

Δημοκρίτειο Πανεπιστήμιο Θράκης
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών
Υπολογιστών



Παραγωγή και μετάδοση κβαντικών κλειδιών

Διπλωματική εργασία

Στόκας Μιλτιάδης

A.E.M: 57716

Επιβλέπων Καθηγητής: Ιωάννης Καραφυλλίδης

Περιεχόμενα

Περίληψη	4
Κεφάλαιο 1°	4
1. Κβαντικοί υπολογιστές	4
1.1 Εισαγωγή στους κβαντικούς υπολογιστές.....	4
1.2 Quantum bit (qubits)	6
1.3 Κβαντικός καταχωριτής	7
1.4 Κβαντικές Πύλες.....	8
1.5 Αδυναμία αντιγραφής κατάστασης ενός qubit	16
Κεφάλαιο 2°	19
2.1Κβαντικοί αλγόριθμοι	19
2.Αλγόριθμος του Grover.....	19
Κβαντικός αλγόριθμος του Shor	22
2.2 Κβαντική κρυπτογραφία	26
2.1 Εισαγωγή	26
2.2 Κβαντική διεμπλοκή.....	27
2.3 Κβαντική τηλεμεταφορά	30
2.4 Quantum Repeaters.....	33
2.4.1 Πρωτόκολλο.....	33
2.4.2 Δημιουργία κόμβων κβαντικών επαναληπτών και οι ατέλειες τους	34
2.4.3 Πλάνο δημιουργίας	35
Κεφάλαιο 3°	38
3.1Παραγωγή και μετάδοση κβαντικών κλειδιών	38
Εισαγωγή.....	38
3.2 Πρωτόκολλο BB84	40
Λειτουργία	40
Κβαντικό Κύκλωμα	42
3.3 Κώδικας BB84	44
3.3.0.Εισαγωγή	44
3.3.1.Πλευρά της Alice.....	45
3.3.2.Πλευρά του Bob.....	48
3.3.3.Πλευρά της Eve.....	50
3.3.4.Παραγωγή κβαντικών κλειδιών.....	51
3.3.5.Έλεγχος κλειδιού.....	52
Κεφάλαιο 4°	52
4.1.Πρωτόκολλο E91.....	52

Εισαγωγή.....	52
CHSH ανισότητα	53
Λειτουργία πρωτοκόλλου E91	55
Θόρυβος στο πρωτόκολλο E91	56
4.2 Κώδικας πρωτοκόλλου E91	58
Εισαγωγή συναρτήσεων	58
Δημιουργία διεμπλοκής.....	59
Δημιουργία των βάσεων Alice&Bob.....	59
Έλεγχος βάσεων και δημιουργία κλειδιού	60
Υπολογισμός CHSH	62
Διάγραμμα CHSH	64
Συμπεράσματα.....	65
Προοπτικές.....	65
Βιβλιογραφία	66

Περίληψη

Στόχος αυτής της διπλωματικής εργασίας είναι μια σύντομη εισαγωγή στο πεδίο των κβαντικών υπολογιστών και της κβαντικής κρυπτογραφίας. Γίνεται μια προσπάθεια ομαλής εισαγωγής και παρουσίασης των έννοιων του πεδίου ώστε να μπορέσουν ακόμη και αναγνώστες οι οποίοι δεν έχουν ιδιαίτερη γνώση στο αντικείμενο να το κατανοήσουν. Παρουσιάζονται οι πιο πρόσφατες εξελίξεις που υπάρχουν στην σύνθεση αποτελεσματικών και βέλτιστων κβαντικών αλγορίθμων κρυπτογραφίας καθώς και βήματα που θα πρέπει να ακολουθηθούν μελλοντικά για την βελτιστοποίηση τους. Αρχικά, παρουσιάζονται βασικά δοκιμά στοιχεία ενός κβαντικού υπολογιστή καθώς και βασικές λειτουργίες που μπορούν αυτοί να επιτελέσουν. Στην συνέχεια γίνεται αναφορά σε απαραίτητες έννοιες και λειτουργίες που σχετίζονται με την κβαντική κρυπτογραφία ώστε να μπορέσει ο αναγνώστης να μεταβεί ομαλά στα επόμενα κεφάλαια που αναφέρονται σε κβαντικά πρωτόκολλα κρυπτογράφησης.

Κεφάλαιο 1^ο

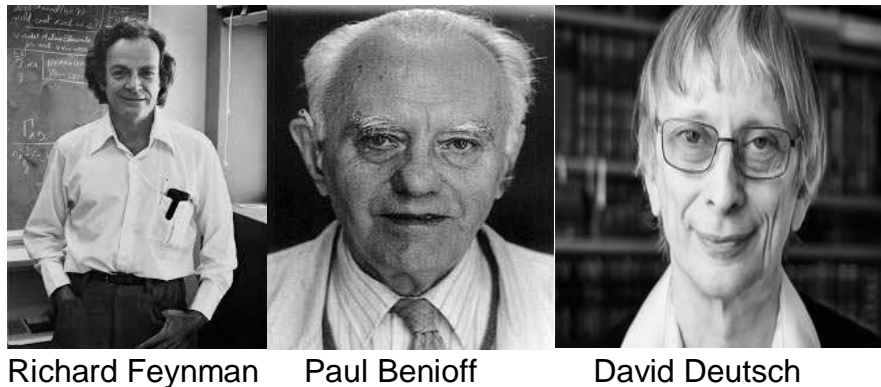
1. Κβαντικοί υπολογιστές

1.1 Εισαγωγή στους κβαντικούς υπολογιστές

Η δημιουργία υπολογιστών που να στηρίζονται στις αρχές της κβαντομηχανικής παρουσιάστηκε σαν ιδέα από τους Richard Feynman, David Deutsch και Paul Benioff στις αρχές της δεκαετίας του 80'. Οι τρεις φυσικοί

παρατήρησαν πως οι κλασσικοί υπολογιστές παρουσίαζαν διάφορες ατέλειες όπως μνήμη και ταχύτητα και αργά ή γρήγορα θα οδηγούνταν στην τεχνολογική τους τελμάτωση. Από το διάγραμμα Moore μπόρεσαν να συμπεράνουν ότι τα τσιπ πυρητίου που χρησιμοποιούνται για την υλοποίηση ενός κλασσικού υπολογιστή θα συμπυκνωθούν τόσο ώστε κάποια στιγμή τα μεμονωμένα στοιχεία δεν θα ήταν μεγαλύτερα από μερικά άτομα.

Λαμβάνοντας αυτά υπόψη ο Feynman προσπάθησε να δώσει μια πρωτοποριακή λύση δημιουργώντας ένα πρότυπο το οποίο έδειχνε το τρόπο που θα μπορούσε ένα κβαντικό σύστημα να χρησιμοποιηθεί ώστε να κάνει υπολογισμούς. Σύμφωνα με το πρότυπό αυτό θα δινόταν η δυνατότητα να πραγματοποιηθούν πειράματα στην κβαντική φυσική μέσα από έναν κβαντικό υπολογιστή.



Εικόνα 1-1 Richard Feynman, Paul Benioff και David Deutsch

Το ερώτημα που γεννάται είναι πως μπορεί ένας τέτοιος κβαντικός υπολογιστής να δημιουργηθεί. Όπως γνωρίζουμε, στους κλασσικούς υπολογιστές η πληροφορία είναι κωδικοποιημένη σε δυαδική μορφή δηλαδή σε μια σειρά από bits τα οποία λαμβάνουν τις τιμές 0 ή 1 και με την χρήση των λογικών πυλών μετασχηματίζονται ώστε να παραχθεί το επιθυμητό αποτέλεσμα. Παρόμοια σε ένα κβαντικό υπολογιστή τα αντίστοιχα qubits (quantum bits) μετασχηματίζονται μέσω των κβαντικών πυλών οι οποίες μπορούν να υλοποιήσουν μετασχηματισμούς σε ένα ή σε ζευγάρι qubits. Ανάλογα με την σειρά που οι κβαντικές πύλες θα τοποθετηθούν οι λειτουργίες που μπορεί ο κβαντικός υπολογιστής να υλοποιήσει είναι αναρίθμητες.

Γενικότερα στην τεχνολογία και όχι μόνο όταν κάτι έχει παγιωθεί είναι πολύ δύσκολο να το αντικαταστήσεις με κάτι διαφορετικό. Τι είναι όμως το οποίο μπορούν να μας παρέχουν οι κβαντικοί υπολογιστές ώστε να μπορέσουν κάποια στιγμή στο μέλλον τους κλασσικούς. Ο πρώτος από τους δυο βασικότερους λόγους είναι ότι οι κβαντικοί υπολογιστές μπορούν να επιλύσουν NP προβλήματα σε μη πολυωνυμικό χρόνο κάτι το οποίο οι κλασσικοί υπολογιστές

δεν μπορούν. Ο δεύτερος και αυτός που θα αναλυθεί σε αυτή την διπλωματική είναι η δυνατότητες που παρέχει στην κρυπτογράφηση. Με την χρήση κβαντικών υπολογιστών μπορείς να παρέχεις ένα πλήρως ασφαλές κλειδί μεταξύ δυο χρηστών χωρίς να μπορέσει κάποιος τρίτος να επεμβεί στην επικοινωνία χωρίς αυτός να γίνει αντιληπτός από το σύστημα.

1.2 Quantum bit (qubits)

Αντίστοιχα με τους κλασσικούς υπολογιστές οι οποίοι έχουν ως μονάδα πληροφορίας το bit το οποίο λαμβάνει τις δυαδικές τιμές 0 ή 1 έτσι και οι κβαντικοί υπολογιστές έχουν τα κβαντικό bit ή αλλιώς qubit. Η διαφορά μεταξύ των δυο είναι ότι το qubit εκτός από τις καταστάσεις 0, 1 μπορεί να βρεθεί και σε οποιαδήποτε υπέρθεση μεταξύ των δυο αυτών καταστάσεων. Πιο συγκεκριμένα, το qubit όταν βρίσκεται σε υπέρθεση καταστάσεων έχει κάποιες πιθανότητες να βρίσκεται στην τιμή 0 και κάποιες στην τιμή 1. Όπως είναι λογικό το άθροισμα των τετραγώνων των δυο αυτών πιθανοτήτων θα πρέπει να μας δίνει 1.

