Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Πρόγραμμα Μεταπτυχιακών Σπουδών, "Εφαρμοσμένα Μαθηματικά", Σχολή Θετικών Επιστημών, Τμήμα Μαθηματικών

Διπλωματική Εργασία

Κβαντική και Μετα-Κβαντική Κρυπτογραφία και Εφαρμογές
Quantum and Post-Quantum Cryptography and Applications

ΒΟΥΔΟΥΡΗΣ Σ. ΑΝΑΣΤΑΣΙΟΣ

Επιβλέπων καθηγητής: *Μπάρδης Νικόλαος, Αναπληρωτής Καθηγητής, Στρατιωτική Σχολή Ευελπίδων*

Αθήνα, 2019

Ευχαριστίες

Ευχαριστώ τον επιβλέποντα καθηγητή αυτής της διπλωματικής εργασίας, Νικόλαο Μπάρδη, για την υποστήριξη που μου παρείχε καθώς και τους καθηγητές της Συμβουλευτικής-Εξεταστικής Επιτροπής για τις πολύτιμες συμβουλές τους, Δημήτρη Βάρσο και Μιχαήλ Δρακόπουλο.

9 Οκτωβρίου 2019

Περιεχόμενα

Περίληψη

Στην παρούσα διπλωματική εργασία, αναλύονται τα θέματα Κβαντικής και Μετά-Κβαντικής Κρυπτογραφίας και εφαρμογές τους σε σύγχρονα συστήματα επικοινωνιών. Ξεκινάει στο πρώτο κεφάλαιο με μια ιστορική και εννοιολογική αναδρομή στα σημαντικότερα σημεία της σημερινής Κλασικής Κρυπτογραφίας και την εφαρμογή της ως ένας τρόπος ασφαλούς επικοινωνίας ανάμεσα σε δύο άτομα ή συστήματα. Παρουσιάζεται συνοπτικά η κλασική κρυπτογραφία με τις κατηγορίες της συμμετρικής και μη συμμετρικής κρυπτογράφησης καθώς και η σύγκριση τους.

Στο δεύτερο κεφάλαιο, θίγουμε θέματα της κβαντικής φυσικής όπως η Αρχή Απροσδιοριστίας του Heisenberg, η εξίσωση του Shrodinger, το παράδοξο των Einstein-Podolsky-Rosen καθώς και τον "απροσδιόριστο" ακόμα και σήμερα όρο, της κβαντικής διεμπλοκής δύο σωματιδίων. Αυτά τα θέματα θεωρούνται η φυσική βάση στην οποία θα στηριχθούν οι προσπάθειες κατασκευής του κβαντικού υπολογιστή. Ασχολούμαστε με την πλέον πιο σημαντική εφαρμογή της κβαντικής φυσικής στο κλάδο της κρυπτογραφίας, αυτής της κβαντικής διαμοίρασης κλειδιού. Πολλοί αναφέρονται στον όρο αυτό και ως κβαντική κρυπτογραφία. Αναλύουμε συγκεκριμένα το πρωτόκολλο BB84. Η κατασκευή ενός κβαντικού υπολογιστή θα σημάνει πολλές αλλαγές στο τρόπο ζωής των ανθρώπων και μια από αυτές, από τη σκοπιά της κρυπτογραφίας, είναι η εφαρμογή του αλγορίθμου του Shor, ο οποίος υπόσχεται τη παραγοντοποίηση μεγάλων πρώτων αριθμών, άρα και τη κατάρριψη της ασφαλούς επικοινωνίας μέσω του γνωστού σε όλους μας κρυπτοσυστήματος,RSA.

Στο τρίτο κεφάλαιο παρουσιάζεται και αναλύεται η μετα-κβαντική κρυπτογραφία. Η ολοκλήρωση των κβαντικών υπολογιστών θα διαταράξει τις συνθήκες ασφάλειας δεδομένων και συστημάτων όπως την ακεραιότητα -αυθεντικοποίηση δεδομένων κατά την μετάδοσης τους αλλά και τη συνθήκη της εμπιστευτικότητας που εξασφαλίζεται με την κρυπτογραφία. Θα στηριχτούμε σε δύσκολα μαθηματικά προβλήματα μέχρι σήμερα, από το χώρο των δικτυωμάτων και των γραμμικών κωδίκων ή αλλιώς κωδίκων Goppa, και θα κατασκευάσουμε κρυπτοσυστήματα τα οποία είναι ανθεκτικά σε κβαντικές κρυπταναλυτικές επιθέσεις.

Τέλος, παρουσιάζεται η δεύτερη εφαρμογή της κβαντικής κρυπτογραφίας, πέρα της κβαντικής διαμοίρασης κλειδιού, αυτή της delegated quantum communication.

Abstract

At the first chapter, we overturn historically and conceptually at the basic parts of our modern classical cryptography, from its application as a way of safe communication between two people to the asymmetric cryptography and the idea of the public key, which allows more users to communicate with each other and the corresponding cryptosystems. At the second chapter we touch on aspects of quantum physics such as the Heisenberg's Uncertainty Principle, the Shrodinger equation, the Einstein-Podolsky-Rosen paradox and the "undefined" term of quantum entaglement of two particles. The construction of a quantum computer will bring a lot of changes in our everyday lives, and from the point of view of cryptography, we will finally be able to apply Shor's algorithm which solves the factorization problem of large prime numbers and breaking the RSA cryptosystem as well as the safe communication between people. We analyze in depth this algorithm, and we focus on the most famous application of quantum physics in cryptography, the quantum key distribution. It is another term of talking about quantum cryptography. We examine the BB84 protocol, which is one the first protocols of quantum key distribution. At last, in the third chapter we analyse the term post-quantum cryptography. The arrival of a quantum computer , will stir up the waters of safe communication between people, and with the help of the Mathematics, we will use hard mathematical problems from the space of lattices and linear codes,namely Goppa Codes, till today, and we will construct based on this assumption, cryptosystems that are resistant in quantum cryptanalytic attacks.

Εισαγωγή

Η Θεωρία Αριθμών, η Άλγεβρα και η Θεωρία Αλγορίθμων (μέσω των ιδιότητων των πρώτων αριθμών, των πεπερασμένων σωμάτων και των ελλειπτικών καμπύλων) σε συνδυασμό με την αύξηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών διεύρυναν και προώθησαν τα πεδία εφαρμογής της κλασικής κρυπτογραφίας για ασφαλή μετάδοση μηνυμάτων ως προς την ακεραιότητα των μηνυμάτων αλλά και την αυθεντικότητα των χρηστών, τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης στα μηνύματα και την αδυναμία αποκήρυξης μηνυμάτων.

Είναι φανερό, από την παραπάνω πραγματικότητα, τι προαπαιτείται ώστε κάποιος να μπορεί να παρακολουθήσει με στοιχειώδη τρόπο και βασική κατανόηση την εξέλιξη της κρυπτογραφίας μέχρι σήμερα.

Η κβαντική θεωρία (ένα από τα πιο σημαντικά επιστημονικά επιτεύγματα του προηγούμενου αιώνα) προκαλεί με την θεωρητικά τουλάχιστον, προς το παρών, ανάμειξή της, στα προβλήματα αιχμής της κρυπτογραφίας ως προς το επίπεδο ασφάλειας και ταχύτητα υλοποίησης των αλγορίθμων. Με την εργασία αυτή λοιπόν, αφού προηγηθεί μια αναφορά στη μέχρι τώρα υφιστάμενη πραγματικότητα, επιχειρείται η είσοδος σε αυτό τον άγνωστο, δαιδαλώδη, και ανεξερεύνητο χώρο της χαρακτηριζόμενης κβαντικής και μετακβαντικής κρυπτογραφίας.

ΚΕΦΑΛΑΙΟ 1

Κρυπτογραφία

1.1 Ιστορική Αναδρομή

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση. Η κρυπτολογία ασχολείται με την μελέτη της ασφαλούς επικοινωνίας.

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης, με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η ασφάλεια πληροφοριών εξασφαλίζεται από τα ακόλουθα χαρακτηριστικά:

- ◇ ***Εμπιστευτικότητα***: Η προς μετάδοση πληροφορία είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- ◇ ***Ακεραιότητα***: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- ◇ ***Μη απάρνηση***: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- ◇ ***Αυθεντικοποίηση-Πιστοποίηση***: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.
- ◇ ***Διαθεσιμότητα***: Εξασφάλιση της ασφάλειας στη χρήση των υπολογιστικών πόρων και δικτύων, κατά τη χρησιμοποίηση ολοκληρωμένων βάσεων δεδομένων και συστημάτων επεξεργασίας πληροφοριών.
- ◇ ***΄Ελεγχος πρόσβασης***: Εξασφάλιση της μη πρόσβασης των μη εξουσιοδοτημένων χρηστών σε υπολογιστικούς πόρους και συστήματα.

Η κρυπτογραφία έχει ακολουθήσει στην εξέλιξή της δύο κατευθύνσεις

1. τη συμμετρική κρυπτογραφία

2. την ασύμμετρη κρυπτογραφία

Στο σημείο αυτό, αναφέρουμε ότι πέρα του διαχωρισμού σε συμμετρική και ασύμμετρη κρυπτογραφία, έχουμε και το διαχωρισμό αναλόγως του τρόπου αλλαγής του αρχικού μηνύματος σε

1. κρυπτογράφηση με αντιμετάθεση

2. κρυπτογράφηση με αντικατάσταση

Ο επόμενος ορισμός περιγράφει τόσο τα κλασσικά κρυπτοσυστήματα συμμετρικής κρυπτογραφίας όσο και τα κρυπτοσυστήματα δημοσίων κλειδιών, ή ασύμμετρης κρυπτογραφίας

Ορισμός 1.1. *Ένα κρυπτοσύστημα αποτελείται από πεπερασμένα σύνολα* $(\Sigma_1, \Sigma_2, K, E, D)$ *όπου:*

- Σ_1*- ένα αλφάβητο (πεπερασμένο σύνολο) και το* Σ_1^* *λέγεται ο χώρος απλών κειμένων (plaintext) (τα στοιχεία του απλά κείμενα), και δηλώνει το σύνολο όλων των πιθανών απλών κειμένων που μπορούν να κρυπτογραφηθούν.*

- Σ_2*- ένα αλφάβητο (όχι απαραίτητα διαφορετικό από το* Σ_1*) και το* Σ_2^* *καλείται χώρος κρυπτοκειμένων (ciphertext) και τα στοιχεία του κρυπτοκείμενα.*

- K *- ένα αλφάβητο και τα στοιχεία του* K^* *λέγονται κλειδιά.*

- E*- μια* $1-1$ *συνάρτηση* $E : (K^* \times \Sigma_1^*) \longrightarrow \Sigma_2^*$*. Η* E *λέγεται συνάρτηση κρυπτογράφησης (encryption). Συμβολίζουμε την* $E(k, x)$ *ως* $E_k(x)$*, όπου* $k \in K^*$ *και* $x \in \Sigma_1^*$*.*

- D *- μια συνάρτηση η οποία ονομάζεται συνάρτηση αποκρυπτογράφησης* $D : (K^* \times \Sigma_2^*) \longrightarrow \Sigma_1^*$*. Συμβολίζουμε την* $D(k, x)$ *ως* $D_k(x)$*, όπου* $k \in K^*$ *και* $x \in \Sigma_2^*$*.*

- *Οι συναρτήσεις* E, D *είναι τέτοιες ώστε*

$$\exists\, (k \in K^*,\ k^{'} \in K^*)\ \forall x \in \Sigma_1^*\ : D_{k^*}(E_k(x)) = x$$

Όπως θα δούμε και στη συνέχεια, στην ασύμμετρη κρυπτογραφία, το κλειδί κρυπτογράφησης k είναι δημόσιο, δηλαδή είναι γνωστό στο καθένα, ενώ το κλειδί αποκρυπτογράφησης $k^{'}$ κρατείται απόρρητο. Ακολουθεί ο ορισμός των συναρτήσεων μονής κατεύθυνσης (one-way functions), οι οποίες παίζουν σημαντικό ρόλο στη σημερινή κρυπτογραφία.

Ορισμός 1.2. *Έστω δύο αλφάβητα* Σ_1, Σ_2*, και* f *μια συνάρτηση* $f : \Sigma_1^* \longrightarrow \Sigma_2^*$*. Λέμε ότι η* f *είναι συνάρτηση μονής κατεύθυνσης αν ισχύουν τα παρακάτω:*

1. *η* f *είναι* $1-1$ *και για όλα τα* $x \in \Sigma_1^*$*, και για την* $f(x)$ *ισχύει*

$$|x|^{\frac{1}{k}} \leq |f(x)| \leq |x|^k$$

για κάποιο $k > 0$*.*

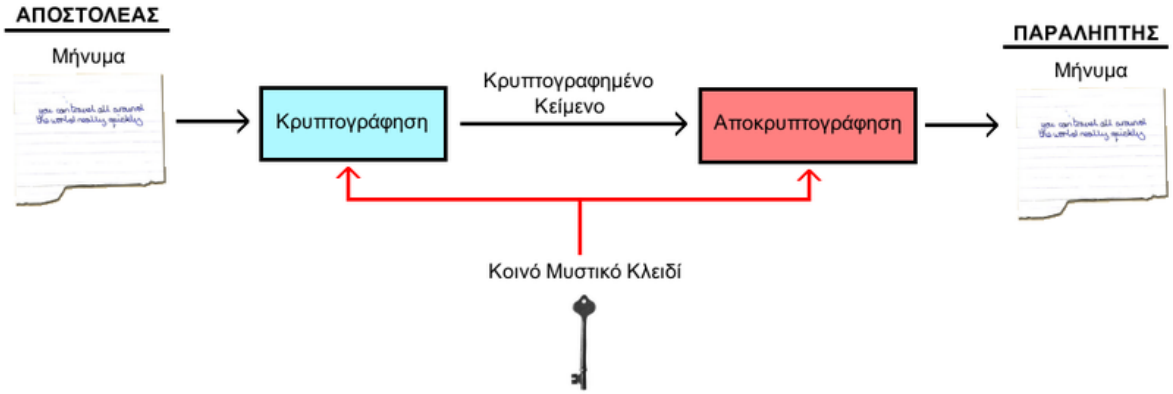
2. *Η $f(x)$ μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο.*

3. *Για την f^{-1}, την αντίστροφη της f δεν υπάρχει αλγόριθμος πολυωνυμικού χρόνου, δηλαδή το πρόβλημα του υπολογισμού του $x \in \Sigma_1$ δεδομένου του $f(x) \in \Sigma_2$ είναι απρόσιτο.*

Υπάρχουν μονόδρομες συναρτήσεις των οποίων η αντιστροφή επιτυγχάνεται μόνο με την εισαγωγή μιας επιπρόσθετης τεχνικής προυπόθεσης, ενός μηχανισμού "καταπακτής" όπως λέγεται και η συνάρτηση τότε καλείται *συνάρτηση καταπακτής (trapdoor function)*.

1.2 Συμμετρική Κρυπτογραφία

Τα συμμετρικά κρυπτοσυστήματα αναφέρονται και ως αλγόριθμοι μυστικού κλειδιού ή συμμετρικής κρυπτογραφίας. Στην περίπτωση των συμμετρικών αλγορίθμων, ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση όπως παρουσιάζεται στην παρακάτω εικόνα.



Σχήμα 1.1: Σχήμα κρυπογράφησης συμμετρικής κρυπτογραφίας

Η συμμετρική κρυπτογραφία κρυπτογραφεί το μήνυμα με το μυστικό κλειδί και εγγυάται την εμπιστευτικότητα (confidentiality) των δεδομένων αφού δεν μπορεί να διαβαστεί από μη εξουσιοδοτημένο χρήστη. Το μήνυμα που παράγεται, αποκρυπτογραφείται από τον παραλήπτη με τη βοήθεια του ίδιου κλειδιού, το οποίο πρέπει να μείνει μυστικό μεταξύ των δύο. Η ασφάλειά τους βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού, μέσω ενός ασφαλούς καναλιού επικοινωνίας ή μέσω της φυσικής παρουσίας των προσώπων. Αυτό το χαρακτηριστικό, καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων χρηστών και αποτελεί μειονέκτημα της χρήσης της συμμετρικής κρυπτογραφίας. Από την άλλη πλευρά, καθώς όλοι οι κρυπτογραφικοί αλγόριθμοι είναι σωστοί και το επίπεδό ασφάλειάς τους έγκυται στο μαθηματικό πρόβλημα που περιέχουν το μόνο μυστικό παραμένει το ίδιο το κλειδί. κατάλληλη για ευρεία χρήση.

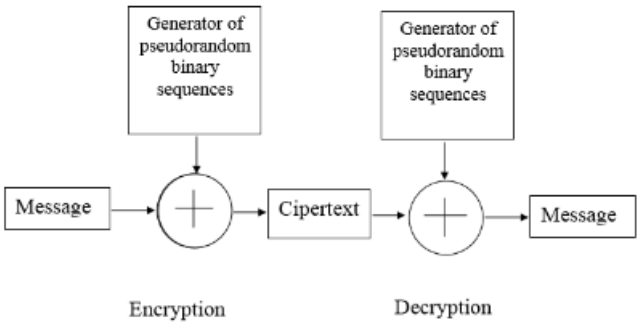
Τα συμμετρικά συστήματα κρυπτογράφησης ταξινομούνται με βάση τον τρόπο με τον οποίο επεξεργάζεται ο αλγόριθμος το αρχικό κείμενο σε:

- Αλγόριθμοι Ροής (stream ciphers)
- Αλγόριθμοι Τμημάτων (block ciphers)

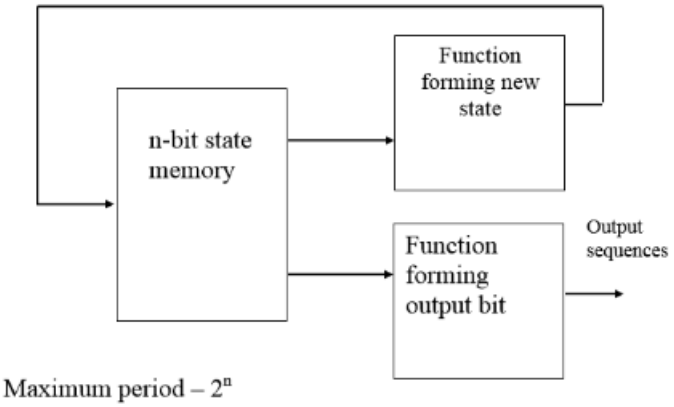
1.2.1 Αλγόριθμοι Ροής

Οι αλγόριθμοι ροής (stream ciphers) ανήκουν στην τοπολογία των συμμετρικών κρυπτογραφικών αλγορίθμων. Κύριο χαρακτηριστικό τους είναι η κρυπτογράφηση μεμονωμένων δυαδικών ψηφίων από μια γεννήτρια ψευδοτυχαιών αριθμών ή ψηφίων που βρίσκονται σε μνήμη, υλοποιώντας μεταξύ τους τη λογική πράξη XOR. Θεωρούνται αλγόριθμοι που υλοποιούνται σε ψηφιακούς καταχωρητές και σε πραγματικό χρόνο. Η αρχιτεκτονική της κρυπτογράφησης ροής παρουσιάζεται στο σχήμα 1.2.

Η ασφάλεια των κρυπτογραφικών αλγορίθμων ροής έγκειται στην ασφάλεια που έχει η γεννήτρια των ψευδοτυχαιών αριθμών. Βασικά χαρακτηριστικά των γεννητριών ψευδοτυχαίων αριθμών είναι το μέγεθος της τάξης του πολυωνύμου που υλοποιεί πρώτο πολυώνυμο τάξης n-bit (1024 και 2048 bits) και παρέχει μέγιστη περίοδο 2^n (σχήμα 1.3). Η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποείται ανά ένα bit και ως κλειδί χρησιμοποιείται μια τυχαία κατάσταση της γεννήτριας ψευδοτυχαίων αριθμών η οποία συγχρονίζεται με τον αποστολέα και τον παραλήπτη.



Σχήμα 1.2: Σχήμα κρυπτογράφησης αλγορίθμου ροής.



Σχήμα 1.3: Σχήμα του γεννήτορα ψευδοτυχαίων δυαδικών ακολουθιών του αλγορίθμου ροής

One-time pad (OTP)

Οι αλγόριθμοι ροής βασίζονται στις θεωρητικές ιδιότητες ενός *one-time pad*. Το 1917, ο Vernam "πατένταρε" ένα cipher το οποίο μας δίνει απόλυτη μυστικότητα. Καθώς δεν υπήρχε ο ορισμός της απόλυτης μυστικότητας τότε, δεν είμασταν σε θέση να ξέρουμε αν όντως ισχύει αυτό, παρά μόνο

25 χρόνια αργότερα ο Shannon έδωσε αυτό τον ορισμό και μας έδειξε ότι τα OTP είναι όντως ασφαλή. One-time pads (ή αλλιώς Vernam-κρυπτοσυστήματα),λοιπόν, είναι τα κρυπτοσυστήματα που χρησιμοποιούν μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη. Η ακολουθία των bits είναι του ίδιου μήκους με το μη-κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας πράξης XOR για τη παραγωγή του κρυπτογραφήματος-κρυπτοκειμένου.

Ορισμός 1.3. *(OTPs) Με $a \bigoplus b = a_1 \bigoplus b_1, \ldots, a_l \bigoplus b_l$ όπου $a = a_1, \ldots, a_l$ και $b = b_1, \ldots, b_l$ και $\bigoplus$ να είναι η πράξη XOR, το σύστημα κρυπτογράφησης OTP ορίζεται ως:*

- *Φιξάρουμε έναν ακέραιο $l > 0$. Τότε ο χώρος M των μηνυμάτων, ο χώρος K των κλειδιών και ο χώρος C των κρυπτοκειμένων είναι όλοι ίσοι με $\{0,1\}^l$, δηλαδή το σύνολο όλων των δυαδικών ακολουθιών μήκους l.*
- *Ο αλγόριθμος παραγωγής κλειδιών (Gen) διαλέγει μια ακολουθία από το $K = \{0,1\}^l$ σύμφωνα με τη κανονική κατανομή, δηλαδή κάθε ακολουθία από τις 2^l ακολουθίες στο χώρο K επιλέγεται ως το κλειδί με πιθανότητα ακριβώς 2^{-l}.*
- *Ο αλγόριθμος κρυπτογράφησης (Enc), δοθέντος ενός κλειδιού $k \in \{0,1\}^l$ και ενός μηνύματος $m \in \{0,1\}^l$, έχει ως έξοδο $c = k \bigoplus m$.*
- *Ο αλγόριθμος αποκρυπτογράφησης (Dec), δοθέντος ενός κλειδιού $k \in \{0,1\}^l$ και ενός κρυπτοκειμένου $c \in \{0,1\}^l$, έχει ως έξοδο $m := k \bigoplus c$.*

Θεώρημα 1.4. *Έστω (Gen, Enc, Dec) ένα απόλυτα ασφαλές σχήμα κρυπτογράφησης σε ένα χώρο μηνυμάτων M και K ο χώρος των κλειδιών που καθορίζεται από το Gen. Τότε*

$$|K| \geq |M|$$

Θεώρημα 1.5. *(Shannon) Έστω (Gen, Enc, Dec) να είναι ένα σχήμα κρυπτογράφησης σε ένα χώρο μηνυμάτων M για το οποίο ισχύει $|M| = |K| = |C|$. Αυτό το σχήμα είναι απόλυτα ασφαλές αvv*

- *Κάθε κλειδί $k \in K$ επιλέγεται με ίση πιθανότητα $1/|K|$ από τον αλγόριθμο Gen.*
- *Για κάθε $m \in M$ και κάθε $c \in C$, υπάρχει ένα μοναδικό κλειδί $k \in K$ τέτοιο ώστε $Enc_k(m)$ να εξάγει c [16].*

Το θεώρημα του Shannon είναι αρκετά εύχρηστο όταν θέλουμε να αποδείξουμε αν ένα σχήμα είναι απόλυτα ασφαλές ή όχι. Ισχύει μόνο όμως, όταν $|M| = |K| = |C|$, αλλιώς δεν μπορούμε να το εφαρμόσουμε.

Επειδή η ακολουθία των bits είναι τελείως τυχαία και είναι του ίδιου μήκους με το αρχικό κείμενο,η εύρεση του κειμένου είναι αδύνατη ακόμα και με τη διάθεση τεράστιας υπολογιστικής ισχύος ή άπειρου χρόνου. Επίσης κάθε κλειδί επιλέγεται σύμφωνα με τη κανονική κατανομή οπότε κανένα κλειδί δεν έχει περισσότερη πιθανότητα να επιλεγεί έναντι κάποιου άλλου. Οπότε το c, δεν αποκαλύπτει τίποτα όσον αφορά το αρχικό μήνυμα m που κρυπτογραφήθηκε επειδή πάλι υπάρχει ίδια πιθανότητα για κάθε m. Ένα τέτοιο κρυπτοσύστημα εφόσον εφαρμοστεί επιτυχημένα, προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για τη διασφάλιση διπλωματικών καναλιών [16].

Θεώρημα 1.6. *Το OTP είναι ένα απόλυτα ασφαλές σύστημα κρυπτογράφησης.*

Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με το μήνυμα, εισάγει σημαντικό πρόβλημα στη διαχείριση του κλειδιού για αυτό και δεν μπορεί να εφαρμοστεί στη πράξη για μεγάλο όγκο μηνυμάτων. Οι μοντέρνοι κρυπτογραφικοί αλγόριθμοι ροής χρησιμοποιούν γεννήτριες κλειδοροών, που παράγουν ψευδοτυχαίες ακολουθίες με πολύ μεγάλες περιόδους, για παράδειγμα 264 bits ή και περισσότερα. Θεωρούνται σχετικά απλοί και εύκολα υλοποιήσιμοι,με πιο γνωστούς τους RC4 και SEAL. Τέλος, είναι ασφαλείς μόνο εναντίον επιθέσεων που στοχεύουν καθαρά στο κρυπτοκείμενο (ciphertext-only attacks).

1.2.2 Αλγόριθμοι Τμημάτων

Οι αλγόριθμοι τμήματος (block ciphers) συμμετρικού κλειδιού είναι οι πιο διάσημοι και οι πιο σημαντικοί με αποτέλεσμα να χρησιμοποιούνται ευρέως σε πολλά κρυπτογραφικά συστήματα. Από μόνοι τους, προσφέρουν εμπιστευτικότητα (confidentiality), αλλά λόγω της προσαρμοστικότητάς τους, συχνά χρησιμοποιούνται και για την γεννήτρια παραγωγής ψευδοτυχαίων ακολουθιών, σε αλγορίθμους ροής, σε συναρτήσεις κατακερματισμού (hash functions) και σε κώδικες αυθεντικοποίησης μηνυμάτων, MACs (Message Authentication Codes). Χρησιμοποιούνται επίσης ως βασικό στοιχείο σε τεχνικές αυθεντικοποίησης μηνύματος, σε μηχανισμούς ακεραιότητας μηνύματος, σε πρωτόκολλα αυθεντικοποίησης οντότητας και σε ψηφιακές υπογραφές.

Ένας αλγόριθμος τμήματος είναι ένα τμήμα (block), αρχικού κειμένου μεγέθους n-bits, που αντιμετωπίζεται σαν ένα σύνολο και χρησιμοποιείται για να παράγει ένα τμήμα κρυπτογραφήματος ίσου μήκους.Οι δύο σημαντικότερες παράμετροι των αλγορίθμων τμήματος, είναι το μήκος του block και το μήκος του κλειδιού που είναι ίσα. Τα περισσότερα κρυπτοσυστήματα αυτού του είδους έχουν μήκος block, $b = 64$ ή 128 bits και μήκος κλειδιού, $k = 64$ ή 128 ή 192 ή 256,512 ή 1024 bits. Οι αλγόριθμοι τμήματος μπορούν να θεωρηθούν και ως μια αντιμετάθεση η οποία εξαρτάται από το κλειδί (key dependent permutation), καθώς χρησιμοποιούν ένα μικρό σύνολο από αντιμεταθέσεις, εξαρτώμενες από τον αριθμό των πιθανών κλειδιών.

Στην πιο απλή υλοποίηση ενός αλγορίθμου τμήματος, το αρχικό κείμενο (plaintext) διαιρείται σε δύο blocks και στη συνέχεια τροφοδοτείται στο σύστημα για να παραχθούν τα κρυπτογραφημένα blocks (cipher text). Οι πιο δημοφιλείς block ciphers είναι οι DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish, Twofish, κ.α.

Το 1949, ο Shannon, εισήγαγε τις έννοιες σύγχυση (Confusion) και διάχυση (Diffusion).

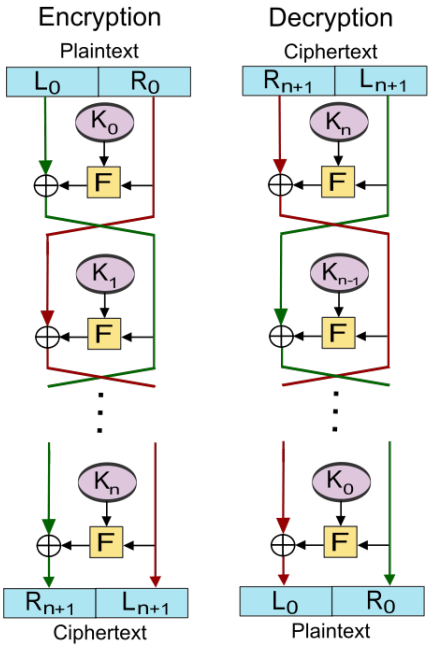
Ορισμός 1.7. *(Σύγχυση) Η σύγχυση ορίζεται ως η λειτουργία η οποία κάνει τη σχέση μεταξύ κλειδιού και κρυπτοκειμένου όσο το δυνατόν πολυπλοκότερη*

Ορισμός 1.8. *(Διάχυση) Η διάχυση ορίζεται ως η λειτουργία η οποία διαχέει την επιρροή των bits του απλού κειμένου έτσι ώστε τα bits του κρυπτοκειμένου να εξαρτώνται από ολόκληρο το κείμενο.*

Η σύγχυση συνήθως δίνεται από τη χρήση μιας αντικατάστασης η οποία ονομάζεται S-Box και η διάχυση δίνεται από τη χρήση μιας αντιμετάθεσης. Ένα δίκτυο αντικατάστασης - αντιμετάθεσης (substitution - permutation network) είναι ένα επαναλαμβανόμενο κρυπτοσύστημα, το οποίο αποτελείται από ένα σύνολο γύρων που ο κάθε γύρος με τη σειρά του αποτελείται και αυτός από αντικαταστάσεις και αντιμεταθέσεις. Η αντικατάσταση, η οποία καλείται και S-Box, αντικαθιστά έναν αριθμό από bits, έστω m, με ένα άλλο σύνολο από m-bits ενώ η αντιμετάθεση, αντιμεταθέτει τα bits. Η λογική του σχεδιασμού των δικτύων αντικατάστασης-αντιμετάθεσης είναι ότι, οι αντικαταστάσεις και οι αντιμεταθέσεις χρησιμοποιούνται με τέτοιο τρόπο ώστε το τελικό κρυπτοσύστημα, μετά από ένα καθορισμένο αριθμό γύρων, είναι πιο ασφαλές από ότι σε κάθε γύρο χωριστά.

Δίκτυα Feistel

Η μεγαλύτερη κατηγορία αλγορίθμων τμήματος βασίζεται στην αρχιτεκτονική δικτύου Feistel, που περιγράφηκε πρώτα από τον H. Feistel της IBM το 1973.



Σχήμα 1.4: Αρχιτεκτονική δικτύου Feistel

Οι είσοδοι σε ένα δίκτυο Feistel είναι ένα τμήμα αρχικού κειμένου (plaintext) και ένα κλειδί K. Το τμήμα αρχικού κειμένου διαιρείται σε δύο ίσα τμήματα, L_0 και R_0. Τα δύο τμήματα του αρχικού κειμένου ακολουθούν n επαναληπτικά βήματα επεξεργασίας και στη συνέχεια συνδυάζονται για να παράγουν το τμήμα κρυπτογραφήματος (ciphertext). Κάθε κύκλος i λαμβάνει ως εισόδους τα L_{i-1} και R_{i-1} που παράγονται από τον προηγούμενο κύκλο, καθώς επίσης και ένα υποκλειδί, K_i (subkey) που παράγεται από το αρχικό κλειδί K μέσω ενός αλγορίθμου παραγωγής υποκλειδιών. Γενικά, τα υποκλειδιά K_i είναι διαφορετικά και από το K αλλά και μεταξύ τους, παρόλο που παράγονται από το αρχικό κλειδί K.

Ακολουθεί μια οπτικοποίηση των επαναληπτικών βημάτων που αναφέραμε παραπάνω στο ακόλουθο σχήμα.

Στα δεδομένα που βρίσκονται στην αριστερή πλευρά πραγματοποιείται μία αντικατάσταση, η οποία επιτυγχάνεται με την εφαρμογή μιας συνάρτησης F (round function) στα δεδομένα της δεξιάς πλευράς και έπειτα συνδυάζοντας την έξοδο της συνάρτησης F με τα δεδομένα της αριστερής πλευράς, εφαρμόζουμε τον τελεστή XOR. Η συνάρτηση F έχει την ίδια γενική δομή για κάθε κύκλο, αλλά παραμετροποιείται από το υποκλειδί K_F του εκάστοτε κύκλου. Μετά από αυτή την αντικατάσταση, εκτελείται μία αντιμετάθεση των πλευρών των δεδομένων.

Το κύριο χαρακτηριστικό του δικτύου Feistel είναι ότι, η συνάρτηση F μπορεί να είναι οποιαδήποτε συνάρτηση ακόμα και αν δεν είναι αντιστρέψιμη, σε αντίθεση με το κάθε γύρο ο οποίος είναι αντιστρέψιμος, ανεξαρτήτως της F.

Θα αναφέρουμε μερικές παραμέτρους και τεχνικά χαρακτηριστικά για την καλύτερη και πιο ακριβέστερη υλοποίηση ενός δικτύου Feistel:

- *Μέγεθος των τμημάτων (block size)*: Όσο μεγαλύτερο είναι το μέγεθος των τμημάτων,

τόσο αυξάνεται ο βαθμός ασφάλειας και μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Τυπικό μέγεθος τμήματος είναι τα 64-bits και αποτελεί το συνηθέστερο στο σχεδιασμό των τμημάτων κρυπτογράφησης.

- *Μέγεθος κλειδιού (key size)*: Όσο μεγαλύτερο είναι το μέγεθος κλειδιού, τόσο εξασφαλίζεται υψηλότερος βαθμός ασφάλειας, αλλά μειώνεται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης. Τυπικό μέγεθος κλειδιού στους σύγχρονους αλγορίθμους είναι 128-bits.

- *Αριθμός κύκλων (number of rounds)*: Βασικό χαρακτηριστικό της δομής Feistel αποτελεί το γεγονός ότι κάθε κύκλος προσφέρει ανεπαρκή ασφάλεια, αλλά η διαδοχή των επαναληπτικών βημάτων προσφέρει αυξημένη ασφάλεια. Τυπικό μέγεθος για τον αριθμό των κύκλων είναι 16 κύκλοι.

- *Αλγόριθμος παραγωγής δευτερευόντων κλειδιών (subkey generation algorithm)*: Μεγαλύτερη πολυπλοκότητα στον αλγόριθμο πρέπει να οδηγεί σε μεγαλύτερη δυσκολία στην κρυπτανάλυση.

- *Συνάρτηση κύκλου (round cycle)*: Μεγαλύτερη πολυπλοκότητα, σε γενικές γραμμές, σημαίνει μεγαλύτερη αντοχή σε κρυπταναλυτικές επιθέσεις.

Εν τέλει, αν θέλαμε να συγκρίνουμε τους αλγόριθμους ροής και τους αλγορίθμους τμήματος θα παρατηρούσαμε ότι με μια προσεκτικά σχεδιασμένη γεννήτρια ψευδοτυχαίων αριθμών, ένας αλγόριθμος ροής μπορεί να είναι το ίδιο ασφαλής όσο και ένας αλγόριθμος τμήματος ίδιου μήκους κλειδιού. Ένα πλεονέκτημα των αλγόριθμων ροής σε σχέση με τους αλγορίθμους τμήματος είναι ότι είναι πιο γρήγοροι. Καταλήγοντας, θα λέγαμε ότι για εφαρμογές που χειρίζονται ροές δεδομένων σε πραγματικό χρόνο, όπως για παράδειγμα δεδομένα τα οποία διακινούνται σε ένα κανάλι επικοινωνίας κινητής τηλεφωνίας ή δεδομένα τα οποία μεταφέρονται από έναν φυλλομετρητή (Web browser), ένας αλγόριθμος ροής είναι η προτιμότερη επιλογή, ενώ για εφαρμογές οι οποίες διαχειρίζονται μεγάλο όγκο δεδομένων,όπως οι εφαρμογές αποθήκευσης και μεταφοράς αρχείων, εφαρμογές email και εφαρμογές διαχείρισης βάσεων δεδομένων, οι αλγόριθμοι τμήματος είναι καταλληλότεροι.

Μειονεκτήματα συμμετρικών συστημάτων κρυπτογράφησης

Όλα τα κλασσικά συμμετρικά συστήματα κρυπτογράφησης εμφανίζουν δύο σοβαρά μειονεκτήματα.

- Ο παραλήπτης πρέπει να διαθέτει το μυστικό κλειδί για την αποκρυπτογράφηση των μηνυμάτων που λαμβάνει.

- Η αυθεντικότητα του αποστολέα του μηνύματος είναι αμφίβολη.

1.3 Ασύμμετρη Κρυπτογραφία

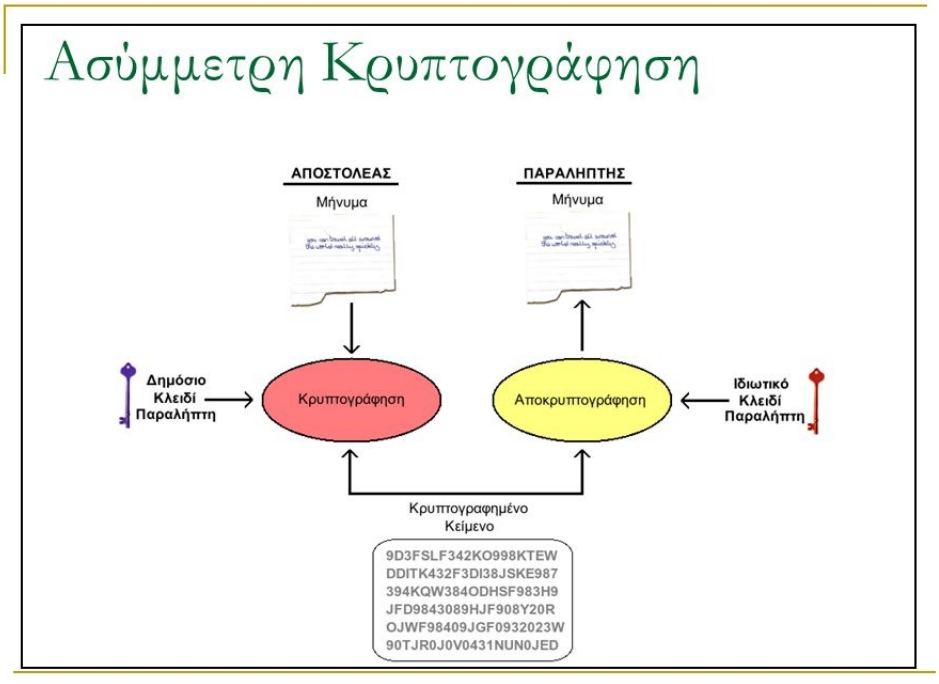
Η βασική ιδέα της ασύμμετρης κρυπτογραφίας ή αλλιώς της κρυπτογράφησης με δημόσιο κλειδί είναι, ότι, αυτός που θέλει να λάβει μηνύματα γνωστοποιεί ορισμένους αριθμούς (το δημόσιο κλειδί) σε όλους εκείνους που θα μπορούσαν να του τα στείλουν. Οι αριθμοί αυτοί πληροφορούν τους δυνητικούς αποστολείς για τον τρόπο που πρέπει να κρυπτογραφήσουν τα μηνύματά τους. Ο παραλήπτης γνωρίζει ένα μυστικό αριθμό (ιδιωτικό κλειδί) που του επιτρέπει να τα αποκρυπτογραφήσει. Το σύστημα κρυπτογράφησης με δημόσιο κλειδί χρησιμοποιεί τόσο την αντιμετάθεση όσο και την αντικατάσταση.

Οι Whitefield Diffie και Martin Hellman το 1976 περιέγραψαν τα μαθηματικά που απαιτούνται για το σύστημα κρυπτογράφησης με δημόσιο κλειδί.[11]

Το κυριότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι για την επικοινωνία δεν χρειάζεται το ίδιο κοινό κλειδί. Ασφαλώς και παραμονεύει η αδυναμία της παραβίασης και στην ασύμμετρη κρυπτογράφηση η οποία μπορεί να οφείλεται

- στην δυσκολία του υποκείμενου μαθηματικού προβλήματος.
- στην πιθανότητα επίθεσης μεσολαβητή (man in the middle attack).

Οι αντίστοιχοι αλγόριθμοι είναι απαιτητικοί σε επεξεργαστική ισχύ συγκρίνοντάς τους με τους συμμετρικούς αλγόριθμους.



Σχήμα 1.5: Σχήμα κρυπτογράφησης ασύμμετρης κρυπτογραφίας

1.3.1 Πρωτόκολλο Diffie-Hellmann

Στην κλασική τους εργασία $[9]$, η οποία έθεσε τα θεμέλια της κρυπτογραφίας δημοσίου κλειδιού, οι Diffie και Hellman, ασχολήθηκαν με το πρόβλημα της ανταλλαγής κλειδιού. Συγκεκριμένα, δύο οντότητες, ο αποστολέας η "Αλίκη" και ο παραλήπτης ο "Bob", θέλουν να συμφωνήσουν σε ένα κοινό κλειδί, ώστε να επικοινωνήσουν χρησιμοποιώντας κρυπτογραφία (πχ. με ένα συμμετρικό κρυπτοσύστημα σαν το DES). Ο μόνος τρόπος επικοινωνίας τους είναι μέσω ενός δημοσίου καναλιού, στο οποίο μπορεί να υπάρχουν ωτοακουστές, οπότε δεν μπορούν απλά να συμφωνήσουν στο κλειδί χωρίς να το μάθει οποιοσδήποτε έχει πρόσβαση στο κανάλι επικοινωνίας. Το πρόβλημα λύθηκε χρησιμοποιώντας το παρακάτω απλό πρωτόκολλο, το οποίο βασίζεται στο πρόβλημα του Διακριτού Λογαρίθμου.

Βήμα 1: Αρχικά δημοσιεύεται ένας πρώτος αριθμός p, κατάλληλα επιλεγμένος (ώστε να καθίσταται «αδύνατη» η επίλυση του αντίστοιχου DLP) και ένας γεννήτορας g του $\mathbb{Z}_p^*$.

Βήμα 2: Η Αλίκη επιλέγει έναν τυχαίο ακέραιο αριθμό $a \in \mathbb{Z}_p^*$ που τον γνωρίζει μόνο αυτή, και στέλνει στον Bob το μήνυμα:

$$y_a = g^a (mod p)$$

Βήμα 3: Ο Bob επιλέγει έναν τυχαίο ακέραιο αριθμό $b \in \mathbb{Z}_p^*$ που τον γνωρίζει μόνο αυτός και στέλνει στην Αλίκη το μήνυμα:

$$y_b = g^b (mod p)$$

Βήμα 4: Ο Bob λαμβάνει το $g^a (mod p)$ και υπολογίζει το

$$K = (g^a)^b (mod p)$$

Βήμα 5: Η Αλίκη λαμβάνει το $g^b (mod p)$ και υπολογίζει το

$$K = (g^b)^a (mod p)$$

Βήμα 6: Η Αλίκη και ο Bob συμφώνησαν στο κοινό κλειδί K

Η ασφάλεια του παραπάνω πρωτοκόλλου βασίζεται στα εξής προβλήματα:

- **Υπολογιστικό Πρόβλημα των Diffie-Hellman (Computational Diffie Hellman Problem (CDH))**

CDH	
Δεδομένα	Ένας πρώτος αριθμός p , ένας γεννήτορας g του $\mathbb{Z}_p^*$ και τα στοιχεία $g^a (mod p), g^b (mod p) \in \mathbb{Z}_p^*$
Ζητούμενο	Να βρεθεί το $g^{ab} (mod p)$

- **Πρόβλημα Απόφασης των Diffie-Hellman (Decisional Diffie Hellman Problem (DDH))**

DDH	
Δεδομένα	Ένας πρώτος αριθμός p, ένας γεννήτορας g του $\mathbb{Z}_p^*$ και τα στοιχεία $g^a(modp), g^b(modp), g^c(modp) \in \mathbb{Z}_p^*$.
Ζητούμενο	Αν ισχύει $$c = ab$$

Τα παραπάνω προβλήματα, όπως είναι φανερό, σχετίζονται με το DLP, κανένα δεν είναι πιο δύσκολο από το DLP και ισχύει το παρακάτω θεώρημα:

Θεώρημα 1.9.

$$DDHP \leq CDHP \leq DLP$$

Παράδειγμα 1.3.1. Η Αλίκη και ο Bob θέλουν να ανταλλάξουν ένα κλειδί μέσω του πρωτοκόλλου Diffie-Hellmann. Θεωρούμε λοιπόν τις παραμέτρους $p = 23$ και $g = 5$. Διαλέγει ένα τυχαίο ακέραιο $a = 6 \in \mathbb{Z}_{23}^*$ η Αλίκη και υπολογίζει το y_A και το στέλνει στον Bob

$$y_A = g^a modp = 5^6 mod23 = 8$$

Το στέλνει στον Bob και αυτός με τη σειρά του διαλέγει έναν ακέραιο $b = 15 \in \mathbb{Z}_{23}^*$ και υπολογίζει το y_B και το στέλνει στην Αλίκη,

$$y_B = g^b(modp) = 5^{15} mod23 = 19$$

Λαμβάνουν και οι δύο τα y_A, y_B αντίστοιχα και υπολογίζει ο καθένας το κοινό κλειδί K,

$$\text{Η Αλίκη} : K = (g^b)^a(modp) = 19^6 mod23 = 2$$
$$\text{Ο Bob} : K = (g^a)^b(modp) = 8^{15} mod23 = 2 \text{ Bob}$$

Το κοινό δημόσιο κλειδί, τελικά, στο οποίο συμφώνησαν είναι το $K = 2$.

Πέρα από το πρόβλημα των Diffie-Hellman στο $\mathbb{Z}_p^*$, αναφέρουμε στη συνέχεια και τη παραλλαγή των αντίστοιχων προβλημάτων στις ελλειπτικές καμπύλες.

Πρωτόκολλο Diffie-Hellman στις ελλειπτικές καμπύλες

Στις αρχές του 1980, οι Miller και Koblitz πρότειναν να αντικαταστήσουν την ομάδα $(\mathbb{Z}/p\mathbb{Z})^*$ στο πρωτόκολλο Diffie-Helmann, με μια ομάδα από ρητά σημεία μιας ελλειπτικής καμπύλης σχεδόν πρώτης τάξης σε ένα πεπερασμένο σώμα. Παρακάτω ακολουθούν τα βήματα για τη παραλλαγή του πρωτοκόλλου Diffie-Helmann για ελλειπτικές καμπύλες (DF-ECC).

Βήμα 1: Δημοσιοποιείται ένα πεπερασμένο σώμα $\mathbb{F}_p$ με $log_2 p \simeq 256$, μια ελλειπτική καμπύλη $E/\mathbb{F}_p$, τέτοια ώστε $\#E(\mathbb{F}_p)$ να είναι πρώτος και ένας γεννήτορας P, ή αλλιώς μια ρητή βάση σημείων P για την $E(\mathbb{F}_p)$.

Βήμα 2: Η Αλίκη και ο Bob διαλέγουν τυχαίους ακέραιους k_A, k_B με $0 < k_A < \#E(\mathbb{F}_p)$ και $0 < k_B < \#E(\mathbb{F}_p)$ ως τα ιδιωτικά κλειδιά τους.

Βήμα 3: Η Αλίκη υπολογίζει το $A = k_A \cdot P$ και ο Bob το $B = k_B \cdot P$ και ανταλλάσουν τις τιμές αυτές μέσω ενός καναλιού.

Βήμα 4: Στη συνέχεια, αφού λάβει ο καθένας τις αντίστοιχες τιμές του άλλου, η Αλίκη υπολογίζει το $S = k_A \cdot B$ και ο Bob το $S = k_B \cdot A$ και το S είναι εν τέλει το δημόσιο κλειδί που θα μοιράζονται οι δύο τους και μόνο αυτοί γνωρίζουν.

Η δυσκολία της συγκεκριμένης διαμοίρασης κλειδιού στηρίζεται στη δυσκολία ενός ωτοακουστή, όπως η Eve να υπολογίσει το S δοθέντων των A, B (ECDLC).

- **Υπολογιστικό Diffie-Hellman στις ελλειπτικές καμπύλες (ECDHP)**

ECDHP	
Δεδομένα	Μια ελλειπτική καμπύλη E ορισμένη στο $\mathbb{F}_q$ ένα σημείο $P \in (\mathbb{F}_q)$ (ως βάση του διακριτού λογαρίθμου) και δύο άλλα σημεία $G, Q \in E(\mathbb{F}_q)$ πολλαπλάσια του P ,δηλαδή $G = aP$ και $G = bP$ με $a, b \in \mathbb{Z}$.
Ζητούμενο	Να βρεθεί το σημείο R, τέτοιο ώστε $$R = abP$$

- **Diffie-Hellman απόφασης στις ελλειπτικές καμπύλες (ECDDH)**

ECDDH	
Δεδομένα	Μια ελλειπτική καμπύλη E ορισμένη στο $\mathbb{F}_q$ ένα σημείο $PE(\mathbb{F}_q)$ (ως βάση του διακριτού λογαρίθμου) και τρία άλλα σημεία $G, Q, R \in E(\mathbb{F}_q)$.
Ζητούμενο	Αποφάσισε αν υπάρχουν $a, b \in \mathbb{Z}$ τέτοια ώστε $aP = Q,\ bP = Q,\ G = abP$

Παράδειγμα 1.3.2. Έστω E μια ελλειπτική καμπύλη στο $\mathbb{F}_p$, όπου θεωρούμε $p = 3023$ και $a = 1, b = 2547$, άρα $(4a^3 + 27b^2) mod p = 20270$. Έχουμε επίσης $\#E = 3083$ ο οποίος είναι πρώτος και τέλος ο γεννήτορας $P = (2237, 2480)$. Αφού ορίσαμε τις παραμέτρους που θα χρησιμοποιήσουμε ακολουθεί μια εφαρμογή του πρωτοκόλλου Diffie-Hellmann πάνω σε ελλειπτικές καμπύλες.

Η Αλίκη θεωρεί ένα τυχαίο $k_A = 2313$ και υπολογίζει το A και το στέλνει στο Bob.

$$A = k_A \cdot P = 2313 \cdot (2237, 2480) = (934, 29)$$

Ο Bob διαλέγει με τη σειρά του ένα $k_B = 1236$ και υπολογίζει το

$$B = k_B \cdot P = 1236 \cdot (2237, 2480) = (1713, 1709)$$

Ύστερα και οι δύο τους υπολογίζουν το κοινό δημόσιο κλειδί, S, που θα χρησιμοποιήσουν για την επικοινωνία τους:

$$(\text{Αλίκη}) : S = k_A \cdot B = 2313 \cdot (1713, 1709) = (2537, 1632) = S$$
$$(\text{Bob} : S = k_B \cdot A = 1236 \cdot (934, 29) = (2537, 1632) = S$$

Ένα κρυπτοσύστημα δημοσίου κλειδιού μπορούμε να το κατασκευάσουμε ακολουθώντας γενικά τα παρακάτω βήματα:

- Διαλέγουμε ένα δύσκολο πρόβλημα Π. Το Π θα πρέπει να είναι υπολογιστικά απρόσιτο. Το Π λέγεται υποκείμενο πρόβλημα.
- Βρίσκουμε ένα εύκολο υπο-πρόβλημα Π_{easy} του Π. Το Π_{easy} θα πρέπει να χρειάζεται μικρό πολυωνυμικό χρόνο για την επίλυσή του.
- "Ανακατεύουμε" το Π_{easy} με τέτοιο τρόπο ώστε το προκύπτον πρόβλημα $\Pi_{shuffle}$ να μοιάζει με το γενικό πρόβλημα Π.
- Δημοσιεύουμε το $\Pi_{shuffle}$ και τη μέθοδο που χρησιμοποιήσαμε για τη κρυπτογράφησή μας. Η μέθοδος ανάκτησης του Π_{easy} είναι η μυστική "καταπακτή". Έτσι ο νόμιμος αποδέκτης θα πρέπει να λύσει το Π_{easy}, ενώ αντίστοιχα ο κρυπταναλυτής βρίσκεται ενάντια στο γενικό και θεωρητικά δύσκολο ως προς την επίλυση πρόβλημα, Π $[16]$.

Ο παρακάτω κατάλογος απαριθμεί μερικά θεμελιώδη αριθμοθεωρητικά προβλήματα που έχουν αντισταθεί ως τώρα σε όλες τις προσπάθειες να ταξινομηθεί η πολυπλοκότητά τους και έχουν αποδειχτεί πολύ χρήσιμα στη κρυπτογραφία δημοσίου κλειδιού. Κανένα από αυτά τα προβλήματα δεν είναι γνωστό να είναι πλήρες για κάποια κλάση πολυπλοκότητας ή να έχει κάποιο ντετερμινιστικό πολυωνυμικό αλγόριθμο επίλυσης $[16]$.

- FACTOR(n): Να βρεθούν οι πρώτοι παράγοντες του n.
- FIND-PRIME$(> n)$: Να βρεθεί ένας πρώτος $> n$.
- SQUAREFREENESS(n): Να αποφασιστεί αν το τετράγωνο ενός πρώτου διαιρεί το n, ή αλλιώς να αποφασιστεί αν το n είναι γινόμενο διακριτών πρώτων.
- QUAD-RESIDUE(a, n): Να αποφασιστεί αν $x^2 \equiv a(mod n)$, για κάποιο x.
- SQUAREROOT(a, n): Να βρεθεί ένα x τέτοιο ώστε $x^2 \equiv a(mod n)$.
- DISCRETE-LOG(a, b, n): Να βρεθεί ένα x τέτοιο ώστε $a^x \equiv b mod(n)$.

1.3.2 RSA

Ένα σύστημα κρυπτογραφίας βασισμένο στις ιδέες των Diffie και Hellman, επινόησαν το 1977 στο MIT, οι Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman. Για να εμπορευτούν το σύστημα, οι παραπάνω ίδρυσαν το 1982 την εταιρεία RSA Data Security στη πόλη RedWood της Καλιφόρνιας.

Κρυπτογραφικός αλγόριθμος RSA

Τα μαθηματικά που βρίσκονται στη βάση του αλγορίθμου RSA αποτελούν εκμετάλλευση στοιχειωδών αρχών της θεωρίας αριθμών και ιδιαίτερα των πρώτων αριθμών.

Έστω τώρα ότι δύο άτομα, η Αλίκη και ο Bob θέλουν να επικοινωνήσουν με το σύστημα RSA. Αρχικά η Αλίκη, επιλέγει δύο (μεγάλους) διαφορετικούς πρώτους αριθμούς p, q και υπολογίζει το $N = p \cdot q$. Διαλέγει επίσης έναν ακέραιο e τέτοιον ώστε:

$$(e, \phi(N)) = 1$$

και υπολογίζει έναν d ώστε:

$$e \cdot d = 1 \ (mod \phi(N))$$

χρησιμοποιώντας τον Επεκτεταμένο Ευκλείδιο Αλγόριθμο.

Η Αλίκη δημοσιοποιεί τα (e, N) τα οποία είναι το δημόσιο κλειδί της και κρατά ως ιδιωτικό κλειδί τα (d, p, q).

