίστευτα ακριβές σε σύγκριση με τις λειτουργίες bit, αλλά η μετά-κβαντική κρυπτογραφία κοιτάζει μπροστά σε ένα μέλλον όπου οι τετριμμένες λειτουργίες είναι προσιτές σε μεγάλη κλίμακα. Σε αυτό το μέλλον φαίνεται ότι ο συνδυασμός συνάφειας καθώς και οι αλγόριθμοι θα έχουν μικρό, αν και κανένα, ενδιαφέρον.[17.68]

Από την άλλη πλευρά, ο αλγόριθμος Shor δεν είναι ανταγωνιστικός σε σχέση με αλγόριθμους δαχτυλιδιών στην εύρεση μικρών αρχικών. Ακόμα κι αν μια λειτουργία qubit είναι τόσο φθηνή όσο λίγο (lg n) $^{2+o(1)}$ οι λειτουργίες qubit είναι τόσο ακριβές όσο (lg n) $^{1+o(1)}$ του δακτυλίου. Στο ECM οι $2(\lg y)^{1/2+o(1)}$ δακτυλιοειδείς λειτουργίες είναι καλύτερες από αυτές για επαρκώς μικρά αρχικά. Η αποκοπή είναι $2^{(\lg \lg n)2+o(1)}$.

Κάποιος μπορεί να σκεφτεί ότι ο αλγόριθμος του Shor μπορεί να τροποποιηθεί για να επωφεληθούμε από ένα μικρό πρωταρχικό διαιρέτη p της n: η συνάρτηση $x \mapsto 3x \bmod p$ έχει μικρή περίοδο και αυτή η περίοδος πρέπει να είναι ορατή για το x που έχει μόνο περίπου 2 lg p bits, αντί των 2 bits που χρησιμοποιήθηκαν από τον Shor. Αυτό θα σώσει έναν παράγοντα 2 ακόμη στην πιο ακραία περίπτωση όπου $p \approx \sqrt{n}$. Η δυσκολία είναι ότι δεν δίνεται η συνάρτηση $x \mapsto \to 3 x \bmod p$. Η λειτουργία $x \mapsto 3 x \bmod n$ έχει μια μικρή ψευδό περίοδο, υπό την έννοια της μετατόπισης της εισόδου που παράγει σχετική παραγωγή, αλλά δεν δίνεται και αυτή η σχέση.

Αν υπήρχε ένας γρήγορος τρόπος για την ανίχνευση ψευδό περιόδων σε σχέση με το άγνωστο τότε θα μπορούσαμε να επιταχύνουμε δραστικά τον αλγόριθμο του Shor βρίσκοντας την ψευδό περίοδο p της απλούστερης λειτουργίας $x \mapsto x \bmod n$. Εάν το x περιορίζεται σε 2 lg p <lg n bits τότε αυτή η συνάρτηση είναι απλά η συνάρτηση της ταυτότητας $x \mapsto x$, που είναι ανεξάρτητη του n, οπότε θα χρειαζόταν κάποιος άλλος τρόπος για να μάθει ο αλγόριθμος n.

GEECM Ένας αλγόριθμος κβαντικού δακτυλίου:. Μια πιο παραγωγική προσέγγιση είναι

να λάβουν τους καλύτερους προ κβαντικούς αλγορίθμους για την εύρεση μικρών πριμοδοτήσεων και για την επιτάχυνση αυτών των αλγορίθμων που χρησιμοποιούν κβαντικές τεχνικές. Υπό τυποποιημένες υποθέσεις, η ECM βρίσκει αρχικές τιμές p ≤ y χρησιμοποιώντας $2(\lg y)^{1/2+o(1)}$ όπως προαναφέρθηκε η μέθοδος rho που βρίσκει τα αρχικά p ≤ y για y $^{1/2+o(1)}$ στις εργασίες του δακτυλίου και η δοκιμαστική διαίρεση στην κλασσική της μορφή βρίσκει τις πρώτες ύλες p ≤ y χρησιμοποιώντας y $^{1+o(1)}$ λειτουργίες του δακτυλίου. Προφανώς, η ECM αντικαθιστά τη μέθοδο rho και την δοκιμή διαίρεσης το y που μεγαλώνει. Η αποκοπή αναφέρεται γενικά με βάση τα περισσότερα στις αναλύσεις του ο για να είναι κάτω από 2^{30}, καθώς και τα πρωταρχικά ενδιαφέροντα σε αυτό το χαρτί που είναι πολύ μεγαλύτερα, επομένως αυτό το έγγραφο επικεντρώνεται στην ECM. [69]

Η υπερσύγχρονη παραλλαγή της ECM είναι η EECM , μια ECM δηλαδή που χρησιμοποιεί καμπύλες Edwards, που εισήχθησαν από τους Bernstein, Birkner, Lange και Peters στις. Η EECM επιλέγει μια καμπύλη Edwards $x^2 + y^2 = 1 + dx^2 y^2$ πάνω από Q, ή γενικότερα μια στριμμένη καμπύλη Edwards, με γνωστό σημείο μη στρέψης P. Η EECM επιλέγει επίσης ένα μεγάλο ακέραιο και χρησιμοποιεί τον νόμο Edwards για να υπολογίσει το sh πολλαπλάσιο του P στην καμπύλη, και συγκεκριμένα την συντεταγμένη x (sP), που αντιπροσωπεύεται ως κλάσμα των ακεραίων. Η έξοδος του αλγόριθμου δακτυλίου είναι ο αριθμητής αυτού του κλάσματος.

Συνολικά ο υπολογισμός παίρνει πολλαπλασιασμούς (7 + o (1)) lg s πιο πάνω από το μισό που είναι κολοβώματα και συγκρίσιμους αριθμούς προσθηκών και αφαιρέσεων.
Αν το s επιλέγεται ως lcm {1,2, ..., z}, τότε lg s ≈ 1,4z έτσι ώστε αυτή η καμπύλη να υπολογιστεί χρησιμοποιείται περίπου 10z πολλαπλασιασμοί. Αν $z \in L^{c+o(1)}$ ως $y \to \infty$, όπου $L = \exp\sqrt{\log y \log\log\log y}$ και c είναι μια θετική πραγματική σταθερά, τότε τυποποιημένες εικασίες υποδηλώνουν ότι κάθε prime p ≤ y βρίσκεται με αυτή την καμπύλη με πιθανότητα $1 / L^{1/2c+o(1)}$.

Οι τυποποιημένες εικασίες υπονοούν επίσης ότι οι καμπύλες είναι σχεδόν ανεξάρτητες. Οι καμπύλες $L^{1/2c+o(1)}$ βρίσκουν κάθε πρωτεύων p με μεγάλη πιθανότητα. Το συνολικό κόστος για να δοκιμαστούν όλες αυτές οι καμπύλες είναι μέσω των λειτουργιών των δακτυλίων $L^{c+1/2c+o(1)}$. Η έκφραση c + 1 / 2c παίρνει την ελάχιστη τιμή 1 για $c = 1 / \sqrt{2}$. το συνολικό κόστος είναι τότε $L\sqrt{2} + o(1)$ δακτύλιος λειτουργίες.

Ο GEECM (Grover plus EECM), με την σειρά του είναι ο αλγόριθμος που χρησιμοποιείται από τους κβαντικούς υπολογιστές για την επιτάχυνση του υπολογισμού του EECM. Ας Θυμηθούμε ότι η μέθοδος του Grover επιταχύνει την αναζήτηση των ριζών των λειτουργιών έτσι ώστε οι είσοδοι σε a και η συνάρτηση f να είναι οι ρίζες του f με πιθανότητα 1 / R, τότε η κλασική αναζήτηση πραγματοποιείται κατά μέσον όρο με εκτιμήσεις R της f, ενώ η μέθοδος του Grover εκτελεί περίπου √R κβαντικές αξιολογήσεις της f. Ειδικότερα, η συνάρτηση f της οποίας η είσοδος είναι μια επιλογή καμπύλης EECM και της οποίας η παραγωγή είναι 0 ακριβώς όταν προκύπτει το αποτέλεσμα της EECM για αυτή την καμπύλη επιλογή έχει ένα nontrivial παράγοντα κοινό με το n. Η EECM βρίσκει μια ρίζα της f με κλασική αναζήτηση. Ενώ η GEECM βρίσκει τη ρίζα της f με τη μέθοδο του Grover. Αν s και z επιλέγονται όπως παραπάνω, τότε οι εισροές στην f είναι οι ρίζες της f με πιθανότητα 1 / $L^{1/2c+o(1)}$, οπότε η GEECM χρησιμοποιεί μόνο κβαντικές εκτιμήσεις της f για $L^{1/4c+o(1)}$ συνολικά στις λειτουργίες του κβαντικού δακτυλίου $L^{c+1/4c+o(1)}$. Η έκφραση c + 1 / 4c παίρνει την ελάχιστη τιμή 1 για c=1/2. το συνολικό κόστος είναι στη συνέχεια μόνο $L^{1+o(1)}$ λειτουργίες δακτυλίου. Συνοψίζοντας, η GEECM μειώνει τον αριθμό των λειτουργιών δακτυλίων από το $L^{\sqrt{2}+o(1)}$ σε $L^{1+o(1)}$, όπου L = exp√log y log log y. Για τον ίδιο αριθμό ενεργειών το GEECM αυξάνει το log y με συντελεστή 2 + o (1), σχεδόν διπλασιάζοντας τον αριθμό των δυαδικών ψηφίων των πρώτων υλών που μπορούν να βρεθούν.

Πως μπορούμε να επεκτείνουμε τον RSA;

Προφανώς, ένα postquantum δημόσιο κλειδί RSA θα πρέπει να είναι αρκετά μεγάλο για να αντισταθεί στις επιθέσεις που περιγράφονται πιο πάνω .Στην συνέχεια πραγματοποιείται μια ανάλυση στους καλύτερους διαθέσιμους αλγόριθμους για την παραγωγή κλειδιών RSA, την κρυπτογράφηση, την αποκρυπτογράφηση, την παραγωγή υπογραφών και την επαλήθευση υπογραφής.[69]

Πριν από την έλευση των κβαντικών υπολογιστών οι κορυφαίες απειλές θεωρούνται ο EECM και ο NFS, καθώς και η εξισορρόπηση αυτών των απειλών που συνεπάγεται ότι κάθε prime p έχει $(\lg n)^{2/3+o(1)}$ bits , δηλαδή, ότι $k \in (\lg n)^{1/3+o(1)}$. Μετά από την έλευση των κβαντικών υπολογιστών ως κορυφαίες απειλές θεωρούνται ο αλγόριθμος GEECM και Shor, και η εξισορρόπηση αυτών των απειλών συνεπάγεται από κάθε prime p έχει μόνο $(\lg \lg n)^{2+o(1)}$ bits, δηλαδή ότι $k \in (\lg n)/(\lg \lg n)^{2+o(1)}$. Όσο αφορά τον RSA και την παραγωγή, την αποκρυπτογράφηση και την δημιουργία υπογραφών λαμβάνονται τότε

$(\lg n)^{1+o(1)}$ bit πράξεις.

Για την δημιουργία κλειδιών στον RSA ισχύει ότι ένα δημόσιο κλειδί k-prime exponent-3 RSA είναι ένα προϊόν των k ξεχωριστών πριμοδοτήσεων p που συμφωνούν με το 2 modulo 3. Ειδικότερα, ένα μετακβαντικό κλειδί. Το δημόσιο κλειδί RSA n με την σειρά του είναι ένα προϊόν k με ξεχωριστές πριμοδοτήσεις p σύμφωνες με 2 modulo 3,όπου κάθε prime p έχει $(\lg \lg n)^{2+o(1)}$ bits.

Οι τυποποιημένες τεχνικές πρώτης γενιάς χρησιμοποιούν λειτουργίες $(\lg p)^{3+o(1)}$ bit. Το θέμα είναι ότι πρέπει να προσπαθήσουμε για τους log p που είναι τυχαίοι αριθμοί προτού βρεθεί ένας πρωταρχικός για τον έλεγχο της πρωτοτυπίας που έχει παρόμοιο κόστος σε ένα μονό μοντέλο exponentiation p.

Μια τυποποιημένη μέθοδος είναι να πραγματοποιηθεί έλεγχος εάν το p είναι διαιρέσιμο από οποιαδήποτε αρχή-όριο, ας πούμε y. Η πιθανότητα ενός τυχαίου ακέραιου να επιβιώνει αυτό το τεστ διαχωρισμού είναι περίπου 1/log y, μειώνοντας την αρχική ομάδα τυχαίων αριθμών log p σε (log p)/log y τυχαίους αριθμούς και την εξοικονόμηση ενός συνολικού παράγοντα log y εάν η δοκιμή η διαίρεση δεν αποτελεί εμπόδιο. Η συμβατική άποψη είναι ότι η διατήρηση του κόστους κατά την δοκιμή ή διαίρεση υπό έλεγχο απαιτεί y για να επιλεγεί ως πολυώνυμο σε lg p, και να γίνει εξοικονόμηση ενός παράγοντα μόνο Θ(lg lg p) που συνεπώς απαιτεί ακόμα λειτουργίες $(\lg p)^{3+o(1)}$ bit.
Μια μη τυποποιημένη μέθοδος αλγορίθμου πρόκειται να αντικαταστήσει τη δοκιμαστική διαίρεση με δοκιμή μιας παρτίδας με διαίρεση ή ανίχνευση της ομαλότητας της. Ο αλγόριθμος α αφορά την πεπερασμένη ακολουθία S θετικών ακέραιων αριθμών και ένα πεπερασμένο σύνολο P των αρχικών τιμών με ευρήματα για τον μεγαλύτερο P ομαλό διαιρέτη κάθε ακέραιου στο S" χρησιμοποιώντας μόνο b $(\lg b)^{2+o(1)}$ bit όπου β είναι ο συνολικός αριθμός των δυαδικών ψηφίων στα P και S. Συγκεκριμένα, αν P είναι το σύνολο πριμοδοτήσεων μέχρι και y και S είναι μια ακολουθία των ακέραιων Θ(y/lg p) όπου κάθε b έχει θ(lg p), τότε το b είναι Θ(y) και αυτός ο αλγόριθμος χρησιμοποιεί μόνο $y(\lg y)^{2+o(1)}$ για $(\lg p)(\lg y)^{2+o(1)}$ λειτουργίες bit για κάθε στοιχείο του S. Το μεγαλύτερο μέρος του S μπορεί να χωριστεί τμηματικά σε άλλα υποτμήματα μεγέθους Θ(y/lg p), δημιουργώντας το ίδια απόδοση ανά στοιχείο του S.

Για να γίνει ακόμα καλύτερο, θεωρούμε ότι το αρχικό μέγεθος του S είναι τουλάχιστον $2^{2^{\alpha}}$, και εφαρμόζουμε διαδοχικά μια ανίχνευση ομαλότητας της παρτίδας για $y = 2^{(2)o}$, $y= 2^{(2)1}$, $y = 2^{(2)2}$,και ούτω καθεξής μέσω $y = 2^{2^{\alpha}}$. Κάθε βήμα κοστίζει περίπου το ήμισυ των υπόλοιπων στοιχείων του S ως σύνθετα υλικά. το επόμενο βήμα κοστίζει περίπου τέσσερις φορές περισσότερο αλλά εφαρμόζεται μόνο στα μισά στοιχεία. Το συνολικό κόστος είναι απλά $(\lg p)\ (2^{\alpha})^{1+0(1)}$ bit λειτουργίες για κάθε ένα από τα αρχικά στοιχεία του S. Κάθε ένα από τα αρχικά στοιχεία έχουν πιθανότητα περίπου $1/2^{\alpha}$ να επιβιώσουν από αυτή τη διαδικασία και προκαλώντας μια εκτόνωση, η οποία κοστίζει $(\lg p)^{2+0(1)}$ bit λειτουργίες. Επιλέγοντας $2^{\alpha} \in (\lg p)^{0,5+0(1)}$ εξισορροπεί αυτές τις δαπάνες ως $(\lg p)^{1,5+0(1)}$ για κάθε ένα από τα πρωτότυπα στοιχεία του S, δηλαδή, $(\lg p)^{2,5+0(1)}$ για κάθε πρωτεύον παραγόμενο.

Στο πλαίσιο της ανάπτυξης του μετακβαντικού RSA η υπόθεση για το αρχικό μέγεθος του S ικανοποιείται εφόσον δημιουργηθούν $(\lg n)^{1+0(1)}$ primes, οπότε το αρχικό μέγεθος του S είναι $(\lg n)^{1+0(1)}$, το οποίο είναι τουλάχιστον $2^{2^{\alpha}}$ για $2^{\alpha} \in (1 + o(1))\ \lg \lg n$ όπου η επιλογή α ικανοποιεί $2^{\alpha} \in (\lg p)^{0,5+0(1)}$ από το $\lg p \in (\lg \lg n)^{2+0(1)}$. Οι πριμοδοτήσεις είναι επίσης $(\lg n)/ k \in (\lg p)^{1+0(1)}$ για κάθε p, έτσι ώστε να δημιουργηθεί στο k τα primes για να χρησιμοποιηθούν $k (\lg p)^{2,5+0(1)} = (\lg n) (\lg p)^{1,5+0(1)} = (\lg n) (\lg \lg n)^{3+0(1)}$ bit.

Ο υπολογισμός του n γίνεται πολλαπλασιάζοντας αυτά τα αρχικά τα οποία χρησιμοποιούν $(\lg n)(\lg \lg n)^{2+0(1)}$ bit λειτουργίες που χρησιμοποιούν τυπικές τεχνικές γρήγορης αριθμητικής. Σε αυτό το επίπεδο λεπτομέρειας δεν έχει σημασία αν κάποιος χρησιμοποιεί το κλασικό Schönhage αλγόριθμο πολλαπλασιασμού Strassen ή τον αλγόριθμο πολλαπλασιασμού του Fürer, γιατί ο συνολικός αριθμός των λειτουργιών bit για την παραγωγή κλειδιών είναι ουσιαστικά γραμμικός στο lg n. Για λόγους σύγκρισης, η συνηθισμένη εικόνα είναι ότι η πρωτογενής γενιά είναι πολύ μεγαλύτερη σε ακρίβεια από οποιοδήποτε από τα άλλα βήματα στον RSA.

Μπορεί κανείς να επιδιώξει να επιταχύνει περαιτέρω την παραγωγή κλειδιών χρησιμοποιώντας την ιδέα του Takagi του επιλέγοντας n ως $p^{\kappa-1} q$.

Οι παλαιότεροι μηχανισμοί χρησιμοποιούν την RSA για να κρυπτογραφήσουν απευθείας το μήνυμα του χρήστη, αυτό απαιτεί προσεκτική συμπλήρωση και κρυπτογράφηση του μηνύματος. Οι νεότεροι μηχανισμοί δημιουργούν ένα μυστικό κλειδί (για παράδειγμα, ένα κλειδί AES), χρησιμοποιώντας το μυστικό κλειδί για την

κρυπτογράφηση και την εξακρίβωση της ταυτότητας του μηνύματος του χρήστη και τη χρήση του RSA για να αποκρυπτογραφήσουν το μυστικό κλειδί αυτό στην απλούστερη μορφή, καθώς το μυστικό κλειδί είναι ήδη τυχαίο. Οι νεότεροι μηχανισμοί όπως ο RSA-KEM της Shoup απλά χρησιμοποιεί RSA για να κρυπτογραφήσει lgn bits τυχαίων δεδομένων, κατακερματίζοντας τα τυχαία δεδομένα που θέλουν να αποκτήσουν ένα μυστικό κλειδί και να χρησιμοποιήσουν το μυστικό κλειδί για την κρυπτογράφηση και τον έλεγχο της ταυτότητας των μηνυμάτων του χρήστη. Για λόγους απλότητας το χαρτί αυτό παίρνει το τελευταίο πλησίον του.

Η παραγωγή μεγάλων ποσοτήτων των πραγματικών τυχαίων δεδομένων είναι δαπανηρή. Ευτυχώς, τα πραγματικά με τα τυχαία δεδομένα μπορούν να προσομοιωθούν με ψευδοτυχαία δεδομένα που παράγονται από την κρυπτογράφηση του μηνύματος a από ένα πολύ μικρότερο κλειδί.

Στο πλαίσιο της ανάλυσης του μετακβαντικού RSA έχουμε b∈Θ(lg lg n) έτσι ώστε να δημιουργούμε lg n με ένα ψευδοτυχαίο κόστος bits (lg n)(lg lg n) $^{1+0(1)}$ bit. Τα ίδια κρυπτοκείμενα μπορούν επίσης να μετατραπούν μέσω των λειτουργιών κατακερματισμού με μόνο απώλεια σταθερού παράγοντα σε (lg n)(lg lg n) $^{1+0(1)}$ bit.
Ο πολλαπλασιασμός λαμβάνει επίσης (lg n)(lg lg n) $^{1+0(1)}$ bit λειτουργίες. Η κοπή,
το modulo n, ο πολλαπλασιασμός και ένα άλλο modulo n μειώνονται μαζί με τις
(lg n)(lg lg n) $^{1+0(1)}$ bit λειτουργίες. Το συνολικό κόστος της κρυπτογράφησης RSA είναι ως εκ τούτου (lg n)(lg lg n) $^{1+0(1)}$ λειτουργίες συν το κόστος κρυπτογράφησης και πιστοποίησης του μηνύματος του χρήστη κάτω από το μυστικό κλειδί που προκύπτει.
Η αποκρυπτογράφηση με την σειρά της είναι πιο περίπλοκη αλλά όχι δεν είναι πιο αργή. Λειτουργεί ως εξής. Αρχικά, πραγματοποιείται μείωση στο modulo ciphertext για όλους τους βασικούς διαιρέτες του n. Αυτό χρειάζεται (lg n)(lg lg n)$^{2+0(1)}$ λειτουργίες bit χρησιμοποιώντας ένα υπόλοιπο δέντρο ή ένα κλιμακωτό υπόλοιπο του δέντρου.

Μια μονάδα ρίζας κύβου modulo p παίρνει (lg p) $^{2+0(1)}$ bit λειτουργίες, έτσι ώστε όλες οι ρίζες κύβων μαζί παίρνουν (lg n)(lg lg n)$^{2+0(1)}$bit λειτουργίες. Στη συνέχεια γίνεται ανοικοδόμηση της ρίζας του κύβου modulo n. Αυτό παίρνει λειτουργίες (lg n)(lg lg n) $^{2+0(1)}$ bit χρησιμοποιώντας γρήγορη παρεμβολή. Στο τέλος γίνεται καταστροφή της ρίζας του κύβου. Το σύνολό του κόστους της αποκρυπτογράφησης RSA είναι (lg n)(lg lg n) $^{2+0(1)}$ με bit λειτουργίες, συν το κόστος της επαλήθευσης και την αποκρυπτογράφηση του μηνύματος του χρήστη κάτω από το μυστικό κλειδί που προκύπτει.