Οι καταστάσεις των qubit συμβολίζονται με $|0\rangle$ και $|1\rangle$ και αναπαρίστανται από τους πίνακες:

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

Και η υπέρθεση καταστάσεων που μπορεί να λάβει ένα qubit είναι:

$$|q\rangle \geq a|0\rangle + b|1\rangle, \text{ όπου } |a|^2 + |b|^2 = 1$$

Οι βασικές καταστάσεις ενός qubit είναι ορθογώνιες μεταξύ τους:

$$\langle 0|0\rangle = 1 \quad \langle 0|1\rangle = 0$$

$$\langle 1|0\rangle = 0 \quad \langle 1|1\rangle = 1$$

Το $|q\rangle$ συμβολίζει το διάνυσμα κατάστασης και είναι ένα δισδιάστατο διάνυσμα στον χώρο Hilbert. Ακόμη οι μιγαδικές μεταβλητές a , b είναι τα πλάτη πιθανότητας των οποίων το άθροισμα θα πρέπει να μας δίνει πάντα 1.

1.3 Κβαντικός καταχωρητής

Σε έναν κλασικό υπολογιστή ο καταχωρητής αποτελείται από ένα σύνολο bits. Ανάλογα με την τιμή που έχουν τα bit που περιέχει προκύπτει και ο αντίστοιχος αριθμός που είναι αποθηκευμένος μέσα σε αυτόν. Για παράδειγμα σε ένα κλασικό καταχωρητή των δυο bit μπορεί να είναι αποθηκευμένοι μια από τις τιμές 00, 01, 10, 11. Από την άλλη, οι κβαντικοί καταχωρητές αποτελούνται από ένα σύνολο από διατεταγμένα σε σειρά qubit. Πιο αναλυτικά, όταν σε έναν κβαντικό καταχωρητή είναι αποθηκευμένα 2 qubit τα οποία βρίσκονται σε υπέρθεση, αυτά μπορούν να αποδώσουν τέσσερις τιμές καθώς κάθε qubit έχει πιθανότητες να πάρει τις τιμές και 0 και 1. Η κατάσταση ενός κβαντικού καταχωρητή των 2 qubits γράφεται ως εξής:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$$

Ο συμβολισμός \otimes αναπαριστά το τανυστικό γινόμενο. Το τανυστικό γινόμενο είναι μια πράξη που γίνεται μεταξύ δυο πινάκων. Έστω λοιπόν ότι $A = \begin{bmatrix} a \\ b \end{bmatrix}$ και $B = \begin{bmatrix} c \\ d \end{bmatrix}$ τότε:

$$A \otimes B = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a * c \\ a * d \\ b * c \\ b * d \end{bmatrix}$$

Δηλαδή εάν οι καταστάσεις των δυο προηγούμενων qubit δίνονται από:

$$|\psi_1\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

Και

$$|\psi_2\rangle = c|0\rangle + d|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$$

Τότε:

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= (a*c)|00\rangle + (a*d)|01\rangle + (b*c)|10\rangle + (b*d)|11\rangle \end{aligned}$$

$$= c_1|00\rangle + c_2|01\rangle + c_3|10\rangle + c_4|11\rangle$$

Οπότε ο $|\psi\rangle$ έχει πλήθος στοιχείων όσο είναι το άθροισμα του πλήθους των στοιχείων του A και του B

1.4 Κβαντικές Πύλες

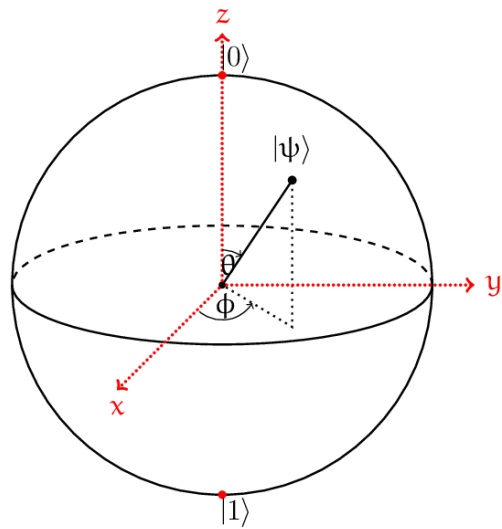
1.4.0 Εισαγωγή στις κβαντικές πύλες

Όπως γνωρίζουμε στους κλασικούς υπολογιστές η πληροφορία μεταφέρεται μέσω των αγωγών υπό μορφή ρεύματος ή τάσης από πύλη σε πύλη. Με την σειρά τους οι πύλες επεξεργάζονται αυτή την πληροφορία και ανάλογα με το τι είδος πύλης είναι (δηλαδή τι λογικό πίνακα έχει) βγάζει και το κατάλληλο αποτέλεσμα. Η κλασικές πύλες κυρίως κατασκευάζονται από πυρίτιο και συνθέτονται από διατάξεις τρανζίστορς, τα οποία ονομάζονται MOSFET.

Από την άλλη, στους κβαντικούς υπολογιστές οι πύλες αποτελούν δράσεις (τους λεγόμενους τελεστές) οι οποίες ασκούνται στα qubits ή στους καταχωρητές και δεν είναι φυσικά συστήματα τα οποία δέχονται και μετατρέπουν την πληροφορία. Η πληροφορία στους κβαντικού υπολογιστές μεταφέρεται μέσω των qubit και οι πύλες λειτουργούν ως φίλτρα μέσω των οποίων διέρχεται το qubit και μεταβάλλεται η πληροφορία του ανάλογα με το είδος της πύλης.

Μια αρκετά χρήσιμη και ενδιαφέρουσα ιδιότητα που παρουσιάζουν οι κβαντικοί υπολογιστές είναι η αντιστρεψιμότητα. Δηλαδή, εάν χρησιμοποιήσουμε πύλες ώστε να τροποποιήσουμε την πληροφορία ενός qubit ή ενός καταχωρητή τότε μπορούμε να επιφέρουμε την αρχική κατάσταση του qubit δρώντας με τις ίδιες πύλες αλλά αντίστροφα (δηλαδή από την τελευταία έως την πρώτη). Σε αυτή την ιδιότητα στηρίζεται και το παιχνίδι του “κβαντικό κέρμα” που συναντάται στην βιβλιογραφία των κβαντικών υπολογιστών.

Επειδή τα πλάτη πιθανότητας ενός qubit είναι συνήθως μιγαδικοί αριθμοί χρησιμοποιείται η αποκαλούμενη σφαίρα Bloch ώστε να αναπαραστηθούν τα χαρακτηριστικά του. Στην σφαίρα Bloch το διάνυσμα $|\psi\rangle$ έχει την αρχή του στο κέντρο της σφαίρας και καταλήγει στην επιφάνεια της σφαίρας η οποία έχει ακτίνα ίση με 1. Ακόμη για να οριστούν οι συντεταγμένες μέσα στον τρισδιάστατο χώρο χρησιμοποιούνται δυο γωνίες οι ϕ , θ όπως φαίνεται και στο παρακάτω σχήμα. Αυτό που κάνουν ουσιαστικά οι κβαντικές πύλες είναι να μεταβάλλουν τις γωνίες ϕ, θ ώστε να μετατοπιστεί το διάνυσμα $|\psi\rangle$. Όπως είναι εύκολα αντιληπτό οι θέσεις που μπορεί να πάρει το διάνυσμα $|\psi\rangle$ είναι άπειρες όπως και αντίστοιχα οι πύλες.



Σχήμα 1-1 Διάνυσμα $|\psi\rangle$ στην σφαίρα Bloch

Παρόλο που υπάρχουν άπειρες κβαντικές πύλες που μπορούν να κατασκευαστούν οι πιο συχνά χρησιμοποιούμενες είναι αυτές που θα αναφερθούν παρακάτω.

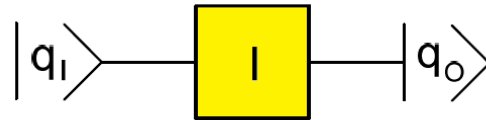
1.4.1 Κβαντική πύλη αδρανείας

Η πύλη αδρανείας ουσιαστικά είναι ένας μοναδιαίος πίνακας $n \times n$ ο οποίος συμβολίζεται με το γράμμα I και ο τελεστής που τον περιγράφει ονομάζεται τελεστής αδρανείας. Όπως προδίδει το όνομα της η πύλη αυτή δεν επιφέρει καμία αλλαγή στην κατάσταση του qubit. Ο πίνακας που περιγράφει τον τελεστή της αντίστοιχης πύλης είναι:

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

Όπως αναφέρθηκε και παραπάνω η πύλη αδράνειας αφήνει αμετάβλητη την κατάσταση του qubit

$$I |q\rangle = |q\rangle$$



Εικόνα 1-2 Κβαντική πύλη αδράνειας

$ q_I\rangle$	$ q_O\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$
$ q\rangle$	$ q\rangle$

Εικόνα 1-3 Πίνακας δράσεων της πύλης αδράνειας

Γίνεται αντιληπτό λοιπόν ότι στους κβαντικούς υπολογιστές ακόμα και η δράση “δεν κάνω τίποτα” έχει σημασία. Γιαυτό και όπως φαίνεται στον παραπάνω πίνακα ο συμβολισμός της εισόδου είναι διαφορετικός από αυτόν της εξόδου καθώς η πύλη I δρά πάνω στο qubit.

