ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Κβαντική Κρυπτογραφία

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Αναστασία Κοσμέτου (ΑΜ: 3120093)

Επιβλέπων: ***Σάββας Ηλίας***

ΛΑΡΙΣΑ, Φεβρουάριος 2025

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Quantum Cryptography

BACHELOR THESIS

Anastasia Kosmetou (RN: 3120093)

Supervisor: *Savvas Ilias*

LARISSA, February 2025

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η Δηλών/ούσα

(Υπογραφή)

Κοσμέτου Αναστασία

Ημερομηνία

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	**Σάββας Ηλίας** Βαθμίδα/ιδιότητα επιβλέποντα, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Ονοματεπώνυμο Μέλους 1** Βαθμίδα/ιδιότητα μέλους 1, Τμήμα/Ιδρυμα μέλους 1
Μέλος	**Ονοματεπώνυμο Μέλους 2** Βαθμίδα/ιδιότητα μέλους 2, Τμήμα/Ιδρυμα μέλους 2

Ημερομηνία έγκρισης: dd-mm-yyyy

Περίληψη

Οι Κβαντικοί Υπολογιστές όταν πλέον θα είναι αξιόπιστοι θα αλλάξουν ριζικά τους αλγόριθμους κρυπτογραφίας. Αυτό οφείλεται στην υπερβολική αύξηση της υπολογιστικής ισχύος με αποτέλεσμα όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι να είναι ανασφαλείς. Η παρούσα πτυχιακή μετά από μία εισαγωγή στην κβαντική υπολογιστική θα ασχοληθεί με υπάρχοντες κρυπτογραφικούς αλγόριθμους που θα καταστούν αναξιόπιστοι και θα εμβαθύνει σε μετα-κβαντικούς κρυπτογραφικούς αλγόριθμους που έχουν προταθεί ώστε να διασφαλισθεί η ασφάλεια στον ερχομό της Κβαντικής Εποχής.

Abstract

Quantum Computers when they are reliable will radically change cryptography algorithms. This is due to the excessive increase in computational power resulting in all modern cryptographic algorithms being insecure. This thesis after an introduction to quantum computing will deal with existing cryptographic algorithms that will become unreliable and will dive into post-quantum cryptographic algorithms that have been proposed to ensure security in the coming of the Quantum Era.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους με βοήθησαν κατά την συγγραφή της πτυχιακής μου εργασίας, καθώς και τον επιβλέποντα καθηγητή μου Κ. Σάββα Ηλία, που συνέβαλε για την ορθή ολοκλήρωση της πτυχιακής.

Κοσμέτου Αναστασία

Περιεχόμενα

1 Εισαγωγή

Η κβαντική υπολογιστική έχει τις ρίζες της στη δεκαετία του 1970, όταν άρχισαν να διαμορφώνονται οι πρώτες θεωρητικές ιδέες για την εφαρμογή της κβαντικής μηχανικής στους υπολογιστές. Από τότε μέχρι σήμερα, ο τομέας έχει εξελιχθεί ραγδαία, με σημαντικές θεωρητικές ανακαλύψεις, πειραματικές προόδους και πρακτικές εφαρμογές.

1.1.1 Δεκαετία 1970-1980: Οι πρώτες θεωρητικές βάσεις

- **1973**: Ο Alexander Holevo διατύπωσε το θεώρημα του Holevo, το οποίο όρισε θεμελιώδεις περιορισμούς στην κβαντική επικοινωνία.
- **1976**: Ο Roman Stanislavovich Ingarden ανέπτυξε πρώτες ιδέες σχετικά με την πληροφορία σε κβαντικά συστήματα.

1.1.2 Δεκαετία 1980-1990: Η διαμόρφωση της Κβαντικής Υπολογιστικής ως πεδίο

- **1982**: Ο Richard Feynman στο Συνέδριο της MIT διατύπωσε τη σκέψη ότι οι κλασικοί υπολογιστές δεν μπορούν να προσομοιώσουν αποδοτικά κβαντικά συστήματα και πρότεινε τη χρήση κβαντικών υπολογιστών.
- **1985**: Ο David Deutsch δημοσίευσε την πρώτη επίσημη θεωρητική διατύπωση ενός καθολικού κβαντικού υπολογιστή, εισάγοντας την έννοια των κβαντικών πυλών.
- **1989**: Ο Howard Barnett εισήγαγε τη χρήση της κβαντικής διεμπλοκής ως υπολογιστικό εργαλείο.

1.1.3 Δεκαετία 1990-2000: Η επανάσταση των κβαντικών αλγορίθμων

- **1994**: Ο Peter Shor παρουσίασε τον περίφημο Αλγόριθμο του Shor, ο οποίος επιτρέπει την παραγοντοποίηση μεγάλων αριθμών εκθετικά πιο γρήγορα από τους κλασικούς αλγορίθμους, απειλώντας την κρυπτογράφηση RSA.
- **1996**: Ο Lov Grover ανέπτυξε τον Αλγόριθμο του Grover, ο οποίος επιταχύνει την αναζήτηση σε μη ταξινομημένες βάσεις δεδομένων.

- **1998**: Ο πρώτος κβαντικός υπολογιστής δύο qubits δημιουργήθηκε από τους Isaac Chuang και Neil Gershenfeld, ανοίγοντας το δρόμο για πειραματικές εφαρμογές.

1.1.4 Δεκαετία 2000-2010: Τα πρώτα πειραματικά επιτεύγματα

- **2001**: Ο αλγόριθμος του Shor εκτελέστηκε για πρώτη φορά σε έναν απλό αριθμό ($15 = 3 \times 5$) από ομάδα ερευνητών της IBM και του Στάνφορντ.
- **2007**: Η D-Wave Systems παρουσίασε τον πρώτο κβαντικό υπολογιστή 16 qubits, αν και υπήρχαν αμφιβολίες για την αυθεντικότητα της λειτουργίας του.

1.1.5 Δεκαετία 2010-2020: Η κβαντική υπολογιστική περνάει στην πράξη

- **2011**: Η D-Wave ανακοίνωσε τον πρώτο εμπορικό κβαντικό υπολογιστή 128 qubits, ο οποίος αγοράστηκε από τη NASA και την Google.
- **2019**: Η Google ανακοίνωσε την επίτευξη "κβαντικής υπεροχής" με τον υπολογιστή Sycamore των 53 qubits, ο οποίος εκτέλεσε σε 200 δευτερόλεπτα έναν υπολογισμό που θα απαιτούσε χιλιάδες χρόνια σε κλασικό υπερυπολογιστή.
- **2019**: Η IBM παρουσίασε τον IBM Q System One, τον πρώτο εμπορικά διαθέσιμο κβαντικό υπολογιστή.

2 Κβαντική Υπολογιστική

2.1 Βασικές έννοιες κβαντικής υπολογιστικής

- **Qubit** : Σε ένα κλασικό υπολογιστή οι πληροφορίες κωδικοποιούνται με ένα κλασικό bit, όπου παίρνει τιμές μηδέν ή ένα. Ενώ σε ένα κβαντικό υπολογιστή χρησιμοποιείται το κβαντικό bit ή αλλιώς qubit, το οποίο μπορεί να πάρει τιμή και μηδέν και ένα ταυτόχρονα. Με καταστάσεις qubit $|0>$ και $|1>$.
- **Υπέρθεση** : Είναι η ικανότητα που έχει ένα σωματίδιο να βρίσκεται σε δύο καταστάσεις ταυτόχρονα (qubit).
- **Κβαντική Διεμπλοκή** : Ονομάζεται μια κβαντική κατάσταση στην οποία τα σωματίδια επηρεάζονται το ένα με το άλλο ανεξάρτητα από την απόσταση που έχουν μεταξύ τους καθώς επίσης αν γνωρίζουμε την τιμή του ενός τότε χωρίς κάποια επιπλέον μέτρηση θα γνωρίζουμε και την κατάσταση του άλλου.
- **Υπεροχή** : Όταν οι κβαντικοί υπολογιστές σταθεροποιηθούν, θα μπορούν να λύνουν προβλήματα σε δευτερόλεπτα από ότι ένας κλασικός υπολογιστής που θα χρειαζόταν χρόνια.
- **Θεώρημα μη-κλωνοποίησης** : Δεν μπορούν να γίνουν αντίγραφα σε ένα κρυπτογραφημένο μήνυμα. Δηλαδή, δεν γίνεται να αποκρυπτογραφηθεί χωρίς να γίνει αντιληπτό από τον αποστολέα. [1]

2.2 Bra & Ket

Ο Paul A.M Dirac, ένας από τους μεγαλύτερους φυσικούς που συνέβαλε στην κβαντομηχανική, δημιούργησε τον σύμβολα bra ($<\psi|$) και ket ($|\psi>$). Στην κβαντική υπολογιστική χρησιμοποιούνται για να δηλώσουν κβαντικές καταστάσεις. Πιο συγκεκριμένα, είναι διανύσματα, όπου το ket είναι ένας πίνακας N γραμμών και μίας στήλης π.χ: $|0> = \begin{pmatrix}1\\0\end{pmatrix}$, $|1> = \begin{pmatrix}0\\1\end{pmatrix}$. Ενώ το bra είναι ένας πίνακας μίας γραμμής και N στηλών, π.χ: $<0| = (1^* \ \ 0^*) = (1 \ \ 0)$, $<1| = (0^* \ \ 1^*) = (0 \ \ 1)$ προκύπτει από τους μιγαδικούς συζυγείς του ket. Εν συνεχεία, θα ορίσουμε δυο πολύ σημαντικά γινόμενα στον χώρο Hilbert, το εσωτερικό και το εξωτερικό γινόμενο δύο διανυσμάτων κατάστασης.

- Το εσωτερικό γινόμενο των δύο καταστάσεων <a| και |b> συμβολίζεται ως <a|b> δηλαδή:

$$< a|b > = (a_0^*, a_1^*, \dots, a_{n-1}^*) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = a_0^* b_0 + a_1^* b_1 + \cdots + a_{n-1}^* b_{n-1}.$$

Υπολογίζοντας τις παρακάτω σχέσεις θα έχουμε:

- $< 0|0 > = (1 \quad 0) \times \binom{1}{0} = 1 \times 1 + 0 \times 0 = 1.$
- $< 0|1 > = (1 \quad 0) \times \binom{0}{1} = 1 \times 0 + 0 \times 1 = 0.$
- $< 1|0 > = (0 \quad 1) \times \binom{1}{0} = 0 \times 1 + 1 \times 0 = 0.$
- $< 1|1 > = (0 \quad 1) \times \binom{0}{1} = 0 \times 0 + 1 \times 1 = 1.$ [1]

Όταν το εσωτερικό γινόμενο δύο καταστάσεων είναι μηδέν, τότε οι δύο καταστάσεις ονομάζονται ορθογώνιες.

- Το εξωτερικό γινόμενο των δύο καταστάσεων |a> και <b| συμβολίζεται ως |a><b| δηλαδή:

$$|a >< b| = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} (b_0^*, b_1^*, \dots, b_{n-1}^*) = \begin{bmatrix} a_0 b_0^* & a_0 b_1^* & \cdots & a_0 b_{n-1}^* \\ \vdots & & \ddots & \vdots \\ a_1 b_0^* & a_1 b_1^* & & \\ a_{n-1} b_0^* & a_{n-1} b_1^* & \cdots & a_{n-1} b_{n-1}^* \end{bmatrix}$$

Υπολογίζοντας τις παρακάτω σχέσεις θα έχουμε:

- $|0 >< 1| = \binom{1}{0} \times (0 \quad 1) = \begin{pmatrix} 1 \times 0 & 1 \times 1 \\ 0 \times 0 & 0 \times 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$
- $|1 >< 1| = \binom{0}{1} \times (0 \quad 1) = \begin{pmatrix} 0 \times 0 & 0 \times 1 \\ 1 \times 0 & 1 \times 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$
- $|00 >< 11| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \times (0 \quad 0 \quad 0 \quad 1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$ [1]

2.3 Qubits

Όπως είδαμε παραπάνω, στην κβαντική υπολογιστική, μονάδα πληροφορίας είναι το qubit. Έχει την δυνατότητα να είναι και μηδέν και ένα ταυτόχρονα, αυτό το φαινόμενο ονομάζεται **υπέρθεση** (Super position), δηλαδή η ενδεχόμενη κατάσταση του είναι πιθανολογική . Για να γίνει πιο εύκολη η κατανόηση του, θα πάρουμε παράδειγμα την ρίψη ενός νομίσματος. Ας υποθέσουμε ότι έχουμε ένα κλασσικό και ένα κβαντικό νόμισμα. Όταν γίνει η ρίψη του κλασσικού κέρματος μπορεί να βρεθεί ή στην κατάσταση ‹‹Γράμματα›› ή στην κατάσταση ‹‹Κορόνα››. Πριν πέσει στο έδαφος το κλασσικό κέρμα βρίσκεται σε μια κατάσταση αβεβαιότητας, με πιθανότητες 50% για ‹‹Γράμματα›› και 50% για ‹‹Κορόνα››, όταν πέσει στο έδαφος θα έχουμε ξεκάθαρο αποτέλεσμα για μια από τις δύο πιθανότητες. Στο κβαντικό νόμισμα όμως, η κατάσταση είναι διαφορετική. Δηλάδη, το νόμισμα μπορεί να είναι ταυτόχρονα Γράμματα και Κορόνα μέχρι να παρατηρηθεί (Υπέρθεση). Όταν το παρατηρήσουμε, τότε η υπέρθεση καταρρέει και θα εμφανίσει σαν αποτέλεσμα είτε Γράμματα είτε Κορόνα με κάποια πιθανότητα. Οι πιθανότητες αυτές που περιγράφουν την κατάσταση ενός νομίσματος ή qubit, εκφράζονται από το **διάνυσμα κατάστασης**. [7]

$|q> = \begin{pmatrix} a \\ b \end{pmatrix}$, π.χ. $\begin{pmatrix} 0.5 \\ 0.7 \end{pmatrix}$ οι τιμές που περιέχει ονομάζονται *πλάτη πιθανότητας*.