Όσο αφορά κατά την φάση της δημιουργίας και επαλήθευσης της μετακβαντικής υπογραφής με τον RSA ασχολούμαστε με τυποποιημένα συστήματα γεμίσματος RSA όπου οι υπογραφές περιλαμβάνουν τις ίδιες λειτουργίες που αναφέρθηκαν παραπάνω, όπως το hashing στο a με σύντομη συμβολοσειρά και χρησιμοποιώντας έναν κρυπτογράφο ροής για να γίνει επέκταση στην σειρά αυτή με μεγάλη χρονική διάρκεια διάρκεια.

Οι τελικές ταχύτητες, όπως ήταν αναμενόμενο είναι (lg n)(lg lg n) $^{2+0(1)}$ με πράξεις bit προς δημιουργία για την επαλήθευση της μιας υπογραφής, συν το κόστος της απόσπασης του μηνύματος του χρήστη.

Συνοψίζοντας όσα έχουμε τονίσει πιο πάνω αναλύουμε τα εξής:

- ο αλγόριθμος Shor παίρνει (lg n) $^{2+0(1)}$ qubit πράξεις από έναν παράγοντα n.
- Αν οι πρωταρχικοί διαιρέτες του n είναι πολύ μικρότεροι τότε ο GEECM γίνεται μεγαλύτερη απειλή από τον αλγόριθμο του Shor.
- Στην συνέχεια αποδείχτηκε ότι σύμφωνα με τον (1g n)(lg lg n)$^{o(1)με\ (0+,1+,2+)}$ μπορούν να εκτελεστούν χρησιμοποιώντας όλες τις λειτουργίες του RSA για τη δημιουργία κλειδιών, για αποκρυπτογράφηση και την παραγωγή υπογραφών καθώς και για κρυπτογράφηση και την επαλήθευση της υπογραφής.

Μελλοντικός σχεδιασμός είναι η μελέτη και ανάπτυξη ενός μετακβαντικού κλειδιού κλειδιού RSA 1-terabyte που θα κατασκευαστεί από 4096 bit primes.

Με τα μέχρι στιγμής υπάρχοντα γνωρίζουμε ότι οι τυπικές αναλύσεις κόστους πριν από το κβάντο καταλήγουν στο συμπέρασμα ότι τα 4096bit RSA παρέχουν περίπου 2^{140} ασφάλεια έναντι όλων των διαθέσιμων αλγορίθμων.

- Ο ECM είναι γνωστό ότι είναι κατώτερος από τον NFS σε τέτοια μεγέθη όπου προφανώς χρησιμοποιεί ακόμη περισσότερες λειτουργίες των 2^{140} bit για να βρει ως πρώτες τιμές 2048bit. Ο ECM θα ήταν ακόμη πιο αργός με έναν μεγαλύτερο συντελεστή, απλά και μόνο επειδή η αριθμητική του είναι πιο αργή διαδικασία. Ωστόσο, η εξέλιξη από τον ECM στον GEECM μειώνει το επίπεδο απειλής μετά την έλευση των κβαντικών υπολογιστών.

Κεφάλαιο 4

Ο NIST και η προκύρηξη των Μετακβαντικών Αλγορίθμων

4.1 Εισαγωγή

Όπως έχουμε αναφέρει προ πολλού στα προηγούμενα κεφάλαια, ο NIST ιδρύθηκε το 1901, και είναι μία μη ρυθμιστική ομοσπονδιακή υπηρεσία εντός του Υπουργείου Εμπορίου των ΗΠΑ. Η αποστολή του NIST είναι η προώθηση της καινοτομίας των ΗΠΑ αρχικά αλλά και μετέπειτα όλου του κόσμου της πληροφορικής και της βιομηχανικής ανταγωνιστικότητας μέσω των προηγμένων επιστημών για μετρήσεις, της εισαγωγής προτύπων και της τεχνολογίας, με τρόπους οι οποίοι είναι δυνατόν να ενισχύουν την οικονομική ασφάλεια και τη βελτίωση της ποιότητας της ζωής του ανθρώπινου γένους . Το NIST εκτελεί την αποστολή του μέσα από διάφορα προγράμματα-διακλαδώσεις του τρόπου λειτουργίας του. Τα προγράμματα αυτά έχουν ως εξής:

1. NIST Laboratories, που διεξάγουν έρευνες παγκόσμιας κλάσης, συχνά σε στενή συνεργασία με τη βιομηχανία, και έτσι προωθούν την τεχνολογία των υποδομών της χώρας και βοηθούν τις εταιρείες των ΗΠΑ να βελτιώνουν συνεχώς τα προϊόντα και τις υπηρεσίες τους.

2. Hollings Manufacturing Extension Partnership. Πρόκειται για ένα πανεθνικό δίκτυο τοπικών κέντρων που προσφέρουν τεχνική και επιχειρησιακή βοήθεια στους μικρότερους κατασκευαστές ώστε να τους βοηθήσουν να δημιουργήσουν και να

διατηρήσουν τις θέσεις εργασίας, και να αύξησουν τα κέρδη τους και να εξοικονομήσουν χρόνο και χρήματα.

3. The Baldrige Performance Excellence Program. Το πρόγραμμα αυτό είναι υπεύθυνο για την προώθηση της αριστείας των επιδόσεων μεταξύ των κατασκευαστών, εταιρειών παροχής υπηρεσιών,εκπαιδευτικών ιδρυμάτων, παρόχους υγειονομικής περίθαλψης, καθώς και μη κερδοσκοπικούς οργανισμούς

Ο οργανισμός του NIST στεγάζεται σε τοποθεσίες:

- Η μία είναι στο Gaithersbur, Md, (έδρα 578 στρεμμάτων)
- Και η άλλη στο Boulder, Colo, (208 στρέμματα).

Ο NIST χάρη στο έργο το οποίο προσφέρει αυτή την στιγμή ,απασχολεί περίπου 3.400 επιστήμονες, μηχανικούς, τεχνικούς και διοικητικό προσωπικό. Ακόμα ο NIST φιλοξενεί επίσης περίπου 2.700 συνεργάτες από την ακαδημαϊκή κοινότητα, τη βιομηχανία, και άλλες κυβερνητικές υπηρεσίες οι οποίοι συνεργάζονται με το προσωπικό και έχουν πρόσβαση στις εγκαταστάσεις. Επιπλέον, οι εταίροι του NIST είναι περισσότεροι από 1.300 ειδικοί επιστήμονες σε 400 σημεία εξυπηρέτησης σε όλη τη χώρα της Αμερικής αλλά και τον υπόλοιπο κόσμο.

4.2 Ο NIST στην Μετακβαντική Κρυπτογραφία [70]

Τα τελευταία χρόνια, πραγματοποιήθηκε σημαντική έρευνα στους κβαντικούς υπολογιστές και τις μηχανές οι οποίες σχετίζονται με τα κβαντομηχανικά φαινόμενα για την επίλυση διάφορων μαθηματικών προβλημάτων που είναι δύσκολα για συμβατικούς υπολογιστές. Επομένως σύντομα θα κατασκευαστούν κβαντικοί υπολογιστές μεγάλης κλίμακας,που θα θέσουν σε κίνδυνο την ασφάλεια πολλών συχνά χρησιμοποιούμενων κρυπτογραφικών αλγορίθμων. Συγκεκριμένα, οι κβαντικοί υπολογιστές θα σπάσουν εντελώς πολλά κρυπτοσυστήματα δημόσιου κλειδιού, συμπεριλαμβανομένων κρυπτοσυστημάτων απλών RSA, DSA και ελλειπτικής καμπύλης. Αυτά τα κρυπτοσυστήματα χρησιμοποιούνται για την υλοποίηση ψηφιακών υπογραφών και την καθιέρωση κλειδιών και διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της εμπιστευτικότητας και της αυθεντικότητας των επικοινωνιών στο Διαδίκτυο και σε άλλα δίκτυα.

Αυτή η εξέλιξη δεν θα μπορούσε να μην περάσει απαρατήρητη από τους αρμόδιους

ερευνητές οι οποίοι έχουν ήδη αρχίσει να ερευνούν τη μετακβαντική κρυπτογραφία (PQC) που ονομάζεται επίσης κβαντοαντοχή ή κβαντοασφαλή κρυπτογραφία.

Έτσι ο NIST το 2016 ξεκίνησε μια διαδικασία για την ανάπτυξη νέων προτύπων κρυπτογραφίας. Αυτά τα νέα πρότυπα θα χρησιμοποιηθούν ως κβαντο ανθεκτικά αντίστοιχα σε υπάρχοντα πρότυπα, συμπεριλαμβανομένων των συστημάτων ψηφιακής υπογραφής που ορίζονται στη Δημοσιευμένη Πρότυπη Επεξεργασία Πληροφοριών (FIPS) 186 και στα συστήματα δημιουργίας κλειδιών που καθορίζονται στο NIST Special Publications (SP) 800-56 A και B.Τα πρότυπα θα δημοσιευθούν ως Ομοσπονδιακά Πρότυπα Επεξεργασίας Πληροφοριών (FIPS) ή Ειδικές Εκδόσεις (SPS).
Ο στόχος αυτής της έρευνας είναι να αναπτυχθούν κρυπτογραφικοί αλγόριθμοι που να είναι ασφαλείς τόσο έναντι κβαντικών όσο και κλασικών υπολογιστών. Αυτοί οι αλγόριθμοι θα μπορούσαν να χρησιμεύσουν ως αντικαταστάτες για τα τρέχοντα κρυπτοσυστήματα του δημόσιου κλειδιού για να προετοιμαστούν για την πιθανότητα να γίνουν πραγματικότητα οι μεγάλης κλίμακας κβαντικοί υπολογιστές.

Ο NIST ζητάει επομένως προτάσεις για μετακβαντικά κρυπτοσυστήματα και θα ζητήσει σχόλια από το κοινό στο πλαίσιο της διαδικασίας αξιολόγησης. Ο NIST ακόμα αναμένει να πραγματοποιήσει πολλαπλούς γύρους αξιολόγησης, σε διάστημα **τριών έως πέντε ετών**. Ο στόχος αυτής της διαδικασίας είναι να επιλεγεί ένας αριθμός αποδεκτών υποψήφιων κρυπτοσυστημάτων για τυποποίηση. Θεωρούν ακόμα ότι η διαδικασία αξιολόγησης αυτών των μετακβαντικών κρυπτοσυστημάτων μπορεί να είναι σημαντικά πιο πολύπλοκη από την αξιολόγηση των υποψηφίων SHA-3 και AES. Ένας λόγος είναι ότι οι απαιτήσεις για κρυπτογράφηση δημόσιου κλειδιού και ψηφιακές υπογραφές είναι πιο περίπλοκες. Ένας άλλος λόγος είναι ότι η τρέχουσα επιστημονική κατανόηση της ισχύος των κβαντικών υπολογιστών δεν είναι καθόλου ολοκληρωμένη. Τέλος, μερικά από τα υποψήφια κβαντικά κρυπτοσυστήματα μπορεί να έχουν τελείως διαφορετικά χαρακτηριστικά σχεδιασμού και μαθηματικά θεμέλια, έτσι ώστε η άμεση σύγκριση των υποψηφίων να είναι δύσκολη ή αδύνατη.

Πιο κάτω στον πίνακα που ακολουθεί εμφανίζεται το χρονοδιάγραμμα που θεωρούν στον NIST ότι θα τηρηθεί προκειμένου να γίνει η σωστή διαδικασία από την στιγμή της προκύρηξης του διαγωνισμού μέχρι και την επιλογή των σωστών αλγόριθμων που θα πρωταγωνιστίσουν στο μετακβαντικό μέλλον.

Timeline and Workshops Table (Πίνακας χρονοδιαγράμματος και εργασιών)		
Α/Α	**ΗΜΕΡΟΜΗΝΙΑ**	**ΑΝΑΚΟΙΝΩΣΗ**
1	**2-3/4/2015**	**Workshop on Cybersecurity in a Post-Quantum World**
2	**24-26/2/2016**	**Nist Presentation at PQCrypto 2016**
3	**28/4/2016**	**Nist releases NISTIR 8105, Report on Post Quantum Cryptography**
4	**20/12/2016**	**Formal Call for Proposals**
5	**30/11/2017**	**Deadline for submissions**
6	**4/12/2017**	**NIST Presentation at AsiaCrypt 2017**
7	**21/12/2017**	**Round 1 algorithms annoynced**
8	**11/4/2018**	**NIST Presentation at PQCrypto 2018**
9	**11-13/4/2018**	**First PQC Standardization Conference**
10	**30/1/2019**	**Second Round Candidates announced**
11	**22-24/8/2019**	**Second PQC Standarization Conference**
12	**2020-2021**	**Round 3 Begins or select Algorithms**
13	**2022-2024**	**Draft Standards Avaliable**

Όπως παροκύπτει από το πιο πάνω χρονοδιάγραμμα εργασιών η επιλογή θα γίνει μέσω 3 γύρων σύγκρισης. Στις 21/12/2017 έγινε η προκύρηξη για τον πρώτο γύρο παράθεσης των αλγορίθμων. Οι αλγόριθμοι αυτοί δεν ήταν απαραίτητο να βασίζονται στις κύριες κατηγορίες μετακβαντικών αλγορίθμων που αναλύσαμε στα πιο πάνω κεφάλαια καθώς επρόκειτο για τις σκέψεις και τους σχεδιασμούς του κάθε ερευνητή. Όταν συμπληρώθηκε η καταληκτική ημερομηνία παράδωσης των αλγορίθμων αυτών τότε οι αλγόριθμοι που προτάθηκαν αρχικά αποτέλεσαν και την πρώτη λίστα. Η λίστα αυτή του πρώτου γύρου έχει ως εξής.

Round 1 List:

1. BIG QUAKE
2. BIKE
3. CFPKM
4. Classic McEliece

5. Compact LWE
6. CRYSTALS-DILITHIUM
7. CRYSTALS-KYBER
8. DAGS
9. Ding Key Exchange
10. DME
11. DRS
12. DualModeMS
13. Edon-K
14. EMBLEM and R.EMBLEM
15. FALCON
16. FrodoKEM
17. GeMSS
18. Giophantus
19. Gravity-SPHINCS
20. Guess Again
21. Gui
22. HILA5
23. HiMQ-3
24. HK17
25. HQC
26. KCL
27. KINDI
28. LAC
29. LAKE
30. LEDAkem
31. LEDApkc
32. Lepton
33. LIMA
34. Lizard
35. LOCKER
36. LOTUS
37. LUOV
38. McNie
39. Mersenne -756839

40. MQDSS
41. NewHope
42. NTRUEncrypt
43. PqNTRUSign
44. NTRU-HRSS-KEM
45. NTRU Prime
46. NTS-KEM
47. Odd Manhattan
48. Ouroboros-R
49. Picnic
50. Post-quantum RSA Encryption
51. Post-quantum RSA Signature
52. PqsigRM
53. QC-MDPC KEM
54. qTESLA
55. RaCoSS
56. Rainbow
57. Ramstake
58. RankSign
59. RLCE-KEM
60. Round2
61. RQC
62. RVB
63. SABER
64. SIKE
65. SPHINCS+
66. SRTPI
67. Three Bears
68. Titanium
69. WalnutDSA

Προς το παρόν, υπάρχουν αρκετά κβαντικά κρυπτοσυστήματα που έχουν προταθεί, συμπεριλαμβανομένων κρυπτοσυστημάτων βασισμένων σε πλέγμα, κρυπτοσυστημάτων βασισμένων σε κώδικα, πολυμεταβλητών κρυπτοσυστημάτων, υπογραφών που βασίζονται σε κατακερματισμό και άλλων. Κάποια από τα πιο πάνω

κρυπτοσυστήματα που έχουν προταθεί έχουν ήδη αναλυθεί σε άλλες υποενότητες όπως είναι το Rainbow ,ο McEliece και ο Post Quantum RSA. Ωστόσο, για τις περισσότερες από αυτές τις προτάσεις, απαιτείται περαιτέρω έρευνα για να αποκτήσουν περισσότερη εμπιστοσύνη στην ασφάλεια τους ιδίως εναντίον αντιπάλων με κβαντικούς υπολογιστές και να βελτιώσουν την απόδοσή τους. Από τους πιο πάνω 69 αλγόριθμους που προτάθηκαν μετά από διάφορα Comments και θέσεις των αναγνωστών αλλά και αξιολογήσεις των ερευνητών και συνεργατών του NIST προχώρησαν στον δεύτερο γύρο μόλις 26 από τις 69 προτάσεις.

4.3 Που βρίσκεται το 2019 ο NIST και με ποιες θέσεις

Όπως προαναφέραμε στην προηγούμενη υποενότητα μετά το Round 1 και την αξιολόγηση τους στις 11 με 13 Απριλίου του 2019 έγινε επιλογή των αλγόριθμων που θα προχωρήσουν στον δεύτερο γύρο . Τα κρυπτοσυστήματα που προχωρούν μειώθηκαν σε 26 και στις 30 Ιανουαρίου του 2019 με σχετική ανακοίνωση που εξέδωσε ο NIST προχώρησε στην δημοσίευση επίσημα της λίστας με τα 26 κρυπτοσυστήματα τα οποία μπορούν αυτή την δεδομένη στιγμή να αξιολογηθούν από τους ερευνητές του οργανισμού, όλους τους συνεργάτες του NIST ακόμα και από τους αναγνώστες και γνώστες των αντικειμένων αυτών. Η αξιολόγηση αυτή θα τελειώσει στις 22 Αυγούστου αφού τις μέρες 22 με 24 Αυγούστου 2019 θα υπάρξει και η σχετική ανακοίνωση με τους αλγόριθμους που δικαιωματικά θα επιλεχτούν και πάλυ να περάσουν στον τρίτο και τελικό γύρο του διαγωνισμού του NIST. [71,76]

Πιο κάτω παρατίθενται όλοι οι αλγόριθμοι (και οι 26 στο μέγεθος) που έχουν την τιμή να συνεχίζουν στον δεύτερο γύρο του διαγωνισμού που τρέχει την δεδομένη στιγμή ο NIST. Αξίζει να σημειωθεί ότι αυτή την φορά ο NIST ξεχώρησε σε δύο κύριες κατηγορίες τα κρυπτοσυστήματα. Τα ξεχώρησε σε κρυπτοσυστήματα δημόσιου κλειδιού κρυπτογράφησης και κρυπτοσυστήματα ψηφιακών υπογραφών.

Public-key Encryption and Key-establishment Algorithms: [72,73,74,75]

1. BIKE

Ο αλγόριθμος BIKE ουσιαστικά είναι μια σειρά αλγορίθμων που στηρίζει την λειτουργία του στους οιονικούς (Quasi) κυκλικούς κώδικες μέτρησης ισοτιμίας (QC-MDPC) που

μπορούν να αποκωδικοποιηθούν χρησιμοποιώντας τεχνικές αποκωδικοποίησης bit flipping decoding.

Quasi Κυκλικοί κωδικοί:

Είναι ουσιαστικά μια δυαδική μήτρα κυκλοφορίας η οποία είναι μια τετραγωνική μήτρα σε κάθε σειρά έτσι που η περιστροφική μήτρα του στοιχείου να είναι στα δεξιά της προηγούμενης σειράς. Ορίζεται πλήρως από την πρώτη του σειρά.Μια μήτρα κυκλοφορίας ένος μπλοκ σχηματίζεται από κυκλικά τετραγωνισμένα τεμάχια όμοιου μεγέθους. Το μέγεθος των κυκλοφορούντων τεμαχίων ονομάζεται σειρά. Ο δείκτης μίας μήτρας κυκλικού μπλοκ είναι ο αριθμός των κυκλοφορητών σε μια σειρά.

Κωδικοί QC-MDPC:

Ένας δυαδικός κώδικας MDPC (Moderate Density Parity Check-έλεγχος ισοτιμίας μέτρησης) είναι ένας δυαδικός γραμμικός κώδικας στον οποίο παραδέχεται ένας κάπως αραιός πίνακας ελέγχου ισοτιμίας, με τυπική πυκνότητα παραγγελίας O $(1/\sqrt{n})$. Η ύπαρξη ενός τέτοιου πίνακα επιτρέπει τη χρήση επαναληπτικών αποκωδικοποιητών παρόμοιους με εκείνους που χρησιμοποιούνται για τους κώδικες LDPC

Ο BIKE βασίζεται αποκλειστικά σε εφήμερα κλειδιά, που σημαίνει ότι παράγεται ένα νέο ζεύγος κλειδιών σε κάθε ανταλλαγή κλειδιών. Με αυτόν τον τρόπο, η επίθεση GJS, η οποία εξαρτάται από την παρατήρηση ένας μεγάλου αριθμού αποτυχιών αποκωδικοποίησης για ένα ίδιο ιδιωτικό κλειδί δεν ισχύει. Για τον BIKE έχουν κατασκεθαστεί τρεις διαφορετικές παραλλαγές του. Ο BIKE-1, BIKE-2 και BIKE-3. Όλες οι παραλλαγές ακολουθούν είτε το McEliece ή το πλαίσιο Niederreiter, αλλά ο καθένας έχει κάποιες σημαντικές διαφορές. Αρχικά για ένα επίπεδο ασφαλείας λ, ας είναι r prime $(x^r - 1) / (X - 1) \in F2 [X]$ είναι μη αναστρέψιμη, dv είναι ένας παράξενος ακέραιος και t είναι ένας ακέραιος έτσι ώστε η αποκωδικοποίηση του t να παρουσιάζει σφάλματα με ένα ομοιόμορφο επιλεγμένο δυαδικό γραμμικό κώδικα διόρθωσης σφαλμάτων μήκους $n = 2r$ και με διάσταση r, καθώς και την ανάκτηση μιας βάσης του βάρους στήλης dv που δίνεται αυθαίρετη με βάση ενός κώδικα με το ίδιο μήκος και διάσταση, και οι δύο έχουν υπολογιστικό κόστος σε $\Omega (\exp (\lambda))$.