1.4.2 Κβαντική πύλη μετατόπισης φάσης

Όπως αναφέρει και το ονομά της η κβαντική πύλη μετατόπισης φάσης μετατοπίζει την φάση του qubit. Ο συμβολισμός που έχει δωθεί για αυτή την πύλη είναι το Φ και ο αντίστοιχος πίνακας του τελεστή της είναι:

$$\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Στην συνέχεια περιγραφεί αναλυτικά η επίδραση που έχει η πύλη Φ σε ένα qubit $|\psi\rangle$:

$$\text{Έστω } |\psi_1\rangle = a|0\rangle + b|1\rangle = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

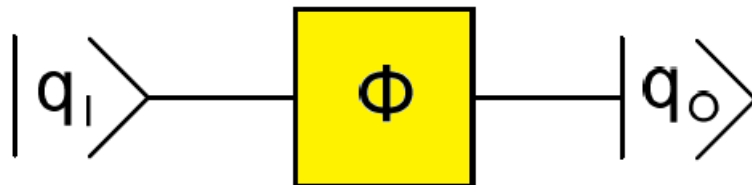
Εάν επέμβουμε στο qubit χρησιμοποιώντας την πύλη Φ , τότε η κατάσταση του qubit αλλάζει με τον εξής τρόπο:

$$|\psi_0\rangle = \Phi|\psi_1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ be^{i\varphi} \end{bmatrix}$$

Συνεπώς η νέα κατάσταση του qubit θα είναι:

$$|\psi_0\rangle = a|0\rangle + be^{i\varphi}|1\rangle$$

Κατά αυτόν τον τρόπο η πύλη έχει την δυνατότητα να αλλάζει μόνο την γωνία φάσης του qubit.



Εικόνα 1-4 Σύμβολο της κβαντικής πύλης μετατόπισης φάσης, Φ

$ q_i\rangle$	$ q_o\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$e^{i\varphi} 1\rangle$
$a 0\rangle + b 1\rangle$	$a 0\rangle + e^{i\varphi}b 1\rangle$

Εικόνα 1-5 Δράση της κβαντικής πύλης μετατόπισης φάσης στις καταστάσεις ενός qubit

Στην πρώτη στήλη του παραπάνω πίνακα φαίνονται οι καταστάσεις που μπορεί να έχει το qubit πριν την επέμβαση της πύλης H και στην δεύτερη στήλη πως μετατρέπονται αυτές αφού επέμβει η πύλη στο qubit.

1.4.3 Κβαντική πύλη Hadamard

Η πύλη Hadamard είναι μια από τις βασικότερες κβαντικές πύλες καθώς θέτει σε κατάσταση υπέρθεσης το qubit. Περιγράφεται από τον τελεστή H και ο πίνακας που αντιστοιχεί σε αυτή την πύλη είναι:

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

Σε αυτή την πύλη θα πρέπει να δειχθούν ξεχωριστά οι περιπτώσεις όπου το qubit έχει την τιμή 0 ή 1 καθώς τα αποτελέσματα που θα δώσει αυτή η πύλη όταν επέμβει πάνω στο qubit θα είναι διαφορετικά.

Αρχικά θα παρουσιαστεί η περίπτωση όπου το qubit θα βρίσκεται στην κατάσταση $|0\rangle$, Τότε:

$$H|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Έπειτα θα παρουσιαστεί η περίπτωση όπου το qubit θα βρίσκεται στην κατάσταση $|1\rangle$, Τότε:

$$H|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Παρόλο που οι δυο εξισώσεις είναι λίγο διαφορετικές το τελικό αποτέλεσμα και των δυο είναι το ίδιο. Δηλαδή και στις δυο περιπτώσεις το qubit έχει 50% πιθανότητες να βρίσκεται στην βασική κατάσταση 0 και 50% πιθανότητες να βρίσκεται στην κατάσταση 1.

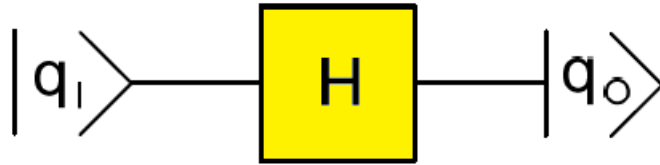
Ας δούμε λοιπόν τι θα γινόταν εάν η πύλη Hadamard δρούσε πάνω σε ένα qubit το οποίο βρισκόταν σε υπέρθεση καταστάσεων. Όπως και προηγουμένως θα εξεταστούν και οι δυο περιπτώσεις. Η πρώτη περίπτωση θα δούμε το αποτέλεσμα όταν το qubit δρα στην υπέρθεση της κατάστασης όπου το qubit ήταν αρχικά $|0\rangle$. Τότε:

$$H \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

Και στην συνέχεια θα παρουσιαστεί η περίπτωση όπου το qubit θα βρίσκεται στην κατάσταση $|1\rangle$, Τότε:

$$H \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Με αυτό το παράδειγμα μπορέσαμε και αποδείξαμε αυτό που αναφέρθηκε παραπάνω ως αντιστρεψιμότητα. Καθώς αρχικά είχαμε ένα qubit σε μια από τις δυο βασικές καταστάσεις και επεμβαίνοντας σε αυτό με την ίδια πύλη δυο φορές το qubit επανήλθε στη αρχική του κατάσταση. Άρα η πύλη Hadamard όχι μόνο μπορεί να δημιουργήσει υπέρθεση σε μια βασική κατάσταση αλλά και να επαναφέρει το qubit από υπέρθεση σε βασική κατάσταση.



Εικόνα 1-6 Σύμβολο κβαντικής πύλης Hadamard (H)

$ q_i\rangle$	$ q_o\rangle$
$ 0\rangle$	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
$ 1\rangle$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$
$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ 0\rangle$
$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ 1\rangle$

Εικόνα 1-7 Δράσεις της πύλης Hadamard πάνω σε qubits

Στον παραπάνω πίνακα με $|q_i\rangle$ συμβολίζονται οι καταστάσεις του qubit πρώτου επέμβει η πύλη Hadamard και με $|q_o\rangle$ οι καταστάσεις αφού επέμβει η πύλη στο qubit.

1.4.4 Κβαντική πύλη ελεγχόμενου ΌΧΙ (CNOT)

Σε αντίθεση με τις πύλη που έχουν αναφερθεί ως τώρα η κβαντική πύλη ελεγχόμενου ΌΧΙ (control not) δρα σε δυο qubit. Στο qubit το οποίο δρα συμβολίζεται με c και ονομάζεται qubit ελέγχου (control) ενώ το άλλο qubit ονομάζεται qubit στόχος (target) και συμβολίζεται με t. Η λειτουργία που επιτελεί αυτή η κβαντική πύλη είναι ότι, αν το qubit ελέγχου βρίσκεται στην βασική κατάσταση $|1\rangle$ τότε το qubit στόχου αλλάζει την τιμή της

βασικής του κατάστασης. Οι καταστάσεις των δυο qubit πρωτού επέμβει η πύλη συμβολίζονται με $|c_i\rangle$ και $|t_i\rangle$ ενώ μετά την δράση είναι $|c_0\rangle$ και $|t_0\rangle$. Όπως είναι εύκολο να συμπαιράνει κανείς η κατάσταση του qubit ελέγχου δεν αλλάζει ποτέ, δηλαδή $|c_i\rangle = |c_0\rangle$.

Ο πίνακας που περιγράφει την πύλη CNOT είναι:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

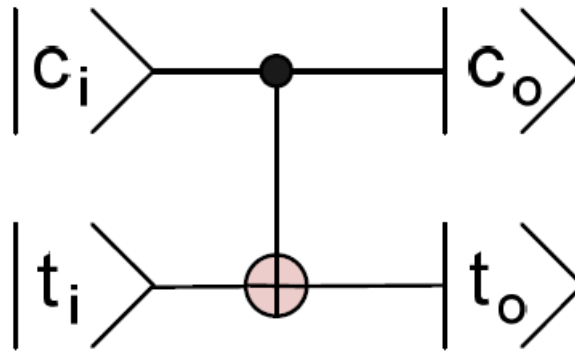
Έστω λοιπόν ότι πριν την δράση της πύλης τα δυο qubit έχουν την τιμή $|01\rangle$ τότε αφού επέμβει η πύλη CNOT γίνεται:

$$\text{CNOT}|01\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

Παρατηρούμε ότι τα δυο qubit έμειναν αμετάβλητα καθώς το qubit ελέγχου βρίσκεται στην κατάσταση $|0\rangle$ οπότε και το qubit στόχος παραμένει στην αρχική του κατάσταση. Ας δούμε λοιπόν τι θα γινόταν εάν το qubit ελέγχου ήταν στην κατάσταση $|1\rangle$. Έστω τα δυο qubit είναι $|10\rangle$ τότε:

$$\text{CNOT}|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

Όπως φαίνεται στο παραπάνω αποτέλεσμα το qubit στόχος (δηλαδή το πρώτο qubit) άλλαξε την τιμή της καταστάσής του από $|0\rangle$ σε $|1\rangle$.



Εικόνα 1-8 Σύμβολο της κβαντική πύλης ελεγχόμενου ΟΧΙ, CNOT

$ c_i t_i\rangle$	$ c_o t_o\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

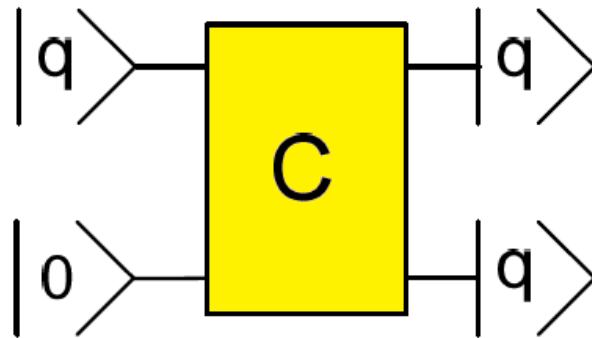
Εικόνα 1-9 Η δράση της κβαντικής πύλης CNOT στα qubits ελέγχου και στόχου

Μια πολύ σημαντική σημείωση είναι ότι όπως στους κλασσικούς υπολογιστές με την χρήση τριών πυλών (AND, NOT, OR) μπορεί να εκτελεστεί οποιαδήποτε διαδικασία έτσι αντίστοιχα και στους κβαντικούς υπολογιστές μπορεί με την χρήση των πυλών H , Φ και CNOT αφού αποτελούν ένα γενικευμένο σύνολο πυλών.

1.5 Αδυναμία αντιγραφής κατάστασης ενός qubit

Μια από τις βασικότερες και πιο χρήσιμες λειτουργίες που παρέχουν οι κβαντικοί υπολογιστές είναι η αδυναμία διακλάδωσης. Όπως γνωρίζουμε η αντιγραφή ενός bit στους κλασσικούς υπολογιστές είναι μια πάρα πολύ εύκολη και συχνά χρησιμοποιούμενη διαδικασία. Από την άλλη στους κβαντικούς υπολογιστές κάτι τέτοιο είναι αδύνατο, δηλαδή η άγνωστη

κατάσταση ενός qubit δεν μπορεί αντιγραφεί. Για να το αποδείξουμε αυτή την θεωρία θα πρέπει να χρησιμοποιηθεί μια πύλη που δεν υπάρχει και θα την συμβολίσουμε με C.