Παρακάτω θα δούμε τι εκφράζει το διάνυσμα κατάστασης ενός qubit:

- Το qubit συμβολίζεται με το **ket** το οποίο αναφέραμε παραπάνω, π.χ $|q>$.
- Το διάνυσμα κατάστασης περιγράψει την κατάσταση ενός qubit και περιέχει δύο τιμές που ονομάζονται **πλάτη πιθανότητας**.
- Θα πρέπει το άθροισμα των πιθανοτήτων $|a|^2 + |b|^2 = 1$. Για παράδειγμα: $(0{,}6)^2 + (0{,}8)^2 = 1$.

Οι βασικές καταστάσεις ενός qubit είναι |0> και |1> και δηλώνονται ως εξής:

$$|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Δηλαδή, όταν το |0> μετρηθεί θα είναι σίγουρα 0 και όταν το |1> μετρηθεί θα είναι σίγουρα 1.

Για κάθε άλλη κβαντική κατάσταση ενός qubit, θα έχουμε την παρακάτω σχέση:

$|q> = a\binom{1}{0} + b\binom{0}{1} = a|0> + b|1>$, $(a,b) \in C^2,\ a^2 + b^2 = 1$.

Η σφαίρα Bloch:

Η σφαίρα Bloch πήρε το όνομα της από τον φυσικό Felix Bloch. Αποτελεί μια γεωμετρική αναπαράσταση μιας κβαντικής κατάστασης ενός qubit. Επίσης, μπορούμε να εκφράσουμε την κατάσταση ενός qubit με μια πιο γενικευμένη μορφή ως εξής:

$$\left|\psi> = \cos\frac{\theta}{2}\right| 0> + e^{i\varphi}\sin\frac{\theta}{2}|1>.$$

2.4 Κβαντικοί Καταχωρητές

Οι κβαντικοί καταχωρήτες είναι ένα θεμελιώδες στοιχείο των κβαντικών υπολογιστών. Πιο συγκεκριμένα, ένας κβαντικός καταχωρητής είναι ένα σύστημα που αποθηκεύει qubits, τα οποία όπως είδαμε μπορούν να βρίσκονται σε υπέρθεση καταστάσεων. Ενώ σε έναν κλασικό υπολογιστή, οι καταχωρητές αποθηκεύουν bits (0 ή 1). Η διαφορά ανάμεσα στους δύο καταχωρητές (κλασικού και κβαντικού) είναι ότι στον κβαντικό καταχωρητή μπορεί να αποθηκευτεί πολύ μεγαλύτερος όγκος πληροφορίας.

Παράδειγμα

Ο κβαντικός καταχωρητής αποτελείται από ένα η περισσότερα qubits, με αρχική κατάσταση 0, δηλαδή |00>. Μέσω του τανυστικού γινομένου των qubits που το αποτελούν που χρησιμοποιείται για να περιγράψει την κατάσταση του καταχωρητή, απεικονίζεται ως εξής:

$$|00> = |0> \otimes |0> = \binom{1}{0} \otimes \binom{1}{0} = \begin{pmatrix} 1 & \binom{1}{0} \\ 0 & \binom{1}{0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Οι υπολοιπες βασικες καταστασεις του κβαντικού καταχωρητή, υπολογίζονται με τον ίδιο τρόπο:

- $|01> = |0> \otimes |1> = \binom{1}{0} \otimes \binom{0}{1} = \begin{pmatrix} 1 & \binom{0}{1} \\ 0 & \binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- $|10> = |1> \otimes |0> = \binom{0}{1} \otimes \binom{1}{0} = \begin{pmatrix} 0 & \binom{1}{0} \\ 1 & \binom{1}{0} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

- $|11> = |1> \otimes |1> = \binom{0}{1} \otimes \binom{0}{1} = \begin{pmatrix} 0 & \binom{0}{1} \\ 1 & \binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

2.5 Κβαντικές Πύλες

Οι κβαντικές πύλες είναι θεμελιώδη στοιχεία των κβαντικών υπολογιστών. Οι πύλες αυτές, είναι μαθηματικές πράξεις που εφαρμόζονται σε qubits και μπορούν να επηρεάσουν την κατάσταση τους, εκμεταλλεύοντας φαινόμενα όπως η υπέρθεση και η συμπλοκή. Στην συνέχεια θα δούμε μια από τις πιο βασικές πύλες, την πύλη Hadamard (H).

2.5.1 Πύλη Hadamard

Η πύλη Hadamard, είναι μια πύλη η οποία επιδρά σε ένα qubit και το θέτει σε υπέρθεση. Δηλαδή, παίρνει ένα qubit που βρίσκεται είτε στην κατάσταση |0> είτε στην |1> και το μετατρέπει σε υπέρθεση αυτών των δύο καταστάσεων.

- Η μαθηματική αναπαράσταση της πύλης Hadamard είναι η εξής:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- <u>Η επίδραση της πύλης στις βασικές καταστασεις:</u>
  - $H|0> = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \binom{1}{0} = \frac{1}{\sqrt{2}} \binom{1}{1} = \frac{1}{\sqrt{2}} \left(\binom{1}{0} + \binom{0}{1} \right) = \frac{|0> + |1>}{\sqrt{2}} = |+>.$

- $H|1> = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\-1\end{pmatrix}\right) = \frac{|0> - |1>}{\sqrt{2}} = |->$.

Όταν η πύλη Hadamard δρα στην κατάσταση |0> το qubit βρίσκεται σε ίση υπέρθεση των βασικών καταστάσεων |0> και |1> . Ενώ, στην κατάσταση |1> είναι επίσης υπέρθεση αλλά με αρνητικό πρόσημο στο |1> . [1]

Ιδιότητα

Εάν εφαρμόσουμε την πύλη Hadamard δύο φορές, επιστρέφουμε στην αρχική κατάσταση:

- $H(H|0>) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0>$.
- $H(H|1>) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1>$.

Παράδειγμα

Να υπολογιστεί η εφαρμογή της πύλης Hadamard στο qubit . $|\psi> = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$

$$H|\psi> = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0>.$$

Το αποτέλεσμα είναι |0>. [1]

2.5.2 Πύλη Αδράνειας

Η πύλη αδράνειας (I) είναι μια από τις πιο απλές πύλες και δεν προκαλεί καμία αλλαγή στην κατάσταση ενός qubit στο οποίο εφαρμόζεται. Η πύλη αδράνειας είναι χρήσιμη για την επίλυση κβαντικών κυκλωμάτων. Αναπαρίσταται από τον μοναδιαίο πίνακα 2χ2 :

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

Δράση της πύλης αδράνειας

Η πύλη αδράνειας (I) δεν αλλάζει την κατάσταση ενός qubit. Εάν η αρχική κατάσταση ενός qubit είναι $|\psi>$ τότε, μετά την εφαρμογή της πύλης παραμένει αμετάβλητη:

$$I|\psi> = |\psi>$$

Για παράδειγμα: [1]

- Αν το qubit είναι στην κατάσταση $|0>$, τότε :

$$I|0> = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\times 1 & + & 0\times 0 \\ 0\times 1 & + & 1\times 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0>.$$

- Αν το qubit είναι στην κατάσταση $|1>$, τότε :

$$I|1> = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\times 0 & + & 0\times 1 \\ 0\times 0 & + & 1\times 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1>.$$

2.5.3 Πύλες Pauli

Οι πύλες pauli είναι θεμελιώδεις ομάδα κβαντικών πυλών που δρουν σε ένα qubit και μπορούν να το περιστρέφουν στην σφαίρα Bloch . Συμβολίζονται και αναπαρίστανται ως εξής:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Η δράση της πύλης X σε ένα qubit είναι:

Η πύλη X λειτουργεί ως κβαντική πύλη NOT. Δηλαδή, ανταλλάσει την κατάσταση |0> με |1> και αντίστροφα.

- $X|0> = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1>.$

- $X|1> = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0>.$

- Η δράση της πύλης Y σε ένα qubit είναι:

- $Y|0> = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i|1>.$

- $Y|1> = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0>.$

- Η δράση της πύλης Z σε ένα qubit είναι:

Η πύλη Z , θα παρατηρήσουμε ότι αλλάζει τη φάση της κατάστασης |1>, διατηρώντας αμετάβλητη την κατάσταση |0>.

- $Z|0> = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0>.$

- $Z|1> = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1>.$

Ιδιότητες των πυλών Pauli

Παρατηρούμε ότι οι πύλες x, y και z είναι ταυτόχρονα ερμιτιανές και μοναδιαίες λόγω της γνωστής τους ιδιότητας $\mathrm{X}^2 = \mathrm{Y}^2 = \mathrm{Z}^2 = \mathrm{I}$ και $X^* \times X = Y^* \times Y = Z^* \times Z = I$. [1]

<u>Παράδειγμα</u>

- $\mathrm{X}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}.$
- $Y^2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \times \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} = \begin{pmatrix} -i^2 & 0 \\ 0 & -i^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$ [1]
- $\mathrm{Z}^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}.$

2.5.4 Πύλη CNOT

Η πύλη CNOT είναι επίσης μια από τις βασικές πύλες στους κβαντικούς υπολογισμούς. Η πύλη ελεγχόμενου not (controlled not-CNOT-CX) δρα σε δυο qubits , το ένα ονομάζεται qubit ελέγχου (control) και το άλλο qubit στόχος (target).

- Αν το qubit ελεγκτής (control) είναι στην κατάσταση |1>, τότε αντιστρέφει το qubit στόχος (target).
- Αν το qubit ελεγκτής είναι στην κατάσταση |0>, τότε δεν συμβαίνει καμία αλλαγή στο qubit στόχο.

Η πύλη CNOT αναπαρίσταται με τον παρακάτω πίνακα:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

<u>Η δράση την πύλης CNOT:</u>

- Στον καταχωρητή |10> :

$$CNOT|10> = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11>.$$ [7]

Αφού η κατάσταση του qubit ελέγχου είναι |1>, η κατάσταση του qubit στόχου αλλάζει.

- Στον καταχωρητή |01> :

$$CNOT|01>= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01>. [7]$$

Αφού η κατάσταση του qubit ελέγχου είναι |0>, η κατάσταση του qubit στόχου δεν αλλάζει.

Με τον ίδιο τρόπο βρίσκουμε και τα υπόλοιπα: CNOT|00> = |00> και CNOT|11> = |10>.

Παρατηρούμε λοιπόν ότι οι καταστάσεις |00> και |01> , παραμένουν αμετάβλητες ενώ στις καταστάσεις |10> και |11> , το qubit στόχος (2^{ο} qubit) αντιστρέφεται.

3 Σύγχρονοι Αλγόριθμοι Κρυπτογράφησης

3.1 Κατηγορίες Σύγχρονων Αλγορίθμων Κρυπτογράφησης

Οι σύγχρονοι αλγόριθμοι κρυπτογράφησης χωρίζονται στις εξής δύο κατηγορίες:

1. Συμμετρικούς (Symmetric).
2. Ασύμμετρους (Asymmetric) ή αλλιώς Δημόσιου κλειδιού (Public key).

Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης είναι το ίδιο με το κλειδί αποκρυπτογράφησης. Δηλαδή χρησιμοποιούν μόνο ένα κλειδί. Θα πρέπει να είναι γνωστό το κλειδί και στον αποστολέα και στον παραλήπτη.

Ασύμμετροι Αλγόριθμοι Κρυπτογράφησης

Στους ασύμμετρους αλγόριθμους χρησιμοποιούνται δύο διαφορετικά κλειδιά. Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση είναι δημόσιο κλειδί και μπορεί να κοινοποιηθεί ελεύθερα, όμως το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι ιδιωτικό κλειδί και πρέπει να είναι κρυφό.

Διαφορές

Εκτός από τους διαφορετικούς τρόπους που χρησιμοποιούν τα κλειδιά οι παραπάνω κατηγορίες αλγορίθμων, υπάρχει διαφορά και στο μήκος τους. Αναλυτικότερα, οι αλγόριθμοι αυτοί δημιουργούν κλειδιά με μια σειρά από bits, για την κρυπτογράφηση και αποκρυπτογράφηση μιας πληροφορίας. (Το μήκος τους μετριέται σε bit), στους συμμετρικούς αλγόριθμους, τα κλειδιά επιλέγονται τυχαία και το μήκος τους είναι 128 ή 256, εξαρτάται από το επίπεδο ασφαλείας. Ενώ στους ασύμμετρους αλγόριθμους, μεταξύ του

δημόσιου και ιδιωτικού κλειδιού συνδέεται μια μαθηματική σχέση. Κατά κανόνα τα ασύμμετρα κλειδιά πρέπει να είναι πολύ μεγαλύτερα για να έχουν ισοδύναμο επίπεδο ασφαλείας. Για παράδειγμα ένα συμμετρικό κλειδί με 128 bit και ένα ασύμμετρο κλειδί με 2.048 bit είναι σχεδόν το ίδιο επίπεδο ασφαλείας.

Πλεονεκτήματα και Μειονεκτήματα

- Συμμετρικοί Αλγόριθμοι Κρυπτογράφησης: Είναι πολύ ταχύτεροι, χρειάζονται λιγότερη υπολογιστική ισχύ. Σημαντική αδυναμία τους όμως είναι η διανομή του κλειδιού αφού για την κρυπτογράφηση και αποκρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί και υπάρχουν κίνδυνοι ασφαλείας.
- Ασύμμετροι Αλγόριθμοι Κρυπτογράφησης: Εδώ βλέπουμε ότι το πρόβλημα διανομής κλειδιού λύνεται. Όμως, συγκρίνοντας τους με συμμετρικά συστήματα, είναι πιο αργά και χρειάζονται περισσότερη υπολογιστική ισχύ, αφού το μήκος του κλειδιού είναι μεγαλύτερο.

3.2 Κρυπτογραφικό Σύστημα RSA

Ένας από τους πιο ευρέως χρησιμοποιημένους αλγόριθμους δημόσιου κλειδιού είναι ο RSA. Πιο συγκεκριμένα, αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Len Adleman όπου το όνομα του από τα αρχικά των επιθέτων τους.

Περιγραφή του αλγόριθμου

Η βασική δομή του κρυπτοσυστήματος RSA είναι η εξής:

- Επιλέγονται δύο μεγάλοι πρώτοι αριθμοί (p,q) και υπολογίζουμε το γινόμενο τους $n = p * q$.
- Επιλέγεται ένας τυχαίος ακέραιος d τέτοιος ώστε να είναι πρώτος ως προς $(p-1) * (q-1) = \Phi(n)$, δηλαδή ο Μέγιστος Κοινός Διαιρέτης των d και Φ(n) είναι το ένα.
- Υπολογίζεται ο αριθμός e από τη σχεση: $e * d \; mod \; \Phi(n) = 1$.
- Το ζεύγος (e,n) αποτελεί το δημόσιο κλειδί, ενώ το ζεύγος (d,n) αποτελεί το ιδιωτικό κλειδί το οποίο δεν δημοσιοποιείται.

Κρυπτογράφηση

Απλό κείμενο: m < n

Κρυπτοκείμενο: $c = m^e \bmod n$

Αποκρυπτογράφηση

Κρυπτοκείμενο: c

Απλό κείμενο: $m = c^d \bmod n$

Παράδειγμα [1]

Έστω οι δύο πρώτοι αριθμοί p = 11 και q = 13 με γινόμενο $n = p * q = 11 * 13 = 143$.

- Υπολογίζεται το γινόμενο $\Phi(n) = (p-1) * (q-1) = (11-1) * (13-1) => \Phi(n) = 120$.
- Επιλέγουμε έναν τυχαίο e τέτοιο ώστε $MK\Delta(e, \Phi(n)) = 1$. Για παράδειγμα e = 13, άρα $(13,120) = 1$.
- Υπολογίζεται ο d: $e * d \bmod \Phi(n) = 1 => 13d \bmod 120 = 1 => d = 37$.
- Δημόσιο κλειδί (e, n) = (13, 143).
- Ιδιωτικό κλειδί (d, n) = (37, 143).

-Κρυπτογράφηση μηνύματος: Θέλουμε να στείλουμε το m = 13, τότε με το δημόσιο κλειδί έχουμε: $c = m^e \bmod n => c = 13^{13} \bmod 143 = 52$.

-Αποκρυπτογράφηση μηνύματος: Με το ιδιωτικό κλειδί έχουμε:

$m = c^d \bmod n = 52^{37} \bmod 143 = 13$.

Ασφάλεια του RSA

Για την κρυπτογράφηση ενός μηνύματος χρειαζόμαστε το δημόσιο και το ιδιωτικό κλειδί. Το δημόσιο κλειδί στέλνεται σε αυτόν που στέλνει το μήνυμα στο άτομο που θέλει να

πραγματοποιήσει μια συναλλαγή και ο παραλήπτης διατηρεί το ιδιωτικό κλειδί. Ο δέκτης έχει το ιδιωτικό κλειδί όλη την ώρα και έτσι δεν υπάρχει κίνδυνος υποκλοπής.

3.3 Αλγόριθμος Diffie-Hellman

Ο πρώτος αλγόριθμος δημόσιου κλειδιού δημοσιεύθηκε στο άρθρο "New Directions in Cryptography" από τους Whitefield Diffie και Martin Hellman. Ο αλγόριθμος είναι γνωστός ως ανταλλαγή κλειδιών Diffie-Hellman (Diffie-Hellman key exchange) , σκοπός του είναι να επιτρέψει σε δύο χρήστες να ανταλλάξουν με ασφάλεια ένα μυστικό κλειδί όπου μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μελλοντικών μηνυμάτων. Ο συγκεκριμένος αλγόριθμος περιορίζεται μόνο στην ανταλλαγή κλειδιών.

Περιγραφή πρωτοκόλλου

Στην συγκεκριμένη μέθοδο, υπάρχουν δύο δημόσια γνωστοί αριθμοί: το q όπου πρέπει να είναι πρώτος αριθμός και το a ο οποίος είναι πρωτοβάθμια ρίζα του q. Έχουμε τους χρήστες Α και Β που θέλουν να ανταλλάξουν ένα κλειδί. Τότε ο χρήστης Α επιλέγει έναν τυχαίο ακέραιο X_A ο οποιος είναι μικρότερος του q και υπολογίζει το $Y_A = \alpha^{X_A} mod\ q$. Επίσης ο χρήστης Β επιλέγει έναν τυχαίο ακέραιο X_B< q και υπολογίζει το $Y_B = a^{X_B} mod\ q$. Και οι δύο χρήστες κρατάνε την τιμή Χ κρυφή και γνωστοποιούν την τιμή Υ. Στην συνέχεια, ο χρήστης Α υπολογίζει το κλειδί k = $Y_B^{X_A} mod\ q$ και ο Β το κλειδί k = $Y_A^{X_B} mod\ q$. Τέλος, το αποτέλεσμα που έχουμε είναι ότι οι δύο χρήστες αντάλλαξαν μια μυστική τιμή.

Παράδειγμα [8]

Έστω ότι για την ανταλλαγή κλειδιού έχουμε τον πρώτο αριθμό q = 353 και μια πρωτοβάθμια ρίζα του 353, στην περίπτωση μας την ρίζα α = 3. Στην συνέχεια οι χρήστες Α και Β επιλέγουν τα κρυφά κλειδιά X_A= 97 και X_B= 233 αντίστοιχα.

- Υπολογίζουμε τα δημόσια κλειδιά του κάθε χρήστη:
  - Για τον Α έχουμε $Y_A = 3^{97} mod\ 353 = 40$.
  - Για τον Β έχουμε $Y_B = 3^{233} mod\ 353 = 248$.
- Αφού αντάλλαξαν τα δημόσια κλειδιά, ο καθένας μπορεί να υπολογίσει το κοινό μυστικό κλειδί:
  - Ο Α υπολογίζει το k = ${Y_B}^{X_A} mod\ 353 = 248^{97} mod\ 353 = 160$.
  - Ο Β υπολογίζει το k = ${Y_A}^{X_B} mod\ 353 = 40^{233} mod\ 353 = 160$.

3.3.1 Αποτελεσματικότητα του αλγόριθμου Diffie – Hellman

Η αποτελεσματικότητα του Diffie – Hellman εξαρτάται από τη δυσκολία υπολογισμού των διακριτών λογαρίθμων. Για παράδειγμα ας υποθέσουμε ότι ένας χάκερ έχει στην διάθεση του τις εξής πληροφορίες από το παραπάνω παράδειγμα:

$$q = 353,\ \alpha = 3,\ Y_A = 40,\ Y_B = 248$$

Μπορεί να βρει το μυστικό κλειδί 160 με την επίθεση "ωμής βίας" ή αλλιώς "brute-force". Πιο συγκεκριμένα, ο χάκερ μπορεί να προσδιορίσει το κοινό κλειδί υπολογίζοντας την εξίσωση $3^{\alpha} mod\ 353 = 40$ ή $3^{b} mod\ 353 = 248$. Η μέθοδος brute-force υπολογίζει στην περίπτωση αυτή, δυνάμεις του 3 modulo 353 και σταματάει όταν το αποτέλεσμα είναι ίσο είτε με 40 είτε με 248. Η απάντηση προκύπτει για εκθέτη με τιμή 97, το οποίο μας δίνει το αποτέλεσμα $3^{97} mod\ 353 = 40$. Για μεγαλύτερους αριθμούς, θεωρείται ανέφικτο να σπάσει με χρήση ωμής βίας λόγω του αστρονομικού αριθμού πιθανοτήτων. [8]

3.3.2 Αυθεντικοποίηση

Το πρωτόκολλο Diffie-Hellman είναι ευάλωτο σε επιθέσεις "Man in the middle attack" ή αλλιώς επιθέσεις μεσάζοντα διότι δεν παρέχει την πιστοποίηση της ταυτότητας των συμμετεχόντων. Συνεπώς, είναι απαραίτητο κατά τη χρήση του πρωτοκόλλου να γίνεται εξακρίβωση της ταυτότητας κάθε συμμετέχοντα για την πρόληψη αυτού του είδους επιθέσεων, αυτό μπορεί να γίνει με την χρήση ψηφιακών υπογραφών.

3.4 Αλγόριθμος El Gamal

Είναι ένας αλγόριθμος δημόσιου κλειδιού, ο οποίος έχει αρκετές ομοιότητες με τον αλγόριθμος Diffie – Hellman. Δημιουργήθηκε το 1984 από τον Tacher El Gamal και η ασφάλεια του αλγορίθμου βασίζεται στο πρόβλημα του διακριτού λογαρίθμου.