BIKE-1:

Σε αυτήν την παραλλαγή, προνοείται μια γρήγορη γενιά κλειδιών χρησιμοποιώντας μια παραλλαγή του McEliece. Πρώτον, σε αντίθεση με το QC-MDPC McEliece και

οποιαδήποτε παραλλαγή QC McEliece,δεν υπολογίζεται η αντιστροφή ενός από τα ιδιωτικά κυκλικά μπλοκ και στη συνέχεια πολλαπλασιάζεται με ολόκληρη την ιδιωτική μήτρα για να πάρει συστηματική μορφή. Αντ 'αυτού, κρύβεται η δομή του ιδιωτικού κώδικα απλά πολλαπλασιάζοντας τον αραιό ιδιωτικό πίνακα από οποιονδήποτε τυχαίο, πυκνό κυκλικό μπλοκ. Η τιμή που πληρώνεται είναι το διπλασιασμένο μέγεθος για το δημόσιο κλειδί και τα δεδομένα ,δεδομένου ότι το δημόσιο κλειδί δεν θα διαθέτει πλέον ένα μπλοκ ταυτότητας. Δεύτερον, ερμηνεύεται η κρυπτογράφηση του McEliece με το μήνυμα που μεταφέρεται στο διάνυσμα σφάλματος, αντί για την κωδική λέξη. Αυτή η τεχνική δεν είναι καινούργια με τις γραμμές του έργου του Micciancio και έχουν ήδη χρησιμοποιηθεί σε κώδικα από τα Cayrel.

BIKE-2

Σε αυτήν την παραλλαγή, ακολουθείται το πλαίσιο του Niederreiter με έναν συστηματικό έλεγχο ισοτιμίας στην μήτρα. Το κύριο πλεονέκτημα είναι ότι αυτό απαιτεί μόνο ένα μπλοκ μήκους r για όλα τα αντικείμενα που εμπλέκονται στο σχέδιο, και έτσι αποδίδει μια πολύ συμπαγή σύνθεση. Από την άλλη πλευρά, αυτό σημαίνει ότι είναι απαραίτητο να γίνεται εκτέλεση μιας πολυωνυμικής αναστροφής. Από την άποψη αυτή, αξίζει να αναφερθεί ότι μια βασισμένη σε αναστροφή βασική γενεά μπορεί να είναι σημαντικά πιο αργή από την κρυπτογράφηση .

BIKE-3

Αυτή η παραλλαγή ακολουθεί το έργο του Ouroboros. Εξετάζοντας την περιγραφή των αλγορίθμων, η παραλλαγή μοιάζει με το BIKE-1, που χαρακτηρίζεται από γρήγορη γενίκευση κλειδιών χωρίς αναστροφή και με δύο μπλοκ για το δημόσιο κλειδί και τα δεδομένα. Η κύρια διαφορά είναι ότι η αποκλιμάκωση επικαλείται τον αλγόριθμο αποκωδικοποίησης σε ένα "θορυβώδες" σύνδρομο.Αυτό σημαίνει επίσης ότι το BIKE-3 είναι θεμελιωδώς διαφορετικός από το BIKE-1 και το BIKE-2, κυρίως όσον αφορά την ασφάλεια και τις πτυχές που σχετίζονται με την ασφάλεια, όπως η επιλογή παραμέτρων.

	BIKE-1	BIKE-2	BIKE-3
SK	(h_0, h_1) with $\|h_0\| = \|h_1\| = w/2$		
PK	$(f_0, f_1) \leftarrow (gh_1, gh_0)$	$(f_0, f_1) \leftarrow (1, h_1 h_0^{-1})$	$(f_0, f_1) \leftarrow (h_1 + gh_0, g)$
Enc	$(c_0, c_1) \leftarrow (mf_0 + e_0, mf_1 + e_1)$	$c \leftarrow e_0 + e_1 f_1$	$(c_0, c_1) \leftarrow (e + e_1 f_0, e_0 + e_1 f_1)$
	$K \leftarrow \mathbf{K}(e_0, e_1)$		
Dec	$s \leftarrow c_0 h_0 + c_1 h_1$; $u \leftarrow 0$	$s \leftarrow ch_0$; $u \leftarrow 0$	$s \leftarrow c_0 + c_1 h_0$; $u \leftarrow t/2$
	$(e'_0, e'_1) \leftarrow \mathsf{Decode}(s, h_0, h_1, u)$		
	$K \leftarrow \mathbf{K}(e'_0, e'_1)$		

Εικόνα 4.1: Algorithm Comparison

2. Classic Mc Eliece

Πρόκειται για έναν από τους κυριότερους μετακβαντικούς αλγόριθμους που πάνω στην λειτουργία του και την δομή του βασίζονται αρκετοί άλλοι αλγόριθμοι που αποτελούν αυτήν την λίστα. Αναλυτική περιγραφή του αλγόριθμου αυτού έγινε στο υποκεφάλαιο 3.2 Κώδικες Διόρθωσης Σφαλμάτων MC-Eliece σελ.21-29.

3. CRYSTALS-KYBER

Ο Kyber είναι ένας μηχανισμός εγκλωβισμού κλειστού τύπου IND-CCA2 (KEM). Η ασφάλεια του Kyber βασίζεται στην σκληρότητα της επίλυσης του προβλήματος της μάθησης με τα σφάλματα στα πλαίσια των. Η υποβολή του στον NIST κατατάσσει τρία διαφορετικά σύνολα παραμέτρων που στοχεύουν σε διαφορετικά επίπεδα ασφαλείας. Συγκεκριμένα, ο Kyber-512 στοχεύει σε ασφάλεια ισοδύναμη με τον AES-128, ο Kyber-768 στοχεύει σε ασφάλεια σχεδόν ισοδύναμη με τον AES-192 και ο Kyber-1024 έχει ως στόχο περίπου ισοδύναμη ασφάλεια με τον AES-256.

Η κατασκευή του Kyber είναι μια προσέγγιση δύο σταδίων:

- Αρχικά οι σχεδιαστές του δημιουργούν ένα ασφαλές σύστημα κρυπτογράφησης δημόσιου κλειδιού, το οποίο κρυπτογραφεί τα μηνύματα ενός μήκους 32 bytes και ονομάζεται Cyber.
- Στη συνέχεια χρησιμοποιούν ένα ελαφρώς μετασχηματισμένο Fujisaki-Okamoto (FO) για να δημιουργήσουν το IND-CCA2-ασφαλές KEM. Και ονομάζεται ως Kyber.

Ο Kyber είναι ουσιαστικά το σύστημα κρυπτογράφησης LPR που εισήχθη για Ring-LWE από τους Lyuba-shevsky, Peikert και Regev στην παρουσίαση του στο Eurocrypt 2010.Η κύρια τροποποίηση που εφαρμόζεται στο σχήμα κρυπτογράφησης LPR είναι η χρησιμοποιήση της Μονάδας-LWE αντί για το Ring-LWE.

Ο σχεδιασμός του Cyber βασίζεται στην έκδοση της μονάδας του σχεδίου κρυπτογράφησης Ring-LWE LPR με πτώση bit. Επομένως ανήκει στην κατηγορία των πλεγμάτων. Η κύρια διαφορά στο Kyber είναι ότι το A είναι τώρα ένα πλέγμα πάνω από έναν πολυωνυμικό δακτύλιο σταθερού μεγέθους και s, e είναι φορείς πάνω στον ίδιο δακτύλιο. Στην ειδική περίπτωση των παραμέτρων Module-LWE που χρησιμοποιούνται στην Kyber, επιτυγχάνεται μια μειωμένη δομή σε σύγκριση με τον Ring-LWE, πολύ μεγαλύτερη σε δυνατότητα κλιμάκωσης και όταν κρυπτογραφεί μηνύματα μεγέθους

256 bits έχει απόδοση πολύ παρόμοια με τα συστήματα που βασίζονται σε Ring-LWE.

Όλα τα συμμετρικά δομικά στοιχεία του Kyber παρουσιάζονται με λειτουργίες που προέρχονται από το Keccak. Στην αιτιοκρατική επέκταση του A από το ρ ουσιαστικά χρειαζεται το SHAKE-128 για να γίνει παραγωγή εξόδου που "φαίνεται ομοιόμορφα τυχαία" και δεν δημιουργεί κανένα backdoors στο υποκείμενο πρόβλημα του πλέγματος. Τα μοντέλα SHAKE-128, SHA3-256 και SHA3-512 προστατεύονται ως τυχαία, αφού υπόκεινται στους τυπικούς περιορισμούς των αποδείξεων στο κβαντικό μοντέλο.

Κύρια Πλεονεκτήματα του Kyber εκτός από τις πολύ ανταγωνιστικές ταχύτητες και τις μικρές παραμέτρους με βάση ένα καλά μελετημένο πρόβλημα, είναι επίσης οι τομείς που αφορούν την Ευκολία εφαρμογής και την Εξέλιξη αφού αποτελεί ένα υποσχόμενο γεγονός στην μετακβαντική κρυπτογράφηση.

4. FrodoKEM

Ο αλγόριθμος FrodoKEM αποτελείται από μια οικογένεια μηχανισμών κλειδώματος-εγκλεισμού (KEM), δηλαδή συλλογικά ονομάζεται FrodoKEM. Τα συστήματα FrodoKEM σχεδιάζονται για συντηρητικές και πρακτικές μετακβανικές κατασκευές, η ασφάλεια των οποίων προέρχεται από προσεκτικές παραμετροποιήσεις καλά μελετημένων προβλήματων μάθησης με λάθη, το οποίο με τη σειρά τους έχουν στενές σχέσεις με εικαστικά σκληρά προβλήματα σε γενικά "αλγεβρικά αδόμητα" πλέγματα.
Συγκεκριμένα, ο FrodoKEM έχει σχεδιαστεί για την ασφάλεια IND-CCA σε δύο επίπεδα:

- FrodoKEM-640, το οποίο στοχεύει στο Επίπεδο 1 στην πρόσκληση υποβολής προτάσεων NIST αντιστοιχώντας ή υπερβαίνοντας την εγγύηση βίαιης δύναμης του AES-128 .
- FrodoKEM-976, το οποίο στοχεύει στο Επίπεδο 3 στην πρόσκληση υποβολής προτάσεων NIST που αντιστοιχεί ή υπερβαίνει την ασφάλεια βίαιων δυνάμεων του AES-192.

Τα πιο πάνω πλέγματα χωρίζονται επιμέρους σε ακόμα δύο παραλλαγές καθενός από τα παραπάνω σχήματα παρέχονται:

- FrodoKEM-640-AES και FrodoKEM-976-AES, τα οποία χρησιμοποιούν το AES128 για την ψευδοτυχαία δημιουργία ενός μεγάλου δημόσιου πίνακα (αποκαλούμενος A).

- FrodoKEM-640-cSHAKE και FrodoKEM-976-cSHAKE, τα οποία χρησιμοποιούν το cSHAKE128 για τη δημιουργία ψευδοτυχώς της μήτρας.

Οι παραλλαγές του AES είναι ιδιαίτερα κατάλληλες για συσκευές που έχουν επιτάχυνση υλικού AES όπως AES-NI σε πλατφόρμες Intel, ενώ οι παραλλαγές cSHAKE γενικά παρέχουν ανταγωνιστικές ή καλύτερες επιδόσεις σε σύγκριση με τις παραλλαγές AES, ελλείψει επιτάχυνσης υλικού.

Ο πυρήνας του FrodoKEM είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού που ονομάζεται FrodoPKE, του οποίου η ασφάλεια IND-CPA σχετίζεται στενά με τη σκληρότητα ενός αντίστοιχου προβλήματος μάθησης με σφάλματα.

Τέλος ο αλγόριθμος αυτός παρουσιάζει ως κύρια πλεονεκτήματα τα εξής:

- Ευκολία εφαρμογής.
- Συμβατότητα με υπάρχουσες αναπτύξεις και υβριδικά συστήματα.
- Εφαρμογές υλικού.
- Αντοχή πλευρικού καναλιού.

5. HQC

Το HQC (Hamming Quasi-Cyclic) είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού που βασίζεται σε κώδικα, το οποίο έχει σχεδιαστεί για να παρέχει ασφάλεια έναντι επιθέσεων από κλασικούς και κβαντικούς υπολογιστές. Χρησιμοποιεί σχεδόν κυκλικούς κώδικες καθώς και κώδικες BCH. Το HQC χρησιμοποιεί δύο τύπους κωδικών: έναν αποκωδικοποιημένο [n, k] κώδικα C, που παράγεται από G ∈ Fk × n και ο οποίος μπορεί να διορθώσει τουλάχιστον δ λάθη μέσω ενός αρχικού αλγορίθμου C.Decode (·). Και έναν τυχαίο διπλό κυκλοφορούντα [2n, n] κώδικα της μήτρας ελέγχου της ισοτιμίας (1, h).

Τα κύρια πλεονεκτήματα του HQC έναντι των υφιστάμενων κρυπτοσυστημάτων με βάση το κώδικα είναι τα εξής:

•Η μείωσή του IND-CPA σε ένα καλά κατανοητό πρόβλημα στη θεωρία κωδικοποίησης που είναι το πρόβλημα αποκωδικοποίησης του τετρακυκλικού συνδρόμου.

•Η ασυλία της από επιθέσεις που στοχεύουν στην ανάκτηση της κρυφής δομής του κωδικού που χρησιμοποιείται.

•Στενές εκτιμήσεις του ποσοστού αποτυχίας αποκρυπτογράφησης.Το τελευταίο στοιχείο επιτρέπει την επίτευξη στενής μείωσης για την ασφάλεια IND-CCA2 της έκδοσης KEM-DEM μέσω του πρόσφατου μετασχηματισμού .

Το HQC χρησιμοποιεί δύο τύπους κωδικών, έναν αποκωδικοποιημένο [n, k] κώδικα C, που παράγεται από G ∈ Fk × n και ο οποίος μπορεί να διορθώσει τουλάχιστον δ λάθη μέσω ενός αρχικού αλγορίθμου C.Decode και έναν τυχαίο διπλό κυκλοφορούντα [2n, n] κώδικα της μήτρας ελέγχου της ισοτιμίας.

6. LAC

Το LAC (Lattice Based Cryptosystems), η κρυπτογραφία δηλαδή που βασίζεται στα πλέγματα συμμετέχει και αυτή με την σειρά της στον δεύτερο γύρο υποψηφιότητων του διαγωνισμού που οργανώνει ο NIST και η συμμετοχή του οποίο περιλαμβάνει τέσσερα κρυπτογραφικά πρωτόκολλα δημόσιου κλειδιού βασισμένα στην εκμάθηση με σφάλματα στην υπόθεση των δακτυλίων:
Συγκεκριμένα:

- LAC.CPA: Είναι ένα ασφαλές σύστημα κρυπτογράφησης δημόσιου κλειδιού IND-CPA. Το ασφαλές σύστημα κρυπτογράφησης δημόσιου κλειδιού IND-CPA και LAC.CPA θέτει τα θεμέλια ολόκληρου του LAC. Περιλαμβάνει τρεις αλγόριθμους:
  - Τον αλγόριθμο δημιουργίας κλειδιών KG.
  - Τον αλγόριθμο κρυπτογράφησης Enc.
  - Τον αλγόριθμο αποκρυπτογράφησης Dec.

- LAC.KE: Είναι ένα παθητικά ασφαλές πρωτόκολλο ανταλλαγής κλειδιών το οποίο μετατρέπεται απευθείας από το LAC.CPA. Το παθητικά ασφαλές μη εξουσιοδοτημένο πρωτόκολλο ανταλλαγής κλειδιών LAC.KE αποκτάται απευθείας από το ασφαλές πρόγραμμα κρυπτογράφησης IND-CPA LAC.CPA. Η περιγραφή του LAC.KE είναι οι ίδια με εκείνη του LAC.CPA. Επιπλέον, χρησιμοποιείται μια συνάρτηση κατακερματισμού H: {0, 1} * → {0, 1} lk για τη δημιουργία του κλειδιού συνεδρίας, όπου το lk υποδηλώνει το μήκος του κλειδιού συνεδρίας και θα ποικίλει ανάλογα με τα διαφορετικά επίπεδα ασφάλειας.

Το LAC.KE που κατασκευάζεται από το LAC.CPA είναι μόνο παθητικά ασφαλές όταν δεν υπάρχει κρυφή αποθήκευση κλειδιών. Εκτός αυτού, υπάρχει ακόμα από τους σχεδιαστές του να γίνει μια κατασκευή για ένα παθητικά ασφαλές πρωτόκολλο ανταλλαγής κλειδιών απευθείας από το LAC.CCA. Σε αυτήν την περίπτωση, επιτρέπεται η προσωρινή

αποθήκευση κλειδιών στο τέλος του διακομιστή (Alice), όπως συμβαίνει με το TLS.

- LAC.CCA: Είναι ένας ασφαλής κλειδωμένος μηχανισμός κλειδιού IND-CCA, ο οποίος επιτυγχάνεται εφαρμόζοντας μια παραλλαγή του μετασχηματισμού FO σε LAC.CPA. Ο μηχανισμός κλεισίματος κλειστού κλειδιού IND-CCA LAC.CCA αποκτάται εφαρμόζοντας το μετασχηματισμό Fujisaki-Okamoto στο ασφαλές σύστημα κρυπτογράφησης IND-CPA LAC.CPA. Η μέθοδος προτάθηκε από τον Peikert.

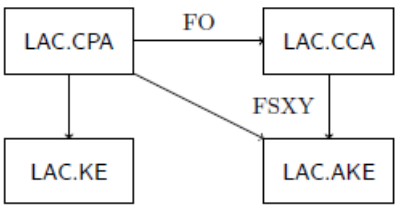
Το LAC.CCA περιλαμβάνει τους ακόλουθους τρεις αλγόριθμους:

- Ο αλγόριθμος δημιουργίας κλειδιών KG, ο οποίος είναι ο ίδιος με τον αλγόριθμο δημιουργίας κλειδιού του LAC.CPA.
- Ο αλγόριθμος ενθυλάκωσης Enc.
- Ο αλγόριθμος αποκωδικοποίησης Dec.

Ο αλγόριθμος decapulation LAC.CCA.Dec στην είσοδο sk σε ένα κρυπτογραφικό κείμενο, ανακτά ένα μήνυμα κάνοντας κλήση LAC.CPA.Dec. Κατόπιν επαληθεύει την ορθότητα της αποκρυπτογράφησης με μια διαδικασία επανακρυπτογράφησης. Σε περίπτωση που η επαλήθευση περάσει, επιστρέφει το κλειδωμένο κλειδί. Διαφορετικά, παράγει ένα ψευδοτυχαίο κλειδί από το μυστικό κλειδί και το κρυπτογραφικό κείμενο.

- LAC.AKE: Είναι το πρωτόκολλο ανταλλαγής κλειδιών που έχει πιστοποιηθεί και επιτυγχάνεται με την εφαρμογή γενικού μετασχηματισμού FSXY σε LAC.CCA και LAC.CPA. Το πρωτόκολλο ανταλλαγής κλειδιών LAC.AKE που έχει επικυρωθεί είναι κατασκευασμένο από την κρυπτογραφημένη κρυπτογράφηση δημόσιου κλειδιού LAC.CPA και τον μηχανισμό LAC.CCA του κλειστού κλειδιού ασφαλούς κλειδιού, ακολουθώντας το πλαίσιο του. Το LAC.AKE είναι ασφαλές σε λειτουργία Canetti-Krawczyk με αδύναμη απόλυτη εμπιστευτικότητα, αντίσταση σε επίθεση βασικής συμβιβαστικής πλαστοπροσωπίας (KCI) και επιθέσεις μέγιστης έκθεσης (MEX).

Οι σχέσεις των τεσσάρων κρυπτογραφικών πρωτόγονων δημόσιου κλειδιού παρουσιάζονται στο παρακάτω σχήμα.



Η ασφάλεια του LAC.CPA ακολουθεί το αποτέλεσμα ασφαλείας, το οποίο αναφέρει ότι το LAC.CPA είναι IND-CPA ασφαλές υπό την υπόθεση poly-LWE.
Η ασφάλεια του σχεδίου LAC.CCA ακολουθεί τον μετασχηματισμό Fujisaki-Okamoto στην έκδοση με σιωπηρή απόρριψη και, επομένως η ασφάλεια IND-CCA του LAC.CCA μπορεί να περιοριστεί στην ασφάλεια INDCPA του LAC.CPA.

Τα βασικά μπλοκ που χρησιμοποιούνται στην υλοποίηση του LAC περιλαμβάνουν γεννήτρια τυχαιότητας, γεννήτρια ψευδοτυχαίων και λειτουργίες κατακερματισμού.

Για απλότητα, αυτά τα μπλοκ κατασκευάζονται με βάση το openssl ως εξής:

- Γεννήτρια τυχαίων τύπων: Η λειτουργία δημιουργίας τυχαίων χαρακτήρων "RAND bytes " χρησιμοποιείται απευθείας στην υλοποίηση για τη δημιουργία τυχαίων ψηφίων.
- Γεννήτρια ψευδοτυχαίων: Η γεννήτρια ψευδοτυχαίων κατασκευάζεται με βάση τον αλγόριθμο κρυπτογράφησης AES256 στη λειτουργία ctr.
- Λειτουργία Hash: Οι λειτουργίες κατακερματισμού που χρησιμοποιούνται στο LAC είναι κατασκευασμένες από SHA256, SHA384 και SHA512 από openssl για διαφορετικές κατηγορίες ισχύος ασφαλείας.

7. LEDAcrypt

Το LEDAcrypt ουσιαστικά αποτελεί συγχώνευση των LEDAkem και LEDApkc που προτάθηκαν στον πρώτο γύρο του διαγωνισμού. Το LEDAkem και το LEDApkc αξιοποιούν το ίδιο θεωρητικό πλαίσιο, η κύρια διαφορά είναι ότι το LEDAkem εφαρμόζει ένα Κρυπτοσύστημα τύπου Niederreiter, ενώ το LEDApkc ακολουθεί την προσέγγιση McEliece.Επιπλέον, το LEDApkc εφαρμόζει μια μετατροπή η οποία επιτρέπει τη χρήση δημόσιων πινάκων γεννήτριας σε συστηματική μορφή και την επίτευξη ασφάλειας έναντι ενός επιλεγμένου (CCA) υπό την προϋπόθεση αμελητέας DFR.

Οι τροποποιήσεις καθιστούν την περιγραφή της LEDApkc περισσότερο εμπλεκόμενη από αυτήν της LEDAkem. Παρόλα αυτά, η ανάλυση μπορεί να εφαρμοστεί εξίσου και στα δύο LEDAkem ή LEDApkc.