Εικόνα 1-10 Θεωρητική πύλη η οποία αντιγράφει την άγνωστη κατάσταση του qubit $|q\rangle$

Στο σχήμα φαίνεται η κβαντική πύλη αντιγραφής κατάστασης της οποίας τον τελεστή τον ονομάσαμε C. Η πύλη δρα σε δυο qubit εκ των οποίων το ένα είναι το qubit $|q\rangle$ το οποίο βρίσκεται σε τυχαία άγνωστη κατάσταση και το άλλο είναι ένα qubit το οποίο βρίσκεται στην βασική κατάσταση $|0\rangle$. Μετά την δράση της πύλης και τα δυο qubit θα βρίσκονται στην ίδια κατάσταση, δηλαδή η άγνωστη κατάσταση του qubit $|q\rangle$ θα αντιγραφεί στο qubit που είχε αρχικά την κατάσταση $|0\rangle$. Όπως αναφέρθηκε και προηγουμένως μια τέτοια πύλη είναι αδύνατο να υπάρξει και η απόδειξη παρουσιάζεται παρακάτω.

Θεώρημα αδυναμίας διακλάδωσης είναι αδύνατο να υπάρξει κβαντική πύλη τέτοια ώστε:

$$C|q0\rangle = |qq\rangle, \text{ όπου } |q\rangle \text{ είναι ένα qubit με άγνωστη κατάσταση}$$

Απόδειξη: Έστω ότι υπάρχει κβαντική πύλη C η οποία μπορεί να αντιγράψει κατάσταση ενός qubit. Βάζουμε την πύλη να δράσει σε δυο qubit το $|q\rangle$ και το $|b\rangle$ τα οποία είναι ορθογώνια μεταξύ τους και να τα αντιγράψει. Τότε:

$$C|q0\rangle = |qq\rangle$$

$$C|b0\rangle = |bb\rangle$$

Στην συνέχεια θα θεωρήσουμε ένα ακόμη qubit το οποίο θα είναι σε κατάσταση υπέρθεσης των qubit $|q\rangle$ και $|b\rangle$ και θα το ονομάσουμε $|c\rangle$.
Οπότε:

$$|c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle)$$

Σε αυτό το σημείο θα δράσει η πύλη C στο qubit $|c\rangle$ αντιγράφοντας την κατάσταση του:

$$\begin{aligned} C|c0\rangle &= \frac{1}{\sqrt{2}}C(|q\rangle + |b\rangle)|0\rangle = \frac{1}{\sqrt{2}}(C|q0\rangle + C|b0\rangle) \\ &= \frac{1}{\sqrt{2}}(|qq\rangle + |bb\rangle) \end{aligned}$$

Αλλά θα πρέπει να ισχύει ότι:

$$\begin{aligned} C|c0\rangle &= |cc\rangle = |c\rangle |c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle)\frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) \\ &= \frac{1}{2}(|qq\rangle + |qb\rangle + |bq\rangle + |bb\rangle) \end{aligned}$$

Όπως παρατηρείται οι δύο εξισώσεις δεν είναι όμοιες διότι ενώ τα αριστερά του μέλη είναι όμοια τα δεξιά διαφέρουν. Επομένως η κβαντική πύλη C δεν είναι δυνατόν να υπάρχει.

Η αδυναμία διακλάδωσης αποτελεί ένα από τα βασικά στοιχεία της κβαντικής κρυπτογραφίας. Εάν για παράδειγμα η Alice επιθυμεί να στείλει στον Bob ένα

Κεφάλαιο 2^ο

2.1 Κβαντικοί αλγόριθμοι

2. Αλγόριθμος του Grover

Ο αλγόριθμος του Grover αποτελεί έναν κβαντικό αλγόριθμο αναζήτησης, ο οποίος επιτυγχάνει την μείωση του χρόνου αναζήτησης σε μια μη-δομημένη βάση δεδομένων. Για να γίνει αυτό καλύτερα αντιληπτό υποθέτουμε ότι έχουμε μια μη-δομημένη βάση δεδομένων με N στοιχεία και χρησιμοποιούμε έναν κλασσικό υπολογιστή για την εύρεση του επιθυμητού μας στοιχείου. Για να γίνει αυτό χρησιμοποιείται ένα σύστημα το οποίο ονομάζεται **oracle** (μαντης). Η λειτουργία του συστήματος αυτού είναι να κάνει αναζήτηση, να επεξεργάζεται κάθε δεδομένο της βάσης και στην συνέχεια να ελέγχει εάν είναι το επιθυμητό ή όχι. Θεωρούμε ότι έχουμε N στοιχεία τα οποία αποτελούν την βάση δεδομένων και ότι έχουμε αντιστοιχίσει σε κάθε στοιχείο έναν αριθμό από το 0 έως το $N-1$. Το στοιχείο που αντιστοιχεί στον αριθμό k συμβολίζεται με x_k . Το oracle θα είναι μια συνάρτηση $f()$ η οποία θα παίρνει την τιμή 1 εάν το στοιχείο της βάσης είναι το επιθυμητό ενώ αλλιώς θα παίρνει την τιμή 0. Δηλαδή:

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

και ο μετασχηματισμός που εκτελεί είναι:

$$|x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle,$$

Όπου:

- x είναι ο καταχωρητής του δείκτη της λίστας
- $|q\rangle$ είναι ένα qubit το οποίο αντιστρέφεται αν $f(x) = 1$, ειδάλλως παραμένει σταθερό.
- Και \oplus συμβολίζεται η πρόσθεση με βάση το 2 (mod 2)

Ας δούμε καλύτερα την λειτουργία του κβαντικού oracle στην διαδικασία αναζήτησης σε μια μη δομημένη βάση δεδομένων. Το qubit του oracle τίθεται στην βασική κατάσταση $|1\rangle$ και στην συνέχεια δρα σ' αυτό μια κβαντική πύλη H .

$$|1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Στην συνέχεια επιλέγουμε ένα τυχαίο στοιχείο από την μη δομημένη βάση δεδομένων το οποίο συμβολίζεται με $|x\rangle$ ώστε να ελέγξουμε εάν αυτό είναι το επιθυμητό. Το oracle δρα στο $|x\rangle$ αλλά και στο qubit του, το οποίο βρίσκεται στην κατάσταση του παραπάνω τύπου. Το αποτέλεσμα της δράσης αυτή είναι:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{o} |x\rangle | f(x) \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rangle$$

Το $|x\rangle$ μπορεί να αντιστοιχεί στο στοιχείο που ψάχνουμε μπορεί και όχι. Ας δούμε αρχικά την περίπτωση στην οποία δεν αντιστοιχεί. Τότε η τιμή $f(x)$ παίρνει την τιμή $|0\rangle$ και η παραπάνω σχέση γίνεται:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{0} |x\rangle \left(|0\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Ας δούμε τώρα την περίπτωση που η $|x\rangle$ αντιστοιχεί στο στοιχείο που ψάχνουμε. Τότε η $f(x)$ παίρνει την τιμή 1 και η σχέση γίνεται:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{1} |x\rangle \left(|1\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) = -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Έτσι από τις δυο παραπάνω σχέσεις έχουμε ότι:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{0} \begin{cases} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{αν η } |x\rangle \text{ δεν αντιστοιχεί στο στοιχείο που ψάχνουμε} \\ -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right), & \text{αν η } |x\rangle \text{ αντιστοιχεί στο στοιχείο που ψάχνουμε} \end{cases}$$

Επειδή η τιμή του qubit $|q\rangle$ δεν αλλάζει ο παραπάνω τύπος μπορεί να γραφεί συνοπτικά και ως:

$$|x\rangle \xrightarrow{0} (-1)^{f(x)} |x\rangle$$

Ο μετασχηματισμός αυτός θα ονομαστεί U_f .

Ο τελεστής του κβαντικού oracle είναι:

$$\hat{O} = \hat{I} - 2|x\rangle\langle x|$$

Όπου \hat{I} είναι ο τελεστής που αντιστοιχεί στην πύλη αδρανείας. Αν το x δεν είναι ο τελεστής ο οποίος ψάχνουμε τότε ο τελεστής \hat{O} αφήνει το πρόσιμο ως έχει. Δηλαδή:

$$\hat{O}|x_k\rangle = (\hat{I} - 2|x_i\rangle\langle x_i|)|x_k\rangle = |x_k\rangle - 2|x_i\rangle\langle x_i||x_k\rangle = |x_k\rangle$$

Ενώ εάν είναι αυτό που ψάχνουμε ο τελεστής αλλάζει πρόσιμο στο στοιχείο της βάσης και αυτό γίνεται:

$$\hat{O}|x_i\rangle = (\hat{I} - 2|x_i\rangle\langle x_i|)|x_i\rangle = |x_i\rangle - 2|x_i\rangle\langle x_i||x_i\rangle = -|x_i\rangle$$

Αυτό συμβαίνει διότι όταν οι δυο βασικές καταστάσεις του κβαντικού καταχωρητή είναι διαφορετικές μεταξύ είναι ορθογώνιες και το εποτέλεσμα είναι $\langle x_i | |x_i \rangle = 0$ ενώ όταν είναι ίδιες το αποτέλεσμα είναι $\langle x_i | |x_i \rangle = 1$.