Ο Bob τώρα, ο οποίος θέλει να επικοινωνήσει με την Αλίκη, λαμβάνει το δημόσιο κλειδί της και κρυπτογραφεί το μήνυμα x ως εξής:

$$E(x) \equiv x^e mod N \quad = y$$

και το στέλνει στην Αλίκη.

Η Αλίκη λαμβάνει με τη σειρά της το κρυπτογραφημένο μήνυμα y και το αποκρυπτογραφεί με την ακόλουθη σχέση:

$$D(y) \equiv y^d mod N \quad = x$$

Παρατηρήσεις:

1. Αφού το N είναι το γινόμενο των δύο πρώτων αριθμών p, q θα ισχύει: $\phi(N) = (p-1)(q-1)$. Έτσι, αν κάποιος γνωρίζει τα p και q μπορεί εύκολα να υπολογίσει το $\phi(N)$ και επομένως και το d.

2. Μια καλή επιλογή για τον (δημόσιο) εκθέτη e είναι κάποιος πρώτος αριθμός $>$max(p, q).

Το ευάλωτο σημείο για υποκλοπή είναι ο προσδιορισμός του N. Στη πράξη οι εμπλεκόμενοι (επιλεγόμενοι) πρώτοι έχουν τουλάχιστον $50 - 60$ ψηφία και η εύρεση πρώτων παραγόντων είναι πολύ πιο δύσκολη υπόθεση από την εύρεση πρώτων αριθμών.

Η επιτυχία του αλγόριθμου οφείλεται στην εξαιρετικά μεγάλη δυσκολία που αντιμετωπίζουν ακόμη και οι πλέον πανίσχυροι υπολογιστές στην προσπάθεια ανάλυσης πολύ μεγάλων αριθμών.

Αυτό έχει ως αποτέλεσμα ο RSA να χρησιμοποιείται συχνά, απλά για την διαβίβαση του μυστικού κλειδιού ενός συμμετρικού αλγόριθμου.

Μέχρι στιγμής διαπιστώσαμε ότι ο παραλήπτης δεν χρειάζεται να γνωρίζει το μυστικό κλειδί της κρυπτογράφησης ώστε με μια "αντίστροφη" πορεία να αποκωδικοποιήσει το μήνυμα, που αποτελούσε το ένα από τα δύο μειονεκτήματα των κλασσικών συστημάτων κρυπτογράφησης. Στη συνέχεια δείχνουμε, πώς ο αλγόριθμος του RSA εξαλείφει και το δεύτερο μειονέκτημα, αυτό της ταυτότητας του αποστολέα.

Υπογραφή-Ταυτότητα αποστολέα

Έστω μια ομάδα ανθρώπων που χρησιμοποιούν τον αλγόριθμο RSA για την αποστολή μηνυμάτων μεταξύ τους. Το κάθε μέλος της ομάδας έχει κοινοποιήσει τον αριθμό M και το pq. Το πρόβλημα που υπάρχει είναι το εξής: *Όταν για παράδειγμα το μέλος Z_Π της ομάδας λάβει ένα μήνυμα πώς θα είναι σίγουρο ότι ο αποστολέας, είναι για παράδειγμα, το μέλος Z_A της ομάδας;*

Έχουμε λοιπόν:

$$Z_A \text{ με } M_A, N_A, p_A, q_A, (pq)_A$$

$$Z_\Pi \text{ με } M_\Pi, N_\Pi, p_\Pi, q_\Pi, (pq)_\Pi$$

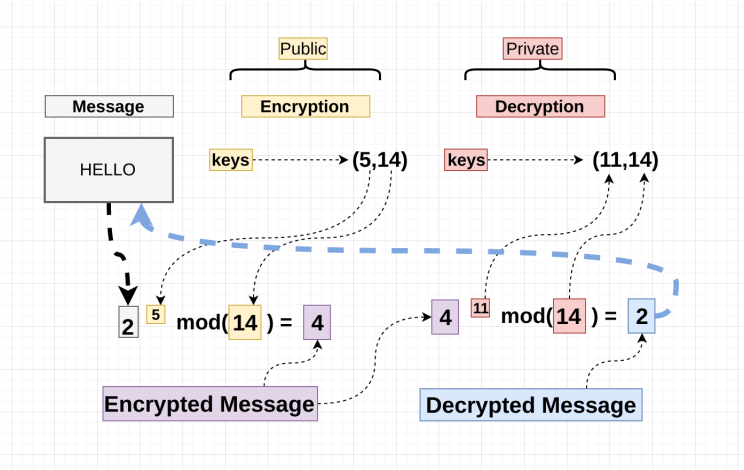
Ο Z_A, κατά τα γνωστά, στέλνει ένα μήνυμα στον Z_Π. Πρέπει όμως, στο τέλος του μηνύματος, να ακολουθήσει και μια υπογραφή, ας πούμε του Z_A, η οποία θα επιβεβαιώσει τον Z_Π ότι το μήνυμα προέρχεται από τον Z_A. Τα βήματα που πρέπει να κάνει ο Z_A και στη συνέχεια ο Z_Π είναι τα εξής:

Ο Z_A χωρίζει το όνομά του σε αριθμούς a και εκτελεί την ακόλουθη διαδικασία με καθένα αριθμό a.

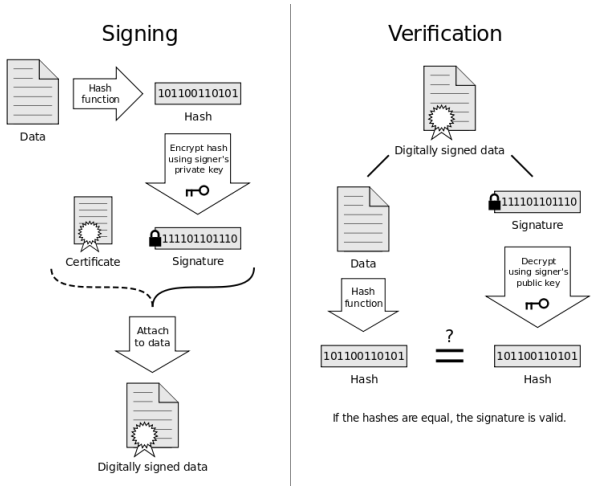
1. Υπολογίζει τον:
$$h_1 \equiv a^{N_A} mod (pq)_A \ \ (h_1 < (pq)_\Pi)$$
2. Κρυπτογραφεί τον h_1 με βάση τις οδηγίες του Z_Π υπολογίζοντας τον:
$$h_2 \equiv h_1^{M_\Pi} mod (pq)_\Pi$$
3. Όταν ο Z_Π λάβει το μήνυμα το αποκρυπτογραφεί υπολογίζοντας το:
$$S_1 = h_2^{N_\Pi} mod (pq)_\Pi$$
4. Υπολογίζει επίσης το:
$$S_2 = S_1^{M_A} mod (pq)_A$$

Το S_2 είναι ένας από τους αριθμούς a που συνθέτουν-αντιπροσωπεύουν το όνομα του Z_A. Η πιστοποίηση ότι η υπογραφή είναι του Z_A προσφέρεται από τη χρήση του μυστικού κλειδιού του εκθέτη στο πρώτο βήμα της κρυπτογράφησης.

Στα παρακάτω σχήματα περιγράφονται οι παραπάνω διαδικασίες:



Σχήμα 1.6: RSA αλγόριθμος



Σχήμα 1.7: RSA-υπογραφή

Το κρυπτογραφικό σύστημα δημόσιας κλείδας με τον κρυπτογραφικό αλγόριθμο RSA είναι στη πραγματικότητα ένας συνδυασμός του συστήματος κρυπτογράφησης συμμετρικών αλγορίθμων (DES,AES και άλλα) και του δικού τους συστήματος με δημόσιο κλειδί. Το σύστημα κρυπτογράφησης συμμετρικού αλγορίθμου χρησιμοποιείται για το κύριο όγκο του μηνύματος διότι είναι ταχύτερο από τον RSA, ενώ το τελευταίο παρέχει δημόσια πρόσβαση στην απόκρυψη και την επαλήθευση ταυτότητας.

Η εταιρεία RSA Data Security έχει καταστεί η σημαντικότερη εταιρία εμπορίας κρυπτογραφικών συστημάτων των ΗΠΑ και τα συστήματά της τα χρησιμοποιούν πολλές εταιρείες υπολογιστών, καθώς και η Ομοσπονδιακή Κυβέρνηση και οι Ένοπλες δυνάμεις. Ένα από τα προϊόντα της RSA Data Security, το Mailsafe, εξασφαλίζει ασφαλή επικοινωνία σε οργανισμούς, όπως η Boeing, το NATO και η Citibank.

Η εταιρεία έχει ξεκινήσει, από το 1990, έναν διαγωνισμό παραγοντοποίησης, με χρηματικά έπαθλα, για την παραγοντοποίηση σε γινόμενο πρώτων αριθμών οποιουδήποτε από 41 αριθμούς,

με αριθμό ψηφίων που κυμαίνεται από 100 μέχρι 500 ψηφία, συμβολίζοντας τους αριθμούς αυτούς ως RSA-100, μέχρι , RSA-500.

Η πρώτη πρόκληση στη μαθηματική κοινότητα έγινε από την ίδια την εταιρεία RSA το 1977, με την ανακοίνωση προς παραγοντοποίηση του αριθμού RSA-129. Η παραγοντοποίηση επιτεύχθει το 1994, από μια ομάδα παραγοντοποίησης με διευθύνοντες τους Derek Atkins και Arjen Lestra. Το 1991 "έσπασε" ο RSA-100 από τους Arjen Lestra και Mark Manesse. Το 1993 "έσπασε" ο RSA-110.

Ολοκληρώνουμε με την επισήμανση ότι η επιτυχία των μεθόδων κρυπτογράφησης με δημόσιο κλειδί, όπως αυτή της RSA, θορύβησε την κυβέρνηση των ΗΠΑ, αλλά και άλλων, και φυσικά δεν έχουν παραμείνει αδρανείς (Copstone Project). Είναι εύκολα κατανοητό, ότι δεν μπορεί να γνωρίζει κάποιος το βάθος και την έκταση των ενεργειών τους, πολύ δε περισσότερο τα αποτελέσματα, αφού χαρακτηρίζονται ως άκρως απόρρητα.

1.3.3 Κρυπτοσύστημα Rabin

Το κρυπτοσύστημα Rabin αποτελεί μια ασύμμετρη κρυπτογραφική τεχνική, που, όπως και ο RSA, σχετίζεται με τη δυσκολία της παραγοντοποίησης. Ο αλγόριθμος δημοσιεύτηκε τον Ιανουάριο του 1979 από τον Michael O. Rabin. Έχει το πλεονέκτημα, ότι το πρόβλημα πάνω στο οποίο βασίζεται έχει αποδειχθεί εξίσου δύσκολο με την παραγοντοποίηση ακεραίων. Έχει όμως το μειονέκτημα, ότι κάθε έξοδος της συνάρτησης Rabin μπορεί να παραχθεί από οποιαδήποτε από τις τέσσερις πιθανές εισόδους. Αν κάθε έξοδος είναι κρυπτογραφημένη, απαιτείται επιπλέον πολυπλοκότητα για την αποκρυπτογράφηση, ώστε να εντοπίσει ποια από τις τέσσερις πιθανές εισόδους είναι το πραγματικό κείμενο $[16]$.

Δημιουργία κλειδιού

Βήμα 1: Ένας χρήστης A, επιλέγει δύο τυχαίους μεγάλους πρώτους αριθμούς p, q και υπολογίζει το γινόμενο τους $N = p \cdot q$. Μια συχνή επιλογή είναι $p \equiv q \equiv 3(mod4)$, για την απλοποίηση του υπολογισμού των τετραγωνικών ριζών $modulo\ p$ και $modulo\ q$ που θα δούμε παρακάτω, αλλά ο αλγόριθμος ισχύει για οποιουσδήποτε πρώτους.

Βήμα 2: Το N αποτελεί το δημόσιο κλειδί και οι πρώτοι αριθμοί p και q αντίστοιχα, αποτελούν το ιδιωτικό κλειδί (p, q).

Κρυπτογράφηση

Η A, που επιθυμεί να στείλει στον B κρυπτογραφημένο μήνυμα, ακολουθεί την εξής διαδικασία:

Βήμα 1: Πληροφορείται το δημόσιο κλειδί N του B.

Βήμα 2: Επιλέγει έναν αριθμό $b < N$.

Βήμα 3: Έστω ότι θέλει να του στείλει ένα μήνυμα x οπότε το κρυπτογραφεί ως

$$y \equiv (x \cdot (x + b)(modN)$$

και του στέλνει το y.

Στην ουσία, η συνάρτηση $y \equiv (x \cdot (x + b)(modN)$ είναι μίας κατεύθυνσης (για πολύ μεγάλο N) δηλαδή κάποιος που γνωρίζει το x μπορεί να υπολογίσει το y, αλλά από την άλλη κάποιος που γνωρίζει το y δεν είναι εύκολο να βρει το x. Όμως, όπως θα δούμε παρακάτω, αν κάποιος γνωρίζει είτε το p είτε το q μπορεί να εξάγει το x από το y (τα p και q ουσιαστικά είναι "καταπακτές" (trapdoors».

Αποκρυπτογράφηση

Για κάθε κρυπτοκείμενο y έχουμε μια λύση u (υπάρχουν τέσσερις λύσεις) της δευτεροβάθμιας

$$y \equiv (x \cdot (x + b))(modN)$$

Η παραπάνω δευτεροβάθμια όμως είναι μια ισοτιμία και έχει μια λύση αν και μόνο αν η ισοτιμία

$$(x^{'})^2 \equiv y + \frac{b^2}{4}(modN)$$

έχει λύση. Άρα μπορούμε να γράψουμε ως συνάρτηση αποκρυπτογράφησης την

$$D_{N,b}(y) = \sqrt{\frac{b^2}{4} + y} - \frac{b}{2}$$

Οπότε για ένα κρυπτογραφημένο μήνυμα y η αποκρυπτογράφηση είναι εύκολη αν p, q είναι γνωστά, χωρίς να διαιρούν το y όμως, καθώς μπορούμε να υπολογίσουμε τις ρίζες r, s των ισοτιμιών

$$x \cdot (x + b) \equiv y \ (modp)$$
$$x \cdot (x + b) \equiv y \ (modq)$$

χρησιμοποιώντας τον Ευκλείδιο Αλγόριθμο για να υπολογίσουμε τους ακέραιους k, l τέτοιους ώστε $k \cdot p + l \cdot q = 1$ και τελικώς η $lqr + kps$ να είναι μια λύση της ισοτιμίας

$$x \cdot (x + b) \equiv y \ (modN)$$

Ουσιαστικά, η αποκρυπτογράφηση του Rabin συνίσταται στην εύρεση ριζών της

$$(x^{'})^2 \equiv y + \frac{b^2}{4}(modN)$$

Επομένως, αν τα p, q είναι γνωστά, αρκεί να βρούμε τις ρίζες των $(x^{'})^2 \equiv y + \frac{b^2}{4}(modp)$ και $(x^{'})^2 \equiv y + \frac{b^2}{4}(modq)$.

Αν τώρα, όπως αναφέραμε και παραπάνω, ισχύει ότι $p \equiv 3(mod4)$, τότε υποθέτουμε ότι το $y + \frac{b^2}{4} = c$, είναι τετραγωνικό υπόλοιπο, οπότε έχουμε

$$\begin{aligned}(\pm c^{(p+1)/4})^2 &\equiv c^{(p+1)/2}(modp) \\ &\equiv c^{(p-1)/2}C(modp) \\ &\equiv c(modp)\end{aligned}$$

Χρησιμοποιώντας τώρα το κριτήριο του Euler ότι αν το c είναι τετραγωνικό υπόλοιπο $modulo\ p$, τότε $c^{(p-1)/2} \equiv 1(modp)$. Επομένως, οι δύο τετραγωνικές ρίζες του $cmodp$ είναι $\pm c^{(p+1)/4} modp$. Παρομοίως, οι δύο τετραγωνικές ρίζες του $cmodq$ είναι $c^{(q+1)/4} modq$ [16].

Συνοψίζοντας, η αποκωδικοποίηση παράγει τρία επιπλέον λανθασμένα αποτελέσματα μαζί με το σωστό, έτσι ώστε το σωστό κείμενο εισόδου να μαντευτεί. Η αποσαφήνιση εισάγει επιπλέον υπολογιστικό κόστος, και αυτή είναι η βασική αιτία που έχει εμποδίσει το συγκεκριμένο κρυπτοσύστημα να χρησιμοποιηθεί σε εφαρμογές.

1.3.4 Κρυπτοσύστημα El-Gamal

Το 1985, ο El Gamal προτείνει ένα κρυπτοσύστημα δημοσίου κλειδιού, το οποίο, βασίζεται στο πρωτόκολλο διανομής κλειδιού των Diffie-Hellman και η ασφάλεια του επιτυχγάνεται από τη δυσκολία επίλυσης των προβλημάτων DLP και DHP στην ομάδα $\mathbb{Z}_p^*$. Το κρυπτοσύστημα El Gamal στηρίζεται στη μονόδρομη συνάρτηση, δηλαδή ότι η κρυπτογράφηση και η αποκρυπτογράφηση γίνονται με διαφορετικές συναρτήσεις. Βασίζεται στην υπόθεση ότι το πρόβλημα του Διακριτού λογαρίθμου (DLP) δεν μπορεί να λυθεί σε πραγματικό χρόνο, ενώ η αντίστροφη διαδικασία, της δύναμης, μπορεί να υπολογιστεί αποτελεσματικά. Μετά τον RSA, ο El Gamal έλυσε τον αλγόριθμο διανομής κλειδιού Diffie-Hellman παρουσιάζοντας ένα τυχαίο εκθετικό τύπου k. Αυτό το εκθετικό αντικαθιστά τον μυστικό τύπο της λαμβάνουσας οντότητας $[12]$.

Παραγωγή κλειδιού

Στο κρυπτοσύστημα El Gamal μόνο ο παραλήπτης χρειάζεται να δημιουργήσει ένα κλειδί εξαρχής και να το κοινοποιήσει. Παρακάτω παρουσιάζονται τα εξής βήματα:

Βήμα 1: Η Αλίκη διαλέγει έναν μεγάλο πρώτο αριθμό p και έναν γεννήτορα g της πολλαπλασιαστικής ομάδας $\mathbb{Z}_p^*$.

Βήμα 2: Ύστερα διαλέγει έναν τυχαίο ακέραιο b από την ομάδα $\mathbb{Z}$ με τον περιορισμό ότι $1 \leq b \leq p-2$.

Βήμα 3: Υπολογίζει το δημόσιο κλειδί που είναι στη μορφή

$$K = g^b mod p$$

Το δημόσιο κλειδί της Αλίκης, είναι η τριάδα (p, g, K), και το ιδιωτικό κλειδί το b.

Βήμα 4: Ύστερα η Αλίκη δημοσιοποιεί το δημόσιο κλειδί της έτσι ώστε ο Bob να το βρεί και να προσπαθήσει να επικοινωνήσει μαζί της.

Κρυπτογράφηση

Δεν τίθεται θέμα ασφάλειας διότι το μόνο κρυφό κομμάτι για τον Bob είναι το b, το οποίο στέλνεται στη μορφή g^b, καθώς η βασική υπόθεση του κρυπτοσυστήματος είναι ότι δεν εφικτό πρακτικά να υπολογίσεις τον διακριτό λογάριθμο. Για την κρυπτογράφηση του μηνύματος, ο Bob πρέπει να ακολουθήσει τα εξής βήματα:

Βήμα 1: Λαμβάνει τη τριάδα, (p, g, K), με το δημόσιο κλειδί της Αλίκης.

Βήμα 2: Έστω ότι θέλει να στείλει ένα μήνυμα m στην Αλίκη και το αντιστοιχεί με ένα σύνολο ακεραίων $(m_1, m_2, \dots)$ στο εύρος $\{0, 1, \dots, p-1\}$.

Βήμα 3: Ο Bob θα διαλέξει έναν τυχαίο εκθέτη k, ο οποίος θα πάρει τη θέση του μυστικού εκθέτη, στη διαμοίραση κλειδιού Diffie-Hellman. Η τυχαιότητα εδώ είναι ένας κρίσιμος παράγοντας, καθώς η πιθανότητα να μαντέψουμε το k δίνει μια λογική ποσότητα πληροφοριών, που απαιτούνται για την αποκρυπτογράφηση του μηνύματος προς τον εισβολέα.

Βήμα 4: Για να δώσει το τυχαίο εκθέτη k στην Αλίκη ο Bob υπολογίζει το $B = g^k modp$ και το συνδυάζει με το κρυπτοκείμενο, το οποίο, πρέπει να σταλθεί στην Αλίκη.

Βήμα 5 Ο Bob κρυπτογραφεί το μήνυμα m, στο κρυπτογραφημένο μήνυμα c, υπολογίζοντας για κάθε m_i του Βήματος 2 το

$$c_i = A^k m_i (modp)$$

Το προκύπτον κρυπτογραφημένο μήνυμα c αποστέλλεται στον Bob μαζί με το κοινό κλειδί $g^k modp$ που προέρχεται από τον τυχαίο μυστικό εκθέτη, δηλαδή η δυάδα (B, c). Ακόμα κι αν ένας εισβολέας ακούσει αυτή τη μετάδοση, και αποκτήσει επίσης το δημόσιο κλειδί g^b του Bob από ένα παροχέα κλειδιών, εξακολουθεί να μην είναι σε θέση να παράξει το $g^{b \cdot k}$ όπως είναι γνωστό από το πρόβλημα του διακριτού λογαρίθμου.

Ο El Gamal συνιστά να χρησιμοποιούμε ένα νέο τυχαίο k για κάθε ένα από τα blocks m_i του μηνύματος. Αυτό βελτιώνει σημαντικά την ασφάλεια, καθώς η γνώση ενός block μηνύματος m_j δεν οδηγεί τον εισβολέα στη γνώση όλων των άλλων m_i. Ο λόγος αυτής της ιδέας είναι ότι αν $c_1 = m_1 \cdot ((g^b)^k)\ modp$ και $c_2 = m_2 \cdot ((g^b)^k)\ modp$, γνωρίζοντας μόνο το m_1 το επόμενο τμήμα του μηνύματος, το m_2 μπορεί να υπολογιστεί με την εξής διαδικασία:

$$\frac{m_1}{m_2} = \frac{c_1}{c_2}$$

Αποκρυπτογράφηση

Αφού λάβει το κρυπτογραφημένο μήνυμα η Αλίκη και το τυχαιοποιημένο δημόσιο κλειδί $B = g^k (modp)$, πρέπει να χρησιμοποιήσει τον αλγόριθμο αποκρυπτογράφησης για να είναι σε θέση να διαβάσει το αρχικό μήνυμα M. Τα βήματα της αποκρυπτογράφησης είναι τα εξής:

Βήμα 1: Η Αλίκη υπολογίζει το

$$B^{p-1-b} c modp$$

Πιο αναλυτικά, έχουμε

$$B^{p-1-b} = (g^b)^{p-1-b} \equiv g^{b(p-1)} g^{-bk} \equiv (g^{bk})^{-1} (modp)$$

και

$$c = A^k \cdot m = g^{bk} m (modp)$$

άρα

$$B^{p-1-b} c \equiv m (modp)$$

Ακολουθεί ένα απλό παράδειγμα για την ευκολότερη κατανόηση του κρυπτοσυστήματος El-Gamal.

Παράδειγμα 1.3.3. Η Αλίκη επιλέγει $p = 23, g = 7$ και $b = 6$. Υπολογίζει το

$$A = 7^6 \equiv 4(mod23)$$

οπότε το δημόσιο κλειδί της Αλίκης είναι το $(p = 23, g = 7, A = 4)$.

Με τη σειρά του ο Bob θέλει να επικοινωνήσει με την Αλίκη και να της στείλει ένα μήνυμα έστω $m = 2$. Παίρνει το δημόσιο κλειδί της $(p = 23, g = 7, A = 4)$ και με τη σειρά του διαλέγει έναν τυχαίο ακέραιο $b = 3$. Στη συνέχεια υπολογίζει

$$\begin{aligned} B &= 7^3 \equiv 21(mod23) \\ c &= 4^3 \cdot 2 \equiv 18 \cdot 2 \equiv 13(mod23) \end{aligned}$$

οπότε έχει το κρυπτοκείμενο $(B, c) = (21, 13)$ και το στέλνει στην Αλίκη.

Η Αλίκη τώρα υπολογίζει το

$$K^{-1} = (B^b)^{-1} \equiv ((21)^6)^{-1} \equiv 18^{-1} \equiv 9(mod23)$$

και τελικά είναι

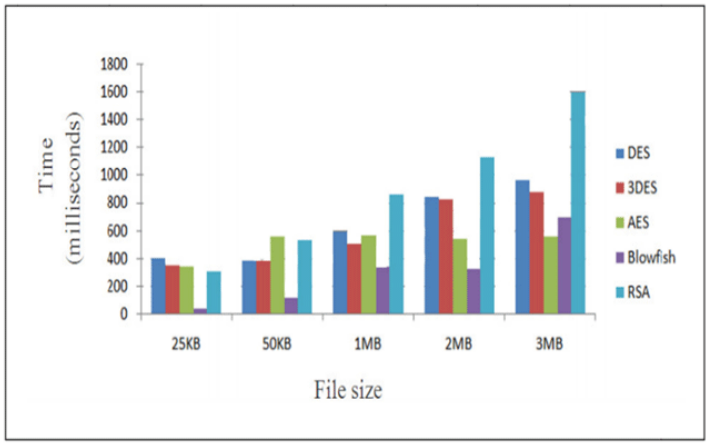
$$K^{-1} \cdot c \equiv 9 \cdot 13 \equiv 2(mod23)$$

όπου το 2 είναι το αρχικό μήνυμα $m = 2$.

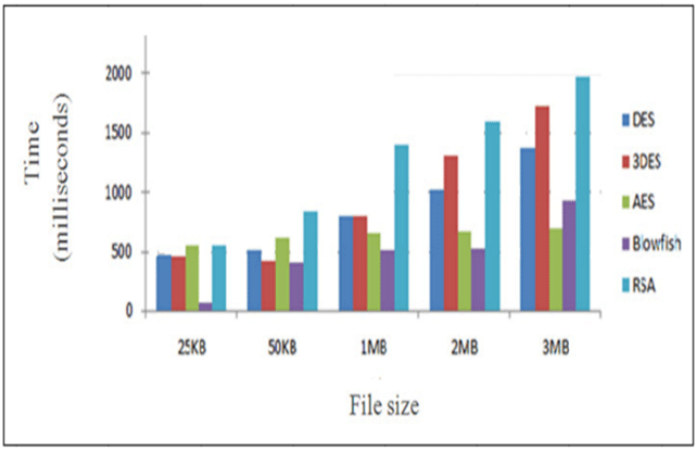
1.3.5 ¨Σύγκριση¨ συμμετρικής-ασύμμετρης κρυπτογραφίας

Στη συνέχεια εκθέτουμε τα διαγράμματα σχήμα 1.8 και σχήμα 1.9, τα οποία οπτικοποιούν τη σύγκριση μερικών από τους πιο γνωστούς αλγόριθμους όπως οι DES, 3DES, AES, Blowfish και RSA.

Οι αλγόριθμοι της συμμετρικής κρυπτογραφίας (σχήμα 1.8) κρυπτογραφούν και αποκρυπτογραφούν (σχήμα 1.9) ταχύτερα από τους ασύμμετρους αλγορίθμους. Ταυτόχρονα οι συμμετρικοί αλγόριθμοι καταναλώνουν λιγότερη υπολογιστική ισχύ κατά πολύ από τους ασύμμετρους αλγόριθμους βασικό κριτήριο προς τις επιθέσεις ανάλυσης ισχύος.

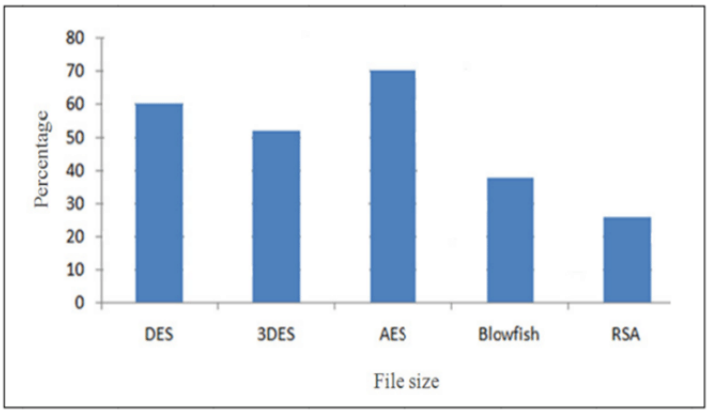


Σχήμα 1.8: Ταχύτητα κρυπτογράφησης σε σχέση με το μέγεθος του αρχικού κειμένου.



Σχήμα 1.9: Ταχύτητα αποκρυπτογράφησης του κρυπτογραφημένου κειμένου.

Στη κρυπτογραφία, ένα χαρακτηριστικό της ασφάλειας ενός κρυπτογραφικού αλγορίθμου είναι το *Avalance effect*. Μας δείχνει ότι μια μικρή αλλαγή στην είσοδο του αλγορίθμου (για παράδειγμα, να αλλάξουμε απλά ένα και μόνο bit από $0 \rightarrow 1$ ή $1 \rightarrow 0$) η έξοδος του αλγορίθμου θα αλλάξει δραματικά (τα μισά bits θα αλλάξουν). Ο όρος χρησιμοποιήθηκε πρώτα από τον Horst Feistel, αλλά η βασική ιδέα προυπήρχε από την εποχή του Shannon και τον ορισμό που έδωσε για τη διάχυση (diffusion). Στο σχήμα 1.10 παρουσιάζεται το διάγραμμα σύγκρισης των γνωστών σημερινών αλγορίθμών (DES, 3DES, AES, Blowfish και RSA) όσον αφορά το avalance effect του καθενός.



Σχήμα 1.10: Διάγραμμα σύγκρισης των γνωστότερων σημερινών αλγορίθμων, όσον αφορά το avalance effect του καθενός.

Καθένας από τους κρυπτογραφικούς αλγόριθμους έχει τα αδύνατα και τα δυνατά του σημεία. Διαλέγουμε τον κρυπτογραφικό αλγόριθμο στηριζόμενοι στις απαιτήσεις της εφαρμογής για την οποία θα χρησιμοποιηθεί. Ύστερα από τη μελέτη των παραπάνω διαγραμμάτων παρατηρούμε ότι η επιλογή συμμετρικών αλγορίθμων είναι η τέλεια επιλογή όσον αφορά το χρόνο υλοποίησης, τον μεγάλο όγκο δεδομένων που πρέπει να κρυπτογραφηθούν και την αποδοτική υλοποίηση σε ψηφιακή τεχνολογία.

Αν η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικοποίηση-ταυτοποίηση του αποστολέα είναι τα κύρια χαρακτηριστικά που μας ενδιαφέρουν τότε μπορούμε να διαλέξουμε το υβριδικό σύστημα συμμετρικού και ασύμμετρου αλγόριθμου με AES, hash αλγόριθμους και RSA [14].

ΚΕΦΑΛΑΙΟ 2

Κβαντική Κρυπτογραφία

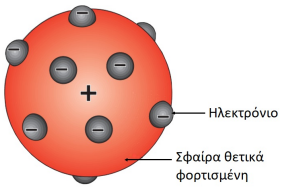
2.1 Περί Φυσικής

Η υπόθεση ότι η ύλη αποτελείται από αδιαίρετες μονάδες, τα άτομα, εκφράστηκε για πρώτη φορά στην Αρχαία Ελλάδα από τον Δημόκριτο. Οι πρώτες επιστημονικές μαρτυρίες όμως ήλθαν την περίοδο του Διαφωτισμού. Πειράματα που έδρασαν αποφασιστικά στην ανάπτυξη της ιδέας του ατόμου ήταν:

- ◇ Τα πειράματα ηλεκτρόλυσης του Faraday, που οδήγησαν στον νόμο της ηλεκτρόλυσης.
- ◇ Το πείραμα του Thomson, όπου μετρήθηκε ο λόγος $\frac{e}{m}$ (φορτίο προς μάζα) για το ηλεκτρόνιο και άρα ανακαλύφθηκε στην ουσία το ηλεκτρόνιο (βραβείο Nobel το 1908).
- ◇ Το πείραμα του Millikan, όπου μετρήθηκε το φορτίο του ηλεκτρονίου (βραβείο Nobel 1923).

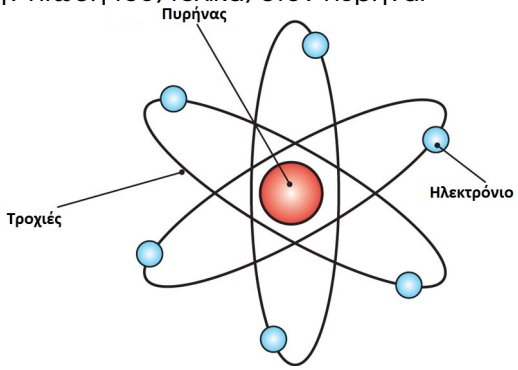
Τα πειράματα του Thomson απέδειξαν την ύπαρξη του ηλεκτρονίου και οδήγησαν στα πρώτα μοντέλα του ατόμου. Στο μοντέλο του Thomson (σχήμα 2.1) τα ηλεκτρόνια ήταν ομοιόμορφα κατανεμημένα μέσα στο άτομο. Το μοντέλο αυτό αμφισβητήθηκε από τον Lenard, ο οποίος στα πειράματά του διαπίστωσε ότι τα ηλεκτρόνια μπορούσαν να περάσουν εύκολα από λεπτά υμένια, πράγμα που σήμαινε ότι το άτομο θα πρέπει να είναι σχετικά "άδειο".

Ο Rutherford, επηρεασμένος από τη δουλειά του Lenard, επιχείρησε να ελέγξει πειραματικά το μοντέλο του Thomson. Το πείραμα του Rutherford συνίστατο στο βομβαρδισμό λεπτών υμενίων χρυσού, με ισχυρά, διεισδυτικά σωματίδια α (πυρήνες He). Το πείραμα αυτό έδειξε ότι κάποια από τα σωματίδια α, υφίσταντο έντονη σκέδαση και κάποια άλλα περνούσαν σχεδόν ανεμπόδιστα



Σχήμα 2.1: Το μοντέλο του Thompson

από τα υμένια. Η ανάλυση των αποτελεσμάτων οδήγησε στο πλανητικό μοντέλο του ατόμου, σύμφωνα με το οποίο σχεδόν όλη η μάζα του ατόμου είναι συγκεντρωμένη σε μια μικρή περιοχή, τον πυρήνα, ενώ τα ηλεκτρόνια κινούνται σε μεγάλη απόσταση από τον πυρήνα. Το μοντέλο του ατόμου Rutherford (σχήμα 2.2) δεν μπορούσε να εξηγηθεί με βάση την κλασική θεωρία. Σύμφωνα με την κλασική θεωρία κάθε επιταχυνόμενο φορτίο ακτινοβολεί. Έτσι, το ηλεκτρόνιο, όντας επιταχυνόμενο γύρω από τον πυρήνα (κεντρομόλος επιτάχυνση) θα ακτινοβολεί χάνοντας συνεχώς ενέργεια, μέχρι την πτώση του, τελικά, στον πυρήνα.



Σχήμα 2.2: Το μοντέλο ατόμου του Rutherford

Το μοντέλο του Bohr (σχήμα 2.3) για το άτομο αναπτύχθηκε στην προσπάθεια ερμηνείας των ατομικών φασμάτων και της σταθερότητας του ατόμου στο μοντέλο του Rutherford. Ερμηνεύει εξαιρετικά το φάσμα του υδρογόνου, τη σταθερότητα του ατόμου, το έργο ιονισμού του, και υπολογίζει την τάξη μεγέθους του ατόμου (βραβείο Nobel, 1922).

Οι υποθέσεις (αξιώματα) που έκανε ο Bohr (αυθαίρετα) στην ανάπτυξη της θεωρίας του είναι οι εξής:

1. Οι ενεργειακές καταστάσεις του ατόμου είναι κβαντωμένες. Το άτομο σε αυτές τις καταστάσεις δεν ακτινοβολεί. Ακτινοβολεί μόνο κατά τη μετάβαση από μια κατάσταση σε άλλη. Η ενέργεια του εκπεμπόμενου φωτονίου ισούται με την ενεργειακή διαφορά των δύο καταστάσεων.

2. Επιτρέπονται μόνο εκείνες οι κυκλικές τροχιές στις οποίες η στροφορμή του ηλεκτρονίου, L, είναι ακέραιο πολλαπλάσιο της ανηγμένης σταθεράς του Planck, $\hbar(\hbar = \frac{h}{2\pi})$, δηλαδή

$$L = mvr_n = n\hbar \text{ (συνθήκη κβάντωσης)}, n = 1, 2, 3, \ldots$$

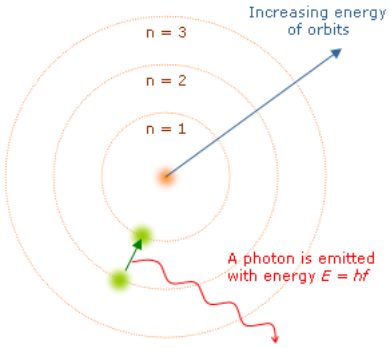
Ο ακέραιος αριθμός n, που αριθμεί τα κβάντα (ελάχιστες διακριτές ποσότητες) της στροφορμής, λέγεται κβαντικός αριθμός της κάθε τροχιάς. Από τη συνθήκη κβάντωσης της στροφορμής και από τις εξισώσεις της κυκλικής κίνησης (δύναμη Coulomb ($\frac{ke^2}{r^2}$) = κεντρομόλος δύναμη ($\frac{mv^2}{r}$), $v = \omega r$), υπολογίζεται η ακτίνα της τροχιάς α_n, η ενέργεια, E_n, και η ταχύτητα v_n του ηλεκτρονίου που βρίσκεται στην τροχιά με κβαντικό αριθμό n στο άτομο του υδρογόνου:

$$r_n = \frac{\hbar^2}{kme^2}n^2 = n^2\alpha_0 \ , \ \alpha_0 = \frac{\hbar^2}{kme^2} = 0.529A$$

$$E_n = \frac{k^2 m^2 e^4}{\hbar^2}\frac{1}{n^2} = -13.6\frac{1}{n^2}eV$$

$$v_n = \frac{ke^2}{\hbar n} = \frac{c}{137}\frac{1}{n}$$

Για τη θεωρία του Bohr ισχύει η γνωστή Αρχή της Αντιστοιχίας: *Στο όριο των μεγάλων κβαντικών αριθμών τα αποτελέσματα του Bohr θα συμπίπτουν με τα αντίστοιχα κλασικά.*



Σχήμα 2.3: Το μοντέλο ατόμου του Bohr

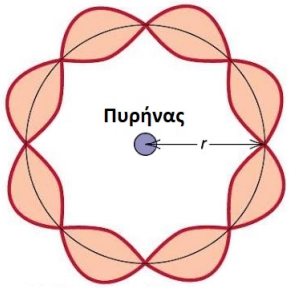
Ενώ το μοντέλο του Bohr έδινε ικανοποιητικές απαντήσεις στα διάφορα μέχρι τότε προβλήματα, υπήρχαν αρκετά θέματα που παρέμεναν ανερμήνευτα (σχετική ένταση ατομικών φασμάτων, φάσματα βαριών στοιχείων, μη περιοδικές κινήσεις κλπ). Επιπλέον δεν υπήρχε μια θεμελίωση-ερμηνεία των βασικών υποθέσεων του Bohr. Η ερμηνεία αυτή δόθηκε από τον De Broglie, το 1923.

Ο De Broglie, υποκινούμενος από τις εργασίες πάνω στην διπή φύση της ακτινοβολίας, υπέθεσε την ίδια διπή φύση και για τα σωματίδια και ανέπτυξε το δικό του μοντέλο ατόμου (σχήμα 2.4). Ο De Broglie έθεσε το βασικό ερώτημα: ¨Αφού τα φωτόνια συμπεριφέρονται ως σωματίδια γιατί και τα σωματίδια να μην συμπεριφέρονται ως κύματα;¨ Επιπλέον, για τα κύματα η κβάντωση ήταν κάτι ήδη γνωστό, π.χ. στάσιμα κύματα σε χορδή.

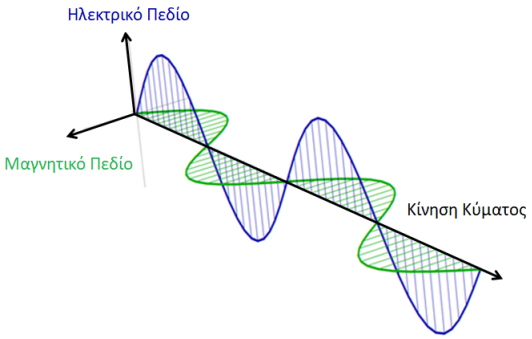
Το βασικό αξίωμα De Broglie ήταν το εξής: *Κάθε σωματίδιο συμπεριφέρεται και ως κύμα.* Οι σχέσεις που συνδέουν τα κυματικά χαρακτηριστικά του (συχνότητα -f, μήκος κύματος-λ) με τα σωματιδιακά χαρακτηριστικά του (ενέργεια-E, ορμή-p) είναι οι

$$f = \frac{E}{h}\ ,\ \lambda = \frac{h}{p}$$

Οι σχέσεις αυτές είναι οι ίδιες με αυτές που είχαν διατυπωθεί από τον Αϊνστάιν για τα ηλεκτρομαγνητικά κύματα (σχήμα 2.5). Δεχόμενοι ότι η κίνηση του ηλεκτρονίου γύρω από τον πυρήνα έχει κυματικό χαρακτήρα (δηλ. τα e^- όταν κινούνται γύρω από τον πυρήνα συμπεριφέρονται ως κύματα) και άρα επιτρέπονται μόνο εκείνες οι κυκλικές τροχιές που φτιάχνουν στάσιμα κύματα ($2\pi r = n\lambda$, με $\lambda = \frac{h}{p}$), μπορούμε να ερμηνεύσουμε, αβίαστα, τη συνθήκη κβάντωσης της στροφορμής του Bohr. Επιπλέον, αφού η συχνότητα, $\omega = 2\pi f = \frac{v}{r}$, είναι κβαντισμένη, είναι φυσιολογική η κβάντωση και της ενέργειας.



Σχήμα 2.4: Το μοντέλο ατόμου του De Broglie



Σχήμα 2.5: Η κίνηση ενός κύματος σε σχέση με το μαγνητικό και το ηλεκτρικό πεδίο.

2.1.1 Αρχή Απροσδιοριστίας του Heisenberg

Ο δυισμός κύματος-σωματιδίου που προέκυψε από τα φαινόμενα κβάντωσης της ενέργειας και των φαινομένων συμβολής, γρήγορα συσχετίστηκε από τον Heisenberg με την απροσδιοριστία. Ο Heisenberg έκανε την συσχέτιση αυτή μέσα από μια σειρά αφηρημένων μαθηματικών συλλογισμών. Θεμέλιό τους ήταν η σκέψη, ότι η κυματοσυνάρτηση Ψ περιγράφει κάθε μια από τις υπερθέσεις, χωρίς να μπορούμε να διευκρινίσουμε ποια από όλες θα συναντήσουμε κατά την εκτέλεση των πειραμάτων μας. Έτσι στο σημείο αυτό εισέρχεται η απροσδιοριστία.

Σύμφωνα με την αρχή αυτή, είναι αδύνατον να μετρηθεί ταυτόχρονα η θέση και η ορμή ενός σωματιδίου με απόλυτη ακρίβεια. Πιο συγκεκριμένα, *Το γινόμενο των αβεβαιοτήτων, θέσης ($\Delta\chi$) και ορμής (Δp), ενός σωματιδίου, δεν μπορεί να είναι μικρότερο από το μισό της σταθεράς του Planck $\hbar$* , δηλαδή

$$\Delta\chi\Delta p > \frac{\hbar}{2}$$

Με άλλα λόγια, όσο πιο αυστηρά καθορισμένη είναι η θέση ενός σωματιδίου, τόσο μεγαλύτερη είναι η αβεβαιότητα στην ορμή του. Στην πράξη, για μικροσκοπικά σωματίδια όπως π.χ. ηλεκτρόνια, το γινόμενο των αβεβαιοτήτων θέσης ορμής είναι περίπου ίσο με $\hbar$, μπορεί κανείς δηλαδή να θεωρήσει ότι $\Delta\chi\Delta p \approx \hbar$.

Αφού τα σωματίδια συμπεριφέρονται σαν κύματα, θα πρέπει να περιγράφονται και αυτά, όπως και κάθε κύμα, από μια κυματοσυνάρτηση, π.χ. $\Psi(x,t) = e^{i(kx-\omega t)}$. Κάθε κυματοσυνάρτηση

όμως περιγράφει μια μεταβολή (ταλάντωση) κάποιας φυσικής ποσότητας, π.χ. των τμημάτων ταλαντούμενης χορδής, των μορίων νερού κλπ. Στην περίπτωση ενός σωματιδίου (εντοπισμένης ποσότητας), όμως δεν θα μπορούσε να περιγράφει π.χ. τη θέση του γιατί τότε θα έπρεπε να είναι παντού μηδέν εκτός από ένα δεδομένο σημείο. Εδώ η κυματοσυνάρτηση εκφράζει πιθανότητα. Δίνει το πλάτος πιθανότητας να βρούμε το σωμάτιο στη μια ή την άλλη περιοχή του χώρου. Δηλαδή αυτό που είναι κύμα (απλωμένο), δεν είναι το ίδιο το σωμάτιο, αλλά η πιθανότητα να το βρούμε στη μια ή την άλλη περιοχή του χώρου. Αν ένα σωματίδιο περιγράφεται από μια κυματοσυνάρτηση $\Psi(x,t)$, τότε το $|\Psi(x,t)|$ λέγεται πλάτος πιθανότητας και η ποσότητα $|\Psi(x,t)|^2 = P(x)$ λέγεται πυκνότητα πιθανότητας (πιθανότητα ανά μονάδα μήκους).

2.1.2 Η εξίσωση Shrödinger

Η κυματοσυνάρτηση $\Psi(x,t)$ ενός υλικού κύματος (σωματιδίου), όπως και κάθε είδους κύματος, δίδεται/υπολογίζεται και εδώ από τη λύση μιας κυματικής εξίσωσης, χαρακτηριστικής του προβλήματος. Η εξίσωση αυτή στην περίπτωσή μας λέγεται εξίσωση Schrödinger και είναι η βασική εξίσωση της Κβαντομηχανικής. Θα ξεκινήσουμε να "παράγουμε" την εξίσωση θεωρώντας τη κλασική μη-ρεαλιστική έκφραση της ενέργειας ενός σωματιδίου E, η οποία είναι το άθροισμα της κινητικής K και της δυναμικής ενέργειας V (όλα θα τα θεωρούμε ως συνάρτηση του x).

Έχουμε λοιπόν

$$E = K + V = \frac{1}{2}mv^2 + V(x) = \frac{p^2}{2m} + V(x)$$

Τώρα θα επικαλεστούμε τον ισχυρισμό του De Broglie, ότι δηλαδή όλα τα σωματίδια μπορούν να αναπαρασταθούν ως κύματα με συχνότητα ω και κυματικό αριθμό k, και ότι $E = \hbar\omega$ και $p = \hbar k$. Οπότε αν τα εφαρμόσουμε στη παραπάνω εξίσωση θα έχουμε:

$$\hbar\omega = \frac{\hbar^2 k^2}{2m} + V(x)$$

Ένα κύμα, όπως αναφέραμε προηγουμένως μπορεί να γραφτεί στη μορφή

$$\Psi(x,t) = Ae^{i(kx-\omega t)}$$

οπότε βρίσκουμε τις μερικές παραγώγους προκειμένου να οδηγηθούμε σε μια διαφορική εξίσωση:

$$\frac{\partial\psi}{\partial t} = -i\omega\psi \Rightarrow \omega\psi = i\frac{\partial\psi}{\partial t}$$

$$\frac{\partial^2\psi}{\partial x^2} = -k^2\psi \Rightarrow k^2\psi = -\frac{\partial^2\psi}{\partial x^2}$$

Πολλαπλασιάζοντας την εξίσωση ενέργειας με ψ και βάζοντας και τις μερικές παραγώγους θα έχουμε

$$\hbar(\omega\psi) = \frac{\hbar^2}{2m}(k^2\psi) + V(x)\psi \Rightarrow i\hbar\frac{\partial\psi}{\partial t} = \frac{-\hbar^2}{2m}\frac{\partial^2\psi}{\partial x^2} + V\psi$$

Η εξίσωση αυτή είναι η *χρονοεξαρτώμενη εξίσωση Shrödinger*.

2.1.3 Το παράδοξο Einstein-Podolsky-Rosen (EPR)

Για ένα φυσικό που είναι ***ρεαλιστής***, μία φυσική θεωρία περιγράφει, κανονικοποιεί και συμπυκνώνει την συμπεριφορά φυσικών αντικειμένων, των οποίων η ύπαρξη είναι αδιαμφισβήτητη: Είναι πραγματικά αντικείμενα!

Για ένα φυσικό που είναι ***θετικιστής***, ο στόχος μία φυσικής θεωρίας, είναι η περιγραφή σχέσεων μεταξύ μετρήσιμων ποσοτήτων, που αφορούν τα αντικείμενα του φυσικού κόσμου. Η θεωρία δεν ασχολείται με το αν υπάρχουν ή όχι τα αντικείμενα αυτά, ούτε καν εάν ένα τέτοιο ερώτημα έχει νόημα.

Για ένα φυσικό που είναι ***ντετερμινιστής***, ακριβής γνώση των αρχικών συνθηκών και των αλληλεπιδράσεων μεταξύ των αντικειμένων του φυσικού κόσμου, επιτρέπει πλήρη πρόβλεψη του μέλλοντος. Ο ντετερμινισμός είναι παγκόσμιο χαρακτηριστικό των φυσικών φαινομένων, ακόμη και αυτών για τα οποία δεν ξέρουμε τίποτε. Με την λογική αυτή, κάθε αναφορά σε τυχαιότητα σχετίζεται με κάποια (προσωρινή) άγνοια.

Για ένα φυσικό που είναι ***πιθανοκρατιστής***, η τυχαιότητα είναι συστατικό στοιχείο της φύσης των μικροσκοπικών φαινομένων. Για αυτόν, ο ντετερμινισμός είναι απλή συνέπεια μιας κατάλληλα μακροσκοπικής θέασης νόμων, που δρουν σε μικροσκοπικότερα επίπεδα.

Ο Albert Einstein ήταν ***ρεαλιστής*** και ***ντετερμινιστής***. Ο Niels Bohr ήταν ***θετικιστής*** και ***πιθανοκρατιστής***.

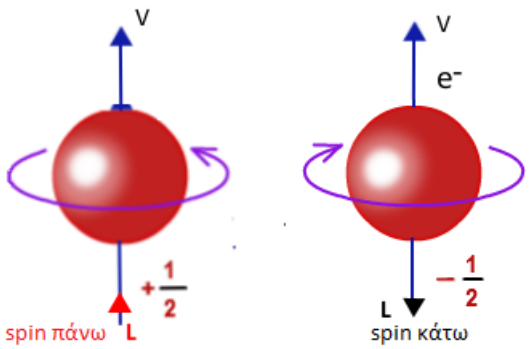
Τον Σεπτέμβριο του 1926 στο Como, ο Bohr, σε μία αξιομνημόνευτη διάλεξη, υποστηρίζει την νέα (τότε) Κβαντική Μηχανική και παρουσιάζει τις ανισότητες του Heisenberg (ή αλλιώς αυτό που αναφέραμε προηγουμένως ως αρχή απροσδιοριστίας) που σημαίνουν ότι είναι αδύνατο να οριστούν ακριβείς αρχικές συνθήκες στα $\Delta\chi$ και Δp, που αυτόματα σημαίνει ότι είναι αδύνατο να στηθεί μία ντετερμινιστική μικροσκοπική θεωρία κατά αναλογία με την κλασική μηχανική. Μόνο πιθανοκρατική θεώρηση είναι δυνατή, και μάλιστα, κατά τον Bohr, αυτή δίδεται από την κβαντομηχανική.

Η λεγόμενη "μη-τοπικότητα" μια από τις πιο παράξενες έννοιες της κβαντικής θεωρίας, μαζί με την γάτα του Schrödinger, ήταν άλλη μια διαμάχη του Einstein με τον υποστηρικτή και συνιδρυτή της κβαντικής θεωρίας Niels Bohr.

Με την θεωρία αυτή οι υποστηρικτές της, πιστεύουν πώς γεγονότα που συμβαίνουν εδώ, μπορούν να επηρεάσουν γεγονότα σε άλλο σημείο, που μπορεί να είναι αρκετά απομακρυσμένο από το πρώτο. Το φαινόμενο αυτό ήταν η αιτία που έκανε τον Einstein να δηλώσει πως "*ο Θεός δεν παίζει ζάρια με το Σύμπαν*"!

Ο Einstein διαφωνεί, και δημοσιοποιεί τις διαφωνίες του από τα 1927 ως τα 1930. Μετά από πολλές συζητήσεις οι απόψεις του Bohr υπερισχύουν. Έχοντας σοκαριστεί από την υποχώρηση του ντετερμινισμού, ο Einstein, επιχειρεί να εκφράσει τις σκέψεις του με μεγαλύτερη ακρίβεια. Πιστεύει ότι η θέση και η ορμή υπάρχουν αντικειμενικά και ταυτόχρονα θεωρεί ότι η κβαντική μηχανική είναι ελλιπής και προσωρινή. Οι απόψεις του κάθε ενός πρωταγωνιστή αυτής της διαμάχης έχουν ως εξής.

Για τον Einstein κάθε φυσική θεωρία πρέπει να είναι μία ντετερμινιστική και πλήρης αναπαράσταση της αντικειμενικής πραγματικότητας. Εμπεριέχει γνωστές μεταβλητές που είναι μετρήσιμες ποσότητες, και άλλες – άγνωστες για την ώρα – μεταβλητές που ονομάζονται κρυφές μεταβλητές. Λόγω της προσωρινής μας άγνοιας, των κρυφών μεταβλητών, η φύση σε μικροσκοπικό επίπεδο εμφανίζεται να συμπεριφέρεται αυθαίρετα και έτσι την περιγράφουμε με μία



Σχήμα 2.6: Το λεγόμενο spin με τις τιμές του.

θεωρία που είναι πιθανοκρατική και μη-πλήρης, δηλαδή με την κβαντομηχανική.

Για τον Bohr κάθε φυσική θεωρία έχει νόημα μόνο ως σύνολο σχέσεων μεταξύ παρατηρήσιμων μεγεθών. Η Κβαντομηχανική προσφέρει μια ορθή και πλήρη περιγραφή της συμπεριφοράς των οντοτήτων στο μικροσκοπικό επίπεδο. Η παρατηρούμενη συμπεριφορά είναι πιθανοκρατική, επειδή η τυχαιότητα είναι ενδογενής στην φύση των φαινομένων.

Μεταξύ της θέσης "τυχαιότητα ως έκφραση άγνοιας" (Einstein) και "τυχαιότητα ως φύση των φαινομένων" (Bohr), η διαμάχη δεν μένει μόνο στο φιλοσοφικό επίπεδο. Πολύ γρήγορα και πολύ φυσικά, εμπλέκει την ίδια την φυσική επιστήμη, με το νοητό πείραμα των Einstein, Podolsky, Rosen (EPR) το 1935. Θα περάσουν 50 χρόνια για να λυθεί μια και καλή το παράδοξο EPR (αν και πειράματα που έδειχναν προς τη κατεύθυνση της υπερίσχυσης των θέσεων Bohr, είχαν γίνει από 1949 από την Wu και τον Shakhov και είχε διακρίνει τη σημασία τους ο David Bohm περί τα 1957).