Το LEDAkem εκμεταλλεύεται ένα μυστικό κλειδί (SK) που αποτελείται από δύο δυαδικές μήτρες.Το H είναι η δυαδική μήτρα ελέγχου ισοτιμίας ενός μυστικού κωδικού QC-LDPC και το Q είναι ένα μυστικό πλέγμα μετασχηματισμού. Ο κώδικας που περιγράφεται από το H έχει μήκος n = pn_0 και διάσταση k = p (n_0 - 1), όπου το p είναι ένας μεγάλος ακέραιος και το n_0 είναι ένας μικρός ακέραιος αριθμός. Η μήτρα H σχηματίζεται από μία σειρά από n_0 κυκλοφορητικές μήτρες με μέγεθος p × p και βάρος dv. Η μήτρα Q σχηματίζεται από n0 × n0 κυκλοφορητικές μήτρες των οποίων τα βάρη συμπίπτουν με τις καταχωρήσεις του $m_¼$ = [m_0, m1,. . ., mn_0-1] για την πρώτη σειρά και με εκείνων των κυκλικά μεταβλημένων εκδόσεων του m για τις επόμενες σειρές. Τόσο το H όσο και το Q είναι αραιά πλέγματα. Το προϊόν H_0 = HQ εξακολουθεί να δίνει μια αραιή μήτρα που είναι μια έγκυρη μήτρα ελέγχου ισοτιμίας του δημόσιου κώδικα. Λόγω της αραιότητας του, H0 δεν μπορεί αποκαλύπτεται, έτσι το δημόσιο κλειδί είναι μια γραμμικά μετασχηματισμένη έκδοση του H_0 που κρύβει την σπανιότητα. Όσον αφορά τη δυνατότητα διόρθωσης σφαλμάτων αυτών των κωδικών, ας υπενθυμίσουμε ότι οι κωδικοί QC-LDPC αποκωδικοποιούνται μέσω επαναληπτικών αλγορίθμων που δεν είναι αποκωδικοποιητές οριακής απόστασης. Επομένως, η ακτίνα αποκωδικοποίησής τους δεν είναι καθοριστική και το ποσοστό αποτυχίας αποκωδικοποίησης περιορίζεται από το μηδέν. Δηλώνουμε ως tn τον αριθμό των σφαλμάτων που μπορούν να διορθωθούν από τον κώδικα που ορίζεται από το H με το α να είναι αρκετά μεγάλη πιθανότητα και ο ίδιος ο κώδικας δηλώνεται ως C (n, k, t). Δεδομένου ότι t είναι η κρυπτογράφηση που ξεκινά με τη χαρτογράφηση του μυστικού μηνύματος ή μέρους του και σε a τυχαίος δυαδικός φορέας e με μήκος n bits και βάρος Hamming t.

Το μυστικό μήνυμα στο LEDAkem είναι ένα τυχαία παραγόμενο κλειδί, επομένως το e είναι τυχαία δημιουργία. Στη συνέχεια, ένα σύνδρομο e υπολογίζεται μέσω του δημόσιου ελέγχου ισοτιμίας matrix και αυτό δίνει το κρυπτοκείμενο. Η αποκρυπτογράφηση ξεκινά με το σύνδρομο αποκωδικοποίησης μέσω του ιδιωτικού κώδικα, η οποία επιτρέπει την ανάκτηση του διευρυμένου σφάλματος σε διάνυσμα e_0 = Eqt.Στη συνέχεια, το e ανακτάται από e_0 διά μέσου ενός πολλαπλασιασμού με το αντίστροφο του Q.

8. NewHope

Το NewHope είναι πρωτόκολλο ανταλλαγής κλειδιών βασισμένο στο πρόβλημα Ring-Learning-with-Errors (Ring-LWE).Η υποβολή στον διαγωνισμό του NIST προτείνει τέσσερις διαφορετικές παραλλαγές:

- Τα NewHope512-CPA-KEM και NewHope1024-CPA-KEM, τα οποία είναι μηχανισμοί κλειδώματος ενθυλάκωσης IND-CPA που στοχεύουν στο επίπεδο 1 και επίπεδο 5 αντίστοιχα στις προτάσεις του διαγωνισμού.
- Το NewHope512-CCA-KEM και το NewHope1024-CCA-KEM, που είναι μηχανισμοί κλειδώματος ενθυλάκωσης IND-CCA που στοχεύουν και αυτά στο επίπεδο 1 και επίπεδο 5 αντίστοιχα στην πρόσκληση υποβολής προτάσεων NIST .

Το NewHope-CPA-KEM ή NewHope-CCA-KEM, βασίζεται στο NewHope-Simple που είναι μια παραλλαγή του NewHope-Usenix . Η κύρια διαφορά είναι ότι το NewHope-Simple χρησιμοποιεί την προσέγγιση που βασίζεται στην κρυπτογράφηση, ενώ το NewHope-Usenix βασίζεται στην προσέγγιση που βασίζεται στη συμφιλίωση. Εναλλακτικά, η υποβολή των ερευνητών-δημιουργών της θα μπορούσε να περιγραφεί και στην περίπτωση του Lyubashevsky, Peikert και Regev στην οποία εφαρμόζονται όλες οι τροποποιήσεις από το NewHope-Usenix και την τεχνική μείωσης του μεγέθους του κρυπτογράφου.

Το βασικό σχήμα NewHope-CPA-PKE είναι μια σημασιολογικά ασφαλή κρυπτογράφηση δημόσιου κλειδιού σε σχέση με τις προσαρμοστικές επιλεγμένες επιθέσεις πλανημάτων. Αυτό επιτρέπει στην εφαρμογή τυποποιημένων μετασχηματισμων για την κατασκευή παθητικών και ενεργά ασφαλών KEM και PKE. Ακόμα επιτρέπει τη χρήση του πρωτοκόλλου ανταλλαγής κλειδιών χωρίς εξακρίβωση ταυτότητας, αλλά και σε ρυθμίσεις όπου απαιτείται ένα ασφαλές CEM ή PKE CCA.

Σε περίπτωση που το επίπεδο ασφάλειας πρέπει να προσδιοριστεί μαζί με το σχήμα, χρησιμοποιείται μια παραδειγματική συμβολοσειρά NewHope1024-CPA-KEM για να γίνει αναφορά στο σχήμα NewHope-CPA-KEM που δημιουργήθηκε με το σύνολο παραμέτρων NewHope1024. Πιο κάτω στον πίνακα που ακολουθεί παρέχονται τα μεγέθη των δημοσίων κλειδιών και για τις εκδόσεις.

Parameter Set	$\|pk\|$	$\|sk\|$	$\|ciphertext\|$
NewHope512-CPA-KEM	928	869	1088
NewHope1024-CPA-KEM	1824	1792	2176
NewHope512-CCA-KEM	928	1888	1120
NewHope1024-CCA-KEM	1824	3680	2208

Εικόνα 4.2: Μεγέθη δημόσιων και ιδιωτικών κλειδιών

Parameter Set	NewHope512	NewHope1024
Dimension n	512	1024
Modulus q	12289	12289
Noise parameter k	8	8
NTT parameter γ	49	7
Decryption error probability	2^{-213}	2^{-216}
Claimed post-quantum bit-security	101	233
NIST Security Strength Category	1	5

Εικόνα 4.3: Πίνακας παραμέτρων

Οι παράμετροι που περιγράφηκαν προηγουμένως στον πίνακα του NewHope και σε όλες τις άλλες παράμετρους της παρεμβολής μπορούν να υπολογιστούν από εκεί. Για ευκολία, απαριθμούν ενδιάμεσες παραμέτρους:

• NewHope512: γ = √ω = 49 · ω = 2401 · ω-1 mod q = 11813 · γ-1 mod q = 1254 · n-1 mod q = 12265

• NewHope1024: γ = ω = 7 · ω = 49 · ω-1 mod q = 1254 · γ-1 mod q = 8778 · n-1 mod q = 12277

Οι παράμετροι αυτοί του NewHope δεν είναι ελεύθερες. Η διάσταση n πρέπει να είναι μια ολόκληρη δύναμη των δύο για να υποστηρίξει τους αρχικούς αλγόριθμους NTT και να διατηρήσει τις ιδιότητες ασφαλείας του RLWE. Οι βαθμοί που δεν είναι δυναμικοί από 2 είναι αλλοπτώσιμοι, αλλά έρχονται με αρκετές επιπλοκές και ειδικότερα το defningpolynomial του δακτυλίου δεν μπορεί να έχει τη μορφή Xn +1 πια. Επιπλέον, το n πρέπει να είναι μεγαλύτερο ή ίσο από 256 λόγω της επιλογής της συνάρτησης κωδικοποίησης που χρειάζεται να ενσωματώσει ένα μήνυμα 256-bit σε ένα n-διαστατικό πολυωνύμιο στο NewHope-CPA-PKE. Το μέτρο q πρέπει να επιλεγεί ως ακέραιο prime q έτσι ώστε q ≡ 1 mod 2n να υποστηρίξει τους αρχικούς αλγόριθμους NTT.

Σε υψηλό επίπεδο, η φαινομενική ασφάλεια του NewHope εξαρτάται από το (q, n, k) όπου είναι ένα μεγαλύτερο n και ένα μεγαλύτερο leadtoahigher επίπεδο ασφαλείας.
Στην απίθανη περίπτωση που απαιτείται υψηλότερο επίπεδο ασφάλειας, ενώ παραμένει η παραδοχή στην παραδοχή RLWE, είναι απλή η επιλογή ενός συνόλου παραμέτρων NewHope Ludicrous με διάσταση n = 2048 και k = 8. Αυτό θα διπλασίαζε βασικά τους χρόνους εκτέλεσης και το μέγεθος των δημόσιων κλειδιών, τα κρυπτογραφικά κείμενα και τα κλειδιά έκφρασης. Μια μικρή αύξηση της ασφάλειας για το NewHope-CPA-KEM είναι εξίσου δυνατή. Καθώς το σχέδιο θα πρέπει στην πράξη να χρησιμοποιείται μόνο σε εφήμερη ρύθμιση όπου τα σφάλματα αποκρυπτογράφησης

είναι λιγότερο κρίσιμα, μπορεί να είναι δυνατή η ελαφρά αύξηση του k .
Το NewHope χρησιμοποιεί απευθείας ιδιότητες ενός negacyclic NTT, οι παράμετροι επιλέγονται έτσι ώστε το q να είναι πρωταρχικό και ότι $q \equiv 1 \bmod 2n$. Ένα σχέδιο χωρίς περιορισμούς σχετικά με το συντελεστή q φαίνεται πολύ διαφορετικό από το NewHope ως ένα προοπτικό υλοποίησης.

Οι σταθερές που χρησιμοποιούνται στο NewHope έχουν ως ακολούθως:
•Διάσταση n: Επιλεγμένα αλγόριθμοι ως προς το πρωτόκολλοNTT ως προς την ασφάλεια του RLWE.
•Modulus q: Επιλέγεται ως το μικρότερο πρότυπο έτσι ώστε $q \equiv 1 \bmod 2n$ και έτσι ώστε ο αριθμητικός-θεωρητικός μετασχηματισμός (NTT) να πραγματοποιηθεί efficiciously.
•Παράμετρος θορύβου k: Επιλέγεται έτσι ώστε η πιθανότητα σφαλμάτων αποκρυπτογράφησης να είναι αμελητέα.
•Παράμετρος NTT γ: Πρέπει να είναι η πρώτη πρωτόγονη ρίζα της ενότητας.
•Διαχωρισμός τομέα σε κλήσεις προς SHAKE: ais δημιουργείται ψευδοτυχαία χρησιμοποιώντας SHAKE128 .

9. NTRU

Το NTRU αποτελεί ουσιαστικά και αυτό μια συγχώνευση των NTRU-HRSS-KEM και NTRUEncrypt που παρουσιάστηκαν στον προηγούμενο γύρο του διαγωνισμού του NIST.

Το NTRU είναι ένα κρυπτοσύστημα δημόσιου κλειδιού που βασίζεται σε πλέγματα και το πιο διεξοδικά διερευνημένο και ευρέως εφαρμοζόμενο εναλλακτικό σε RSA και ECC. Υποστηρίζει κρυπτογράφηση, αποκρυπτογράφηση και υπογραφή. Όχι μόνο ταχύτερη και μικρότερη από τον RSA και τον ECC, το NTRU είναι η κορυφαία επιλογή για τους οργανισμούς που αναγνωρίζουν την ανάγκη να προστατευθούν από την επικείμενη απειλή των επιθέσεων Quantum Computing. Το NTRU είναι ακόμα πρότυπο χρηματοοικονομικών υπηρεσιών IEEE 1363.1 και X9.98.

Τα κύρια πλεονεκτήματα της κρυπτογράφησης NTRU μετά την συγχνώνευση της από τις δύο μορφές που προτάθηκαν στον διαγωνισμό έχουν ως έχει:

- Μικροσχηματισμένος κώδικας (8 kb).

- Καταναλώνει ελάχιστες πηγές CPU και μπαταρίας.
- Ιδανικό για όλα τα περιβάλλοντα, αλλά ιδιαίτερα κατάλληλο για ενσωματωμένες και κινητές συσκευές, όπου το μέγεθος του κώδικα αποτελεί σημαντικό περιορισμό.
- Σημαντικά μειώνει τη χρήση του διακομιστή για εφαρμογές μεγάλης κλίμακας αύξηση της απόδοσης.

Η αποκρυπτογράφηση με NTRU είναι μεγαλύτερη και έως και 92 φορές ταχύτερη από την αποκρυπτογράφηση RSA σε ισοδύναμο επίπεδο ασφάλειας.Το NTRU είναι σχεδόν 60% ταχύτερο από το RSA στην κρυπτογράφηση και το TLS με 370 φορές βελτίωση στον χρόνο δημιουργίας πλήκτρων.

Το ίδιο ισχύει και για τον ECC με τις καλύτερες επιδόσεις σε ισοδύναμα επίπεδα ασφαλείας.

Ακόμα επιτυγχάνει τον έλεγχο ταυτότητας TLS και τη βασική διαπραγμάτευση, συνδυάζοντας την κλασσική κρυπτογραφία του σήμερα με την κβαντική κρυπτογράφηση NTRU, εξασφαλίζοντας το καλύτερο και των δύο κόσμων.
Η παράλληλη εφαρμογή επιτρέπει τα οφέλη της NTRU πέρα από την υπάρχουσα υποδομή κρυπτογράφησης με αμελητέα ποινή απόδοσης.

Επίσης αποτρέπει τις επιθέσεις συλλογής δεδομένων καθώς και έχει την δυνατότητα για πρόβλεψη των προκαταρκτικών ενέργειων των δεδομένων. Προστατεύει δηλαδή τις πληροφορίες που πρέπει να παραμείνουν μυστικές για πολλά χρόνια διατηρώντας την κρυπτογραφημένη κίνηση από την καταγραφή και την αποθήκευση σήμερα .

10. NTRU Prime

Οι δομές που χρησιμοποιούνται στις κορυφαίες προτάσεις για κρυπτογραφία με βάση το κβαντικό πλέγμα αφορούν το κλασικό κρυπτοσυστήμα NTRU και τα κρυπτοσυστημάτα βασισμένα σε Ring-LWE. Όμοιο είναι και το παρόν.

Το NTRU Prime προτρέπει το NTRU να χρησιμοποιεί δακτυλίους χωρίς αυτές τις δομές. Εδώ υπάρχουν δύο κρυπτοσυστήματα δημόσιου κλειδιού στην οικογένεια NTRU Prime, και τα δύο έχουν σχεδιαστεί για τον τυπικό στόχο της ασφάλειας IND-CCA2.Το βελτιωμένο NTRU Prime βελτιστοποιείται από την άποψη της εφαρμογής. Το NTRU

LPRime που προφέρεται "ell-prime" είναι μια παραλλαγή που προσφέρει διαφορετικές συμφωνίες. Τα βελτιωμένα πρωτόκολλα NTRU Prime 4591761 και NTRU LPRime 4591761 είναι τα Streamlined NTRU Prime και NTRU LPRime με μετακβαντικές παραμέτρους υψηλής ασφάλειας. Τα προκύπτοντα μεγέθη και οι ταχύτητες Haswell από τα επίσημα δείγματα αναφοράς supercop-20181216 για το titan 0 δείχνουν ότι η μείωση της επιφάνειας επίθεσης έχει πολύ χαμηλό κόστος.

Ο τρόπος που σχεδιάστηκε το κρυπτοσύστημα αυτό από τους σχεδιαστές του θεωρούν ότι θα είναι πολύ ανθεκτικό ακόμα και από εξειδικευμένες επιθέσεις με κβαντικούς υπολογιστές. Συγκεκριμένα για τον αλγόριθμο του Grover, η ενίσχυση του εύρους και οι κβαντικές βολές του, παράγουν καλύτερους εκθέτες για ορισμένες από τις υπορουτίνες που χρησιμοποιήθηκαν. Οι προκαταρκτικές εκτιμήσεις δείχνουν ότι ο συνολικός αντίκτυπος στα βελτιωμένα επίπεδα ασφαλείας NTRU Prime είναι πολύ μεγαλύτερος από τον αντίκτυπο στα επίπεδα ασφαλείας AES-256.

Αυτή η πρόταση έχει σχεδιαστεί ώστε να έχει τη μικρότερη επιφάνεια επίθεσης, ελαχιστοποιώντας τον αριθμό των διαθέσιμων διευθύνσεων για τους κρυπτοαναλυτές. Ορισμένες πρόσφατες επιθέσεις κατά κρυπτοσυστημάτων βασισμένων σε πλέγμα βασίζονται σε ομομορφισμούς που εξαλείφθηκαν από αυτήν την πρόταση.

Ταυτόχρονα, η πρόταση αυτή προσφέρει ασυνήθιστα μικρά μεγέθη και εξαιρετική ταχύτητα. Ένας από τους λόγους αυτής της απόδοσης είναι ότι αυτή η πρόταση παρέχει την ευελιξία να στοχεύσει οποιαδήποτε επιθυμητή διάσταση πλέγματος μάλλον με ακρίβεια, χωρίς τα "άλματα" που εμφανίζονται στις περισσότερες προτάσεις. Οι μελλοντικές εξελίξεις στην κατανόηση του ακριβούς επιπέδου ασφάλειας της κρυπτογραφίας βάσει πλέγματος θα επιτρέψουν την κατάλληλη ρύθμιση αυτής της πρότασης.

Ωστόσο, υπάρχουν και άλλες πρόσφατες επιθέσεις εναντίον κρυπτογραφίας βασισμένης σε πλέγμα, συμπεριλαμβανομένων εντυπωσιακών προόδων κατά του SVP. Αυτός είναι ένας γενικός περιορισμός της κρυπτογραφίας που βασίζεται σε πλέγματα. Ο ίδιος περιορισμός μοιράζεται με πολλές - αλλά όχι όλες τις μετακβαντικές προτάσεις.

11. NTS-KEM

Μπορεί να δει κανείς ότι το NTS-KEM θεωρείται ως μια παραλλαγή των συστημάτων κρυπτογράφησης δημόσιου κλειδιού McEliece και Niederreiter.Ωστόσο, σε σύγκριση με τα αρχικά συστήματα, το NTS-KEM δεν ασχολείται πλέον με την επικοινωνία ενός κρυπτογραφημένου μηνύματος αλλά μάλλον με την ασφαλή επικοινωνία ενός τυχαίου πλήκτρου.

Ούτε το McEliece ούτε το Niederreiter, με την καθαρή μορφή τους, επιτυγχάνουν την αδιαμφισβήτητη θέση κάτω από τα δύο IND-CPA ή επιλεγμένες επιθέσεις κρυπτογράφων IND-CCA. Αντίθετα, το NTS-KEM επιτυγχάνει την ασφάλεια IND-CCA ως KEM στο τυχαίο μοντέλο Oracle χρησιμοποιώντας ένα μετασχηματισμό σαν Fujisaki-Okamoto ή Dent .Η ασφάλεια IND-CCA του NTS-KEM μειώνεται άμεσα στο μέγεθος της θραύσης της οδού του συστήματος McEliece, το οποίο με τη σειρά του σχετίζεται με το πολύ γνωστό πρόβλημα της αποκωδικοποίησης τυχαίων γραμμικών κωδίκων. Αυτό επιτρέπει στο NTS-KEM να χρησιμοποιείται σε εφαρμογές με μια σειρά προ και μετακβαντικής ασφάλειας των αλγορίθμων.

Το NTS-KEM διαθέτει αποτελεσματικές λειτουργίες ενθυλάκωσης και απόσυρσης κλειδιών, οι οποίες οφείλονται σε αποτελεσματικούς αλγόριθμους αποκωδικοποίησης για τους κώδικες Goppa. Τα κρυπτογραφημένα κείμενα είναι σχετικά συμπαγή με το σχήμα να είναι κατάλληλο για εφαρμογές με περιορισμένο εύρος ζώνης επικοινωνίας.Με τα περισσότερα συστήματα που βασίζονται σε κώδικα, το NTS-KEM απαιτεί μεγάλα δημόσια κλειδιά. Αυτό προκύπτει από τη δική μας συντηρητική επιλογή κωδίκων, στην οποία αποφεύγουμε οποιαδήποτε κυκλική ή σχεδόν κυκλική δομή. Υπάρχει ακόμα μια σειρά εφαρμογών στις οποίες η χρήση μεγάλων δημόσιων κλειδιών δεν θα θεωρείται ως μειονεκτήμα και όπου οι γρήγορες λειτουργίες και τα συμπαγή κρυπτογραφήματα θεωρούνται πιο σημαντικά. Παραδείγματα τέτοιων εφαρμογών είναι όσοι χρησιμοποιούν μακροπρόθεσμα δημόσια κλειδιά.

Η επιλογή για ένα συντηρητικό σχεδιασμό KEM που βασίζεται σε κώδικες διόρθωσης λαθών υποκινείται από την επιθυμία να παρέχουν μακροχρόνια μετα-κβαντική ασφάλεια, η οποία βασίζεται σε ένα απλό, εύχρηστο και μια αποτελεσματική προσέγγιση, η οποία έχει μελετηθεί εκτενώς και έχει εμπιστευτεί για σχεδόν τέσσερις δεκαετίες.

Οι εγγυήσεις ασφάλειας προέρχονται από ένα πολύ γνωστό μαθηματικό πρόβλημα και από καλές εκτιμήσεις της πολυπλοκότητας των κλασσικών αλγορίθμων αποκωδικοποίησης, οι οποίες μπορούν να αξιοποιηθούν για την παροχή κατάλληλων σε επίπεδα ασφάλειας έναντι επιλεγμένων επιθέσεων κρυπτοκείμενο. Όπως προαναφέρθηκε πιο πάνω το NTS-KEM επιτυγχάνει την ασφάλεια IND-CCA στο τυχαίο μοντέλο Oracle με τη χρήση ενός μετασχηματισμού όπως ο μετασχηματισμός Fujisaki-Okamoto] ή Dent.