Για να ερευνηθεί με έναν κβαντικό υπολογιστή μια μη δομημένη βάση δεδομένων που περιέχει N στοιχεία, πρέπει να αντιστοιχηθεί κάθε στοιχείο με μια από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή. Θα πρέπει $N = 2^n - 1$ όπου το n είναι ο αριθμός των qubits. Σε περίπτωση που δεν υπάρχει n το οποίο να ικανοποιεί ακριβώς αυτή την σχέση θα χρησιμοποιηθεί το αμέσως μεγαλύτερο και αν υπάρχει περίσσεια αριθμών. Θέτουμε λοιπόν τον κβαντικό καταχωρητή σε μια κατάσταση $|s\rangle$ η οποία είναι μια υπέρθεση όλων των βασικών καταστάσεων. Όλες οι καταστάσεις της υπέρθεσης θα έχουν το ίδιο πλάτος πιθανότητας: x_i

$$|s\rangle = \frac{1}{\sqrt{N}}|0\rangle + \frac{1}{\sqrt{N}}|1\rangle + \frac{1}{\sqrt{N}}|2\rangle + \dots + \frac{1}{\sqrt{N}}|(N-1)\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle$$

Παρόμοια με τον τελεστή \hat{O} ο Grover όρισε έναν ακόμα τελεστή τον \hat{G} που δίνεται από:

$$\hat{G} = -(\hat{I} - 2|s\rangle\langle s|) = 2|s\rangle\langle s| - \hat{I}$$

Ο τρόπος λειτουργίας του αλγόριθμου του Grover είναι μια επαναλαμβανόμενη διαδοχική εφαρμογή των τελεστών \hat{O} και \hat{G} για περίπου $\left(\frac{\pi}{4}\sqrt{N}\right) - 0,5$ φορές. Τα βήματα του αλγορίθμου είναι τα εξής:

Βήμα 1^ο

Όπως αναφέραμε και προηγουμένως σαν βήμα πρώτο θέτουμε τον κβαντικό καταχωρητή με n qubits σε κατάσταση υπέρθεσης. Το πλάτος πιθανότητας είναι το ίδιο για κάθε βασική κατάσταση. Για επιτευχθεί αυτό ξεκινάμε έχοντας τον καταχωρητή στην κατάσταση $|0\rangle$ δηλαδή $|000\dots 00\rangle$. Στην συνέχεια δράμε σε κάθε qubit με την πύλη Hadamard (H). Η κατάσταση του κβαντικού είναι:

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

Αντιστοιχούμε κάθε βασική κατάσταση με ένα στοιχείο της μη δομημένης βάσης δεδομένων. Έστω λοιπόν ότι ψάχνουμε το στοιχείο $|x_i\rangle$.

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

Βήμα 2^ο

Δρούμε στον κβαντικό καταχωρητή με τον τελεστή

$$\hat{O} = \hat{I} - 2|x\rangle\langle x|$$

Βήμα 3^ο

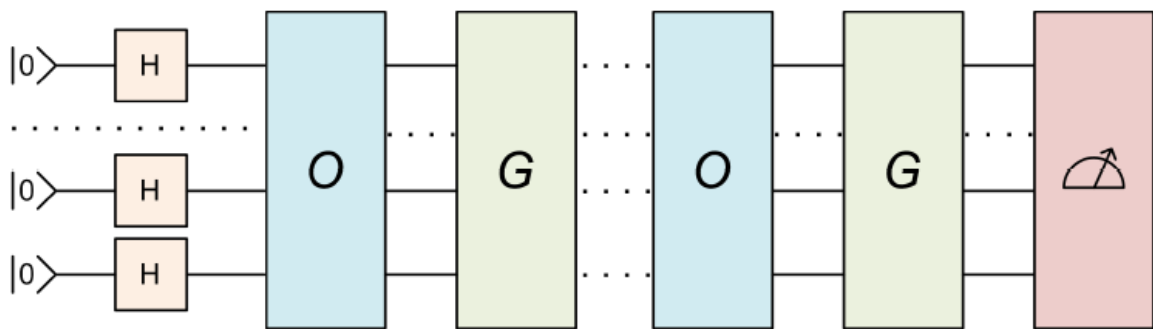
Στην συνέχεια δρούμε με τον κβαντικό τελεστή:

$$\hat{G} = 2|s\rangle\langle s| - \hat{I}$$

Έπειτα γίνεται ο έλεγχος για το εάν ο αριθμός των επαναλήψεων είναι μεγαλύτερος από το $\left(\left(\frac{\pi}{4}\right)\sqrt{N}\right) - 0,5$. Εάν είναι τότε πάμε στο βήμα 4^ο αλλιώς αυξάνουμε το b κατά 1 και πηγαίνουμε πάλι στο βήμα 2^ο.

Βήμα 4^ο

Μετράμε την κατάσταση του κβαντικού καταχωρητή. Είναι στατιστικά βεβαίο ότι θα βρίσκεται στην κατάσταση $|x_i\rangle$ η οποία αντιστοιχεί και στο στοιχείο που αναζητάμε.



Εικόνα 2-1 Κβαντικό κύκλωμα του αλγορίθμου του Grover

Κβαντικός αλγόριθμος του Shor

Το 1994 ο Peter Shor απέδειξε ότι με την χρήση κβαντικών υπολογιστών μπορεί εύκολα και γρήγορα να βρεθεί περίοδος περιοδικών συναρτήσεων, δηλαδή να αναλυθούν σε γινόμενο δυο πρώτων αριθμών μεγάλοι ακέραιοι αριθμοί. Ένα τέτοιο παράδειγμα επίλυσης είναι η επίλυση του κρυπτογραφικού συστήματος RSA. Το 1978 δημιουργήθηκε το κρυπτογραφικό σύστημα RSA το οποίο πήρε τα αρχικά του από τους Ronald Rivest, Adi Shamir και Leonard Adelman. Είναι ένα κρυπτογραφικό σύστημα με δημόδιο κλειδί και θεωρείται ότι είναι αδύνατο να σπάσει με την χρήση κλασσικών υπολογιστών. Αν και δεν έχει αποδειχθεί ότι η παραγοντοποίηση πρώτων αριθμών δεν μπορεί να επιτευχθεί σε πολυωνυμικό χρόνο, μέχρι στιγμής δεν έχει αναπτυχθεί κάποιος αλγόριθμος που να το επιτυγχάνει. Μέχρι το 2015 ο πιο ταχύς διαθέσιμος αλγόριθμος έτρεχε σε $O(e^{\frac{64}{9}n^{\frac{1}{3}}(\log n)^{\frac{2}{3}}})$ πράξεις, όπου n είναι ο αριθμός των bit που είναι απαραίτητα για την αναπαράσταση του αριθμού που θέλουμε να παραγοντοποιήσουμε. Σε αντίθεση, ο αλγόριθμος του Shor τρέχει σε $O((\log n)^2 * \log \log n)$ πράξεις σε κβαντικό υπολογιστή, ακολουθούμενες από $O(\log n)$ βήματα μετέπειτα επεξεργασίας σε κλασσικό υπολογιστή. Η επιτάχυνση, την οποία επιτυγχάνει, όπως παρατηρούμε, είναι εκπληκτική.

Συνοπτικά, ο αλγόριθμος του Shor προσπαθεί να βρει το r , το οποίο είναι η περίοδος της συνάρτησης $f(a) = x^a \bmod n$, όπου το n είναι ο αριθμός που προσπαθούμε να παραγοντοποιήσουμε και x είναι ένας ακέραιος που έχει μοναδικό κοινό θετικό, ακέραιο, πρώτο παράγοντα με το n το 1 (coprime numbers).

Αρχικά, παίρνουμε δυο καταχωρητές και σαν πρώτο μέρος βάζουμε στον πρώτο καταχωρητή σε υπέρθεση τους αριθμούς που δύναται να είναι το a δηλαδή ακέραιους αριθμούς από το 0 έως το $q-1$ ($[0, \dots, q-1]$) όπου θα πρέπει να ισχύει: $2n^2 \leq q \leq 3n^2$. Ο αριθμός a που θα επιλεγεί θα πρέπει να είναι πρώτος ως προς τον n .

Στην συνέχεια με την χρήση της κβαντικής παραλληλίας υπολογίζεται η τιμή της $f_{n,a}(x)$ για κάθε x και τα αποτελέσματα καταγράφονται στον δεύτερο καταχωρητή ο οποίος πλέον κρατά την υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Έπειτα θα πρέπει να γίνει μέτρηση της κατάστασης του δεύτερου καταχωρητή. Η μέτρηση που θα γίνει στον δεύτερο καταχωρητή θα καταστρέψει την υπέρθεση και έτσι θα δώσει μια συγκεκριμένη τιμή, ας πούμε k . Σε αυτό το σημείο θα πρέπει να τονιστεί ότι η μέτρηση της κατάστασης του δεύτερου καταχωρητή καθορίζει την κατάσταση του πρώτου καταχωρητή αφού βρίσκονται σε κβαντική διεμπλοκή μεταξύ τους.

Έπειτα από όλα αυτά στον πρώτο καταχωρητή θα υπάρχουν ως υπέρθεση καταστάσεων οι αριθμοί $(x, x+r, x+2r, x+3r, \dots)$. Τα πλάτη πιθανότητας όλων των καταστάσεων είναι ίσα μεταξύ τους. Φυσικά, r είναι η ζητούμενη περίοδος της συνάρτησης. Προκειμένου να μπορέσει να βρεθεί η περίοδος r χωρίς να καταστραφεί η υπέρθεση στον πρώτο καταχωρητή θα χρησιμοποιηθεί ο κβαντικός μετασχηματισμός Fourier. Αυτό έχει ως αποτέλεσμα την ενίσχυση των πλατών πιθανότητας του πρώτου καταχωρητή για ακέραια πολλαπλάσια του q/r .

Έπειτα μια μέτρηση στον πρώτο καταχωρητή μας δίνει ένα ακέραιο πολλαπλάσιο της αντίστροφης περιόδου. Τέλος, το αποτέλεσμα της τελευταίας μέτρησης το παίρνει ένας κλασσικός υπολογιστής, ο οποίος κάνει μια εικασία για την πραγματική τιμή του r , και από αυτό να υπολογίσει τους πιθανούς παράγοντες του n .

Έστω λοιπόν ότι θέλουν να αναλύσουμε έναν ακέραιο αριθμό n σε γινόμενο δύο πρώτων αριθμών. Για να το πετύχουμε αυτό θα πρέπει να υπολογίσουμε την περίοδο της συνάρτησης $f_{n,a}(x) = a^x \bmod n$.

Βήμα 1^ο

Επιλέγεται ένας ακέραιος αριθμός q τέτοιος ώστε $2n^2 \leq q \leq 3n^2$

Βήμα 2°

Γίνεται τυχαία επιλογή ενός ακέραιου αριθμού a ο οποίος πρέπει να είναι πρώτος ως προς τον n .