3.4.1 Περιγραφή του αλγορίθμου

1) Δημιουργία δημόσιου και ιδιωτικού κλειδιού:
    - Επιλέγουμε έναν μεγάλο πρώτο αριθμό q και ένα γεννήτορα g της ομάδας G^*q.
    - Επιλέγουμε τυχαίο x και υπολογίζουμε το $h = g^x$.
    - Το δημόσιο κλειδί είναι η τριάδα (q,g,h) και το μυστικό κλειδί το x.
2) Αλγόριθμος Κρυπτογράφησης:
    - Έστω ότι ο Β θέλει να στείλει το μήνυμα m στον Α. Ο Β διαλέγει έναν τυχαίο y∈N.
    - Στην συνέχεια υπολογίζει το $c_1 = g^y$ και $c_2 = mh^y$.
    - Τέλος , ο Β στέλνει στον Α το μήνυμα (c_1, c_2).
3) Αλγόριθμος Αποκρυπτογράφησης:

    Ο Α λαμβάνει το μήνυμα (c_1, c_2) και υπολογίζει το m = $c_2 c_1^{-x}$. [9]

3.4.2 Παράδειγμα

Έστω λοιπόν ότι επιλέγονται από τον Α τα q = 607 , g = 3, x = 413. Τότε το $h = g^x = 3^{413} mod\ 607 = 588 => h = 588$. Άρα το δημόσιο κλειδί είναι (607, 3, 588). Ο Β θέλει να στείλει το μήνυμα m = 38. Θα διαλέξει έναν τυχαίο y = 175 και θα υπολογίσει [9]:

$$c_1 = g^y = 3^{175} mod\ 607 = 279.$$

$$c_2 = mh^y = 38 \cdot 588^{175} mod\ 607 = 38 \cdot 221\ mod\ 607 = 507.$$

Άρα ο Β στέλνει το μήνυμα (279, 507) στον Α. Ο Α λαμβάνει και υπολογίζει:

$$c_2 c_1^{-x} = 507 \cdot\ 279^{-413} \bmod 607 = 507 \cdot 206 \bmod 607 = 38 \bmod 607 = 38.$$

Συνεπώς, το μήνυμα που θα λάβει ο Α είναι το 38. [9]

3.5 ECC

Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) είναι ένας κλάδος της ασύμμετρης κρυπτογραφίας, που βασίζεται στις μαθηματικές ιδιότητες των ελλειπτικών καμπυλών. Η ECC είναι ένα είδος κρυπτοσυστήματος δημόσιου κλειδιού και ψηφιακών υπογραφών όπως το RSA.

3.5.1 Εφαρμογές της ECC

- Ασφαλής επικοινωνία: Χρησιμοποιείται σε πρωτόκολλα όπως TLS/SSL για την ασφαλή σύνδεση στο διαδίκτυο.
- Ψηφιακές υπογραφές: Χρησιμοποιείται σε διάφορα σχήματα ψηφιακών υπογραφών, όπως το ECDSA (Elliptic Curve Digital Signature Algorithm).
- Συσκευές IoT και κινητά τηλέφωνα: Χρησιμοποιείται για την ασφάλεια της επικοινωνίας μεταξύ των συσκευών με μικρότερη επεξεργαστική ισχύ και μνήμη.

3.5.2 Πλεονεκτήματα και μειονεκτήματα

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Μικρότερα μεγέθη κλειδιών	Περίπλοκες μαθηματικές πράξεις
Ταχύτεροι υπολογισμοί	Ευαισθησία στην επιλογή ασφαλών καμπυλών
Κατάλληλη για συσκευές χαμηλής ισχύος	

3.5.3 Προκλήσεις και περιορισμοί

- Επιλογή ασφαλών καμπυλών: Η επιλογή ασφαλών παραμέτρων είναι κρίσιμη διότι ορισμένες καμπύλες μπορεί να είναι ευάλωτες σε εξειδικευμένες επιθέσεις.
- Κβαντικοί υπολογιστές: Η ECC , όπως και άλλοι αλγόριθμοι ασύμμετρης κρυπτογραφίας, κινδυνεύουν από αλγορίθμους κβαντικών υπολογιστών, όπως ο αλγόριθμος Shor που θα δούμε στο επόμενο κεφάλαιο .

3.5.4 Σύγκριση ECC και του RSA

Ενώ και η ECC αλλά και το RSA χρησιμοποιούνται για ασύμμετρη κρυπτογράφηση, ψηφιακές υπογραφές και ασφαλή ανταλλαγή κλειδιών. Υπάρχουν σημαντικές διαφορές όσον αφορά την απόδοση, το μέγεθος κλειδιών και την μακροπρόθεσμη ασφάλεια. Πιο συγκεκριμένα, το πλήθος των bit που απαιτούνται για ασφαλή χρήση του RSA είναι αυξημένο, με αποτέλεσμα ο επεξεργαστικός φόρτος να είναι μεγάλος. Ενώ, το ελκυστικότερο χαρακτηριστικό της ECC σε σύγκριση με το RSA είναι να προσφέρει την ίδια ασφάλεια για πολύ μικρότερο πλήθος bit , μειώνοντας έτσι την επεξεργαστική επιβάρυνση. Επίσης, το επίπεδο εμπιστοσύνης στον ECC δεν είναι τόσο υψηλό όσο το αντίστοιχο επίπεδο στον RSA, όμως και οι δύο μέθοδοι είναι ευάλωτες σε κβαντικούς υπολογιστές. Τέλος, η κρυπτογραφία ελλειπτικής καμπύλης είναι πιο δύσκολο να εξηγηθεί από ότι οι παραπάνω αλγόριθμοι και η πλήρης μαθηματική περιγραφή της ξεφεύγει από τους στόχους της πτυχιακής. [8]

4 Ο αλγόριθμος του Shor

Όπως έχουμε αναφερθεί και σε προηγούμενο κεφάλαιο, το πρόβλημα της παραγοντοποίησης ενός μεγάλου ακέραιου αριθμού, είναι ένα δύσκολο μαθηματικό πρόβλημα. Το 1994 ο Αμερικάνος μαθηματικός και κρυπτογράφος Peter Shor, πρότεινε έναν πολυωνυμικού χρόνου, κβαντικό αλγόριθμο που μπορεί να υπολογίσει τους πρώτους παράγοντες ενός ακέραιου μεγάλου αριθμού. Απέδειξε ότι με τους κβαντικούς υπολογιστές η περίοδος μιας περιοδικής συνάρτησης μπορεί να βρεθεί με ευκολία και σε σύντομο χρονικό διάστημα, καθώς και οι πρώτοι παράγοντες των μεγάλων πρώτων αριθμών. [1]

4.1 Περιγραφή του αλγόριθμου (Κβαντικού)

Ο αλγόριθμος του Shor χρειάζεται δυο κβαντικούς καταχωριτές (quantum registers) οι οποίοι λέγονται R1 και R2 δηλαδή τα qubits ομαδοποιούνται σε δύο σύνολα. Οι R1 και R2 δημιουργούν ένα κβαντικό καταχωρητή τον Reg. Επίσης, ο καταχωρητής R1 βρίσκεται σε κατάσταση $|\psi 1>$ και ο καταχωρητής R2 σε κατάσταση $|\psi 2>$. Επομένως, η κατάσταση του Reg θα είναι $|\psi>$:

$$|\psi> = |\psi 1> |\psi 2> = |\psi 1 \psi 2> = |\psi 1, \psi 2>.$$

Η αρχική κατάσταση του Reg είναι $|0,0>$.

Με τα δύο δεδομένα x, n που έχουμε, ο κλασικός αλγόριθμος Shor, αναζητά την τάξη του x όπου r είναι μικρότερος ακέραιος τ.ω. να ισχύει: $x^r \equiv 1(\text{mod} n)$. [1]

4.2 Τα βήματα του κλασικού αλγόριθμου Shor

Τα παρακάτω βήματα μπορούν να εκτελεστούν και από έναν απλό υπολογιστή [10]:

1. Θα προσδιορίσουμε αν ο n είναι πρώτος αριθμός, σύνθετος αριθμός ή δύναμη του πρώτου.
2. Επιλέγουμε έναν τυχαίο ακέραιο α όπου ισχύει α<n. Υπολογίζουμε τον μέγιστο κοινό διαιρέτη των δύο αριθμών (α , n). Αν (α , n) ≠ 1, τότε έχουμε βρει έναν παράγοντα του n.
3. Αν ΜΚΔ (α , n) = 1, τότε θα βρούμε την περίοδο r της συνάρτησης

$f(a) = \alpha^x \, mod \, n$. Για την εύρεση της περιόδου θα χρησιμοποιήσουμε έναν κβαντικό υπολογιστή.

4. Προσδιορίζουμε τις τιμές λ , r όπου πρέπει να ισχύει (λ, r) = 1.
5. Αν ο αριθμός r είναι περιττός, τότε σταματάει η διαδικασία και γυρνάμε πίσω στο βήμα 2.
6. Αν $x^{\frac{r}{2}} \equiv$ -1(modn) , τότε επιστρέφουμε στο βήμα 2.
7. Οι αριθμοί που παραγοντοποιούν το n θα είναι gcd ($\alpha^{\frac{r}{2}}$ + 1 , n) και gcd ($\alpha^{\frac{r}{2}}$ – 1 , n).

4.3 Τα βήματα του κβαντικού αλγόριθμου Shor

Το κβαντικό κομμάτι του αλγορίθμου χρησιμοποιείται για την εύρεση περιόδου [10].

1. Επιλέγουμε έναν ακέραιο αριθμό q τέτοιο ώστε $n^2 \leq q \leq 2n^2$.
2. Η κατάσταση του καταχωρητή Reg είναι $|\psi> = |00>$.
3. Ο καταχωρητής R_1, μπαίνει σε κατάσταση υπέρθεσης όλων των κβαντικών καταστάσεων από 0 εώς q-1. Μετά από αυτό το σύστημα μας βρίσκεται στην κατάσταση

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

Το |0> είναι ο 2ος καταχωρητής R_2 και δεν δρούμε σε αυτόν.

4. Στον καταχωρητή R_2 , υπολογίζεται η τιμή της συνάρτησης $f_{n,a}(x)$ και τα αποτελέσματα καταγράφονται. Επίσης, ο καταχωρητής R_2 βρίσκεται πλέον σε υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Ο καταχωρητής Reg βρίσκεται σε κατάσταση

$$|\psi> = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |x> |a^x (modn)>$$

Υπολογίζεται η κατάσταση του R_2 ο οποίος βρίσκεται σε υπέρθεση και το αποτέλεσμα θα είναι μόνο μια τιμή της συνάρτησης, που θα την πούμε k. Άρα βρίσκεται σε κατάσταση |k> . Η μέτρηση της κατάστασης του καταχωρητή R_2, καθορίζει την κατάσταση του καταχωρητή R_1, διότι και οι δύο καταχωρητές βρίσκονται σε κατάσταση κβαντικής διεμπλοκής. Οι αριθμοί για τους οποίους ισχύει: $a^x \, mod \, n = k$, θα συμβολίζονται x′ και αποτελούν ένα σύνολο A = $\{x' = a^{x'} \, mod \, n = k\}$. Έστω ότι ||A|| είναι ο

αριθμός των στοιχείων του συνόλου Α. Μετά την μέτρηση η κατάσταση του Reg δίνεται από την σχέση:

$$|\psi> = \frac{1}{\sqrt{||A||}} \sum_{x'} |x'> |k>$$

5. Στην συνέχεια, εφαρμόζεται ο κβαντικός μετασχηματισμός Fourier στον καταχωρητή R_1, ο οποίος μετασχηματίζει κάθε κατάσταση |x'> σε μια υπέρθεση καταστάσεων που δίνεται από την σχέση:

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

Μετά την εφαρμογή του κβαντικού μετασχησματισμού Fourier η κατασταση του Reg είναι:

$$|\psi> = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{\frac{2\pi i a c}{q}} |c> |x^a (mod n)>$$

6. Μετράται η κατάσταση του R_1 και η τιμή του είναι μοναδική και είναι λ πολλαπλάσιο του $\frac{q}{r}$, δηλαδή $c' = \lambda \frac{q}{r}$ και r η περίοδος που πρέπει να προσδιοριστεί.
7. Τα βήματα 2 ως 6 επαναλαμβάνονται περίπου log(q) φορές, μέχρι να προκύψουν πολλαπλάσια του $\frac{1}{r}$ για να υπολογιστεί η περίοδος r.

4.4 Εφαρμογή του αλγόριθμου

[1] Για να κατανοήσουμε τον αλγόριθμο Shor, θα βρούμε τους παράγοντες του n = 21.

1) Επιλέγεται ένας τυχαίος ακέραιος αριθμός α (1< α < n) που είναι πρώτος ως προς το n, δηλαδή ΜΚΔ (α , n) = 1. Για α = 11 έχουμε ΜΚΔ (11,21) = 1 και είναι πρώτος ως προς το n = 21.
2) Επιλέγεται ένας ακέραιος αριθμός q τέτοιος ώστε $n^2 \leq q \leq 2n^2$. Υπολογίζουμε $n^2 = 21^2 = 441$ και $2n^2 = 882$. Επιλέγουμε q = 512 διότι $q = 2^L => q = 2^9 = 512$.
3) Φέρνουμε τον R_1 σε κατάσταση υπέρθεσης όλων των καταστάσεων x mod q :

$$|\Phi_0> = \frac{1}{512} \sum_{x=0}^{511} |x> |0>$$

Δεν δρούμε στον R_2.