Το πείραμα λοιπόν που έγινε την περίοδο 1934-1935, τότε που ο Einstein και οι συνεργάτες του δούλευαν στο Princeton, πρωτοδημοσιεύθηκε στο περιοδικό Physical Rewiew, με την επιδίωξη να αποδειχθεί πως η κβαντική θεωρία ήταν ελλιπής. Το πείραμα έχει να κάνει με μια ιδιότητα των σωματιδίων την ορμή, την περιστροφή κλπ. Εδώ ας θεωρήσουμε το χαρακτηριστικό της φοράς του ηλεκτρονίου, το λεγόμενο spin. Σε αυτό το χαρακτηριστικό αποδίδουμε μόνο δύο τιμές $\frac{1}{2}$ και $-\frac{1}{2}$ (πάνω και κάτω, σχήμα 2.6), και αυτό μόνο όταν κάνουμε την μέτρησή του. Σύμφωνα με την "αρχή της απροσδιοριστίας", πριν τη μέτρηση δεν είμαστε σε θέση να γνωρίζουμε την τιμή του spin. Μπορεί να είναι ένα μίγμα των δυνατών τιμών (καταστάσεων), αλλά μόνο μετά την διαδικασία της μέτρησης είμαστε σε θέση να την γνωρίζουμε.

Στο πείραμα EPR, έχουμε δύο σωματίδια, π.χ. ηλεκτρόνια, που αλληλεπιδρούν μεταξύ τους, με αντίθετα spin που το άθροισμά τους είναι συνολικά μηδέν. Είναι δυνατόν με κατάλληλες πειραματικές διατάξεις, να γνωρίζουμε το άθροισμα των ιδιοτήτων τους, χωρίς όμως την γνώση των επιμέρους ιδιοτήτων τους (εδώ του spin).

Αν χωρίσουμε τα δύο ηλεκτρόνια, έστω και σε μακρυνές αποστάσεις, μετρώντας την τιμή της ιδιότητας αυτής στο ένα ηλεκτρόνιο τότε αυτόματα γνωρίζουμε την τιμή της ιδιότητας και του απομακρυσμένου σωματιδίου, έστω και αν δεν την μετρήσουμε, λόγω της γνώσης του αθροίσματος τους, γιατί παραμένει σταθερό και ίσο με μηδέν.

Το παράδοξο κατά την κβαντική θεωρία έγκειται στο γεγονός ότι, με την μέτρηση του spin

του ηλεκτρονίου, που σημαίνει όπως είπαμε και πιο πάνω, πως "επιλέξαμε" την τιμή του spin του, έγινε ταυτόχρονα και "επιλογή" της τιμής του spin του δεύτερου και απομακρυσμένου ηλεκτρονίου. Ταυτόχρονα με την "κατάρρευση κύματος" στο πρώτο, είχαμε και την "κατάρρευση κύματος" στο δεύτερο.

Ακόμη και ο Einstein δεν μπορούσε να δεχθεί πως η "επιλογή" της ιδιότητας στο δεύτερο ηλεκτρόνιο, μεταδίδεται ακαριαία, αφού έτσι παραβιαζόταν η αρχή της θεωρίας της σχετικότητας, που θέτει όριο στην ταχύτητα των σωμάτων. Έτσι όπως φαίνεται από το νοητικό πείραμα, είτε η θεωρία της κβαντομηχανικής δεν είναι πλήρης, είτε παραβιάζεται η θεωρία της σχετικότητας.

Ο Bohr στις αιτιάσεις του Einstein και των άλλων διαφωνούντων στο παράδοξο αυτό, απάντησε πως οι ιδιότητες του μακρόκοσμου διαφέρουν από τον μικρόκοσμο και πως στην Κβαντομηχανική δεν έχει νόημα να μιλάμε για γνώση των φυσικών μεταβλητών του απομακρυσμένου σωματιδίου από την στιγμή που δεν μπορούμε να το παρατηρήσουμε.

Το παράδοξο EPR προκάλεσε συζητήσεις, διαμάχες και πολλές προσπάθειες για να αποδειχθεί ότι η κβαντική μηχανική είναι μια πλήρης φυσική θεωρία και ότι δεν υπάρχουν κρυμμένες μεταβλητές. Η διαμάχη συνεχίστηκε μέχρις ότου, ο John Bell απέδειξε με τη χρήση ανισοτήτων (που είναι πλέον γνωστές ως «ανισότητες Bell») ότι δεν υπάρχουν κρυμμένες μεταβλητές και ότι η κβαντική μηχανική είναι μία πλήρης φυσική θεωρία (Bell, 1964). Η ανισότητες Bell αποδείχτηκαν αργότερα και πειραματικά $[67]$.

2.1.4 Διεμπλοκή ή entaglement

Ο Erwin Schrödinger σε άρθρο του που δημοσιεύτηκε το 1935, για να περιγράψει την άγνωστη, μη κλασική, διασύνδεση μεταξύ δύο κβαντικών συστημάτων τα οποία, αφού αλληλεπιδράσουν, απομακρύνονται το ένα από το άλλο, χρησιμοποίησε το γερμανικό όρο «verschränkung» που έχει την έννοια «σταυρώνω (τα χέρια)» $[68]$. Ο όρος αποδόθηκε στα αγγλικά ως «entanglement» και στα ελληνικά μπορεί να αποδοθεί ως «διαπλοκή» ή «διεμπλοκή». Η κβαντική διεμπλοκή είναι ίσως η πιο αινιγματική πλευρά της κβαντικής μηχανικής και δεν έχει κλασικό ανάλογο.

Για τους κβαντικούς υπολογιστές, η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, όπως η ενέργεια, τον οποίο μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγορίθμους, για τους Niesen & Chuang, 2004 $[69]$. Αυτό που έχει δηλαδή σημασία, δεν είναι να κατανοήσουμε τη φύση της κβαντικής διεμπλοκής (πράγμα που είναι ίσως αδύνατο), αλλά να μάθουμε να την παράγουμε και να τη χρησιμοποιούμε. Ας ορίσουμε λοιπόν την κβαντική διεμπλοκή με έναν απλό, αλλά χρήσιμο για εμάς τρόπο:

Ορισμός 2.1. *Ένα **κβαντικό σύστημα** είναι ένα κομμάτι του Σύμπαντος (περιβαλλοντολογικού ή φυσικού κόσμου) το οποίο ερευνάται με σκοπό την ανάλυση και τη μελέτη των κβαντικών μηχανισμών όσον αφορά το δυισμό του κύματος-σωματιδίου μέσα σε αυτό το σύστημα. Οτιδήποτε ερευνάται έξω από αυτό το σύστημα, παράδειγμα το περιβάλλον, έχει μοναδικό σκοπό την παρατήρηση της επίδρασής του στο σύστημα.*

Ορισμός 2.2. *Η **κβαντική διεμπλοκή** είναι το φαινόμενο, κατά το οποίο δύο σωματίδια ή ομάδες σωματιδίων που δημιουργούνται μαζί ή αλληλεπιδρούν συνενώνοντας τις κυματοσυναρτήσεις τους και μένουν σε κατάσταση διεμπλοκής μεταξύ τους, ασχέτως του χώρου που μεσολαβεί πλέον από το ένα στο άλλο. Αν σταλεί το ένα από τα δύο στο άλλο άκρο του σύμπαντος και συμβεί κάτι σε οποιοδήποτε από τα δύο, το άλλο αντιδρά ακαριαία.*

Ορισμός 2.3. *Πιο φορμαλιστικά, δύο κβαντικά συστήματα βρίσκονται σε* ***κβαντική διεμπλοκή****, όταν η κατάστασή τους δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων.*

Έτσι, φαίνεται πως είτε η πληροφορία μπορεί να ταξιδέψει με άπειρη ταχύτητα, είτε στην πραγματικότητα τα δύο αντικείμενα βρίσκονται ακόμα σε «επαφή», σε σύνδεση μεταξύ τους, σε κατάσταση διεμπλοκής.

2.2 Κβαντική πληροφορία ή Qubit

Σε ένα συμβατικό ψηφιακό υπολογιστή, σαν αυτούς που χρησιμοποιούμε καθημερινά, η στοιχειώδης μονάδα πληροφορίας είναι το δυαδικό ψηφίο ή bit, δηλαδή η ελάχιστη ποσότητα πληροφορίας που μπορεί να αποθηκευτεί σε μια συσκευή. Αυτή η στοιχειώδης μονάδα πληροφορίας μπορεί να έχει δύο τιμές, 0 ή 1.

Το πρόβλημα που προκύπτει με αυτό το υπάρχον σύστημα, είναι η έλλειψη χώρου αποθήκευσης καθώς και χρόνου επεξεργασίας δεδομένων. Με την πληθώρα δεδομένων που δημιουργούνται, χρησιμοποιούνται και επεξεργάζονται σε καθημερινή βάση, έχει δημιουργηθεί η ανάγκη για κάτι πιο μεγάλο, κάτι πρωτοποριακό $[66]$.

2.2.1 Διανύσματα bra-ket

Στη κβαντική θεωρία, η βασική μαθηματική δομή με την οποία θα ασχοληθούμε είναι αυτή ενός μιγαδικού χώρου Hilbert. Ένα μιγαδικός χώρος Hilbert είναι ως γνωστόν ένας μιγαδικός διανυσματικός χώρος με εσωτερικό γινόμενο και πλήρης σύμφωνα με τη νόρμα που ορίζει το αντίστοιχο εσωτερικό γινόμενο. Στη κβαντική υπολογιστική ασχολούμαστε κυρίως με χώρους Hilbert οι οποίοι περιέχουν μιγαδικά διανύσματα διάστασης d και θα χρησιμοποιούμε στο εξής το συμβολισμό, $\mathbb{C}^d$, για να συμβολίζουμε τον χώρο στον οποίο δουλεύουμε $[66]$.

Ορισμός 2.4. *Ένα ket, το οποίο συμβολίζεται ως $|. >$, αναπαριστά ένα $d-$διάστατο διάνυσμα στήλη στο μιγαδικό διανυσματικο χώρο $\mathbb{C}^d$. Ένα bra, το οποίο συμβολίζεται $< .|$, είναι ένα $d-$διάστατο διάνυσμα γραμμή ίσο με το μιγαδικό συζυγή του αντίστοιχου ket, και συγκεκριμένα*

$$\left\langle \cdot \right| = (|\cdot\rangle^*)^T$$

όπου το $*$ συμβολίζει το συζυγή, και T τον ανάστροφο.

Ορισμός 2.5. *Δοθέντων δύο $d-$διάστατων διανυσμάτων*

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \quad \text{και} \quad |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}$$

το εσωτερικό τους γινόμενο είναι $\langle v_1|v_2\rangle := \langle v_1||v_2\rangle = \sum_{i=1}^{d} a_i^* b_i$.

Ορισμός 2.6. *Έστω ένα ket διάνυσμα*

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$$

το μήκος του $|v >$ δίνεται από

$$\||v\rangle\|_2 = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{d} a_i^* a_i} = \sqrt{\sum_{i=1}^{d} |a_i|^2}$$

Αν $\||v\rangle\|_2 = 1$, λέμε ότι το $|v>$ έχει νόρμα 1, ή αλλιώς ότι είναι κανονικοποιημένο.

2.2.2 Το κβαντικό bit (qubit)

Θα ξεκινήσουμε από τα κλασσικά bits 0 και 1 και θα τα αντιστοιχίσουμε το καθένα σε ένα διάνυσμα

$$0 \to |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ και } 1 \to |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ορισμός 2.7. *Μια κατάσταση ενός qubit μπορεί να αναπαρασταθεί ως ένα 2-διάστατο ket διάνυσμα $|\psi> \in \mathbb{C}^2$,*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{όπου } \alpha, \beta \in \mathbb{C} \text{ και } |\alpha|^2 + |\beta|^2 = 1$$

Η συνθήκη στα α, β σημαίνει ότι το $|\psi>$ είναι κανονικοποιημένο. Οι μιγαδικοί αριθμοί α, β καλούνται και ορίσματα (amplitudes) του $|\psi>$.

Γενικότερα, η κβαντική πληροφορία μπορεί να κωδικοποιηθεί και σε υψηλότερης διάστασης κβαντικά συστήματα. Οπότε θα ορίσουμε και το $qudit$.

Ορισμός 2.8. *Ένα qudit, ή αλλιώς ένα $d-$διάστατο κβαντικό σύστημα μπορεί να αναπαρασταθεί ως ένα $d-$διάστατο ket διάνυσμα $|\psi> \in \mathbb{C}^d$,*

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \quad \text{όπου } \forall i, \alpha_i \in \mathbb{C} \text{ και } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1$$

Η συνθήκη στους συντελεστές a_i, υποδηλώνει ότι το $|\psi>$ είναι ένα διάνυσμα μήκους 1.

Όταν δώσαμε τον ορισμό για τα qubits, ξεκινήσαμε από το να αντιστοιχίσουμε με έναν τρόπο τα κλασσικά bits στα διανύσματα $|0>$ και $|1>$. Τα διανύσματα αυτά είναι ορθοκανονικά. Σχηματίζουν λοιπόν μια βάση για τον χώρο $\mathbb{C}^2$, με αποτέλεσμα κάθε διάνυσμα $|v> \in \mathbb{C}^2$ να γράφεται ως $|v>= \alpha|0> + \beta|1>$ για κάποιους συντελεστές $\alpha, \beta \in \mathbb{C}$. Αυτή ή βάση έχει ένα ιδιαίτερο όνομα και θα την ονομάσουμε τυπική βάση ή κανονική (standard basis).

Ορισμός 2.9. *Θεωρούμε τον 2-διάστατο μιγαδικό διανυσματικό χώρο $\mathbb{C}^2$. Η τυπική βάση ή αλλιώς βάση υπολογισμού (computational basis) , $\mathscr{S} = \{|0\rangle, |1\rangle\}$, είναι μια ορθοκανονική βάση του διανυσματικού χώρου, όπου τα διανύσματα βάσης είναι*

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ και } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ορισμός 2.10. *Η βάση Hadamard είναι μια ορθοκανονική βάση, $\mathscr{H} = \{|+\rangle, |-\rangle\}$, που αποτελείται από δύο στοιχεία βάσης,*

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{και } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Πολλαπλά qubits

Αν έχουμε δύο κλασσικά bits τα γράφουμε ως $"00", "01"$ κτλ. Όταν έχουμε δύο qubits όμως τα πράγματα αλλάζουν. Θα αντιστοιχίσουμε λοιπόν τα δύο κλασσικά bits έστω $x_1, x_2 \in \{0,1\}^2$ με ένα διάνυσμα. Έστω A το πρώτο qubit και B το δεύτερο. Θα αντιστοιχίσουμε λοιπόν τις ακολουθίες σε ορθοκανονικά διανύσματα ως εξής

$$0_A 0_B \to |00\rangle_{AB} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad 0_A 1_B \to |01\rangle_{AB} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$1_A 0_B \to |10\rangle_{AB} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad 1_A 1_B \to |11\rangle_{AB} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Για δυαδικές ακολουθίες τώρα μήκους n, θεωρούμε τον διανυσματικό χώρο $\mathbb{C}^{2^n}$, όπου κάθε συντεταγμένη αναπαρίσταται από μια ακολουθία $x = x_1, \ldots, x_n$. Υπάρχουν $d = 2^n$ τέτοιες ακολουθίες λοιπόν, οπότε μπορούμε να αναπαραστήσουμε κάθε ακολουθία x με έναν διαφορετικό ακέραιο $i \in [1, d]$. Μπορούμε να εκφράσουμε λοιπόν την ακολουθία x ως ένα διάνυσμα $|x>$ το οποίο είναι 0 παντού, εκτός από τη θέση i. Έχουμε λοιπόν τον παρακάτω ορισμό.

Ορισμός 2.11. *Έστω ο χώρος καταστάσεων των n qubits $\mathbb{C}^d$, όπου $d = 2^n$. Για κάθε διακεκριμένη ακολουθία $x \in \{0,1\}^n$ συσχετίζουμε το x με ένα διακεκριμένο ακέραιο $i \in \{1, 2, \ldots, d\}$. Η τυπική βάση για τον $\mathbb{C}^d$ είναι μια ορθοκανονική βάση που δίνεται από $\mathscr{S}_n = \{|x\rangle\}_{x \in \{0,1\}^n}$, όπου $|x>$, τα $d-$διάστατα διανύσματα*

$$|x\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \to i \text{ ι-οστή θέση}$$

Ορισμός 2.12. *Μια $n-$qubit κατάσταση $|\psi> \in \mathbb{C}^d$ με $d = 2^n$ μπορεί να γραφεί ως υπέρθεση των στοιχείων της τυπικής βάσης*

$$|\psi\rangle = \sum_{x_\mathrm{J}} \alpha_i |i\rangle, \quad \text{όπου } \forall i, \alpha_i \in \mathbb{C} \text{ και } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1$$

Τανυστικό γινόμενο

Έστω δύο qubits A, B, με κατάσταση $|\psi>_A$ και $|\phi>_B$ αντίστοιχα

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}$$

$$|\phi\rangle_B = \alpha_B|0\rangle_B + \beta_B|1\rangle_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix}$$

Η αρθρωτή κατάσταση $|\psi\rangle_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$, μπορεί να εκφραστεί ως το τανυστικό γινόμενο των $|\psi >_A$ και $|\phi >_B$

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi\rangle_B = \begin{pmatrix} \alpha_A|\psi\rangle_B \\ \beta_A|\psi\rangle_B \end{pmatrix} = \begin{pmatrix} \alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B \end{pmatrix}$$

Ο γενικός ορισμός του τανυστικού γινομένου δύο διανυσμάτων είναι ο εξής

Ορισμός 2.13. *Δοθέντος δύο διανυσμάτων $|\psi_1\rangle \in \mathbb{C}^{d_1}$ και $|\psi_2\rangle \in \mathbb{C}^{d_2}$, το τανυστικό γινόμενο δίνεται από*

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 |\psi_2\rangle \\ \vdots \\ \alpha_d |\psi_2\rangle \end{pmatrix}$$

όπου $|\psi_1\rangle \otimes |\psi_2\rangle$ βρίσκεται στο χώρο καταστάσεων $\mathbb{C}^{d_1} \times \mathbb{C}^{d_2}$.

Πρόταση 2.14. *Το τανυστικό γινόμενο έχει τις εξής ιδιότητες*

- *Επιμεριστική:* $|\psi_1\rangle \otimes (|\psi_2\rangle + |\psi_3\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi_3\rangle$
- *Προσεταιριστική:* $|\psi_1\rangle \otimes (|\psi_2\rangle \otimes |\psi_3\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) \otimes |\psi_3\rangle$
- *Μη αντιμεταθετική:* $|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle$ *εκτός αν* $|\psi_1 >= |\psi_2 >$

Πώς μετράμε ένα qubit;

Οι κβαντικές μετρήσεις μας δίνουν πιθανοκρατικά αποτελέσματα, δείχνοντάς μας ότι η κβαντική πληροφορία διαφέρει ριζικά από τη κλασική.

Έστω ένα qubit με κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ όπου a, b είναι μιγαδικοί αριθμοί. Κατά τη μέτρηση του qubit, λαμβάνουμε ως αποτέλεσμα 0 με πιθανότητα p_0 και 1 με πιθανότητα p_1. Αυτές οι πιθανότητες μπορούν να καθοριστούν υπολογίζοντας τα εσωτερικά γινόμενα

$$p_0 = |\langle\psi|0\rangle|^2 = \left| \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right|^2 = |\alpha|^2$$
$$p_1 = |\langle\psi|1\rangle|^2 = \left| \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right|^2 = |\beta|^2$$

Παρατηρούμε κιόλας ότι το $|a|^2 + |\beta|^2 = 1$ καταλήγει ότι $p_0 + p_1 = 1$, ότι το άθροισμα των πιθανότητων του να βρεις 0 ή 1 αθροίζονται στη μονάδα.

Ορισμός 2.15. *Αν υποθέσουμε ότι μετράμε μια κβαντική κατάσταση $|\psi>$, στην ορθοκανονική βάση $\{|b_j\rangle\}_{j=1}^{d}$. Η πιθανότητα να παρατηρήσουμε το αποτέλεσμα "b_j" βρίσκεται υπολογίζοντας το*

$$p_j = |\langle b_j|\psi\rangle|^2$$

Η κατάσταση μετά τη μέτρηση όταν θα έχουμε ως αποτέλεσμα το b_j είναι $|b_j>$.

Μετασχηματισμοί σε qubits

Όπως και στα κλασσικά bits, μπορούμε να εφαρμόσουμε πράξεις και στα qubits.

Ορισμός 2.16. *Ο ταυτοτικός πίνακας $\mathbb{I}$ είναι πίνακας διαγώνιος και τετραγωνικός όπου κάθε διαγώνιο στοιχείο είναι μονάδα, δηλαδή*

$$\mathbb{I} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Ο ταυτοτικός πίνακας είναι μια ταυτοτική[i] (unitary) πράξη που διατηρεί όλες τις κβαντικές καταστάσεις, δηλαδή για κάθε κβαντική κατάσταση $|\psi\rangle$, $\mathbb{I}|\psi\rangle = |\psi\rangle$.

Ορισμός 2.17. *Έστω ο πίνακας*

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

Ο πίνακας H καλείται μετασχηματισμός Hadamard και μετατρέπει την υπολογιστική βάση $\{|0\rangle, |1\rangle\}$ σε μια βάση Hadamard $\{|+\rangle, |-\rangle\}$.

Ορισμός 2.18. *Για κάθε $\theta \in \mathbb{R}$, θεωρούμε το πίνακα*

$$R(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

Ο μετασχηματισμός R καλείται πίνακας αλλαγής φάσης. Όταν δρα στην υπολογιστική βάση έχουμε,

$$R(\theta)|0\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}$$
$$R(\theta)|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix}$$

και για $\theta = \frac{\pi}{2}$, έχουμε

$$R\left(\frac{\pi}{2}\right)|0\rangle = |+\rangle \quad \textit{και} \quad R\left(\frac{\pi}{2}\right)|1\rangle = -|-\rangle$$

[i] Ένας τελεστής U λέγεται ταυτοτικός αν $U^\dagger U = UU^\dagger = \mathbb{I}$

Μερικοί ακόμα χρήσιμοι μετασχηματισμοί στη φυσική, όπως και στη κβαντική υπολογιστική είναι οι πίνακες Pauli, X, Y, Z. Είναι ορθογώνιοι 2×2 πίνακες, με την ακόλουθη μορφή

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$Y = iXZ$$

Ο πίνακας Pauli-X δρα στη τυπική βάση αλλάζοντας τα διανύσματα,

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Αυτή η διαδικασία ονομάζεται συχνά και bit flip διαδικασία διότι αλλάζει το 0 σε 1 και αντίστροφα.

Ο πίνακας Pauli-Z όταν δρα στη τυπική βάση, προσθέτει ένα phase flip,

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = |-1\rangle$$

Επίσης ο πίνακας Pauli αλλάζει τα διανύσματα $|+>, |->$,

$$Z|+\rangle = Z(|0\rangle + |1\rangle)/\sqrt{2} = (Z|0\rangle + Z|1\rangle)/\sqrt{2} = (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle$$

Άρα παρατηρούμε ότι ο Z δρα ως bit flip στη βάση Hadamard και ως phase flip στη τυπική βάση.

Τέλος, ο Pauli-Y όταν δρα στα διανύσματα της τυπικής βάσης, δρα και ως bit και ως phase flip,

$$Y|0\rangle = iXZ|0\rangle = iX|0\rangle = i|1\rangle$$
$$Y|1\rangle = -iXZ|0\rangle = -iX|1\rangle = -i|0\rangle$$

Στους κβαντικούς υπολογιστές μονάδα πληροφορίας είναι το κβαντικό bit (quantum bit) το οποίο για συντομία γράφεται ως qubit. Το qubit είναι ένα κβαντικό σύστημα δύο καταστάσεων.Οι δύο βασικές καταστάσεις του qubit συμβολίζονται με $|0>$ και $|1>$ αντίστοιχα.

Τέλος, αξίζει να αναφέρουμε μια ιδιαιτερότητα των qubits σε σχέση με τα κλασικά. Δεν μπορούν να αντιγραφούν! Έστω ότι μπορούμε να αντιγράψουμε ένα qubit με ένα ορθογώνιο μετασχηματισμό αντιγραφής, έστω C. Θα είχαμε λοιπόν $C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ για κάθε qubit $|\psi>$. Πιο συγκεκριμένα, έχουμε

$$\begin{aligned} \langle\psi_1|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle \langle 0|0\rangle \\ &= \left(\langle\psi_1| \otimes \langle 0|\right) C^\dagger C \left(|\psi_2\rangle \otimes |0\rangle\right) \\ &= \left(\langle\psi_1| \otimes \langle\psi_1|\right) \left(|\psi_2\rangle \otimes |\psi_2\rangle\right) = \left(\langle\psi_1|\psi_2\rangle\right)^2 \end{aligned}$$

Από τη στιγμή που ο C είναι ορθογώνιος, έχουμε $C^\dagger C = \mathbb{I}$, άρα

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle\langle 0|0\rangle \\ &= \left(\langle\psi_1|\otimes\langle 0|\right)C^\dagger C\left(|\psi_2\rangle\otimes|0\rangle\right) \\ &= \left(\langle\psi_1|\otimes\langle\psi_1|\right)\left(|\psi_2\rangle\otimes|\psi_2\rangle\right) = \left(\langle\psi_1|\psi_2\rangle\right)^2\end{aligned}$$

Άρα όταν έχουμε $0 < |\langle\psi_1|\psi_2\rangle| < 1$, η παραπάνω σχέση δεν μπορεί να ισχύει συνεπώς ένας τέτοιος μετασχηματισμός δεν μπορεί να υπάρχει.

Η αδυναμία διακλάδωσης, δηλαδή η αδυναμία αντιγραφής των qubits που αναφέραμε προηγουμένως, αποτελεί τη βάση της κβαντικής κρυπτογραφίας με την οποία θα ασχοληθούμε στη συνέχεια και είναι το κυρίως θέμα της παρούσας διπλωματικής, μαζί με τον αιώνιο αντίπαλο της, τη μετα-κβαντική κρυπτογραφία.

Η αδυναμία αντιγραφής ισχύει μόνο για τη γενική περίπτωση που έχουμε ένα άγνωστο qubit (με άγνωστη κατάσταση). Αν το qubit βρίσκεται στην κατάσταση 0 ή στην κατάσταση 1 (στις βασικές καταστάσεις), τότε η αντιγραφή είναι δυνατή και ως πύλη αντιγραφής μπορεί να θεωρηθεί η πύλη $CNOT$ (με την προϋπόθεση βέβαια ότι το δεύτερο qubit θα είναι πάντα 0). Αυτό το γεγονός , χρησιμοποιείται στις τεχνικές διόρθωσης σφάλματος (quantum error correction).

Υπάρχουν αρκετά κβαντικά συστήματα δύο καταστάσεων τα οποία μπορούν να χρησιμοποιηθούν ως qubits.

- ◇ Η κατάσταση του spin ενός σωματιδίου με spin $(\pm\frac{1}{2})$ μπορεί να θεωρηθεί ως qubit, όπου η κατάσταση spin $+\frac{1}{2}$ αντιστοιχεί στην βασική κατάσταση $|0>$ και η κατάσταση spin $-\frac{1}{2}$ αντιστοιχεί στη βασική κατάσταση $|1>$.
- ◇ Η διεύθυνση πόλωσης ενός φωτονίου μπορεί να αναπαραστήσει ένα qubit, όπου η οριζόντια πόλωση αντιστοιχεί στην κατάσταση $|0>$ και η κάθετη πόλωση στην $|1>$.
- ◇ Δύο διακριτά ενεργειακά επίπεδα, E_0 και E_1, σε ένα άτομο ή σε μία κβαντική στιγμή όπου η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_1 αντιστοιχεί στην κατάσταση $|1>$ και η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_0 αντιστοιχεί στην κατάσταση $|0>$.
- ◇ Ο τρόπος ταλάντωσης δύο ιόντων που βρίσκονται μέσα σε μία παγίδα ιόντων.

Η τεχνολογία κατασκευής των κβαντικών υπολογιστών θα καθορίσει ποιο φυσικό κβαντικό σύστημα δύο καταστάσεων θα επιλεγεί για να αναπαραστήσει το qubit.

2.2.3 Σφαίρα Bloch

Για μοναδικά qubits, υπάρχει μια εικονική αναπαράσταση (σχήμα 2.7) την οποία ονομάζουμε σφαίρα Bloch. Εκφράζουμε το qubit ως

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

όπου γ, θ, ϕ είναι πραγματικοί αριθμοί. Ο όρος $e^{i\gamma}$, ο οποίος ονομάζεται γενικός όρος φάσης, δεν έχει εμφανή επίδραση στη πιθανότητα του αποτελέσματος κατά τη μέτρηση οπότε τον αγνοούμε. Θεωρούμε τις καταστάσεις

$$|\psi_1\rangle = e^{i\gamma_1}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\phi}\sin\tfrac{\theta}{2}|1\rangle\right)$$
$$|\psi_2\rangle = e^{i\gamma_2}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\phi}\sin\tfrac{\theta}{2}|1\rangle\right)$$

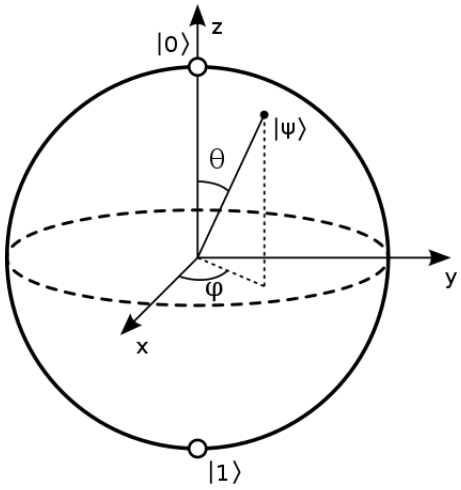
για κάποιους πραγματικούς αριθμούς γ_1, γ_2. Ας σημειώσουμε ότι $|\psi_1\rangle = e^{i(\gamma_1-\gamma_2)}|\psi_2\rangle$. Έτσι έχουμε για οποιαδήποτε μέτρηση σε σχέση με τη βάση $\{|b\rangle\}_b$, η πιθανότητα να πάρουμε ως αποτέλεσμα το b είναι ίση και για τις δύο καταστάσεις, καθώς

$$|\langle\psi_1|b\rangle|^2 = \langle b|\psi_1\rangle\langle\psi_1|b\rangle = e^{i(\gamma_1-\gamma_2)}e^{-i(\gamma_1-\gamma_2)}\langle b|\psi_2\rangle\langle\psi_2|b\rangle = |\langle\psi_2|b\rangle|^2$$

Ορισμός 2.19. *Η παραμετρικοποίηση (θ, ϕ) του*

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

καλείται αναπαράσταση κατά τη σφαίρα Bloch και ένα qubit μπορεί να περιγραφεί από ένα Bloch διάνυσμα $\vec{r} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.



Σχήμα 2.7: Αναπαράσταση ενός qubit μέσω της σφαίρας Bloch

2.3 Κβαντικά "εργαλεία"

Θα αναλύσουμε χρήσιμες μαθηματικές έννοιες και συμβολισμούς που θα βοηθήσουν στη κατανόηση της κβαντικής κρυπτογραφίας.

2.3.1 Πίνακες πυκνότητας

Πιθανότητες και συμβολισμοί

Έστω μια διακριτή τυχαία μεταβλητή X η οποία παίρνει τιμές από ένα αλφάβητο $\mathscr{X}$ μεγέθους n. Γράφουμε ως $P_X(\cdot)$ τη κατανομή της X και ως $|X|$ το μέγεθος του αλφαβήτου $\mathscr{X}$. Ο συμβολισμός P_X συμβολίζει την πιθανότητα η τυχαία μεταβλητή να πάρει ένα συγκεκριμένο σύμβολο $x \in \mathscr{X}$ ως τιμή της. Άλλοι συμβολισμοί είναι οι $p_x = p(x) = P(X = x) = P_X(x)$.

Πρόταση 2.20. *Οι ιδιότητες της κατανομής είναι*

- $\forall x \in \mathscr{X}, P_X(x) \geq 0.$
- $\sum_{x \in \mathscr{X}} P_X(x) = 1.$

Μια τυχαία μεταβλητή X μπορεί να συσχετιστεί με μια άλλη τυχαία μεταβλητή Y. Άρα αυτό σημαίνει ότι έχουν μια κοινή κατανομή $P_{XY}(x, y)$, η οποία δεν είναι αναγκαστικά γινόμενο, δηλαδή $P_{XY}(x, y) \neq P_X(x)P_Y(y)$ γενικά. Αυτό οδηγεί στο συμβολισμό των πιθανοτήτων υπό συνθήκη $P_{X|Y}(x|y)$, όπου $P_{X|Y}(x|y)$ είναι η πιθανότητα η X μεταβλητή να πάρει τη τιμή x, υπό συνθήκη με το γεγονός ότι η Y θα πάρει τη τιμή y.

Θα χρησιμοποιήσουμε το παρακάτω συμβολισμό

$$p_{x|y} = p(x|y) = P(X = x|Y = y) = P_{X|Y}(x|y)$$

Ορισμός 2.21. *Αφού $P_{XY}(x, y) = P_X(x)P_{Y|X}(y|x) = P_Y(y)P_{X|Y}(x|y)$, έχουμε*

$$P_{X|Y}(x|y) = \frac{P_{XY}(x, y)}{P_Y(y)}$$

όταν $P_Y(y) > 0$. Αυτό ονομάζεται κανόνας του Bayes και συνδέει τη πιθανότητα υπο συνθήκη με τις αρθρωτές πιθανότητες.

Πρέπει λοιπόν να βρούμε έναν γενικότερο φορμαλιστικό κανόνα με τον οποίο θα γράφουμε τις κβαντικές καταστάσεις και αυτό για δύο λόγους.

Πρώτον, ας υποθέσουμε ότι θέλουμε να γράψουμε τη κατάσταση ενός qubit μέσα από πολλά qubits και ας φανταστούμε ότι έχουμε δύο κβαντικά συστήματα A, B. Αυτά έχουν μια αρθρωτή κατάσταση $|\psi >_{AB}$, η οποία δεν γνωρίζουμε πάντα αν έχει προέλθει από απλό τανυστικό γινόμενο των δύο καταστάσεων $|\psi >_A, |\psi >_B$, ώστε να απομονώσουμε για το qubit A παραδείγματος χάριν την κατάσταση $|\psi >_A$. Μπορεί η $|\psi >_{AB}$, να έχει προέλθει από την υπέρθεση των τανυστικών γινομένων.

Δεύτερον, αν θέλουμε να κάνουμε μια μέτρηση για παράδειγμα, η οποία είναι μια πιθανοκρατική διαδικασία, προετοιμάζει τις διάφορες καταστάσεις με κάποια πιθανότητα. Οπότε αν θέλουμε να απομονώσουμε μια κατάσταση $|\psi >_i$ πρέπει να λάβουμε υπόψη και τη πιθανότητα της, p_i.

Ο μαθηματικός τρόπος και η λύση στα παραπάνω προβλήματα είναι να γράψουμε τη κβαντική κατάσταση $|\psi >$ ενός μόνο συστήματος ως ένα πίνακα $\rho = |\psi >< \psi|$, ο οποίος έχει τάξη 1 και ακριβώς μια μη-μηδενική ιδιοτιμή ($= 1$) με αντίστοιχη ιδιοκατάσταση $|\psi >$.

Γραφή μέσω πινάκων πυκνότητας

Ας υποθέσουμε ότι κάποιος προετοιμάζει δύο πιθανές καταστάσεις $|\psi >_1$ και $|\psi >_2$, με ίσες πιθανότητες $p_1 = p_2 = \frac{1}{2}$. Προφανώς, η υπέρθεση δεν είναι μια σωστή περιγραφή, διότι το σύστημα είναι ακριβώς σε μια από τις δύο καταστάσεις με πιθανότητα $\frac{1}{2}$. Μόνο αυτός που το προετοίμασε το ξέρει. Μπορούμε να γράψουμε χωρίς να ξέρουμε την ταυτότητα της κατάστασης, τη τελική κατάσταση; Ναι, περιγράφοντας το τελικό σύστημα ως μια μίξη ανάμεσα στις $|\psi >_1$ και $|\psi >_2$, με τύπο

$$\rho = \frac{1}{2} |\psi_1\rangle \left\langle \psi_1 \left| + \frac{1}{2} \right| \psi_2 \right\rangle \langle \psi_2|$$

Καλούμε λοιπόν τον πίνακα ρ, πίνακα πυκνότητας.

Γενικότερα, αν μια πηγή προετοιμάσει τη κατάσταση $|\psi_x >$, με πιθανότητα p_x, το τελικό σύστημα θα είναι στη κατάσταση

$$\rho = \sum_x p_x |\psi_x\rangle \langle \psi_x|$$

Έστω ότι μετράμε το σύστημα με την τυπική βάση. Αν το σύστημα είναι σε μια κατάσταση $|\psi_j >$, θα περιμέναμε τις πιθανότητες των αποτελεσμάτων να είναι

$$q_{0|j} = |\langle 0||\psi_j\rangle|^2 = \langle 0\|\psi_j\rangle \langle \psi_j\|0\rangle$$
$$q_{1|j} = |\langle 1||\psi_j\rangle|^2 = \langle 1\|\psi_j\rangle \langle \psi_j||1\rangle$$

Αν η κατάσταση $|\psi_j >$ έχει προετοιμαστεί με πιθανότητα p_j, τότε θα περιμέναμε οι πιθανότητες του αποτελέσματος να είναι

$$q_0 = \sum_j p_j q_{0|j}$$
$$q_1 = \sum_j p_j q_{1|j}$$

Αν επεκτείνουμε τον όρο q_0, με το φορμαλισμό του πίνακα πυκνότητας, θα έχουμε

$$q_0 = \sum_j p_j q_{0|j} = \sum_j p_j \langle 0\|\psi_j\rangle \langle \psi_j||0\rangle = \left\langle 0 \left| \left(\sum_j p_j |\psi_j\rangle \langle \psi_j| \right) \right| 0 \right\rangle = \langle 0|\rho|0\rangle$$

Άρα καταλήγουμε ότι ο πίνακας πυκνότητας αντικατοπτρίζει ακριβώς ότι περιμέναμε διαισθητικά για τις πιθανότητες των απολεσμάτων κατά τη μέτρηση.

Παρατήρηση: Δεν πρέπει να συγχέουμε την υπέρθεση και τη μίξη δύο κβαντικών καταστάσεων. Η μίξη γίνεται κλασσικά και είναι μια διαδικασία που προετοιμάζει τη μία ή την άλλη κατάσταση με κάποια πιθανότητα, ενώ η υπέρθεση μιας κατάστασης είναι και η μία και ή άλλη συγχρόνως.

Μια περίεργη ιδιότητα των πινάκων πυκνότητας, που δεν ισχύει στη περίπτωση των κλασσικών κατανομών πιθανότητας, είναι ότι ο ίδιος πίνακας πυκνότητας μπορεί να δημιουργηθεί από διαφορετικά σύνολα, επί παραδείγματι ο

$$\rho = \frac{\mathbb{I}}{2}$$

ο οποίος καλείται και μέγιστη μικτή κατάσταση (maximally mixed state) και ισχύει

$$\frac{\mathbb{I}}{2} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$$

Ιδιότητες των πινάκων πυκνότητας

Υπάρχουν δύο ιδιότητες τις οποίες πρέπει να τηρεί ένας πίνακας πυκνότητας ώστε να αναπαριστά μια έγκυρη κβαντική κατάσταση. Να είναι θετικά ημιορισμένος και το ίχνος του να είναι ίσο με 1.

Ορισμός 2.22. *Έστω ένα κβαντικό σύστημα με χώρο καταστάσεων $\mathbb{C}^d$, ένας πίνακας πυκνότητας συμβολικά ρ, είναι ένας γραμμικός τελεστής $\rho \in \mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^d\right)$, τέτοιος ώστε*

- $\rho \geq 0$
- $tr(\rho) = 1$

Αν $rank(\rho) = 1$, τότε ο ρ καλείται καθαρή κατάσταση (pure), αλλιώς μικτή (mixed).

Ορισμός 2.23. *Έστω ένα κβαντικό σύστημα σε κατάσταση ρ. Αν μετρήσουμε το ρ στη βάση $\{|b_j\rangle\}_j$, θα πάρουμε ως αποτέλεσμα το j με πιθανότητα*

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

Μπορούμε να γράψουμε κάθε πίνακα πυκνότητας ενός qubit ως

$$\rho = \frac{1}{2}\left(\mathbb{I} + v_x X + v_z Z + v_y Y\right)$$

όπου X, Y, Z οι πίνακες Pauli, και αν ο ρ είναι καθαρή κατάσταση, τότε το διάνυσμα $\vec{v} = (v_x, v_y, v_z)$, είναι ακριβώς το διάνυσμα Bloch, $\vec{r} = (\cos\phi \sin\theta, \sin\phi \sin\theta, \cos\theta)$.

Αν έχουμε δύο κβαντικά συστήματα A, B που περιγράφονται από τους πίνακες πυκνότητας ρ_A και ρ_B πώς γράφουμε την αρθρωτή κατάσταση ρ_{AB};

Για 2×2 πίνακες έχουμε

$$\rho_A \otimes \rho_B = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \otimes \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} = \begin{pmatrix} m_{11}\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} & m_{12}\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} \\ m_{21}\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} & m_{22}\begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} m_{11}n_{11} & m_{11}n_{12} & m_{12}n_{11} & m_{12}n_{12} \\ m_{11}n_{21} & m_{11}n_{22} & m_{12}n_{21} & m_{12}n_{22} \\ m_{21}n_{11} & m_{21}n_{12} & m_{22}n_{11} & m_{22}n_{12} \\ m_{21}n_{21} & m_{21}n_{22} & m_{22}n_{21} & m_{22}n_{22} \end{pmatrix}$$

Ορισμός 2.24. *Έστω ένας $d' \times d$ πίνακας ρ_A και $k' \times k$ πίνακας ρ_B*

$$\rho_A = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & \ddots & \ddots & m_{2d} \\ \vdots & \ddots & \ddots & \vdots \\ m_{d'1} & m_{d'2} & \cdots & m_{d'd} \end{pmatrix}, \quad \rho_B = \begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1k} \\ n_{21} & \ddots & \ddots & n_{2k} \\ \vdots & \ddots & \ddots & \vdots \\ n_{k'1} & n_{k'} & \cdots & n_{k'k} \end{pmatrix}$$

Το τανυστικό γινόμενο αυτών των πινάκων δίνεται από τον $d^{'}k^{'} \times dk$ πίνακα

$$\rho_{AB} = \rho_A \otimes \rho_B = \begin{pmatrix} m_{11}\rho_B & m_{12}\rho_B & \cdots & m_{1d}\rho_B \\ m_{21}\rho_B & \ddots & \ddots & m_{2d}\rho_B \\ \vdots & \ddots & \ddots & \vdots \\ m_{d'1}\rho_B & m_{d'^2\rho_B} & \cdots & m_{d'd}\rho_B \end{pmatrix}$$

Το γινόμενο αυτό είναι μη-αντιμεταθετικό.

Κλασικές καταστάσεις

Έστω ότι έχουμε μια κλασσική κατανομή πιθανότητας με σύμβολα από το αλφάβητο $\mathscr{X} = \{0, \ldots, d-1\}$ όπου p_x συμβολίζει την πιθανότητα του να παρατηρήσεις το σύμβολο ξ. Αν ταυτοποιήσουμε τα κλασσικά bits με στοιχεία της τυπικής βάσης $\{|0\rangle, \ldots, |d-1\rangle\}$, μπορούμε να εκφράσουμε κάθε πιθανή κατάσταση $|x>$ με πιθανότητα p_x μέσω της μίξης

$$\rho = \sum_{x=0}^{d-1} p_x |x\rangle\langle x|$$

Ορισμός 2.25. *Έστω ένα σύστημα X με χώρο καταστάσεων $\mathbb{C}^d$, και έστω $\{|x\rangle\}_{x=0}^{d-1}$ να συμβολίζει τη τυπική βάση για το $\mathbb{C}^d$. Ένα σύστημα X είναι σε κλασική κατάσταση, ή $c-state$ (classical state), όταν ο αντίστοιχος πίνακας πυκνότητας ρ_x είναι διαγώνιος στη τυπική βάση του x καταστάσεων του X, δηλαδή ο ρ_x έχει τη μορφή*

$$\rho = \sum_{x=0}^{d-1} p_x |x\rangle\langle x|$$

όπου $\{p_x\}_{x=0}^{d-1}$ είναι κάθε κανονικοποιημένη κατανομή πιθανότητας.

Ορισμός 2.26. *Μια κλασική κβαντική κατάσταση, ή αλλιώς $cq-state$ έχει τη μορφή*

$$\rho_{XQ} = \sum p_x |x\rangle \left\langle x\right|_X \otimes \rho_x^Q$$

Αποτελείται από ένα κλασικό καταχωρητή X και ένα κβαντικό καταχωρητή Q.

2.4 Γενικές μετρήσεις

Μέχρι στιγμής μετρούσαμε κβαντικές καταστάσεις σε μια δοσμένη βάση. Η Κβαντομηχανική μας επιτρέπει μια εκλεπτυσμένη έννοια του όρου μέτρηση, η οποία θα παίξει σημαντικό ρόλο στη κβαντική θεωρία πληροφορίας και τη κβαντική κρυπτογραφία.

2.4.1 POVMs

Αν μας ενδιαφέρουν μόνο οι πιθανότητες ως αποτέλεσμα της μέτρησης, αλλά όχι τι συμβαίνει μετά τη μέτρηση, η πιο γενική μέθοδος μέτρησης μπορεί να περιγραφεί από έναν θετικό τελεστή-μετρητή που καλείται POVM (positive operator-valued measure).

Ορισμός 2.27. *Ένα POVM στο $\mathbb{C}^d$ είναι ένα σύνολο από θετικά ημιορισμένους τελεστές $\{M_x\}_{x\in\mathscr{X}}$ τέτοιοι ώστε*

$$\sum_x M_x = \mathbb{I}_{\mathbb{C}^d}$$

Το μικρό x είναι σαν μια ταμπέλα για το αποτέλεσμα της μέτρησης. Η πιθανότητα p_x του να παρατηρήσεις το αποτέλεσμα x μπορεί να εκφραστεί μέσω του κανόνα του Born ως

$$p_x = \mathrm{tr}\left(M_x\rho\right)$$

Ύστερα από μια μέτρηση σε μια κβαντική κατάσταση, με μια βάση, η κατάσταση πέφτει στο στοιχείο της βάσης που σχετίζεται με το αποτέλεσμα της μέτρησης. Στη περίπτωση του POVM, προκύπτει ότι η πληροφορία που δίνεται από τους τελεστές $\{M_x\}$ δεν είναι επαρκής ώστε να καθορίσει πλήρως την κατάσταση μετά τη μέτρηση. Διαισθητικά, ο λόγος είναι ότι μια τέτοια μέτρηση μπορεί να μη ρίξει ολόκληρη τη κατάσταση (δηλαδή η μετά τη μέτρηση κατάσταση να μην είναι pure), οπότε ως συνέπεια έχουμε τη δυνατότητα να εφαρμόσουμε έναν τυχαίο ορθογώνιο τελεστή στη κατάσταση μετά τη μέτρηση, χωρίς να επηρεάσουμε τις πιθανότητες.

Για να καθορίσουμε τις καταστάσεις μετά τη μέτρηση, χρειαζόμαστε την αναπαράσταση του POVM μέσω των τελεστών Kraus.

Ορισμός 2.28. *Έστω $M = \{M_x\}$ ένα δοσμένο POVM στο $\mathbb{C}^d$. Η αναπαράσταση κατά Kraus του M είναι ένα σύνολο από γραμμικούς τελεστές $A_x \in \mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$, τέτοιο ώστε $M_x = A_x^\dagger A_x$ για όλα τα x.*

Δεν υπάρχει μοναδική Kraus αναπαράσταση για ένα δοσμένο POVM.

Η πιο γενική μορφή ώστε να γράψουμε μια κβαντική μέτρηση είναι μέσω ολόκληρου του συνόλου των Kraus τελεστών $\{A_x\}_x$. Από αυτούς μπορούμε εύκολα να βρούμε τους POVM τελεστές ως $M_x = A_x^\dagger A_x$, αλλά και να υπολογίσουμε και τις καταστάσεις μετά τη μέτρηση.

Ορισμός 2.29. *Έστω ρ ένας πίνακας πυκνότητας και $\{M_x\}$ ένα POVM με Kraus ανάλυση που δίνεται από τους τελεστές $\{A_x\}$. Ας υποθέσουμε ότι η μέτρηση έχει προκατασκευαστεί και παίρνουμε ως αποτέλεσμα x. Τότε η κατάσταση του συστήματος μετά τη μέτρηση, συναρτήσει του αποτελέσματος x, είναι*

$$\rho_{|x} = \frac{A_x\rho A_x^\dagger}{\mathrm{tr}\left(A_x^\dagger A_x\rho\right)}$$

Ορισμός 2.30. *Μια προβολική μέτρηση (projective measurement), ή αλλιώς von Neumann μέτρηση, δίνεται από το σύνολο των ορθογώνιων τελεστών $M_x = \Pi_x$ τέτοιο ώστε $\sum_x \Pi_x = \mathbb{I}$. Η πιθανότητα q_x, του να παρατηρήσεις το αποτέλεσμα x κατά τη μέτρηση, είναι*

$$q_x = \mathrm{tr}\left(\Pi_x \rho\right)$$

και οι καταστάσεις μετά τη μέτρηση είναι

$$\rho_{|x} = \frac{\Pi_x \rho \Pi_x}{\mathrm{tr}\left(\Pi_x \rho\right)}$$

2.4.2 Μερικό ίχνος

Έστω ρ_{AB} ο πίνακας πυκνότητας σε ένα διανυσματικό χώρο τανυστικού γινομένου, $\mathbb{C}_A^{d_A} \otimes \mathbb{C}_B^{d_B}$, αλλά ας υποθέσουμε ότι η Αλίκη κρατά το κομμάτι του ρ που αντιστοιχεί στο σύστημα A και ο B κρατά το κομμάτι ρ που αντιστοιχεί στο σύστημα B. Πώς θα περιγράψουμε τη κατάσταση ρ_A του συστήματος της Αλίκης; Η διαδικασία με την οποία λαμβάνουμε το ρ_A από το ρ_{AB} λέγεται μερικό ίχνος (partial trace).

Ορισμός 2.31. *Ας θεωρήσούμε μια γενική κατάσταση*

$$\rho_{AB} = \sum_{ijk\ell} \gamma_{ij}^{k\ell} |i><j|_A \otimes |k><\ell|_B$$

όπου $|i\rangle_A, |j\rangle_A$ και $|k\rangle_B, |\ell\rangle_B$, "τρέχουν" σε ορθοκανονικές βάσεις των A και B αντίστοιχα. Τότε το μερικό ίχνος ως προς το B ορίζεται ως

$$\rho_A = \mathrm{tr}_B\left(\rho_{AB}\right) = \sum_{ijk\ell} \gamma_{ij}^{k\ell} |i\rangle \left\langle j \right| \otimes \mathrm{tr}(|k\rangle\langle\ell|) = \sum_{ij} \left(\sum_k \gamma_{ij}^{kk} \right) \left| i \right\rangle \langle j|$$

και ως προς το A αντίστοιχα

$$\rho_B = \mathrm{tr}_A\left(\rho_{AB}\right) = \sum_{ijk\ell} \gamma_{ij}^{k\ell} \mathrm{tr}(|i\rangle\langle j|) \otimes |k\rangle \left\langle \ell \right| = \sum_{k\ell} \left(\sum_j \gamma_{jj}^{k\ell} \right) \left| k \right\rangle \langle \ell|$$

Οι καταστάσεις ρ_A, ρ_B χαρακτηρίζονται και ως μειωμένες κατάστασεις (reduced states).

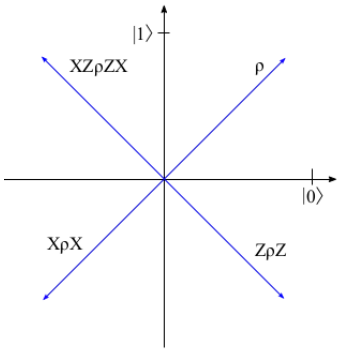
2.4.3 Το κβαντικό one-time pad

Για να κρυπτογραφήσουμε ένα qubit, θέλουμε δύο bits κλειδιού k_1, k_2. Η ιδιομορφία-πλεονέκτημα του κβαντικού OTP είναι να εφαρμόσουμε ένα bit flip και στις δύο βάσεις και τη τυπική και τη Hadamard βάση. Αυτό μπορεί να επιτευχθεί αν εφαρμόσουμε το $X^{k_1} Z^{k_2}$. Όταν τα k_1, k_2 έχουν διαλεχτεί τυχαία, ένα τυχαίο qubit ρ κρυπτογραφείται ως

$$\frac{1}{4} \sum_{k_1, k_2 \in \{0,1\}} X^{k_1} Z^{k_2} \rho Z^{k_2} X^{k_1}$$

Από τη στιγμή που μπορούμε να γράψουμε κάθε μοναδικού qubit τη κατάσταση ως

$$\rho = \frac{1}{2}\left(\mathbb{I} + v_x X + v_y Y + v_z Z\right)$$



Σχήμα 2.8: Ένα qubit κωδικοποιημένο από δύο bits κλειδιού: οι τελεστές $\mathbb{I}, X, Z, XZ$ εφαρμόζονται στο qubit με ίση πιθανότητα. Το αποτέλεσμα είναι μια μίξη όλων των καταστάσεων, την οποία ονομάζουμε maximally mixed state και αναπαρίσταται από την αρχή των αξόνων

έχουμε

$$\frac{1}{4}\sum_{k_1,k_2} X^{k_1}Z^{k_2}\rho Z^{k_2}X^{k_1} = \frac{\mathbb{I}}{2}$$

Για κάποιον που δεν ξέρει τα k_1, k_2, η τελική κατάσταση είναι τελείως ανεξάρτητη της εισόδου ρ.

Ορισμός 2.32. *Πρωτόκολλο. Το κβαντικό OTP είναι ένα σχήμα κρυπτογράφησης για qubits. Για την κρυπτογράφηση, η Αλίκη εφαρμόζει το $X^{k_1}Z^{k_2}$ στο qubit ρ και στέλνει τη κατάσταση στον Bob. Για την αποκρυπτογράφηση, ο Bob εφαρμόζει το αντίστροφο $\left(X^{k_1}Z^{k_2}\right)^\dagger$, για να πάρει το ρ.*

Για να κρυπτογραφήσουμε n qubits, χρειαζόμαστε 2^n bits κλασικού κλειδιού.

2.5 Η βαρύτητα της διεμπλοκής

Θα ορίσουμε τον όρο της διεμπλοκής πιο φορμαλιστικά και θα εξερευνήσουμε μερικούς από τους λόγους για τους οποίους η διεμπλοκή είναι τόσο σημαντική στη κβαντική θεωρία πληροφορίας.

2.5.1 Διεμπλοκή

Ορισμός 2.33. *Έστω δύο κβαντικά συστήματα A και B. Η αρθρωτή κατάσταση ρ_{AB} είναι διαχωρίσιμη αν υπάρχει μια κατανομή πιθανότητας $\{\rho_i\}_i$, και συνόλα πινάκων πυκνότητας, $\left\{\rho_i^A\right\}_i, \left\{\rho_i^B\right\}_i$ τέτοιο ώστε*

$$\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$$

Αν δεν υπάρχει τέτοιου είδους ανάλυση, η ρ_{AB} καλείται διεμπλεκόμενη (entagled). Αν $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$, είναι μια καθαρή κατάσταση, η $|\Psi>_{AB}$ είναι διαχωρίσιμη αν υπάρχουν $|\Psi>_A, |\Psi>_B$, τέτοια ώστε

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$$

2.5.2 Purifications

Ακόμα και αν η κατάσταση ενός μεγαλύτερου συστήματος είναι καθαρή, η μειωμένη κατάσταση μπορεί μερικές φορές να είναι mixed. Ας υποθέσουμε ότι έχουμε έναν πίνακα πυκνότητας ρ_A που περιγράφει μια κβαντική κατάσταση σε ένα σύστημα A. Είναι πάντα δυνατό να βρούμε μια καθαρή κατάσταση $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ τέτοια ώστε $tr(\rho_{AB}) = \rho_A$;

Ορισμός 2.34. *Δοθέντος ενός οποιοσδήποτε πίνακα πυκνότητας ρ_A, μια καθαρή κατάσταση $|\Psi_{AB} >$ είναι ένα purification του A αν* $\mathrm{tr}_B(|\Psi\rangle\langle\Psi|_{AB}) = \rho_A$

Πώς μπορεί ένας τυχαίος πίνακας πυκνότητας ρ_A να γίνει purified;
Αρχικά θα διαγωνοποιήσουμε τον ρ_A, εκφράζοντάς τον ως μια μίξη

$$\rho_A = \sum_{j=1}^{d_A} \lambda_j \, |\phi_j\rangle \, \langle\phi_j|$$

όπου λ_j οι ιδιοτιμές του ρ_A (οπωσδήποτε μη αρνητικές) και $|\phi_j >$ οι αντίστοιχες ιδιοκαταστάσεις.