Βήμα 3°

Στην συνέχεια παίρνουμε έναν κβαντικό καταχωρητή (reg) ο οποίος αποτελείται από δυο κβαντικούς καταχωρητές (reg1, reg2) οι οποίοι βρίσκονται στην κατάσταση $|0\rangle$. Δηλαδή η κατάσταση του Register είναι η:

$$|\psi\rangle = |00\rangle$$

Βήμα 4°

Φέρνουμε τον καταχωρητή reg1 σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως $q-1$. Σε αυτό το βήμα δεν δρούμε καθόλου στον καταχωρητή reg2 και η κατάσταση του reg θα δίνεται από:

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

Βήμα 5°

Έπειτα με την χρήση της κβαντικής παραλληλίας υπολογίζεται η τιμή της $f_{n,a}(x)$ και τα αποτελέσματα που θα ληφθούν καταγράφονται στον reg2 ο οποίος κρατά πλέον την υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Έτσι η κατάσταση του reg θα δίνεται από:

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

Και όπως είναι λογικό έπειτα από αυτό το βήμα ο reg1 και ο reg2 βρίσκονται σε κβαντική διεμπλοκή

Βήμα 6°

Μετράμε τον δεύτερο καταχωρητή, από την οποία μέτρηση θα λάβουμε ως αποτέλεσμα κάποια τιμή k . Αυτό το βήμα έχει ως παράπλευρη επίδραση την κατάρρευση του πρώτου καταχωρητή σε μια κατάσταση υπέρθεσης όλων των τιμών $a \in [0, q-1]$, έτσι ώστε:

$$x^a \bmod n = k$$

Η συνολική κατάσταση του συστήματος τώρα γίνεται:

$$\frac{1}{\sqrt{\|A\|}} \sum_{a \in A} |a, k\rangle$$

Όπου A είναι ένα σύνολο που περιέχει τα a , έτσι ώστε $x^a \bmod n = k$ και $\|A\|$ ο αριθμός των στοιχείων σε αυτό το σύνολο.

Βήμα 7^ο

Εφαρμόζουμε τον μετασχηματισμό Fourier στον πρώτο καταχωρητή.

Το αποτέλεσμα που θα δώσει ο μετασχηματισμός Fourier σε μια κατάσταση $|a\rangle$ είναι η εξής:

$$\text{QFT}|a\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{\frac{2\pi i a c}{q}} |c\rangle$$

Έτσι λοιπόν η συνολική κατάσταση του συστήματος των δυο καταχωρητών γίνεται η:

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

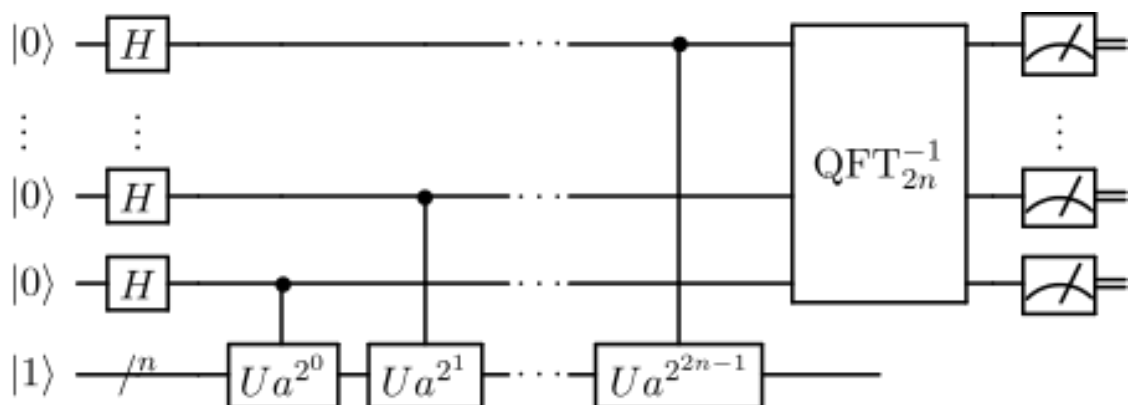
Βήμα 8^ο

Κάνουμε μέτρηση της κατάστασης του πρώτου καταχωρητή και αποκαλούμε την τιμή που παίρνουμε m . Η τιμή m έχει πολύ μεγάλη πιθανότητα να είναι πολλαπλάσιο του $\frac{q}{r}$ (το οποίο μπορεί να επιβεβαιωθεί με την επανάληψη του αλγορίθμου έως εδώ μερικές φορές), όπου r είναι η επιθυμητή περίοδος.

Βήμα 9^ο

Στο τελευταίο βήμα αφού γνωρίζουμε την τιμή m , q και με την βοήθεια του κλασσικού υπολογιστή υπολογίζουμε το r . Πιο αναλυτικά:

- 1) Το m είναι: $m = \lambda * \frac{q}{r}$, όπου το λ είναι κάποιος ακέραιος πραγματικός αριθμός.
- 2) Πραγματοποιούμε διαίρεση κινητής υποδιαστολής (floating point division) στο $\frac{m}{q}$ και έπειτα υπολογίζουμε την καλύτερη λογική προσέγγιση του $\frac{m}{q}$, της οποίας ο παρανομαστής είναι $\leq q$.
- 3) Παίρνουμε τον παρανομαστή ως υποψήφιο για την τιμή r .
- 4) Αν ο υποψήφιος μας είναι περιττός, τον διπλασιάζουμε αν κάτι τέτοιο οδηγεί σε τιμή $\leq q$ ή διαλέγουμε έναν νέο τυχαίο αριθμό q , και επιστρέφουμε στο βήμα 2.
- 5) Τέλος, έχοντας την τιμή του r ένας παράγοντας του n είναι δυνατό να καθοριστεί από τον μέγιστο κοινό διαιρέτη (ΜΚΔ) των $(x^{\frac{r}{2}+1}, n)$ και ένας παράγοντας παίρνοντας τον μέγιστο κοινό διαιρέτη των $(x^{\frac{r}{2}-1}, n)$. Ο πολλαπλασιασμός αυτό τον πρώτων παραγόντων μας δίνει επιτυχώς τον αριθμό n .
Σε αυτό το σημείο γίνεται έλεγχος για το εάν έχει βρεθεί πρώτος παράγοντας n . Αν έχει βρεθεί σταματάμε αλλιώς πηγαίνουμε στο βήμα 4.



Εικόνα 2-2 Εικόνα κβαντικού κυκλώματος του κβαντικού αλγορίθμου Shor

2.2 Κβαντική κρυπτογραφία

2.1 Εισαγωγή

Η κρυπτογραφία είναι κλάδος της επιστήμης της κρυπτολογίας η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο βασικός στόχος είναι να μελετά και να εφαρμόζει τεχνικές διαφύλαξης εμπιστευτικών δεδομένων από τη μη εξουσιοδοτημένη πρόσβαση. Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω την Alice και τον Bob, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (Eve), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Η κβαντική κρυπτογραφία συνίσταται στην εκμετάλλευση κάποιων ιδιοτήτων ενός φυσικού συστήματος, οι οποίες προβλέπονται από την κβαντομηχανική, έτσι ώστε να δημιουργηθεί ένα κλειδί κρυπτογράφησης το οποίο θα εξασφαλίζει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των κατόχων του.

Η βασική διαφορά μεταξύ της κλασσικής και της κβαντικής κρυπτογραφίας είναι ότι οι χρήστες έχουν την δυνατότητα να κατανοήσουν πότε υπάρχει παραβίαση του συστήματος. Αυτό συμβαίνει διότι η διαδικασία της μέτρησης διαταράσσει την κατάσταση των qubit και βάση κάποιων τεχνικών που θα εξηγηθούν πιο αναλυτικά σε επόμενο κεφάλαιο οι μετέχοντες μπορούν να αντιληφθούν την επέμβαση τρίτου στο σύστημα. Εν αντιθέση η κλασσική κρυπτογραφία βασίζεται πάνω σε ιδιότητες υπολογιστικής πολυπλοκότητας κάποιων συγκεκριμένων μαθηματικών συναρτήσεων, οι οποίες δεν προσφέρουν καμία εγγύηση καθώς εξαρτώνται μεταξύ άλλων και από την υπάρχουσα τεχνολογία, η κβαντική κρυπτογραφία βασίζεται πάνω στα καλά ελεγμένα θεμέλια της κβαντικής μηχανικής.

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι στις υπάρχουσες μεθόδους κβαντικής κρυπτογραφίας η χρήση του κβαντικού συστήματος γίνεται μόνο για την παραγωγή και την μετάδοση του κβαντικού κλειδιού. Η μεταφορά της πληροφορίας γίνεται μέσω κλασσικού καναλιού. Ακόμη, οι διάφορες μέθοδοι κβαντικής κρυπτογράφησης στην ουσία αποτελούν παραλλαγές δύο βασικών διαφορετικών μεθόδων που αξιοποιούν είτε το φαινόμενο της κβαντικής διαπλοκής το οποίο στηρίζεται στο παράδοξο EPR, είτε στην αρχή της απροσδιοριστίας του Heisenberg.

2.2 Κβαντική διεμπλοκή

Όπως αναφέρθηκε και παραπάνω η κβαντική διεμπλοκή στηρίχθηκε σε ένα άρθρο που δημοσιεύτηκε το 1935 από του Albert Einstein, Boris Podolsky και

Nathan Rosen από τους οποίους και πήρε τα αρχικά (EPR paradox). Σαν πρώτο στάδιο στο πειραματικό μοντέλο χρησιμοποιήθηκαν δυο κβαντικά συστήματα τα οποία αφού αλληλεπιδράσαν μεταξύ τους απομακρύνθηκε το ένα από το άλλο. Στην συνέχεια παρατηρήθηκε ότι μετρώντας μια φυσική ποσότητα στο έναν σύστημα καθορίζεται το αποτέλεσμα της μέτρησης του άλλου συστήματος. Έπειτα από μελέτη διαπιστώθηκε ότι τα δυο αυτά συστήματα παραμένουν διασυνδεδεμένα μεταξύ τους με έναν άγνωστο μη κλασσικό τρόπο.