4) Στην συνέχεια, στον R_2 υπολογίζουμε τις τιμές $\alpha^x(mod\ n)$ για κάθε x, και τα αποτελέσματα καταγράφονται στον R_2 ο οποίος βρίσκεται πλέον σε υπέρθεση όλων των καταστάσεων $\alpha^x(mod\ n)$. Έχουμε:

$$|\Phi_1> = \frac{1}{512}\sum_{x=0}^{511}|x>|11^x mod\ 21>$$

$$= \frac{1}{512}(|0>|1> +|1>|11> +|2>|16> +|3>|8> +|4>|4> +|5>|2> +|6>|1> +|7>|11> +|8>|16> +|9>|8> +|10>|4>.$$

Οι δύο καταχωρητές R_1 και R_2 βρίσκονται σε κβαντική διεμπλοκή. Επίσης παρατηρούμε ότι η περίοδος r = 6.

5) Ο κβαντικός Μετασχηματισμός Fourier (QFT) δρα στον R_1, ενώ το περιεχόμενο του R_2 παραμένει αμετάβλητο.

$$|\tilde{\Phi}> = \frac{1}{512}\sum_{x=0}^{511}\sum_{c=0}^{511} e^{\frac{2\pi i x c}{q}}|c>|11^x(mod 21)>.$$

6) Στο καταχωρητή R_1 μετράμε την πιθανότητα της κατάστασης |c, α^k (mod n) >. Το αποτέλεσμα της μέτρησης δίνει μια μόνο τιμή την c΄ και είναι ένα λ ακέραιο πολλαπλάσιο του $\frac{q}{r}$, δηλαδή $ć = \lambda\frac{q}{r}$, όπου r είναι η περίοδος που πρέπει να προσδιοριστεί. Για k=2 και |c,16> έχουμε:

$$p(c) = \left|\frac{1}{512}\sum_{x:\,11^x mod 21=16}^{511} e^{\frac{2\pi i x c}{q}}\right|^2 = \frac{1}{512}\sum_{\lambda} e^{2\pi i(6\lambda+2)c/512}\Big|^2$$

Από την μέτρηση προκύπτει ότι η πιο πιθανή τιμή για το c είναι:

$$c = \frac{512}{6} \approx 427.$$

Επομένως: $\left|\frac{c}{q} - \frac{\lambda}{r}\right| = \left|\frac{427}{512} - \frac{\lambda}{r}\right| \leq \frac{1}{1024}$.

Στην συνέχεια χρησιμοποιούμε συνεχή κλάσματα για να βρούμε το r:

$$\frac{427}{512} = 0 + \frac{\frac{1}{512}}{427 mod 512} = 0 + \frac{\frac{1}{512}}{427}$$

$$= 0 + \frac{1}{1 + \frac{85}{427}} = 0 + \frac{1}{1 + \frac{427}{85}}$$

$$= 0 + \frac{1}{1 + \frac{1}{5 + \frac{85}{2}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}}}$$

Άρα $\alpha_0 = 0\,, \alpha_1 = 1,\ \alpha_2 = 5,\ \alpha_3 = 42,\ \alpha_4 = 2.$

Έχουμε:

- $\lambda_0 = \ \alpha_0 => \ \lambda_0 = 0$
- $\lambda_1 = 1 + \alpha_0\alpha_1 = 1 + 0 => \lambda_1 = 1$
- $\lambda_2 = \alpha_2\lambda_1 + \lambda_0 = 5 \cdot 1 + 0 = 5 => \lambda_2 = 5$
- $\lambda_3 = \alpha_3\lambda_2 + \lambda_1 = 42 \cdot 5 + 1 = 211 => \lambda_3 = 211$
- $\lambda_4 = \alpha_4\lambda_3 + \lambda_2 = 2 \cdot 211 + 5 = 427 => \lambda_4 = 427$

Για να βρούμε το r:

- $r_0 = 1$
- $r_1 = \alpha_1 => r_1 = 1$
- $r_2 = \alpha_2 r_1 + r_0 = 5 \cdot 1 + 1 = 6 => r_2 = 6$
- $r_3 = \alpha_3 r_2 + r_1 = 42 \cdot 6 + 1 = 253 => r_3 = 253$
- $r_4 = \alpha_4 r_3 + r_2 = 2 \cdot 253 + 6 = 512 => r_4 = 512$

Επομένως έχουμε:

$\frac{\lambda_0}{r_0} = 0$ και $\frac{\lambda_1}{r_1} = 1$, δοκιμάζουμε στην συνέχεια το $\frac{\lambda_2}{r_2} = \frac{5}{6}$, το οποίο είναι αποτελεσματικό. Άρα r = 6.

7) Ελέγχουμε αν το r είναι άρτιος και αν $11^{\frac{r}{2}} mod\ 21\ \neq\ -1$. Εφόσον ισχύουν οι δύο παραπάνω συνθήκες τότε προσδιορίζουμε τους παράγοντες

- $11^{\frac{r}{2}}\ (mod\ n) - 1 =\ 11^3\ mod\ 21 - 1 = 7$
- $11^{\frac{r}{2}}\ (mod\ n) - 1 =\ 11^3\ mod\ 21 + 1 = 9$

Ο πρώτος παράγοντας είναι $\lambda_1 = \text{ΜΚΔ}\left(11^{\frac{6}{2}} - 1,\ 21\right) = (1331,21) = 7$

και ο δεύτερος $\lambda_2 = \frac{21}{7} = 3$. Άρα το 21 γράφεται $21 = 7 \cdot 3$.

4.5 Συμπέρασμα

Ο αλγόριθμος Shor χρησιμοποιεί κβαντικούς υπολογισμούς για να βρίσκει πιο γρήγορα την περίοδο r, κάτι που επιτρέπει την παραγοντοποίηση μεγάλων αριθμών σε πολυωνυμικό χρόνο. Τα πρώτα βήματα όμως μπορούν να εφαρμοστούν και σε ένα κλασικό υπολογιστή. Τέλος, ο αλγόριθμος του Shor θεωρείται τεράστια απειλή για το RSA διότι μπορεί να το «σπάσει» αν εφαρμοστεί σε κβαντικούς υπολογιστές μεγάλης κλίμακας.

5 Κβαντική Κρυπτογραφία

Αφού κάναμε μια εισαγωγή στην κλασική κρυπτογραφία σε προηγούμενο κεφάλαιο, τώρα σε αυτό το κεφάλαιο θα αναλύσουμε την κβαντική κρυπτογραφία. Πιο συγκεκριμένα η κβαντική κρυπτογραφία εμφανίστηκε το 1970 , εκμεταλλεύεται τις ιδιότητες της κβαντομηχανικής για την ασφάλεια μεταφοράς ή αποθήκευσης δεδομένων. Στην κβαντική κρυπτογραφία είναι σημαντική η διαδικασία διανομής κβαντικού κλειδιού (Quantum Key Distribution – QKD) όπου χρησιμοποιείται για τη δημιουργία ιδιωτικού κλειδιού μέσω ενός κβαντικού καναλιού.

5.1 Κβαντική διανομή κλειδιών (Quantum Key Distribution)

Η κβαντική διανομή κλειδιών είναι ένα μαθηματικώς αποδεδειγμένα ασφαλές πρωτόκολλο, καθώς σε μια προσπάθεια υποκλοπής και αναμετάδοσης από κάποιος χάκερ δεν υπάρχει ανησυχία για το αν θα αποκαλυφθεί μια συγκεκριμένη τιμή από το αποτέλεσμα μέτρησης μιας κβαντικής κατάστασης. Πιο συγκεκριμένα, η διαφορά αυτού του πρωτόκολλου από αυτό της κλασικής διανομής κλειδιών είναι ότι ακόμη κι αν ο χάκερ καταφέρει να αποκτήσει πρόσβαση σε μια πληροφορία, δεν μπορεί ποτέ να την υποκλέψει. Οι ιδιότητες που το επιτρέπουν αυτό είναι, η αρχή της αβεβαιότητας, όπου διασφαλίζει από την αρχή την ασφάλεια της διανομής κβαντικού κλειδιού. Δηλαδή αν ένας χάκερ θελήσει να πάρει δεδομένα από κάποιο σύστημα, θα πρέπει να μετρήσει την κβαντική κατάσταση του, αλλά από την αρχή της αβεβαιότητας ξέρουμε ότι αυτές οι μετρήσεις επηρεάζουν ολόκληρο το σύστημα, έτσι οι χρήστες που επικοινωνούν μεταξύ τους θα αντιληφθούν ότι πέφτουν θύματα ενός κακόβουλου χάκερ. Η δεύτερη ιδιότητα, είναι αυτή της μη-κλωνοποίησης (no-cloning theorem), το οποίο απαγορεύει την πιθανότητα κάποιος να φτιάξει αντίγραφο μιας άγνωστης κβαντικής κατάστασης[1],[3]. Υπάρχουν πολλά πρωτόκολλα κβαντικής κρυπτογραφίας, αλλά εμείς σε αυτό το κεφάλαιο θα αναλύσουμε τα BB84 και E91.

5.2 Πρωτόκολλο BB84

Πρόκειται για το πρώτο πρωτόκολλο της κβαντικής κρυπτογραφίας που δημοσιεύτηκε το 1984, όπου ονομάστηκε BB84 από τα αρχικά των δημιουργών του Charles Bennett και Gilles Brassard.

5.2.1 Λειτουργία του BB84

Το πρωτόκολλο περιλαμβάνει δύο μέρη: Την Μαρία που στέλνει κβαντικά δεδομένα και τον Μπάμπη που τα λαμβάνει. Θεωρούμε αρχικά δύο βάσεις [1]:

Bit	$\oplus$ (Ορθογώνια βάση)	$\otimes$ (Διαγώνια βάση)
0	$\|0>=\alpha_{00}$	$\|+>=\alpha_{10}$
1	$\|1>=\alpha_{01}$	$\|->=\alpha_{11}$

Όπου $|+>=\frac{1}{\sqrt{2}}(|0>+|1>)$ και $|->=\frac{1}{\sqrt{2}}(|0>-|1>)$.

- Κβαντική μεταφορά [1]:
    1. Η Μαρία επιλέγει (4+δ)n τυχαία bits δεδομένων.
    2. Στην συνέχεια, επιλέγει τυχαία (4+δ)n ακολουθία b, όπου καθορίζει τις βάσεις κωδικοποίησης:
        - Αν b=0, τότε το bit κωδικοποιείται στην ορθογώνια βάση |0> ή |1>.
        - Αν b=1, τότε το bit κωδικοποιείται στην διαγώνια βάση |+> ή |->.
    3. Η Μαρία στέλνει τα qubits που προκύπτουν στον Μπάμπη μέσω του κβαντικού καναλιού.
    4. Ο Μπάμπης μετράει κάθε qubit σε μια από τις παραπάνω βάσεις που επιλέχθηκε τυχαία, με μια νέα ακολουθία b΄:
        - Αν επιλέξει σωστή βάση, παίρνει το σωστό αποτέλεσμα
        - Αν επιλέξει λάθος βάση, τότε το αποτέλεσμα θα είναι τυχαίο (υπάρχει 50% πιθανότητα να είναι σωστό).
- Δημόσια συζήτηση [1]
    1. Η Μαρία ανακοινώνει τη βάση κωδικοποίησης b.

2. Ο Μπάμπης θα κρατήσει μόνο τα αποτελέσματα που μέτρησε στη σωστή βάση όπου b = b΄.
3. Η Μαρία διαλέγει τυχαία n bits και λέει στον Μπάμπη ποια είναι.
4. Οι δύο χρήστες ελέγχουν τα n bits που επίλεξε η Μαρία και τα συγκρίνουν. Αν τα αποτελέσματα από τις μετρήσεις του Μπάμπη δεν είναι όμοιες με τις τιμές που αποκαλύφθηκαν, αυτό σημαίνει ότι κάποιος (τρίτο προσώπο) έχει παρεμβάλει και η επικοινωνία εγκαταλείπεται. Αλλιώς συνεχίζουν.
5. Τέλος, τα bits του b που απομένουν, αποτελούν το κοινό μυστικό κλειδί $k = \{0,1\}^N$.

5.2.2 Ασφάλεια του πρωτοκόλλου BB84

Το πρωτόκολλο BB84 αποδεικνύεται ασφαλές, αφού οποιαδήποτε απόπειρα υποκλοπής από κάποιο τρίτο πρόσωπο (χακερ) αλλάζει την κατάσταση των qubits, κάτι που εντοπίζεται από τον έλεγχο σφαλμάτων. Απορρίπτει μη ασφαλές κλειδιά, αν υπάρχει υποκλοπή ή μεγάλα σφάλματα, το πρωτόκολλο τερματίζει.