Αναφορικά με το γεγονός ότι το NTS-KEM δημιουργεί ενθυλάκωση που είναι ουσιαστικά κρυπτογραφήσεις στο σύστημα McEliece PKE με δημόσιο κλειδί σε συστηματική μορφή των διανυσμάτων μηνύματος της φόρμας m = (ea | ke) ∈ Fk2, όπου ke = H (e) `2 το κλειδωμένο κλειδί είναι τότε de kr = H` (ke | e) ∈ F`2. Αντίθετα, το σχήμα NTS-KEM δημιουργεί εγκλεισμούς που είναι κρυπτογραφήσεις των φορέων μηνύματος της φόρμας (ea | rb), όπου rb είναι μια ομοιόμορφα τυχαία σειρά στο F2 και πέρνεται το rb ως το κλειδωμένο κλειδί για το NTS-KEM.

12. ROLLO

Όπως και σε προηγούμενες υποψηφιότητες για να μπορεί αυτό το κρυπτοσύστημα να βρίσκεται στον δεύτερο γύρο του διαγωνισμού αποτελείται και αυτό από συγχωνεύσεις άλλων κρυπτοσυστημάτων. Συγκεκριμένα αποτελεί συγχώνευση του LAKE, του LOCKER και του Ouroboros-R (Rank-Ouroboros, LAKE and LOCKER). Τα προηγούμενα κρυπτοσυστήματα προτάθηκαν στον διαγωνισμό στον πρώτο γύρο του διαγωνισμού και μετά την συγχώνευση τους προχώρησαν στον δεύτερο γύρο του διαγωνισμού ώς ένα ενιαίο σύστημα. Πρόκειται όμως για ένα κρυπτοσύστημα που βασίζεται σε κώδικα και έχει σχεδιαστεί για να παρέχει ασφάλεια έναντι επιθέσεων από κλασικούς και κβαντικούς υπολογιστές. Ο προτεινόμενος σχηματισμός είναι πολύ αποδοτικός, τόσο ως προς το μέγεθος των κλειδιών όσο και ως προς τον υπολογισμό. Επίσης, επωφελείται από έναν αλγόριθμο σταθερής χρονικής αποκωδικοποίησης και την αποτυχία του με πιθανότητα τέτοια ώστε να είναι πολύ καλά μελετημένη και εκτιμημένη και μπορεί εύκολα να επιλεγεί για να καλύψει την ασφάλεια.Επιπλέον, η επιλογή των παραμέτρων είναι πολύ ευέλικτη. Για τους LAKE και LOCKER,υπάρχει μια μείωση σε ένα καλά κατανοητό γενικό πρόβλημα IRSD, το οποίο είναι μια φυσική γενίκευση του κυκλικού RSD προβλήματος. Αυτό το είδος προβλημάτων έχει

χρησιμοποιηθεί εδώ και πολλά χρόνια για τις αποστάσεις Hamming και Euclidean.
Η σειρά Ouroboros επωφελείται επίσης από τα ωραία χαρακτηριστικά του πρωτοκόλλου LRPC, αλλά με μείωση στα γενικά προβλήματα 2s-QCRSD. Το μέγεθος του κρυπτογράφου διπλασιάζεται, αλλά λόγω της εγγενούς δυσκολίας των κωδικών αποκωδικοποίησης στην κατάταξη των μετρικών παραμέτρων είναι μάλλον χαμηλές και συγκρίνονται πολύ καλά με άλλους τύπους πρωτοκόλλων.

Ο περιορισμός της κατάταξης έχει πολύ ωραία χαρακτηριστικά, αλλά η χρήση της μέτρησης κατάταξης για κρυπτογραφικούς σκοπούς δεν είναι πολύ παλιός. Μπορεί να φαίνεται ως ένας περιορισμός, αλλά ακόμα τα τελευταία χρόνια υπήρξαν πολλές δραστηριότητες για την κατανόηση της εγγενούς υπολογιστικής δυσκολίας των σχετικών προβλήμαων που φαίνεται πολύ δύσκολο να βελτιωθεί η γενική τους πολυπλοκότητα. Όπως για τα κρυπτοσυστήματα McEliece, τα αποδεικτικά ασφαλείας LAKE και LOCKER βασίζονται στην σκληρότητα της ανάκτησης της δομής ενός δομημένου κώδικα, στην περίπτωσή μας των κωδικών LRPC. Ωστόσο, το πρόβλημα αυτό έχει μελετηθεί και για τις μετρήσεις Hamming και euclidean και είναι θεωρητικά πολύ σκληρό από την κοινότητα.

13. Round5

Όπως και το προηγούμενο κρυπτοσύστημα και αυτό αποτελεί συγχώνευση άλλων κρυπτοσυστημάτων που είχαν προταθεί στον πρώτο γύρο του διαγωνισμού του NIST. Συγκεκριμένα αποτελεί συγχώνευση του HILA5 και του Round1. Το Round5 είναι ένας κορυφαίος υποψήφιος για την κρυπτογράφηση κλειδιών NIST PQC και την κρυπτογράφηση δημόσιων κλειδιών του διαγωνισμού. Το κρυπτοσύστημα Round5 βασίζεται στο πρόβλημα της Γενικής Μάθησης με στρογγυλοποίηση (GLWR) για την ενοποίηση των καλά μελετημένων προβλημάτων μάθησης με στρογγυλοποίηση (LWR) και δακτυλίου μάθησης με στρογγυλοποίηση (RLWR). Επιτρέπει ακόμα μια απλή περιγραφή και υλοποίηση του IND-CPA KEM του Round5 και ενός PKE IND-CCA που ονομάζεται r5_cpa_kem και r5_cca_pke.

Οι επιλογές σχεδιασμού του Round5 έχουν γίνει με γνώμονα την ασφάλεια και την απόδοση. Ο ευέλικτος και ενοποιημένος σχεδιασμός επιτρέπει στο χρήστη να επιλέξει τη διαμόρφωση που ταιριάζει καλύτερα στις ανάγκες ασφάλειας και απόδοσης. Η

εκμάθηση με στρογγυλοποίηση επιτρέπει χαμηλότερο εύρος ζώνης σε σχέση με τις τυπικές προτάσεις για την εκμάθηση με σφάλματα. Οι εκδηλώσεις δαχτυλιδιών του Round5 βασίζονται περαιτέρω σε κύκλωμα πολυωνυμικού δακτυλιδιού πρώτης τάξης που απολαμβάνουν αποδεδειγμένες αποδείξεις ασφαλείας και προσφέρουν ένα μεγάλο χώρο σχεδιασμού, που επιτρέπει την ακριβή ρύθμιση της διάστασης του δακτυλίου. Είναι επομένως εύκολο να υπάρξει παραμετροποιήση ή μείωση των παραμέτρων του Round5 για να στοχεύσουν διαφορετικούς στόχους ασφάλειας. Η χρήση της δύναμης των δύο moduli q και p κάνει σπονδυλωτές λειτουργίες γρήγορα έτσι ώστε το Round5 να είναι πολύ αποτελεσματικό σε διάφορες πλατφόρμες. Τα τριμερή μυστικά σταθερού βάρους εξασφαλίζουν γρήγορη λειτουργία και χαμηλή πιθανότητα αποτυχίας. Τέλος, η χρήση του ισχυρού κώδικα διόρθωσης σφαλμάτων σταθερού χρόνου XEf επιτρέπει στο Round5 να υποστηρίζει τις μικρότερες παραμέτρους διαμόρφωσης μεταξύ των προτάσεων που βασίζονται σε πλέγματα NIST και έτσι να προσφέρουν τις καλύτερες επιδόσεις από άποψη εύρους ζώνης, CPU και χρήσης μνήμης. Δεδομένου ότι το XEf είναι σταθερό, οι επιθέσεις χρονισμού στη διόρθωση σφαλμάτων δεν είναι εφικτές.

14. RQC

Το RQC (Rank Quasi-Cyclic) είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού με κωδικό που έχει σχεδιαστεί για να παρέχει ασφάλεια έναντι επιθέσεων και από κλασικούς και κβαντικούς υπολογιστές. Χρησιμοποιεί σχεδόν κυκλικούς κώδικες καθώς και κώδικες Gabidulin. Τα προκύπτοντα μεγέθη σε bytes για το RQC χρησιμοποιώντας τον διαστολέα των «σπόρων» του NIST είναι αρχικοποιημένο με 40 μακρούς σπόρους. Το pk δημόσιο κλειδί αποτελείται από (seed1, s) και έχει μέγεθος 40 + nm. Το μυστικό κλειδί sk αποτελείται από (seed2) και έχει μέγεθος 40. Το ciphertext ct αποτελείται από (u, v, d) και έχει μέγεθος 2nm + 64. Το κοινό μυστικό ss αποτελείται από K και έχει μέγεθος 64 ως output SHA512. Η ασφάλεια αυτή είναι εκφρασμένη σε bits.

Τα βασικά πλεονεκτήματα του RQCover είναι το υπάρχον κρυπτοσυστήμα με βάση το κώδικα:

- Η IND-CPA αναγωγή του σε ένα καλά κατανοητό πρόβλημα σχετικά με τη θεωρία κωδικοποίησης με το Decoding πρόβλημα του συνδρόμου.
- Όσο αφορά την ασυλία της από επιθέσεις που στοχεύουν στην ανάκτηση της κρυφής δομής του κωδικού που χρησιμοποιείται.

- Ακόμα διαθέτει ένα μηδενικό ποσοστό αποτυχίας αποκρυπτογράφησης.
- Το τελευταίο στοιχείο επιτρέπει στην επίτευξη στενής μείωσης για την ασφάλεια IND-CCA2 της έκδοσης του KEM-DEM μέσω της πρόσφατης μετατροπής.
-

Για το RQC κρυπτογραφικό σύστημα ως περιορισικό μέτρο τυγχάνει το γεγονός ότι τα αντικείμενα που θεωρούνται κωδικοί επεκτάσεων μπορεί να φανούν μόνιμα, αλλά με την πρακτική εφαρμογή των αποτελεσμάτων που προκύπτουν δείχνουν ότι έχουν εκτελεστεί οι χρόνοι.

15. SABER

Το κρυπτοσύστημα SABER ουσιαστικά αποτελεί μια οικογένεια κρυπτογραφικών πρωτόγονων που βασίζονται στη σκληρότητα του προβλήματος Module Learning With Rounding Mod-Lue με στρογγυλοποίηση Mod-LWR. Οι στόχοι σχεδίασης του Saber ήταν η απλότητα, η αποδοτικότητα και η ευελιξία που οδήγησαν στις ακόλουθες επιλογές με όλα τα ακέραια modi να είναι οι δυνάμεις των 2 αποφεύγοντας πλήρως τη δειγματοληψία αρθρωτής μείωσης και απόρριψης. Η χρήση του LWR μειώνει κατά το ήμισυ την ποσότητα τυχαιότητας που απαιτείται σε σύγκριση με τα συστήματα που βασίζονται σε LWE και μειώνει το εύρος ζώνης. Η δομή της μονάδας παρέχει ευελιξία επαναχρησιμοποιώντας ένα βασικό στοιχείο για πολλαπλά επίπεδα ασφαλείας.

Οι παράμετροι για το Saber είναι οι ακόλουθοι:
•q, p, t: Οι συντελεστές που εμπλέκονται στο σχήμα επιλέγονται να είναι εξουσίες 2, ειδικότερα 2 q 2 p 2 t q =, p = και t = με q> p> (t + 1), έτσι καταλήγουν ότι 2t | p | q. Μια μεγαλύτερη επιλογή για τις παραμέτρους p και t, θα έχει ως αποτέλεσμα την χαμηλότερη ασφάλεια, και την υψηλότερη ορθότητα. Ένα σενάριο python που υπολογίζει τις βέλτιστες τιμές για p και t είναι μέρος της υποβολής.
• μ: Οι συντελεστές των μυστικών διανυσμάτων s και sss0 λαμβάνουν δειγματοληψία σύμφωνα με μια κεντρική διωνυμική κατανομή βμ (Rql × 1) με την παράμετρο μ, όπου μ <p. Μια υψηλότερη τιμή για μ θα οδηγήσει σε μεγαλύτερη ασφάλεια, αλλά σε χαμηλότερη ορθότητα του συστήματος.
• n, l: Ορίζονται ως ο βαθμός n και ο αριθμός l πολυωνύμων στους μυστικούς φορείς s και sss0 καθορίζουν τη διάσταση του υποκείμενου προβλήματος πλέγματος ως ln. Η αύξηση της διάστασης του προβλήματος πλέγματος αυξάνει την ασφάλεια, αλλά μειώνει την ορθότητα.

•F, G, H: Είναι οι λειτουργίες κατακερματισμού που χρησιμοποιούνται στο πρωτόκολλο. Οι λειτουργίες F και H υλοποιούνται χρησιμοποιώντας το SHA3-256, ενώ το G υλοποιείται χρησιμοποιώντας το SHA3-512.
•gen: Η συνάρτηση προέκτασης εξόδου που χρησιμοποιείται στο πρωτόκολλο, η οποία υλοποιείται χρησιμοποιώντας το SHAKE-128.

Οι σχεδιαστικοί στόχοι του SABER δεν είναι άλλοι από την απλότητα, την αποδοτικότητα και την ευελιξία που έχουν ως αποτέλεσμα τις επιλογές όπως τα τα ακέραια modi να είναι εξουσίες των 2 αποφεύγοντας πλήρως τη δειγματοληψία αρθρωτής μείωσης και απόρριψης. Ακόμα η χρήση του LWR είναι να μειώνει κατά το ήμισυ την ποσότητα τυχαιότητας που απαιτείται σε σύγκριση με τα συστήματα που βασίζονται σε LWE και μειώνει το εύρος ζώνης.Η δομή της μονάδας παρέχει ευελιξία επαναχρησιμοποιώντας ένα βασικό στοιχείο για πολλαπλά επίπεδα ασφαλείας.

Το κρυπτοσύστημα SABER προσφέρει τρία επίπεδα ασφάλειας:

- LightSABER: Είναι επίπεδο μετά-κβαντικής ασφάλειας παρόμοιο με το AES-128.
- SABER: Είναι επίπεδο μετά-κβαντικής ασφάλειας παρόμοιο με το AES-192.
- FireSABER: Είναι επίπεδο μετά-κβαντικής ασφάλειας παρόμοιο με το AES-256.

Τέλος αξίζει να σημειωθεί το γεγονός ότι το SABER έχει σχεδιαστεί για να λειτουργεί σε συνεχή χρόνο για να αναχαιτίσουν τις επιθέσεις πλευρικών διαύλων που εκμεταλλεύονται χρονικές διαφορές.

16. SIKE

Το κρυπτοσύστημα SIKE είναι βασισμένο σε ισογονίδια σουίτες ενθυλάκωσης κλειδιών που βασίζονται σε ψευδοτυχαίες βόλτες σε γραφήματα υπερηχητικής ισογονίας, τα οποία υποβλήθηκαν στη διαδικασία τυποποίησης NIST για την μετάκβαντική κρυπτογράφηση. Περιέχει δύο αλγόριθμους:

- Ένα μηχανισμό που είναι ασφαλής με CPA αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού SIKE.PKE.
- Και ενα μηχανισμό εγκλεισμού κλειδιού κλειστού τύπου CCA SIKE.KEM

Υπάρχουν τρείς μορφές παραμέτρων που έχουν ως εξής: SIKEp503, SIKEp751 και SIKEp964.
Όσο αφορά τις δημόσιες παραμέτρους του κρυπτοσυστήματος SIKE αυτές έχουν ως

εξής:

- Δύο θετικοί ακέραιοι e_2 και e_3 που ορίζουν ένα πεπερασμένο πεδίο Fp^2 όπου $p = 2e^{23}e^3 - 1$,
- Μια αρχική υπερηχητική ελλειπτική καμπύλη $E_0 = Fp^2$,
- Â Ένα σύνολο τριών συντεταγμένων x που αντιστοιχούν στα σημεία στο E_0 $[2^{e2}]$, και
- Ένα σύνολο τριών συντεταγμένων χ αντιστοιχεί σε σημεία στο E_0 $[3^{e3}]$.

Ο επιταχυντής υλικού SIKE μπορεί να εκτελέσει λειτουργίες KEM για τις δημόσιες παραμέτρους που παρατίθενται στο SIKEp751. Υπάρχει κάποια δυνατότητα ρύθμισης στον αριθμό των διπλών πολλαπλασιαστών που πολλαπλασιάζονται με τον αριθμό των κύκλων ανά λειτουργία. Δεδομένου ότι οι εργασίες ισογονισμού απαιτούν τον περισσότερο χρόνο, η εφαρμογή αυτή παραλληλίζεται με διάφορους υπολογισμούς αριθμητικών πεπερασμένων πεδίων και ισογονισμού. Ο πυρήνας του επιταχυντή του SIKE συντέθηκε χρησιμοποιώντας το Synopsys Design Compiler. Ο TSMC 65 nm CMOS στην τυπική τεχνολογία και την βασική βιβλιοθήκη κυττάρων CORE65LPSVT χρησιμοποιήθηκαν για τα αποτελέσματα. Αυτή η εφαρμογή βελτιστοποιήθηκε για απόδοση.

Η περιοχή μετατράπηκε σε ισοδύναμα πύλης (GE), όπου λαμβάνεται υπόψη το μέγεθος μιας μοναδικής πύλης NAND 1 GE. Για τη συγκεκριμένη τεχνολογική βιβλιοθήκη, το μέγεθος μιας συνθετικής πύλης NAND ήταν 1:41 μm^2, επομένως αυτό χρησιμοποιήθηκε ως συντελεστής μετατροπής. Για την εφαρμογή ASIC πάνω από SIKEp751, η ενθυλάκωση και η απόψυξη μπορεί να γίνει σε 9,20 και 9,67 msec, αντίστοιχα. Έτσι, ο συνολικός χρόνος KEM είναι 18,87 msec.

17. Three Bears

Το τελευταίο σύστημα δημοσίων και ιδιωτικών κλειδιών που πέρασε στον δεύτερο γύρο του διαγωνισμού είναι το Three Bears . Το εν λόγω σύστημα ThreeBears βασίζεται στο Lyubashevsky-Peikert-Regev και το Ding με κρυπτοσυστήματα σφαλμάτων (RLWE). Δηλαδή βασίζεται σε Alkim NewHope και Bos Cyber , το τελευταίο του οποίου χρησιμοποιεί την εκμάθηση των μονάδων με σφάλματα (MLWE). Οι σχεδιαστές του όμως έκαναν αντικατάσταση του πολυωνυμικού δακτύλιου που βρίσκεται κάτω από

αυτή την ενότητα με το ακέραιο modulo ενός γενικευμένου αριθμού Mersenne, κάνοντας έτσι ακέραιο (I-MLWE), όπως και στο έργο του Gu. Έπειτα χρησίμοποίησαν την διόρθωση σφαλμάτων προς τα εμπρός, όπως το trunc8 του Saarinen και το Hila5.Το όνομα του ThreeBears προέρχεται από το γεγονός ότι το μέτρο του έχει το ίδιο golden-ratio Solinas ως Ed448-Goldilocks, και μάλιστα μερικοί του αριθμητικού κώδικα στην υλοποίησή του προέρχεται από το Goldilocks ενός αριθμητικού κώδικα.

Ένας από τους στόχους των σχεδιαστών του με το ThreeBears είναι να ενθαρρύνουν τη διερεύνηση δυνητικά και επιθυμητά αλλά με λιγότερο συμβατικά σχέδια. Αυτός είναι ο λόγος για τον ThreeBears που χρησιμοποιεί I-MLWE αντί για MLWE. γιατί το ιδιωτικό κλειδί ως μόνο σπόρο. Γιατί χρησιμοποιούν ρητή απόρριψη και γιατί παραλείπουν το hash του Targhi-Unruh. Το έν λόγω κρυπτοσύστημα φέρει τα εξής πλεονεκτήματα στον τομέα της κρυπτογραφίας σε σχέση με τα συνδιαγωνιζόμενα του:

- Η ταχύτητα του ThreeBears αφορά τα πλεονεκτήματα των περισσότερων RLWE και MLWE συστημάτων. Η δημιουργία του κλειδιού είναι πολύ γρήγορη, τόσο γρήγορη ώστε είναι συνήθως καλύτερη η αποθήκευση του σπόρου αντί του διευρυμένου ιδιωτικού κλειδιού. Η Κρυπτογράφηση και Αποκρυπτογράφηση είναι επίσης πολύ γρήγορες, και τυπικά σημαντικά ταχύτερες από τις ελλειπτικές καμπύλες.
- Στο μέγεθος των δημοσίων κλειδιών και τα κρυπτογραφικά εύλογα μεγέθη είναι περίπου 1: 2kB και 1: 3kB αντίστοιχα για το MamaBear. Αυτό είναι αρκετά μικρό για να είναι πρακτικό για τα περισσότερα συστήματα συνδεδεμένα στο Διαδίκτυο, αλλά όχι τόσο μικρά . Τα ιδιωτικά κλειδιά είναι μόνο 40 byte. Τα μεγέθη κώδικα είναι κάτω από 10kB περισσότερα από τον Keccak, και οι απαιτήσεις στοίβας μπορούν να ωθηθούν κοντά σε 3kB περρισότερης εισροής και παραγωγής.
- Το λογισμικό ThreeBears μπορεί να χρησιμοποιηθεί με υπάρχοντα μεγάλο ακέραιο αριθμό του λογισμικού και το υλικού, το οποίο είναι χρήσιμο για τις έξυπνες κάρτες και την ασφάλεια υλικού σε ενότητες. Αυτό μειώνει την περιοχή υλικού σε συστήματα που πρέπει να υποστηρίζουν και τα δύο . Δηλαδή και τους προκβαντικούς αλλά και τους μετακβαντικούς αλγορίθμους.
- Η απλότητα ThreeBears έχει μια σχετικά απλή προδιαγραφή, ειδικά αφού δεν χρησιμοποιεί τον αριθμοθεωρητικό μετασχηματισμό.
- Το ThreeBears δεν χρειάζεται διάνυσμα για να επιτύχει αξιοσέβαστη ταχύτητα. Αυτό σημαίνει ότι ο κωδικός του είναι μικρός, απλός και εύκολος στον έλεγχο. Προς τα εμπρός η διόρθωση σφαλμάτων προσθέτει πολυπλοκότητα, αλλά είναι μόνο περίπου 75 γραμμές του κώδικα C και είναι εύκολο να δοκιμάστεί ξεχωριστά.