Ο ρ_A περιγράφει ένα κβαντικό σύστημα το οποίο είναι σε μια πιθανοκρατική μίξη του να είναι στη κατάσταση $|\phi_j >$ με πιθανότητα λ_j. Το πώς ελέγχεται ποιό κομμάτι του A είναι σε αυτή τη μίξη παρουσιάζεται παρακάτω:

Ας εισάγουμε ένα φανταστικό σύστημα B το οποίο επιτυγχάνει ακριβώς αυτό. Έστω $\{|j\rangle_B\}_{j\in\{1,\ldots,d_B\}}$, να είναι η τυπική βάση για το σύστημα B με διάσταση $d_B = d_A$ και ας θεωρήσουμε τη καθαρή βάση

$$|\Psi\rangle_{AB} = \sum_{j=1}^{d_A} \sqrt{\lambda_j \, |\phi_j\rangle_A \otimes |j\rangle_B}$$

όπου $\{|j\rangle_B\}_j$ η τυπική βάση του συστήματος B.

Ας υποθέσουμε ότι θέλουμε να μετρήσουμε το B σύστημα της $|\Psi >_{AB}$ με τη τυπική βάση. Ξέρουμε ότι θα πάρουμε το αποτέλεσμα j με πιθανότητα $\langle\Psi|_{AB} M_j |\Psi\rangle_{AB}$, όπου $M_j = \mathbb{I}_A \otimes |j\rangle\langle j|_B$, που αυτό είναι ίσο με το λ_j. Αφού χρησιμοποιήσουμε μια προβολική μέτρηση, μπορούμε να περιγράψουμε τη κατάσταση μετά τη μέτρηση εύκολα ανάλογα με το $M_j|\Psi\rangle \langle\Psi|_{AB} M_j$ και κοιτώντας το σύστημα A μόνο να βρούμε ότι αυτό είναι το $|\phi_j\rangle \langle\phi_j|_A$.

Συνοψίζοντας, μια μέτρηση του συστήματος B θα δώσει αποτέλεσμα j με πιθανότητα λ_j και η κατάσταση μετά τη μέτρηση στο A είναι ακριβώς $|\phi_j\rangle \langle\phi_j|$.

Αυτό συνεπάγεται ότι $\mathrm{Tr}_B(|\Psi\rangle \langle\Psi|_{AB}) = \rho_A$.

Είναι τα purifications μοναδικά; Φαίνεται ότι έχουμε την επιλογή τουλάχιστον να διαλέξουμε σε ποιά βάση θα μετρήσουμε το σύστημα B, οπότε υπάρχει ένας βαθμός ελευθερίας.

Ανάλυση Schmidt

Θεώρημα 2.35. *Έστω δύο κβαντικά συστήματα A, B με διαστάσεις d_A, d_B αντίστοιχα, και έστω $d = min(d_A, d_B)$. Κάθε καθαρή διμελής κατάσταση $|\Psi>_{AB}$ έχει μια Schmidt ανάλυση*

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{\lambda_i} |u_i\rangle_A |v_i\rangle_B$$

όπου $\lambda_i \geq 0$ και $\{|u_i\rangle_A\}_i, \{|v_i\rangle_B\}_i$ ορθοκανονικά σύνολα διανυσμάτων. Οι συντελεστές $\sqrt{\lambda_i}$ καλούνται Schmidt συντελεστές και τα $|u_i\rangle_A, |v_i\rangle_B$ Schmidt διανύσματα.

Δύο συνέπειες της Schmidt ανάλυσης

1. Δοθέντος δύο πινάκων πυκνότητας ρ_A και ρ_B υπάρχει καθαρή διμελής κατάσταση $|\Psi>_{AB}$ τέτοια ώστε $\rho_A = \sum_i \lambda_i |u_i\rangle \langle u_i|_A$, και $\rho_B = \sum_i \lambda_i |v_i\rangle \langle v_i|_B$, αvv ρ_A και ρ_B έχουν το ίδιο φάσμα.

2. Μας παρέχει ένα τρόπο ώστε να μετράμε τη διεμπλοκή ανάμεσα στα συστήματα A, B σε μια καθαρή κατάσταση $|\Psi>_{AB}$. Αυτό επιτυγχάνεται μέσω της βαθμίδας Schmidt (Schmidt rank).

Ορισμός 2.36. *Για κάθε διμελή καθαρή κατάσταση με Schmidt ανάλυση $|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{\lambda_i} |a_i\rangle_A |b_i\rangle_B$, η Schmidt βαθμίδα ορίζεται ως ο αριθμός των μη-μηδενικών συντελεστών $\sqrt{\lambda_i}$. Είναι επίσης ίση με τα $rank(\rho_A)$ και $rank(\rho_B)$.*

Όπως αναφέραμε και παραπάνω, έχουμε έναν βαθμό ελευθερίας όσον αφορά την επιλογή του purification ενός πίνακα πυκνότητας. Είδαμε ότι έχουμε έναν unitary βαθμό ελευθερίας διαλέγοντας μια βάση στο purifying σύστημα B. Το παρακάτω θεώρημα μας εξασφαλίζει ότι αυτός είναι ακριβώς ο μοναδικός βαθμός ελευθερίας που έχουμε.

Θεώρημα 2.37. *Έστω ότι έχουμε έναν πίνακα πυκνότητας ρ_A και ένα purification του A που δίνεται από την $|\Psi>_{AB}$. Τότε μια άλλη κατάσταση $|\Phi>_{AB}$ είναι επίσης purification του A αvv υπάρχει ένας ορθογώνιος U_B τέτοιος ώστε*

$$|\Phi\rangle_{AB} = \mathbb{I}_A \otimes U_B |\psi\rangle_{AB}$$

2.5.3 Διαμοιρασμός μυστικού

Έστω ότι δίνουμε στην Αλίκη και τον Bob τυχαία μιας από τις εξής 4 καταστάσεις

$$|\psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}), \quad |\psi_{01}\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} - |11\rangle_{AB})$$
$$|\psi_{10}\rangle_{AB} = \frac{1}{\sqrt{2}} (|01\rangle_{AB} + |10\rangle_{AB}), \quad |\psi_{11}\rangle_{AB} = \frac{1}{\sqrt{2}} (|01\rangle_{AB} - |10\rangle_{AB})$$

Αυτές οι καταστάσεις ονομάζονται καταστάσεις Bell. Είναι ορθοκανονικές και σχηματίζουν μια βάση για τον $\mathbb{C}^2 \otimes \mathbb{C}^2$. Υπολογίσαμε ήδη το μειωμένο πίνακα πυκνότητας για το σύστημα της Αλίκης για μια από αυτές τις καταστάσεις, το EPR ζευγάρι, $|\psi_{00}>_{AB}$.

$$\begin{aligned}\rho_{00}^{A} =& \operatorname{tr}_B \left(|\psi_{00}\rangle \langle \psi_{00}|_{AB} \right) \\ =& \frac{1}{2} \left(|0\rangle \langle 0|_A \operatorname{tr}_B \left(|0\rangle \langle 0|_B \right) + |0\rangle \langle 1|_A \operatorname{tr}_B \left(|0\rangle \langle 1|_B \right) \right. \\ & \left. + |1\rangle \langle 0|_A \operatorname{tr}_B \left(|1\rangle \langle 0|_B \right) + |1\rangle \langle 1|_A \operatorname{tr}_B \left(|1\rangle \langle 1|_B \right) \right) \\ =& \frac{1}{2} \left(|0\rangle \langle 0|_A + |1\rangle \langle 1|_A \right) = \frac{\mathbb{I}_A}{2}\end{aligned}$$

Υπολογίζοντας τις μειωμένες καταστάσεις είτε στο A είτε στο B για κάθε μια από τις καταστάσεις πάντα θα παίρνουμε το ίδιο αποτέλεσμα

$$\begin{aligned}\rho_{00}^{A} = \rho_{01}^{A} = \rho_{10}^{A} = \rho_{11}^{A} = \tfrac{\mathbb{I}}{2} \\ \rho_{00}^{B} = \rho_{01}^{B} = \rho_{10}^{B} = \rho_{11}^{B} = \tfrac{\mathbb{I}}{2}\end{aligned}$$

Από τη στιγμή που μια μειωμένη κατάσταση σε κάθε υποσύστημα, είναι μέγιστα μπλεγμένη (maximally mixed), ούτε η Αλίκη ούτε ο Bob μπορεί να κερδίσει κάποια πληροφορία σε ποιά από τις καταστάσεις $|\psi_{00}\rangle_{AB}, |\psi_{01}\rangle_{AB}, |\psi_{10}\rangle_{AB}, |\psi_{11}\rangle_{AB}$ έχουν ένα qubit. Παρόλα αυτά, από τη στιγμή που οι καταστάσεις αυτές μαζί δημιουργούν μια βάση, όταν η Αλίκη και ο Bob συναντηθούν μπορούν να κάνουν μια μέτρηση σε αυτή τη βάση η οποία θα ξεχωρίζει τέλεια σε ποια κατάσταση έχουν, δίνοντας δύο bits πληροφορίας.

Υπερπυκνή κωδικοποίηση

Ο σκοπός της πυκνής κωδικοποίησης dense coding είναι να στέλνουμε κλασικά bits πληροφορίας από την Αλίκη στον Bob κωδικοποιώντας τα σε μια κβαντική κατάσταση που είναι όσο το δυνατόν μικρότερη. Θα δούμε πώς μέσω της διεμπλοκής μπορούμε να στείλουμε δύο κλασικά bits μέσω ενός μόνο qubit.

Ας υποθέσουμε ότι η Αλίκη και ο Bob μοιράζονται τη κατάσταση $|\psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|00\rangle_{AB} + |11\rangle_{AB} \right)$ και ότι η Αλίκη εφαρμόζει έναν ορθογώνιο μετασχηματισμό στο qubit της, όπως θα δούμε παρακάτω, που εξαρτάται από ποιά bits $ab \in \{00, 01, 10, 11\}$ θέλει να στείλει στον Bob.

Κλασική Πληροφορία a, b	Τελεστής $X_4^a Z_4^b$	Τελική Αρθρωτή Κατάσταση
00	$\mathbb{I}_A$	$\frac{1}{\sqrt{2}}(\|00\rangle_{AB} + \|11\rangle_{AB}$
01	X_A	$\frac{1}{\sqrt{2}} \left(\|10\rangle_{AB} + \|01\rangle_{AB} \right)$
10	Z_A	$\frac{1}{\sqrt{2}}(\|00\rangle_{AB} - \|11\rangle_{AB}$
11	$-X_A Z_A$	$\frac{1}{\sqrt{2}}(\|01\rangle_{AB} - \|10\rangle_{AB}$

Η δεξιά στήλη του πίνακα είναι μια Bell βάση, οπότε αν στείλει η Αλίκη στον Bob το qubit της, μπορεί να κάνει μια μέτρηση ο Bob στη Bell βάση και να ανακτήσει τα δύο κλασικά bits πληροφορίας της Αλίκης.

2.5.4 Μη τοπικότητα του Bell

Η διεμπλοκή έχει πολλές αντι-διαισθητικές ιδιότητες. Η πιο σημαντική είναι ότι επιτρέπει συσχετισμούς μεταξύ δύο σωματιδίων - δύο qubits- που δεν μπορούν να αναπαραχθούν κλασικά. Το

πρώτο παράδειγμα τέτοιων συσχετισμών αποδείχτηκε από τον Bell $[46]$, ο οποίος έδειξε ότι οι προβλέψεις της κβαντικής θεωρίας δεν είναι συμβατές με καμία από τις κλασικές θεωρίες που ικανοποιούν μια φυσική έννοια της τοπικότητας (locality).

Ένας μοντέρνος τρόπος για να καταλάβουμε τη μη-τοπικότητα του Bell είναι τα λεγόμενα μη-τοπικά παιχνίδια $[47]$. Ας φανταστούμε ότι παίζουμε ένα παιχνίδι με δύο παίχτες, την Αλίκη και τον Bob. Η Αλίκη έχει το σύστημα A και ο Bob το B. Σε αυτό το παιχνίδι, θα κάνουμε ερωτήσεις στους δύο παίχτες και θα συλλέγουμε απαντήσεις. Τις ερωτήσεις θα τις συμβολίσουμε με x και y και τις απαντήσεις με a και b αντίστοιχα. Θα παίξουμε το παιχνίδι πολλές φορές, και σε κάθε γύρο θα διαλέγουμε τις ερωτήσεις με κάποια πιθανότητα $p(xy)$. Έχουμε κάποιους κανόνες όμως. Έχουμε ένα κατηγορούμενο $V(a,b|x,y)$, το οποίο λαμβάνει τη τιμή 1 αν οι a και b είναι απαντήσεις νίκης για τις αντίστοιχες ερωτήσεις x και y. Για να είμαστε δίκαιοι, η Αλίκη και ο Bob γνωρίζουν τους κανόνες που δίνονται από το $V(a,b|x,y)$ και τη κατανομή $p(xy)$. Μπορούν να συμφωνήσουν σε οποιαδήποτε στρατηγική πριν το παιχνίδι. Μόλις ξεκινήσουν όμως οι ερωτήσεις απαγορεύεται η μεταξύ τους επικοινωνία.

Μας ενδιαφέρει η πιθανότητα, η Αλίκη και ο Bob να νικήσουν το παιχνίδι, και να μεγιστοποιηθεί σύμφωνα με όλες τις πιθανές στρατηγικές, δηλαδή έχουμε

$$p_{\text{νικη}} = \max_{\text{στρατεγψ}} \sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y) p(a,b|x,y)$$

όπου $p(a,b|x,y)$ είναι η πιθανότητα η Αλίκη και ο Bob να παράγουν απαντήσεις a και b δοθέντος x και y σύμφωνα με την επιλεγμένη τους στρατηγική.

Τι εννοούμε όμως με τον όρο στρατηγική; Σε έναν κλασικό κόσμο, η Αλίκη και ο Bob μπορούν να έχουν μόνο κλασική στρατηγική. Μια ντετερμινιστική κλασική στρατηγική δίνεται απλά από συναρτήσεις $f_A(x) = a$ και $f_B(y) = b$, οι οποίες παίρνουν τις ερωτήσεις x, y και τις δίνουν στις απαντήσεις a, b. Έπειτα έχουμε $p(a,b|x,y) = 1$ όταν $a = f_A(x)$ και $b = f_B(y)$, και $p(a,b|x,y) = 0$ αλλιώς. Πιθανότατα, η Αλίκη και ο Bob χρησιμοποιούν μια τυχαιότητα μεταξύ τους. Αυτό είναι σαν να έχουμε μια ακολουθία r, την οποία μοιράζονται με πιθανότητα $p(r)$. Στη φυσική, το r, καλείται και κρυφή μεταβλητή (hidden variable), αλλά θα πάρουμε την πιο λειτουργική άποψη της κοινής τυχαιότητας. Σε μια στρατηγική με κοινή τυχαιότητα r λοιπόν, κλασικά η Αλίκη και ο Bob μπορούν να εφαρμόσουν συναρτήσεις: $a = f_A(x,r)$ και $b = f_B(y,r)$. Σε όρους πιθανοτήτων θα έχουμε $p(a,b|x,y,r) = 1$ αν $a = f_A(x,r)$ και $b = f_B(y,r)$ και $p(a,b|x,y,r) = 0$ αλλιώς. Αυτό μας δίνει,

$$p(a,b|x,y) = \sum_n p(r) p(a,b|x,y,r)$$

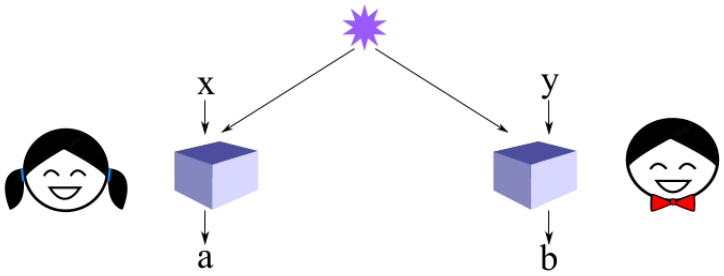
Το ερώτημα είναι αν βοηθάει η κοινή τυχαιότητα. Ας σημειώσουμε ότι για μια κλασική στρατηγική που βασίζεται σε κοινή τυχαιότητα έχουμε

$$\begin{aligned} p_{win} &= \max_{class.strat} \sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y) \sum_r p(r) p(a,b|x,y,r) \\ &= \max_{class.trat} \sum_r p(r) \left(\sum_{x,y} p(x,y) \sum_{a,b} V(a,b|x,y) p(a,b|x,y,r) \right) \end{aligned}$$

Η ποσότητα στις παρενθέσεις είναι μέγιστη για κάποιες συγκεκριμένες τιμές του r. Από τη στιγμή που θέλουν να μεγιστοποιήσουν την πιθανότητα να νικήσουν, η Αλίκη και ο Bob μπορούν να φτιάξουν το r με τέτοιο τρόπο που να τους δίνει μια ντετερμινιστική στρατηγική $a = f_A(x, r)$ και $b = f_A(y, r)$, όπου το r θα είναι σταθερό.

Γιατί όμως τα κάνουμε όλα αυτά; Αποδεικνύεται ότι, για πολλά παιχνίδια, μια κβαντική στρατηγική μπορεί να πετύχει μεγαλύτερη πιθανότητα για νίκη. Αυτό είναι θεμελιώδους σημασίας για τη κατανόηση της φύσης. Επίσης το να παρατηρείς υψηλή πιθανότητα νίκης είναι σημάδι διεμπλοκής: κβαντικά, η Αλίκη και ο Bob μπορούν να επιτύχουν υψηλότερη πιθανότητα νίκης μόνο αν είναι κατάσταση διεμπλοκής, κάνοντας αμέσως τα παιχνίδια τεστ ουσιαστικά διεμπλοκής.

Πιο συγκεκριμένα, μια κβαντική στρατηγική σημαίνει ότι η Αλίκη και ο Bob μπορούν να διαλέξουν μια κατάσταση ρ_{AB} να μοιραστούν, και να συμφωνήσουν στις μετρήσεις που θα πραγματοποιήσουν ανάλογα με τις αντίστοιχες ερωτήσεις. Δηλαδή, τα x και y θα επισημαίνουν μια επιλογή μέτρησης και τα a και b να είναι τα αποτελέσματα αυτής της μέτρησης.



Σχήμα 2.9: Ένα μη τοπικό παιχνίδι. Δίνουμε στην Αλίκη και τον Bob ερωτήσεις x και y, και πρέπει να μας γυρίσουν απαντήσεις a και b.Αν η Αλίκη και ο Bob είναι κβαντικοί, τότε τα x και y μας δείχνουν τις ρυθμίσεις της μέτρησης και τα a και b είναι τα αποτελέσματα της μέτρησης.

Παράδειγμα ενός μη-τοπικού παιχνιδιού: CHSH

Ας δούμε ένα πολύ απλό παιχνίδι που στηρίζεται στην ανισότητα CHSH. Στην αρχή του παιχνιδιού, στέλνουμε δύο bits x και y στην Αλίκη και τον Bob αντίστοιχα, όπου διαλέγουμε το x με ομοιόμορφες πιθανότητες $p(x = 0) = p(x = 1) = 1/2$ και το y με πιθανότητες $p(y = 0) = p(y = 1) = 1/2$. Με τη σειρά τους, η Αλίκη και ο Bob θα επιστρέψουν τα bits απαντήσεων a και b. Κερδίζουν το παιχνίδι αν

$$x \cdot y = a + b \bmod 2$$

Σε όρους του κατηγορούμενου $V(a, b|x, y)$ αυτό σημαίνει $V(a, b|x, y) = 1$ αν $x \cdot y = a + b \bmod 2$. Μας ενδιαφέρει η πιθανότητα η Αλίκη και ο Bob να νικήσουν το παιχνίδι. Η πιθανότητα αυτή μπορεί να γραφεί ως

$$p_{\text{win}}^{\text{CHSH}} = \frac{1}{4} \sum_{x,y \in \{0,1\}} \sum_{\substack{a,b \\ a+b \bmod 2 = x \cdot y}} p(a, b|x, y)$$

όπου $p(a, b|x, y)$ είναι η πιθανότητα η Αλίκη και ο Bob να απαντήσουν a και b δοθέντων των ερωτήσεων x και y. Τι μπορούν να κάνουν για να νικήσουν το παιχνίδι;

Κλασική πιθανότητα νίκης

Κλασικά, το a είναι απλά μια συνάρτηση του x. Για παράδειγμα, αν $x = 0$, τότε η Αλίκη και ο Bob μπορούν να συμφωνήσουν για τη στρατηγική τους ότι πάντα η Αλίκη θα απαντάει $a = 0$. Βλέπουμε ότι από τη στιγμή που $x = 0$ ή $y = 0$, τότε $x \cdot y = 0$. Σε αυτή τη περίπτωση, η Αλίκη και ο Bob θέλουν να πετύχουν $a + b \bmod 2 = 0$. Όμως, αν $x = y = 1$ πρέπει να δώσουν απαντήσεις τέτοιες ώστε $a + b \bmod 2 = 1$. Αυτό που το κάνει δύσκολο είναι ότι δεν μπορούν να επικοινωνήσουν κατά τη διάρκεια του παιχνιδιού. Αυτό σημαίνει ότι η απάντηση a της Αλίκης εξαρτάται από το x (και όχι από το y) και του Bob παρομοίως, η απάντηση b εξαρτάται από το y (και όχι από το x).

Δοκιμάζοντας όλες τις πιθανές στρατηγικές για την Αλίκη και τον Bob, η κλασική μέγιστη πιθανότητα νίκης που μπορεί να επιτευχθεί είναι

$$p_{\text{win}}^{\text{CHSH}} = \frac{3}{4}$$

Μπορεί να επιτευχθεί με τη στρατηγική του να απαντάνε πάντα $a = b = 0$, που σημαίνει $a + b \bmod 2 = 0$ και είναι σωστό στις 3 από τις 4 πιθανές περιπτώσεις. Μόνο όταν $x = y = 1$ θα κάνουν λάθος.

Κβαντική πιθανότητα νίκης

Από ότι φαίνεται, η Αλίκη και ο Bob μπορούν να έχουν καλύτερα αποτελέσματα με μια κβαντική στρατηγική, χρησιμοποιώντας κβαντική διεμπλοκή. Ας θεωρήσουμε ότι η Αλίκη και ο Bob μοιράζονται ένα EPR ζευγάρι, όπου βάζουμε ως ετικέτα στο qubit της Αλίκης το (A) και του Bob το (B).

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)$$

Ας υποθέσουμε τώρα, ότι όταν $x = 0$, η Αλίκη μετράει το qubit της στη βάση $\{|0\rangle, |1\rangle\}$. Αλλιώς, όταν $x = 1$, το μετράει στη βάση $\{|+\rangle, |-\rangle\}$. Επίσης, ας υποθέσουμε ότι όταν $y = 0$, ο Bob μετράει το qubit του στη βάση $|v_1\rangle, |v_2\rangle$, όπου

$$|v_1\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, \quad |v_2\rangle = -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$$

και όταν $y = 1$, στη βάση $|w_1\rangle, |w_2\rangle$, όπου

$$|w_1\rangle = \cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle, \quad |w_2\rangle = \sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$$

Ας θεωρήσουμε τη περίπτωση όπου $x = 0, y = 0$. Αυτό σημαίνει ότι η Αλίκη μετράει στη βάση $\{|0\rangle, |1\rangle\}$ και ο Bob στη βάση $|v_1\rangle, |v_2\rangle$. Η πιθανότητα νίκης, δεδομένων των $x = 0$ και $y = 0$, δίνεται από

$$\begin{aligned} p_{\text{νίκη}\,|x=0,y=0} &= p(a=0,b=0|x=0,y=0) + p(a=1,b=1|x=0,y=0) \\ &= |\langle 0_A v_{1B}|\Psi_{AB}\rangle|^2 + |\langle 1_A v_{2B}|\Psi_{AB}\rangle|^2 \\ &= 2\left|\frac{1}{\sqrt{2}}\cos\frac{\pi}{8}\right|^2 = \cos^2\frac{\pi}{8} \end{aligned}$$

Η πιθανότητα νίκης, δεδομένων των $x = 0$ και $y = 1$, δίνεται από

$$\begin{aligned} p_{win|x=1,y=0} &= p(a=0,b=0|x=1,y=0) + p(a=1,b=1|x=1,y=0) \\ &= |\langle 0_A w_{1B}|\Psi_{AB}\rangle|^2 + |\langle 1_A w_{2B}|\Psi_{AB}\rangle|^2 \\ &= 2\left|\frac{1}{\sqrt{2}}\cos\frac{\pi}{8}\right|^2 = \cos^2\frac{\pi}{8} \end{aligned}$$

Από την άλλη όμως,

$$\begin{aligned} p_{win|x=0,y=1} &= p(a=0,b=0|x=0,y=1) + p(a=1,b=1|x=0,y=1) \\ &= |\langle +_A v_{1B}|\Psi_{AB}\rangle|^2 + |\langle -_A v_{2B}|\Psi_{AB}\rangle|^2 \\ &= \frac{1}{2}\left(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8} + \frac{1}{\sqrt{2}}\sin\frac{\pi}{8}\right)^2 + \frac{1}{2}\left(\frac{1}{\sqrt{2}}\cos\frac{\pi}{8} + \frac{1}{\sqrt{2}}\sin\frac{\pi}{8}\right)^2 \\ &= \frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2 \end{aligned}$$

και για $x = 1, y = 1$ είναι $p_{\text{νίκη}}\ |x=1,y=1 = p_{\text{ωιν}}\,|\,x=1,y=0 = \frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2$ και ισχύει ότι $\frac{1}{2}\left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)^2 = \cos^2\frac{\pi}{8}$. Αυτό συνεπάγεται ότι

$$p_{win} = \frac{1}{4}\sum_{x,y} p_{\text{νίκη}\,|x,y} = \cos^2\frac{\pi}{8} \approx 0.85$$

2.6 Αβεβαιότητες και εντροπίες

Θα αναλύσουμε τους τρόπους με τους οποίους ποσοτικοποιούμε τη κβαντική πληροφορία, το οποίο θα παίξει κύριο ρόλο στην ασφάλεια των κβαντικών πρωτοκόλλων.

2.6.1 Πότε δύο κβαντικές καταστάσεις είναι σχεδόν ίδιες;

Είναι πολύ σημαντικό να έχουμε μια ιδέα του τι σημαίνει το να παράγουμε κατά προσέγγιση μια συγκεκριμένη κβαντική κατάσταση.

Απόσταση ίχνους (trace distance)

Ας υποθέσουμε ότι θέλουμε να εφαρμόσουμε ένα πρωτόκολλο ή έναν αλγόριθμο που παράγει τη κατάσταση ρ_{ideal}. Δυστυχώς, λόγω ατελειών, το πρωτόκολλο παράγει τη κατάσταση ρ_{real}. Αν χρησιμοποιήσουμε αυτό το πρωτόκολλο ή τον αλγόριθμο ως υπο-ρουτίνα σε ένα μεγαλύτερο πρωτόκολλο ή αλγόριθμο, πώς επηρεάζεται το μεγαλύτερο πρωτόκολλο αν μπορούμε να φτιάξουμε μόνο το ρ_{real} αντί του ρ_{ideal};

Διαισθητικά, είναι προφανές ότι αν τα ρ_{ideal} και ρ_{real} είναι εξαιρετικά δύσκολο να ξεχωριστούν, τότε δεν παίζει πολύ ρόλο. Άρα χρειαζόμαστε μια μονάδα μέτρησης απόστασης που είναι άμεσα συνδεδεμένη με το κατά πόσο μπορούμε να ξεχωρίζουμε τις δύο καταστάσεις. Έστω ότι δεν ξέρουμε ποιά κατάσταση έχουμε. Έστω ότι μας δίνονται η καθεμία με πιθανότητα $1/2$, και ο στόχος

είναι να τις ξεχωρίσουμε. Μπορούμε λοιπόν να εφαρμόσουμε μια μέτρηση χρησιμοποιώντας τελεστές, M_{real} και $M_{ideal} = \mathbb{I} - M_{real}$. Η πιθανότητα του να ξεχωρίσουμε τις δύο καταστάσεις είναι

$$p_{\text{succ}} = \frac{1}{2}\,\text{tr}\left[M_{\text{real}}\rho_{\text{real}}\right] + \frac{1}{2}\,\text{tr}\left[M_{\text{ideal}}\rho_{\text{ideal}}\right] = \frac{1}{2} + \frac{1}{2}\,\text{tr}\left[M_{\text{real}}\left(\rho_{\text{real}} - \rho_{\text{ideal}}\right)\right]$$

Για να βρούμε τη καλύτερη μέτρηση μπορούμε να βελτιστοποιήσουμε τον όρο M_{real} σε σχέση με όλους τους τελεστές μέτρησης. Ξέρουμε ότι $0 \leq M_{\text{ρεαλ}} \leq \mathbb{I}$, δηλαδή οι ιδιοτιμές του M_{real} βρίσκονται όλες ανάμεσα στο 0 και το 1. Άρα η μέγιστη πιθανότητα επιτυχίας δίνεται από τη σχέση

$$p_{succ}^{\max} = \frac{1}{2} + \frac{1}{2}\max_{0\leq M\leq\mathbb{I}}\text{tr}\left[M\left(\rho_{real} - \rho_{ideal}\right)\right]$$

Ποιός είναι λοιπόν ο τελεστής M που θα μεγιστοποιήσει τη ποσότητα του ίχνους $\text{tr}\left[M\left(\rho_{\text{ρεαλ}} - \rho_{ideal}\right)\right]$; Αυτή η ερώτηση αναλύθηκε στο $[51]$, και ο ιδανικός M είναι η προβολή πάνω στη θετικό ιδιοχώρο του $\rho_{real} - \rho_{ideal}$. Πιο συγκεκριμένα, ας θεωρήσουμε τη διαγωνοποιημένη μορφή του γραμμικού τελεστή $\rho_{real} - \rho_{ideal}$, και ας συμβολίσουμε το διαγώνιο πίνακα ως $D = \Sigma_i d_i \left|d_i\right\rangle\left\langle d_i\right|$. Επίσης, ας ορίσουμε το σύνολο $S_+ = \{j | d_j > 0\}$. Το ιδανικό M δίνεται από τη σχέση

$$M_{\text{opt}} = \sum_{j\in S_+}\left|d_j\right\rangle\left\langle d_j\right|$$

Ορισμός 2.38. *(Trace distance) Η απόσταση ίχνους μεταξύ δύο καταστάσεων ρ_{real} και ρ_{ideal} δίνεται από τη σχέση*

$$D\left(\rho_{real}, \rho_{ideal}\right) = \max_{0\leq M\leq\mathbb{I}}\text{tr}\left[M\left(\rho_{real} - \rho_{ideal}\right)\right]$$

Μπορεί να γραφεί επίσης και ως

$$D\left(\rho_{real}, \rho_{ideal}\right) = \frac{1}{2}\,\text{tr}[\sqrt{A^\dagger A}]$$

όπου $A = \rho_{real} - \rho_{ideal}$. Στη βιβλιογραφία μπορούμε να τη συναντήσουμε και ως

$$D\left(\rho_{real}, \rho_{ideal}\right) = \frac{1}{2}\left\|\rho_{real} - \rho_{ideal}\right\|_{\text{tr}} = \frac{1}{2}\left\|\rho_{real} - \rho_{ideal}\right\|_1$$

Αν δύο καταστάσεις είναι κοντά σε απόσταση ίχνους, δεν υπάρχει μέτρηση - καμία διαδικασία στο σύμπαν- που μπορεί να τα ξεχωρίσει πολύ καλά.

Ορισμός 2.39. *Δύο κβαντικές καταστάσεις ρ και σ είναι $\epsilon - close$ αν $D(\rho,\sigma) \leq \varepsilon$. Επίσης γράφουμε και $\rho \approx_\varepsilon \sigma$.*

Πρόταση 2.40. *Η απόσταση ίχνους είναι μια μετρική και έχει τις εξής ιδιότητες για όλες τις καταστάσεις ρ, σ, τ.*

1. *Μη αρνητική: $D(\rho,\sigma) \geq 0$, όπου η ισότητα ικανοποιείται αν $\rho = \sigma$.*
2. *Συμμετρική: $D(\rho,\sigma) = D(\sigma,\rho)$.*

3. *Τριγωνική ανισότητα:* $D(\rho,\sigma) \leq D(\rho,\tau) + D(\tau,\sigma)$.

4. *Κυρτότητα:* $D\left(\sum_i p_i\rho_i, \sigma\right) \leq \sum_i p_i D\left(\rho_i,\sigma\right)$.

Ορισμός 2.41. *Δοθέντος ενός οποιουδήποτε πίνακα πυκνότητας ρ, η $\epsilon-$μπάλα του ρ ,$\mathscr{B}^{\varepsilon}(\rho)$,ορίζεται ως το σύνολο όλων των καταστάσεων $\rho^{'}$ που είναι $\epsilon - close$ στο ρ σε σχέση με την απόσταση ίχνους, δηλαδή*

$$\mathscr{B}^{\varepsilon}(\rho) := \{\rho' | \rho' \geq 0, \mathrm{tr}\left(\rho'\right) = 1, D\left(\rho,\rho'\right) \leq \varepsilon\}$$

Πιστότητα (fidelity)

Ένας άλλος τρόπος μέτρησης του πόσο κοντά είναι οι καταστάσεις είναι αυτός της πιστότητας, που συνδέεται άμεσα με το εσωτερικό γινόμενο.

Ορισμός 2.42. *Δοθέντων πινάκων πυκνότητας ρ_1 και ρ_2, η πιστότητα , $F\left(\rho_1,\rho_2\right)$, ανάμεσα στους ρ_1 και ρ_2 είναι*

$$F\left(\rho_1,\rho_2\right) = \mathrm{tr}[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}]$$

Για καθαρές καταστάσεις, $\rho_1 = |\Psi_1\rangle\langle\Psi_1|$ και $\rho_2 = |\Psi_2\rangle\langle\Psi_2|$ η πιστότητα παίρνει μια πιο απλή μορφή

$$F\left(\rho_1,\rho_2\right) = |\langle\Psi_1|\Psi_2\rangle|$$

Αν μια μόνο από τις καταστάσεις $\rho_1 = |\Psi_1\rangle\langle\Psi_1|$ είναι καθαρή, τότε

$$F\left(\rho_1,\rho_2\right) = \sqrt{\langle\Psi_1|\rho_2|\Psi_1\rangle}$$

Παρόλο που η πιστότητα δεν είναι μετρική, έχει μια διαισθητική ερμηνεία, αν θέλουμε να επαληθεύσουμε αν καταφέραμε να παράξουμε την επιθυμητή κατάσταση $|\Psi\rangle$. Ας υποθέσουμε ότι θέλουμε να φτιάξουμε μια μηχανή που παράγει την $|\Psi\rangle\langle\Psi|$, όμως έχουμε τη δυνατότητα να παράξουμε μόνο κάποια κατάσταση ρ. Μετράμε την ρ για να ελέγξουμε για επιτυχία. Μπορούμε να το κάνουμε αυτό (θεωρητικά) μετρώντας το

$$M_{\mathrm{succ}} = |\Psi\rangle\langle\Psi|$$
$$M_{\mathrm{fail}} = \mathbb{I} - |\Psi\rangle\langle\Psi|$$

Η πιθανότητα επιτυχίας είναι άμεσα συνδεδεμένη με τη πιστότητα ανάμεσα στη πραγματική έξοδο ρ και τη κατάσταση $|\Psi\rangle$ που θέλουμε να επιτύχουμε ως

$$\mathrm{tr}\left[M_{\mathrm{succ}}\boldsymbol{\rho}\right] = \langle\Psi|\rho|\Psi\rangle = F(|\Psi\rangle,\rho)^2$$

Ένας άλλος τρόπος για να γράψουμε τη πιστότητα είναι

$$\max_{|\rho_{AP}\rangle,|\sigma_{AP}\rangle} |\langle\rho_{AP}|\sigma_{AP}\rangle|$$

όπου $|\rho_{AP}\rangle$ και $|\sigma_{AP}\rangle$ είναι καθαρισμοί (purifications) των καταστάσεων ρ_A και σ_A χρησιμοποιώντας ένα σύστημα καθαρισμού P.

Πρόταση 2.43. *Για οποιεσδήποτε δύο κβαντικές καταστάσεις ρ, σ η πιστότητα ικανοποιεί τις εξής ιδιότητες*

1. *Μεταξύ 0 και 1: $0 \leq F(\rho, \sigma) \leq 1$*
2. *Συμμετρική: $F(\rho, \sigma) = F(\sigma, \rho)$.*
3. *Πολλαπλασιαστική υπό το τανυστικό γινόμενο: $F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1, \sigma_1) \cdot F(\rho_2, \sigma_2)$.*
4. *Αναλλοίωτη υπό ορθογώνιες πράξεις: $F(\rho, \sigma) = F\left(U\rho U^\dagger, U\sigma U^\dagger\right)$.*
5. *Σχέση με την απόσταση ίχνους: $1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F^2(\rho, \sigma)}$. Αντιστρόφως, έχουμε ότι $1 - D(\rho, \sigma) \leq F(\rho, \sigma) \leq \sqrt{1 - D^2(\rho, \sigma)}$.*

   Αυτή είναι γνωστή και ως Fuchs-van de Graaf ανισότητα.

2.6.2 Μετρώντας την αβεβαιότητα: η ελάχιστη εντροπία (min-entropy)

Σε πολλά κβαντικά πρωτόκολλα, θα μετράμε κβαντικές καταστάσεις αλλά δεν θα παίρνουμε το κλειδί κατευθείαν. Αυτό μας παρακινεί να βρούμε ένα μέτρο για την αβεβαιότητα για μια κλασική ακολουθία X.

Ελάχιστη εντροπία

Ας θεωρήσουμε τη κατάσταση

$$\rho_X = \sum_x p_x |x\rangle \langle x|_X$$

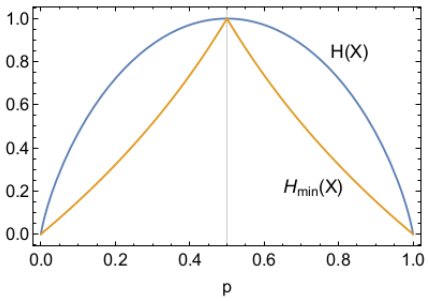
Όταν μιλάμε για επικοινωνίες, ένα πολύ σημαντικό μέτρο είναι η εντροπία von Neumann ή Shannon.

$$H(X) = -\sum_x p_x \log p_x$$

η οποία όμως δεν είναι τόσο καλή για τη κρυπτογραφία, για αυτό θα ορίσουμε την ελάχιστη εντροπία (σχήμα 2.10).

Ορισμός 2.44. *Δοθέντος οποιασδήποτε κατανομής πιθανότητας $\{p_x\}_x$, η ελάχιστη εντροπία H_{min} ορίζεται ως*

$$\mathrm{H}_{\min}(X) = \mathrm{H}_{\min}(\rho_X) = -\log \max_x p_x$$



Σχήμα 2.10: Για μια δυαδική τυχαία μεταβλητή $X = \{0, 1\}$, η σύγκριση μεταξύ της εντροπίας Shannon $H(X)$ και της ελάχιστής της εντροπίας $H_{min}(X)$.

Η ελάχιστη εντροπία υπό όρους (conditional min-entropy)

Μπορούμε να ποσοτικοποιήσουμε την αβεβαιότητα όσον αφορά το X αν μας δοθεί ένας επιπλέον κβαντικός καταχωρητής E; Φαίνεται ότι όπως για την von Neumann εντροπία, η ελάχιστη εντροπία έχει και αυτή μια υπό όρους παραλλαγή $\mathrm{H}_{\min}(X|E)$ όπως παρουσιάζεται στο [53] . Ο εύκολος τρόπος για τη φανταστούμε είναι να τη σκεφτούμε με τον όρο της πιθανότητας που έχει η Eve να καταφέρει να μαντέψει το X αν της δώσουμε πρόσβαση σε έναν κβαντικό καταχωρητή E. Η Eve έχει τη κατάσταση ρ_x^E με πιθανότητα p_x και ο στόχος της είναι να μαντέψει το x κάνοντας μια μέτρηση στον E. Αυτό είναι ακριβώς το πρόβλημα διαχωρισμού κβαντικών καταστάσεων που είδαμε προηγουμένως.

Ορισμός 2.45. *Ας θεωρήσουμε μια διμερή $cq-$κατάσταση ρ_{XE} όπου X είναι κλασική. Η ελάχιστη εντροπία υπό όρους (conditional min-entropy) $\mathrm{H}_{\min}(X|E)$ μπορεί να γραφεί ως*

$$\mathrm{H}_{\min}(X|E)_{\rho_{XE}} := -\log P_{\mathrm{guess}}(X|E)$$

όπου $P_{guess}(X|E)$ είναι η πιθανότητα η Eve να μαντέψει το x, μεγιστοποιημένη για όλες τις πιθανές μετρήσεις

$$P_{guess}(X|E) := \max_{\{M_x\}_x} \sum_x p_x \,\mathrm{tr}\left[M_x \rho_x^E\right]$$

όπου η μεγιστοποίηση λαμβάνεται από όλα τα POVMS $\{M_x \geq 0 | \sum_x M_x = \mathbb{I}\}$. Το E καλείται και πλευρική πληροφορία (side information) του X.

Όταν το $x \in \{0, 1\}$ παίρνει μόνο δύο τιμές, είναι εύκολο να βρούμε την ιδανική μέτρηση και η πιθανότητα να μαντέψουμε P_{guess}, είναι άμεσα συνδεδεμένη με τη διαχωρισιμότητα των μειωμένων καταστάσεων ρ_0^E και ρ_1^E, δηλαδή η απόσταση ίχνους $D\left(\rho_0^E, \rho_1^E\right)$.

Κβαντική ελάχιστη εντροπία υπό όρους

Στη γενική μορφή, το σύστημα μπορεί να είναι και κβαντικό, και έστω ότι ονομάζουμε A τη κβαντική εκδοχή. Πώς μοιάζει η ελάχιστη εντροπία υπό όρους, $\mathrm{H}_{\min}(A|E)$;

Ορισμός 2.46. *Δοθέντος ενός οποιοδήποτε διμερή πίνακα πυκνότητας ρ_{AE}, με το A να έχει διάσταση $|A|$, η ελάχιστη εντροπία υπό όρους είναι*

$$\mathrm{H}_{\min}(A|E) := -\log[|A| \cdot \mathrm{Dec}(A|E)]$$
$$\mathrm{Dec}(A|E) := \max_{R_E \to A'} F\left((\mathbb{I}_A \otimes \Lambda_{E\to A'})\,\rho_{AE}, |\Phi\rangle\langle\Phi|_{AA'}\right)^2$$

όπου $|\Phi\rangle_{AA'} := \frac{1}{\sqrt{|A|}} \sum_{i=1}^{|A|} |a_i\rangle_A \otimes |a_i\rangle_{A'}$ είναι η μέγιστη διεμπλεγμένη κατάσταση ανάμεσα στα A και $A^{'}$, και η μεγιστοποίηση πραγματοποιείται σε όλα τα κβαντικά κανάλια Λ που αντιστοιχίζουν το σύστημα E στο $A^{'}$. Η συνάρτηση F είναι η πιστότητα. Ένας εναλλακτικός τρόπος να ορίσουμε την ελάχιστη εντροπία υπό όρους είναι

$$\mathrm{H}_{\min}(A|E) := \max_{\sigma_B} \sup\left\{\lambda \in \mathbb{R} | \rho_{AB} \leq 2^{-\lambda}\mathbb{I}_A \otimes \sigma_B\right\}$$

Ομαλή ελάχιστη εντροπία (smoothed min-entropy)

Όπως είδαμε παραπάνω στην αναφορά μας περί απόστασης ίχνους, λόγω ατελειών του πρωτοκόλλου ή του αλγορίθμου, δεν μπορούμε να παράξουμε τη κατάσταση ρ_{XE} που θέλουμε, αλλά μια κατάσταση $\rho_{XE}^{'}$ κοντά σε αυτή, αλλά της οποίας δεν ξέρουμε τη μορφή, μόνο ότι είναι $e - close$ στην ρ_{XE}. Για αυτό, κοιτάμε την ομαλή ελάχιστη εντροπία, η οποία μας δίνει τη μέγιστη τιμή της $\mathrm{H}_{\min}(X|E)$ για όλες τις καταστάσεις $\rho'_{AE} \in \mathscr{B}^{\varepsilon}(\rho_{AE})$.

Ορισμός 2.47. *Έστω μια διμερής $cq-$κατάσταση ρ_{XE} όπου η X είναι κλασική. Η ομαλή ελάχιστη εντροπία $\mathrm{H}^{\varepsilon}_{\min}(X|E)$ μπορεί να γραφεί ως*

$$\mathrm{H}^{\varepsilon}_{\min}(X|E)_\rho := \max_{\rho' \in \mathscr{B}^{\varepsilon}(\rho)} \mathrm{H}_{\min}(X|E)_{\rho'}$$

2.6.3 Προστασία επικοινωνίας

Γενικά, προσπαθούμε να προστατεύσουμε την επικοινωνία δύο ατόμων από ένα τρίτο όσο περισσότερο μπορούμε. Ένας ωπτοακουστής, η Eve είναι τελείως αδαής για το κλειδί αν ισχύει η παρακάτω συνθήκη.

Ορισμός 2.48. *Έστω μια αρθρωτή $cq-$κατάσταση ρ_{KE}, ενός $n-$bit κλειδιού K, και της Eve, E. Η Eve είναι αδαής για το κλειδί K, αν*

$$\rho_{KE} = \frac{1}{2^n}\mathbb{I}_K \otimes \rho_E$$

Αυτό σημαίνει ότι το κλειδί είναι ομοιόμορφα κατανεμημένο και ασύνδετο με την Eve.

Βέβαια, σε πρακτικές εφαρμογές, δεν μπορούμε να επιτύχουμε τελειότητα της κατάστασης ρ_{KE}, για αυτό προσπαθούμε να είμαστε όσο το δυνατόν κοντύτερα σε μια ιδανική κατάσταση.

Ορισμός 2.49. *Έστω μια αρθρωτή $cq-$κατάσταση $\rho^{\text{ρεαλ}}_{KE}$ ενός n -bit κλειδιού K και της Eve, E. Η Eve είναι σχεδόν αδαής για το κλειδί K, αν*

$$D\left(\rho_{KE}^{real}, \rho_{KE}^{ideal}\right) \leq \varepsilon$$

όπου $\rho_{KE}^{ideal} = \frac{1}{2^n}\mathbb{I}_K \otimes \rho_E$.

2.7 Από μερική πληροφορία στη σχεδόν τέλεια ασφάλεια

Θα αναλύσουμε τον όρο της προστασίας προσωπικών δεδομένων (privacy amplification), ο οποίος είναι βασικό συστατικό πολλών κβαντικών πρωτοκόλλων, και πιο συγκεκριμένα είναι το τελευταίο βήμα στο κβαντικό πρωτόκολλο διαμοίρασης κλειδιού BB84 μαζί με το βήμα της ενίσχυσης της ιδιωτικότητας.

2.7.1 Προστασία προσωπικών δεδομένων (privacy amplification)

Ας θεωρήσουμε το ακόλουθο σενάριο. Δύο οντότητες, η Αλίκη και ο Bob, ο καθένας από τους δύο κρατάει ένα αντίγραφο της ίδιας ακολουθίας από bits, έστω X η ακολουθία, την οποία θα αποκαλέσουμε "αδύναμο μυστικό". Αυτό το μυστικό το έχουνε λάβει από μια συγκεκριμένη κατανομή P_x, την οποία μπορούμε να αναπαραστήσουμε μέσω μιας τυχαίας μεταβλητής X. Αργότερα θα τη καλούμε αυτή τη X, "πηγή" (source). Η κατανομή X δεν είναι γνωστή, το δείγμα όμως x είναι διαθέσιμο και στις δύο οντότητες. Ένας ωπτοακουστής έχει μερική πληροφορία, έστω E, η οποία μπορεί να συσχετίζεται με τη X, για παράδειγμα το E μπορεί να είναι το πρώτο bit του x, ο πίνακας ισοτιμίας του x ή μια τυχαία κβαντική κατάσταση ρ_x^E. Στόχος της Αλίκης και του Bob είναι να παράξουν την ίδια ακολουθία z, η οποία μπορεί να είναι μικρότερη της x, αλλά πρέπει η κατανομή της να ειναι ομοιόμορφη, ακόμα και από τη σκοπιά του ωπτοακουστή. Συμβολικά, η προστασία των προσωπικών δεδομένων (privacy amplification), είναι ο μετασχηματισμός

$$\rho_{XE} \quad \xrightarrow{\mathrm{PA}_X \otimes \mathrm{I}_E} \quad \rho_{ZE} \approx_\varepsilon \frac{\mathbb{I}_Z}{|Z|} \otimes \rho_E$$

Στη συνέχεια θα δούμε τη διαδικασία εξαγωγής τυχαίων στοιχείων και τους αντίστοιχους εξαγωγείς.

2.7.2 Εξαγωγείς τυχαιότητας

Έχουμε μια οντότητα την Αλίκη, η οποία έχει πρόσβαση σε μια $n-$bit ακολουθία x με κατανομή X. Καλούμε X τη πηγή. Η X είναι άγνωστη και μπορεί να συσχετίζεται με ένα επιπλέον σύστημα E στο οποίο η Αλίκη δεν έχει κανένα έλεγχο. Για παράδειγμα το E μπορεί να περιέχει κάποια πληροφορία για το τρόπο με τον οποίο παράγεται η πηγή, ή κάποια πληροφορία την οποία συνέλεξε ο ωπτοακουστής κατά τη διαδικασία ενός προηγούμενου πρωτοκόλλου το οποίο περιείχε τη X. Η μόνη υπόσχεση που δίνεται στην Αλίκη είναι το κατώτερο όριο της ελάχιστης εντροπίας, $\mathrm{H}_{\min}(X|E) \geq k$. Ο στόχος της Αλίκης είναι να κατασκευάσει μια νέα ακολουθία z που είναι σχεδόν ομοιόμορφα κατανεμημένη και μη-σχετιζόμενη με το E. Άρα πρέπει η Αλίκη να εξάγει τυχαία στοιχεία από τη X με κάποιο τρόπο.

Πηγές τυχαιότητας

Ακολουθούν μερικά παραδείγματα πηγών X και πώς εξάγουμε ομοιόμορφα κατανεμημένα bits από αυτές.

Πηγές I.D.D

Η απλούστερη περίπτωση πηγής τυχαίων στοιχείων είναι μια i.d.d πηγή, όπου i.d.d τα αρχικά από τις λέξεις independent and indentically distributed. Μια κλασική i.d.d πηγή $X \in \{0,1\}^n$ έχει μια κατανομή $\{p_x\}$, η οποία έχει τη μορφή γινομένου: υπάρχει μια κατανομή $\{p_0, p_1\}$ σε ένα μοναδικό bit τέτοια ώστε για όλα τα $(x_1, \ldots, x_n) \in \{0,1\}^n$, να έχουμε

$$\Pr[X = (x_1, \ldots, x_n)] = \Pr[X_1 = x_1] \cdots \Pr[X_n = x_n] = p_{x_1} \cdots p_{x_n}$$

Τέτοιες πηγές καλούνται και von Neumann πηγές.

Ανεξάρτητων bits πηγές (independent bits sources)

Οι πηγές αυτές χαρακτηρίζονται από τη συνθήκη ότι κάθε bit επιλέγεται ανεξάρτητα. Παρόλα αυτά η κατανομή μπορεί να είναι διαφορετική για διαφορετικά bits. Κάθε i.d.d πηγή είναι και i.b.s, αλλά το αντίστροφο δεν ισχύει.

Επάγεται σαν αποτέλεσμα ότι αν πάρουμε το πίνακα ισοτιμίας για όλα τα bits στην ακολουθία που έχουν παραχθεί από πηγή ανεξάρτητων bits, τότε έχουμε ένα bit το οποίο είναι απίστευτα κοντά σε ομοιόμορφα κατανεμημένο καθώς το $n \to \infty$, δεδομένου ότι κάθε bit της πηγής δεν είναι τελείως αμερόληπτο: $0 < \Pr[X_j = 0] < 1$ για όλα τα j.

Bit-fixing πηγές

Είναι μια ειδική περίπτωση των ανεξάρτητων πηγών όπου κάθε bit της X μπορεί να είναι δύο ειδών μόνο: ή το bit θα είναι τελείως καθορισμένο, ή θα είναι τυχαία ομοιόμορφα κατανεμημένο.

Γενικές πηγές

Υπάρχουν πολλών ειδών διαφορετικές πηγές. Η διαφοροποίηση τους γίνεται ανάλογα με τη μετρήση της εντροπίας. Αποδυκνείεται ότι η ελάχιστη εντροπία μας παρέχει ακριβώς τη "σωστή" μέτρηση για την εξαγόμενη τυχαιότητα, με ακριβή τρόπο.

Ορισμός 2.50. *Μια τυχαία μεταβλητή X είναι μια $k-$πηγή αν*

$$\mathrm{H}_{\min}(X) \geq k$$

Έχουμε ως στόχο να εφαρμόσουμε αυτή τη διαδικασία σε κρυπτογραφικές λειτουργίες, αλλά δεν συμπεριλάβαμε τον ωπτοακουστή. Η διαδικασία της εξαγωγής τυχαιότητας δεν πρόκεται να συμβεί στο κενό: πρέπει να λάβουμε υπόψη μας τη πιθανότητα ότι ένα άλλο σύστημα E μπορεί να συσχετίζεται με τη X. Ας ονομάσουμε το E, μερική πληροφορία (side information). Το X είναι μια κλασική ακολουθία από bits, αλλά το E μπορεί να είναι κβαντικό. Για αυτό πρέπει να εισάγουμε μια $cq-$κατάσταση ρ_{XE}, η οποία γενικά παίρνει τη μορφή

$$\rho_{XE} = \sum_x |x\rangle \langle x|_X \otimes \rho_x^E$$

όπου ρ_x^E είναι θετικά ημιορισμένο και $\mathrm{Tr}\left(\rho_{XE}\right) = \sum_x \mathrm{Tr}\left(\rho_x^E\right) = 1$.

Χρησιμοποιώντας τη μερική πληροφορία, παίρνουμε έναν εύχρηστο τρόπο να μοντελοποιήσουμε οποιαδήποτε τιμή X ως αποτέλεσμα μιας αρχικής ομοιόμορφης ακολουθίας, για την οποία ένας τρίτος έχει αποκτήσει μερική πληροφορία.