5.3 Πρωτόκολλο E91

Το πρωτόκολλο E91 παρουσιάστηκε για πρώτη φορά το 1991 από τον Artur Ekert. Πρότεινε ένα πρωτόκολλο διανομής κβαντικού κλειδιού, βασισμένο στο φαινόμενο κβαντικής διεμπλοκής με μια κεντρική πηγή μεταξύ δυο μερών για την ταυτόχρονη μετάδοση μηνυμάτων. Ένα πείραμα που επινοήθηκε το 1935 από του Einstein – Podolsky – Rosen (EPR), θεωρούν πως σε ένα ζεύγος σωματιδίων (EPR) ότι η τιμή μέτρησης ενός A σωματιδίου, καθορίζει και την τιμή μέτρησης του άλλου σωματιδίου B. Η κεντρική πηγή που χρησιμοποιεί το E91 μέσω ενός κβαντικού καναλιού παράγει ζεύγη σωματιδίων όπου βρίσκονται σε κατάσταση κβαντικής διεμπλοκής και τα οποία μπορεί να είναι πολωμένα φωτόνια και μετά να διαχωρίζονται. Υπάρχουν τρεις καταστάσεις πόλωσης για το ζεύγος φωτονίων [1]:

- $|S_0> = \frac{1}{\sqrt{2}} (|0>_1 |\frac{3\pi}{6}>_2 + |\frac{3\pi}{6}>_1 |0>_2)$

- $|S_1> = \frac{1}{\sqrt{2}} (|\frac{\pi}{6}>_1 |\frac{4\pi}{6}>_2 + |\frac{4\pi}{6}>_1 |\frac{\pi}{6}>_2)$
- $|S_2> = \frac{1}{\sqrt{2}} (|\frac{2\pi}{6}>_1 |\frac{5\pi}{6}>_2 + |\frac{5\pi}{6}>_1 |\frac{2\pi}{6}>_2)$

Το πρωτόκολλο E91 επίσης χρησιμοποιεί δύο βάσεις μέτρησης $\oplus$={|0>,|1>} και $\otimes$ = {|+>,|->}.

5.3.1 Εκτέλεση του E91

Έστω η Μαρία και ο Μπάμπης θέλουν να επικοινωνίσουν [1].

1. Επιλέγεται μια από τις παραπάνω καταστάσεις $|S_i>$ για να δημιουργηθεί το EPR ζεύγος σωματιδίων. Η πηγή δημιουργεί συμπλεκόμενα φωτόνια που βρίσκονται σε κβαντική διεμπλοκή $|\Psi^+> = \frac{1}{\sqrt{2}}(|01> + |10>)$. Το πρώτο σωματίδιο $|\Psi^+>_1$ αποστέλλεται στην Μαρία και το δεύτερο $|\Psi^+>_2$ στον Μπάμπη.
2. Η Μαρία και ο Μπάμπης επιλέγουν τυχαία μια βάση $\otimes$ ή $\oplus$ για να μετρήσουν το σωματίδιο. Στην συνέχεια καταγράφουν τα αποτελέσματα τους και αποκαλύπτουν τις βάσεις που χρησιμοποίησαν μέσω του κλασικού καναλιού.
3. Οι δύο χρήστες διαχωρίζουν τα αποτελέσματα σε δύο σύνολα: σε qubits G_a που επιλέχθηκαν διαφορετικές βάσεις και σε qubits G_b όπου επιλέχθηκε η ίδια βάση.
4. Το G_a χρησιμοποιείται για να ελέγξει αν υπάρχει κάποιο τρίτο πρόσωπο που προσπαθεί να κλέψει δεδομένα. Στην περίπτωση που υπάρχουν σφάλματα, τότε το κβαντικό κανάλι δεν είναι ασφαλές και εγκαταλείπουν την επικοινωνία.
5. Αν το κανάλι είναι ασφαλές το G_b μπορεί να χρησιμοποιηθεί σαν κλειδί αφού έχουν τις ίδιες μετρήσεις και το πρωτόκολλο ολοκληρώνεται επιτυχώς.

5.3.2 Ασφάλεια του E91

Το πρωτόκολλο E91 λοιπόν, αποδεικνύεται ασφαλές καθώς ακόμη και σε ένα θορυβώδες κανάλι, επιτυγχάνεται με ασφάλεια η απόκτηση μυστικού κλειδιού.

5.4 Επιθέσεις σε κβαντικά πρωτόκολλα

Είδαμε παραπάνω το πρώτο πρωτόκολλο διανομής κβαντικού κλειδιού καθώς και κάποιες παραλλαγές του, δηλαδή νέα πρωτόκολλα διανομής κβαντικού κλειδιού. Όσο αξιόπιστα και να είναι, υπήρξαν επιτυχημένες προσπάθειες ανθρώπων που αμφισβήτησαν την

ασφάλεια πρωτοκόλλων. Για παράδειγμα. Το BB84 ενώ θεωρείται αξιόπιστο, η εφαρμογή του από την θεωρία στην πράξη έχει κάποιες ατέλειες. Δηλαδή, λόγω ατελειών στην δημιουργία φωτονίων αλλά και στην μέτρηση τους, υπάρχουν πολλοί τρόποι για να σπάσουν τα πρωτόκολλα διανομής κβαντικού κλειδιού, τους οποίους θα δούμε παρακάτω.

5.4.1 Επίθεση αναχαίτισης εκ νέου αποστολής(Intercept-resend attack)

Σε αυτή την επίθεση ένας χάκερ μπορεί να μετρήσει το σήμα που κοινοποιήθηκε από την Μαρία και να στείλει την μέτρηση αυτή μέσω ενός θορυβώδους καναλιού στον Μπάμπη. Ο χάκερ, δεδομένου ότι το περιβάλλον είναι ιδανικό και οι ανιχνευτές είναι αποτελεσματικοί, κατέχει τα φωτόνια που στέλνει η Μαρία, τα αντικαθιστά και τα στέλνει στον Μπάμπη σύμφωνα με τη βάση της πόλωσης του. Ο Μπάμπης θα λάβει τα φωτόνια με τον ίδιο ρυθμό. Οι προσπάθειες του χάκερ θα είναι αποτελεσματικές μόνο όταν είναι σε θέση να λάβει τουλάχιστον το $\frac{1}{\sqrt{2}}$ των πληροφοριών της Μαρίας. [1]

5.4.2 Επίθεση Δούρειου Ίππου (Trojan Horse Attack)

Στις επιθέσεις Δούρειου Ίππου ή αλλιώς επιθέσεις έγχυσης φωτός (light injection attacks), ο χάκερ στοχεύει τις συσκευές κβαντικής κρυπτογράφησης που χρησιμοποιούνται κατά την επικοινωνία και όχι στην άντληση πληροφορίας μέσω παρεμβολής στο μεταδιδόμενο σήμα. Δηλαδή, ο χάκερ έχει την δυνατότητα να στείλει παλμούς φωτός στην οπτική ίνα της Μαρίας και του Μπάμπη οι οποίοι αντανακλούνται πίσω στην συσκευή που έχει στην κατοχή του ο χάκερ. Με το αντανακλόμενο σήμα ο χάκερ μπορεί να ανιχνεύσει τη βάση που χρησιμοποίησε η Μαρία. Αν η πληροφορία γίνει γνωστή στον χάκερ πριν τον Μπάμπη, μπορεί να μάθει ακριβώς τη ροή των qubits. [1]

5.4.3 Επίθεση πλασματικής κατάστασης (Faked-state attack)

Σε αυτού του είδους την επίθεση, ο υποκλοπέας εκμεταλλεύεται αυτή την αδυναμία του συστήματος στον ανιχνευτή του δέκτη(Μπάμπη). Βασίζεται στην έννοια των πλαστών καταστάσεων του φωτός , καταστάσεις που προετοιμάζονται από τον υποκλοπέα και αποστέλλονται στον Μπάμπη για να τον ελέγξει και να τον αναγκάσει να μετρήσει στη βάση που εκείνος υπαγορεύει. Ο χάκερ υποκλέπτει και μετρά τα φωτόνια της Μαρίας επιλέγοντας τυχαία μια βάση και προετοιμάζει μια νέα πλαστή κατάσταση για να την

στείλει στον Μπάμπη. Λέγεται ψεύτικη γιατί δεν στέλνει κβαντική κατάσταση αλλά κάνει τον ανιχνευτή του Μπάμπη να νομίζει ότι ανιχνεύει μια κβαντική κατάσταση. Ο υποκλοπέας μετράει την κατάσταση της Μαρίας και ετοιμάζει την αντίθετη βάση και το αντίθετο bit. [1]

5.4.4 PNS επιθέσεις (Photon Number Splitting Attack)

Η επίθεση διάσπασης αριθμού φωτονίων εκμεταλλεύεται ατέλειες και αδυναμίες στην εφαρμογή των πρωτοκόλλων διανομής κβαντικού κλειδιού. Ένας τυπικός παλμός σήματος περιέχει μεγάλο αριθμό φωτονίων, ωστόσο είναι δύσκολο να κατασκευαστούν ιδανικές πηγές μεμονωμένων φωτονίων. Πολλές φορές είναι αδύναμοι οι παλμοί laser για την κωδικοποίηση των bits στην εφαρμογή. Όταν η Μαρία στέλνει τα φωτόνια της στον Μπάμπη με ασθενείς παλμούς laser, ο υποκλοπέας αποσπά ένα φωτόνιο σήματος και αφήνει το υπόλοιπο σήμα να περάσει στον Μπάμπη. Ο υποκλοπέας περιμένει από την Μαρία να αποκαλύψει τη βάση που χρησιμοποίησε για κάθε σήμα και στην συνέχεια μετράει το φωτόνιο που λαμβάνει και εξάγει πληροφορίες για τα κωδικοποιημένα bits και το μυστικό κλειδί. [1]

ΣΥΜΠΕΡΑΣΜΑ

Καταλήγουμε λοιπόν ότι με αυτού του είδους οι επιθέσεις, η ασφάλεια των πρωτοκόλλων διανομής κβαντικού κλειδιού δεν βασίζεται μόνο στις αρχές της κβαντομηχανικής αλλά και σε ελαττωματικές οπτικές ίνες, μη καλά κατασκευασμένοι ανιχνευτές και άλλα κενά όπου γίνονται η αιτία των επιθέσεων που πραγματοποιούνται κατά των πρωτοκόλλων διανομής κβαντικού κλειδιού.

6 Μετα-κβαντική Κρυπτογραφία

Τα τελευταία χρόνια η κβαντική κρυπτογραφία εξελίσσεται με ραγδαία ταχύτητα. Αυτό σημαίνει ότι εξακολουθούν να υπάρχουν προκλήσεις και οι κβαντικοί υπολογιστές μεγάλης κλίμακας, θα είναι σε θέση να σπάσουν πολλά από τα κρυπτοσυστήματα δημόσιου κλειδιού που χρησιμοποιούνται σήμερα. Ο σκοπός της μετα-κβαντικής κρυπτογραφίας είναι να μας προετοιμάσει για την εποχή κβαντικών υπολογιστών, αναβαθμίζοντας τους

υπάρχοντες αλγόριθμους και πρωτόκολλα έτσι ώστε να είναι ασφαλή απέναντι σε κβαντικούς αλλά και κλασικούς υπολογιστές.

Κρυπτογραφικός Αλγόριθμος	Τύπος	Σκοπός	Επίπτωση στους κβαντικούς υπολογιστές
AES	Συμμετρικό κλειδί	Κρυπτογράφηση	Απαιτούνται μεγάλα κλειδιά
RSA	Δημόσιο κλειδί	Υπογραφές	Δεν είναι ασφαλές
ECDSA, ECDH	Δημόσιο κλειδί	Υπογραφές , Ανταλλαγή κλειδιών	Δεν είναι ασφαλές
DSA	Δημόσιο κλειδί	Υπογραφές , Ανταλλαγή κλειδιών	Δεν είναι ασφαλές

[1]

Η βασική πρόκληση στην μετακβαντική κρυπτογραφία είναι η ικανοποίηση των απαιτήσεων κρυπτογραφικής χρηστικότητας και ευελιξίας χωρίς να θυσιάζεται η εμπιστοσύνη.