Digital Signature Algorithms: [77,78]

18. CRYSTALS-DILITHIUM

Όσο αφορά τους αλγόριθμους της δεύτερης ομάδας έτσι όπως μοιράστηκαν από τον NIST αυτοί αφορούν τους αλγόριθμους ψηφιακής υπογραφής. Το Crystals Dilithium είναι ένα σχέδιο ψηφιακής υπογραφής που είναι έντονα ασφαλές υπό επιλεγμένες επιθέσεις μηνυμάτων που βασίζονται στην σκληρότητα των προβλημάτων πλέγματος πάνω από τα πλαίσια των υπομονάδων. Η έννοια της ασφάλειας σημαίνει ότι ένας αντίπαλος που έχει πρόσβαση σε ένα oracle υπογραφής δεν μπορεί να παράγει μια υπογραφή ενός μηνύματος του οποίου η υπογραφή δεν έχει ακόμη δει, ούτε να παράγει διαφορετική υπογραφή ενός μηνύματος που έχει ήδη υπογράψει.

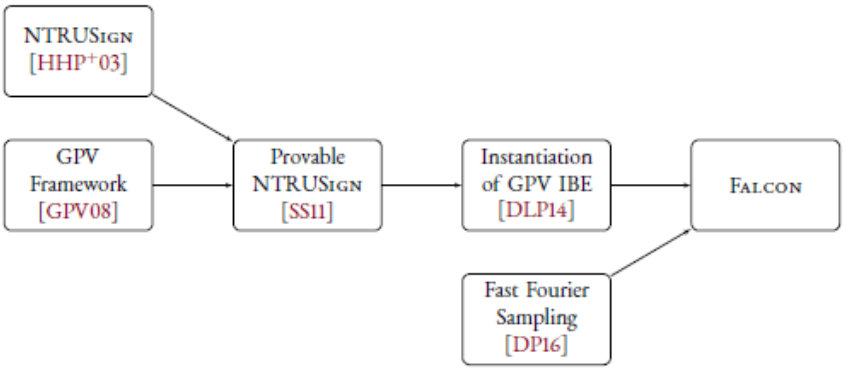
Η καινοτομία του Crystals Dilithium είναι πάνω από ταπροηγούμενα συστήματα καθώς επίσης συρρικνώνεται το μέγεθος του δημόσιου κλειδιού κατά 2,5 φορές στην δαπάνη αύξησης της υπογραφής κατά περίπου 150 byte. Για τη συνιστώμενη ασφάλεια στο επίπεδο, το σύστημα έχει υπογραφές 2.7KB και δημόσια κλειδιά 1.5KB. Η κύρια παρατήρηση για την επίτευξη αυτού του πολύ ευνοϊκού συμβιβασμού είναι ότι όταν ο επαληθευτής υπολογίζει το w'_1 στη Γραμμή 13, τα bits υψηλής τάξης του Az - ct δεν εξαρτώνται πάρα πολύ από τα bits χαμηλής τάξης του t επειδή το t πολλαπλασιάζεται με πολυώνυμο πολύ χαμηλού βάρους c. Στο σχέδιο των σχεδιαστών του παρουσιάζονται, μερικά bits χαμηλής τάξης t που δεν περιλαμβάνονται στο δημόσιο κλειδί και έτσι ο επαληθευτής δεν μπορεί πάντα να υπολογίσει σωστά τα bits υψηλής τάξης του Az-ct. Για να αντισταθμιστεί αυτό, ο υπογράφων περιλαμβάνει κάποιες "συμβουλές" ως μέρος της υπογραφής, οι οποίες ουσιαστικά φέρουν που προκαλείται από την προσθήκη στο προϊόν του c με τα λείπει κομμάτια χαμηλής τάξης του t. Με αυτή την υπόδειξη, ο επαληθευτής είναι σε θέση να υπολογίσει σωστά w'_1.

Ο πιο απλός τρόπος αύξησης ή μείωσης της ασφάλειας του Dilithium είναι με την αλλαγή στι τιμές του (k, `) και στη συνέχεια με την προσαρμογή την τιμή του αναλόγως.Η αύξηση (k, `) κατά 1 το καθένα έχει ως αποτέλεσμα το δημόσιο κλειδί να αυξάνεται κατά 300 bytes και η υπογραφή με 700 bytes. Η ασφάλεια αυξάνεται κατά 30 bits.

Ένας διαφορετικός τρόπος για να αυξηθεί η ασφάλεια θα ήταν η μείωση των τιμών του 1 και ή 2. Αυτό θα έκανε υπογραφές σφυρηλασίας. Αντί να αυξάνεται το μέγεθος του δημόσιου κλειδιού - υπογραφής, η αρνητική επίδραση της μείωσης της είναι ότι η υπογραφή θα απαιτούσε περισσότερες επαναλήψεις. Θα μπορούσε επίσης να αυξήσει την αξία του προκειμένου να καταστήσει το πρόβλημα LWE δυσκολότερο στις περισσότερες επαναλήψεις.

19. FALCON

Το Falcon (Fast-Fourier Lattice-based) είναι ένα κρυπτοσύστημα ψηφιακής υπογραφής που συμμετέχει στον διαγωνισμό και ανήκει στην κατηγορία των πλεγμάτων. Το συγκεκριμένο κρυπτοσύστημα για να δημιουργηθεί έπρεπε να υπάρξει συνδιασμός του πλαίσιου GPV με τα πλέγματα NTRU καθώς και την δειγματοληψία Fast Fourier. Ο τρόπος με τον οποίο σχηματίστηκε το FALCON φένεται ξεκάθαρα στον σχήμα που ακολουθεί.



Εικόνα 4.4: Γενεαλογικό Δέντρο FALCON

Υπάρχουν τρείς συγκεκριμένες εκδοχές του FALCON. Το FALCON 512,το FALCON 768 και το FALCON 1024.Για να δωθεί ένα σημείο σύγκρισης, το Falcon-512 είναι περίπου ισοδύναμο, με κλασικούς όρους ασφαλείας, με το RSA-2048, των οποίων οι υπογραφές και τα δημόσια κλειδιά χρησιμοποιούν 256 byte το καθένα. Σχετικά με τον συγκεκριμένο φορητό υπολογιστή στον οποίο έχουν ληφθεί αυτά τα μέτρα, η εφαρμογή της OpenSSL για την πλήρη υλοποίηση της συναρμολόγησης επιτυγχάνει περίπου 1500 υπογραφές ανά δευτερόλεπτο. Έτσι, η υλοποίηση αναφοράς Falcon, η οποία είναι φορητή και δεν χρησιμοποιεί συναρμολόγηση ή εγγενή, είναι ήδη τέσσερις φορές

ταχύτερη και βελτιώνεται σε μεγαλύτερα μεγέθη για μακροπρόθεσμη ασφάλεια. Ακόμα το Falcon προσφέρει τις ακόλουθες λειτουργίες ως προς τις διάφορες πτυχές της λειτουργίας της κρυπτογραφίας:

- Ασφάλεια: Χρησιμοποιείται εσωτερικός δειγματολήπτης Gauss, ο οποίος εγγυάται αμελητέα διαρροή πληροφοριών στο μυστικό κλειδί μέχρι έναν πρακτικά άπειρο αριθμό υπογραφών .
- Συμπαγές: χάρη στη χρήση πλεγμάτων NTRU, οι υπογραφές είναι σημαντικά μικρότερες από ό, τι σε οποιοδήποτε σύστημα υπογραφής βασισμένο σε πλέγμα με τις ίδιες εγγυήσεις ασφάλειας, ενώ τα δημόσια κλειδιά έχουν περίπου το ίδιο μέγεθος.
- Ταχύτητα: η χρήση της γρήγορης δειγματοληψίας Fourier επιτρέπει πολύ γρήγορες υλοποιήσεις, στις χιλιάδες υπογραφές ανά δευτερόλεπτο σε έναν κοινό υπολογιστή η επαλήθευση είναι πέντε έως δέκα φορές ταχύτερη.
- Επεκτασιμότητα: Οι λειτουργίες έχουν κόστος O (n log n) για τον βαθμό n, επιτρέποντας τη χρήση πολύ μακροπρόθεσμων παραμέτρων ασφαλείας με μέτριο κόστος.
- Οικονομία RAM: Ο βελτιωμένος αλγόριθμος δημιουργίας κλειδιών Falcon χρησιμοποιεί λιγότερο από 30 kilobytes μνήμης RAM, εκατοντάδες βελτιώσεις σε σχέση με τα προηγούμενα σχέδια όπως το NTRUSign. Το Falcon είναι συμβατό με μικρές ενσωματωμένες συσκευές με περιορισμένη μνήμη.

20. GeMSS

Το GeMSS σύμφωνα και με το όνομα του είναι ένα μεγάλο σύστημα πολλαπλών μεταβλητών υπογραφής. Το GeMSS είναι ένα σύστημα υπογραφής πολλαπλών μεταβλητών που παράγει μικρές υπογραφές. Έχει μια γρήγορη διαδικασία επαλήθευσης και ένα μέσο ή μεγάλο δημόσιο κλειδί. Το GeMSS βρίσκεται σε άμεση προέλευση από το σύστημα πολλαπλών μεταβλητών υπογραφής QUARTZ. Το QUARTZ παράγει υπογραφές 128 bit για επίπεδο ασφαλείας 80 bit και υποβλήθηκε στον διαγωνισμό Nessie Ecrypt για υπογραφές δημόσιου κλειδιού. Σε αντίθεση με πολλά συστήματα πολλαπλών μεταβλητών, δεν έχουν αναφερθεί πρακτικές επιθέσεις κατά του QUARTZ. Αυτό είναι αξιοσημείωτο γνωρίζοντας την έντονη δραστηριότητα στην κρυπτοανάλυση πολλών μεταβλητών σχημάτων. Η πιο γνωστή επίθεση παραμένει που χρησιμεύει ως αναφορά για τον ορισμό των παραμέτρων για το GeMSS. Έτσι, το GeMSS είναι χτισμένο από το κρυπτοσύστημα Εξισώσεων Κρυφού Πεδίου (HFE) χρησιμοποιώντας τροποποιητές HFEv-. Το GeMSS είναι μια ταχύτερη παραλλαγή του

QUARTZ που ενσωματώνει τα πιο πρόσφατα αποτελέσματα στην πολυπαραγοντική κρυπτογραφία για να φτάσει σε υψηλότερα επίπεδα ασφάλειας από το QUARTZ, βελτιώνοντας παράλληλα την αποτελεσματικότητα.

Άλλη μια παραλλαγή που σχεδιάστηκε από τους ίδιους διαγωνιζόμενους είναι το DualModeMS, η οποία χρησιμοποιεί μια γενική τεχνική που επιτρέπει τη μετατροπή οποιουδήποτε συστήματος πολλαπλών μεταβλητών υπογραφών που βασίζεται στο MI σε ένα νέο σχήμα με πολύ μικρότερες υπογραφές δημόσιου κλειδιού.

Σε αντίθεση με άλλους σχεδιαστές που πρότειναν κρυπτοσυστήματα για τον διαγωνισμό του NIST οι συγκεκριμένοι αναλυτές όχι μόνο δεν σταμάτησαν στην πρώτη υποβολή του κρυπτοσυστήματος αυτού αλλά μετά από εισηγήσεις και προτάσεις που υπόθηκαν στον πρώτο γύρο , πρότειναν σημαντικές αλλαγές στο κρυπτοσύστημα τους και τις εφάρμοσαν σε αυτό στον δεύτερο γύρο του διαγωνισμού. Αλλαγές όπως για παράδειγμα στις παραμέτρους που ακολουθούν. Οι παράμετροι που προτάθηκαν για το GeMSS στον πρώτο γύρο ήταν πολύ συντηρητικές όσον αφορά την ασφάλεια. Για να αντιμετώπιστεί λοιπόν αυτό έπραξαν ως έχει:

• Διέυρυναν τη χρήση αραιών πολυωνύμων στο GeMSS για να βελτιώσουν την αποτελεσματικότητα της διαδικασίας υπογραφής.

• Στη συνέχεια προτείναν 3 σύνολα παραμέτρων για κάθε επίπεδο ασφάλειας με πολλές εμπορικές συναλλαγές. Αυτό περιλαμβάνει τις αρχικές παραμέτρους του GeMSS που προτάθηκαν στον πρώτο κύκλο και δύο νέες πιο επιθετικές παραμέτρους οι οποίες είναι το BlueGeMSS και το RedGeMSS. Το RedGeMSS 128 είναι 269 φορές ταχύτερο από το GeMSS128.Το BlueGeMSS128 είναι 7.08 φορές ταχύτερο από το GeMSS128.

• Τέλος σχεδίασαν μια οικογένεια πιθανών τιμών που εξαρτάται από μία μόνο παράμετρο n και την ονόμασαν αυτή την οικογένεια FGeMSS (n).

21. LUOV

Ένας από τους σημαντικότερους υποψήφιους για την παροχή ασφαλών κρυπτογραφικών πρωτόγονων σε ένα μετακβαντικό κόσμο είναι η Πολυπαραγοντική Κρυπτογραφία. Η πολυπαραγοντική κρυπτογραφία βασίζεται στη σκληρότητα των προβλημάτων που σχετίζονται με πολυώνυμα πολυώνυμα με πεπερασμένα πεδία, όπως συστήματα επίλυσης πολυμεταβλητών εξισώσεων πολλαπλών μεταβλητών. Γενικά, η

Πολλαπλή Κρυπτογραφία είναι πολύ γρήγορη και απαιτεί μόνο μέτρια υπολογιστικά μέσα, γεγονός που την καθιστά ελκυστική για εφαρμογές σε συσκευές χαμηλού κόστους. Στον τομέα της Πολλαπλασιαστικής Κρυπτογραφίας, το Σχέδιο Σήμανσης Εξωγενούς Λιπαντικού και Οξέα (UOV) είναι ένα από τα παλαιότερα και καλύτερα μελετημένα κρυπτοσυστήματα. Το UOV αντέδρασε με επιτυχία σε σχεδόν δύο δεκαετίες κρυπτανάλυσης. Το σχήμα UOV είναι πολύ απλό και έχει μικρές υπογραφές και είναι και γρήγορο. Το κύριο μειονέκτημα του UOV είναι αναμφισβήτητα ότι τα δημόσια κλειδιά του είναι αρκετά μεγάλα. Αυτό το έγγραφο παρουσιάζει το σύστημα ανυψωμένης έλλειψης ισορροπίας λαδιού και ξυδιού (LUOV), το οποίο είναι μια απλή βελτίωση του συστήματος UOV που μειώνει σημαντικά το μέγεθος των δημόσιων κλειδιών. Το πρόγραμμα LUOV είναι μια προσαρμογή του συστήματος υπογραφής ισορροπημένων συστατικών. Διαφέρει από το αρχικό σύστημα UOV με διάφορους τρόπους. Η πρώτη τροποποίηση, λόγω του Petzoldt, αλλάζει τον αλγόριθμο δημιουργίας κλειδιού για να καταστεί δυνατή η επιλογή ενός μεγάλου μέρους του δημόσιου κλειδιού. Μπορεί κανείς να επιλέξει αυτό το μέρος για να αντιστοιχεί με την έξοδο μιας γεννήτριας ψευδοτυχαίων αριθμών και να αντικαταστήσει ένα μεγάλο μέρος του δημόσιου κλειδιού με ένα σπόρο. Αυτός ο τροποποιημένος αλγόριθμος δημιουργίας κλειδιών εξακολουθεί να παράγει την ίδια κατανομή ζευγών κλειδιών και ως εκ τούτου η τροποποίηση αυτή δεν επηρεάζει την ασφάλεια του σχεδίου, υποθέτοντας ότι η έξοδος του PRNG δεν διακρίνεται από την πραγματική τυχαιότητα. Σε σύγκριση με άλλα σχήματα MQ του πρώτου γύρου του NIST, ήταν σαφές ότι η επιλογή παραμέτρων του LUOV ήταν πολύ συντηρητική. Ως εκ τούτου, για τον δεύτερο γύρο υπήρξε το περιθώριο ασφαλείας "10% στο εκθέτη" που υπήρχε στην έκδοση του Γύρου 1 του εγγράφου. Οι ενημερωμένες παράμετροι που άλλαξαν στην συνέχεια του διαγωνισμού έχουν ως αποτέλεσμα ταχύτερη υπογραφή με μικρότερα πλήκτρα και υπογραφές. Η έκδοση του δεύτερου γύρου περιλαμβάνει ένα 16 byte SALT σε κάθε μήνυμα. Αυτό βελτιώνει την ασφάλεια του LUOV από τις επιθέσεις πλαϊνών καναλιών και την επίθεση κατά της έγχυσης σφαλμάτων.

22. MQDSS

Το MQDSS είναι μια ψηφιακή υπογραφή που βασίζεται στη σκληρότητα του προβλήματος MQ δηλαδή στο πολυπαραγοντικό τετραγωνικό. Είναι το πρώτο σύστημα υπογραφής πολλών μεταβλητών, του οποίου η ασφάλεια έχει αποδειχθεί στο τυχαίο

μοντέλο ORACLE. Ο σχεδιασμός του MQDSS ακολουθεί το πρότυπο Fiat-Shamir για τη μετατροπή ασφαλών συστημάτων αναγνώρισης σε ασφαλείς ψηφιακές υπογραφές. Λαμβάνεται από το σύστημα ταυτοποίησης SSH (Sakumoto, Shirai και Hiwatari) 5-pass. Ο MQDSS είναι ένας από τους υποψήφιους αλγορίθμους του έργου NIST μετά την κβαντική κρυπτογράφηση.

Η υποβολή του στον διαγωνισμό προτείνεται από δύο σύνολα παραμέτρων με τα επίπεδα στόχου 1-2 και 3-4. Το MQDSS-31-48 που αφορά το επίπεδο ασφαλείας 1-2 και το MQDSS-31-64 που αφορά το επίπεδο ασφαλείας 3-4. Όσο αφορά την συμμετοχή του κρυπτοσυστήματος στον δεύτερο γύρο του διαγωνισμού δεν έχουν και τρομερές αλλαγές από την ομάδα που το σχεδίασε ωστόσο έγιναν κάποιες μικρές αλλαγές σχεδιασμού που είχαν ως αποτέλεσμα τη βελτίωση της ευαισθησίας όσον αφορά το μέγεθος και την ταχύτητα υπογραφής, καθώς και τη βελτίωση της ανάλυσης ασφαλείας. Οι παρακάτω μικρές τροποποιήσεις σχεδίασης έγιναν με την δέσμευση λειτουργίας που αποτελεί πρόσθετο επιχείρημα με μια τυχαία σειρά μήκους 2k. Ο λόγος αυτής της αλλαγής είναι ότι με αυτή την πρόσθετη τυχαία είσοδο μπορεί να αποδειχθεί ότι η συνάρτηση δέσμευσης στο MQDSS παράγεται χρησιμοποιώντας το SHAKE256 που κρύβεται υπολογιστικά με μια ιδιότητα που χρειάζεται για να δείξει την ασφάλεια EU-CMA του MQDSS. Υπάρχη επιπλέον μια ενημέρωση των αλγορίθμων για τη δημιουργία, την υπογραφή και την επαλήθευση των κλειδιών ανάλογα με την αλλαγή αυτής της αλλαγής. Έχουμε επίσης ενημερώσει την ανάλυση ασφάλειας.

Ο αριθμός των γύρων r έχει μειωθεί στο μισό. Ο λόγος αυτής της αλλαγής είναι ότι ο απαιτούμενος αριθμός γύρων r είναι ο μισός από τον αριθμό που δίνεται στον αρχικό τερματισμό. Συνέπεια των εισαγόμενων τροποποιήσεων είναι ότι για όλα τα επίπεδα ασφαλείας, το μέγεθος της υπογραφής μειώνεται κατά περισσότερο από 35%. Υπάρχει επίσης μείωση του μεγέθους του κοινού και των μυστικών κλειδιών . Ακόμα η απόδοση της αναφοράς και η βελτιστοποιημένη εφαρμογή βελτιώνονται σημαντικά. Δηλαδή, στην εφαρμογή αναφοράς η διαδικασία υπογραφής και επαλήθευσης είναι 50% ταχύτερη από τους ίδιους αλγόριθμους στην Έκδοση 1.0. Η βελτίωση της βελτιστοποιημένης εφαρμογής δεν είναι τόσο δραματική, αλλά εξακολουθεί να είναι περίπου το 40%. Επιπλέον, έγινε πιο ακριβής ανάλυση για τις καλύτερες κλασσικές επιθέσεις κατά του προβλήματος MQ και η εκτιμώμενη κλασσική πολυπλοκότητα δίνεται τώρα από την άποψη των πύλων. Εν κατακλείδι όποιες αδυναμίες ή αρνητικά σχόλια είχε μαζέψει το κρυπτοσύστημα στον πρώτο γύρω του διαγωνισμού φένεται να

τα επιλύει σημαντικά στον δεύτερο γύρο και να θέτει σοβαρή ηποψηφιότητα για να συμμετέχει και στον τρίτο γύρο του διαγωνισμού.