Ορισμός 2.51. *Μια $cq-$κατάσταση ρ_{XE} καλείται $k-$πηγή αν*

$$\mathrm{H}_{\min}(X|E) \geq k$$

Οι διαδικασίες εξαγωγής τυχαίων στοιχείων που παράγουν ομοιόμορφα κατανεμημένα τυχαία bits από οποιαδήποτε $k-$πηγή, χωρίς να ξέρουμε οτιδήποτε άλλο για τη πηγή είναι οι εξής:

Strong-seeded extractors

Σε όλα τα παραπάνω, εφαρμόζουμε μια συνάρτηση, έστω Ext, στη πηγή X. Αυτή η συνάρτηση είναι γνωστή ως ντετερμινιστικός εξαγωγέας, που σημαίνει ότι είναι μια δεδομένη συνάρτηση $Z = Ext(X)$, η οποία δεν εισάγει καμία περαιτέρω τυχαιότητα στη X, πέρα από αυτή που ήδη έχει.

Το ιδανικό θα ήταν να εξάγουμε τυχαιότητα από οποιαδήποτε $k-$πηγή εφαρμόζοντας μια τέτοια ντετερμινιστική συνάρτηση. Αυτό όμως είναι αδύνατο. Δεν υπάρχει σταθερή ντετερμινιστική διαδικασία τέτοια ώστε να χρησιμοποιηθεί και να εξάγουμε έστω και ένα μοναδικό bit τυχαιότητας από κάθε δυνατή $k-$πηγή, ακόμα και αν το k είναι μέγιστο, δηλαδή $k = n - 1$!

Λήμμα 2.52. *Για κάθε συνάρτηση $\mathrm{Ext} : \{0,1\}^n \to \{0,1\}$, υπάρχει μια $(n-1)-$πηγή X τέτοια ώστε η $\mathrm{Ext}(x)$ να είναι σταθερή.*

Για το σχεδιασμό συναρτήσεων ανάλογα με τη περίσταση ή το είδος της πηγής, εισάγουμε λίγη επιπλέον τυχαιότητα, την οποία θα ονομάσουμε σπόρο (seed) του εξαγωγέα. Ας το φανταστούμε ως μια δεύτερη είσοδο $Y \in \{0,1\}^d$, στην οποία έχει πρόσβαση η Αλίκη και είναι σίγουρα ομοιόμορφα κατανεμημένη και ανεξάρτητη των X και E.

Ορισμός 2.53. *Ένας (k,ϵ)-ασθενούς πόρου εξαγωγέας τυχαιότητας είναι μια συνάρτηση $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ τέτοια ώστε για κάθε $k-$πηγή ρ_{XE},*

$$D\left(\rho_{\mathrm{Ext}}(X,Y)E, \frac{\mathbb{I}}{2^m} \otimes \rho_E\right) \leq \varepsilon$$

όπου $Y \sim U_d$ είναι ομοιόμορφα κατανεμημένη και ανεξάρτητη των X και E και

$$\rho_{\mathrm{Ext}}(X,Y)E = \sum_z |z\rangle \langle z|_Z \otimes \rho_z^E$$

με $\rho_z^E = 2^{-d} \sum_y \sum_{x:\mathrm{Ext}(x,y)=z} \rho_x^E$

Ο σπόρος είναι τέλεια ομοιόμορφα κατανεμημένος, αλλά δεν τον παίρνουμε ως έξοδο, δηλαδή να ορίσουμε $\mathrm{Ext}(X,Y) = Y$, διότι ο στόχος μας είναι να εξάγουμε τυχαιότητα από το X, και αυτή η επιπλέον τυχαιότητα δεν πρέπει να θεωρηθεί ελεύθερη. Άρα πρέπει να κρατήσουμε το Y όσο μικρότερο γίνεται, ακόμα και αν το X και το k μπορούν να γίνουν πολύ μεγάλα, που σε αυτή τη περίπτωση θα θέλαμε να διατηρήσουμε μια μεγάλη έξοδο (μεγάλο m) με μόνο μια μικρή βοήθεια από το σπόρο (μικρό d).

Στη περίπτωσή μας, η Αλίκη και ο Bob μοιράζονται ένα αδύναμο μυστικό X, και θέλουν να παράξουν ένα ομοιόμορφα τυχαίο μυστικό R. Η λύση μας, το ότι δηλαδή ο εξαγωγέας να βγάλει ως έξοδο το σπόρο του, θα ήταν παρόμοιο με το να ρωτήσουμε την Αλίκη και τον Bob να πετάξουν το αρχικό τους μυστικό X και να μοιραστούν μια καινούργια ακολουθία Y. Αλλά έχουν πρόσβαση μόνο σε δημόσιο κανάλι επικοινωνίας, πώς θα συμφωνήσουν στο ίδιο Y χωρίς να το μάθει ένας ωπτοακουστής;

Ορισμός 2.54. *Ένας $(k,\epsilon)-$strong seeded εξαγωγέας τυχαιότητας είναι μια συνάρτηση $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, τέτοια ώστε για οποιαδήποτε $k-$πηγή ρ_{XE}, έχουμε*

$$D\left(\rho_{\mathrm{Ext}(X,Y)YE}, \frac{\mathbb{I}}{2^m} \otimes \rho_{YE}\right) \leq \varepsilon$$

όπου $Y \sim U_d$ είναι ομοιόμορφα κατανεμημένη και ανεξάρτητη των X και E.

Ελάχιστη εντροπία και προσδιορισμός ποσότητας τυχαιότητας

Ισχυριζόμαστε ότι η ελάχιστη εντροπία είναι ένα άνω φράγμα στη ποσότητα της τυχαιότητας που μπορούμε να εξάγουμε: δεν υπάρχει δυνατός εξαγωγέας ο οποίος έχει έξοδο μήκους περισσότερο από $\mathrm{H}_{\min}(X|E)$. Έχουμε ότι $\mathrm{H}_{\min}(X|E) = -\log P_{\mathrm{guess}}(X|E)$. Ας υποθέσουμε ότι εφαρμόζουμε μια συνάρτηση f στη X. Πόσο δύσκολο είναι να μαντέψουμε την $f(X)$ δοθέντος της E, δηλαδή ποιό είναι το $P_{guess}(f(X)|E)$; Ένας τρόπος για να μαντέψουμε το $f(X)$ είναι να μαντέψουμε το X, και μετά να εφαρμόσουμε την f, έχοντας δηλαδή $P_{guess}(f(X)|E) \geq P_{guess}(X|E)$. Αυτό είναι παρόμοιο με το

$$\mathrm{H}_{\min}(f(X)|E) \leq \mathrm{H}_{\min}(X|E)$$

Αυτό σημαίνει ότι η έξοδος του εξαγωγέα, η οποία για φιξαρισμένο y αποκτιέται ως μια συνάρτηση $f(X) = \mathrm{Ext}(X,y)$, πρέπει να έχει ελάχιστη εντροπία το πολύ $\mathrm{H}_{\min}(X|E)$, το οποίο συνεπάγεται ότι η έξοδος $\mathrm{Ext}(X,y)$, με συνθήκη στο $Y = y$, μπορεί να είναι ομοιόμορφη σε το πολύ $\mathrm{H}_{\min}(X|E)$ bits. Το αντίστροφο τώρα: μπορεί να υπάρξει ένας εξαγωγέας ο οποίος να εξάγει περίπου $\mathrm{H}_{\min}(X|E)$ bits από οποιαδήποτε $k-$πηγή ρ_{XE}. Η απάντηση είναι ναι και θα δούμε αναλυτικότερα στη συνέχεια πώς συμβαίνει αυτό.

2.7.3 Ένας εξαγωγέας που στηρίζεται στο hashing

Ο κύριος σκοπός ενός εξαγωγέα είναι να εξάγει όσο το δυνατόν περισσότερη τυχαιότητα (μεγάλο m) χρησιμοποιώντας το μικρότερο δυνατό σπόρο (μικρό d) και με το καλύτερο δυνατό σφάλμα (μικρό ϵ), όλα από τυχαίες πηγές με ελάχιστη εντροπία (το λιγότερο) k.

Χρησιμοποιώντας πιθανοκρατικό ισχυρισμό, για κάθε είσοδο μήκους k και ελάχιστη εντροπία k η καλύτερη ανταλλαγή που μπορεί να επιτευχθεί είναι σπόρος μήκους $d = \log(n-k) + 2\log(1/\varepsilon) + O(1)$ και έξοδος με μήκος $m = k + d - 2\log(1/\varepsilon) + O(1)$ [55].

Two-universal families of hash functions

Μια hash συνάρτηση είναι μια συνάρτηση που αντιστοιχεί μεγάλες ακολουθίες σε μικρότερες, με την ιδιότητα ότι η έξοδος των hash συναρτήσεων τείνει να είναι "καλά κατανεμημένη".

Ορισμός 2.55. *Μια οικογένεια από hash συναρτήσεις $\mathscr{F} = \{f : \{0,1\}^n \to \{0,1\}^m\}$, όπου $m \leq n$ καλείται $1-$universal αν για κάθε ακολουθία $x \in \{0,1\}^n$ και $z \in \{0,1\}^m$ έχουμε*

$$\Pr_{f\in\mathscr{F}}[f(x) = z] = \frac{1}{2^m}$$

Τα x και z είναι καθορισμένα, και η πιθανότητα παίρνεται από μια ομοιόμορφα τυχαία κατανεμημένη συνάρτηση, από την οικογένεια. Η συνθήκη είναι ανάλογη με το να πούμε ότι για κάθε φιξαρισμένο x, η τυχαία μεταβλητή $F(x)$, όπου F ομοιόμορφα κατανεμημένη για όλα τα f στο $\mathscr{F}$, είναι ομοιόμορφα κατανεμημένη στο $\{0,1\}^m$.

Η ιδιότητα των $1-$universal είναι ικανή ώστε να μας εξασφαλίσει τη δυνατότητα να κατασκευάσουμε έναν weak-seeded εξαγωγέα, άλλα όχι για ένα strong. Θέλουμε μια ισχυρότερη ιδιότητα που προτάθηκε από τους Carter και Wegman:

Ορισμός 2.56. *Μια οικογένεια hash συναρτήσεων $\mathscr{F} = \{f : \{0,1\}^n \to \{0,1\}^m\}$ καλείται $2-$universal family αν για κάθε δύο ακολουθίες $x, x' \in \{0,1\}^n$ με $x \neq x'$, και οποιαδήποτε $\operatorname{two} z, z' \in \{0,1\}^m$, έχουμε*

$$\Pr_{f\in\mathscr{F}}\left[f(x) = z \wedge f\left(x'\right) = z'\right] = \frac{1}{2^{2m}}$$

Η παραπάνω συνθήκη θα ικανοποιούταν αν $f(x)$ και $f(x^{'})$ ήταν διαλεγμένες αρθρωτά, ομοιόμορφα ανεξάρτητα αλλά τυχαία στο $\{0,1\}^m$. Αυτή είναι μια ισχυρότερη συνθήκη από τη προηγούμενη που είδαμε. Απαιτούμε το ζευγάρι των τυχαίων μεταβλητών $\left(F(x), F\left(x'\right)\right)$, για F ομοιόμορφα κατανεμημένη για όλα τα $f \in \mathscr{F}$ να είναι από κοινού ομοιόμορφες.

Έστω $q = 2^n$ και $\mathbb{F}_q$ το πεπερασμένο σώμα με 2^n στοιχεία. Για οποιαδήποτε $(a,b) \in \mathbb{F}_q^2$ θέτουμε

$$f_{a,b} : \mathbb{F}_q \to \mathbb{F}_q, \quad f_{a,b}(x) = ax + b$$

όπου η πρόσθεση και ο πολλαπλασιασμός γίνονται στο $\mathbb{F}_q$. Τότε η $\mathscr{F} = \left\{f_{a,b}, (a,b) \in \mathbb{F}_q^2\right\}$ είναι μια $2-$universal οικογένεια από μόνο $q^2 = 2^{2n}$ hash συναρτήσεις.

Ο $2-$universal εξαγωγέας

Έστω ότι έχουμε μια τυχαία οικογένεια $2-$universal hash συναρτήσεων.

Ορισμός 2.57. *Έστω $\mathscr{F} = \left\{f_y : \{0,1\}^n \to \{0,1\}^m, y \in \{0,1\}^d\right\}$ να είναι μια $2-$universal οικογένεια από hash συναρτήσεις τέτοια ώστε $|\mathscr{F}| = 2^d$. Ο αντίστοιχος $2-$universal εξαγωγέας είναι*

$$\mathrm{Ext}_{\mathscr{F}} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m, \quad \mathrm{Ext}_{\mathscr{F}}(x,y) = f_y(x)$$

Ένας τρόπος να σκεφτούμε το $\mathrm{Ext}_{\mathscr{F}}$ είναι σαν να χρησιμοποιούμε το σπόρο του y για να διαλέξουμε μια συνάρτηση από την οικογένεια $\mathscr{F}$ ομοιόμορφα τυχαία, και ύστερα να επιστρέφει την έξοδο της συνάρτησης όταν υπολογιστεί στη πηγή X.

Θεώρημα 2.58. ***Leftover hash lemma*** *Έστω n και $k \leq n$ να είναι τυχαίοι ακέραιοι, $\epsilon > 0$, $mk - 2\log(1/\varepsilon)$, και $\mathscr{F} = \{f : \{0,1\}^n \to \{0,1\}^m\}$ μια $2-$universal οικογένεια από hash συναρτήσεις. Τότε ο $2-$universal εξαγωγέας $\mathrm{Ext}_{\mathscr{F}}$ είναι ένας $(k,\varepsilon)-$ strong seeded randomness εξαγωγέας.*

Λύνοντας το πρόβλημα της ενίσχυσης της ιδιωτικότητας μέσω των εξαγωγέων

Έστω Ext να είναι ένας $(k,\varepsilon)-$ strong seeded randomness εξαγωγέας. Ακολουθεί ένα απλό πρωτόκολλο:

- Η Αλίκη και ο Bob μοιράζονται ένα αδύναμο μυστικό X, το οποίο μπορεί να συνδέεται με έναν ωπτοακουστή που διαθέτει παράπλευρη κβαντική πληροφορία E.
- Η Αλίκη διαλέγει έναν τυχαίο σπόρο Y από τον εξαγωγέα και υπολογίζει το $R_A = \mathrm{Ext}(X,Y)$. Στέλνει το Y στον Bob μέσω του δημόσιου καναλιού.
- Όταν το λάβει, ο Bob θέτει $R_B = \mathrm{Ext}(X,Y)$.

Αυτό το πρωτόκολλο είναι πάντα σωστό. Η Αλίκη και ο Bob παίρνουν σαν έξοδο την ίδια ακολουθία $R_A = R_B$. Είναι ασφαλές όμως;

Η Eve, στο τέλος, έχει πρόσβαση στην αρχική πληροφορία E, καθώς και σε οποιαδήποτε άλλη επικοινωνία που ανταλλάχθηκε στο δημόσιο κανάλι: πιο συγκεκριμένα στο σπόρο Y. Άρα η συνθήκη γίνεται

$$X : \mathrm{H}_{\min}(X|E)_\rho \geq k \quad \overset{\mathrm{PA}}{\longmapsto} \quad R = \mathrm{Ext}(X,Y) : \rho_{RYE} \approx_\varepsilon \frac{\mathbb{I}_R}{|R|} \otimes \rho_{YE}$$

η οποία είναι ακριβώς η απαίτηση για έναν $(k,\varepsilon)-$ strong seeded randomness εξαγωγέα. Προετοιμάζοντας τον εξαγωγέα με έναν $2-$universal εξαγωγέα που στηρίζεται στην $2-$universal οικογένεια των hash συναρτήσεων που είδαμε προηγουμένως, έχουμε μια ολοκληρωμένη κατασκευή ενός ασφαλούς μονόδρομου πρωτοκόλλου για ενίσχυση της ιδιωτικότητας. Αυτό θα χρησιμοποιηθεί κατά κόρον στα κβαντικά πρωτόκολλα διαμοίρασης κλειδιού παρακάτω.

2.8 Διανομή κλειδιών

Καθόλη τη διάρκεια θα υποθέτουμε ότι η Αλίκη και ο Bob μοιράζονται ένα κλασικό αυθεντικοποιημένο κανάλι CAC (classical authenticated channel).

2.8.1 Ασφαλής διαμοίραση κλειδιού

Ορισμός 2.59. *Ειλικρινής και μη ειλικρινής. Δοθέντος οποιουδήποτε πρωτοκόλλου ανάμεσα σε πολλές οντότητες έχουμε:*

- *Μια οντότητα θα καλείται ειλικρινής αν ακολουθεί το πρωτόκολλο ακριβώς. Δηλαδή θα δίνει τη σωστή είσοδο στο πρωτόκολλο, θα εκτελεί όλα τα βήματα όπως έχουν καθοριστεί από το πρωτόκολλο και θα παράγει το θεμιτό αποτέλεσμα.*
- *Μια οντότητα θα καλείται μη-ειλικρινής ή ύποπτη, αν δεν ακολουθεί το πρωτόκολλο. Αλλιώς θα καλείται αντίπαλος (adversary).*

Ορισμός 2.60. *Ένα πρωτόκολλο διαμοίρασης κλειδιού μεταξύ της Αλίκης και του Bob έχει σκοπό να πετύχει τους ακόλουθους στόχους, δοθέντος μιας παραμέτρου ασφαλείας $\epsilon \geq 0$:*

- $e - correctness$*: Η Αλίκη και ο Bob συμφωνούν σε ένα* $m-$*bit κλειδί* $k \in \{0,1\}^m$*, εξαιρουμένου μιας πιθανότητας σφάλματος το πολύ* ϵ*. Αυτό σημαίνει ότι έχουν ο καθένας από ένα* k_A, k_B *αντίστοιχα και ισχύει* $\mathrm{Prob}\left(K_A \neq K_B\right) \leq \varepsilon$*.*
- $\epsilon - security$*: Οποιοσδήποτε άλλος, όπως η Eve, είναι σχεδόν αδαής όσον αφορά το κλειδί, δηλαδή* $\rho_{KE}^{real} \approx_\varepsilon \rho_{KE}^{ideal}$ *όπου* $\rho_{KE}^{ideal} = \frac{1}{2^m} \otimes \rho_E$*.*

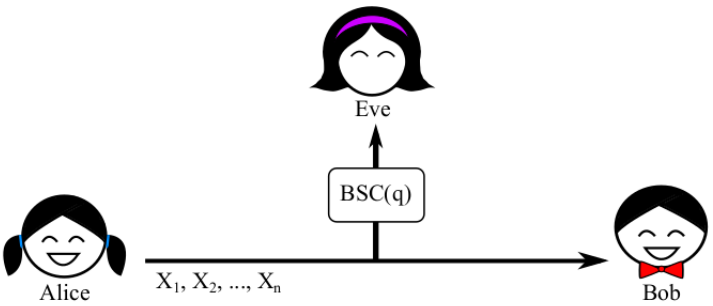
Για να επιτύχουμε ένα τέτοιου είδος πρωτόκολλο διαμοίρασης κλειδιού, θεωρούμε τα παρακάτω κανάλια επικοινωνίας στα οποία έχουν πρόσβαση η Αλίκη και ο Bob.

- Κλασικό κανάλι: Η Αλίκη και ο Bob μπορούν να στέλνουν κλασικά bits μεταξύ τους, αλλά η Eve έχει πλήρη πρόσβαση στο κανάλι, μπορεί να διαβάσει όλα τα μηνύματα ακόμα και να γίνει η Αλίκη.
- Κλασικό αυθεντικοποιημένο κανάλι (CAC): Το ίδιο με το κλασικό κανάλι απλά η Eve τώρα δεν μπορεί να γίνει η Αλίκη ή να αλλάξει τα μηνύματα.
- Κλασικό μυστικό κανάλι: Η Eve δεν έχει καμία γνώση των μηνυμάτων, αλλά μπορεί να γίνει η Αλίκη ή ο Bob.
- Κλασικό μυστικό αλλά αυθεντικοποιημένο: Τα δύο παραπάνω μαζί.
- Κβαντικό κανάλι: Η Αλίκη και ο Bob στέλνουν κβαντική πληροφορία στην μορφή των qubits και η Eve έχει πλήρη πρόσβαση.

2.8.2 Διαμοίραση κλειδιού δοθέντος ενός ειδικά διαμορφωμένου κλασικού καναλιού

Το κανάλι που θα χρησιμοποιήσουν η Αλίκη και ο Bob έχει την ιδιότητα ότι η Eve δεν μπορεί πλήρως να ανακτήσει όλα τα μηνύματα, αλλά η δυνανότητα της να ωτοακούσει είναι κάπως εξασφαλισμένα περιορισμένη (σχήμα 2.11). Το κανάλι έχει τις εξής ιδιότητες: κάθε φορά που η Αλίκη στέλνει ένα bit $b \in \{0,1\}$ μέσω του ειδικού καναλιού (special channel, SC) ο Bob λαμβάνει

σωστά το b και η Eve λαμβάνει σωστά το b με πιθανότητα q, αλλιώς με πιθανότητα $1-q$ λαμβάνει το bit $1-b$ (αλλά δεν ξέρει αν αυτό το bit είναι σωστό ή όχι). Μοντελοποιήσαμε κάπως το θόρυβο της Eve όσον αφορά τη πληροφορία με ρητό τρόπο, όπου κάθε bit του b^E λαμβάνεται από το b μέσω ενός flipping του b με πιθανότητα $1-q$. Αυτό το μοντέλο καλείται δυαδικό συμμετρικό κανάλι (binary symmetric channel,BSCq).



Σχήμα 2.11: Διανομή κλειδιών μέσω ενός ειδικού καναλιού BSCq

Πρωτόκολλο

- Η Αλίκη διαλέγει μια ακολουθία $x = x_1, \ldots, x_n \in \{0,1\}^n$ τυχαία κατανεμημένη, και στέλνει κάθε bit x_j στο Bob μέσω του ειδικού καναλιού.
- Η Αλίκη διαλέγει ένα τυχαίο σπόρο $r \in \{0,1\}^m$, χρησιμοποιεί μια συνάρτηση $Ext : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^l$ και εφαρμόζει τον εξαγωγέα στο X, υπολογίζοντας το $k = Ext(x,r)$.
- Η Αλίκη στέλνει το r στον Bob μέσω του CAC.
- Ο Bob υπολογίζει το $k = Ext(x,r)$.

Για να δείξουμε ότι το πρωτόκολλο λειτουργεί πρέπει να δείξουμε ότι είναι $\epsilon-$σωστό, το οποίο σημαίνει ότι η Αλίκη και ο Bob βγάζουν το ίδιο κλειδί (εκτός από μια μικρή πιθανότητα αποτυχίας). Επίσης πρέπει να δείξουμε ότι το πρωτόκολλο είναι $\epsilon-$ασφαλές, για κάποια παράμετρο ϵ. Για να δούμε το πρωτόκολλο ότι είναι σωστό, πρέπει να τονίσουμε ότι το ειδικό κανάλι είναι τέτοιο ώστε ο Bob να λαμβάνει τα bits σωστά. Δηλαδή να λαμβάνει $x = x_1, \ldots, x_n$ χωρίς σφάλμα. Από τη στιγμή που μαθαίνει και αυτός το r, δηλαδή ξέρει ποιά συνάρτηση $\mathrm{Ext}(\cdot, r)$ να εφαρμόσει στο x, μπορεί να υπολογίσει το $k = Ext(x,r)$ χωρίς σφάλμα.

Θα δείξουμε πώς μπορούμε να εξασφαλίσουμε την ασφάλεια του πρωτοκόλλου. Ας τονίσουμε πρώτα ότι η πιθανότητα της Eve να μαντέψει κάθε bit ακριβώς δίνεται από το q. Έχουμε λοιπόν

$$P_{\mathrm{guess}}(X|E) = q^n$$

ή ισοδύναμα

$$H_{\min}(X|E) = -\log P_{\mathrm{guess}}(X|E) = n(-\log q)$$

Αν το r, για παράδειγμα χρησιμοποείται για να διαλέξουμε μια συνάρτηση $Ext(\cdot, r)$ από ένα σύνολο από $2-$universal συναρτήσεις τότε έχουμε εξασφαλισμένο ότι

$$D\left(\rho_{KRE}, \frac{\mathbb{I}}{2^\ell} \otimes \rho_{RE}\right) \leq \varepsilon$$

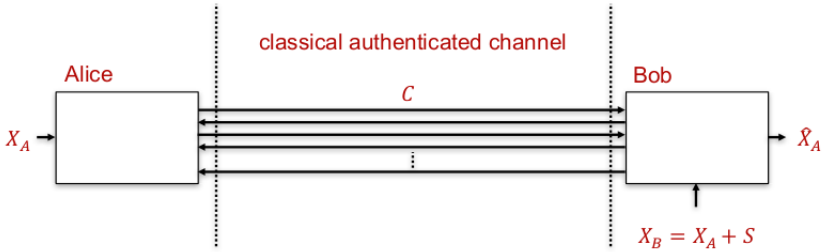
κάθε φορά που $\ell \leq H_{\min}(X|E) - 2\log(1/\varepsilon) - 1$ όπως δείχνεται στο [57]. Άρα, κάθε φορά που παράγουμε ένα κλειδί που είναι το πολύ $\ell \leq n(-\log q) - 2\log(1/\varepsilon) - 1$ bits σε μήκος με αυτή τη διαδικασία, τότε ξέρουμε ότι είναι $\epsilon-$ασφαλές. Γενικά, στη κρυπτογραφία τυπικά σταθεροποιούμε τα ϵ και ℓ από πριν, και μετά θέτουμε το ερώτημα πόσο μεγάλο πρέπει να είναι το n για να επιτύχουμε το επιθυμητό μήκος κλειδιού ℓ με την εγγύηση του ε.

Στην από πάνω εξίσωση μπορούμε να παρατηρήσουμε ότι αν η Eve μάθει αργότερα ποιά συνάρτηση $Ext(\cdot, r)$ χρησιμοποιήσαμε, δεν μπορεί να μάθει τίποτα για το κλειδί. Το γεγονός όμως ότι μαθαίνει το r αργότερα είναι ζωτικής σημασίας, διότι αν ήξερε το r από πριν, τότε τα πράγματα ίσως να ήταν τελείως διαφορετικά.

2.8.3 Συνδιαλλαγή πληροφοριών (information reconciliation)

Πριν την ενίσχυση της ιδιωτικότητας (privacy amplification), χρειαζόμαστε ένα ακόμα βήμα αυτό της συνδιαλλαγής πληροφοριών (information reconciliation), κατά το οποίο ανταλλάσουμε πληροφορίες ώστε να διορθωθούν τυχόν σφάλματα (σχήμα 2.12).

Η Αλίκη και ο Bob, λοιπόν κρατάνε δύο ακολουθίες X_A και X_B. Η ακολουθία του Bob η X_B, ισούται με την ακολουθία X_A και επιπλέον μια ακολουθία από σφάλματα που τη λέμε S. Η Αλίκη και ο Bob συνδέονται μέσω ενός CAC. Συμβολίζουμε με C την ακολουθία που αποτελείται από όλα τα μηνύματα τα οποία στάλθηκαν μέσω του κλασικού καναλιού. Τέλος, ο Bob, με τη βοήθεια του X_B και του C θα βγάλει ένα X_A, το οποίο είναι η εκτίμηση ,$\hat{X}_A$, της ακολουθίας της Αλίκης.



Σχήμα 2.12: Σχέδιο πρωτοκόλλου συμφωνίας γενικής πληροφόρησης

Ορισμός 2.61. *Συνδιαλλαγή πληροφοριών. Έστω X_A, X_B να είναι κατανεμημένα σύμφωνα με την από κοινού κατανομή πιθανότητας $P_{X_A X_B}$. Ένα πρωτόκολλο συνδιαλλαγής πληροφοριών για τα X_A, X_B είναι $\varepsilon-$σωστό και δίνει $|C|$ bits αν*

- $\text{Prob}\left(X_A \neq X_B\right) \leq \varepsilon$.
- *Το μήκος των μηνυμάτων που ανταλλάσονται στο δημόσιο κανάλι είναι $|C|$.*

Οι στόχοι της συνδιαλλαγής πληροφοριών είναι δύο:

1. Η Αλίκη και ο Bob θέλουν να σιγουρευτούν ότι μετά το r οι ακολουθίες X_A και $\hat{X}_A$ είναι $\varepsilon-$σωστές, δηλαδή ότι η πιθανότητα ότι είναι διαφορετικές είναι το πολύ ε.

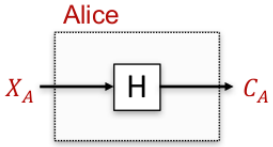
2. Όλη η κλασική επικοινωνία μεταξύ τους είναι δημόσια, που σημαίνει ότι η Eve μπορεί να ανακτήσει πληροφορία από τη πληροφορία για τη διόρθωση σφαλμάτων που ανταλλάσουν μεταξύ τους η Αλίκη και ο Bob. Αν θυμηθούμε τον κανόνα της αλυσίδας για την ελάχιστη εντροπία, έχουμε

$$H_{\min}(X|EC) \geq H_{\min}(X|E) - |C|$$

όπου C είναι η πληροφορία για τη διόρθωση σφαλμάτων που στάλθηκε μέσω του καναλιού. Έτσι έχουμε την ελάχιστη εντροπία της Eve μαζί με τη πληροφορία C να μπορεί να μειωθεί μόνο έως $|C|$ bits.

2.8.4 Κωδικοποίηση συνδρόμου (syndrome coding)

Από την θεωρία γραμμικών κωδίκων, έχουμε ότι η αντιστοίχηση $s_H : \mathbb{F}_2^n \to \mathbb{F}_2^m$ που δίνεται από $v \mapsto H \cdot v^T$ καλείται σύνδρομο. Το σχήμα συνδιαλλαγής (σχήμα 2.13) που θα δούμε στη συνέχεια στηρίζεται στο πίνακα ισοτιμίας H που συμφωνεί η Αλίκη με τον Bob. Ας δούμε πρώτα το βήμα κωδικοποίησης της Αλίκης. Το σχήμα στηρίζεται στους γραμμικούς κώδικες, δοθέντος ενός πίνακα ισοτιμίας H και ένα διάνυσμα x_A για την Αλίκη, η κωδικοποίηση του x_A είναι το σύνδρομό του. Αυτό σημαίνει, ότι το μήνυμα που στέλνει η Αλίκη στον Bob για συνδιαλλαγή πληροφοριών είναι το σύνδρομο του x_A.

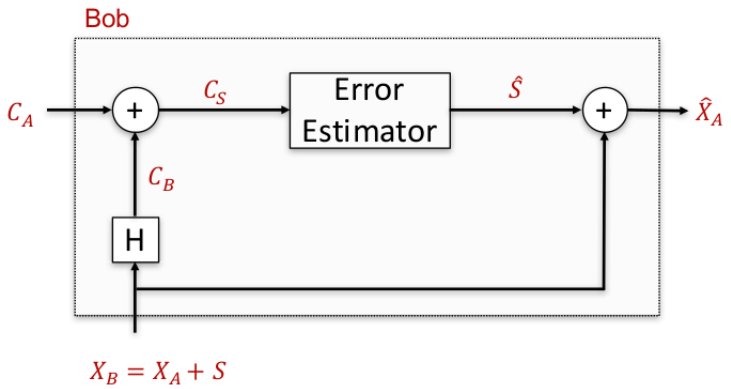


Σχήμα 2.13: Η κωδικοποίηση μέσω γραμμικών κωδίκων για τη συνδιαλλαγή πληροφοριών

Παράδειγμα 2.8.1. Έστω $v = (001)$ και $H = \begin{pmatrix} 110 \\ 011 \end{pmatrix}$. Τότε $s_H(v) = H \cdot v^T = (01)^T$. Αυτό σημαίνει ότι αν το v ήταν η ακολουθία που είχε η Αλίκη, το μήνυμα που έστειλε στον Bob για reconciliation θα είναι το $s_H(v)$, το οποίο είναι αυτό που υπολογίσαμε: $(01)^T$.

Στη συνέχεια, ας υποθέσουμε ότι ο Bob, έχει έναν αποκωδικοποιητή, ο οποίος είναι μια διαδικασία που τον βοηθάει να εκτιμά την ακολουθία σφάλματος S (όπου $X_B = X_A + S$), ώστε να πάρει το X_A. Ο αποκωδικοποιητής είναι λίγο πιο περίπλοκος (σχήμα 2.14) καθώς παίρνει ως είσοδο και το C_A και το X_B. Το πρώτο πράγμα που συμβαίνει στον αποκωδικοποιητή είναι ότι υπολογίζει το σύνδρομο X_B το οποίο καλούμε C_B. Ύστερα ο Bob υπολογίζει το $C_S = C_B + C_A$, όπου C_A το σύνδρομο του X_A. Το C_S είναι το σύνδρομο της ακολουθίας σφάλματος, δηλαδή $C_S = s_H(S)$. Τότε το C_S στέλνεται σε ένα module που εκτιμά την ακολουθία σφάλματος S και παράγει την εκτίμηση την οποία καλούμε $\hat{S}$. Στο τέλος το $\hat{S}$ προστίθεται στο X_B και αυτό είναι η αποκωδικοποιημένη ακολουθία που θα παραλάβει ο Bob.

Βέβαια, όπως μπορούμε να παρατηρήσουμε, όσο το μήκος της ακολουθίας της Αλίκης που στέλνει στον Bob, είναι μικρότερο από την ακολουθία της Αλίκης, τότε δεν μπορούν να διορθωθούν όλα τα σφάλματα. Αν η συνάρτηση εκτίμησης παράγει διαφορετική τιμή για κάθε σύνδρομο έχουμε 2^n διαφορετικά αποτελέσματα, και 2^n διαφορετικές ακολουθίες σφάλματος, με άλλα



Σχήμα 2.14: Η αποκωδικοποίηση μέσω γραμμικών κωδίκων για τη συνδιαλλαγή πληροφοριών.

λόγια αν το m δεν είναι ίσο με το n, δεν είναι εφικτό να διορθωθούν όλα τα λάθη. Παρόλα αυτά, αν διαφορετικά σφάλματα παρουσιαστούν με διαφορετικές πιθανότητες μπορούμε να είμαστε ικανοποιημένοι αν διορθώσουμε τα πιο πιθανά σφάλματα.

2.8.5 Όρια του reconciliation

Ας υποθέσουμε ότι οι ακολουθίες της Αλίκης και του Bob, τις οποίες συμβολίζουμε ως X_A^n και X_B^n, είναι μήκους n, όπου καθένα σύμβολο έχει παρθεί ανεξάρτητα από την κοινή κατανομή $P_{X_A X_B}$. Τότε το πρωτόκολλο για συνδιαλλαγή πληροφοριών, από το οποίο διαρρέουν $|C|$ bits πληροφορίας ικανοποιεί τη σχέση:

$$|C| \geq n \cdot H\left(X_A|X_B\right)$$

Η ισότητα επιτυγχάνεται για $n \to \infty$ [58], [59].

2.9 BB84 πρωτόκολλο

Αφού μελετήσαμε τις βάσεις για ένα σωστό και ασφαλές πρωτόκολλο διαμοίρασης κλειδιού, στη συνέχεια θα αναλύσουμε το πρωτόκολλο BB84 που είναι από τα σημαντικότερα κβαντικής διαμοίρασης κλειδιού. Το μόνο το οποίο θα έχουμε να κάνουμε είναι να προετοιμάσουμε και να μετρήσουμε απλές κβαντικές καταστάσεις [66].

Ορισμός 2.62. *BB84 καταστάσεις-κωδικοποίηση. Οι καταστάσεις του BB84 είναι οι* $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. *Αυτό το σύνολο καταστάσεων αντιστοιχεί στη κωδικοποίηση ενός κλασικού bit* $x_j \in \{0, 1\}$ *σε μια τυχαία επιλεγμένη βάση* $\theta_j \in \{0, 1\}$, *όπου* $\theta_j = 0$ *συμβολίζει τη τυπική βάση (η οποία είναι και ιδιοβάση του πίνακα Pauli-Z και η* $\theta_j = 1$ *τη βάση Hadamard (η οποία είναι ιδιοβάση του Pauli-X).*

Ορισμός 2.63. *Οι* $6-$*κατάστασεις κωδικοποίησης (six-state encoding) είναι οι* $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+y\rangle, |-y\rangle\}$, *όπου*

$$|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

Αυτό το σύνολο καταστάσεων αντιστοιχεί στη κωδικοποίηση ενός κλασικού bit $x_j \in \{0,1\}$ σε μια τυχαία επιλεγμένη βάση $\theta_j \in \{0,1,2\}$, όπου $\theta_j = 0$ συμβολίζει τη τυπική βάση, $\theta_j = 1$ τη βάση Hadamard και $\theta_j = 2$ την ιδιοβάση του πίνακα Pauli-Y.

Πρωτόκολλο BB84 (χωρίς θόρυβο) (1)

1: Για μια παράμετρο $\eta \ll 1$ που παίρνει μικρές τιμές πραγματικές, και ένα μεγάλο ακέραιο $n >> 1$, η Αλίκη διαλέγει μια ακολουθία $x = x_1, \ldots, x_N \in \{0,1\}^N$ τυχαία, ομοιόμορφα κατανεμημένη όπου $N = (4+\eta)n$. Επίσης διαλέγει μια ακολουθία βάσης $\theta = \theta_1, \ldots, \theta_N$ πάλι τυχαία και ομοιόμορφα κατανεμημένη. Στέλνει στον Bob κάθε bit x_j το οποίο κωδικοποιεί σε μια κβαντική κατάσταση σύμφωνα με τη βάση θ_j : $H^{\theta_j} |x_j\rangle$.

2: Ο Bob διαλέγει μια ακολουθία βάσης $\tilde{\theta} = \tilde{\theta}_1, \ldots, \tilde{\theta}_N$ τυχαία ομοιόμορφα κατανεμημένη. Μετράει το qubit j στη βάση $\tilde{\theta}_j$ για να πάρει το αποτέλεσμα $\tilde{x}_j$. Αυτό του δίνει μια ακολουθία $\tilde{x} = \tilde{x}_1, \ldots, \tilde{x}_N$.

3: Ο Bob λέει στην Αλίκη μέσω του CAC, ότι έλαβε τα qubits και τα μέτρησε.

4: Η Αλίκη και ο Bob λένε μέσω του CAC τις ακολουθίες βάσεων θ και $\tilde{\theta}$ αντίστοιχα.

5: Η Αλίκη και ο Bob πετάνε όλους τους γύρους j για τους οποίους δεν μέτρησαν στην ίδια βάση. Έστω $S = \left\{ j | \theta_j = \tilde{\theta}_j \right\}$ να συμβολίζει τους δείκτες των γύρων για τους οποίους μέτρησαν στην ίδια βάση. Αφού έχουν διαλέξει τα $\theta, \tilde{\theta}$ τυχαία, για μεγάλες τιμές του n, πετάνε περίπου $N/2 \approx 2n$ bits.

6: Η Αλίκη διαλέγει ένα τυχαίο υποσύνολο $T \subseteq S$ για να ελέγξει και λέει στον Bob το T στο CAC. Άρα η Αλίκη και ο Bob τεστάρουν περίπου $|T| \approx N/4 \approx n$ bits.

7: Ανακοινώνουν τα x_T και $\hat{x_T}$ μεταξύ τους στο CAC, όπου συμβολίζουμε με x_T την υπακολουθία του x που αντιστοιχεί στους δείκτες του συνόλου για το τεστ T. Υπολογίζουν το ποσοστό σφάλματος $\delta = W/|T|$, όπου $W = |\{j \in T | x_j \neq \tilde{x}_j\}|$ είναι ο αριθμός των σφαλμάτων όταν μέτρησαν στην ίδια βάση.

8: Αν το ποσοστό σφάλματος είναι $\delta \neq 0$, τότε παρατάνε το πρωτόκολλο. Αλλιώς προχωράνε και συμβολίζουν με $x_{remain} = x_{S \setminus T}$ και $\tilde{x}_{remain} = \tilde{x}_{S \setminus T}$, τα εναπομείναντα bits, δηλαδή τα bits όπου μέτρησαν και οι δύο στην ίδια βάση, αλλά αυτά τα οποία δεν χρησιμοποίησαν για το τέστ. Το μήκος των x_{remain} και $\tilde{x}_{remain}$ είναι περίπου n bits.

9: Εφαρμόζουν privacy amplification: Η Αλίκη διαλέγει ένα τυχαίο r, και υπολογίζει το $k = Ext\left(x_{remain}, r\right)$. Στέλνει στον Bob το r, ο οποίος υπολογίζει το $k = Ext\left(\tilde{x}_{remain}, r\right)$.

Αν δεν υπάρχουν σφάλματα κατά τη μετάδοση, τότε κάθε φορά που ο Bob μετράει στην ίδια βάση όπως αυτή που διάλεξε η Αλίκη $\left(\theta_j = \tilde{\theta}_j\right)$, τότε μαθαίνει το bit τέλεια $(x_j = \tilde{x}_j)$. Αν δεν υπάρχει ωπτοακουστής, θα περάσουν το τεστ. Καθώς $x_{remain} = \tilde{x}_{remain}$ και ο Bob ξέρει το r μπορεί να παράξει το ίδιο k με πριν.

Κάθε φορά που η Eve προσπαθεί να μπει ανάμεσα, και να ανακτήσει κάποια πληροφορία για τα μεταδιδόμενα qubits, θα επηρεάσει κατά κανόνα τις κβαντικές καταστάσεις και η Αλίκη και ο Bob θα εντοπίσουν αυτή τη διατάραξη. Μπορεί να αποδειχθεί ότι

$$H_{\min}\left(X_{remain}|E\right) > n[1 - h(\delta)]$$

όπου $h(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$ είναι η δυαδική συνάρτηση εντροπίας και το δ είναι το error rate μεταξύ τους. Ας σημειώσουμε ότι η διαδικασία ανάλυσης του δείγματος, δηλαδή

ποιά qubits να τεστάρουμε, για μικρές τιμές του N είναι αρκετά περίπλοκο πρόβλημα που θέλει ιδιαίτερη προσοχή, όπως αναλύεται στο $[62]$.

Στη περίπτωση που έχουμε σφάλμα κατά τη μετάδοση, το error rate είναι πάντα $\delta \neq 0$. Αυτό επηρεάζει τη σωστότητα του πρωτοκόλλου, καθώς η Αλίκη και ο Bob θα πάρουν τα $x_{remain}, \tilde{x}_{remain}$ αντίστοιχα, με $x_{remain} \neq \tilde{x}_{remain}$. Στη πραγματικότητα, όταν $x_{remain} \neq \tilde{x}_{remain}$, από ιδιότητα του εξαγωγέα Ext , με πιθανότητα σχεδόν 1, έχουμε $Ext\left(x_{remain}, r\right) \neq Ext\left(\tilde{x}_{remain}, r\right)$. Αυτό σημαίνει, ότι σχεδόν σίγουρα, η Αλίκη και ο Bob θα καταλήξουν με διαφορετικά κλειδιά.

Για να προσπεράσουμε αυτό το πρόβλημα, πρέπει και οι δύο να εφαρμόσουν άλλο ένα βήμα αυτό της συνδιαλλαγής πληροφοριών. Άρα έχουμε το πρωτόκολλο που ακολουθεί.

Πρωτόκολλο BB84 με θόρυβο (2)

1: Τα βήματα 1-7 είναι ίδια όπως πριν.
2: Αν το error rate είναι μεγαλύτερο από κάποιο όριο $\delta > \delta_t$, η Αλίκη και ο Bob παρατάνε το πρωτόκολλο. Αλλιώς προχωράνε, να συμβολίσουν με $x_{\text{ρεμαιν}} = x_{S\setminus T}$ και $\tilde{x}_{\text{ρεμαιν}} = \tilde{x}_{S\setminus T}$ τα εναπομείναντα bits, δηλαδή τα bits τα οποία μέτρησαν και οι δύο στην ίδια βάση, αλλά δεν χρησιμοποίησαν για τεστ.
3: Εφαρμόζουν συνδιαλλαγή πληροφοριών: Η Αλίκη στέλνει κάποια πληροφορία διόρθωσης σφάλματος C, μέσω του CAC, στον Bob και ο ο Bob διορθώνει τα σφάλματα στην ακολουθία $\tilde{x}_{remain}$, ώστε να λάβει και αυτός το x_{remain} από τη διαδικασία.
4: Το βήμα 10 είναι ίδιο όπως πριν.

2.9.1 Ασφάλεια του BB84

¨Καθαρισμένο¨ BB84 πρωτόκολλο (purified)

Στο πρώτο πείραμα, η Αλίκη και ο Bob διαλέγει $x, \theta \in \{0,1\}$ και επιστρέφει $|x\rangle_\theta = H^\theta |x\rangle$, μια κωδικοποίηση ενός bit x στη καθορισμένη βάση θ. Στο δεύτερο πείραμα, η Αλίκη ετοιμάζει ένα EPR ζευγάρι $|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Ύστερα διαλέγει ένα $\theta \in \{0,1\}$ και μετράει το πρώτο qubit στη βάση $\{|0\rangle_\theta, |1\rangle_\theta\}$, παίρνοντας ως αποτέλεσμα $x \in \{0,1\}$. Επιστρέφει το δεύτερο qubit. Ισχυριζόμαστε ότι τα δύο πειράματα είναι εντελώς ισάξια. Πρέπει να εξακριβώσουμε δύο πράγματα.

Αρχικά, ενώ στο πρώτο πείραμα η Αλίκη κάνει την επιλογή του x τυχαία, στο δεύτερο, το x καθορίζεται ως το αποτέλεσμα της μέτρησης ενός EPR ζευγαριού. Ξέρουμε όμως ότι καθώς ο μειωμένος πίνακας πυκνότητας του EPR ζευγαριού στο πρώτο qubit είναι το totally mixed state, κάθε μέτρηση βάσης σε αυτό το qubit θα γυρίσει καθένα από τα δύο πιθανά αποτελέσματα με πιθανότητα $1/2$. Άρα η κατανομή του x είναι πανομοιότυπη και στα δύο πειράματα.

Στη συνέχεια, πρέπει να ελέγξουμε ότι όταν η Αλίκη παίρνει το αποτέλεσμα x μετρώντας το πρώτο qubit από το EPR ζευγάρι στη βάση θ, το qubit που επιστρέφει, δηλαδή το δεύτερο qubit του EPR ζευγαριού, είναι όντως προβαλόμενο στη κατάσταση $|x\rangle_\theta$. Πάλι αυτή είναι μια ιδιότητα της EPR κατάστασης η οποία είναι έγκυρη για οποιαδήποτε επιλογή μέτρησης βάσης στο πρώτο qubit, οπότε είμαστε εντάξει. Τα δύο πειράματα είναι πανομοιότυπα.

Οπότε ας θεωρήσουμε μια παρόμοια διατύπωση με το πρωτόκολλο BB84, στο οποίο αντί να ετοιμάζουμε κατευθείαν BB84 καταστάσεις, η Αλίκη ετοιμάζει EPR ζευγάρια, κρατάει το πρώτο qubit από κάθε ζευγάρι για τον εαυτό της, και στέλνει το δεύτερο qubit στον Bob. Σε μετέπειτα

στάδιο μετράει το qubit της σε μια βάση $\theta_j \in \{0,1\}$ που έχει διαλέξει τυχαία, και καταγράφει το αποτέλεσμα x_j.

¨Καθαρό¨ πρωτόκολλο BB84 χωρίς θόρυβο (3)

1: Για σχετικά μικρή πραγματική παράμετρο $\eta \ll 1$, και μεγάλο ακέραιο $n \gg 1$, θέτουμε $N = (4+\eta)n$. Η Αλίκη ετοιμάζει N EPR ζευγάρια $|\phi^+\rangle_{AB}$, και στέλνει το δεύτερο qubit από κάθε ζευγάρι στον Bob. Διαλέγει τυχαία μια ακολουθία βάσης $\theta = (\theta_1, \ldots, \theta_N) \in \{0,1\}^N$ και μετράει καθένα από τα qubits της στις θέσεις θ για να πάρει μια ακολουθία $x = x_1, \ldots, x_N$.

2: Ο Bob διαλέγει μια ακολουθία βάσης τυχαία $\tilde{\theta} = \left(\tilde{\theta}_1, \ldots, \tilde{\theta}_N\right) \in \{0,1\}^N$. Μετράει το $j-$οστό qubit που παρέλαβε από την Αλίκη στη βάση $\tilde{\theta}_j$ ώστε να πάρει το αποτέλεσμα $\tilde{x}_j$.

3: Ο Bob λέει στην Αλίκη μέσω του CAC ότι έλαβε και μέτρησε όλα τα qubits.

4: Ανταλλάσουν τις βάσεις θ και $\tilde{\theta}$ μέσω του CAC.

5: Πετάνε όλα τα δεδομένα από όλους τους γύρους $j \in \{1, \ldots, N\}$, στους οποίους δεν μέτρησαν στην ίδια βάση. Έστω $S = \left\{j | \theta_j = \tilde{\theta}_j\right\}$ να δηλώνει τους δείκτες για τους οποίους μέτρησαν στην ίδια βάση.

6: Η Αλίκη διαλέγει ένα τυχαίο υποσύνολο $T \subseteq S$ μεγέθους $T \approx |S|/2$ για να τεστάρει και λέει στον Bob το T μέσω του CAC.

7: Ανακοινώνουν τα x_T και $\tilde{x_T}$ μεταξύ τους μέσω του CAC. Υπολογίζουν το ρυθμό σφάλματος $\delta = W/|T|$, όπου $W = |\{j \in T | x_j \neq \tilde{x}_j\}|$ είναι ο αριθμός των διαφωνιών που βρίσκονται στο T. Αν το δ είναι πολύ μεγάλο, εγκαταλείπουν το πρωτόκολλο.

8: Έστω $R = S \backslash T$. Εφαρμόζουν information reconciliation και privacy amplification στο x_R.

Το παραπάνω πρωτόκολλο στηρίζεται στην ιδέα του Ekert. Γενικά είναι πιο εύκολο να ετοιμάσουμε κβαντικές BB84 καταστάσεις παρά να διαμοιράσουμε EPR ζευγάρια σε μακρινές αποστάσεις.

Περισσότερη δύναμη στον ωπτοακουστή

Το κίνητρο για τη δεύτερη παραλλαγή του BB84 είναι ότι είναι δύσκολο να μοντελοποιήσουμε τα είδη επίθεσης που μπορεί να επιχειρήσει η Eve στο κβαντικό κανάλι επικοινωνίας μεταξύ της Αλίκης και του Bob. Για παράδειγμα, μπορεί να διεμπλακεί μερικώς με τα qubits που στέλνει η Αλίκη, δημιουργώντας έτσι μια αρθρωτή κατάσταση ρ_{ABE} στην οποία θα έχουμε μειωμένο έλεγχο και δυνατότητες.

Θα δώσουμε τη δυνατότητα στην Eve να προετοιμάσει μια τυχαία καθαρή κατάσταση ρ_{ABE}, όπου A και B συστήματα φτιαγμένα από N qubits, και να δώσει το A στην Αλίκη και το B στον Bob και να κρατήσει το E. Η Αλίκη και ο Bob θα μετρήσουν τα αντίστοιχα qubits τους χρησιμοποιώντας τυχαίες επιλογές βάσεων όπως πρωτόκολλο που εξηγήσαμε προηγουμένως.

Αυτό φαίνεται παράλογο, να φτιάχνει τις καταστάσεις η Eve, αλλά θα δούμε στη συνέχεια γιατί το διαλέξαμε έτσι.

Τοπική εφαρμογή μιας διεμπλεγμένης μέτρησης

Ας υποθέσουμε ότι τροποποιούμε λίγο το BB84 προσθέτωντας πριν από όλα το εξής βήμα.

- Καθώς λαμβάνουν τα αντίστοιχα N qubits από την Eve, η Αλίκη και ο Bob μετράνε μαζί κάθε ζευγάρι των qubits χρησιμοποιώντας το POVM

  $\left\{\left|\phi^+\right\rangle\left\langle\phi^+\right|_{AB}, \mathbb{I}_{AB} - \left|\phi^+\right\rangle\left\langle\phi^+\right|_{AB}\right\}$, όπου $\left|\phi^+\right\rangle_{AB}$ συμβολίζει το EPR ζευγάρι του από κοινού συστήματος της Αλίκης και του Bob. Αν ο αριθμός των ζευγαριών που δεν βρέθηκαν ίσα με το $\left|\phi^+\right\rangle_{AB}$ είναι μεγαλύτερος από δn τότε εγκαταλείπουν το πρωτόκολλο 3. Αλλιώς προχωράνε κανονικά.

Ύστερα από αυτό το βήμα, η Αλίκη και ο Bob έχουν την εγγύηση ότι τουλάχιστον $(1-\delta)n$ από τα ζευγάρια που πήραν είναι τέλεια EPR ζευγάρια. Συγκεκριμένα, κάθε bit του raw κλειδιού που αποκτιέται από μετρήσεις σε αυτές τις καταστάσεις είναι ασύνδετο με την Eve (οι σχέσεις από καθαρές καταστάσεις είναι πάντα τέλεια μονογαμικές).

Το πρόβλημα με αυτό το βήμα είναι ότι η Αλίκη και ο Bob πρέπει να εφαρμόσουν μια αρθωτή μέτρηση, την οποία δεν ξέρουμε αν μπορούν την υλοποιήσουν τοπικά.

Έστω μια 'τριπλή' κατάσταση ρ_{ABE} όπου A, B συστήματα ενός qubit. Η πιθανότητα μια μέτρηση των συστημάτων A, B στη standard βάση μας δίνει αποτέλεσμα ακριβώς $\mathrm{Tr}\left(\Pi_1\rho_{AB}\right)$, όπου

$$\Pi_1 = \left|\phi^+\right\rangle\left\langle\phi^+\right| + \left|\Psi_{01}\right\rangle\left\langle\Psi_{01}\right|, \quad \text{και} \quad \left|\Psi_{01}\right\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Επίσης, αν η μέτρηση εφαρμοστεί στη βάση Hadamard η πιθανότητα είναι $\mathrm{Tr}\left(\Pi_2\rho_{AB}\right)$, με

$$\Pi_2 = \left|\phi^+\right\rangle\left\langle\phi^+\right| + \left|\Psi_{10}\right\rangle\left\langle\Psi_{10}\right|, \quad \text{και} \quad \left|\Psi_{10}\right\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

Συμπεράσματα

Συμπεραίνουμε ότι, τα matching outcomes tests που η Αλίκη και ο Bob εφαρμόζουν στο βήμα 7 του πρωτοκόλλου 3 είναι ουσιαστικά ισοδύναμα με το βήμα που είδαμε προηγουμένως. Άρα η ασφάλεια του πρωτοκόλλου με το βήμα $"0"$ ας το πούμε, συνεπάγεται κατευθείαν την ασφάλεια του πρωτοκόλλου χωρίς το βήμα $"0"$, αλλά με το βήμα 7.

Για να εκφράσουμε τη σχέση ανάμεσα στα δύο βήματα, ας θεωρήσουμε το μειωμένο πίνακα πυκνότητας, $\rho_{A_jB_j}$ της κατάστασης που ετοίμασε η Eve σε οποιαδήποτε δύο qubits για την Αλίκη και τον Bob, και έστω p_j η πιθανότητα επιτυχίας του τεστ matching outcomes. Ύστερα, εκφράζοντας το $\rho_{A_jB_j}$ στη Bell βάση έχουμε

$$\rho_{A_jB_j} = q_{00}\left|\phi^+\right\rangle\left\langle\phi^+\right| + q_{01}\left|\Psi_{01}\right\rangle\left\langle\Psi_{01}\right| + q_{10}\left|\Psi_{10}\right\rangle\left\langle\Psi_{10}\right| + q_{11}\left|\Psi_{11}\right\rangle\left\langle\Psi_{11}\right|$$

και χρησιμοποιώντας τις εκφράσεις για τα Π_1 και Π_2 από παραπάνω, έχουμε τη συνθήκη

$$q_{00} = \left\langle\Psi_{00}\right|\rho_{A_jB_j}\left|\Psi_{00}\right\rangle \geq 2p_j - 1$$

που ικανοποείται. Πιο συγκεκριμένα, η πιθανότητα επιτυχίας του τέστ είναι κοντά στο 1, ας πούμε $p_j = 1-\delta$ για κάποιο μικρό δ.

Τα δύο tests δεν είναι ακριβώς ισάξια, και αυτό απαιτεί λίγο περισσότερη δουλειά. Μια πρώτη διαφορά είναι ότι στο πρωτόκολλο 3, το βήμα 7 εφαρμόζεται στους γύρους T που έχουν διαλεχτεί για τον έλεγχο , ενώ είναι οι γύροι $R = S\backslash T$ που χρησιμοποιούνται για το raw key.