Αφού είδαμε προηγουμένως την έννοια της μετα-κβαντικής κρυπτογραφίας και τον σκοπό της, θα μελετήσουμε τις κυριότερες κατηγορίες που την απαρτίζουν. Η μετα-κβαντική κρυπτογραφία εστιάζει σε 4 βασικούς τύπους κρυπτογραφικών συστημάτων, η διαφορά μεταξύ τους είναι ότι βασίζονται σε διαφορετικές μαθηματικές πράξεις. Είναι οι ακόλουθοι:

- Κρυπτογραφία βασισμένη σε κώδικα (Code-based Cryptography)
- Συναρτήσεις κατακερματισμού (Hash based Cryptography)
- Κρυπτογραφία με χρήση πολλών μεταβλητών (Multivariate Cryptography)
- Κρυπτογραφία βασισμένη σε πλέγματα (Lattice -based Cryptography)

6.1 Κρυπτογραφία βασισμένη σε κώδικα (Code-based Cryptography)

Τα κρυπτογραφικά συστήματα που βασίζονται σε κώδικες, βασίζονται στη θεωρία των κωδικών διόρθωσης σφαλμάτων όπου είναι σημαντικοί για την εποχή των κβαντικών υπολογιστών. Το 1978, προτάθηκε το πρώτο κρυπτοσύστημα δημόσιου κλειδιού βασισμένο στον κώδικα McEliece από τον Robert J. McEliece. Τα περισσότερα πρωτόκολλα που βασίζονται σε κώδικα χρησιμοποιούν πολύ μεγάλο μέγεθος κλειδιών (100 kilobytes σε αρκετά megabytes) , ίσως γι'αυτό να μην είναι γνωστή η πρακτική εφαρμογή κρυπτογραφίας με βάση τον κώδικα, ωστόσο γίνονται προσπάθειες για μείωση του μεγέθους δημοσίων κλειδιών. Η αυθεντική εκδοχή από τον McEliece βασίζεται στους δυαδικούς κώδικες Goppa, διότι έχουν πολύ καλές ιδιότητες όσον αφορά τη διόρθωση σφαλμάτων και πυκνό πίνακα γεννήτορα ο οποίος είναι δύσκολο να διαχωριστεί από έναν τυχαίο δυαδικό πίνακα. [4]

6.1.1 Λειτουργία του McEliece

Έστω P ένας πίνακας μετάθεσης nxn δυαδικός, με κάθε στήλη και γραμμή να περιέχει ένα μοναδικό 1 και τα υπόλοιπα 0.

- Παραγωγή κλειδιών:
    1. Έστω C είναι ένας γραμμικός κώδικας $[n,\ k,\ 2k+1]\ στο\ GF(2^m)$ ο οποίος έχει έναν αποτελεσματικό αλγόριθμο αποκωδικοποίησης D όπου διορθώνει μέχρι t σφάλματα.
    2. Υπολογίζουμε έναν γεννήτορα πίνακα $G[kxn]$ του C.
    3. Δημιουργούμε έναν τυχαίο, δυαδικό και αντιστρέψιμο πίνακα $S[kxk]$.
    4. Δημιουργούμε έναν τυχαίο πίνακα μετάθεσης $P[nxn]$.
    5. Υπολογίζουμε τον πίνακα $\acute{G} = S \cdot G \cdot P$ Το δημόσιο κλειδί είναι το $(\acute{G}, t)$ όπου t είναι ο αριθμός των σφαλμάτων που διορθώνει ο κώδικας. Το ιδιωτικό κλειδί είναι το (S, G, P, D).

- Κρυπτογράφηση:
  Για να κρυπτογραφήσουμε ένα μήνυμα $m \in \{0,1\}^k$, επιλέγουμε ένα τυχαίο διάνυσμα $z \in \{0,1\}^k$ βάρους t και υπολογίζουμε: $c = m\acute{G} + z$.

- Αποκρυπτογράφηση:
  Για να αποκρυπτογραφήσουμε το παραπάνω κρυπτοκείμενο, πρώτα υπολογίζουμε το : $CP^{-1} = (mS)G + zP^{-1}$. Στην συνέχεια εφαρμόζουμε τον πίνακα D και έχουμε $D(cP^{-1}) = mS$. Τέλος λύνουμε ως προς το m, άρα:
  $$m = (mS) \cdot S^{-1}$$

6.1.2 Συμπέρασμα

Ο αλγόριθμος McEliece προσφέρει υψηλή ασφάλεια και αντοχή στους κβαντικούς υπολογιστές, διότι δεν βασίζεται στην παραγοντοποίηση ή διακριτό λογάριθμο, αλλά σε ένα NP-hard πρόβλημα αποκωδικοποίησης. Το βασικό μειονέκτημα του είναι το μεγάλο μέγεθος κλειδιών και κρυπτοκειμένων, παρόλα αυτά στις σύγχρονες παραλλαγές του κρυπτοσυστήματος γίνεται προσπάθεια για την μείωση μεγέθους κλειδιών. Τέλος, αποτελεί μια από τις πιο υποσχόμενες τεχνικές για το μέλλον της κρυπτογραφίας.

6.2 Υπογραφές βασισμένες σε συναρτήσεις κατακερματισμού (Hash- based Signatures)

Οι υπογραφές βασισμένες στις συναρτήσεις κατακερματισμού είναι ένα από τα πιο ασφαλή κρυπτογραφικά πρωτόκολλα που αντέχουν σε επιθέσεις από κβαντικούς υπολογιστές. Τα HBS (Hash-based Signatures) χρησιμοποιούν ασφαλείς συναρτήσεις κατακερματισμού (SHA-3) για την δημιουργία και επαλήθευση ψηφιακών υπογραφών. Τα συστήματα υπογραφής με βάση τον κατακερματισμό επινοήθηκαν από τον Ralph Merkle το 1979, συνδυάζουν ένα σχήμα υπογραφής μίας χρήσης (One-Time Signatures-OTS) με μια δομή του συστήματος Merkle. Οι υπογραφές Lamport είναι ένα παράδειγμα ενός συστήματος υπογραφής μιας χρήσης (OTS) που μπορεί να συνδυαστεί με μια δομή τύπου Merkle. Οι υπογραφές μιας χρήσης είναι πιο θεμελιώδες και η κατασκευή ενός ασφαλούς σχήματος υπογραφής one-time απαιτεί μόνο μια συνάρτηση μιας κατεύθυνσης. Ωστόσο

έχουν ένα σοβαρό ελάττωμα, ένα ζεύγος κλειδιών που αποτελείται από ένα μυστικό και ένα δημόσιο κλειδί επαλήθευσης μπορεί να χρησιμοποιηθεί μόνο για την υπογραφή και την επαλήθευση ενός μόνο εγγράφου. Ο Merkle είχε την ιδέα να χρησιμοποιεί ένα hash δέντρο που μειώνει την εγκυρότητα πολλών κλειδιών επαλήθευσης one-time στην εγκυρότητα ενός δημόσιου κλειδιού. Η αρχική κατασκευή του Merkle δεν ήταν τόσο αποτελεσματική, κυρίως σε σύγκριση με το σύστημα RSA.Επίσης, πολλά από τα πιο αποδοτικά συστήματα υπογραφής που βασίζονται στον κατακερματισμό έχουν το μειονέκτημα ότι ο υπογράφων πρέπει να κρατά αρχείο με τον ακριβή αριθμό μηνυμάτων που έχουν υπογραφεί προηγουμένως και κάθε λάθος σε αυτό το αρχείο θα έχει ως αποτέλεσμα κενό ασφαλείας σε αυτό. Ένα άλλο μειονέκτημα είναι ότι μπορούν να παράγουν μόνο έναν περιορισμένο αριθμό υπογραφών. Ο αριθμός των υπογραφών μπορεί να αυξηθεί αλλά θα αυξηθεί και το μέγεθος της υπογραφής. Ωστόσο έχουν βελτιωθεί πολύ και πλέον οι υπογραφές με βάση τον κατακερματισμό αποτελούν την πιο υποσχόμενη λύση για το RSA και τις Ελλειπτικές καμπύλες . [4]

- Σχήμα υπογραφής Merkle (Merkle Signature Scheme-MSS)
  Το σχήμα Merkle βασίζεται σε δέντρα Merkle και υπογραφές μιας χρήσης (OTS) όπως και οι Lamport OTS και Winternitz OTS. Επίσης, μπορεί να χρησιμοποιηθεί για την υπογραφή ενός αυθαίρετου αριθμού μηνυμάτων χρησιμοποιώντας ένα δημόσιο κλειδί. Τα δέντρα Merkle δημιουργούνται με επαναλαμβανόμενο κατακερματισμό ζευγών κόμβων μέχρι να απομείνει μόνο ένας κατακερματισμός, η ρίζα Merkle. Παρακάτω θα δούμε τις βελτιωμένες παραλλαγές του MSS. [11]

- Σχήμα eXtended Merkle Signature (XMSS)
  Δημοσιεύθηκε το 2011 και έχει αρκετά κοινά με το MSS, όμως είναι μια ασφαλέστερη έκδοση και μπορεί να παράγει μικρότερα μεγέθη υπογραφών. Χρησιμοποιεί κυρίως ως βασικό πρωτόκολλο το WOTS+ (Winternitz One -Time Signature Plus), είναι ανθεκτικό σε κβαντικούς υπολογιστές καθώς βασίζεται σε ασφαλείς συναρτήσεις κατακερματισμού. Τέλος, είναι ένα από τα πρώτα σχήματα υπογραφών που εγκρίθηκαν από το NIST (Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας – National Institute of Standards and Technology) για την μετακβαντική κρυπτογραφία. [11]

- Υπογραφές Leighton-Micali (LMS)

Το LMS βασίζεται σε δέντρα Merkle και είναι παρόμοιο με το XMSS απλα σε πιο απλοποιημένη μορφή. Χρησιμοποιεί πιο συχνά HORS OTS (Hierarchical One-Time Signature) ως βάση για τις υπογραφές και στην συνέχεια, στο πλήρες σχήμα συνδυάζεται το σχήμα μιας χρήσης ως υπορουτινα με μια κατασκευή δεντρου Merkle για να έχουμε πλήρες stateful LMS σχήμα υπογραφής. Τέλος, αποτελεί επίσης μια από τις επιλογές του NIST για την μετακβαντική κρυπτογραφία και είναι κατάλληλο για συστήματα με περιορισμένους πόρους (IoT). [11]

- SPHINCS/SPHINCS+

Δημοσιεύθηκε το 2015, είναι ένα stateless μετακβαντικό σχήμα υπογραφών βασισμένο στο MSS (Merkle Signature Scheme). Κύριο πλεονέκτημα είναι ότι σε αντίθεση με τα LMS και XMSS δεν απαιτεί παρακολούθηση κατάστασης, ενώ ένα μειονέκτημά του είναι ότι έχει μεγαλύτερα μεγέθη υπογραφών (41 kilobytes) και είναι πιο αργό. Το σχήμα όμως προσφέρει ισχυρή ασφάλεια έναντι στους κβαντικούς υπολογιστές. Το SPHINCS+ είναι μια αναβάθμιση αφού αντιμετωπίζει το μέγεθος κλειδιών, με την υψηλότερη ασφάλεια να οδηγεί σε υπογραφές μεγέθους 30 kilobytes. Το σχήμα μπορεί να φτάσει τα οκτώ kilobytes αλλά θα είναι χαμηλότερη η ασφάλεια. [11]

6.3 Κρυπτογραφία με χρήση πολλών μεταβλητών (Multivariate Cryptography)

Η πολυμεταβλητή κρυπτογραφία είναι ένας κλάδος που βασίζεται στην δυσκολία επίλυσης πολυμεταβλητών πολυωνυμικών συστημάτων πάνω από πεπερασμένα σώματα. Ενα πολυμεταβλητό κρυπτογραφικό σύστημα χρησιμοποιεί πολυωνυμικά συστήματα της μορφής $P_i = (x_1, x_2, \dots, x_n) = c$ όπου τα P_i είναι πολυώνυμα με πολλαπλές μεταβλητές και η επίλυση τέτοιων συστημάτων είναι υπολογιστικά δύσκολη (NP-hard), καθιστώντας τα πολυμεταβλητά σχήματα ανθεκτικά σε κβαντικές επιθέσεις. Όμως αρκετά κρυπτοσυστήματα έχουν προταθεί τις τελευταίες δεκαετίες, με πολλά από αυτά να έχουν καταρριφθεί. Παρακάτω θα δούμε τα πιο δημοφιλή πολυμεταβλητά κρυπτοσυστήματα. [4]

- Εξισώσεις κρυμμένου πεδίου (Hidden Field Equations – HFE)

  Το 1996 ο Jacque Patarin παρουσίασε ένα κρυπτοσύστημα δημόσιου κλειδιού. Το HFE βασίζεται στην δυσκολία των προβλημάτων επίλυσης ενός συστήματος τετραγωνικών εξισώσεων. Επίσης, βασίζεται σε πολυώνυμα πάνω σε πεπερασμένα πεδία διαφορετικών μεγεθών για την απόκρυψη της σύνδεσης μεταξύ ιδιωτικών και δημόσιων κλειδιών. Αποτελεί μια από τις πιο γνωστές προσεγγίσεις στην πολυμεταβλητη κρυπτογραφία, είναι ανθεκτικό στους περισσότερους κβαντικούς υπολογιστές, αν και έχει δεχθεί αρκετές επιθέσεις, οι παραλλαγές του αποτελούν ισχυρούς υποψήφιους για μετακβαντικές εφαρμογές.