23. Picnic

Η ομάδα των Picnic αλγορίθμων ψηφιακής υπογραφής έχει σχεδιαστεί για να παρέχει ασφάλεια έναντι επιθέσεων από κβαντικούς υπολογιστές, εκτός από τις επιθέσεις από κλασικούς υπολογιστές. Τα δομικά στοιχεία είναι ένα σύστημα απόδειξης μηδενικής γνώσης με μετακβαντική ασφάλεια και συμμετρικά βασικά πρωτότυπα, όπως λειτουργίες κατακερματισμού και κρυπτογραφημένα ψηφία, με καλά κατανοητή μετακβαντική ασφάλεια. Το Picnik δεν απαιτεί αριθμητικές θεωρητικές ή δομημένες υποθέσεις σκληρότητας. Πρόκειται για ένα σχέδιο υπογραφής που έχει σχεδιαστεί για να παρέχει ασφάλεια από επιθέσεις από κβαντικούς υπολογιστές, εκτός από επιθέσεις από τους κλασσικούς υπολογιστές. Το σύστημα χρησιμοποιεί σύστημα απόδειξης μηδενικής γνώσης και βασίζεται σε συμμετρικά αρχέγονα κλειδιά όπως λειτουργίες κατακερματισμού και κρυπτογράφηση μπλοκ με υποτιθέμενη ασφάλεια postquantum. Συγκεκριμένα, το Picnic δεν βασίζεται σε υποθετικές αριθμητικές θεωρητικές ή αλγεβρικές συνθήκες σκληρότητας. Το δημόσιο κλειδί στο Picnic είναι το ζεύγος (C, p) όπου C = E (sk, p) και όπου E είναι ένας κρυφός κωδικός, sk ένα μυστικό κλειδί και το p είναι ένα block plaintext. Ο κρυπτογραφικός αποκλεισμός E είναι LowMC [ARS + 16, ARS +15]. Για να δημιουργήσει μια υπογραφή, ο υπογράφων δημιουργεί μια μη ενδιαφέρουσα απόδειξη της γνώσης του sk και δεσμεύει την απόδειξη με το μήνυμα που θα υπογραφεί. Το LowMC επιλέχθηκε επειδή το προκύπτον μέγεθος υπογραφής είναι μικρότερο από τις εναλλακτικές επιλογές. Η απόδειξη της γνώσης είναι είτε μια εξειδικευμένη έκδοση του ZKBoo, που ονομάζεται ZKB + CDG + 17b. Στην άτυπη μορφή της αλληλεπιδραστικής έκδοσης ενός από τα συστήματα απόδειξης, ο διαχειριστής προσομοιώνει ένα πρωτόκολλο υπολογισμού πολλαπλών μερών σε πρωτόκολλο MPC το οποίο επιτρέπει στα μέρη να επαληθεύσουν από κοινού ότι E(sk, p) = C, όταν κάθε μέρος έχει ένα μερίδιο sk. Για το Picnic, ο αριθμός των κομμάτων είναι μια παράμετρος. Η ιδέα είναι να δεσμευτεί ο υπεύθυνος για την προσομοίωση της κατάστασης και των μεταγραφών όλων των μερών, και στη συνέχεια να έχει ανοίξει ένα τυχαίο υποσύνολο των προσομοιωμένων κομμάτων, βλέποντας την πλήρη κατάσταση τους. Ο ελεγκτής ελέγχει έπειτα ότι ο υπολογισμός έγινε σωστά από την πλευρά των ανοιχτών μερών και εάν ναι, έχει κάποια βεβαιότητα ότι η παραγωγή είναι σωστή. Το πρωτόκολλο MPC διασφαλίζει ότι το άνοιγμα ενός υποσυνόλου των συμβαλλομένων δεν αποκαλύπτει

πληροφορίες σχετικά με το μυστικό. Η παρεμπόδιση αυτής της διαδικασίας πολλές φορές παράλληλα δίνει τη βεβαιότητα ότι ο διαχειριστής γνωρίζει το μυστικό. Με την συνέχεια του αλγορίθμου στον δεύτερο γύρο του διαγωνισμού η αυστριακή ερευνητική ομάδα που το σχεδίασε προχώρησε σε αλλαγή σχετικά με το spec για να αντιμετωπιστεί μια επίθεση πολλαπλών στόχων που ανέφερθηκε σαν σχόλιο στον πρώτο γύρο από τους Dinur και Nadler . Σε υψηλό επίπεδο, η επίθεσή τους περιλαμβάνει έναν επιτιθέμενο που υποθέτει μια μυστική αξία που χρησιμοποιείται από έναν υπογράφοντα, αντλεί δεδομένα από αυτό το μυστικό ως υπογράφοντα και στη συνέχεια συγκρίνει αυτά τα δεδομένα με δεδομένα από πολλαπλές υπογραφές για να ελέγξει για αγώνες. Εάν το μυστικό είναι μακρύ και έχει υπογραφεί με T, αυτό μειώνει τον αναμενόμενο χρόνο για να επιτύχει μια επίθεση από 2k σε περίπου 2k-7 / T. Η αλλαγή στο spec για την αντιμετώπιση αυτής της επίθεσης συνεπάγεται ότι ο υπογράφων χρησιμοποιεί μια τυχαία τιμή salt ανά υπογραφή. Προσθέτουν τέλος επιπλέον μετρητές για να διασφαλίσουν ότι όλες οι εισροές μέσα σε μια υπογραφή χρησιμοποιώντας το ίδιο salt έχουν επίσης ένα μοναδικό salt.

24. qTESLA

Στο qTESLA όλα πρόκεινται για μια ευέλικτη οικογένεια συστημάτων μετά την κβαντική υπογραφή που βασίζονται στη σκληρότητα του προβλήματος του RLWE (Decision Learning With Errors). Το qTESLA είναι μια αποτελεσματική παραλλαγή του σχεδίου υπογραφής Bai-Galbraith το οποίο με τη σειρά του βασίζεται στο πλαίσιο "Fiat-Shamir with Aborts" από τον Lyubashevsky προσαρμοσμένο στη ρύθμιση των ιδανικών πλεγμάτων.

Το qTESLA χρησιμοποιεί δύο διαφορετικές προσεγγίσεις για την παραγωγή παραμέτρων προκειμένου να στοχεύει ένα ευρύ φάσμα σεναρίων εφαρμογής. Η πρώτη προσέγγιση, που αναφέρεται ως " heuristic qTESLA", ακολουθεί μια γενετική ευρετική παράμετρο. Η δεύτερη προσέγγιση, που αναφέρεται ως "provably secure qTESLA", ακολουθεί μια αποδεδειγμένα ασφαλή παραγωγή παραμέτρων σύμφωνα με τις υπάρχουσες μειώσεις ασφαλείας.

Επιπλέον, το qTESLA περιλαμβάνει την επιλογή της χρήσης μιας τεχνικής συμπίεσης κλειδιών, η οποία αναφέρεται ως "διαχωρισμός δημόσιου κλειδιού", η οποία επιτρέπει σημαντική μείωση του μεγέθους του δημόσιου κλειδιού σε βάρος μιας σχετικά μικρής

αύξησης του μεγέθους της υπογραφής.

Τα κύρια χαρακτηριστικά της qTESLA μπορούν να συνοψιστούν ως εξής:

• Απλότητα. Το qTESLA είναι απλό και εύκολο στην υλοποίηση και ο σχεδιασμός του καθιστά δυνατή την υλοποίηση συμπαγών και φορητών υλοποιήσεων που επιτυγχάνουν υψηλή απόδοση. Επιπλέον, η χρήση ενός απλοποιημένου δειγματολήπτη Gauss περιορίζεται στην παραγωγή κλειδιών.

• Ευελιξία παραμέτρων. Ο ευέλικτος σχεδιασμός του qTESLA υποστηρίζει παραμέτρους που ορίζονται ετεροδικώς ή ακολουθώντας μια αποδεδειγμένα ασφαλή προσέγγιση και υποστηρίζει και τους κυκλοτομικούς δακτυλίους ισχύος δύο και μη ισχύος.

• Συμπαγή. Οι υπογραφές qTESLA σχεδιάζονται να είναι σχετικά μικρές, καθιστώντας το συνδυασμένο μέγεθος της υπογραφής και του δημόσιου κλειδιού ανταγωνιστικό με άλλες υπάρχουσες εναλλακτικές λύσεις σε σχέση με τα ιδανικά σύνολα. Επιπλέον, το qTESLA περιλαμβάνει μια παραλλαγή που χρησιμοποιεί μια απλή τεχνική διαχωρισμού δημόσιου κλειδιού για να επιτύχει μια δραματική μείωση του μεγέθους του δημόσιου κλειδιού σε βάρος μιας σχετικά μικρής αύξησης του μεγέθους της υπογραφής.

• Θεμέλιο ασφάλειας. Η υποκείμενη ασφάλεια του qTESLA βασίζεται στη σκληρότητα του αποφασιστικού προβλήματος R-LWE και συνοδεύεται από μια σφικτή απόδειξη ασφαλείας στο κβαντικό τυχαίο μοντέλο Oracle.

• Πρακτική ασφάλεια. Με το σχεδιασμό, το qTESLA διευκολύνει τις ασφαλείς εφαρμογές. Συγκεκριμένα, υποστηρίζει υλοποιήσεις ασφαλής από επιθέσεις χρονισμού και προσωρινής μνήμης από τη στιγμή που ο χρόνος εκτέλεσης τους δεν εξαρτάται από τις μυστικές αξίες και είναι εγγενώς προστατευμένο από ορισμένες απλές αλλά ισχυρές επιθέσεις σφαλμάτων.

• Επεκτασιμότητα και φορητότητα. Ο απλός σχεδιασμός του qTESLA καθιστά εύκολη την υποστήριξη περισσότερων από ένα επιπέδων ασφαλείας και παραμέτρων με μία και μοναδική φορητή εφαρμογή.

• Υψηλή ταχύτητα. Το qTESLA, ειδικά η περίπτωση των ευρετικών συνόλων παραμέτρων, επιτυγχάνει πολύ υψηλές επιδόσεις για τις λειτουργίες που είναι συνήθως κρίσιμες κατά το χρόνο, δηλαδή την υπογραφή και την επαλήθευση. Αυτό επιτυγχάνεται σε βάρος μιας μέτρια πιο ακριβής γενεάς κλειδιού, η οποία συνήθως εκτελείται με μεγάλη προσοχή.

Η ασφάλεια του qTESLA αποδεικνύεται χρησιμοποιώντας την αναγωγική προσέγγιση. Δηλαδή δημιουργήθηκε μια αποτελεσματική μείωση που μετατρέπει κάθε επιτυχημένο αντίπαλο έναντι του qTESLA σε ένα που λύει το R-LWE. Αντίστοιχα, όσο αφορά την ευριστική του qTESLA έτσι ώστε οι αντίστοιχες παράμετροι R-LWE δηλαδή η διάσταση n, και η τυπική απόκλιση της διακριτής Gaussian κατανομής σ, και το μέτρο q γίνεται παροχή της περίπτωσης R-LWE ορισμένης σκληρότητας. Αυτή η προσέγγιση χαρακτηρίζει την εκτέλεση υψηλής ταχύτητας και ένα μικρό αποτύπωμα μνήμης ενώ απαιτεί σχετικά συμπαγή κλειδιά και υπογραφές. Εφόσον οι μειώσεις ασφαλείας είναι επίσης σαφείς και αναφέρονται ρητά μια παράσταση του qTESLA με μια παράσταση R-LWE, γίνεται επιλογή παραμέτρων τέτοιων ώστε να συμφωνούν με τη μείωση της ασφάλειας. Δηλαδή, αυτές οι instantiations qTESLA, που ονομάζονται σύνολα παραμέτρων qTESLA και είναι αποδεδειγμένα ασφαλείς, είναι προφανώς ασφαλείς στο κβαντικό μοντέλο μαντείου.

25. Rainbow

Όπως και στον MC-Eliece έτσι και εδώ το κρυπτοσύστημα Rainbow αναλύθηκε ξεχωριστά στο κεφάλαιο 3 και συγκεκριμένα στο υποκεφάλαιο 3.5 Συναρτήσεις πολλών Μεταβλητών σελ. 45-46 καθώς πρόκειται για ένα από τα κρυπτοσυστήματα που αποτελούν ήδη διάσημα και μένεται ότι θα πρωταγωνιστήσουν στον μέλλον.

26. SPHINCS+

Το τελευταίο κρυπτοσύστημα που συμπληρώνει αυτή την λίστα του δεύτερου γύρου του διαγωνισμού του NIST είναι το κρυπτοσύστημα SPHINCS+. Το SPHINCS σχεδιάστηκε ως ένα σύστημα απάτης που βασίζεται σε κατακερματισμό και ήταν το πρώτο σχέδιο υπογραφής για να προτείνει παραμέτρους για να αντισταθεί στην κβαντική κρυπτανάλυση. Το SPHINCS χρησιμοποιεί πολλά στοιχεία από το XMSS αλλά συνεργάζεται με μεγαλύτερα πλήκτρα και υπογραφές για την εξάλειψη της κατάστασης.

Σε υψηλό επίπεδο, το SPHINCS + λειτουργεί σαν το SPHINCS. Η βασική ιδέα είναι ότι γίνεται πιστοποίηση για ένα τεράστιο αριθμό ζευγών κλειδιών (FTS) με λίγα χρονικά διαστήματα χρησιμοποιώντας ένα λεγόμενο hypertree. Τα σχήματα FTS είναι σχήματα υπογραφής που επιτρέπουν σε ένα ζεύγος κλειδιών να παράγει ένα μικρό αριθμό

υπογραφών, π.χ., με τη σειρά των δέκα για τα σύνολα παραμέτρων. Για κάθε νέο μήνυμα, ένα (ψευδο) τυχαίο ζεύγος κλειδιών FTS επιλέγεται για να υπογράψει το μήνυμα. Η υπογραφή αποτελείται στη συνέχεια από την υπογραφή FTS και από τις πληροφορίες ελέγχου ταυτότητας για αυτό το ζεύγος κλειδιών FTS. Οι πληροφορίες αυθεντικοποίησης είναι κατά προσέγγιση μια υπογραφή hypertree, δηλ. Μια υπογραφή που χρησιμοποιεί ένα δέντρο πιστοποίησης των υπογραφών δένδρων Merkle. Πιο συγκεκριμένα, ένα hypertree είναι ένα δέντρο των υπογραφών που βασίζονται σε κατακερματισμό (MTS). Αυτές οι πολυάριθμες υπογραφές επιτρέπουν σε ένα ζεύγος κλειδιών να υπογράψουν έναν ορισμένο αριθμό N μηνυμάτων για το SPHINCS + και το N είναι δύναμη 2, για παράδειγμα 256. Τα ίδια τα ζεύγη κλειδιών MTS είναι οργανωμένα σε ένα Nary tree με d στρώματα. Στο πάνω στρώμα d-1 υπάρχει ένα μοναδικό ζεύγος κλειδιών MTS το οποίο χρησιμοποιείται για την υπογραφή των δημόσιων κλειδιών των ζευγών κλειδιών N MTS που σχηματίζουν το στρώμα d-2. Κάθε ένα από αυτά τα ζεύγη κλειδιών N MTS χρησιμοποιείται για να υπογράψει ένα άλλο δημόσιο κλειδί N-MTS που σχηματίζει το επίπεδο d-3. Αυτό πηγαίνει προς τα κάτω στα ζεύγη κλειδιών N d-1 στο κάτω στρώμα τα οποία χρησιμοποιούνται για την υπογραφή δημόσιων κλειδιών N FTS, το καθένα, οδηγώντας σε ένα συνολικό αριθμό ζευγών κλειδιών FTS που έχουν πιστοποιηθεί με Nd. Οι πληροφορίες ελέγχου ταυτότητας για ένα ζεύγος κλειδιών FTS αποτελούνται από τις υπογραφές d MTS που δημιουργούν μια διαδρομή από το ζευγάρι κλειδιών FTS στο κορυφαίο δέντρο MTS. Μια υπογραφή MTS είναι απλά μια κλασσική υπογραφή Merkle-tree στην περίπτωση του SPHINCS +. Αποτελείται από μια μονοσήμαντη υπογραφή (OTS) στο δεδομένο μήνυμα συν τη διαδρομή επαλήθευσης ταυτότητας στο δυαδικό hash-tree, που πιστοποιεί τα ζεύγη κλειδιών N OTS ενός ζεύγους κλειδιών MTS. Το δημόσιο κλειδί του SPHINCS + είναι ουσιαστικά το δημόσιο κλειδί του κορυφαίου επιπέδου MTS, το οποίο είναι ακριβώς ο ριζικός κόμβος του δυαδικού δέντρου κατακερματισμού και ως εκ τούτου, μια μοναδική τιμή hash. Ωστόσο, τα πραγματικά SPHINCS + δημόσια κλειδιά περιέχουν επιπλέον μια δημόσια τιμή σπόρου του ίδιου μήκους με τον κόμβο ρίζας. Αυτό οφείλεται σε τεχνικούς λόγους που εξηγούνται στην λεπτομερή προδιαγραφή κατωτέρω. Το μυστικό κλειδί SPHINCS + είναι μόνο μία μυστική τιμή σπόρου.

Από αυτά, όλα τα μυστικά κλειδιά OTS και FTS δημιουργούνται με ψευδοτυχαίο τρόπο. Τα μυστικά κλειδιά OTS και FTS από κοινού καθορίζουν πλήρως ολόκληρη την εικονική δομή ενός ζεύγους κλειδιών SPHINCS +. Και πάλι, τα πραγματικά μυστικά κλειδιά SPHINCS + περιέχουν μια επιπλέον μυστική αξία του ίδιου μεγέθους με τον μυστικό

σπόρο καθώς και ένα αντίγραφο του δημόσιου κλειδιού. Η πρόσθετη τιμή χρησιμοποιείται για το κλειδί μιας PRF που χρησιμοποιείται σε τυχαιοποιημένο hashing όπως περιγράφεται λεπτομερώς στην παρακάτω σύγκριση.

4.4 Συγκριτική Ανάλυση Αλγορίθμων NIST

Σε αυτήν την υποενότητα θα προσπαθήσει να γίνει μια σιγκριτική ανάλυση των αλγορίθμων που συνεχίζουν αυτή την στιγμή στον διαγωνισμό του NIST. Δηλαδή των 26 αλγορίθμων ως προς τα τεχνικά χαρακτηριστικά τους για να αποδειχτεί έτσι ποιοί αλγόριθμοι ξεχωρίζουν και σε ποιες πτυχές τους.

Μέγεθος κλειδιών:

- Δημόσιο κλειδί:

Ο αλγόριθμος με το μεγαλύτερο μέγεθος δημοσίου κλειδιού είναι ο MCEliece με 1mb ενώ το μικρότερο δημόσιο κλειδί παρουσιάζει ο SIKE 1b που είναι κρυπτοσύστημα ελλειπτικής καμπύλης.

- Ιδιωτικό κλειδί:

Ο αλγόριθμος με το μεγαλύτερο μέγεθος ιδιωτικού κλειδιού είναι ο RAINBOW με 95kb ενώ με το μικρότερο μέγεθος κλειδιού είναι και πάλυ ο SIKE με 32b.

Υπογραφή:

Το μέγεθος της μεγαλύτερης υπογραφής το διαθέτει ο SPHINCS+ με 41 KB και την μικρότερη υπογραφή ο SIKE με 65b. Ακόμα την ασφαλέστερη υπογραφή διαθέτει το CRYSTALS-Dilithium και το qTesla είναι ανώτερο για την επαλήθευση της υπογραφής.

Ταχύτητα:

Το NewHope είναι ο πιο δοκιμασμένος και ο γρηγορότερος των αλγορίθμων που τον κάνει καλό υποψήφιο για να αντικαταστήσει τα τρέχοντα κρυπτοσυστήματα. Η ταχύτητά του είναι συγκρίσιμη με τον RSA που χρησιμοποιείται σήμερα αλλά και τον

ECDH. Το κύριο μειονέκτημα του σε σχέση με τον RSA και τον ECDH είναι το γεγονός ότι το δικό του πρωτόκολλο απαιτεί τη μετάδοση περισσότερων δεδομένων ,συγκεκριμένα 5 φορές περισσότερο από αυτό του RSA και 50 φορές περισσότερο από αυτό του ECDH.

Επιπλέον αξίζει να σημειωθεί το γεγονός ότι το NTRU είναι μεταξύ του SIDH και του NewHope όταν πρόκειται για το μέγεθος και την απόδοση του κλειδιού. Είναι ταχύτερο από το SIDH, αλλά έχει μεγαλύτερο γενικό κόστος επικοινωνίας. Είναι πιο αργό από το NewHope, αλλά έχει λιγότερα έξοδα επικοινωνίας. Έτσι να το καθιστά ικανό να πλασαριστεί και αυτό με την σειρά του ψηλά στον πίνακα των μετακβαντικών κρυπτοσυστημάτων.[82]

Χρόνος Καθυστέρησης:

Μεταξύ των αλγορίθμων KEM του επιπέδου ασφάλειας 1, το NTRU HRSS είναι ανώτερο όσον αφορά την καθυστέρηση και το LAP. Παράλληλα το κρυπτοσύστημα SPHINCS + είναι το πιο δαπανηρό όσον αφορά την καθυστέρηση και το LAP.

Κατανάλωση Ισχύς:

Τα FrodoKEM και SPHINCS+ όσο αφορά τα ASICs διαθέτουν μικρές μονάδες αποκατάστασης που καταναλώνουν χαμηλή ισχύ και χρησιμεύουν έτσι σε IoT συσκευές, αν το επίπεδο ασφάλειας 1 αρκεί.

Χρήση σε διακομιστές:

Το NTRU-HRSS και το NewHope σε επίπεδο ασφάλειας 1 είναι τα γρηγορότερα ASIC και τα πιο κατάλληλα για χρήση σε διακομιστές. [83]

4.5 Που στηρίζεται η ανάγκη για προκήρυξη του Διαγωνισμού [79,80]

Ο NIST αποφάσισε ότι είναι συνετό να αρχίσουμε τώρα να αναπτύσσουμε πρότυπα για τη μετακβαντική κρυπτογράφηση. Αυτό οφείλεται σε δύο παράγοντες. Πρώτον, υπήρξε αξιοσημείωτη πρόοδος στην ανάπτυξη κβαντικών υπολογιστών, συμπεριλαμβανομένων των θεωρητικών τεχνικών για τη διόρθωση του κβαντικού σφάλματος και τον κβαντικό υπολογισμό ανεκτικών σε σφάλματα, καθώς και πειραματικές επιδείξεις φυσικών qubits και λειτουργιών εμπλοκής σε αρχιτεκτονικές που έχουν τη δυνατότητα να κλιμακώνονται στα μεγαλύτερα συστήματα.

Δεύτερον, φαίνεται ότι η μετάβαση στην μετάκβαντική κρυπτογραφία δεν θα είναι απλή, καθώς είναι απίθανο να είναι μια απλή "drop-in" αντικατάσταση για τους τρέχοντες κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού. Θα χρειαστεί μια σημαντική προσπάθεια για την ανάπτυξη, την τυποποίηση και την ανάπτυξη νέων κβαντικών κρυπτοσυστημάτων. Επιπλέον, αυτή η μετάβαση πρέπει να πραγματοποιηθεί πολύ πριν κατασκευαστούν μεγάλοι κβαντικοί υπολογιστές, έτσι ώστε οποιαδήποτε πληροφορία που αργότερα θα διακυβευτεί από την κβαντική κρυπτανάλυση να μην είναι πλέον ευαίσθητη όταν συμβεί αυτός ο συμβιβασμός. Ως εκ τούτου, είναι επιθυμητό να προγραμματιστεί η μετάβαση αυτή νωρίς.

Ως αποτέλεσμα αυτών των περιπλοκών, ο NIST πιστεύει ότι η διαδικασία ανάπτυξης των μετακβαντικών προτύπων δεν πρέπει να αντιμετωπίζεται ως ανταγωνισμός. Σε ορισμένες περιπτώσεις, μπορεί να μην είναι δυνατόν να γίνει μια καλά υποστηριζόμενη κρίση ότι ένας υποψήφιος είναι "καλύτερος" από άλλος. Αντίθετα, ο NIST θα εκτελέσει μια λεπτομερή ανάλυση των υποβαλλόμενων αλγορίθμων με τρόπο ανοιχτό και διαφανή για το κοινό, καθώς και να ενθαρρύνει την κρυπτογραφική κοινότητα να διεξάγει επίσης αναλύσεις και αξιολόγηση. Στο πλαίσιο της καλής και συλλογικής προσπάθειας που θέλει να προβάλει ο NIST άλλωστε είναι και τα παραδείγματα που αναφερθήκαμε ποιο πάνω τα οποία συνεχίζουν στον διαγωνισμό με την μορφή συγχωνεύσεων από άλλους αλγόριθμους που είχαν προταθεί στον πρώτο γύρο του διαγωνισμού.