Μια άλλη δυσκολία είναι ότι τα αποτελέσματα των tests που εκτελούνται σε διαφορετικούς γύρους δεν είναι ανεξάρτητα μεταξύ τους: παρόλο που η Αλίκη και ο Bob κάνουν ανεξάρτητες μετρήσεις, η κατάσταση ρ_{ABE} που ετοιμάζεται από την Eve δεν είναι απαραίτητο ότι έχει τη μορφή τανυστικού γινομένου.

Η δεύτερη διαφορά υψώνει μια δυσκολία. Θα τη δούμε αργότερα όμως. Ας επικεντρωθούμε στη πρώτη. Πώς συμπεραίνουμε συνθήκες στα qubits στους γύρους $j \in S\backslash T$ από τα αποτελέσματα των tests που εκτελούνται στα qubits στους γύρους $j \in T$;

Μια ανισότητα συγκέντρωσης

Ας υποθέσουμε για απλότητα ότι ο αριθμός (S) των γύρων στους οποίους η Αλίκη και ο Bob διαλέγουν την ίδια βάση είναι ακριβώς $|S| = 2n$, και ότι το T έχει μέγεθος $|T| = |S|/2 = n$. Για κάθε $j \in S$, εισάγουμε μια τυχαία μεταβλητή ως δείκτη $Z_j \in \{0, 1\}$ τέτοια ώστε $Z_j = 1$ να δηλώνει την αποτυχία στο matching outcomes test και $Z_j = 0$ αν $x_j = \tilde{x}_j$. Με αυτό το συμβολισμό η συνθήκη που ικανοποείται και τους δύο στο βήμα 7 του πρωτοκόλλου 3 μπορεί να γραφεί ως $\Sigma_{j\in T} Z_j \leq \delta|T|$. Για να αναλύσουν όμως την ασφάλεια του κλειδιού τους, πρέπει να φράξουν το $\sum_{j\in S\backslash T} Z_j$.

Η ιδέα για να γίνει αυτό είναι να χρησιμοποιήσουμε το γεγονός ότι το T είναι τυχαία επιλεγμένο υποσύνολο. Διαισθητικά, ο μέσος όρος αποτυχιών στο T πρέπει να είναι περίπου ο ίδιος με ολόκληρο το S.

Για να γίνει αυτή η διαίσθηση ακριβής, χρειαζόμαστε κάτι που αποκαλούμε φράγμα συγκέντρωσης (concetration bound). Υπάρχουν πολλά τέτοια, το πιο διάσημο όμως είναι το φράγμα Chernoff ή αλλιώς ανισότητα Hoeffding. Ακολουθεί μια παραλλαγή του concetration bound:

Θεώρημα 2.64. *Έστω $m = n + k$ και ας θεωρήσουμε δυαδικές τυχαίες μεταβλητές $X_1, \ldots, X_m$ (τα X_i μπορεί να συσχετίζονται μεταξύ τους). Έστω T ένα τυχαίο υποσύνολο $\{1, \ldots, m\}$ μεγέθους k. Τότε για κάθε $\delta, v > 0$:*

$$\Pr\left(\sum_{j\in T} X_j \leq \delta k \wedge \sum_{j\in\{1,\ldots,m\}\backslash T} X_j \geq (\delta + v)n\right) \leq e^{-2v^2 \frac{n^2}{(n+k)(k+1)}}$$

Για τη περίπτωσή μας, θέτουμε $m = |S| = 2n$ και $k = n$. Επίσης $v = \delta$ για διευκόλυνση. Με αυτές τις παραμέτρους έχουμε

$$\Pr\left(\sum_{j\in T} Z_j \leq \delta n \wedge \sum_{j\in S\backslash T} Z_j \geq 2\delta n\right) \leq e^{-\delta^2 n}$$

το οποίο είναι έγκυρο για οποιοδήποτε $\delta > 0$. Αυτό το φράγμα συνεπάγεται ότι η πιθανότητα ότι το test που εφαρμόζεται στο βήμα 7 περνάει, αλλά το αποτέλεσμα στους γύρους χωρίς test $R = S\backslash T$ δεν ταιριάζουν σε βαθμό κλάσματος μεγαλύτερου του 2δ, είναι μικροσκοπική ή αλλιώς εκθετικά μικρή στο n. Γράφοντας ως ABORT το γεγονός να εγκαταλείψουν το πρωτόκολλο στο βήμα 7, μπορούμε να χρησιμοποιήσουμε το νόμο του Bayes για να ξαναγράψουμε το φράγμα ως

$$\Pr\left(\sum_{j\in ST} Z_j \geq 2\delta n | \neg \mathrm{ABORT}\right) \leq \frac{e^{-\delta^2 n}}{\Pr(\neg\,\mathrm{ABORT})}$$

Πρέπει να λαμβάνουμε υπόψη αυτή τη πιθανότητα να εγκαταλείψουμε το πρωτόκολλο.Στη συνέχεια, λόγω του θέματος με τις εξαρτήσεις μεταξύ διαφόρων τεστς που μπορεί να προκύψουν αν η Eve ετοιμάσει μια κατάσταση η οποία δεν είναι σε μορφή τανυστικού γινομένου.

2.10 Κβαντικοί αλγόριθμοι γύρω από τη κρυπτογραφία

Κβαντικός Μετασχηματισμός Fourier

Διακριτός Μετασχηματισμός Fourier (DFT)

Ο Διακριτός Μετασχηματισμός Fourier (Discrete Fourier Transform-DFT), ο οποίος είναι το πεπερασμένο διακριτό αντίστοιχο των σειρών Fourier, αποτελεί το σημαντικότερο εργαλείο ευρείας χρήσεως της ψηφιακής τεχνολογίας. Μπορεί να θεωρηθεί ως μία προσέγγιση των συνήθων σειρών Fourier, αλλά πιο συγκεκριμένα, ο DFT μετασχηματίζει πεπερασμένες ακολουθίες πραγματικών ή μιγαδικών αριθμών (διακριτά σήματα) σε μιγαδικές ακολουθίες, οι οποίες διατηρούν όλη την πληροφορία του αρχικού σήματος.

Ας υποθέσουμε ότι έχουμε ένα διάνυσμα f με N μιγαδικούς αριθμούς, $f_k, k \in \{0, 1, \ldots, N-1\}$. Τότε ο DFT είναι μια απεικόνιση των N μιγαδικών αριθμών σε αντίστοιχους N μιγαδικούς αριθμούς, οι οποίοι είναι οι αλλαγμένες κατά Fourier συντεταγμένες $\tilde{f}_j$, που δίνονται από το τύπο

$$\tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{-jk} f_k$$

όπου $\omega = \exp\left(\frac{2\pi i}{N}\right)$. Ο αντίστροφος μετασχηματισμός Fourier δίνεται από το τύπο

$$f_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} \tilde{f}_k$$

Μια σημαντική ιδιότητα του DFT είναι το θεώρημα συνέλιξης. Η κυκλική συνέλιξη δύο διανυσμάτων f, g δίνεται από

$$(f * g)_i = \sum_{j=0}^{N-1} f_j g_{i-j}$$

όπου ορίζουμε $g_{-m} = g_{N-m}$. Το θεώρημα της συνέλιξης μας λέει ότι ο DFT μετατρέπει τη συνέλιξη σε κατά σημείο πολλαπλασιασμό διανυσμάτων, δηλαδή αν οι συνιστώσες του DFT της συνέλιξης $(f * g)$ είναι $\tilde{c}_k$, τότε το $\tilde{c}_k = \tilde{f}_k \tilde{g}_k$.

Γρήγορος Μετασχηματισμός Fourier (FFT)

Για να εφαρμόσουμε έναν DFT χρειαζόμαστε N^2 μιγαδικούς πολλαπλασιασμούς και $N(N-1)$ μιγαδικές προσθέσεις. Ο στόχος του FFT είναι να το κάνουμε αυτό με λιγότερες μαθηματικές πράξεις. Στη περίπτωση που θα εξετάσουμε είναι $N = 2^n$. Θα θεωρήσουμε ότι ο Γρήγορος Μετασχηματισμός Fourier βασίζεται στο γεγονός ότι υπάρχουν κάποιες συμμετρίες όσον αφορά τους συντελεστές του DFT, όπως βλέπουμε παρακάτω

$$\omega^{k+N/2} = -\omega^k$$
$$\omega^{k+N} = \omega^k$$

Έστω ότι θέλουμε να εφαρμόσουμε τον DFT σε ένα διάνυσμα f. Χωρίζουμε τις συνιστώσες του f σε μικρότερα διανύσματα μήκους $N/2$, και τα ονομάζουμε e και o. Οι συντελεστές του e είναι οι συνιστώσες του f που είναι άρτιες (even) και οι συντελεστές του o οι συνιστώσες του f που είναι περιπές (odd). Η σειρά των συντελεστών διατηρείται. Οπότε θα έχουμε

$$\begin{aligned}\tilde{f}_j &= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\omega^{-ij}f_i = \frac{1}{\sqrt{N}}\sum_{i=0}^{N/2-1}\omega^{-2ij}e_i + \sum_{i=0}^{N/2-1}\omega^{-(2i+1)j}o_i \\ &= \frac{1}{\sqrt{N}}\left(\sum_{i=0}^{N/2-1}\omega_{N/2}^{-ij}e_i + \omega_N^{-j}\sum_{i=0}^{N/2-1}\omega_{N/2}^{-ij}o_i\right)\end{aligned}$$

όπου $\omega_{N/2} = \exp\left(\frac{2\pi i}{N}\right)$ και αλλάξαμε το ω σε ω_N για περισσότερη σαφήνεια. Οπότε έχουμε μια μέθοδο να υπολογίζουμε τον DFT της f με βάση τα e και o:

$$\tilde{f}_j = \tilde{e}_j + \omega_N^{-j}\tilde{o}_j$$

Το j διατρέχει τις τιμές από 0 έως $N-1$ και οι DFTs των e και f είναι περιοδικοί με περίοδο $N/2$. Οπότε βάσει αυτού και της συμμετρίας για τα ω παραπάνω, θα έχουμε

$$\begin{aligned}\sqrt{2}\tilde{f}_j &= \tilde{e}_j + \omega_N^{-j}\tilde{o}_j \quad 0 \le j \le N/2-1 \\ \sqrt{2}\tilde{f}_j &= \tilde{e}_j - \omega_N^{-j}\tilde{o}_j \quad N/2-2 \le j \le N-1\end{aligned}$$

Ας υποθέσουμε ότι πρώτα υπολογίζουμε το DFT για τα e και o και ύστερα χρησιμοποιούμε αυτή τη μέθοδο για τον υπολογισμό του DFT για ολόκληρο το f. Για να υπολογίσουμε το e και το o χρειαζόμαστε $2\frac{N^2}{2} = \frac{N^2}{2}$ πολλαπλασιασμούς. Επίσης χρειαζόμαστε άλλους $N/2$ για τον υπολογισμό του $\omega_N^{-j}\tilde{o}_j$. Ο συντελεστής $\sqrt{2}$ δεν παίζει τόσο ρόλο, απλά στο τέλος θα προσθέσει N πολλαπλασιασμούς. Άρα τελικά χρειαζόμαστε $\frac{N^2}{2} + \frac{N}{2}$ μιγαδικούς πολλαπλασιασμούς για να υπολογίσουμε το DFT, σε αντίθεση με τους N^2 που χρειαστήκαμε αρχικά. Αυτή η μείωση είναι της τάξης του 2 για μεγάλα N. Όσον αφορά τη τάξη πολυπλοκότητας μπορούμε να υπολογίσουμε τον DFT μέσω του FFT σε $NlogN$ πράξεις.

Μια εφαρμογή του FFT

Ας υποθέσουμε ότι έχουμε δύο πολυώνυμα με μιγαδικούς συντελεστές $f(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1}$ και $g(x) = b_0 + b_1x + \cdots + b_{N-1}x^{N-1}$. Αν πολλαπλασιάσουμε τα δύο αυτά πολυώνυμα

μεταξύ τους θα έχουμε ένα άλλο πολυώνυμο $f(x)g(x) = \sum_{ij=0}^{N-1} a_i b_j x^{i+j} = \sum_{k=0}^{2(N-1)} c_k x^k$. Οι νέοι συντελεστές για αυτό το πολυώνυμο θα είναι μια συνάρτηση των συντελεστών των δύο πολυωνύμων

$$c_k = \sum_{l=0}^{N-1} a_l b_{k-l}$$

Για να υπολογίσουμε το c_K απαιτούνται N^2 πολλαπλασιασμοί. Αν παρατηρήσουμε καλύτερα όμως, το c_K μοιάζει με συνέλιξη. Πράγματι, ας υποθέσουμε ότι κατασκευάζουμε ένα $2N-$διάστατο διάνυσμα $a = (a_0, \ldots, a_{N-1}, 0, \ldots, 0)$ και $b = (b_0, \ldots, b_{N-1}, 0, \ldots, 0)$. Το διάνυσμα c που θα αναπαριστά τους συντελεστές του νέου πολυωνύμου θα δίνεται από τη σχέση

$$c_k = \sum_{l=0}^{2N-1} a_l b_{k-l} \bmod 2N$$

Αυτό είναι ακριβώς μια συνέλιξη. Οπότε για να υπολογίσουμε τους συντελεστές c_K, υπολογίζουμε τους DFTs των a, b. Πολλαπλασιάζουμε κατά σημείο τα δύο διανύσματα και ύστερα αντιστρέφουμε τον DFT στο νέο διάνυσμα. Το αποτέλεσμα θα είναι το c_K από το θεώρημα συνέλιξης. Αν χρησιμοποιήσουμε τον FFT, τότε θα χρειαστούμε $O(N \log N)$ πολλαπλασιασμούς, το οποίο είναι αρκετά γρηγορότερο από τους κλασσικούς αλγορίθμους πολλαπλασιασμού πολυωνύμων.

Έστω η πύλη Hadamard

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

και έστω ένα qubit στη κατάσταση $a_0|0\rangle + a_1|1\rangle$. Αν εφαρμόσουμε το τελεστή Hadamard θα έχουμε τη νέα κατάσταση

$$\frac{1}{\sqrt{2}}(a_0 + a_1)|0\rangle + \frac{1}{\sqrt{2}}(a_0 - a_1)|1\rangle = \tilde{a}_0|0\rangle + \tilde{a}_1|1\rangle$$

Με άλλα λόγια η πύλη Hadamard εφαρμόζει τον DFT για $N = 2$ στα ορίσματα της κατάστασης. Αυτό είναι διαφορετικό από το να υπολογίσουμε τον DFT για $N = 2$. Τα ορίσματα δεν είναι αριθμοί, απλά αναπαριστούν τη περιγραφή του κβαντικού μας συστήματος. Για αυτό το λόγο η πύλη Hadamard αναφέρεται και ως "μετασχηματισμός Hadamard".

Ο κβαντικός μετασχηματισμός Fourier (QFT) είναι ένας μετασχηματισμός που παίρνει τα ορίσματα μιας $N-$διάστατης κατάστασης και υπολογίζει το μετασχηματισμό Fourier σε αυτά τα ορίσματα. Με άλλα λόγια, ο QFT εκτελεί το μετασχηματισμό

$$\sum_{x=0}^{N-1} a_x|x\rangle \to \sum_{x=0}^{N-1} \tilde{a}_x|x\rangle = \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} a_y|x\rangle$$

και απλά στις βασικές καταστάσεις

$$|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} |y\rangle$$

Οπότε ο QFT δίνεται από το πίνακα

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega_N^{-yx} |y\rangle\langle x|$$

ο οποίος είναι ορθογώνιος.

Ο QFT είναι από τους σημαντικότερους μετασχηματισμούς στην κβαντική υπολογιστική, αλλά ιδιαίτερα για τον αλγόριθμο του Shor με τον οποίο θα ασχοληθούμε στη συνέχεια. Πρώτα όμως πρέπει να δούμε πώς τον εφαρμόζουμε σε ένα κβαντικό κύκλωμα. Θα εξάγουμε λοιπόν ένα κβαντικό κύκλωμα για τον QFT για $N = 2^n$. Ο QFT εφαρμόζει το μετασχηματισμό

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_N^{-xy} |y\rangle$$

Αναπτύσσουμε το άθροισμα

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \sum_{y_1,y_2,\ldots,y_n \in \{0,1\}} \omega_N^{-x \sum_{k=1}^{n} 2^{n-k} y_k} |y_1, y_2, \ldots, y_n\rangle$$

Αναπτύσσουμε στη συνέχεια το εκθετικό άθροισμα σε γινόμενο εκθετικών και έχουμε

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \sum_{y_1,y_2,\ldots,y_n \in \{0,1\}} \bigotimes_{k=1}^{n} \omega_N^{-x 2^{n-k} y_k} |y_k\rangle$$

Ξαναμαζεύουμε λίγο τα αθροίσματα και τα γινόμενα

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \bigotimes_{k=1}^{n} \left[\sum_{y_k \in \{0,1\}} \omega_N^{-x 2^{n-k} y_k} |y_k\rangle \right]$$

και αναπτύσσουμε το άθροισμα που μας δίνει

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \bigotimes_{k=1}^{n} \left[|0\rangle + \omega_N^{-x 2^{n-k}} |1\rangle \right]$$

Μπορούμε να παρατηρήσουμε ότι το $\omega_N^{-x 2^{n-k}}$ δεν εξαρτάται από τα bits του x με μεγάλη τάξη, οπότε μπορούμε να χρησιμοποιήσουμε τον κλασματικό δυαδικό συμβολισμό

$$0.x_l x_{l+1} \ldots x_n = \frac{x_l}{2} + \frac{x_{l+1}}{4} + \cdots + \frac{x_n}{2^{n-l+1}}$$

και να έχουμε

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \left[|0\rangle + e^{-2\pi i 0.x_n}|1\rangle\right] \otimes \left[|0\rangle + e^{-2\pi i 0 \cdot x_{n-1}x_n}|1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{-2\pi i 0.x_1 x_2 \cdots x_n}|1\rangle\right]$$

Παρατηρούμε ότι μόνο το τελευταίο qubit εξαρτάται από όλες τις τιμές των qubits εισόδου και κάθε επόμενο qubit εξαρτάται όλο και λιγότερο από τα qubits εισόδου. Επίσης το $e^{-2\pi i 0.a}$ ισούται είτε με $+1$ είτε με -1, το οποίο μας θυμίζει το μετασχηματισμό Hadamard.

Συνοψίζοντας, για να παράξουμε ένα κύκλωμα για τον QFT για $N = 2^n$ παίρνουμε το πρώτο qubit $|x_1, \ldots, x_n\rangle$ και εφαρμόζουμε έναν μετασχηματισμό Hadamard, ο οποίος μας δίνει

$$|x\rangle \rightarrow \frac{1}{\sqrt{2}} \left[|0\rangle + e^{-2\pi i 0 \cdot x_1}|1\rangle\right] \otimes |x_2, x_3, \ldots, x_n\rangle$$

Ορίζουμε στη συνέχεια την πύλη μετατόπισης φάσης

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{-2\pi i}{2^k}\right) \end{bmatrix}$$

και εφαρμόζουμε ανάλογες ελεγχόμενες πύλες R_2, R_3 κτλ, στα κατάλληλα bits, το οποίο μας δίνει τον εξής μετασχηματισμό

$$|x\rangle \rightarrow \frac{1}{\sqrt{2}} \left[|0\rangle + e^{-2\pi i 0 \cdot x_1 x_2 \ldots x_n}|1\rangle\right] \otimes |x_2, x_3, \ldots, x_n\rangle$$

Αυτό θα μας ξαναπαράξει τον τελευταίο όρο της QFT κατάστασης, οπότε αυτό αν το κάνουμε για όλα τα qubits θα έχουμε

$$|x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \left[|0\rangle + e^{-2\pi i 0.x_1 x_2 \cdots x_n}|1\rangle\right] \otimes \left[|0\rangle + e^{-2\pi i 0 \cdot x_1 x_2 \cdots x_{n-1}}|1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{-2\pi i 0 \cdot x_n}|1\rangle\right]$$

Αν αλλάξουμε τη σειρά αυτών των qubits θα έχουμε παράξει τον κβαντικό μετασχηματισμό Fourier.

2.10.1 Αλγόριθμος του Shor

Το 1994, ο Peter Shor, στηριζόμενος στην εργασία του Daniel Simon περί των δενδρικών προβλημάτων απόφασης (tree decision problems) ανακάλυψε έναν πιθανοκρατικά φραγμένο αλγόριθμο πολυωνυμικού χρόνου, για να παραγοντοποιεί αριθμούς $n-$ψηφίων σε κβαντικούς υπολογιστές. Μέχρι το 1970 οι άνθρωποι έψαχναν για αποτελεσματικούς αλγόριθμους που θα λύνουν το πρόβλημα παραγοντοποίησης μεγάλων αριθμών, με πιο γνωστό τον αλγόριθμο των A.K. Lenstra και H.W Lenstra το 1993, ο οποίος όμως και αυτός είναι εκθετικού χρόνου σε αντιστοιχία με το μέγεθος της εισόδου. Αυτό είχε ως αποτελέσμα, οι άνθρωποι να πιστεύουν ότι τα κρυπτοσυστήματα που είχαν κατασκευάσει, στηριζόμενοι σε αυτό το πολύ δύσκολο πρόβλημα παραγοντοποίησης μεγάλων αριθμών, όπως το RSA, είναι ασφαλή και αξιόπιστα. Τα αποτελέσματα του Shor όμως από την άλλη εξέπληξαν όλη τη μαθηματική κρυπτογραφική κοινότητα και όχι μόνο και κίνησαν το ενδιαφέρον πολλών επιστημόνων προς το κλάδο των κβαντικών υπολογιστών.

Οι περισσότεροι αλγόριθμοι παραγοντοποίησης, συμπεριλαμβανομένου και του Shor, χρησιμοποιούν μια καθιερωμένη (standard) "μείωση" του προβλήματος παραγοντοποίησης σε πρόβλημα εύρεσης περιόδου μιας συνάρτησης. Ο Shor χρησιμοποιεί κβαντική παραλληλία με το κανονικό τρόπο με σκοπό να αποκτήσει μια υπέρθεση όλων των τιμών της συνάρτησης σε ένα μόνο βήμα. Ύστερα υπολογίζει τον κβαντικό μετασχηματισμό Fourier της συνάρτησης, ο οποίος όπως και ο κλασσικός μετασχηματισμός Fourier, βάζει όλο το πλάτος-εύρος της συνάρτησης σε πολλαπλάσια της αντίστροφης περιόδου. Με μεγάλη πιθανότητα, μετρώντας τη κατάσταση αποφαινόμαστε για τη περίοδο, που με τη σειρά της οδηγεί στον υπολογισμό των παραγόντων ενός αριθμού $n-$ψηφίων. Ο συνοπτικός τρόπος που περιγράψαμε τη διαδικασία σκοπό έχει να σχηματίσουμε μια ιδέα για το πώς λειτουργεί ο αλγόριθμος του Shor αλλά δεν παύει να παραμένει μια υπεραπλούστευση. Το περίεργο ή αλλιώς πολύπλοκο κομμάτι του αλγορίθμου είναι ότι ο κβαντικός μετασχηματισμός Fourier στηρίζεται στο γρήγορο μετασχηματισμό Fourier, ο οποίος στις περισσότερες περιπτώσεις δίνει κατά προσέγγιση και όχι ακριβή αποτελέσματα. Έτσι, η εύρεση της περιόδου ίσως είναι πιο περίπλοκη απότι θα περιμέναμε, αλλά αυτό δεν μας εμποδίζει να την υπολογίσουμε με τους κλασσικούς μαθηματικούς τρόπους που γνωρίζουμε. Παρακάτω ακολουθεί εκτενέστερη περιγραφή των βημάτων του αλγορίθμου $[70]$.

Το πρόβλημα που λύνει ο κβαντικός αλγόριθμος του Shor είναι το εξής:

Δοθέντος ενός σύνθετου περιττού ακέραιου N, να βρεθούν οι πρώτοι του παράγοντες.

Είναι γνωστό ότι το να παραγοντοποιήσουμε έναν αριθμό N, μπορεί να μειωθεί στο πρόβλημα του να διαλέξεις έναν ακέραιο m τυχαία, σχετικά πρώτο με το N, και να καθορίσεις την modulo N πολλαπλασιαστική τάξη του P, δηλαδή να βρεις το μικρότερο θετικό ακέραιο P τέτοιο ώστε

$$m^P = 1 \bmod N$$

Έστω $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ να συμβολίζει το σύνολο των φυσικών αριθμών. Ο αλγόριθμος του Shor παρέχει λύση στο παραπάνω πρόβλημα. Αποτελείται από 5 βήματα, με μόνο το βήμα 2 να απαιτεί τη χρήση κβαντικού υπολογιστή. Όλα τα υπόλοιπα βήματα πραγματοποιούνται σε κλασικό υπολογιστή.

Βήμα 1: Διαλέγουμε έναν τυχαίο ακέραιο θετικό αριθμό m. Χρησιμοποιούμε τον Ευκλείδιο αλγόριθμο για να υπολογίσουμε το ΜΚΔ των m και N. Αν ο ΜΚΔ$(m, N) \neq 1$, τότε βρήκαμε έναν μη-τετριμένο παράγοντα του N και τελειώσαμε. Αλλιώς, προχωράμε στο βήμα 2.

Βήμα 2: Χρησιμοποιούμε έναν κβαντικό υπολογιστή για να προσδιορίσουμε την άγνωστη περίοδο P της συνάρτησης

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{f_N} & \mathbb{N} \\ a & \longmapsto & m^a \bmod N \end{array}$$

Βήμα 3: Αν P είναι περιττός ακέραιος, πάμε στο βήμα 1 (η πιθανότητα το P να είναι περιττός είναι $\frac{1}{2}^k$, όπου k ο αριθμός των διακεκριμένων πρώτων παραγόντων του N). Αν ο P είναι άρτιος, πάμε στο επόμενο βήμα.

Βήμα 4: Αφού ο P είναι άρτιος, έχουμε

$$\left(m^{P/2} - 1\right)\left(m^{P/2} + 1\right) = m^P - 1 = 0 \bmod N$$

Αν $m^{P/2}+1 = 0 \bmod N$, πάμε στο βήμα 1. Αν $m^{P/2}+1 \neq 0 \bmod N$ πάμε στο βήμα 5. Η πιθανότητα να ισχύει το $m^{P/2}+1 = 0 \bmod N$ είναι λιγότερη από $\frac{1}{2}^{k-1}$, όπου k ο αριθμός των διακεκριμένων πρώτων παραγόντων του N.

Βήμα 5: Χρησιμοποιούμε τον Ευκλείδιο αλγόριθμο για να υπολογίσουμε το $d = \gcd\left(m^{P/2}-1, N\right)$. Από τη στιγμή που $m^{P/2}+1 \neq 0 \bmod N$, μπορεί εύκολα να δειχθεί ότι ο d είναι ένας μη τετριμένος παράγοντας του N. Ο αλγόριθμος τερματίζει με απάντηση d.

Άρα το πρόβλημα παραγοντοποίησης ενός περιττού ακέραιου θετικού N, μειώνεται στο εξής πρόβλημα

Δοθείσης μιας περιοδικής συνάρτησης

$$f : \mathbb{N} \longrightarrow \mathbb{N}$$

να βρεθεί η περίοδος P της f.

Στη συνέχεια θα αναλύσουμε το κβαντικό μέρος του αλγορίθμου που είναι το βήμα 2.

Διαλέγουμε μια δύναμη του 2

$$Q = 2^L$$

τέτοια ώστε

$$N^2 \leq Q = 2^L < 2N^2$$

και θεωρούμε την f περιορισμένη στο σύνολο

$$S_Q = \{0, 1, \ldots, Q-1\}$$

το οποίο επίσης συμβολίζουμε με f, δηλαδή

$$f : S_Q \longrightarrow S_Q$$

Κατασκευάζουμε δύο $L-$qubit κβαντικούς καταχωρητές REGISTER1 και REGISTER2, ώστε να κρατήσουμε τα ορίσματα και τις τιμές της f αντίστοιχα, δηλαδή

$$|\mathrm{REG1}\rangle|\mathrm{REG2}\rangle = |a\rangle|f(a)\rangle = |a\rangle|b\rangle = |a_0 a_1 \cdots a_{L-1}\rangle\,|b_0 b_1 \cdots b_{L-1}\rangle$$

Σε ένα κβαντικό υπολογιστή, αναπαριστούμε έναν ακέραιο a με βάση 2 αναπαριστώντας τον ως

$$a = \sum_{j=0}^{L-1} a_j 2^j$$

καθώς ένας κβαντικός καταχωρητής αποτελείται από 2^n qubits

$$|a\rangle = |a_0 a_1 \cdots a_{L-1}\rangle = \bigotimes_{j=0}^{L-1} |a_j\rangle$$

Το κβαντικό κομμάτι τώρα του αλγορίθμου, δηλαδή το **βήμα 2** έχει ως εξής:

Βήμα 1: Αρχικοποιούμε τους καταχωρητές, δηλαδή

$$|\psi_0\rangle = |\mathrm{REG1}\rangle|\mathrm{REG2}\rangle = |0\rangle|0\rangle = |00\cdots0\rangle|0\cdots0\rangle$$

Βήμα 2: Εφαρμόζουμε κβαντικό μετασχηματισμό Fourier στον καταχωρητή 1

$$|\psi_0\rangle = |0\rangle|0\rangle \xrightarrow{\mathcal{F}\otimes I} |\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}\omega^{0.x}|x\rangle|0\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle$$

Οπότε ο REGISTER1 κρατάει όλους τους ακέραιους

$$0, 1, 2, \ldots, Q-1$$

σε υπέρθεση.

Βήμα 3: Έστω U_f να είναι ο ορθογώνιος μετασχηματισμός που παίρνει το $|x\rangle|0\rangle$ και το στέλνει στο $|x\rangle|f(x)\rangle$. Εφαρμόζουμε το γραμμικό μετασχηματισμό U_f και στους δύο καταχωρητές. Το αποτέλεσμα είναι

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle \xrightarrow{U_f} |\psi_2\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle$$

Η κατάσταση των δύο καταχωρητών τώρα είναι κάτι παραπάνω από υπέρθεση των καταστάσεών τους. Τους έχουμε πλέον σε κβαντική διεμπλοκή.

Βήμα 4: Εφαρμόζουμε κβαντικό μετασχηματισμό Fourier στον καταχωρητή 1. Η κατάσταση που θα πάρουμε είναι

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle \quad \xrightarrow{\mathcal{F}\otimes I} |\psi_3\rangle = \frac{1}{Q}\sum_{x=0}^{Q-1}\sum_{y=0}^{Q-1}\omega^{xy}|y\rangle|f(x)\rangle$$
$$= \frac{1}{Q}\sum_{y=0}^{Q-1}\||\Upsilon(y)\rangle\|\cdot|y\rangle\frac{|\Upsilon(y)\rangle}{\||\Upsilon(y)\rangle\|}$$

όπου

$$|\Upsilon(y)\rangle = \sum_{x=0}^{Q-1}\omega^{xy}|f(x)\rangle$$

Βήμα 5: Μετράμε τον καταχωρητή 1, δηλαδή πραγματοποιούμε μια μέτρηση σε σχέση με τις ορθοκανονικές προβολές

$$|0\rangle\langle0|\otimes I,\ \ |1\rangle\langle1|\otimes I,\ \ |2\rangle\langle2|\otimes I,\ \ \ldots,\ \ |Q-1\rangle\langle Q-1|\otimes I$$

όπου I συμβολίζει τον ταυτοτικό τελεστή στο χώρο Hilbert του δεύτερου καταχωρητή.

Αν μετρήσουμε λοιπόν τη κατάσταση αυτή θα έχουμε με μεγάλη πιθανότητα

$$\mathrm{Prob}\left(y_0\right) = \frac{\| \left|\Upsilon\left(y_0\right)\right\rangle \|^2}{Q^2}$$

το οποίο μετακινήθηκε στη κατάσταση

$$\left|y_0\right\rangle \frac{\left|\Upsilon\left(y_0\right)\right\rangle}{\| \left|\Upsilon\left(y_0\right)\right\rangle \|}$$

και μετρήσαμε τη τιμή

$$y_0 \in \{0, 1, 2, \ldots, Q-1\}$$

Αν ύστερα από αυτή τη μέτρηση αγνοήσουμε τους δύο καταχωρητές $Reg1$ και $Reg2$, τότε παρατηρούμε ότι έχουμε μια κλασσική κατανομή πιθανότητας S στο δειγματικό χώρο

$$\{0, 1, 2, \ldots, Q-1\}$$

Όπως θα δούμε, θα εξάγουμε πληροφορίες για την εύρεση της περιόδου της συνάρτησης f μέσω αυτής της στοχαστικής πηγής.

Στοχαστική πηγή S του αλγορίθμου Shor

Θα αναλύσουμε λίγο περισσότερο τώρα τη κατανομή πιθανότητας $\mathrm{Prob}(y)$ [70].

Πρόταση 2.65. *Έστω q, r οι μοναδικοί μη-αρνητικοί ακέραιοι τέτοιοι ώστε $Q = Pq + r$, όπου $0 \leq r < P$; και έστω $Q_0 = Pq$. Τότε*

$$\mathrm{Prob}(y) = \begin{cases} \frac{r \sin^2\left(\frac{\pi P y}{Q} \cdot \left(\frac{Q_0}{P} + 1\right)\right) + (P-r)\sin^2\left(\frac{\pi P y}{Q} \cdot \frac{Q_0}{P}\right)}{Q^2 \sin^2\left(\frac{\pi P y}{Q}\right)} & \text{αν } Py \neq 0 \bmod Q \\ \frac{r(Q_0+P)^2 + (P-r)Q_0^2}{Q^2 P^2} & \text{αν } Py = 0 \bmod Q \end{cases}$$

Ως πόρισμα έχουμε το παρακάτω

Πόρισμα 2.66. *Αν P είναι ένας ακριβής διαιρέτης του Q τότε*

$$\mathrm{Prob}(y) = \begin{cases} 0 & \text{αν } Py \neq 0 \bmod Q \\ \frac{1}{P} & \text{αν } Py = 0 \bmod Q \end{cases}$$

Συνεχή Κλάσματα

Κάθε θετικός ρητός αριθμός ξ μπορεί να γραφεί στη μορφή

$$\xi = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_N}}}}$$

όπου a_0 είναι μη-αρνητικός ακέραιος και $a_1, \ldots, a_N$ θετικοί ακέραιοι. Αυτός ο τρόπος γραφής ονομάζεται ***συνεχές κλάσμα*** και καθορίζεται εξ' ολοκλήρου από το ξ δεδομένου ότι εφαρμόζουμε τη συνθήκη $a_N > 1$.

Για τυπογραφική απλότητα, συμβολίζουμε αλλιώς τη παραπάνω μορφή ως

$$[a_0, a_1, \ldots, a_N]$$

Ένα συνεχές κλάσμα μπορεί να υπολογιστεί από την ακόλουθη αναδρομική σχέση, η οποία πάντα τερματίζει αν ξ ρητός:

$$\begin{cases} a_0 = \lfloor \xi \rfloor \\ \xi_0 = \xi - a_0 \end{cases}, \quad \text{και αν } \xi_n \neq 0, \text{ τότε } \begin{cases} a_{n+1} = \lfloor 1/\xi_n \rfloor \\ \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1} \end{cases}$$

Η $n-$οστή συγκλίνουσα $(0 \leq n \leq N)$ του παραπάνω συνεχούς κλάσματος ορίζεται από το ρητό αριθμό ξ_n που δίνεται από

$$\xi_n = [a_0, a_1, \ldots, a_n]$$

Κάθε συγκλίνουσα ξ_n μπορεί να γραφεί στη μορφή, $\xi_n = \frac{p_n}{q_n}$, όπου p_n και q_n σχετικώς πρώτοι ακέραιοι $(\gcd(p_n, q_n) = 1)$. Οι ακέραιοι p_n και q_n ορίζονται από την αναδρομική σχέση

$$\begin{array}{lll} p_0 = a_0, & p_1 = a_1 a_0 + 1, & p_n = a_n p_{n-1} + p_{n-2} \\ q_0 = 1, & & q_1 = a_1, \quad q_n = a_n q_{n-1} + q_{n-2} \end{array}$$

Τελευταίο κομμάτι του αλγορίθμου

Ορισμός 2.67. *Για κάθε ακέραιο a, έστω $\{a\}_Q$ να συμβολίζει το ολοκληρωτικό υπόλοιπο modulo Q του μικρότερου μεγέθους. Με άλλα λόγια το $\{a\}_Q$ είναι ο μοναδικός ακέραιος τέτοιος ώστε*

$$\begin{cases} a = \{a\}_Q \bmod Q \\ -Q/2 < \{a\}_Q \leq Q/2 \end{cases}$$

Πρόταση 2.68. *Έστω y ένας ακέραιος ο οποίος βρίσκεται στο S_Q. Τότε*

$$\mathrm{Prob}(y) \geq \begin{cases} \frac{4}{\pi^2} \cdot \frac{1}{P} \cdot \left(1 - \frac{1}{N}\right)^2 & \text{αν } 0 < |\{Py\}_Q| \leq \frac{P}{2} \cdot \left(1 - \frac{1}{N}\right) \\ \frac{1}{P} \cdot \left(1 - \frac{1}{N}\right)^2 & \text{αν } \{Py\}_Q = 0 \end{cases}$$

Λήμμα 2.69. *Έστω*

$$Y = \left\{ y \in S_Q || \{Py\}_Q| \leq \frac{P}{2} \right\} \quad \text{και} \quad S_P = \{d \in S_Q | 0 \leq d < P\}$$

Τότε η απεικόνιση

$$\begin{aligned} Y &\longrightarrow S_P \\ y &\longmapsto d = d(y) = \mathrm{round}\left(\frac{P}{Q} \cdot y\right) \end{aligned}$$

είναι αμφιμονοσήμαντη και επί με αντίστροφο

$$y = y(d) = \text{round}\left(\frac{Q}{P} \cdot d\right)$$

Άρα, οι Y και S_P είναι σε 1 προς 1 αντιστοιχία. Επίσης,

$$\{Py\}_Q = P \cdot y - Q \cdot d(y)$$

Επίσης, τα δύο ακόλουθα σύνολα ρητών είναι σε ένα προς ένα αντιστοιχία

$$\left\{\frac{y}{Q} | y \in Y\right\} \longleftrightarrow \left\{\frac{d}{P} | 0 \leq d < P\right\}$$

Όπως είδαμε μετά τη μέτρηση, έχουμε στη κατοχή μας έναν ακέραιο $y \in Y$ και στη συνέχεια θα δούμε πώς αυτό θα μας βοηθήσει να βρούμε τη περίοδο P.

Θεώρημα 2.70. *Έστω ξ ένας πραγματικός αριθμός και έστω a, b ακέραιοι αριθμοί με $b > 0$. Αν*

$$\left|\xi - \frac{a}{b}\right| \leq \frac{1}{2b^2}$$

τότε ο ρητός αριθμός a/b είναι μια συγκλίνουσα της επέκτασης του συνεχούς κλάσματος ξ.

Πόρισμα 2.71. *Αν $|\{Py\}_Q| \leq \frac{P}{2}$, τότε ο ρητός αριθμός $\frac{d(y)}{P}$ είναι μια συγκλίνουσα της επέκτασης του συνεχούς κλάσματος του $\frac{y}{Q}$.*

Αφού $\frac{d(y)}{P}$ είναι μια συγκλίνουσα του $\frac{y}{Q}$, συνεπάγεται ότι για κάποιο n,

$$\frac{d(y)}{P} = \frac{p_n}{q_n}$$

όπου p_n και q_n σχετικά πρώτοι θετικοί ακέραιοι που δίνονται από την αναδρομική σχέση που είδαμε παραπάνω. Άρα φαίνεται να βρήκαμε ένα τρόπο να εξάγουμε τη περίοδο P από το αποτέλεσμα της μέτρησης y. Βέβαια, πρέπει να προσέξουμε ότι πρέπει να ισχύει

$$\begin{cases} p_n = d(y) \\ q_n = P \end{cases}$$

για να πάρουμε τη περίοδο, και αυτό ισχύει μόνο όταν τα $d(y)$, P είναι σχετικά πρώτοι. Άρα ποιά είναι η πιθανότητα το $y \in Y$ να ικανοποιεί επιπλέον τη συνθήκη $\text{MKD}(P, d(y)) = 1$;

Πρόταση 2.72. *Η πιθανότητα το τυχαίο y να είναι τέτοιο ώστε τα $d(y)$ και P να είναι σχετικώς πρώτοι είναι κάτω φραγμένη και ισχύει η σχέση*

$$\text{Prob}\{y \in Y | \gcd(d(y), P) = 1\} \geq \frac{4}{\pi^2} \cdot \frac{\phi(P)}{P} \cdot \left(1 - \frac{1}{N}\right)^2$$

όπου $\phi(P)$ η συνάρτηση Euler που συμβολίζει τον αριθμό των θετικών ακεραίων μικρότερων του P που είναι σχετικά πρώτοι με το P.

Θεώρημα 2.73. *Ισχύει*

$$\liminf \frac{\phi(N)}{N/\ln(\ln N)} = e^{-\gamma}$$

όπου γ *η σταθερά Euler* $\gamma = 0.57721566490153286061\ldots$ *και* $e^{-\gamma} = 0.5614594836$.

Πόρισμα 2.74.

$$\text{Prob}\{y \in Y | \gcd(d(y), P) = 1\} \geq \frac{4}{\pi^2 \ln 2} \cdot \frac{e^{-\gamma} - \epsilon(P)}{\lg(\lg N)} \cdot \left(1 - \frac{1}{N}\right)^2$$

όπου $\epsilon(P)$ *είναι μια μονότονη φθίνουσα ακολουθία που συγκίνει στο* 0. *Σε ασυμπτωτικό συμβολισμό,*

$$\text{Prob}\{y \in Y | \gcd(d(y), P) = 1\} = \Omega\left(\frac{1}{\lg(\lg N)}\right)$$

Αν λοιπόν το βήμα στο οποίο προσδιορίζουμε το y *επαναληφθεί* $O(\lg(\lg N))$ *φορές, η πιθανότητα επιτυχίας είναι* $\Omega(1)$.

Παράδειγμα του Αλγορίθμου Shor

Θα δείξουμε πώς παραγοντοποιούμε τον αριθμό $N = 91 = 7 \cdot 13$. Διαλέγουμε $Q = 2^{14} = 16384$ τέτοιο ώστε $N^2 \leq Q < 2N^2$ [70].

- Διαλέγουμε έναν τυχαίο αριθμό $m = 3$. Καθώς $\gcd(91, 3) = 1$ προχωράμε ώστε να βρούμε τη περίοδο της συνάρτησης f που δίνεται από το τύπο

  $$f(a) = 3^a \bmod 91$$

  Κάνουμε ότι δεν γνωρίζουμε τη περίοδο της συνάρτησης αυτής προς το παρών, αλλά επειδή τα νούμερα είναι μικρά ξέρουμε ότι έχει περίοδο $P = 6$.

a	0	1	2	3	4	5	6	7	$\cdots$
$f(a)$	1	3	9	27	81	61	1	3	$\cdots$

- Αρχικοποιούμε τους δύο καταχωρητές μας reg1,reg2, οπότε η κατάστασή τους γίνεται

  $$|\psi_0\rangle = |0\rangle|0\rangle$$

- Εφαρμόζουμε τον QFT στον πρώτο καταχωρητή

  $$\mathcal{F}|k\rangle = \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} \omega^{0 \cdot x} |x\rangle$$

  όπου ω, η $Q-$οστή ρίζα της μονάδας, $\omega = e^{\frac{2\pi i}{16384}}$. Οπότε η κατάσταση των δύο καταχωρητών τώρα γίνεται

$$|\psi_1\rangle = \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} |x\rangle|0\rangle$$

- Εφαρμόζουμε στη συνέχεια τον ορθογώνιο μετασχηματισμό U_f στους δύο καταχωρητές, όπου

$$U_f|x\rangle|\ell\rangle = |x\rangle|f(x) - \ell \bmod 91\rangle$$

Οπότε η νέα κατάστασή τους γίνεται

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} |x\rangle\,|3^x \bmod 91\rangle \\
&= \frac{1}{\sqrt{16384}}(\quad |0\rangle|1\rangle + |1\rangle|3\rangle + |2\rangle|9\rangle + |3\rangle|27\rangle + |4\rangle|81\rangle + |5\rangle|61\rangle \\
&\quad +|12\rangle|1\rangle + |7\rangle|3\rangle + |8\rangle|9\rangle + |9\rangle|27\rangle + |10\rangle|81\rangle + |11\rangle|61\rangle \\
&\quad +|12\rangle|1\rangle + |13\rangle|3\rangle + |14\rangle|9\rangle + |15\rangle|27\rangle + |16\rangle|81\rangle + |17\rangle|61\rangle \\
&\quad +\cdots \\
&\quad +|16380\rangle|1\rangle + |16381\rangle|3\rangle + |16382\rangle|9\rangle + |16383\rangle|27\rangle \\
&\quad)
\end{aligned}$$

Η κατάσταση πλέον των καταχωρητών είναι μια υπέρθεση και βρίσκονται και σε κβαντική διεμπλοκή.

- Εφαρμόζουμε πάλι τον QFT στο πρώτο καταχωρητή, οπότε η νέα κατάσταση θα είναι

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} \frac{1}{\sqrt{16384}} \sum_{y=0}^{16383} \omega^{xy}|y\rangle\,|3^x \bmod 91\rangle \\
&= \frac{1}{16384} \sum_{x=0}^{16383} |y\rangle \sum_{x=0}^{16383} \omega^{xy}\,|3^x \bmod 91\rangle \\
&= \frac{1}{16384} \sum_{x=0}^{16383} |y\rangle|\Upsilon(y)\rangle
\end{aligned}$$

όπου

$$|\Upsilon(y)\rangle = \sum_{x=0}^{16383} \omega^{xy}\,|3^x \bmod 91\rangle$$

οπότε

$$\begin{aligned}
|\Upsilon(y)\rangle = \quad & |1\rangle + \omega^{y}|3\rangle + \omega^{2y}|9\rangle + \omega^{3y}|27\rangle + \omega^{4y}|81\rangle + \omega^{5y}|61 \\
& +\omega^{6y}|1\rangle + \omega^{7y}|3\rangle + \omega^{8y}|9\rangle + \omega^{9y}|27\rangle + \omega^{10y}|81\rangle + \omega^{11y}|61\rangle \\
& +\omega^{12y}|1\rangle + \omega^{13y}|3\rangle + \omega^{14y}|9\rangle + \omega^{15y}|27\rangle + \omega^{16y}|81\rangle + \omega^{17y}|61\rangle \\
& \qquad +\ldots \\
& +\omega^{16380y}|1\rangle + \omega^{16381y}|3\rangle + \omega^{16382y}|9\rangle + \omega^{16383y}|27\rangle
\end{aligned}$$

- Μετράμε τον καταχωρητή ένα και το αποτέλεσμα της μέτρησης τυχαίνει να είναι

$$y = 13453$$

Άγνωστο προς εμάς, η πιθανότητα να πάρουμε αυτό το y είναι

$$0.3189335551 \times 10^{-6}$$

Το αντίστοιχο d είναι σχετικά πρώτο με το P, δηλαδή

$$d = d(y) = \text{round}\left(\frac{P}{Q} \cdot y\right) = 5$$

Ξέρουμε ότι η πιθανότητα το $d(y)$ να είναι σχετικά πρώτο με το P είναι μεγαλύτερη από

$$\frac{0.232}{\lg\lg N} \cdot \left(1 - \frac{1}{N}\right)^2 \approx 8.4\% \text{ (δεδομένου ότι } P > 3$$

και ξέρουμε επίσης ότι το

$$\frac{d(y)}{P}$$

είναι μια συγκλίνουσα της επέκτασης του συνεχούς κλάσματος του

$$\xi = \frac{y}{Q} = \frac{13453}{16384}$$

Οπότε προχωράμε στο επόμενο βήμα.

- Χρησιμοποιώντας τις αναδρομικές σχέσεις που αναφέραμε προηγουμένως για τα συνεχή κλάσματα, υπολογίζουμε τα a_n και q_n για το

$$\xi = \frac{y}{Q} = \frac{13453}{16384}$$

Για κάθε μη-τετριμμένο n που βρίσκουμε, ελέγχουμε αν ισχύει η σχέση

$$3^{q_n} = 1 \bmod 91$$

Αν ναι, τότε ξέρουμε ότι $q_n = P$ οπότε προχωράμε στο επόμενο βήμα.

Στο συγκεκριμένο παράδειγμα οι τιμές $n = 0$ και $n = 1$ είναι τετριμμένες. Προχωράμε για $n = 2, a_2 = 4$ και $q_2 = 5$ και υπολογίζουμε

$$3^{q_2} = 3^5 = \left(3^{2^0}\right)^1 \cdot \left(3^{2^1}\right)^0 \cdot \left(3^{2^0}\right)^1 = 61 \neq 1 \bmod 91$$

Δεν μας κάνει οπότε πάμε για $n = 3$ άρα για $a_3 = 1$ και $q_3 = 6$ και ελέγχουμε

$$3^{q_3} = 3^6 = \left(3^{2^0}\right)^0 \cdot \left(3^{2^1}\right)^1 \cdot \left(3^{2^0}\right)^1 = 1 \bmod 91$$

το οποίο μας κάνει, οπότε $q_3 = P$.

- Ο $P = 6$ είναι άρτιος οπότε προχωράμε στο επόμενο βήμα.
- Ελέγχουμε
$$3^{P/2} = 3^3 = 27 \neq -1 \bmod 91$$
οπότε προχωράμε στο επόμενο βήμα.
- Με τον Ευκλείδιο αλγόριθμο υπολογίζουμε το
$$\gcd\left(3^{P/2} - 1, 91\right) = \gcd\left(3^3 - 1, 91\right) = \gcd(26, 91) = 13$$
οπότε καταφέραμε να βρούμε έναν μη τετριμμένο παράγοντα του $N = 91$, τον αριθμό 13.

ΚΕΦΑΛΑΙΟ 3

Μετα-Κβαντική Κρυπτογραφία και Εφαρμογές

Η ολοκλήρωση των κβαντικών υπολογιστών θα διαταράξει τις συνθήκες ασφάλειας δεδομένων και συστημάτων όπως την ακεραιότητα -αυθεντικοποίηση δεδομένων κατά την μετάδοσης τους αλλά και τη συνθήκη της εμπιστευτικότητας που εξασφαλίζεται με την κρυπτογραφία. Θα στηριχτούμε σε δύσκολα μαθηματικά προβλήματα μέχρι σήμερα, από το χώρο των δικτυωμάτων και των γραμμικών κωδίκων ή αλλιώς κωδίκων Goppa, και θα κατασκευάσουμε κρυπτοσυστήματα τα οποία είναι ανθεκτικά σε κβαντικές κρυπταναλυτικές επιθέσεις.

3.1 Γραμμικοί Κώδικες

3.1.1 Κώδικες Goppa

Ένας κώδικας $C(n,k)$ είναι εν γένει υποσύνολο του F_q^n. Ο κώδικας ονομάζεται γραμμικός αν είναι F_q-γραμμικός υπόχωρος του F_q^n, το k είναι η διάσταση του διανύσματος C και το n το μήκος του κώδικα.

Ορισμός 3.1. *Έστω ένα πολυώνυμο $g(x)$, που ορίζεται στο $GF(p^m)$ με*

$$g(x) = g_0 + g_1 \cdot (x) + \cdots + g_t \cdot (x^t) = \sum_{i=0}^{t} g_i x^i$$

για κάθε $g_i \in GF(p^m)$.

Έστω επίσης L ένα πεπερασμένο υποσύνολο του πεδίου $GF(p^m)$, με p πρώτο αριθμό και μορφή

$$L = \{a_1, \ldots, a_n\} \subseteq GF(p^m)$$

τέτοιο ώστε $g(a_i) \neq 0, \forall a_i \in L$. Δοθέντος ενός διανύσματος $c = (c_1, \ldots, c_n)$ στο $GF(p^m)$, (αργότερα για αυτό το c θα χρησιμοποιούμε τον όρο "κωδικολέξη"), έχουμε τη συνάρτηση

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - a_i}$$

όπου $\frac{1}{x-a_i}$ *είναι το μοναδικό πολυώνυμο με*

$$(x-a_i)\cdot\frac{1}{x-a_i}\equiv 1(modg(x))$$

και βαθμό μικρότερο ή ίσο του $(t-1)$.

Ορίζουμε ως κώδικα $Goppa$, *και συμβολίζουμε* $\Gamma(L,g(x))$ *όλα εκείνα τα διανύσματα* c *για τα οποία ισχύει*

$$R_c(x)\equiv 0(modg(x))$$

Είναι φανερό ότι το πολυώνυμο $g(x)$ *διαιρεί το* $R_c(x)$.

Παράμετροι ενός κώδικα Goppa

Ας μη ξεχνάμε ότι οι κώδικες Goppa είναι γραμμικοί κώδικες, οπότε μπορούμε να χρησιμοποιήσουμε το συμβολισμό $[n,k,d]$, με n το μήκος το οποίο στηρίζεται μόνο στο υποσύνολο L, k τη διάσταση και d την ελάχιστη Hamming απόσταση.

Θεώρημα 3.2. *Ο κώδικας* $Goppa,\Gamma(L,g(x))$, *μεγέθους* n *έχει τις εξής ιδότητες*

- *Η διάσταση* k *του κώδικα ικανοποιεί την ανίσωση*

$$k\geq n-mt$$

- *Η ελάχιστη απόσταση* d *ικανοποιεί την ανίσωση*

$$d\geq t+1$$

Συνήθως στις εφαρμογές χρησιμοποιούμε δυαδικούς κώδικες Goppa, δηλαδή το πολυώνυμο $g(x)$ να ορίζεται στο $GF(2^m)$ με βαθμό t, διότι για το κώδικα που θα προκύψει έχουμε τη δυνατότητα να υπολογίσουμε ακριβώς το κάτω φράγμα της Hamming απόστασής του.

Θεώρημα 3.3. *Έστω* $\Gamma(L,g(x)))$ *ένας δυαδικός κώδικας Goppa με πολυώνυμο* $g(x)$ *βαθμού* t. *Τότε ο* $\Gamma(L,g(x)))$ *έχει ελάχιστη απόσταση Hamming,* d, *που ικανοποιεί την ανίσωση*

$$d\geq 2t+1$$

Πίνακας ισοτιμίας ενός κώδικα Goppa

Ο πίνακας ισοτιμίας $\mathcal{H}$ ενός κώδικα Goppa χρησιμοποιείται για την κωδικοποίηση ενός μηνύματος.

Αν θέσουμε $H=XYZ$, με

$$X=\begin{bmatrix} g_t & 0 & 0 & \dots & x_{1n}\\ g_{t-1} & g_t & 0 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ g_1 & g_2 & g_3 & \dots & g_t \end{bmatrix}\quad Y=\begin{bmatrix} 1 & 1 & \dots & 1\\ a_1 & a_2 & \dots & x_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{t-1} & a_2^{t-1} & \dots & a_n^{t-1} \end{bmatrix}\ Z=\begin{bmatrix} \frac{1}{g(a_1)} & 0 & \dots & 0 & \\ 0 & \frac{1}{g(a_2)} & \dots & 0 & \\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & \dots & \dots & 0 & \frac{1}{g(a_n)} \end{bmatrix}$$

Γεννήτορας Πίνακας ενός κώδικα Goppa

Ο πίνακας ισοτιμίας H χρησιμοποιείται για την διόρθωση σφαλμάτων, αλλά χρειαζόμαστε και έναν γεννήτορα πίνακα για να κωδικοποιεί ή να αποκωδικοποιεί τα μηνύματα. Ένα μήνυμα της μορφής $m = (m_1, \ldots, m_k)$ μετατρέπεται σε κωδικομήνυμα c αν πολλαπλασιαστεί με έναν γεννήτορα πίνακα G. Στη συνέχεια μπορεί να διορθωθεί μέσω της σχέσης

$$cH^T = \mathcal{O},\ \forall\ c \in \Gamma(L, g(x))$$

οπότε άμεσα από τη σχέση

$$GH^T = \mathcal{O}$$

μπορούμε να βρούμε τον πίνακα G. Όπως παρατηρούμε, οι γραμμές του πίνακα G είναι τα διανύσματα του μηδενόχωρου $H\ modulo\ q$.