Την ίδια χρονιά (1935) σε ένα άρθρο που δημοσιεύτηκε απο τον Erwin Schrödinger σχετικά με την μη κλασσική διασύνδεση των κβαντικών συστημάτων αποδόθηκε στο πείραμα ο Γερμανικό όρος «verschränkung» το οποίο μεταφράστηκε στα Αγγλικά ως «entanglement» και στα ελληνικά ως «διεμπλοκή». Ο ορισμός που αποδίδεται στην κβαντική διεμπλοκή είναι ο εξής:

Ορισμός: Δυο κβαντικά συστήματα βρίσκονται σε κβαντική διεμπλοκή, όταν η κατάσταση τους δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών του καταστάσεων.

Για να γίνει πιο κατανοητός ο παραπάνω ορισμός θα θεωρήσουμε ότι έχουμε δυο κβαντικά συστήματα τα οποία περιγράφονται από δυο qubit. Στο πρώτο σύστημα αντιστοιχεί το $|q_1\rangle$ και στο δεύτερο σύστημα το $|q_2\rangle$. Όταν τα δυο qubits έρθουν σε διεμπλοκή δημιουργείται η κατάσταση $|q_s\rangle$ η οποία περιγράφεται από τον τύπο:

$$|q_s\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

Η $|q_s\rangle$ στην συνέχεια μπορεί να γραφεί:

$$|q_s\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)] \otimes |1\rangle$$

Σε αυτό το βήμα παρατηρούμε ότι έχουν δημιουργηθεί δυο καταστάσεις η $|q_{s0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ και η $|q_{s1}\rangle = |1\rangle$. Η $|q_s\rangle$ λοιπόν γράφεται ως τανυστικό γινόμενο των δυο καταστάσεων:

$$|q_s\rangle = |q_{s0}\rangle \otimes |q_{s1}\rangle$$

Όπως αναφέραμε και στον ορισμό επειδή τα δυο συστήματα μπορούν να γραφούν σε μορφή τανυστικού γινομένου δεν βρίσκονται σε διεμπλοκή. Αυτό συμβαίνει διότι εάν μετρήσουμε το πρώτο qubit στην κατάσταση $|0\rangle$ τότε το δεύτερο qubit μπορεί να είναι είτε στην κατάσταση $|0\rangle$ είτε στην κατάσταση $|1\rangle$.

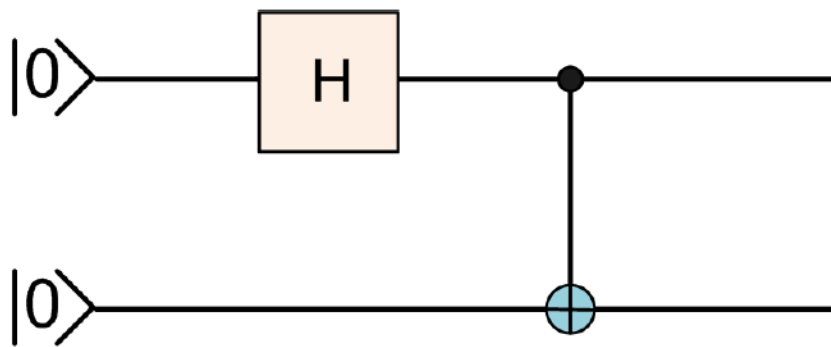
Σαν δεύτερο παράδειγμα θα δωθεί ακόμη ένα κβαντικό σύστημα το οποίο αποτελείται από δυο κβαντικά συστήματα. Αντίστοιχα με την προηγούμενη περίπτωση κάθε κβαντικό σύστημα θα περιγράφεται από ένα qubit. Στο πρώτο σύστημα αντιστοιχεί το $|q_a\rangle$ και στο δεύτερο το $|q_b\rangle$. Όταν τα δυο qubits έρθουν σε διεμπλοκή δημιουργείται η κατάσταση $|q_e\rangle$ η οποία όμως αυτή την φορά θα περιγράφεται από έναν διαφορετικό τύπο ο οποίος θα είναι:

$$|q_e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

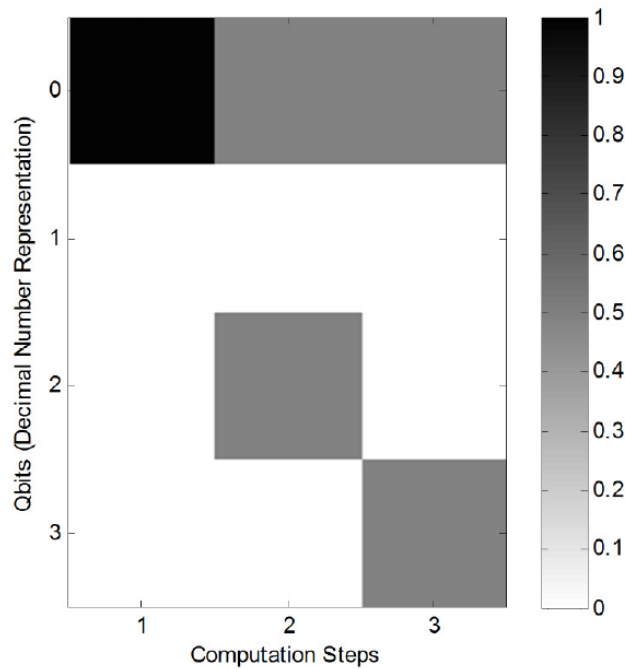
Όπως φαίνεται από την παραπάνω εξίσωση σε περίπτωση που το πρώτο qubit (q_a) μετρηθεί στην κατάσταση $|0\rangle$ θα γνωρίζουμε ότι και το δεύτερο qubit βρίσκεται σε κατάσταση $|0\rangle$ και αντίστοιχα εάν βρίσκεται στην κατάσταση $|1\rangle$ θα γνωρίζουμε ότι και το δεύτερο qubit βρίσκεται στην κατάσταση $|1\rangle$.

Στο πρώτο παράδειγμα που αναφέραμε τα δυο qubit βρίσκονται σε κατάσταση υπέρθεσης. Η διαφορά της υπέρθεσης και της διεμπλοκής είναι ότι στην υπέρθεση όπως αναφέραμε και παραπάνω εάν μετρηθεί η κατάσταση τους ενός qubit τότε δεν μπορούμε να γνωρίζουμε με ακρίβεια την κατάσταση του άλλου. Σε περίπτωση δηλαδή που το πρώτο qubit μετρηθεί στην κατάσταση $|0\rangle$ τότε το δεύτερο qubit έχει 50% πιθανότητες να βρίσκεται στην κατάσταση $|0\rangle$ και 50% πιθανότητες να βρίσκεται στην κατάσταση $|1\rangle$. Αντίθετα στην διεμπλοκή είναι βέβαιο με πιθανότητα 100% ότι η κατάσταση του δεύτερου qubit θα είναι η αναμενόμενη.

A)



B)



Εικόνα 2-3 2-4 A) Το κβαντικό κύκλωμα για την κβαντική διεμπλοκή δυο qubits. B) Η προσομοίωση της διεμπλοκής από τον προσομοιωτή QCS.

2.3 Κβαντική τηλεμεταφορά

Η κβαντική τηλεμεταφορά είναι μια διαδικασία μεταφοράς της κατάστασης ενός ή περισσότερων qubits από τον αποστολέα στον παραλήπτη οι οποίοι μπορούν να βρίσκονται σε οποιαδήποτε χωρική απόσταση μεταξύ τους. Η διαδικασία αυτή στηρίζεται στο φαινόμενο της κβαντικής διεμπλοκής, ένα κβαντικό φαινόμενο που έγινε γνωστό από ένα άρθρο του Albert Einstein, Boris Podolsky, Nathan Rosen το 1935. Με το φαινόμενο αυτό μπόρεσε να αντικατεστηθεί το κβαντικό κανάλι και η μεταφορά την πληροφορίας του qubit να γίνεται ακαριαία. Παρακάτω θα περιγραφεί αναλυτικά η διαδικασία της κβαντικής τηλεμεταφοράς.

Στο παράδειγμά μας θα υποθέσουμε πως έχουμε δυο άτομα που θέλουν να επικοινωνήσουν με κβαντική τηλεμεταφορά την Alice και τον Bob.

- Αρχικά θα πρέπει η Alice και ο Bob να συναντηθούν και να δημιουργήσουν κβαντική διεμπλοκή μέσω ενός κβαντικού κυκλώματος διεμπλοκής. Στην αρχή και τα δυο qubit βρίσκονται στον κατάσταση $|0\rangle$ και στην συνέχεια τα φέρνουν

σε κβαντική διεμπλοκή. Η κατάσταση διεμπλοκής συμβολίζεται και $|E\rangle$ και δίνεται από τον τύπο:

$$|E\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Έπειτα ο καθένας παίρνει ένα από τα δυο qubits και απομακρύνονται ο ένας από τον άλλον (πχ. Alice στην Γη και Bob στον Άρη). Για να έχει νόημα το παράδειγμα μας θα πρέπει το φως να χρειάζεται αρκετά λεπτά της ώρας για να διανύσει την απόσταση του Bob από την Alice.
- Στην συνέχεια η Alice επιθυμεί να στείλει στον Bob την κατάσταση ενός qubit $|\psi\rangle$. Το qubit βρίσκεται σε υπέρθεση καταστάσεων. Έστω $|\psi\rangle = a|0\rangle + b|1\rangle$, όπου a, b είναι τα πλάτη πιθανότητας των βασικών καταστάσεων τα οποία η Alice δεν γνωρίζει πόσο είναι. Πάραυτα η Alice μπορεί να στείλει αυτή την άγνωστη κατάσταση στον Bob επειδή μοιράζονται ένα ζεύγος qubits τα οποία βρίσκονται σε διεμπλοκή.