Κεφάλαιο 5

Επίλογος

5.1 Σύνοψη

Η παρούσα διατριβή εστίασε στο ανοιχτό ερευνητικό πρόβλημα που έχει δημιουργηθεί στον σύγχρονο τομέα της κρυπτογράφησης. Συγκεκριμένα στην παρούσα βιβλιογραφική ανασκόπηση έγινε ανάλυση της κρυπτογραφίας του σήμερα και του αύριο. Αρχικά τονίστηκαν τα κύρια είδη της κρυπτογραφίας. Στην συνέχεια αναφέρθηκε η κβαντική κρυπτογραφία μέσω του κβαντικού υπολογισμού και έγινε μια όχι ιδιαίτερη αλλά υπαρκτή σύγκριση της κβαντικής κρυπτογραφίας με την μετέπειτα της μετακβαντική κρυπτογραφία.

Για την ανάλυση της μετακβαντικής κρυπτογραφίας έγινε ξεχωριστό κεφάλαιο όπου αναλύθηκε η κρυπτογραφία αυτή και οι κύριες κατηγορίες που την απαρτίζουν σε ξεχωριστές υποενότητες. Και οι έξι κατηγορίες που την απαρτίζουν αποτέλεσαν αντικείμενα μελέτης όπου μέσα από την κάθε κατηγορία γεννήθηκαν αρκετά και σημαντικά κρυπτοσυστήματα που κυριάρχησαν στον διαγωνισμού του οργανισμού του NIST.

Στην συνέχεια και συγκεκριμένα στο τέταρτο κεφάλαιο της εργασίας μου έγινε λεπτομερής αναφορά στον οργανισμό ο οποίος είναι αρμόδιος για την ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών στην εποχή μας. Ο οργανισμός αυτός δεν είναι άλλος από τον NIST. Ένα εδρεύων στην Αμερική οργανισμό που αναλύει ταυτόχρονα αρκετά θέματα που αφορούν την πληροφορική και στοχεύουν στην καλυτέρευση και εξειδίκευση της, στην εποχής μας. Σε επόμενη ενότητα του

κεφαλαίου αυτού έγινε παρουσίαση της προκήρυξης που δημοσίευσε στον ιστότοπο του ο οργανισμός μέσω της οποίας επικήρυξε τον διαγωνισμό για την δημιουργία μετακβαντικών κρυπτοσυστημάτων τα οποία μέλλεται να είναι ισχυρά έναντι σε επιθέσεις από κβαντικούς υπολογιστές.
Κατά την πρώτη φάση του διαγωνισμού και με την ολοκλήρωση της κατατέθηκαν από διάφορους διαγωνιζόμενους και ερευνητικές ομάδες 69 ιδέες για την δημιουργία ανάλογων κρυπτοσυστημάτων. Μετά από ένα χρονικό διάστημα που έθεσε ο NIST οι ιδέες αυτές αναλύθηκαν και αξιολογήθηκαν από το κοινό, από διάφορους ερευνητές και συνεργάτες του διαγωνισμού για να υπάρξει ένα σωστό ξεκαθάρισμα των κρυπτοσυστημάτων που ήταν άξια να προχωρήσουν στον δεύτερο γύρο του διαγωνισμού. Στον δεύτερο γύρο του διαγωνισμού προχώρησαν 26 από τους 69 αλγόριθμους οι οποίοι πέτυχαν τις καλύτερες αξιολογήσεις-σχόλια από τους διάφορους αξιολογητές τους. Οι 26 αυτοί αλγόριθμοι αναλύθηκαν ένας προς ένας σε μικρές υποενότητες ως συνέχεια του κεφαλαίου μου. Τελευταίο κομμάτι που αφορά τους μετακβαντικούς αλγόριθμους είναι η υποενότητα στην οποία έγινε μια μικρή σύγκριση διαφόρων χαρακτηριστικών μεταξύ των αλγορίθμων και τέθηκαν κάποιες γνώμες σχετικά με σκέψεις των διαφόρων αξιολογητών που αφορούν τους αλγόριθμους αυτούς σχετικά με την ασφάλεια τους, την ταχύτητα τους και άλλα χαρακτηριστικά που ενδεχομένως να απορρέουν ενδιαφέρον στο αναγνωστικό κοινό της παρούσας βιβλιογραφικής ανασκόπησης.

5.2 Συμπεράσματα–Μελλοντική έρευνα

Μέσω της βιβλιογραφικής ανασκόπησης της και της ιδιαίτερης αναφοράς στον οργανισμό NIST που έγινε στην παρούσα διατριβή γεννιούνται τα εξής συμπεράσματα τα οποία παρατίθενται τα εξής:

1. Γενικό συμπέρασμα της όλης διατριβής είναι ότι με τους ρυθμούς που εξελίσσεται η τεχνολογία της πληροφορικής και συγκεκριμένα με την δημιουργία και έλευση των κβαντικών υπολογιστών τα περισσότερα κρυπτοσυστήματα σε πολύ λίγο καιρό θα θεωρούνται απαρχαιωμένα και θα χρίζουν ριζικής αλλαγής από κρυπτοσυστήματα τα οποία θα αντέχουν από διάφορες επιθέσεις κβαντικών υπολογιστών.
2. Τα κρυπτοσυστήματα τα οποία προτείνονται για τον διαγωνισμό του οργανισμού του NIST ανήκουν και αυτά με την σειρά τους στις κύριες κατηγορίες που αναφέρθηκαν πιο πάνω στην διατριβή μου.
3. Η κύρια φιλοσοφία στην οποία είναι κατασκευασμένα τα κρυπτοσυστήματα που παρατίθενται στον διαγωνισμό του NIST είναι είτε συγγενικά με τα ήδη υπάρχων

κρυπτοσυστήματα τα οποία θεωρούνται ασφαλή και στις μέρες μας είτε είναι κομμάτια της μετεξέλιξης τους.

4. Κρυπτοσυστήματα όπως είναι αυτό του McEliece και κάποια άλλα όπως αυτά που ανήκουν στις Ελλειπτικές Καμπύλες μπορούν να ανταποκριθούν άξια στις μέρες της μετακβαντικής κρυπτογραφίας.
5. Είναι αναντίρρητο γεγονός ότι ο οργανισμός NIST έχει κατανοήσει πρώτος πλήρως το πρόβλημα που μέλλεται να υπάρξει στο μέλλον με την έλευση των κβαντικών υπολογιστών και όντας συνειδητοποιημένος προσπαθεί να συμβάλει ενεργά στην αντιμετώπιση του με τις κατάλληλες μεθόδους.
6. Μέσω του διαγωνισμού μπορούμε να δούμε πως δεν είναι μόνο η Αμερική που μπορεί να προσφέρει στην βελτίωση του τομέα της πληροφορικής καθώς πολλά κρυπτοσυστήματα έχουν προταθεί από ομάδες και ερευνητικά κέντρα στην Αυστρία , στην Γερμανία και στην Αγγλία και σε άλλες χώρες τόσο της Ευρώπης αλλά και σε άλλες Ηπείρους.
7. Από τις αξιολογήσεις του κοινού και των συνεργατών του οργανισμού τα πιο κολακευτικά σχόλια τα μάζεψε αδιαμφησβήτητα το κρυπτοσύστημα McEliece . Αυτό δηλώνει πως το κοινό φέρει προτίμηση στα ήδη δοκιμασμένα κρυπτοσυστήματα που υπάρχουν και δείχνουν τις δυνατότητες τους για επιτυχία της κρυπτογραφικής δυνατότητας τους από τώρα.
8. Όσο αφορά τα μεγέθη και κλειδιών και υπογραφών αυτά δείχνουν πως δεν είναι απαραίτητα κάποιου συγκεκριμένου μεγέθους καθώς αυτά διαφέρουν αναλόγως του τρόπου που σχεδιάστηκαν. [81]

Ως μελλοντική έρευνα αποτελεί το γεγονός που φέρει τον οργανισμό να οδεύει σύμφωνα με το χρονοδιάγραμμα το οποίο έχει δημοσιεύσει. Στην παρούσα φάση ο οργανισμός NIST τρέχει τον διαγωνισμό και σύμφωνα με το εν λόγω χρονοδιάγραμμα βρίσκεται στο κομμάτι της δημοσίευσης και αξιολόγησης των 26 κρυπτοσυστημάτων που έχουν περάσει στον δεύτερο γύρο του διαγωνισμού. Επομένως όταν λήξει η περίοδος αξιολόγησης του δεύτερου γύρου των αλγορίθμων τότε η μελλοντική έρευνα θα πορευτεί σύμφωνα με το υπόλοιπο του χρονοδιαγράμματος του διαγωνισμού. Θεωρείται ως καταληκτική ημερομηνία για την αξιολόγηση του δεύτερου γύρου η 24 Αυγούστου 2019. Μέσα στην επόμενη διετία και συγκεκριμένα μέσα στο 2020 και 2021 θα πραγματοποιηθεί κατά σειρά η δημοσίευση και αξιολόγηση των αλγορίθμων που θα πετύχουν στον τρίτο γύρο και στην συνέχεια αφού επαναξιολογηθούν πάλι από τους

αρμόδιους φορείς του οργανισμού, αλλά και τους συνεργάτες του καθώς και το ευρύ αναγνωστικό κοινό, ο οργανισμός θα προχωρήσει μέσα στο 2022 με 2024 στην τελική φάση της επιλογής των «νικητήριων» κρυπτοσυστημάτων όπου με αυτά θα πορευτεί η πληροφορική στην μετακβαντική περίοδο που μέλλεται .

Βιβλιογραφία

1. Ivan Damgard. A 'proof-reading' of some issues in cryptography. In *Automata, Languages and Programming*, pages 2–11. Springer, 2007.
2. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, November 1976.
3. Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC '82: Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 365–377, New York, NY, USA, 1982. ACM Press.
4. "Schneier on Security." *Blog*, www.schneier.com/cryptogram/archives/1999/0215.html. 1.2-1.4
5. Σύγχρονη κρυπτογραφία: Θεωρία και εφαρμογές Κεφ. 1(1.1–1.4.3), Κεφ. 7(7.2-7.3)
6. Τεχνικές κρυπτογραφίας και κρυπτανάλυσης Κεφ. 1(σελ. 1-6, 9),Κεφ. 3 (3.3 έως σελ.90)
7. Κρυπτογραφία και ασφάλεια δικτύων: Αρχές και εφαρμογές Κεφ. 2 (2.2 – 2.3)
8. Handbook of Applied Cryptography Κεφ. 1 (1.1 – 1.5), Κεφ. 7 (7.3)
9. J. Stolze and D. Suter. Quantum Computing: A Short Course from Theory to Experiment. Physics Textbook. John Wiley & Sons, 2004.
10. T.F. Sturm and J. Schulze. Quantum Computation aus algorithmischer Sicht. Oldenbourg Wissensch.Vlg, 2009.
11. Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M., 2016, August. Breaking symmetric cryptosystems using quantum period finding. In Annual Cryptology Conference (pp. 207-237). Springer, Berlin, Heidelberg.
12. "Google Plans to Demonstrate the Supremacy of Quantum Computing". IEEE Spectrum: Technology, Engineering, and Science News. Retrieved2018-01-11.https://spectrum.ieee. org/tech-talk/computing/hardware/ibmedges-closer-to-quantum-supremacy-with50qubit-processor
13. Introduction to Cryptography, W. Trappe / L. Washington, Prentice Hall Editions
14. Κβαντομηχανική Ι, ΙΙ Σ. Τραχανάς, Πανεπιστημιακές Εκδόσεις Κρήτης
15. Grimes, Roger A. "How Quantum Computers Will Destroy and (Maybe) Save Cryptography." *CSO Online*, CSO, 2 Aug. 2018,
16. Grimes, Roger A. "Preparing for the Day Quantum Computing Cracks Public-Key Cryptography: What to Do Now." *CSO Online*, CSO, 8 Aug. 2018,

17. Shor, P.:Polynomial-time algorithm for prime factorization and discrete logarithmson a quantum computer. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, vol. 124 (1994)

18. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post-Quantum Cryptography.

19. Springer, Heidelberg (2008)

20. Buchmann, J.: Introduction to Cryptography. Springer, Heidelberg (2004)

21. Buchmann, J., Dahmen, E., Ereth, S., H¨ulsing, A., R¨uckert, M.: On the security of the Winternitz one-time signature scheme. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 363–378. Springer, Heidelberg (2011)

22. D. Moody, Let's Get Ready to Rumble – The NIST PQC "Competition", PQCrypto 2018, Ft. Lauderdale, Florida, April 11, 2018,

23. Ducas, L., Micciancio, D.: FHEW: bootstrapping homomorphic encryption in less than a second. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol.9056, pp. 617–640. Springer, Heidelberg (2015)

24. Chen, L., et al.: Report on post-quantum cryptography (2016)

25. 1 https://www.keylength.com/en/4/, Keylength - NIST Report on Cryptographic Key Length and...recommendations and cryptoperiods extract from NIST Special Publication 800-57 Part 1, Recommendation for Key Management.

26. Berger, T.P., Cayrel, P.-L., Gaborit, P., Otmani, A.: Reducing key length of the McEliece cryptosystem. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 77–97. Springer, Heidelberg (2009).

27. Misoczki, R., Barreto, Paulo S.L.M.: Compact McEliece keys from goppa codes. In: Jacobson, Michael J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 376–392. Springer, Heidelberg (2009).

28. NIST: post-quantum cryptography standardization (2016).

29. Courtois, Nicolas T., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 157–174. Springer, Heidelberg (2001).

30. Berger, T.P., Cayrel, P.-L., Gaborit, P., Otmani, A.: Reducing key length of the McEliece cryptosystem. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 77–97. Springer, Heidelberg (2009).

31. R.J. McEliece, "Public Key Cryptosystem Based On Algebraic Coding Theory," JPL DSN Progress Report, pp. 114–116, 1978.

32. P.J. Lee, E.F. Brickell, "An Observation on the Security of McEliece's Public-Key Cryptosystem," in Proc. EUROCRYPT'88, vol. 330 of LNCS, pp. 275–280, Springer, 1988.

33. Boledovi˘c, A., Varga, J.: Practical implementation of McEliece cryptosystem on Android. In: 16th Central European Conference on Cryptology (CECC 2016) (2016)

34. https://cseweb.ucsd.edu/~daniele/papers/ PostQuantum.pdf Micciancio, D., Regev, O. 2008, December. Lattice-Based Cryptography

35. https://web.eecs.umich.edu/~cpeikert/pubs/ suite.pdf Peikert, C. 2014, July. Lattice Cryptography for the Internet

36. Chen, R., Peng, D.: A novel NTRU-based handover authentication scheme forwireless networks. IEEE Commun. Lett. 22(3), 586–589 (2018)

37. Bernstein, D. J. A subfield-logarithm attack against ideal lattices. The cr.yp.to blog https://blog.cr.yp.to/20140213-ideal.html (2014). 24. Bernstein, D. J., Chuengsatiansup, C., Lange, T. & van Vredendaal, C. NTRU Prime. Preprint at https://eprint.iacr.org/2016/461 (2016).

38. Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRUPrime: reducing attack surface at low cost (2017).

39. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H. & Whyte, W. NTRUSIGN: digital signatures using the NTRU lattice. In Topics in Cryptology, Proc. Cryptographers' Track at the RSA Conf. 2003 (CT-RSA 2003) (ed. Joye, M.) 122–140 (Springer, 2003)

40. Nguyen, P. Q. & Regev, O. Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures. In Advances in Cryptology, Proc. 25th Ann. International Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2006) (ed. Vaudenay, S.) 271–288 (Springer, 2006)

41. Ducas, L. & Nguyen, P. Q. Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures. In Advances in Cryptology, Proc. 18th International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012) (eds Wang, X. & Sako, K.) 433–450 (Springer, 2012)

42. Micciancio, Daniele, and Oded Regev. "Lattice-Based Cryptography." *Post-Quantum Cryptography*, pp. 147–191., doi:10.1007/978-3-540-88702-7_5.

43. Gray, Ken, and Thomas D. Nadeau. "Etsi Nfv Isg." *Network Function Virtualization*, 2016, pp. 49–76., doi:10.1016/b978-0-12-802119-4.00003-1.

44. P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Computing, vol. 26, no. 5, 1997, pp. 1484–1509.

45. S. Akleylek et al., "An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation," Proc. 9th Int'l Conf. Cryptology in Africa (AFRICACRYPT 16), LNCS 9646, Springer, 2016, pp. 44–60

46. R.C. Merkle, "A Certified Digital Signature," Proc. 9th Ann. Int'l Cryptology Conf. (CRYPTO 89), LNCS 435, Springer, 1989, pp. 218–238

47. J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS—A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions," Proc. 4th Int'l Workshop Post-Quantum Cryptography (PQCrypto 11), LNCS 7071, Springer, 2011, pp. 117–129.

48. Bernstein, Daniel J., Chou, T., Schwabe, P.: McBits: fast constant-time code-based cryptography. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 250–272. Springer, Heidelberg (2013).

49. X. Charles, E. Goren, K. Lauter, Cryptographic hash functions from expander graphs, J. Cryptol. 22 (2009), 93–113.

50. J. Ding and D. Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme," Proc. Applied Cryptography and Network Security (ACNS 05), LNCS 3531, Springer, 2005, pp. 164–175.

51. Buchmann, J., Dahmen, E., Hülsing, A.: XMSS - a practical forward secure signature scheme based on minimal security assumptions. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 117–129. Springer, Heidelberg (2011).

52. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005).

53. D.J. Bernstein, T. Chou, P. Schwabe: McBits: Fast constant-time code based cryptography. CHES 2013, LNCS vol. 8086, pp. 250 - 272. Springer, 2013.

54. L. Bettale, J.-C. Faug´ere, L. Perret: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology, 3: 177197, 2009.

55. O. Billet, H. Gilbert. Cryptanalysis of Rainbow: SCN 2006, LNCS vol. 4116, pp. 336 - 347. Springer, 2006.

56. J. Bonneau, I. Mironov: Cache-Collision Timing Attacks Against AES. CHES 2006, LNCS vol. 4249, pp. 201 - 215. Springer, 2006.

57. "Elliptic Curve Cryptography." *SpringerReference*, doi:10.1007/springerreference_234.

58. "Elliptic Curve Cryptography: The Tech Behind Digital Signatures in Cryptocurrencies." *Blockonomi*, 6 Aug. 2018, blockonomi.com/elliptic-curve-cryptography/.

59. "8. Elliptic Curve Cryptography." *A Course in Mathematical Cryptography*, doi:10.1515/9783110372779-009.

60. "Kristin Lauter at Microsoft Research." *Microsoft Research*, www.microsoft.com/en-us/research/people/klauter/.

61. De Feo, L., Jao, D., Plût, J., Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, J. Math. Cryptology 8, 209–247 (2014)

62. G. Bisson and A.V. Sutherland, Computing the endomorphism ring of an ordinary elliptic curve over a finite field, J. Number Theory, 113 (2011), 815-831.

63. Lynch, Vincent. "Understanding ECC (Elliptic Curve Cryptography) in 5 Minutes." *Hashed Out by The SSL Store™*, 4 Aug.2016, www.thesslstore.com/blog/understanding-ecc-5-minutes/.

64. Sullivan, Nick, and Utc. "A (Relatively Easy to Understand) Primer on Elliptic Curve Cryptography." *Ars Technica*, 24 Oct. 2013, arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve cryptography/.

65. "What Is Elliptical Curve Cryptography (ECC)? - Definition from WhatIs.com." *SearchSecurity*,searchsecurity.techtarget.com/definition/elliptical-curve cryptography.

66. Kocher, P. C. Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In Advances in Cryptology, Proc. 16th Ann. International Cryptology Conf. (CRYPTO '96) (ed. Koblitz, N.) 104–113 (Springer, 1996)

67. Tayoub, W., Somia, L., Chikouche, N.: Implementation of public-key cryptographic systems on embedded devices (case: Computation speed). In: The First International Symposium on Informatics and its Applications (ISIA 2014) (2014)

68. Yan, Song Y. "Quantum Computing Attacks." *Cryptanalytic Attacks on RSA*, pp. 135–148., doi:10.1007/978-0-387-48742-7_5.

69. Ekerå, Martin, and Johan Håstad. "Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers." *Post-Quantum Cryptography Lecture Notes in Computer Science*, 2017, pp. 347–363., doi:10.1007/978-3-319-59879-6_20.

70. Computer Security Division, et al. “Round 1 Submissions - Post-Quantum Cryptography.” *CSRC*, csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

71. Computer Security Division, et al. “Round 2 Submissions - Post-Quantum Cryptography.” *CSRC*, csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions.

72. U.S. Department of Commerce. Digital Signature Standard (DSS), Federal Information Processing Standards (FIPS) Publication 186-4, July 2013, 121pp.

73. NIST Special Publication (SP) 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2018, 141pp.

74. NIST Special Publication (SP) 800-56B Revision 1, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2014, 121pp.

75. NIST Workshop on Cybersecurity in a Post-Quantum World, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2-3, 2015, https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-aPost-Quantum-World

76. L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smithtone, Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 10pp. “Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms,” 81 Federal Register 92787 (December 20, 2016), pp. 92787-92788. https://federalregister.gov/a/2016-30615

77. “Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members,” 75 Federal Register 7 (January 12, 2010), pp.

78. Alagic, et al. “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process.” *CSRC*, 31 Jan. 2019, csrc.nist.gov/publications/detail/nistir/8240/final.

79. D. Moody, Post-Quantum Cryptography Standardization: Announcement and outline of NIST’s Call for Submissions, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, https://csrc.nist.gov/Presentations/2016/Announcement-and-outline-ofNIST-s-Call-for-Submis

80. "Post-Quantum Cryptography: Proposed Requirements and Evaluation Criteria," 81 Federal Register 50686 (August 2, 2016), pp. 50686-50687. https://federalregister.gov/a/2016-18150

81. Computer Security Division, et al. "Post-Quantum Cryptography Standardization - Post-Quantum Cryptography." *CSRC*, csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.

82. Valyukh, Vladimir. "Performance and Comparison of Post-Quantum Cryptographic Algorithms." Linkoping University.

83. NIST Post-Quantum Cryptography ''A Hardware Evaluation Study'' ,by Kanad Basu, Deepraj Soni, Mohammed Nabeel, and Ramesh Karri