Πρόταση 3.4. *Κάθε $n \times k$ πίνακας G με τάξη k, τέτοιος ώστε $GH^T = \mathcal{O}$, είναι ένας γεννήτορας πίνακας.*

Διόρθωση σφαλμάτων ενός μήνυματος

Έστω y η κωδικολέξη, μετά τη κωδικοποίηση, η οποία περιέχει r σφάλματα, με $2r + 1 \leq d$ ή $r \leq [\frac{t}{2}]$ στη περίπτωση που $d = t + 1$ (που είναι το κάτω φράγμα της ελάχιστης $Hamming$ απόστασης). Το y θα έχει τη μορφή

$$(y_1, \ldots, y_n) = (c_1, \ldots, c_n) + (e_1, \ldots, e_n)$$

με $e_i \neq 0$ σε r θέσεις. Για να διορθώσουμε την λέξη y και να πάρουμε τη σωστή λέξη c, πρέπει να προσδιορίσουμε το διάνυσμα σφάλματος e, οπότε ουσιαστικά να βρούμε

- το σύνολο B, των θέσεων στις οποίες βρίσκονται τα σφάλματα, το οποίο συμβολίζουμε με

$$B = \{i | e_i \neq 0\}$$

- τις αντίστοιχες τιμές e_i, για $i \in B$

Ορισμός 3.5. *Ορίζουμε το πολυώνυμο εντοπισμού σφαλμάτων $\sigma(x)$ και το πολυώνυμο εκτίμησης σφαλμάτων $w(x)$ ως*

$$\sigma(x) := \prod_{i \in B}(x - a_i)$$
$$w(x) := \sum_{i \in B} e_i \prod_{j \in B, j \neq 1} (x - a_j)$$

Στις εφαρμογές χρησιμοποιούμε, όπως αναφέραμε και παραπάνω δυαδικούς κώδικες Goppa, στους οποίους η εύρεση σφαλμάτων είναι ευκολότερη. Ακολουθεί ο αλγόριθμος του Patterson για την διόρθωση $r \leq t$ σφαλμάτων για ανάγωγα πολυώνυμα $g(x)$ στο $GF(2^m)$.

Έστω $y = (y_1, \ldots, y_n)$ μια κωδικολέξη που περιέχει r σφάλματα για $r \leq t$.

Αλγόριθμος Patterson

1: Υπολογίζουμε το

$$s(x) = \sum_{i=1}^{n} \frac{y_i}{x - a_i}$$

.

2: Καθορίζουμε το $\sigma(x)$

- Χρησιμοποιούμε τον Ευκλείδιο Αλγόριθμο για να προσδιορίσουμε το $h(x)$ τέτοιο ώστε

$$s(x)h(x) \equiv 1(mod(g(x))$$

  Αν $h(x) = x$, η λύση είναι $\sigma(x) = x$.

- Υπολογίζουμε το $d(x)$ τέτοιο ώστε

$$d^2(x) \equiv h(x) + x(modg(x))$$

- Βρίσκουμε τα $a(x)$ και $b(x)$ με $b(x)$ ελάχιστου βαθμού, που ικανοποιούν την

$$d(x)b(x) \equiv a(x)(modg(x))$$

- Θέτουμε

$$\sigma(x) = a^2(x) + b^2(x)x$$

3: Καθορίζουμε το σύνολο των θέσεων των σφαλμάτων

$$B = \{i|\sigma(a_i) = 0\}$$

4: Το διάνυσμα σφαλμάτων $e = (e_1, \ldots, e_n)$ ορίζεται ως

$$e = \begin{cases} e_i = 1, \text{ για } i \in B \\ e_i = 0, \text{ διαφορετικά} \end{cases}$$

5: Η κωδικολέξη είναι

$$c = y - e$$

.

Αποκωδικοποίηση

Όταν διορθώσουμε όλα τα σφάλματα σε μια κωδικολέξη, ο παραλήπτης μπορεί εύκολα να ανακτήσει το αρχικό μήνυμα με την εξής διαδικασία.

Ισχύει ότι

$$(m_1, m_2, \ldots, m_k) \cdot G = (c_1, \ldots, c_n)$$

ή αλλιώς σε μορφή πινάκων

$$G^T \cdot \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

Αυτό το σύστημα είναι ένα σύστημα $n-$εξισώσεων με k αγνώστους, οπότε λύνεται με τη μέθοδο μείωσης-γραμμών

$$\begin{bmatrix} g_t & 0 & 0 & \ldots & x_{1n} \\ g_{t-1} & g_t & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & g_3 & \ldots & g_t \end{bmatrix}$$

$$\left(\begin{array}{c|c} & c_1 \\ G^T & \ldots \\ & c_n \end{array} \right)$$

$$\sim \cdots \sim$$

$$\left(\begin{array}{ccccc} 1 & 0 & \ldots & 0 & m_1 \\ 0 & 1 & \ldots & 0 & m_2 \\ \ldots & \ldots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & m_k \\ -- & -- & -- & -- & -- \\ & & X & & \end{array} \right)$$

όπου X ένας $(n-k) \times (k+1)$ πίνακας.

Πρώτο παράδειγμα γραμμικών κωδίκων

Διαλέγουμε μια επέκταση πεδίου, το $GF\,(2^4)$, το οποίο είναι ισομορφικό με το

$$GF(2)[X]/(k(X))$$

για κάθε πρώτο πολυώνυμο $k(X)$ βαθμού 4 [71]. Για να απλοποιήσουμε την εύρεση ενός αρχικού-αρχέτυπου στοιχείου, ψάχνουμε για εκείνα τα πρώτα πολυώνυμα που ικανοποιούν το $X^{15} = 1$, οπότε παίρνουμε τη παραγοντοποίηση $X^{15} - 1\ modulo 2$

$$X^{15}-1=(X+1)\left(X^2+X+1\right)\left(X^4+X+1\right)\left(X^4+X^3+1\right)\left(X^4+X^3+X^2+X+1\right)$$

Αν θεωρήσουμε $k(X)=X^4+X+1$, τότε το α, μια ρίζα του $k(X)$, είναι αρχέτυπο στοιχείο ανν η τάξη του α είναι 15. Από τη στιγμή που η τάξη ενός στοιχείου, διαιρεί τη τάξη της ομάδας, και το $\alpha \neq 1$, πρέπει να ελέγξουμε μόνο αν $\alpha^3 \neq 1$ και $\alpha^5 \neq 1$. Χρησιμοποιώντας τη σχέση $\alpha^4=\alpha+1$, έχουμε

$$\begin{aligned}\alpha^3 &= \alpha^3 \neq 1\\ \alpha^5 &= \alpha\cdot\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha\neq 1\end{aligned}$$

οπότε $GF\left(2^4\right)^* =< \alpha >$, ή αντίστοιχα

$$GF\left(2^4\right)=\left\{0,\alpha,\alpha^2,\ldots,\alpha^{14}\right\}$$

Αναπαριστούμε τα στοιχεία του $GF\left(2^4\right)$ ως δυνάμεις του α χρησιμοποιώντας τη σχέση $\alpha^4=\alpha+1$ και το στοιχείο 0 αντιστοιχεί στο $(0,0,0,0)^T$, οπότε θα έχουμε

$$\begin{aligned}
1 &= 1 && = (1,0,0,0)^T\\
\alpha &= \alpha && = (0,1,0,0)^T\\
\alpha^2 &= \alpha^2 && = (0,0,1,0)^T\\
\alpha^3 &= \alpha^3 && = (0,0,0,1)^T\\
\alpha^4 &= 1+\alpha && = (1,1,0,0)^T\\
\alpha^5 &= \alpha+\alpha^2 && = (0,1,1,0)^T\\
\alpha^6 &= \alpha^2+\alpha^3 && = (0,0,1,1)^T\\
\alpha^7 &= 1+\alpha+\alpha^3 && = (1,1,0,1)^T\\
\alpha^8 &= 1+\alpha^2 && = (1,0,1,0)^T\\
\alpha^9 &= \alpha+\alpha^3 && = (0,1,0,1)^T\\
\alpha^{10} &= 1+\alpha+\alpha^2 && = (1,1,1,0)^T\\
\alpha^{11} &= \alpha+\alpha^2+\alpha^3 && = (0,1,1,1)^T\\
\alpha^{12} &= 1+\alpha+\alpha^2+\alpha^3 && = (1,1,1,1)^T\\
\alpha^{13} &= 1+\alpha^2+\alpha^3 && = (1,0,1,1)^T\\
\alpha^{14} &= 1+\alpha^3 && = (1,0,0,1)^T
\end{aligned}$$

Θεωρούμε τον γραμμικό κώδικα $\Gamma(L,g(z))$ που ορίζεται ως

$$\begin{aligned}g(z) &= (z+\alpha)\left(z+\alpha^{14}\right)=z^2+\alpha^7 z+1\\ L &= \left\{\alpha^i | 2\leq i\leq 13\right\}\end{aligned}$$

με $q = 2, m = 4, n = 12$ και $t = 2$. Το k πρέπει να είναι το λιγότερο $12 - 4 \cdot 2 = 4$ και για το d να ισχύει $d \geq 2 \cdot 2 + 1 = 5$. Άρα έχουμε έναν $[12, \geq 4, \geq 5]$ κώδικα Goppa.

Για να βρούμε το πίνακα ισοτιμίας H, χρησιμοποιούμε τα $g_1 = \alpha^7, g_2 = 1$ και τα $\alpha_1 = \alpha^2, \ldots, \alpha_{12} = \alpha^{13}$. Οι παράγοντες $h_i = g\left(\alpha_i\right)^{-1}$ υπολογίζονται για $1 \leq i \leq 12$ ως

$$\begin{aligned}
h_1 &= g\left(\alpha^2\right)^{-1} = \left(\alpha^4 + \alpha^9 + 1\right)^{-1} \\
&= \left((1,1,0,0)^T + (0,1,0,1)^T + (1,0,0,0)^T\right)^{-1} \\
&= \left((0,0,0,1)^T\right)^{-1} = \alpha^{-3} = \alpha^{12} \\
h_2 &= g\left(\alpha^3\right)^{-1} = \left(\alpha^6 + \alpha^{10} + 1\right)^{-1} \\
&= \left((0,0,1,1)^T + (1,1,1,0)^T + (1,0,0,0)^T\right)^{-1} \\
&= \left((0,1,0,1)^T\right)^{-1} = \alpha^{-9} = \alpha^6, \text{ κτλ.}
\end{aligned}$$

Ο καθορισμός του H είναι θέμα αλλαγής στην έκφραση

$$H = \begin{pmatrix} -\left(\alpha^2 + \alpha^7\right) h_1 & \ldots & -\left(\alpha^{13} + \alpha^7\right) h_{12} \\ -h_1 & \ldots & -h_{12} \end{pmatrix}$$

και καθώς έχουμε δυαδικό κώδικα, μπορούμε να διαγράψουμε τα αρνητικά πρόσημα, οπότε να έχουμε τον ακόλουθο πίνακα ισοτιμίας H,

$$H = \begin{pmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha \end{pmatrix}$$

Επίσης σε δυαδική μορφή ο H είναι

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

και για να βρούμε το γεννήτορα πίνακα G, τον υπολογίζουμε μέσω της σχέσης $GH^T = 0$, άρα τα διανύσματα του μηδενόχωρου του H modulo 2 σχηματίζουν τον χώρο γραμμών του G, οπότε ο G είναι

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

Καταλήγουμε λοιπόν ότι η διάσταση του $\Gamma(L, g(z))$ είναι 4 και έχει παραμέτρους $[12, 4, \geq 5]$.

Δεύτερο Παράδειγμα γραμμικών κωδίκων

Τα ανάγωγα πολυώνυμα μπορούν να χρησιμοποιηθούν και σαν πολυώνυμα γεννήτορες και είναι αρκετά χρήσιμα [71]. Δουλεύουμε πάλι στο $GF\left(2^4\right)$. Θα δοκιμάσουμε τώρα ένα άλλο ανάγωγο παράγοντα του πολυωνύμου $X^{15}-1$. Αν παρατηρήσουμε τη ρίζα α, του πολυωνύμου $k(X)=X^4+X^3+X^2+X+1$, θα δούμε ότι έχει τάξη 5, καθώς

$$\begin{aligned}\alpha^5 &= \alpha\cdot\alpha^4\\ &= \alpha\left(\alpha^3+\alpha^2+\alpha+1\right)\\ &= \alpha^4+\alpha^3+\alpha^2+\alpha\\ &= 1\end{aligned}$$

Άρα το α δεν είναι πρωταρχικό στοιχείο. Θα μπορούσαμε να συνεχίσουμε με τον ίδιο τρόπο την αναζήτηση ενός πρωταρχικού στοιχείου του $k(X)$, αλλά μπορούμε να στρέψουμε τη προσοχή μας στο πολυώνυμο $k(X)=X^4+X^3+1$ το οποίο είναι το τρίτο ανάγωγο πολυώνυμο βαθμού 4 στη παραγοντοποίηση του $X^{15}-1$. Έστω λοιπόν, β, η ρίζα του X^4+X^3+1. Ελέγχουμε αν $\beta\neq 1, \beta^3\neq 1$, και $\beta^5\neq 1$ και καταλήγουμε ότι το β είναι ένα πρωταρχικό στοιχείο του $GF\left(2^4\right)$.

Χρησιμοποιώντας $\beta^4=\beta^3+1$, βρίσκουμε την ακόλουθη αναπαράσταση του $GF\left(2^4\right)$:

$$\begin{array}{lll}
1 & = 1 & = (1,0,0,0)^T\\
\beta & = \beta & = (0,1,0,0)^T\\
\beta^2 & = \beta^2 & = (0,0,1,0)^T\\
\beta^3 & = \beta^3 & = (0,0,0,1)^T\\
\beta^4 & = 1+\beta^3 & = (1,0,0,1)^T\\
\beta^5 & = 1+\beta+\beta^3 & = (1,1,0,1)^T\\
\beta^6 & = 1+\beta+\beta^2+\beta^3 & = (1,1,1,1)^T\\
\beta^7 & = 1+\beta+\beta^2 & = (1,1,1,0)^T\\
\beta^8 & = \beta+\beta^2 & = (0,1,1,1)^T\\
\beta^9 & = 1+\beta^2 & = (1,0,1,0)^T\\
\beta^{10} & = \beta+\beta^3 & = (0,1,0,1)^T\\
\beta^{11} & = 1+\beta^2+\beta^3 & = (1,0,1,1)^T\\
\beta^{12} & = 1+\beta & = (1,1,0,0)^T\\
\beta^{13} & = \beta+\beta^2 & = (0,1,1,0)^T\\
\beta^{14} & = \beta^2+\beta^3 & = (0,0,1,1)^T
\end{array}$$

Θεωρούμε τώρα το κώδικα Goppa $\Gamma(L,g(z))$, που ορίζεται ως

$$\begin{aligned}g(z) &= z^2+z+\beta\\ L &= GF\left(2^4\right)\end{aligned}$$

με $q = 2, m = 4, n = 16$ και $t = 2$. Βρίσκουμε $k \leq 16 - 4 \cdot 2 = 8$ και $d \geq 2 \cdot 2 + 1 = 5$. Άρα ο κώδικας Goppa έχει τις εξής παραμέτρους $[16, \geq 8, \geq 5]$.

Για να βρούμε το πίνακα ισοτιμίας H, χρησιμοποιούμε τα $g_1 = 1, g_2 = 1, \alpha_1 = 0, \alpha_2 = 1, \ldots, \alpha_{16} = \beta^{14}$ και υπολογίζουμε τους παράγοντες $h_i = g\left(\alpha_i\right)^{-1}$ για $1 \leq i \leq 16$.

$$
\begin{aligned}
h_1 &= g(0)^{-1} = (\beta)^{-1} = \beta^{14} \\
h_2 &= g(1)^{-1} = (1 + 1 + \beta)^{-1} = \beta^{14} \\
h_3 &= g(\beta)^{-1} = \left(\beta^2 + \beta + \beta\right)^{-1} = \beta^{13}, \text{ κτλ.}
\end{aligned}
$$

Ο υπολογισμός του H δεν είναι κάτι άλλο παρά μια αλλαγή στην έκφραση

$$
H = \begin{pmatrix} (0+1)h_1 & (1+1)h_2 & (\beta+1)h_3 & \ldots & (\beta^{16}+1)\,h_{16} \\ h_1 & h_2 & h_3 & \ldots & h_{16} \end{pmatrix}
$$

Αδιαφορώντας για τα αρνητικά πρόσημα όπως και στο προηγούμενο παράδειγμα, παίρνουμε τελικά το πίνακα ισοτιμίας,

$$
\begin{pmatrix}
\beta^{14} & 0 & \beta^{10} & \beta^3 & \beta^{10} & \beta^9 & \beta^{13} & 1 & \beta^9 & \beta^{13} & \beta^{11} & \beta^8 & \beta^{11} & \beta^{14} & \beta^3 & \beta^8 \\
\beta^{14} & \beta^{14} & \beta^{13} & \beta^9 & \beta^6 & \beta^6 & \beta^3 & \beta^7 & \beta^{11} & \beta^7 & \beta^9 & \beta^3 & \beta^{12} & \beta^{13} & \beta^{11} & \beta^{12}
\end{pmatrix}
$$

ή αλλιώς σε δυαδική μορφή

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

Οι γραμμές του γεννήτορα πίνακα G γίνονται τα διανύσματα του μηδενόχωρου του H, οπότε

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

Βλέπουμε λοιπόν ότι η διάσταση του $\Gamma(L, g(z))$ είναι ίση με 8 και ο κώδικας Goppa έχει τις παραμέτρους $[16, 8, \geq 5]$.

Παράδειγμα διόρθωσης σφάλματος

Έστω ο $\Gamma(L, g(z))$ να είναι ο Goppa κώδικας όπως στο προηγούμενο παράδειγμα [71]. Έστω ότι θέλουμε να στείλουμε το μήνυμα $(1, 1, 1, 1)$. Πολλαπλασιάζουμε με G προκειμένου να το κρυπτογραφήσουμε

$$c = (1,1,1,1)\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = (1,1,0,0,0,0,1,0,1,1,1,1)$$

Ο κώδικας έχει τις παραμέτρους $[12, 4, \geq 5]$, οπότε διορθώνει $r \leq 2$ σφάλματα. Προσθέτουμε τα σφάλματα στις τελευταίες δύο θέσεις και στέλνουμε το μήνυμα

$$y = (1,1,0,0,0,0,1,0,1,1,0,0)$$

Ο παραλήπτης μπορεί να χρησιμοποίησει την ισότητα $\Gamma(L, g(z)) = \Gamma\left(L, g^2(z)\right)$.
Πρώτα πρέπει να βρούμε το πίνακα ισοτιμίας του $\Gamma\left(L, g^2(z)\right)$. Χρησιμοποιούμε το

$$\hat{g}(t) = g^2(t) = \left(z^2 + \alpha^7 z + 1\right)^2 = z^4 + \alpha^{14} z + 1$$

ως πολυώνυμο γεννήτορα , τέτοιο ώστε $\hat{g}_4 = 1, \hat{g}_3 = 0, \hat{g}_2 = \alpha^{14}, \hat{g}_1 = 0, \hat{g}_0 = 1$. Οι νέοι παράγοντες $\hat{h}_i$, βρίσκονται υψώνοντας στο τετράγωνο τους παλιούς παράγοντες h_i, καθώς

$$\hat{h}_i = \left(g^2\left(\alpha_i\right)\right)^{-1} = \left(g\left(\alpha_i\right)^{-1}\right)^2 = h_i^2$$

Ο πίνακας ισοτιμίας $\hat{H}$ μοιάζει κάπως έτσι

$$\hat{H} = \begin{pmatrix} \left(\left(\alpha^2\right)^3 + \alpha^{14}\alpha^2\right) h_1^2 & \dots & \left(\left(\alpha^{13}\right)^3 + \alpha^{14}\alpha^{13}\right) h_{12}^2 \\ \left(\left(\alpha^2\right)^2 + \alpha^{14}\right) h_1^2 & \dots & \left(\left(\alpha^{13}\right)^2 + \alpha^{14}\right) h_{12}^2 \\ \alpha^2 h_1^2 & \cdots & \alpha^{13} h_{12}^2 \\ h_1^2 & \cdots & h_{12}^2 \end{pmatrix}$$

και βρίσκουμε ύστερα από πράξεις ότι

$$\hat{H} = \begin{pmatrix} \alpha^5 & \alpha^8 & \alpha^7 & \alpha^3 & \alpha^3 & 0 & \alpha^{13} & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{10} & \alpha^{10} \\ \alpha^3 & \alpha^5 & \alpha^3 & \alpha^{13} & \alpha^{12} & 0 & \alpha^5 & 1 & \alpha^4 & \alpha^{14} & \alpha^{13} & \alpha^{12} \\ \alpha^{11} & 1 & \alpha & \alpha^7 & \alpha^{13} & \alpha^7 & \alpha^6 & \alpha^{10} & \alpha^2 & \alpha^9 & \alpha^6 & 1 \\ \alpha^9 & \alpha^{12} & \alpha^{12} & \alpha^2 & \alpha^7 & 1 & \alpha^{13} & \alpha & \alpha^7 & \alpha^{13} & \alpha^9 & \alpha^2 \end{pmatrix}$$

Μπορούμε να διορθώσουμε τώρα το διάνυσμα $y = (1,1,0,0,0,0,1,0,1,1,0,0)$ με τη βοήθεια του αλγορίθμου του Patterson:

1. Υπολογίζουμε πρώτα το σύνδρομο

$$s(z) = \sum_{i=1}^{9} \frac{y_i}{z - \alpha_i}$$

$$
\begin{aligned}
&= \tfrac{1}{z-\alpha^2} + \tfrac{1}{z-\alpha^3} + \tfrac{1}{z-\alpha^8} + \tfrac{1}{z-\alpha^{10}} + \tfrac{1}{z-\alpha^{11}} \\
&\equiv \left(\alpha^5 + \alpha^8 + \alpha^{13} + \alpha^{14} + \alpha^{10}\right) + \\
&\left(\alpha^3 + \alpha^5 + \alpha^5 + \alpha^4 + \alpha^{14}\right) z + \\
&\quad \left(\alpha^{11} + 1 + \alpha^6 + \alpha^2 + \alpha^9\right) z^2 + \\
&\left(\alpha^9 + \alpha^{12} + \alpha^{13} + \alpha^7 + \alpha^{13}\right) z^3 \\
&= \alpha^{11} z^3 + \alpha^{13} z^2 + \alpha z
\end{aligned}
$$

2. Υπολογίζουμε το $\sigma(z)s(z) \left(\mathrm{mod} z^4 + \alpha^{14} z^2 + 1\right)$

$$
\begin{aligned}
\sigma(z)s(z) &= \left(z^2 + \sigma_1 z + \sigma_0\right)\left(\alpha^{11} z^3 + \alpha^{13} z^2 + \alpha z\right) \\
&= \alpha^{11} z^5 + \left(\alpha^{13} + \alpha^{11}\sigma_1\right) z^4 + \left(\alpha + \alpha^{13}\sigma_1 + \alpha^{11}\sigma_0\right) z^3 + \\
&\quad \left(\alpha\sigma_1 + \alpha^{13}\sigma_0\right) z^2 + \alpha\sigma_0 z \\
&\equiv \left(\alpha^{13} + \alpha^{11}\sigma_1\right) z^4 + \left(\alpha + \alpha^{13}\sigma_1 + \alpha^{11}\sigma_0 + \alpha^{10}\right) z^3 + \\
&\quad \left(\alpha\sigma_1 + \alpha^{13}\sigma_0\right) z^2 + \left(\alpha\sigma_0 + \alpha^{11}\right) z
\end{aligned}
$$

$$
\begin{aligned}
&\equiv \left(\alpha + \alpha^{13}\sigma_1 + \alpha^{11}\sigma_0 + \alpha^{10}\right) z^3 + \left(\alpha\sigma_1 + \alpha^{13}\sigma_0 + \alpha^{12} + \alpha^{10}\sigma_1\right) z^2 + \\
&\left(\alpha\sigma_0 + \alpha^{11}\right) z + \left(\alpha^{13} + \alpha^{11}\sigma_1\right)
\end{aligned}
$$

στο 3ο βήμα προσθέσαμε $\alpha^{11} z \hat{g}(z)$ και το 4ο $\left(\alpha^{13} + \alpha^{11}\sigma_1\right) \hat{g}(z)$. Καθώς ο κώδικας είναι δυαδικός, έχουμε την εξίσωση

$$
\sigma(z)s(z) \equiv \sigma'(z) \quad \left(\mathrm{mod} z^4 + \alpha^{14} z + 1\right)
$$

οπότε πρέπει να λύσουμε το παρακάτω σύστημα εξισώσεων

$$
\begin{cases}
\sigma_1 = \alpha^{13} + \alpha^{11}\sigma_1 \\
0 = \alpha\sigma_0 + \alpha^{11} \\
0 = \alpha\sigma_1 + \alpha^{13}\sigma_0 + \alpha^{12} + \alpha^{10}\sigma_1 \\
0 = \alpha + \alpha^{13}\sigma_1 + \alpha^{11}\sigma_0 + \alpha^{10}
\end{cases}
$$

Βρίσκουμε ότι $\sigma_0 = \alpha^{10}, \sigma_1 = \alpha$, οπότε

$$
\sigma(z) = z^2 + \alpha z + \alpha^{10} = \left(z + \alpha^{12}\right)\left(z + \alpha^{13}\right)
$$

3. Καθώς $\alpha_{11} = \alpha^{12}$ και $\alpha_{12} = \alpha^{13}$, βρίσκουμε ότι το σύνολο με τις θέσεις των σφαλμάτων είναι

$$
B = \{i | \sigma\left(\alpha_i\right) = 0\} = \{11, 12\}
$$

4. Το διάνυσμα σφάλματος λοιπόν είναι $e = (0,0,0,0,0,0,0,0,0,0,1,1)$.

5. Η αντίστοιχη κωδικολέξη είναι

$$
y - e = (1,1,0,0,0,0,1,0,1,1,1,1)
$$

Από τη κωδικολέξη μπορούμε να βρούμε το αρχικό μήνυμα m από

$$\left[G^T|c^T\right] = \left(\begin{array}{cccc|c} 10 & 0 & 0 & 1 & \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 10 & 0 & 0 & 1 & \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

Άρα καταλήγουμε, ότι το μήνυμα που μεταδώσαμε είναι το $(1, 1, 1, 1)$.

3.1.2 Κρυπτοσύστημα McEliece

Το κρυπτοσύστημα McEliece είναι ένας αλγόριθμος ασύμμετρης κρυπτογράφησης και κατασκευάστηκε από τον Robert McEliece το 1978. Ήταν από τα πρώτα κρυπτοσυστήματα που εισήγαγε την τυχαιότητα κατά τη διαδικασία της κρυπτογράφησης. Στηρίζεται στη δυσκολία του προβλήματος αποκωδικοποίησης ενός γραμμικού κώδικα, που θεωρείται ότι είναι ένα NP- πλήρες πρόβλημα, οπότε το καθιστά ισχυρό υποψήφιο για τον κλάδο της μετα-κβαντικής κρυπτογραφίας.

Πολλές παραλλαγές έχουν προταθεί για το συγκεκριμένο κρυπτοσύστημα, όπως και αυτή του Niederreiter με το οποίο θα ασχοληθούμε αργότερα, αλλά η αυθεντική εκδοχή από τον McEliece βασίζεται στους αμείωτους 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. Ακολουθεί μια πιο λεπτομερής περιγραφή του συστήματος.

Έστω P ένας $n \times n$ πίνακας μετάθεσης, δυαδικός με κάθε στήλη και γραμμή να περιέχει ένα μοναδικό 1 και όλα τα υπόλοιπα στοιχεία να είναι 0.

Παραγωγή κλειδιών

Βήμα 1: Επιλέγουμε ένα τυχαίο γραμμικό κώδικα $C[n, k, 2k + 1]$ στο $GF(2^m)$, ο οποίος έχει έναν αποτελεσματικό αλγόριθμο αποκωδικοποίησης D ο οποίος διορθώνει μέχρι t σφάλματα.

Βήμα 2: Υπολογίζουμε έναν $k \times n$ γεννήτορα πίνακα G, του C.

Βήμα 3: Παράγουμε έναν τυχαίο δυαδικό και αντιστρέψιμο $k \times k$ πίνακα, S.

Βήμα 4: Παράγουμε έναν τυχαίο $n \times n$ πίνακα μετάθεσης, P.

Βήμα 5: Υπολογίζουμε τον $k \times n$ πίνακα

$$G^{'} = SGP$$

Το δημόσιο κλειδί είναι το $(G^{'}, t)$ και το ιδιωτικό κλειδί είναι το (S, G, P, D).

Κρυπτογράφηση

Για να κρυπτογραφήσουμε ένα μήνυμα $m \in \{0,1\}^k$ επιλέγουμε ένα τυχαίο διάνυσμα $e \in \{0,1\}^k$ βάρους t και υπολογίζουμε το κρυπτοκείμενο

$$c = mG^{'} + e$$

Αποκρυπτογράφηση

Για να αποκρυπτογραφήσουμε ένα κρυπτοκείμενο $c \in \{0,1\}^k$, αρχικά υπολογίζουμε το

$$cP^{-1} = (mS)G + eP^{-1}$$

Στη συνέχεια εφαρμόζουμε τον πίνακα D και παίρνουμε το

$$c^{'} = mS$$

και έπειτα, εύκολα, λύνουμε ως προς το m οπότε είναι

$$m = c^{'}S^{-1}$$

3.1.3 Κρυπτοσύστημα Niederreiter

Προτάθηκε το 1986 από τον Herald Niederreiter. Είναι ντετερμινιστικό, έχει μεγαλύτερη ταχύτητα κρυπτογράφησης και μπορεί να χρησιμοποιηθεί για τη κατασκευή μιας ψηφιακής υπογραφής. Είναι μια παραλλαγή του κρυπτοσυστήματος McEliece με τη διαφορά ότι αντί για το γεννήτορα πίνακα, χρησιμοποιείται ο πίνακας ισοτιμίας για τη κρυπτογράφηση.[103]

Διαλέγουμε ένα τυχαίο διαχωρίσιμο πολυώνυμο $g(z)$ βαθμού t στο $GF(2^m)$. Ο κώδικας Goppa ορίζεται ως Γ και το $g(z)$ έχει παραμέτρους $[n, \geq n - mt, \geq 2t + 1]$. Υπολογίζουμε έναν πίνακα ισοτιμίας H, διαστάσεων $(n-k) \times n$. Στη συνέχεια διαλέγουμε έναν τυχαίο πυκνό $(n-k) \times (n-k)$ μη-χαρακτηριστικό πίνακα S και έναν τυχαίο πίνακα μεταθέσεων P ($n \times n$) και υπολογίζουμε το $H^* = SHP$. Κοινοποιούμε το H^* και το t και κρατάμε τα άλλα μυστικά.

Κάποιος που θέλει να στείλει ένα μήνυμα, το αναπαριστά σε μορφή δυαδικών ακολουθιών μήκους n, ικανοποιώντας τη συνθήκη $wt(m) \leq t$ για κάθε δυαδική ακολουθία m. Η κρυπτογράφηση του m γίνεται ως εξής

$$y = m\,(H^*)^T$$

το οποίο και στέλνεται.

Ο παραλήπτης μπορεί να υπολογίσει με το μυστικό πίνακα S το

$$y' = y\left(S^T\right)^{-1} = m\,(H^*)^T\left(S^T\right)^{-1} = mP^TH^TS^T\left(S^T\right)^{-1} = mP^TH^T$$

και με το κώδικα αποκωδικοποίησης Goppa, μπορεί να βρει ο παραλήπτης το $m^{'}$ τέτοιο ώστε $m'H^T = y'$, από το οποίο στη συνέχεια να πάρει το αρχικό μήνυμα υπολογίζοντας το

$$m'P = mP^TP = m$$

Παράδειγμα Niederreiter

Έστω Γ ο κώδικας Goppa του παραδείγματος 2 (σελ 104). Ας θυμίσουμε ότι κατά τη διαδικασία διόρθωση σφάλματος μπορούμε να διορθώσουμε μέχρι δύο σφάλματα. Είχαμε βρει ότι ο πίνακας ισοτιμίας,H, είναι ο

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

Αν διαλέξουμε, S, P

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

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

θα έχουμε

$$H^* = SHP = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Έστω ότι θέλουμε να στείλουμε το $m = (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$. Το κρυπτογραφημένο μήνυμα είναι

$$y = m\left(H^*\right)^T = (1,0,1,0,1,1,0,0)$$

Αφού παραλάβουμε το y, μπορεί ο παραλήπτης να χρησιμοποιήσει το μυστικό πίνακα S για να πάρει το

$$y' = y\left(S^T\right)^{-1} = (1,1,1,1,0,0,0,0)$$

Αυτό το διάνυσμα είναι ίσο με το mP^TH^T, άρα πάμε να βρούμε το $m' = mP^T$.

Όπως έχουμε δει το σύνδρομο $s(z)$ ενός διανύσματος v είναι

$$s(z) = \sum_{i=1}^{n} \frac{v_i}{z - \alpha_i}$$

και βρίσκεται από την εξίσωση

$$s(z) = vH^T$$

καθώς ο πίνακας ισοτιμίας H, είναι τέτοιος ώστε οι στήλες του να αποτελούνται από τα πολυώνυμα $\frac{1}{z-\alpha_i}$. Άρα το σύνδρομο του m' μπορεί να βρεθεί από τη σχέση

$$y' = (1,1,1,1,0,0,0,0) = \left(\beta^6, 0\right)$$

Άρα το σύνδρομο του m' είναι

$$s(z) = \beta^6 + 0 \cdot z = \beta^6$$

Εφαρμόζοντας τον αλγόριθμο του Patterson βρίσκουμε ότι

$$\sigma(z) = z^2 + z + \beta^7 = \left(z + \beta^3\right)\left(z + \beta^4\right)$$

Άρα

$$m' = (0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0)$$

Στο τέλος, παίρνουμε το m υπολογίζοντας το

$$m = m'P = (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$$

Πλεονεκτήματα-Μειονεκτήματα των κρυπτοσυστημάτων που βασίζονται σε γραμμικούς κώδικες

Πλεονεκτήματα

- Η ασφάλειά του McEliece είναι καλά μελετημένη ύστερα από την εισαγωγή του, το 1978.
- Οι εφαρμογές που χρησιμοποιούν το McEliece παρέχουν σχετικά υψηλές ταχύτητες κρυπτογράφησης-αποκρυπτογράφησης. Οι ταχύτητες των διαδικασιών για μια ασφαλή $n-$bit κρυπτογράφηση - αποκρυπτογράφηση είναι το πολύ της τάξεως του $O(n^2)$ ενώ για το RSA της τάξης του $O(n^6)$.
- Πιο γρήγορη παραγωγή κλειδιών σε σχέση με άλλα κλασσικά κρυπτοσυστήματα. Η υπολογιστική πολυπλοκότητα είναι της τάξεως του $O(n^3)$ για τα κρυπτοσυστήματα που βασίζονται σε γραμμικούς κώδικες, ενώ η παραγωγή του ζεύγους κλειδιών του RSA είναι της τάξεως του $O(n^4)$.
- Ο ρυθμός αύξησης της ανθεκτικότητας είναι πιο γρήγορος σε σχέση με το RSA όταν αυξάνουν σε μέγεθος τα κλειδιά. Τα μεγέθη των κλειδιών που απαιτούνται ώστε να επιτευχθεί μια $n-$bit ασφαλής επικοινωνία είναι της τάξεως του $\mathrm{O}\left(\mathrm{n}^2 \log^2 \mathrm{n}\right)$ για αυτού του είδους τα μετακβαντικά κρυπτοσύστηματα και για το RSA, της τάξεως του $O\left(n^3/\log^2 n\right)$ [105].

Μειονεκτήματα

- Όταν χρησιμοποιούνται πολλαπλές κρυπτογραφήσεις με τη βοήθεια του McEliece για το μήνυμα, το σύστημα είναι ευκολότερο να σπάσει.
- Τα κρυπτογραφημένα μηνύματα του McEliece είναι $\frac{n}{k}$ φορές μεγαλύτερα από τα απλά κείμενα.
- Το μέγεθος των κλειδιών είναι πολύ μεγάλο σε σύγκριση με το RSA. Τα κλειδιά κρυπτογράφησης των McEliece και Niederreiter έχουν μέγεθος 429.5 KB και 69.2 KB αντίστοιχα, ώστε να είναι το ίδιο ασφαλή όσο το RSA-2048, του οποίου έχουν μέγεθος μόλις 0.5KB.
- Δεν υπάρχει προφανής τρόπος ώστε να χρησιμοποιηθεί το McEliece για τη παραγωγή υπογραφής, όπως το RSA. Οι Courtois,Finiasz και Sendrier πρότειναν το κρυπτοσύστημα Niederreiter για αυτό το σκοπό.

Όπως αναφέραμε παραπάνω, το κρυπτοσύστημα Niederreiter χρησιμοποιείται για τη παραγωγή ηλεκτρονικής ψηφιακής υπογραφής και αυτό πραγματοποιείται με τη χρήση hash συναρτήσεων.

Παρόλα αυτά, το κρυπτοσύστημα Niederreiter έσπασε από τους Sidelnikov και Shestakov, μέσω μιας επίθεσης στο πυρήνα του συστήματος, που βασίζεται στη σχέση μεταξύ των γραμμικών κωδίκων Goppa και τους γενικευμένους Reed-Solomon κώδικες.

Ο Gabidulin, με τη σειρά του, πρότεινε τη χρήση μικρότερων κωδίκων, αλλά και πάλι υπάρχει γνωστή επίθεση που σπάει το κρυπτοσύστημα ακόμα και για τις παραμέτρους που πρότεινε.

Υπάρχουν αρκετές προτάσεις όσον αφορά τη βελτίωση των κρυπτοσυστημάτων που βασίζονται σε γραμμικούς κώδικες ή παραλλαγές αυτών. Μια ενδιαφέρουσα προσέγγιση είναι αυτή των

Misoczki,Tilich,Sendrier και Barreto, οι οποίοι κάνουν χρήση σχεδόν κυκλικών κωδίκων με πίνακες ελέγχου ισοτιμίας με "πειραγμένη" πυκνότητα. Επίσης, γίνεται χρήση μειωμένων ελλειπτικών κωδίκων, από τους Yevseiv,Rzayev,Korol και Imanova, με στόχο τη μείωση του μεγέθους των κλειδιών, την αύξηση της ταχύτητας των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης αλλά και τη μείωση του κόστους ενέργειας για τις διαδικασίες αυτές.

3.2 Δικτυώματα

Σε αυτό το κεφάλαιο περιγράφουμε μερικές από τις πιο πρόσφατες εξελίξεις στην κρυπτογραφία που στηρίζεται στη χρήση δικτυωμάτων. Οι κρυπτογραφικές κατασκευές με βάση τα δκτυώματα θεωρούνται ισχυροί υποψήφιοι για την μετά-κβαντική κρυπτογραφία, καθώς έχουν πολύ ισχυρά αποδεικτικά στοιχεία ασφαλείας που βασίζονται στη δυσκολία της χειρότερης-περίπτωσης προβλημάτων (worst-case hardness), σχετικά αποδοτικές εφαρμογές, καθώς και μεγάλη απλότητα. Επιπλέον, η κρυπτογραφία βάσει δικτυωμάτων πιστεύεται ότι είναι ασφαλής έναντι κβαντικών υπολογιστών.

Ένα δικτύωμα είναι παρόμοιο με έναν διανυσματικό χώρο, με τη σημαντική όμως διαφορά ότι παράγεται από όλους τους ακέραιους γραμμικούς συνδυασμούς των διανυσμάτων βάσης και όχι χρησιμοποιώντας πραγματικούς συντελεστές.

Ορισμός 3.6. *Έστω d, n φυσικοί αριθμοί και ένα σύνολο γραμμικά ανεξάρτητων διανυσμάτων $b_1, b_2, \ldots, b_d$ του $\mathbb{R}^n$. Ορίζουμε ως δικτύωμα (lattice) $L \subset \mathbb{R}^n$ τη διακριτή προσθετική υποομάδα του $\mathbb{R}^n$ που παράγεται από τα διανύσματα $b_i, i = 1, 2, \ldots, d$, δηλαδή το γραμμικό συνδυασμό*

$$L(b_1, b_2, \ldots, b_d) = \sum_{i=1}^{d} x_i \cdot b_i \ : x_i \in \mathbb{Z}$$

Αναφερόμαστε στην ακολουθία $b_1, b_2, \ldots, b_d$, ως βάση του δικτυώματος. Η βάση ενός δικτυώματος δεν είναι μοναδική και μπορεί να αναπαρασταθεί από ένα πίνακα $B = [b_1, \ldots, b_d] \in \mathbb{R}^n \times \mathbb{R}^n$ του οποίου οι στήλες είναι τα διανύσματα βάσης. Ο ακέραιος d καλείται βαθμίδα (rank) ή διάσταση του δικτυώματος (lattice dimension) και ο αριθμός n διάσταση του χώρου (embedding dimension). Εάν $d = n$, τότε λέμε ότι το δικτύωμα είναι δικτύωμα πλήρους βαθμίδας (full-rank lattice). Θα ασχοληθούμε μόνο με πλήρη δικτυώματα ακεραίων.

Αναφέραμε παραπάνω τον όρο «διακριτή προσθετική υποομάδα». Αυτό σημαίνει πως αν θεωρήσουμε ένα οποιοδήποτε σημείο-διάνυσμα $v \in L$, τότε μπορούμε πάντοτε να βρούμε ένα $\epsilon > 0$,(οσοδήποτε μικρό), έτσι ώστε:

$$L \cap \{w \ \in \mathbb{R}^n \ : ||v - w|| < \epsilon \ \} = \{v\}$$

Με άλλα λόγια, είναι πάντα δυνατόν να "κατασκευάσουμε" μια n-διάστατη σφαίρα με κέντρο το διάνυσμα v και ακτίνα ϵ, η οποία να μην τέμνει το δικτύωμα L.

Ορισμός 3.7. *Έστω L ένα πλήρες δικτύωμα και $\{b_1, b_2, \ldots, b_n\}$ μια βάση του. Τα διανύσματα βάσης σχηματίζουν ένα n-διάστατο παραλληλεπίπεδο F στον $\mathbb{R}^n$, το οποίο καλείται θεμελιώδες χωρίο ή θεμελιώδες παραλληλεπίπεδο (fundamental domain ή fundamental parallelepiped) της βάσης του δικτυώματος και συμβολίζεται*

$$F(b_1, b_2, \ldots, b_n) = \{t_1 + b_1, t_2 + b_2, \ldots, t_n + b_n \ : 0 \leq t_i < 1 \ , \forall i = 1, \ldots, n\}$$

Πρόταση 3.8. *Έστω ότι $B = \{b_1, b_2, \ldots, b_n\}$ είναι μια βάση ενός δικτυώματος L και ότι F είναι το n-διάστατο ορθογώνιο παραλληλόγραμμο με ακμές τα διανύσματα βάσης. Τότε:*

$$vol(F) = det(L)$$

Πρόταση 3.9. *Έστω ότι $B = \{b_1, b_2, \ldots, b_n\}$ είναι μια βάση ενός δικτυώματος L και F το αντίστοιχο θεμελιώδες χωρίο της. Τότε ισχύει η ανίσωση:*

$$det(L) = vol(F) \leq ||b_1||||b_2|| \ldots ||b_n||$$

Η ανισότητα αυτή γίνεται ισότητα αν τα διανύσματα είναι ορθογώνια.

Στενά συνδεδεμένος με ένα δικτύωμα L, είναι ο πίνακας Gram που του αντιστοιχεί και περιέχει τα εσωτερικά γινόμενα για κάθε δυνατό ζεύγος διανυσμάτων μιας βάσης B.

Ορισμός 3.10. *Ορίζουμε ως πίνακα του Gram (Gram matrix) του δικτυώματος L με βάση $B = b_1, b_2, \ldots, b_n$ τον $n \times n$ συμμετρικό πίνακα:*

$$G = B \cdot B^T = b_i \cdot b_j$$

Ορισμός 3.11. *Η ορίζουσα (determinant) ενός δικτυώματος ορίζεται ως:*

$$det(L) = \sqrt{det(G)} = \sqrt{det(B \cdot b^T)}$$

Στη περίπτωση πλήρη δικτυωμάτων ισχύει: $det(L) = |det(B)|$.

Πρόταση 3.12. *Η ορίζουσα ενός δικτυώματος $L \subset \mathbb{R}^n$ είναι ανεξάρτητη από την επιλογή βάσης.*

Το γεγονός αυτό είναι αναμενόμενο καθώς η ορίζουσα, det, ενός δικτυώματος γεωμετρικά αναπαριστά τον n-διάστατο όγκο του παραλληλεπιπέδου του $\mathbb{R}^n$ με πλευρές τα διανύσματα βάσης που αναφέραμε προηγουμένως.

Ορισμός 3.13. *(Δυϊκό Δικτύωμα - Dual Lattice). Το δυϊκό ενός δικτυώματος $L \in \mathbb{R}^n$ ορίζεται ως:*

$$L^* = \{x \in span(L) :< x, y >\in \mathbb{Z}, \forall y \in (L)$$

Εάν διαθέτουμε ένα σύνολο γραμμικά ανεξάρτητων διανυσμάτων τα οποία είναι σε πλήθος λιγότερα από τη διάσταση του χώρου, τότε προφανώς αυτά παράγουν ένα (υπο)δικτύωμα στον χώρο.

Ορισμός 3.14. *Έστω $L \subset \mathbb{R}^n$ ένα δικτύωμα και $\{x_1, x_2, \ldots, x_n\}$ μια βάση του. Επιπλέον, έστω ότι $y_1, y_2, \ldots, y_n$ είναι ένα σύνολο από γραμμικά ανεξάρτητα διανύσματα και $M \subset \mathbb{R}^n$ το δικτύωμα που παράγεται από αυτά. Αν ισχύει*

$$y_i = \sum_{j=1}^{n} c_{i,j} x_j \ , \ \forall i = 1, 2, \ldots, n \text{ όπου } c_{i,j} \in \mathbb{Z}, \forall i, j$$

το M καλείται υποδικτύωμα (sublattice) του L και ισχύει $M \subseteq L$.

Η παραπάνω σχέση μπορεί να γραφεί επίσης με τη βοήθεια πινάκων ως εξής:

$$Y = CX$$

όπου $C = (c_{i,j})$ είναι ο αντιστρέψιμος $n \times n$ πίνακας των ακεραίων συντελεστών, X ο πίνακας με γραμμές τα διανύσματα x_i και Y με τα διανύσματα y_i αντίστοιχα.

Η προηγούμενη εξίσωση πινάκων συνεπάγεται πως και οι αντίστοιχες ορίζουσες είναι ίσες, δηλαδή:

$$det(Y) = det(CX) \Longrightarrow det(C) = \frac{det(Y)}{det(X)},\ (det(X) \neq 0)$$

Ορισμός 3.15. *Ορίζουμε ως δείκτη (index) ρ του υποδικτυώματος M ενός δικτυώματος L τον φυσικό αριθμό:*

$$\rho = |det(C)| = \frac{|det(Y)|}{|det(X)|} = \frac{det(M)}{det(L)}$$

Από τα παραπάνω παρατηρούμε πως ο δείκτης ρ είναι ανεξάρτητος από την εκλογή βάσεων για τα δικτυώματα M και L.

Λήμμα 3.16. *Εάν L είναι ένα δικτύωμα και M ένα υποδικτύωμά του με δείκτη ρ,τότε:*

$$\rho L \subseteq M \subseteq L$$

Λήμμα 3.17. *Δοθείσης μιας οποιασδήποτε βάσης του υποδικτυώματος M, ενός δικτυώματος L, μπορούμε πάντοτε να βρούμε μια βάση του δικτυώματός του L.*

Ορισμός 3.18. *(ιδεώδες δικτύωμα) Ένα ιδεώδες δικτυώματος είναι ένα δικτύωμα ακέραιων $L(B) \subseteq \mathbb{Z}^n$, τέτοιο ώστε $B = \{gmodf : g \in I\}$ για κάποιο μονικό πολυώνυμο f βαθμού n και ένα ιδεώδες $I \subseteq \mathbb{Z}[x]/ < f >$ το οποίο καθορίζει ένα αντίστοιχο υποδικτύωμα ακέραιων $L(I) \subseteq \mathbb{Z}^n$.*

Ορισμός 3.19. *(Κυκλικό δικτύωμα) Ένα σύνολο $L \subset \mathbb{Z}^n$ λέγεται κυκλικό δικτύωμα αν είναι ένα ιδεώδες στο $\mathbb{Z}[x]/(x^n - 1)$.*

Στη πράξη θεωρούμε την ενσωμάτωση συντελεστών ως εξής:

$$\sigma : \mathbb{Z}[x]/(x^n - 1) \longrightarrow \mathbb{Z}^n$$
$$a_0 + a_1 x + \hat{\cdots} + a_{n-1}x^{n-1} \mapsto (a_0, \ldots, a_{n-1})$$

και έτσι αναγνωρίζουμε το L ως $\sigma(L)$. Με αυτό το τρόπο, αφού το L είναι κλειστό ως προς τον πολλαπλασιασμό $xmod(x^n - 1)$, μπορούμε να "φανταζόμαστε" ένα κυκλικό δικτύωμα ως ένα σύνολο $n-$άδων στο $\mathbb{Z}^n$ τέτοιο ώστε:

- *Για $v, u \in L$,έχουμε $v + u \in L$.*
- *Δοθέντος ενός $v \in L$, το $-v \in L$.*
- *Για $v = (v_1, \ldots, v_n) \in L$, κάθε κυκλική μετατόπιση των συντελεστών βρίσκεται και αυτή εντός του L.*

Ορισμός 3.20. *(q-ary δικτύωμα) Ένα δικτύωμα $L \subset \mathbb{Z}^n$ καλείται $q-ary$ δικτύωμα για κάποιον συγκεκριμένο ακέραιο q (πιθανότατα πρώτο), αν ισχύει*

$$q\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$$

Τέτοιου είδους δικτυώματα είναι σε $1-1$ αντιστοιχία με τους γραμμικούς κώδικες στο $\mathbb{Z}_q^n$. Τα περισσότερα κρυπτοσυστήματα που βασίζονται στα δικτυώματα χρησιμοποιούν $q-ary$ δικτυώματα.

Θα ασχοληθούμε με δύο είδη $q-ary$ δικτυωμάτων: Δοθέντος ενός πίνακα $A \in \mathbb{Z}_q^{n\times m}$ για q, n, m ακέραιους έχουμε:

- $L_q(A) = \{y \in \mathbb{Z}^m : y = A^T s mod q, \text{ για κάποιο } s \in \mathbb{Z}^n\}$. Παράγεται από τις γραμμές του A και αντιστοιχεί στο κώδικα που παράγουν.
- $L_q^{\perp}(A) = \{y \in \mathbb{Z}^m : Ay = 0 mod\ q\}$. Περιέχει όλα τα διανύσματα που είναι ορθοκανονικά $mod q$ στις γραμμές του A και αντιστοιχεί στο κώδικα στον οποίο ο πίνακας ελέγχου ισοτιμίας του A είναι ο ίδιος ο A.

Επίσης είναι δυικά μεταξύ τους εξ ορισμού, δηλαδή

$$\begin{cases} L_q^{\perp}(A) = qL_q(A)^* \\ L_q(A) = qL_q^{\perp}(A)^* \end{cases}$$

Ορισμός 3.21. *(Ελάχιστη απόσταση) Για κάθε δικτύωμα L, η ελάχιστη απόσταση του L, είναι η μικρότερη απόσταση μεταξύ δύο σημείων του δικτυώματος, δηλαδή*

$$\lambda(L) = inf\{||x-y|| : x, y \in L, x \neq y\}$$

Παρατηρούμε ότι η ελάχιστη απόσταση μπορεί να οριστεί και ως το μήκος του βραχύτερου μη μηδενικού διανύσματος στο δικτύωμα L

$$\lambda_1(L) = inf\{||v|| : v \in L\ \{0\}\}$$

Ορίζουμε ως $i-$οστό διαδοχικό ελάχιστο (successive minimum) $\lambda_i(L)$ το μικρότερο $r > 0$, τέτοιο ώστε το L να περιέχει τουλάχιστον k γραμμικά ανεξάρτητα διανύσματα μήκους $\leq r$. Τώρα ορίζουμε το

$$\lambda_1(L) = min_{v\neq 0\ \in L}||v|| = min_{x\neq y \in L}||x-y||$$

Φράγματα για το λ_1

Κάτω φράγμα

Θεώρημα 3.22. *Για κάθε βάση B ενός δικτυώματος L και τη γραμμικοποίησή της $\bar{B}$ κατά Gram-Schmidt, έχουμε*

$$\lambda_1(L(B)) \geq min_i||\bar{b_i}||$$

΄Ανω Φράγμα

Θεώρημα 3.23. *(Πρώτο θεώρημα Minkowski) Κάθε κυρτό συμμετρικό σώμα S, με $vol(S) > 2^n det(L)$ περιέχει ένα μη μηδενικό σημείο του δικτύωματος L.*

Πρόταση 3.24.

$$\lambda_1(L) \leq \sqrt{n}(det(L))^{\frac{1}{n}}$$

Θεώρημα 3.25. *(Δεύτερο θεώρημα Minkowski) Ισχύει ότι*

$$(\sum_{i=1}^{n} \lambda_i(L))^{\frac{1}{n}} \leq \sqrt{n}(det(L))^{\frac{1}{n}}$$

3.2.1 Υπολογιστικά Προβλήματα

Ορισμός 3.26. *(Πρόβλημα βραχύτερου διανύσματος SVP) Δοθείσης μιας αυθαίρετης βάσης B ενός δικτυώματος L, να βρεθεί το βραχύτερο μη μηδενικό διάνυσμα στο δικτύωμα, δηλαδή να βρεθεί ένα διάνυσμα $v \in L$ τέτοιο ώστε*

$$||v|| = \lambda_1(L)$$

Συνήθως στις εφαρμογές, ασχολούμαστε με τα προσεγγιστικά προβλήματα δικτυωμάτων. Είναι τα ίδια προβλήματα απλά παραμετρικοποιημένα με έναν παράγοντα προσέγγισης $\gamma \geq 1$, ο οποίος συνήθως εξαρτάται από τη διάσταση n του δικτυώματος, δηλαδή $\gamma = \gamma(n)$. Ακριβέστερα, στα πρωτόκολλα, ο παράγοντας αυτός πρέπει να είναι πολυωνυμικός ως προς το n, δηλαδή $\gamma = poly(n)$.

Παραλλαγές του SVP:

- Προσεγγιστικό Πρόβλημα Αναζήτησης βραχύτερου διανύσματος $(SVP)_\gamma$: Δοθείσης μιας αυθαίρετης βάσης B ενός $n-$διάστατου δικτυώματος L, να βρεθεί το βραχύτερο μη μηδενικό διάνυσμα v στο δικτύωμα, τέτοιο ώστε:

$$||v|| = \gamma(n)\lambda_1(L)$$

- Προσεγγιστικό Πρόβλημα Αναζήτησης βραχύτερου Ανεξάρτητου διανύσματος $(SIVP)_\gamma$: Δοθείσης μιας αυθαίρετης βάσης B ενός $n-$διάστατου δικτυώματος L, να βρεθεί ένα σύνολο $S = \{s_i\}_{i=1}^n \subset L,\ n$ το πλήθος γραμμικά ανεξάρτητων διανυσμάτων του δικτυώματος με

$$||s||_i \leq \gamma(n) \cdot \lambda_n(L)\ \forall i$$

- Προσεγγιστικό Πρόβλημα Απόφασης βραχύτερου διανύσματος ($GapSVP_\gamma$): Δοθείσης μιας αυθαίρετης βάσης B ενός $n-$διάστατου δικτυώματος L και ενός θετικού πραγματικού αριθμού d , να αποφασιστεί αν $\lambda_1(L) \leq d$ ή $\lambda_1(L) > \gamma(n)d$.