- Rainbow

  Είναι πολυμετάβλητο σχήμα ψηφιακής υπογραφής το οποίο αναπτύχθηκε από τους Jintai Ding και Dieter Schmidt το 2005. Αποτελεί μια επέκταση του Unbalanced Oil and Vinegar (UOV). Ενώ είναι πολύ γρήγορο, το Rainbow έχει το ίδιο μειονέκτημα με τα προηγούμενα, δηλαδή μεγάλο μέγεθος κλειδιών και υπογραφών. [11]

6.4 Κρυπτογραφία βασισμένη σε πλέγματα (Lattice-based Cryptography)

Τα πλέγματα είναι διανύσματα συντεταγμένων σε ένα χώρο n- διαστάσεων. Τα κρυπτογραφικά σχήματα που βασίζονται στην θεωρία πλεγμάτων είναι ίσως τα πιο διάσημα από όλα τα υποψήφια για μετακβαντική κρυπτογραφία. Οι αλγόριθμοι που βασίζονται σε αυτά είναι απλοί και αποδοτικοί. Τα κρυπτογραφικά πρωτόκολλα βασισμένα σε πλέγματα, είναι ασφαλή καθώς βασίζονται στην ισχυρή τους ασφάλεια σε γνωστά προβλήματα πλέγματος όπως το πρόβλημα του συντομότερου διανύσματος (Shortest Vector Problem – SVP) και το πρόβλημα μάθησης με σφάλματα (Learning With Errors – LWE). [3]

6.4.1 Τα πιο γνωστά προβλήματα που χρησιμοποιούνται στην κρυπτογραφία πλεγμάτων είναι:

- SVP (Shortest Vector Problem – Πρόβλημα του συντομότερου Διανύσματος)

Είναι ένα πολύ ενδιαφέρον και μελετημένο υπολογιστικό πρόβλημα στα πλέγματα. Το SVP ορίζει ότι, δεδομένου ενός πλέγματος L, πρέπει να βρεθεί το συντομότερο μη μηδενικό διάνυσμα μέσα στο L. Μια παραλλαγή αυτού του προβλήματος είναι ο υπολογισμός του μήκους του συντομότερου μη μηδενικού διανύσματος στο L χωρίς να βρεθεί το ίδιο το διάνυσμα. [12]

- CVP (Closest Vector Problem – Πρόβλημα Πλησιέστερου Διανύσματος)
  Είναι ένα υπολογιστικό πρόβλημα στα πλέγματα που σχετίζεται με το SVP. Το CVP ορίζει ότι, δεδομένου ενός σημείου στόχου t, πρέπει να βρεθεί το πιο κοντινό σημείο του πλέγματος στο t. [12]

- LWE (Learning With Errors – Μάθηση Με Σφάλματα)
  Βασίζεται στην δυσκολία ανακατασκευής ενός μυστικού διανύσματος από έναν θορυβώδη γραμμικό συνδυασμό. Αποτελεί τη βάση για πολλά ασφαλή μετακβαντικά κρυπτοσυστήματα. Στην συνέχεια θα δούμε δύο από τα πιο σημαντικά κρυπτοσυστήματα με πλέγματα.

6.4.2 Goldreich – Goldwasser – Halevi (GGH)

Το GGH είναι ένα κρυπτοσύστημα δημόσιου κλειδιού που χρησιμοποιεί το πρόβλημα του πλησιέστερου διανύσματος (CVP). Προτάθηκε το 1997 από τους Oded Goldreich, Shafi Goldwasser και Shai Haveli.

- Λειτουργία του GGH [12]:
  1. Η Μαρία δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί:
     - Ιδιωτικό κλειδί (Private Key) → Μια "καλή" βάση V (εύκολη στην αποκρυπτογράφηση).
     - Δημόσιο κλειδί (Public Key) → Μια "κακή" βάση W (για χρήση στην κρυπτογράφηση).
     - Για να δημιουργήσει την "κακή" βάση W, πολλαπλασιάζει την καλή βάση με έναν τυχαίο unimodular πίνακα U:

$$W=UV.$$

Το W είναι το δημόσιο κλειδί που δημοσιεύεται.

2. Κρυπτογράφηση (Μπάμπης):

   Ο Μπάμπης θέλει να στείλει ένα μήνυμα m στην Μαρία

   - Μετατρέπει το μήνυμα m σε ένα διάνυσμα (π.χ., μια σειρά από αριθμούς 0 και 1).
   - Επιλέγει έναν μικρό τυχαίο θόρυβο r για να κάνει το κρυπτοκείμενο πιο δύσκολο στην επίθεση.
   - Υπολογίζει το κρυπτοκείμενο ως εξής χρησιμοποιώντας το δημόσιο κλειδί της Μαρίας και στην συνέχεια στέλνει το e σε εκείνη :

$$e=mW+r$$

3. Αποκρυπτογράφηση (Μαρία):

   - Χρησιμοποιεί το ιδιωτικό της κλειδί (την "καλή" βάση V) για να βρει το πλησιέστερο σημείο του πλέγματος στο e.
   - Εφαρμόζει τον αλγόριθμο Babai's Nearest Plane για να αφαιρέσει τον θόρυβο και να ανακτήσει το μήνυμα.
   - Υπολογίζει: $aW^{-1} = mWW^{-1}$, προκύπτει το m.

Συμπέρασμα

Αν και το GGH βασίζεται σε σκληρά μαθηματικά προβλήματα, μπορεί να σπάσει με αλγορίθμους μείωσης βάσης όπως ο **LLL (Lenstra-Lenstra-Lovász)**. Για αυτόν τον λόγο, δεν χρησιμοποιείται πλέον στην πράξη και αντικαταστάθηκε από πιο ασφαλή συστήματα όπως το NTRU που θα δούμε στην συνέχεια.

6.4.3 NTRU (N-th degree Truncated Polynomial Ring Units)

Το NTRU (N-th degree Truncated Polynomial Ring Units) είναι ένα ασφαλές και αποδοτικό κρυπτοσύστημα πλέγματος, το οποίο ανήκει στην κατηγορία της κβαντικής κρυπτογραφίας. Δημιουργήθηκε το 1996 από τους Hoffstein, Pipher και Silverman ως εναλλακτική λύση στα κρυπτοσυστήματα RSA και ECC και Βασίζεται σε δύσκολα προβλήματα πλεγμάτων, τα SVP και CVP .

- Λειτουργία του NTRU [12]:
    4. Η Μαρία δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί:
        - Επιλέγει δύο πολυώνυμα f(x) και g(x) τυχαία. Αυτά είναι το ιδιωτικό κλειδί.
        - Υπολογίζει τα αντίστροφα f^{-1} σε δύο διαφορετικές μορφές (mod q και mod p).
        - Υπολογίζει το δημόσιο κλειδί ως:

$$h(x) = f^{-1} \cdot g(x) mod q.$$

Το δημόσιο κλειδί είναι το h(x) και το ιδιωτικό κλειδί είναι το ζεύγος(f(x),F_p(x)).

5. Κρυπτογράφηση (Μπάμπης):

   Ο Μπάμπης θέλει να στείλει ένα μήνυμα m στην Μαρία
    - Μετατρέπει το μήνυμα m σε πολυώνυμο με μικρούς συντελεστές.
    - Επιλέγει ένα τυχαίο πολυώνυμο θορύβου r(x).
    - Υπολογίζει το κρυπτοκείμενο και στέλνει το e(x) στην Μαρία:

$$e(x)=h(x)\cdot r(x)+m(x) mod q$$

6. Αποκρυπτογράφηση (Μαρία):
    - Υπολογίζει: $a(x)=f(x)\cdot e(x) mod q$.
    - Μεταφέρει τους συντελεστές του a(x)a(x) στο διάστημα $[-q/2,q/2]$.
    - Υπολογίζει: $b(x) = F_p(x) \cdot a(x) mod p$.

      Το b(x) ισούται με το αρχικό μήνυμα m(x).

Συμπέρασμα

Το NTRU είναι ένα γρήγορο, αποδοτικό και ανθεκτικό σε κβαντικούς υπολογιστές κρυπτοσύστημα που βασίζεται σε πλέγματα και είναι κατάλληλο για το μέλλον της κρυπτογραφίας.

7 Συμπεράσματα

Στην παρούσα πτυχιακή μετά από μία εισαγωγή στην κβαντική υπολογιστική ασχοληθήκαμε με υπάρχοντες κρυπτογραφικούς αλγόριθμους που μερικοί από αυτούς αποδείχθηκαν αναξιόπιστοι και εμβαθύναμε σε μετα-κβαντικούς κρυπτογραφικούς αλγόριθμους που έχουν προταθεί ώστε να διασφαλισθεί η ασφάλεια στον ερχομό της Κβαντικής Εποχής. Η κβαντική υπολογιστική δεν αποτελεί απλώς μια εξέλιξη, αλλά μία επανάσταση της πληροφορικής παγκοσμίως και η εξέλιξη της είναι ραγδαία. Ωστόσο, βρίσκονται ακόμα σε αρχικό στάδιο και υπάρχουν πολλά προβλήματα που πρέπει να προβλεφθούν και να λυθούν. Το πιο σημαντικό είναι να δημιουργηθούν ανθεκτικά και σταθερά υλικά για τους κβαντικούς υπολογιστές, καθώς και να διασφαλιστεί ότι μπορούν να λύνουν προβλήματα με αξιοπιστία και χωρίς σφάλματα. Τέλος, η κβαντική υπολογιστική προσφέρει δυνατότητες που ξεπερνούν τα όρια της σημερινής τεχνολογίας. Πρέπει να τη διαχειριστούμε με προσοχή, ώστε να εκμεταλλευτούμε όλα τα οφέλη της και να συμβάλουμε σε μια θετική αλλαγή για τον κόσμο.

Βιβλιογραφία

[1] Ηλία Κ. Σάββας | Μαρία Ε. Σαμπάνη. Κβαντική Υπολογιστική: από την θεωρία στην πράξη. 2022.

[2] ΜΑΝΤΩΣ, Παναγιώτης Α. Κβαντική υπολογιστική: παρούσα κατάσταση και μελλοντικές τάσεις. 2023. Master's Thesis.

[3] SAMPANI, Maria. Post-quantum cryptographic algorithms. 2024. PhD Thesis. Πανεπιστήμιο Θεσσαλίας. Σχολή Τεχνολογίας. Τμήμα Ψηφιακών Συστημάτων.

[4] ΜΟΝΟΓΙΌΣ, Κωνσταντίνος. Μετακβαντικοί κρυπτογραφικοί αλγόριθμοι (Post-Quantum Cryptography). 2019.

[5] ΜΗΛΟΎΣΗ, Κωνσταντίνα Γεωργίου. Κβαντική Διανομή Κλειδιού: Βασικά Πρωτόκολλα και Επιθέσεις. 2023. PhD Thesis. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

[6] "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.

[7] ΚΑΡΑΦΥΛΛΊΔΗΣ, Ιωάννης. Κβαντική Υπολογιστική. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015.

[8] William Stallings | Lawrie Brown. Ασφάλεια Υπολογιστών: Αρχές και πρακτικές– 3η αμερικανική έκδοση.

[9] Ν. ΑΛΕΞΑΝΔΡΗΣ | Β. ΧΡΥΣΙΚΟΠΟΥΛΟΣ | Κ. ΠΑΤΣΑΚΗΣ. Εισαγωγή στην θεωρία πληροφοριών, κωδικών & κρυπτογραφίας.

[10] ΓΙΑΝΝΟΎΤΣΟΣ, Παναγιώτης. *Ο κβαντικός αλγόριθμος του Σόρ*. 2020. PhD Thesis. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

[11] CIESLA, Robert. Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography. Apress, 2020.

[12] Maria E. Sabani, “Quantum Key Distribution Protocols & Threats” , Dept of Digital Systems, University of Thessaly