Ορισμός 3.27. *(Bounded-Distance Decoding BDD) Δοθείσης μιας βάσης $B, t \in \mathbb{R}^n$ και πραγματικό αριθμό $d < \frac{\lambda_1}{2}$ τέτοιο ώστεε dist$(t, L) \leq d$, βρείτε το μοναδικό $v \in L$ πλησιέστερα στο t. Το BDD είναι αντίστοιχο της εύρεσης του $e \in (t + L)$ τέτοιο ώστε $||e|| \leq d$.*

Για την επίλυση του παραπάνω προβλήματος έχουμε τον εξής αλγόριθμο:

- **Babai's Round off**: Χρησιμοποιώντας μια καλή βάση B ενός δικτυώματος L τότε

$$t = \sum a_i b_i \longrightarrow e := \sum (a_i - [a_i])b_i$$

  Ο αλγόριθμος "δουλεύει" αν Ball$(d) \leq P(b)$. Δηλαδή, $d \leq min||b_i^{\perp}/2||$, όπου $b_i^{\perp}$ είναι το ορθογώνιο του b_i στο υπερεπίπεδο που φτιάχνεται από το span$\{b_1, \ldots, b_i, \ldots, b_n\}$.

Όσον αφορά την ασφάλεια, οι κρυπτογραφικές κατασκευές δικτυωμάτων μπορούν να διαχωριστούν σε δύο είδη. Στο πρώτο είδος, περιέχονται πρακτικές προτάσεις, που τυπικά είναι πολύ αποτελεσματικές, αλλά συνήθως δεν διαθέτουν αποδεικτικά στοιχεία ασφαλείας. Ο δεύτερος τύπος παρέχει ισχυρές εγγυήσεις ασφάλειας, που στηρίζονται στο worst-case hardness των προβλημάτων σε δικτυώματα, αλλά λίγα από αυτά είναι εφαρμόσιμα στη πράξη.

3.2.2 Το κρυπτοσύστημα δημοσίου κλειδιού GGH-βάση HNF

Το 1996 οι Goldreich, Goldwasser και Halevi πρότειναν ένα κρυπτοσύστημα δημοσίου κλειδιού στο πεδίο των δικτυωμάτων, το οποίο είναι ανάλογο του κρυπτοσυστήματος McEliece το οποίο είχε προταθεί 20 χρόνια νωρίτερα και στηρίζεται στη δυσκολία αποκωδικοποίησης γραμμικών κωδίκων πάνω σε πεπερασμένα σώματα (ή αλλιώς στο πρόβλημα Bounded Distance Decoding). Αν και ο Nguygen το 1999 κατάφερε να επιτεθεί και να σπάσει το κρυπτοσύστημα τους, η βασική ιδέα, όντας απλή, παραμένει ως βάση για πολλά μετέπειτα κρυπτοσυστήματα σε αυτόν τον τομέα $[107]$.

Δημιουργία κλειδιών

- Ιδιωτικό κλειδί: Ως ιδιωτικό κλειδί θεωρούμε μια "καλή" βάση B του δικτυώματος L. Με τον όρο καλή βάση εννοούμε μια βάση που αποτελείται από σχεδόν ορθοκανονικά διανύσματα. (Από υπολογιστική σκοπιά, οι "καλές" βάσεις μας επιτρέπουν να λύνουμε αποτελεσματικά διάφορες παραλαγές του προβλήματος CVP στο $L(B)$, όπως π.χ. περιπτώσεις στις οποίες ο στόχος είναι πολύ κοντά στο δικτύωμα.)

- Δημόσιο κλειδί: Ως δημόσιο κλειδί H επιλέγουμε μια "κακή" βάση του δικτυώματος L με $L(H) = L(B)$. Ως "κακή" βάση είχε προτείνει ο Micciancio $[107]$, τη Κανονική Μορφή Hermite (Hermite Normal Form, HNF) της βάσης B.

  Ορισμός 3.28. *(HNF μορφή ενός πίνακα) Ένας μη-μοναδιαίος πίνακας $B = [b_1, \ldots, b_n] \in \mathbb{R}^{m \times n}$ είναι σε HNF μορφή αν*

  - *Υπάρχουν $1 \leq i_1 < \cdots < i_n \leq m$, τέτοιο ώστε $b_{i,j} \neq 0 \Rightarrow (j < h) \wedge (i \geq i_j)$*

– *Για όλα τα* $k > j,\ 0 \leq b_{i_j,k} < b_{i_j,j}$*, δηλαδή όλα τα στοιχεία στις γραμμές* i_j *μειώνονται κατά* $modulo\ b_{i_j,j}$.

Το h *είναι ο αριθμός των μη-μηδενικών στηλών του πίνακα και το* i_j *είναι η γραμμή του μεγαλύτερου μη μηδενικού στοιχείου της στήλης* j*. Επειδή αυτά αυξάνουν αυστηρά, κάθε στήλη περιέχει γραμμές τις οποίες δεν έχει καμία άλλη στήλη. Για αυτό, οι μη-μηδενικές στήλες ενός πίνακα σε* HNF *μορφή είναι εξασφαλισμένο ότι θα είναι γραμμικά ανεξάρτητες. Επίσης η* HNF *μορφή είναι μοναδική, δηλαδή αν δύο πίνακες* B *και* B' *είναι σε* HNF *και παράγουν το ίδιο δικτύωμα* $L(B) = L(B')$ *τότε* $B = B'$*. Λέμε ότι* H *είναι η* HNF *μορφή του* B *αν* $L(H) = L(B)$ *και η* H *δεν περιέχει μηδενικές στήλες.*

Η HNF μορφή δίνει μια κάτω τριγωνική βάση για το $L(B)$, η οποία είναι μοναδική όπως αναφέραμε και στον ορισμό παραπάνω.

Κρυπτογράφηση

Κατά τη διαδικασία της κρυπτογράφησης, θεωρούμε ένα διάνυσμα $v \in L(B)$ και προσθέτουμε σε αυτό ένα διάνυσμα r. Ο Micciancio, πάλι, είχε προτείνει $[107]$ να διαλέξουμε το v, σύμφωνα με την HNF βάση, δηλαδή όλοι οι συντελεστές του διανύσματος $v + r$ να μειώνονται με βάση το $modulo$ του αντίστοιχου κατά μήκους στοιχείου της διαγωνίου της δημόσιας HNF βάσης H. Ύστερα από αυτή τη διαδικασία, το διάνυσμα το συμβολίζουμε με $rmodH$, και έχει αποδειχτεί ότι η κρυπτανάλυση αμέσως γίνεται πολύ δυσκολότερη καθώς το $rmodH$ μπορεί να υπολογιστεί από κάθε διάνυσμα της μορφής $r + v$, απλά υπολογίζοντας πρώτα το $r + vmodH = rmodH$.

Αποκρυπτογράφηση

Κατά τη διαδικασία της αποκρυπτογράφησης, θα χρησιμοποιήσουμε την "καλή" βάση και το πρόβλημα είναι να βρούμε το πιο κοντινό διάνυσμα v στο κρυπτοκείμενο $c = rmodH = r + v$ και το αντίστοιχο διάνυσμα σφάλματος $r = c - v$.

Η ασφάλεια του συγκεκριμένου κρυπτοσυστήματος βασίζεται στο ότι γνωρίζοντας μια "κακή" βάση είναι δύσκολο να κατασκευάσουμε μια "καλή" από αυτήν και επίσης είναι ακόμα δυσκολότερο να λύσουμε το CVP πρόβλημα, χρησιμοποιώντας μια "κακή" βάση $[107]$.

3.2.3 Το κρυπτοσύστημα δημοσίου κλειδιού NTRU

Το κρυπτοσύστημα δημοσίου κλειδιού $NTRU$, προτάθηκε το 1996 από τους Hoffestein,Pipher και Silverman. Το $NTRU$ στηρίζεται στη δυσκολία εύρεσης "μικρών" λύσεων σε συστήματα γραμμικών εξισώσεων πάνω σε συγεκριμένες κλάσεις δικτυωμάτων σε Ευκλείδιους χώρους πολλών διαστάσεων. Αυτό που το ξεχωρίζει είναι η υψηλή ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης σε σχέση με τα κλασικά συστήματα. Επίσης είναι το πιο ευρέως αποδεκτό ως προς την ανθεκτικότητά του σε γνωστές κβαντικές επιθέσεις.

Το μαθηματικό υπόβαθρο που κρύβεται πίσω από το συγκεκριμένο κρυπτοσύστημα είναι αρκετά ενδιαφέρον αλλά και περίπλοκο καθώς συνδυάζει πολλές ιδέες από την άλγεβρα, τη θεωρία αριθμών αλλά και μεθόδους μείωσης δικτυωμάτων $[87]$.

NTRU με δακτύλιους

Η βασική αριθμητική, στην οποία στηρίζονται οι διαδικασίες του κρυπτοσυστήματος $NTRU$, βρίσκεται στο δακτύλιο πολυωνύμων $P = \frac{\mathbb{Z}_q[X]}{X^N - 1}$. Στον συγκεκριμένο δακτύλιο, οι συντελεστές ενός πολυωνύμου f ορίζονται από τη βάση $\{1, X, X^2, \ldots, X^{N-1}\}$ και έχει τη μορφή:

$$f = (f_0, f_1, \ldots, f_{N-1}) = f_0 + f_1 X + \ldots f_{N-1} X^{N-1}$$

Ορίζουμε δύο πράξεις, τη πρόσθεση δύο στοιχείων f, g ως προς συντεταγμένες

$$f + g = (f_0 + g_0, f_1 + g_1, \ldots, f_{N-1} + g_{N-1})$$

και το πολλαπλασιασμό

$$f \cdot g = h = (h_0, h_1, \ldots, h_{N-1}) \text{ με } h_k = \sum_{i+j \equiv k mod N} f_i g_j$$

.

Επίσης ορίζουμε την Ευκλείδια νόρμα ενός στοιχείου f ως

$$||f|| = \sqrt{\sum_{i=0}^{N-1} f_i^2}$$

Τέλος, ορίζουμε το δυαδικό σύνολο $B(d)$, που αποτελείται από πολυώνυμα με θετικούς ακέραιους d, με d συντελεστές ίσους με 1 και όλους τους υπόλοιπους ίσους με το μηδέν και το δυαδικό σύνολο $B(d)$ έχει τη μορφή

$$B(d) = \{f(x) = \sum_{i=0}^{N-1} f_i X^i \in P \mid f_i \in \{0, 1\} \ , \ \sum_{i=0}^{N-1} f_i = d\}$$

Στο κρυπτοσύστημα $NTRU$ οι παράμετροι που χρησιμοποιούνται είναι έξι (6) δημόσιοι ακέραιοι N, p, q, d_f, d_g, d_r και τέσσερις (4) δημόσιοι χώροι L_f, L_g, L_m, L_r τους οποίους θα αναφέρουμε παρακάτω αναλυτικά.

- Ο N είναι πρώτος αριθμός και αρκετά μεγάλος προκειμένου να αποτρέψουμε κρυπταναλυτικές επιθέσεις που στηρίζονται σε δικτυώματα.
- Οι p και q είναι πρώτοι αριθμοί με $p >> q$ (αρκετά μεγαλύτερο).
- $L_f = B(d_f)$, είναι ένα σύνολο από μικρά πολυώνυμα από τα οποία διαλέγουμε τα ιδιωτικά μας κλειδιά.
- $L_g = B(d_g)$, επίσης είναι ένα σύνολο από μικρά πολυώνυμα από τα οποία διαλέγουμε άλλα ιδιωτικά κλειδιά.

- $L_m = \dfrac{\mathbb{Z}_p[X]}{X^N - 1}$, είναι ο χώρος που βρίσκεται το απλό κείμενο που θέλουμε να κρυπτογραφήσουμε (plaintext). Είναι ένα σύνολο πολυωνύμων $m \in \dfrac{\mathbb{Z}_p[X]}{X^N - 1}$, τα οποία αναπαριστούν τα κρυπτογραφημένα μηνύματα.
- $L_r = B(d_r)$, είναι ένα σύνολο πολυωνύμων από το οποίο λαμβάνουμε τη "κρυφή τιμή", όπως συνηθίζεται να την αποκαλούμε, που χρησιμοποιούμε κατά τη διαδικασία της κρυπτογράφησης.

Δημιουργία κλειδιών

- Διαλέγουμε τυχαία ένα πολυώνυμο $f \in L_f$, τέτοιο ώστε το f να είναι αντιστρέψιμο στο $Pmodulop$ και $moduloq$ αντίστοιχα.
- Υπολογίζουμε τα
$$f_p \equiv f^{-1}(modp)$$
$$f_q \equiv f^{-1}(modq)$$
- Επιλέγουμε τυχαία ένα πολυώνυμο $g \in L_g$.
- Υπολογίζουμε το $h \equiv g * f_q(modq)$.
- Δημοσιοποιούμε το δημόσιο κλειδί (N, h) και το σύνολο των παραμέτρων p, q, L_f, L_r, L_m.
- Αντίστοιχα, το ιδιωτικό μας κλειδί θα είναι το (f, f_p).

Κρυπτογράφηση

- Αναπαριστούμε το μήνυμα σε μορφή πολυωνύμου $m \in L_m$.
- Επιλέγουμε τυχαία ένα πολυώνυμο $r \in L_r$.
- Κρυπτογραφούμε το μήνυμα m με το δημόσιο κλειδί (N, h) σύμφωνα με τη παρακάτω διαδικασία
$$e \equiv p \cdot r \cdot h + m(modq)$$

Αποκρυπτογράφηση

- Ο παραλήπτης υπολογίζει το $a \equiv f \cdot e(modq)$.
- Συνήθως, αν το πολυώνυμο έχει πολύ μεγάλους συντελεστές, χρησιμοποιούμε μια διαδικασία που ονομάζεται centering και μετατρέπουμε το a σε πολυώνυμο με συντελεστές από το εσωτερικό του $[-\frac{q}{2}, \frac{q}{2}]$, δηλαδή μειώνουμε τους συντελεστές όσο χρειάζεται ώστε η αποκρυπτογράφηση να γίνει επιτυχώς.
- Υπολογίζουμε το $m \equiv f_p * a(modp)$.

Η μέθοδος της αποκρυπτογράφησης είναι σωστή αν το πολυώνυμο $p * r * q + f * m(modq)$ είναι ίσο-ανάλογο με το $p * r * g + f \cdot m \in \dfrac{\mathbb{Z}[X]}{(X^N - 1)}$ χωρίς να χρησιμοποιούμε το $moduloq$.

NTRU με δικτυώματα

Πέρα από το NTRU που στηρίζεται στη θεωρία δακτυλίων, μπορούμε να κατασκευάσουμε ένα ανάλογο κρυπτοσύστημα NTRU βασιζόμενοι στη θεωρία δικτυωμάτων $[107]$.

Ένας τυχαίος πίνακας $A \in \mathbb{Z}_q^{n \times m}$ μπορεί να αντικατασταθεί από έναν πίνακα από blocks της μορφής

$$A = [A^{(1)}| \dots |A^{(m/n)}]$$

όπου κάθε block $A^{(i)} \in \mathbb{Z}_q^{n \times n}$ είναι ένας κυκλομεταθετικός πίνακας

$$A^{(i)} = \begin{bmatrix} a_1^{(i)} & a_n^{(i)} & \dots & a_3^{(i)} & a_2^{(i)} \\ a_2^{(i)} & a_1^{(i)} & \dots & a_4^{(i)} & a_3^{(i)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1}^{(i)} & a_{n-2}^{(i)} & \dots & a_1^{(i)} & a_n^{(i)} \\ a_n^{(i)} & a_{n-1}^{(i)} & \dots & a_2^{(i)} & a_1^{(i)} \end{bmatrix}$$

δηλαδή ένας πίνακας με τις στήλες να είναι όλες κυκλικές περιστροφές της πρώτης στήλης $a^{(i)} = (a_1^i, \dots, a_n^i)$. Χρησιμοποιώντας τώρα το συμβολισμό πινάκων,

$$A^{(i)} = [a^{(i)}, Ta^{(i)}, \dots, T^{n-1}a^{(i)}]$$

όπου

$$T = \left[\begin{array}{ccc|c} & O^T & & 1 \\ \hline \ddots & & & \\ & I & & 0 \\ & & \ddots & \end{array}\right]$$

είναι ένας πίνακας μεταθέσεων που περιστρέφει τις συντεταγμένες του $a^{(i)}$ κυκλικά. Η κυκλομεταθετική δομή των blocks έχει δύο άμεσες συνέπειες.

1. Μειώνει την απαίτηση αποθηκευτικού χώρου για το κλειδί από nm στοιχεία του $\mathbb{Z}_q$ σε μόνο m στοιχεία, διότι κάθε block $A^{(i)}$ είναι πλήρως καθορισμένο από τη πρώτη στήλη $a^{(i)} = (a_1^{(i)}, \dots, a_n^1)$.

2. Μειώνει επίσης (τουλάχιστον ασυμπτωτικά) το χρόνο διαδικασίας του να υπολογίσουμε το γινόμενο πίνακα-διάνυσμα $Aymodq$, από $O(mn)$ αριθμητικές πράξεις (στο $\mathbb{Z}_q$) σε μόνο $\tilde{O}(m)$ πράξεις,διότι ο πολλαπλασιασμός με έναν κυκλομεταθετικό πίνακα μπορεί να υλοποιηθεί σε $\tilde{O}(n)$ χρόνο χρησιμοποιώντας τον Γρήγορο Μετασχηματισμό Fourier (FFT).

Έστω λοιπόν T ο γραμμικός μετασχηματισμός που περιστρέφει τις συντεταγμένες ενός διανύσματος εισόδου κυκλικά, και ορίζουμε $T^*v = [v, Tv, \dots, T^{n-1}v]$ να είναι ο κυκλομεταθετικός πίνακας του διανύσματος $v \in \mathbb{Z}^n$. Τα δικτυώματα που χρησιμοποιούμε στο συγκεκριμένο κρυπτοσύστημα NTRU είναι συνελικτικά κατά μέτρο δικτυώματα (convolutional modular lattices), διάστασης $2n$ και έχουν τις εξής δύο ιδιότητες:

1. Είναι κλειστά ως προς τον γραμμικό μετασχηματισμό που αντιστοιχεί το διάνυσμα (x, y) (όπου x, y είναι $n-$διάστατα διανύσματα) στο διάνυσμα (Tx, Ty).

2. Είναι q-ary δικτυώματα, με την έννοια ότι πάντα διατηρούν ως υποδικτύωμα το $q\mathbb{Z}^{2n}$ και έτσι η ιδιότητα του να είναι στοιχείο το (x, y) στο δικτύωμα εξαρτάται μόνο από το $(x, y) moduloq$.

Οι παράμετροι του συστήματος είναι η διάσταση n η οποία είναι πρώτος αριθμός, ένας ακέραιος modulus q, ένας μικρός ακέραιος p και ένας ακέραιος φραγμένου βάρους d_f.

Παραγωγή κλειδιών

Ιδωτικό κλειδί: Το ιδιωτικό κλειδί στο NTRU είναι ένα μικρό διάνυσμα $(f, g) \in \mathbb{Z}^{2n}$. Ένα δικτύωμα που αντιστοιχεί στο ιδιωτικό κλειδί (f, g) είναι το $L_q((T^*f, T^*g)^T)$, που είναι το ελάχιστο συνελικτικό κατά μέτρο δικτύωμα που περιέχει το (f, g). Τα μυστικά διανύσματα f, g είναι υποκείμενα στους ακόλουθους τεχνικούς περιορισμούς:

1. Ο πίνακας $[T^*f]$ πρέπει να είναι αντιστρέψιμος $moduloq$.

2. $f \in e_1 + \{p, 0, -p\}^n$ και $g \in \{p, 0, -p\}^n$ είναι δύο τυχαία επιλεγμένα πολυώνυμα τέτοια ώστε $f - e_1$ και g να έχουν ακριβώς $d_f + 1$ θετικές εισόδους και d_f αρνητικές. Οι υπόλοιπες $N - 2d_f - 1$ είσοδοι είναι μηδέν.

Υπό τους περιορισμούς αυτούς παρατηρούμε ότι

$$\begin{cases} Tf = I(modp) \\ Tg = O(modp) \end{cases}$$

όπου O ο μηδενικός πίνακας.

Δημόσιο κλειδί: Το δημόσιο κλειδί του NTRU αντιστοιχεί στην HNF βάση, του συνελικτικά κατά μέτρο δικτυώματος $L_q((T^*f, T^*g)^T)$ ορισμένου όμως από το ιδιωτικό κλειδί. Λόγω των δομών κατασκευής αυτών των δικτυωμάτων και τους περιορισμούς όσον αφορά το f, η HNF δημόσια βάση έχει την παρακάτω μορφή

$$H = \begin{bmatrix} I & O \\ T^*h & qI \end{bmatrix}$$

όπου $h = [T^*f]^{-1}g(modq)$ και μπορεί να αναπαρασταθεί μόνο από το διάνυσμα $h \in \mathbb{Z}_q^n$.

Κρυπτογράφηση

Ένα μήνυμα εισόδου κωδικοποιείται ως ένα διάνυσμα $m \in \{1, 0, -1\}^n$ με ακριβώς $d_f + 1$ θετικές εισόδους και d_f αρνητικές. Το διάνυσμα m είναι σε αλληλουχία (συγγραμμικό) με ένα τυχαία επιλεγμένο μικρό διάνυσμα σφάλματος $(-r, m) \in \{1, 0, -1\}^{2n}$. Μειώνοντας το διάνυσμα σφάλματος $(-r, m)$ κατά modulo της δημόσιας βάσης H παίρνουμε

$$\begin{bmatrix} -r \\ m \end{bmatrix} mod \begin{bmatrix} I & O \\ T^*h & qI \end{bmatrix} = \begin{bmatrix} 0 \\ (m + [T^*h]r) mod q \end{bmatrix}$$

Καθώς οι πρώτες n συντεταγμένες του διανύσματος είναι πάντα 0, μπορούμε να τις παραβλέψουμε, αφήνοντας μόνο, το $n-$διάστατο διάνυσμα $c = m + [T^*h]r mod q$ ως το κρυπτοκείμενο.

Αποκρυπτογράφηση

Το κρυπτοκείμενο c αποκρυπτογραφείται πολλαπλασιάζοντάς το με το μυστικό πίνακα $[T^*f] moduloq$, δίνοντας

$$[T^*f]c mod q = [T^*f]m + [T^*f][T^*h]r mod q = [T^*f]m + [T^*g]r mod q$$

όπου χρησιμοποιήσαμε τη ταυτότητα $[T^*f][T^*h] = [T^*([T^*f])h]$ που ισχύει για οποιαδήποτε διανύσματα f και h. Η διαδικασία αποκρυπτογράφησης στηρίζεται στο γεγονός ότι οι συντεταγμένες του διανύσματος

$$[T^*f]m + [T^*g]r$$

είναι όλες φραγμένες από $q/2$ σε απόλυτη τιμή, οπότε αυτός που αποκρυπτογραφεί μπορεί να λάβει ακριβώς τη τιμή $[T^*f]m + [T^*g]r$ για όλους τους ακέραιους (χωρίς μείωση κατά modulo$p$). Η διαδικασία ολοκληρώνεται μειώνοντας την $[T^*f]m + [T^*g]r$ κατά modulo$p$, ώστε να πάρουμε τελικά

$$[T^*f]m + [T^*g]r mod p = I \cdot m + O \cdot r = m$$

Τα προαναφερθέντα κρυπτοσύστηματα δυστυχώς είναι αρκετά αναποτελεσματικά. Όταν στηρίζουμε την ασφάλεια σε δικτυώματα n διάστασης, το μέγεθος του δημόσιου κλειδιού είναι της τάξης του $O(n^4)$ και κάθε κρυπτογραφημένο bit μετατρέπεται σε $\tilde{O}(n^2)$ bits. Οπότε στη πράξη αν χρειαζόμαστε η διάσταση n του δικτυώματος να είναι μερικές εκατοντάδες bits, το δημόσιο κλειδί είναι της τάξης μερικών εκατοντάδων gigabytes, το οποίο είναι μη-πρακτικό.

3.3 Πολυμεταβλητή Κρυπτογραφία Δημοσίου Κλειδιού (MPKCs)

Οι Diffie και Hellmann είχαν οραματιστεί ότι ένα κρυπτοσύστημα δημοσίου κλειδιού (public key cryptosystem, PKC) στηρίζεται στην ύπαρξη μιας κλάσης μονόδρομων συναρτήσεων που αποτελούν ένα είδος "κερκόπορτας" για το σύστημα (trapdoor). Αυτή η κλάση συναρτήσεων και η μαθηματική δομή θα καθορίσουν τα ζωτικά χαρακτηριστικά του κρυπτοσυστήματος $[108]$.

Η Πολυμεταβλητή κρυπτογραφία είναι η μελέτη των PKCs, όπου η μονόδρομη συνάρτηση παίρνει τη μορφή μιας πολυμεταβλητής τετραγωνικής πολυωνυμικής απεικόνισης σε ένα πεπερασμένο πεδίο. Το δημόσιο κλειδί δίνεται από ένα σύνολο τετραγωνικών πολυωνύμων της μορφής

$$P = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$$

όπου p_i τετραγωνικό μη-γραμμικό πολυώνυμο με τη παρακάτω μορφή

$$\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
\vdots \quad &= \quad \vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}$$

Οι συντελεστές και οι μεταβλητές του p_i ανήκουν στο $\mathbb{K}=\mathbb{F}_q$ πεδίο, με q στοιχεία. Το να ανιστρέψουμε μια τετραγωνική πολυμεταβλητή απεικόνιση είναι σαν να λύνουμε ένα σύνολο από τετραγωνικές εξισώσεις σε φραγμένο σώμα ή αλλιώς το εξής πρόβλημα:

Ορισμός 3.29. *(MQ-πρόβλημα) Να λυθεί το σύστημα*

$$P_1(x)=P_2(x)=\cdots=P_m(x)=0$$

όπου P_i με $1\leq i\leq q, m$ τετραγωνικά πολυώνυμα και $x=(x_1,\ldots,x_n)$. Όλες οι μεταβλητές και οι συντελεστές ανήκουν στο $\mathbb{K}=\mathbb{F}_q$, όπου είναι το σώμα με $q-$στοιχεία.

Το MQ-πρόβλημα θεωρείται ένα NP-πλήρες πρόβλημα και τα μαθηματικά πίσω από τη πολυμεταβλητή κρυπτογραφία ανήκουν σε ένα γενικότερο κλάδο που ονομάζουμε Αλγεβρική Γεωμετρία.

Βασική ιδέα και συμβολισμοί

Γενικά, η κατασκευή των MPKCs στηρίζεται στη κατασκευή απεικονίσεων της μορφής

$$F=T\circ G\circ S$$

όπου S,T αντιστρέψιμες ομοπαραλληλικές απεικονίσεις και G μια τετραγωνική απεικόνιση που δύναται να αντιστραφεί και F μια δημόσια τετραγωνική απεικόνιση (αργότερα το δημόσιο μας κλειδί). Την G απεικόνιση τη καλούμε κεντρική απεικόνιση και ουσιαστικά χαρακτηρίζει το εκάστοτε MPKC. Η ασφάλεια και η ταχύτητα αποκρυπτογράφησης επίσης, εξαρτώνται σε μεγάλο βαθμό από την κεντρική απεικόνιση G.

Πιο αναλυτικά, έστω $n,m\geq 1$ ακέραιοι, $\mathbb{K}$ ένα πεπερασμένο σώμα και $q=\#\mathbb{K}$. Το μυστικό κλειδί ενός MPKC είναι η τριάδα (S,G,T) όπου

$$\begin{aligned}
S &: \mathbb{K}^n \to \mathbb{K}^n \\
T &: \mathbb{K}^m \to \mathbb{K}^m \\
G &: \mathbb{K}^n \to \mathbb{K}^m
\end{aligned}$$

Το δημόσιο κλειδί F είναι η συνέλιξη αυτών των S, G, T με

$$F : \mathbb{K}^n \overset{S}{\mapsto} \mathbb{K}^n \overset{G}{\mapsto} \mathbb{K}^m \overset{T}{\mapsto} \mathbb{K}^m$$

- ◇ Για να επικυρώσουμε μια υπογραφή ή να κρυπτογραφήσουμε ένα μήνυμα $x \in \mathbb{K}^n$, υπολογίζουμε την απεικόνιση F και παίρνουμε το κρυπτοκείμενο $y = F(x)$.
- ◇ Για να υπογράψουμε ή να αποκωδικοποιήσουμε ένα κρυπτογραφημένο μήνυμα, πρέπει να βρούμε ένα $z \in \mathbb{K}^n$ τέτοιο ώστε $G(z) = T^{-1}(y)$. Τότε το απλό κείμενο είναι $x = S^{-1}(z)$.

Στη συνέχεια ακολουθούν κάποια χαρακτηριστικά μεγέθη όσον αφορά τα μεγέθη των μηνυμάτων, των υπογραφών, των κλειδιών αλλά και του αριθμού των πράξεων που απαιτούνται για τον υπολογισμό τους.

- Μέγεθος μηνύματος: m στοιχεία του $\mathbb{F}_q$.
- Μέγεθος κρυπτοκειμένου ή υπογραφής: n στοιχεία του $\mathbb{F}_q$.
- Μέγεθος δημοσίου κλειδιού: $m \cdot n \cdot (n+3)/2$, $\mathbb{F}_q$ στοιχεία
- Μέγεθος ιδιωτικού κλειδιού: $(n^2 + m^2 + [\#\text{παράμετροι του } Q])$, $\mathbb{F}_q$ στοιχεία.
- Χρονική πολυπλοκότητα της κρυφής κεντρικής απεικόνισης (Q): $(n^2 + m^2)$ $\mathbb{F}_q$ πολλαπλασιασμοί με επιπλέον το χρόνο που απαιτεί ο υπολογισμός της αντίστροφης απεικόνισης του Q.
- Χρονική πολυπλοκότητα της δημόσιας απεικόνισης: περίπου $m \cdot n^2$ $\mathbb{F}_q$ πολλαπλασιασμοί.
- Χρονική πολυπλοκότητα της παραγωγής κλειδιού: n^2 φορές το κόστος επίκλησης του P, περίπου μεταξύ $O(n^4) - O(n^5)$.

Συμπεραίνουμε λοιπόν κοιτώντας τα προηγούμενα μεγέθη, ότι τα $MPKCs$ έχουν ένα τεράστιο μειονέκτημα. Τα κλειδιά είναι πολύ μεγάλα σε μέγεθος, σε σχέση με τα παραδοσιακά συστήματα όπως το RSA ή των ελλειπτικών καμπυλών (ECC). Παρόλα αυτά, παρακάτω θα αναφέρουμε το κρυπτοσύστημα των Matsumoto-Imai που είναι από τα βασικότερα κρυπτοσυστήματα πολυμεταβλητής κρυπτογράφησης $[108]$.

3.3.1 Κρυπτοσύστημα Matsumoto-Imai

Έστω k ένα πεπερασμένο πεδίο με χαρακτηριστική 2 και πληθάριθμο q, και $g(x) \in k[x]$ ένα ανάγωγο(αμείωτο) πολυώνυμο βαθμού n. Ορίζουμε το πεδίο $K = \dfrac{k[x]}{g(x)}$, το οποίο είναι μια επέκταση n βαθμού του k.

Έστω $\phi : K \to k^n$ ο κλασσικός $k-$γραμμικός ισομορφισμός ανάμεσα στο K και το k^n, που δίνεται από

$$\phi(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = (a_0 + a_1 + \cdots + a_{n-1})$$

Το υποπεδίο k του K είναι ενσωματωμένο στο k^n ως

$$\phi(a) = (a, 0, \ldots, 0),\ \forall a \in K$$

Το ϕ είναι μια $k-$γραμμική απεικόνιση αν θεωρήσουμε το k ως υποπεδίο στο K.
Διαλέγουμε ένα θ τέτοιο ώστε $0 < \theta < n$ και

$$\text{ΜΚΔ}(g^\theta + 1, q^n - 1) = 1$$

και ορίζουμε την απεικόνιση $\bar{F}$ στο K

$$\hat{F}(X) = X^{1+q^\theta}$$

Οι συνθήκες του θ μας εξασφαλίζουν ότι το $\bar{F}$ είναι μια αντιστρέψιμη απεικόνιση, καθώς αν t ένας ακέραιος τέτοιο ώστε

$$t(1 + q^\theta) \equiv 1 mod(q^n - 1)$$

τότε

$$\hat{F}^{-1}(X) = X^t$$

Ορίζουμε F απεικόνιση στο k^n ως

$$F(x_1, \ldots, x_n) = \phi \circ \bar{F} \circ \phi^{-1}(x_1, \ldots, x_n) = (f_1, \ldots, f_n)$$

όπου $(f_1, \ldots, f_n) \in k[x_1, \ldots, x_n]$. Επίσης έστω L_1, L_2 δύο αντιστρέψιμοι affine μετασχηματισμοί στο k^n. Ορίζουμε την απεικόνιση στο k^n

$$\bar{F} = (x_1, \ldots, x_n) = L_1 \circ F \circ L_2 \circ (x_1, \ldots, x_n) = (\bar{f}, \ldots, \bar{f}_n)$$

όπου $\bar{f}, \ldots, \bar{f}_n\ \in k[x_1, \ldots, x_n]$.

Δημιουργία κλειδιών

Το δημόσιο κλειδί του MI περιέχει

- Το πεδίο k με τις ανάλογες ιδιότητες για τη πρόσθεση και το πολλαπλασιαμό.
- Τα n πολυώνυμα $\hat{f}_1, \ldots, \hat{f}_n \in k[x_1, \ldots, x_n]$.

Το ιδιωτικό κλειδί περιέχει τους δύο μετασχηματισμούς L_1, L_2. Η παράμετρος θ μπορεί να κρατηθεί μυστική, αν και δν είναι και απολύτως απαραίτητο.

Κρυπτογράφηση

Δοθέντος ενός μηνύματος $(x_1^{'}, \ldots, x_n^{'})$ παίρνουμε το κρυπτοκείμενο $y_1^{'}, \ldots, y_n^{'}$

$$y_i^{'} = \hat{f}_i(x_1^{'}, \ldots, x_n^{'}),\ \text{για}\ i = 1, \ldots, n$$

Αυτό μπορεί να γίνει από τον καθένα με γνώση του δημόσιου κλειδιού.

Αποκρυπτογράφηση

Αποκρυπτογραφούμε το κρυπτοκείμενο $y_1^{'}, \ldots, y_n^{'}$ υπολογίζοντας το

$$\begin{aligned}\hat{F}^{-1} &= L_2^{-1} \circ F^{-1} \circ L_1^{-1}(y_1^{'}, \ldots, y_n^{'}) \\ &= L_2^{-1} \circ \phi \circ F^{-1} \circ \phi^{-1} \circ L_1^{-1}(y_1^{'}, \ldots, y_n^{'})\end{aligned}$$

Πιο συγκεκριμένα στη πράξη, για να αποκρυπτογραφήσουμε το μήνυμα ακολουθούμε τα εξής βήματα, επειδή οι πράξεις με το $\hat{F}^{-1}$ είναι πολύ υψηλού βαθμού.

1. Υπολογίζουμε το $(z_1^{'}, \ldots, z_n^{'}) = L_1^{'}(y_1^{'}, \ldots, y_n^{'})$.
2. Έπειτα υπολογίζουμε το $(\bar{z}_1, \ldots, \bar{z}_n) = \phi \circ \bar{F}^{-1} \circ \phi^{-1}(z_1^{'}, \ldots, z_n^{'})$.
3. Τελικά υπολογίζουμε το $(x_1^{'}, \ldots, x_n^{'}) = L_2^{'}(\bar{z}_1, \ldots, \bar{z}_n)$.

Εάν το αντίστοιχο κρυπτοσύστημα είναι ασφαλές, τότε η αποκρυπτογράφηση μπορεί να εφαρμοστεί μόνο από αυτούς που έχουν πρόσβαση στο ιδιωτικό κλειδί.

Το δημόσιο κλειδί του κρυπτοσυστήματος MI είναι ένα σύνολο που αποτελείται από πολυώνυμα βαθμού δύο, $\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_n \ \in k[x_1, \ldots, x_n]$. Κάθε πολυώνυμο έχει $1 + n + \dfrac{n(n+1)}{2} = \dfrac{(n+1)(n+2)}{2}$ όρους, άρα το δημόσιο κλειδί είναι ένα σύνολο με $\dfrac{n(n+1)(n+2)}{2}$ συντελεστές στο k όταν $q > 2$. Αν το $q = 2$ το μέγεθος του κλειδιού θα είναι μικρότερο επειδή δεν θα υπάρχουν τετραγωνικοί όροι αφού $x_i^2 = x_i$.

Το 1988, οι Matsumoto-Imai πρότειναν οι αρχικές παράμετροι για το k να είναι το $GF(2^8)$ και το $n = 32$,παρόλα αυτά το δημόσιο κλειδί παραμένει αρκετά μεγάλο. Ακόμα και αν το μέγεθος του δημόσιου κλειδιού είναι μεγάλο σε σχέση με άλλα σχήματα όπως αυτό του RSA, το μεγαλύτερο πλεονέκτημα του MI κρυπτοσυστήματος είναι η υπολογιστική του αποτελεσματικότητα.

Αν διαλέξουμε το $q = |k|$ να είναι μικρό, τότε μπορούμε να αποθηκεύσουμε το πολλαπλασιαστικό πίνακα στη μνήμη στηριζόμενοι στο ότι τα μη-μηδενικά στοιχεία του k σχηματίζουν μια κυκλική πολλαπλασιαστική ομάδα. Αυτό κάνει τη μέθοδο αποκρυπτογράφησης πολύ πιο γρήγορη σε σύγκριση με σχήματα που λειτουργούν με μεγάλους πρώτους αριθμούς, όπως το RSA. Επίσης, αυτό το χαρακτηριστικό μπορούμε να το χρησιμοποιήσουμε και στη μέθοδο της κρυπτογράφησης, στον υπολογισμό του $\bar{F}^{-1}$.

Παρόλο που θεωρήθηκε ως υποψήφιος για την ασφάλεια της Γιαπωνέζικης κυβέρνησης το 1988, το κρυπτοσύστημα MI έσπασε το 1995 από τον Patarin και την αλγεβρική του επίθεση η οποία στηρίζεται στις γραμμικοποιημένες εξισώσεις.

Επίλογος

Η κβαντική κρυπτογραφία επιτρέπει πολλά περισσότερα από απλά μια κβαντική διαμοίραση κλειδιού. Τα κβαντικά κρυπτογραφικά πρωτόκολλα μπορούν να διαιρεθούν γενικά σε δύο κατηγορίες. Η πρώτη κατηγορία αφορά τη χρήση της κβαντικής επικοικωνίας με στόχο την εφαρμογή κλασικών διαδικασιών. Παράδειγμα αυτής της κατηγορίας είναι η διαμοίραση κλειδιού που αναλύσαμε στην παρούσα εργασία που στόχο έχει τη παραγωγή ενός κλασικού κλειδιού ανάμεσα σε δύο απομακρυσμένες οντότητες. Υπάρχει όμως η περίπτωση, οι δύο οντότητες που θέλουν να επικοινωνήσουν να μην εμπιστεύονται ο ένας τον άλλον, όποτε να έχουμε για παράδειγμα τον "ύποπτο" Bob ενάντια της "έντιμης Αλίκης" και το αντίστροφο.

Η δεύτερη κατηγορία, αφορά πραγματικές κβαντικές "εργασίες", για τις οποίες τουλάχιστον μια, η είσοδος ή η έξοδος είναι κβαντική. Ένα παράδειγμα, είναι όταν θέλουμε να μοιραστούμε κβαντικά ένα μυστικό (quantum secret sharing), όπου στόχος είναι η διανομή ενός qubit ανάμεσα σε πολλούς συμμετέχοντες με τέτοιο τρόπο ώστε να απαιτείται τουλάχιστον ένας συγκεκριμένος αριθμός εξ' αυτών να βρεθεί από κοντά ώστε να ξανακατασκευάσουν το μυστικό.

Τέλος, πολλές κρυπτογραφικές ασχολίες δεν ανήκουν σε καμία από τις δύο κατηγορίες. Ένα παράδειγμα, που αποτελεί κομμάτι της σύγχρονης κβαντικής έρευνας, είναι αυτό της μεταβιβαζόμενης κβαντικής υπολογιστικής (delegated quantum computation). Σε αυτή τη περίπτωση, μπορούμε να φανταστούμε έναν χρήστη ο οποίος έχει πρόσβαση σε έναν παντοδύναμο, αλλά απομακρυσμένο υπολογιστή, τη στιγμή που ο ίδιος έχει από ελάχιστες έως και καθόλου κβαντικές δυνατότητες. Ο στόχος του χρήστη είναι να "μεταβιβάσει" έναν σύνθετο κβαντικό υπολογισμό που τον ενδιαφέρει στον κβαντικό υπολογιστή, χωρίς να διαρεύσει καμία πληροφορία για τον υπολογισμό ή την είσοδο. Αυτό είναι ένα πολύ σημαντικό και ανοιχτό θέμα στον επιστημονικό χώρο της κβαντικής κρυπτογραφίας.

Βιβλιογραφία

(1) Christof Paar, Jan Pelzl *Understanding cryptography a textbook for students and practitioners*. Springer-Verlag Berlin Heidelberg (2009)

(2) Κ. Χαλατσης ,Lecture Notes. *«Εισαγωγή στην Κρυπτογραφία»*.

(3) Michael J Wiener. *Cryptanalysis of short rsa secret exponents. Information Theory*. IEEE Transactions on, 36(3):553–558, 1990

(4) Adi Shamir. *A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In Advances in Cryptology*. pages 279-288. Springer, 1983.

(5) R.L. Rivest, A. Shamir, and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM*. 21:120–126, 1978.

(6) Pascal Paillier. *Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the 17th international conference on Theory and application of cryptographic techniques*. EUROCRYPT'99,pages 223-238, Berlin, Heidelberg, 1999. Springer-Verlag.

(7) Rivest, Ronald L., and Burt Kaliski. *"RSA problem." Encyclopedia of cryptography and security (2011): 1065-1069.*

(8) Josh D. Cohen and Michael J. Fischer. *A robust and verifiable cryptographically secure election scheme (extended abstract).*. In FOCS,pages 372-382, 1985.

(9) Whitefield Diffie and Martin E. Hellman . *"Privacy and authentication: An introduction to cryptography." Proceedings of the IEEE 67.3 (1979): 397-427"*.

(10) Ivan Damgård and Mats Jurik. *A generalisation, a simplification and some applications of paillier's probabilistic public-key system.*. In Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography, PKC '01, pages 119-136, London, UK, UK, 2001. Springer-Verlag.

(11) W. Diffie and M. Hellman. *New directions in cryptography*. IEEE Trans. Inf. Theor., 22(6):644-654, November 1976.

(12) Taher El Gamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*. In CRYPTO, pages 10-18, 1984.

(13) Ralph Charles Merkle *"Secrecy, authentication, and public key systems." Ph. D. Thesis, Stanford University (1979)*.

(14) Journal of Computer Science Applications and Information Technology , *A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention*.

(15) Πτυχιακή Εργασία, Παπαδόπουλος Παύλος, *Κρυπτογραφία και το κρυπτοσύστημα Rabin*.

(16) Ευστάθιος Ζάχος, Αριστείδης Παγουρτζής, Παναγιώτης Γροντάς, *Υπολογιστική Κρυπτογραφία*.

(17) Leon van Dommelen, *Fundamental Quantum Mechanics for Engineers 5/5/07 Version 3.1 beta 3*.

(18) David Morin, *"Introduction to quantum mechanics." (2008)*.

(19) Atsushi Yamada, *The Quantum Revolution: Security Implications and Considerations*.

(20) O. Sami Saydjari, *Quantum Cryptography*.

(21) cloudsecurityalliance.org, *What is Quantum Key Distribution?*.

(22) Henning Weier, *"Experimental quantum cryptography." Diploma Dissertation, Technical University of Munich (2003).*

(23) Petra Pajic, *"Quantum Cryptography." Bachelor Thesis for the degree of Bachelor of Science at the University of Vienna (2013): 6-10.*

(24) J. Aditya, P. Shankar Rao, *"Quantum Cryptography." Proceedings of computer society of India (2005)*.

(25) Sheila Cobourne, *"Quantum Key Distribution Protocols and Applications." Surrey TW20 0EX, England (2011)*.

(26) Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, *"Quantum cryptography." Reviews of modern physics 74.1 (2002): 145.*

(27) Ashley Montanaro, *"Quantum computational supremacy." Nature 549.7671 (2017): 203*.

(28) Edward R. Floyd, *"EPR-Bohr and Quantum Trajectories: Entaglement and Nonlocality." arXiv preprint arXiv:1001.4575 (2010)*.

(29) Thomas Baigneres, *Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol. No. STUDENT. 2003*.

(30) Hitesh Singh, D.L. Gupta , A.K Singh, *"Quantum key distribution protocols: a review." Journal of Computer Engineering 16.2 (2014): 1-9*.

(31) Guihua Zeng, *"A simple eavesdropping strategy of BB84 protocol." arXiv preprint quant-ph/9812064 (1998)*.

(32) Andrew M. Steane, *"A tutorial on quantum error correction." PROCEEDINGS-INTERNATIONAL SCHOOL OF PHYSICS ENRICO FERMI. Vol. 162. IOS Press; Ohmsha; 1999, 2007.*

(33) Dieter van Melkebeek, *Lecture 23: Cryptographic Protocols*.

(34) Jungsang Kim, *Introduction to Quantum Cryptography*.

(35) Peter W. Shor and John Preskill, *"Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85.2 (2000): 441*.

(36) Emma Strubell, *"An introduction to quantum algorithms." COS498 Chawathe Spring 13 (2011): 19.*

(37) Dieter van Melkebeek, *Cryptographic Protocols*.

(38) Impagliazzo, Russell; Levin, Leonid A.; Luby, Michael *"Pseudo-random Generation from one-way functions", in Johnson, David S. (ed.), Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA, ACM, pp. 12{24.*

(39) M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information. Cambridge University Press, 2000 (cited on page 2).*

(40) B. Schumacher and M. Westmoreland. *Quantum Processes Systems, and Information. Cambridge University Press, 2010 (cited on page 2).*

(41) A. Ambainis et al. *"Private quantum channels". In: Proceedings of FOCS. arXiv:quant-ph/0003101. 2000 (cited on page 20)*.

(42) P. O. Boykin and V. Roychowdhury. *"Optimal encryption of quantum bits". quant- ph/0003059. 2000 (cited on page 20)*.

(43) D.G. Kelly. *Introduction to Probability. Macmillan Publishing Company, 1994. ISBN : 9780023631450 (cited on page 3).*

(44) S.M. Ross. *A First Course in Probability. Pearson Prentice Hall, 2010. ISBN : 9780136033134 (cited on page 3).*

(45) Claude E Shannon. *"Communication theory of secrecy systems". In: Bell system technical journal 28.4 (1949), pages 656-715 (cited on page 17).*

(46) John S Bell. *On the Einstein Podolsky Rosen Paradox. 1964 (cited on page 9).*

(47) Nicolas Brunner et al. *"Bell nonlocality". In: Reviews of Modern Physics 86.2 (2014), page 419 (cited on page 9).*

(48) Bas Hensen et al. *"Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: Nature 526.7575 (2015), pages 682-686 (cited on page 12).*

(49) Ben Toner. \Monogamy of non-local quantum correlations". In: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences. Volume 465. 2101. The Royal Society. 2009, pages 59-69 (cited on page 14).

(50) Christopher A Fuchs and Jeroen Van De Graaf. "Cryptographic distinguishability measures for quantum-mechanical states". In: IEEE Transactions on Information Theory 45.4 (1999), pages 1216-1227 (cited on page 5).

(51) Carl W. Helstrom. Quantum detection and estimation theory / Carl W. Helstrom. English. Academic Press New York, 1976, ix, 309 p. : ISBN : 0123400503 (cited on page 3).

(52) Robert Konig, Renato Renner, and Christian Schaffner. "The operational meaning of min-and max-entropy". In: IEEE Transactions on Information theory 55.9 (2009), pages 4337{4347 (cited on page 9).

(53) Renato Renner. "Security of quantum key distribution". In: International Journal of Quantum Information 6.01 (2008), pages 1-127 (cited on page 7).

(54) M. Tomamichel et al. "A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography". In: New Journal of Physics 15 (2013). EUROCRYPT 2013, arXiv:1210.4359, page 103002 (cited on pages 16, 17).

(55) Jaikumar Radhakrishnan and Amnon Ta-Shma. \Bounds for dispersers, extractors, and depth-two superconcentrators". In: SIAM Journal on Discrete Mathematics 13.1 (2000), pages 2-24 (cited on page 8).

(56) Gilles Brassard and Louis Salvail. "Secret-key reconciliation by public discussion". In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer.1993, pages 410-423 (cited on page 10).

(57) R. Renner. "Security of Quantum Key Distribution". PhD thesis. ETH Zurich, 2005 (cited on page 5).

(58) David Slepian and Jack Wolf. Noiseless coding of correlated information sources". In: IEEE Transactions on information Theory 19.4 (1973), pages 471-480 (cited on page 9).

(59) Marco Tomamichel et al. "Fundamental finite key limits for information reconciliation in quantum key distribution". In: 2014 IEEE International Symposium on Information Theory. IEEE. 2014, pages 1469-1473 (cited on page 9).

(60) C. H. Bennett and G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984), pages 175-179 (cited on page 3).

(61) Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: Physical review letters 67.6 (1991), page 661 (cited on page 6).

(62) Corsin Pfister et al. *"Sifting attacks in finite-size quantum key distribution". In: New Journal of Physics 18.5 (2016), page 053001 (cited on page 5).*

(63) Rafael Pass and Abhi Shelat. *A Course in Cryptography. Lecture notes available at http://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf. 2010 (cited on pages 10, 12).*

(64) Marco Tomamichel and Anthony Leverrier. *"A rigorous and complete proof of finite key security of quantum key distribution". In: arXiv preprint arXiv:1506.08458 (2015) (cited on page 9).*

(65) Stephen Wiesner. *"Conjugate Coding". In: SIGACT News 15 (1983), pages 78{88 (cited on page 3).*

(66) CaltechDelftX: QuCryptox *Course: Quantum Cryptography.*

(67) Aspect, Alain, Jean Dalibard, and Gérard Roger. *"Experimental test of Bell's inequalities using time-varying analyzers." Physical review letters 49.25 (1982): 1804.*

(68) Schrodinger, E., 1935, *Naturwissenschaften23, 807.*

(69) Καραφυλλίδης, Ιωάννης. *"Η Κβαντική Διεπλοκή και ο Κβαντικός Μετασχηματισμός Fourier." (2015).*

(70) Lomonaco, Samuel J. *"A Lecture on Shor's Quantum Factoring Algorithm." (2000).*

(71) Jochemsz, Ellen. *"Goppa Codes & the McEliece Cryptosystem." Vrije Universiteit Amsterdam (2002): 63.*

(72) Nicolas Sendrier, *"Code-based cryptography: State of the art and perspectives." IEEE Security & Privacy 15.4 (2017): 44-50.*

(73) Tanja Lange, *Code-Based Cryptography.*

(74) Löndahl, Carl, *Some Notes on Code-Based Cryptography. Department of Electrical and Information Technology, Lund University, 2015.*

(75) Federico Bergami, *"Lattice-Based Cryptography."*

(76) Daniele Micciancio, *Basic Algorithms.*

(77) Daniele Micciancio, Oded Regev, *"Lattice-based cryptography." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2006.*

(78) Dong Pyo Chi, Jeong Woon Choi, Jeong San Kim, Taewan Kim, *"Lattice based cryptography for beginners." IACR Cryptology ePrint Archive 2015 (2015): 938.*

(79) Daniele Micciancio, *Lattice Problems.*

(80) Daniele Micciancio, *Minkowski's theorem.*

(81) Michael Rose, *"Lattice-based cryptography: a practical implementation." (2011)*

(82) Nigel Smart, *FHE-MPC Notes*.

(83) Χριστίνα Ζερβοπούλου, *"ΚΡΥΠΤΟΓΡΑΦΙΑ ΒΑΣΙΣΜΕΝΗ ΣΕ ΔΙΚΤΥΩΜΑΤΑ ΑΚΕΡΑΙΩΝ ΘΕΩΡΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ"*.

(84) Δημήτριος Γ. Παπαχρηστούδης, *"ΑΝΑΓΩΓΗ ΒΑΣΕΩΝ ΔΙΚΤΥΩΜΑΤΩΝ"*.

(85) Μαρία Ι. Φουτζοπούλου, *"ΚΡΥΠΤΑΝΑΛΥΣΗ ΜΕ LATTICES"*.

(86) Abderrahmane Nitaj, *"The Mathematics of the NTRU Public Key Cryptosystem."*

(87) Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. *"NTRU: A ring-based public key cryptosystem." International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 1998.*

(88) Ron Steinfeld, *"NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings." Algebraic Curves and Finite Fields: Cryptography and Other Applications 16 (2014): 179*.

(89) JINTAI DING, DIETER SCHMIDT, *"Multivariable Public Key Cryptosystems." Contemporary Mathematics 419 (2006): 79*.

(90) Ming-Shing Chen, Wen-Ding Li, Bo-Yuan Peng, BoYin Yang, Chen-Mou Cheng, *"Implementing 128-bit secure mpkc signatures." IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 101.3 (2018): 553-569.*

(91) Yasufumi Hashimoto, *"Multivariate public key cryptosystems." Mathematical Modelling for Next-Generation Cryptography. Springer, Singapore, 2018. 17-42*.

(92) ELWYN R. BERLEKAMP, *"Goppa codes." IEEE Transactions on Information Theory 19.5 (1973): 590-592*.

(93) FERNANDO TORRES, *"Notes on Goppa codes." (2000)*.

(94) Key One Chung, *"Goppa Codes" (2004)*.

(95) Ashley Valentijn, *"Goppa Codes and Their Use in the McEliece Cryptosystems." (2015)*.

(96) Ellen Jochemsz, *"Goppa Codes & the McEliece Cryptosystem." Vrije Universiteit Amsterdam (2002): 63*.

(97) Andreas V. Meier, *"The elgamal cryptosystem." (2005)*.

(98) Thomas Risse, *"Generating Goppa Codes." Int. Conf. on Information Technologies. 2013.*

(99) Ειρήνη Χρόνη, *Ο Αλγόριθμος Κρυπτογράφησης NTRU*.

(100) Γεώργιος Α. Ζηρδέλης, *Lattices and Cryptography*.

(101) Valerie Gauthier Umana, *"Post-quantum cryptography." (2011)*.

(102) Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, *"The impact of quantum computing on present cryptography." arXiv preprint arXiv:1804.00200 (2018)*.

(103) Mehran Mozaffari-Kermani, *"Reliable hash trees for post-quantum stateless cryptographic hash-based signatures." 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). IEEE, 2015*.

(104) Katz & Lindell, *Introduction to modern cryptography. Chapman and Hall/CRC, 2014*.

(105) Aleksei Vambol, Olexandr Potii, Vyacheslav Kharchenko, Nikolaos Bardis, *McEliece and Niederreiter Cryptosystems Analysis in the Context of Post-Quantum Network Security. In 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI) (pp. 134-137). IEEE*

(106) Bardis, Nikolaos G., Athanasios Drigas, and Oleksandr P. Markovskyi. *"Performance increase of error control operation on data transmission." 2009 3rd International Conference on New Technologies, Mobility and Security. IEEE, 2009*.

(107) Micciancio, Daniele. *"Lattice-based cryptography." Encyclopedia of Cryptography and Security (2011): 713-715*.

(108) Ding, Jintai, Jason E. Gower, and Dieter S. Schmidt. *Multivariate public key cryptosystems. Vol. 25. Springer Science & Business Media, 2006.*