Παρακάτω θα δειχθεί η εξέλιξη της κατάστασης των τριών σωματιδίων. Αρχικά θα έχουμε

$$|\Phi_0\rangle = |\psi\rangle |E\rangle = (a|0\rangle + b|1\rangle) \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \Rightarrow$$

$$|\Phi_0\rangle = \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle$$

Στην συνέχεια δρα η πύλη CNOT στο $|\Phi_0\rangle$ και έτσι θα έχουμε:

$$|\Phi_1\rangle = \text{CNOT} |\Phi_0\rangle = \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|101\rangle + \frac{b}{\sqrt{2}}|101\rangle$$

Έπειτα θα δράσει η πύλη Hadamard και η νέα κατάσταση του κβαντικού καταχωρητή θα είναι:

$$|\Phi_2\rangle = (H \oplus I \oplus I) |\Phi_1\rangle \Rightarrow$$

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}} (H \oplus I \oplus I) (a|0\rangle (|00\rangle + |11\rangle) + b|1\rangle (|10\rangle + |10\rangle)) \Rightarrow$$

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}} (a(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + b(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)) \Rightarrow$$

$$|\Phi_2\rangle = \frac{1}{2} (a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle))$$

Σε αυτό το σημείο θα ξεχωρίσουμε το qubit του Bob το οποίο είναι το πρώτο qubit (δηλαδή τα δεξιά) και η εξίσωση θα γίνει:

$$|\phi_2\rangle = \frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle))$$

Όπως βλέπουμε στον παραπάνω τύπο ακολουθώντας αυτά τα βήματα η Alice μπόρεσε να δημιουργήσει στα δυο δικά της qubit (το δεύτερο και το τρίτο) τις τέσσερις βασικές καταστάσεις. Κάθε μια κατάσταση συνδιάζεται με μια κατάσταση υπέρθεσης του Bob η οποία θα έχει πλάτη πιθανότητας a και b . Δηλαδή μπόρεσε να μεταφέρει τα άγνωστα πλάτη πιθανότητας που υπήρχαν στο δικό της qubit στο qubit του Bob εκμεταλλευόμενη τη διεμπλοκή. Έτσι όταν η Alice μετρήσει την κατάσταση των δικών της qubit θα έχει ως αποτέλεσμα μια από τις τέσσερις βασικές καταστάσεις στις οποίες μπορούν να βρεθούν αυτά. Οπότε:

- Αν η Alice μετρήσει $|00\rangle$ τότε ο Bob θα βρίσκεται στην κατάσταση $a|0\rangle + b|1\rangle$
- Αν η Alice μετρήσει $|01\rangle$ τότε ο Bob θα βρίσκεται στην κατάσταση $a|1\rangle + b|0\rangle$
- Αν η Alice μετρήσει $|10\rangle$ τότε ο Bob θα βρίσκεται στην κατάσταση $a|0\rangle - b|1\rangle$
- Αν η Alice μετρήσει $|11\rangle$ τότε ο Bob θα βρίσκεται στην κατάσταση $a|1\rangle - b|0\rangle$

Σε αυτό το σημείο θα πρέπει ο Bob να μάθει την μέτρηση της Alice ώστε να μπορέσει να φέρει το qubit του στην μορφή που πρέπει (δηλαδή $|\psi\rangle = a|0\rangle + b|1\rangle$). Η επικοινωνία αυτή θα πρέπει να γίνει μέσω ενός κλασσικού καναλιού. Για κάθε μια από τις τέσσερις μετρήσεις της Alice ο Bob θα πρέπει να επενεργήσει με διαφορετικές πύλες πάνω στο qubit του ώστε να δημιουργήσει την μορφή που θέλει.

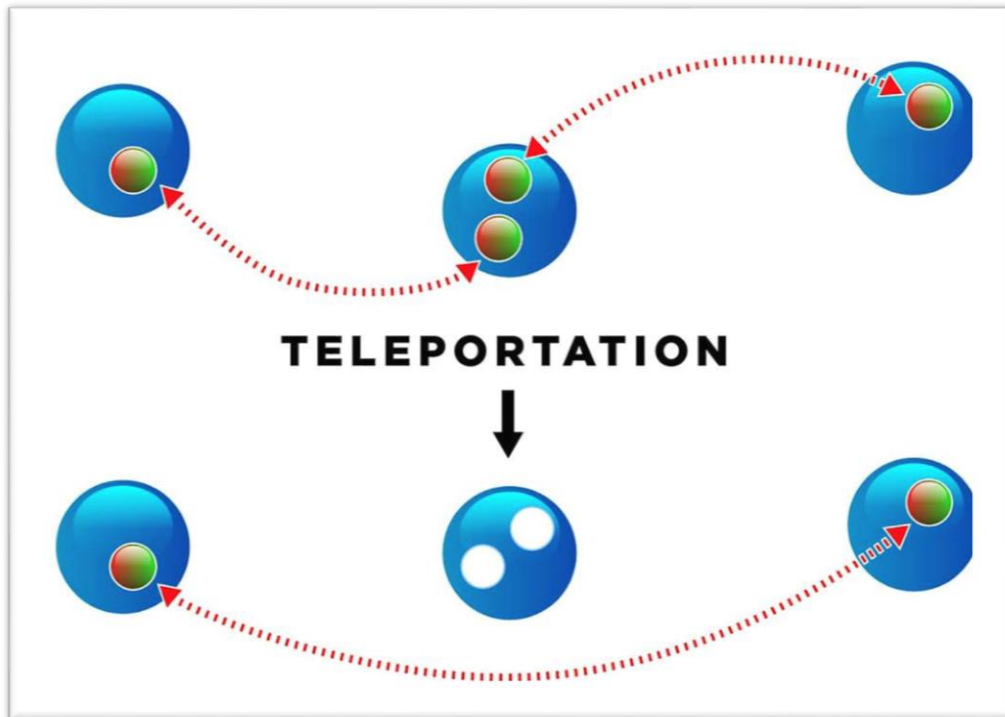
Μόλις η Alice μετρήσει τα δυο qubits της το qubit του Bob μεταφέρεται στην αντίστοιχη κατάσταση ακαριαία. Έτσι αντιλαμβανόμαστε ότι στη κβαντική τηλεμεταφορά δεν μεταφέρεται το φυσικό σύστημα που υλοποιεί το άγνωστο qubit $|\psi\rangle$ αλλά η καταστασή του. Όμως γνωρίζουμε ότι η πληροφορία δεν μπορεί να ξεπεράσει την ταχύτητα του φωτός. Η κβαντική τηλεμεταφορά δεν αντιτίθεται σε αυτή την αρχή καθώς χρειάζεται και ένα κλασσικό κανάλι επικοινωνίας για να υλοποιηθεί η διαδικασία. Τέλος θα πρέπει να τονιστεί πως ούτε το θεώρημα της αδυναμίας διακλάδωσης (no cloning theorem) παραβιάζεται καθώς μετά την μεταφορά η κατάσταση $|\psi\rangle$ δεν υπάρχει στον τόπο της Alice.

2.4 Quantum Repeaters

2.4.1 Πρωτόκολλο

Έχοντας ως στόχο την δημιουργία του κβαντικού ίντερνετ οι επιστήμονες χρειάστηκαν να εφεύρουν μια μέθοδο ώστε να μπορέσουν να μεταφέρουν τα qubits σε μεγάλες αποστάσεις. Ένα από τα βασικότερα εμπόδια στο να διενέμεις διεμπλεκόμενα φωτόνια σε μεγάλη απόσταση είναι η εξασθένηση της ίνας. Για παράδειγμα υπάρχει η Alice και ο Bob οι οποίοι είναι συνδεδεμένοι με ίνα και έχουν μεγάλη απόσταση μεταξύ τους, για να μπορέσουν να μεταδώσουν φωτόνια με τον απαιτούμε ρυθμό πρέπει να τοποθετήσουν στο ενδιάμεσο της απόστασης τους έναν repeater έτσι ώστε αυτός να δέχεται τα φωτόνια και των δυο και να δημιουργεί την διεμπλοκή τους. Έτσι τα φωτόνια αναγκάζονται να διανύσουν την μισή απόσταση, και αυτό συμβάλει στην ταχύτερη μετάδοσης αλλά και στην μείωση του ποσοστού σφάλματος. Από την στιγμή που θα γίνει η διεμπλοκή των επιθυμητών qubits η Alice και ο Bob έχουν την δυνατότητα να εκτελέσουν οποιαδήποτε ενέργεια χρειαστεί μέσω της λειτουργίας teleportation. Σαν πρώτο βήμα του πρωτοκόλλου σκοπός ήταν να μπορέσει να δημιουργηθεί ισχυρή διεμπλοκή ανάμεσα σε δυο μερίες που επιθυμούν να επικοινωνήσουν και οι οποίες βρίσκονται πολύ μακριά ή μια από την άλλη. Το πρόβλημα που τέθηκε σε αυτό το σημείο είναι ότι στην κβαντική επικοινωνία όσο αυξάνεται η απόσταση μεταξύ των δύο μεριών το ποσοστό σφάλματος των bit γίνεται όλο και μεγαλύτερο. Για παράδειγμα όταν χρησιμοποιείται οπτική ίνα και ένα φωτόνιο ως κβαντικό κανάλι οι απώλειες πλήρης ανάκλασης αυξάνονται εκθετικά όσο μεγαλύτερο είναι το κανάλι. Εάν η κατάσταση του φωτονίου ή το φωτόνιο το ίδιο καταστραφεί αυτό προκαλεί καταστροφή της επικοινωνίας. Την λύση σε αυτό το πρόβλημα ήρθαν να το δώσουν οι quantum repeaters.

Ανεξάρτητα από το όνομα τους οι κβαντικοί επαναλήπτες χρησιμοποιούν τελείως διαφορετική μεθοδολογία από αυτή των κλασικών επαναληπτών για να διαχειριστούν το πρόβλημα της απώλειας. Πιο συγκεκριμένα το πρωτόκολλο ξεκινάει δημιουργώντας κβαντική διεμπλοκή μεταξύ δυο κβαντικών μνημών οι οποίες έχουν απόσταση μεταξύ τους L_0 . Σε περίπτωση που η κβαντική διεμπλοκή είναι κακής ποιότητας θα πρέπει να χρησιμοποιηθεί η τεχνική **entanglement distillation**. Η βασική ιδέα πίσω από τον μηχανισμό αυτό είναι ότι μπορείς να έχεις πολύ καλή ποιότητα διεμπλοκής χρησιμοποιώντας πολλές κακής ποιότητας διεμπλοκές. Σαν επόμενο βήμα θα γίνεται **entanglement swapping** στον αντίστοιχο σταθμό του επαναλήπτη με σκοπό να συνδεθούν δυο γειτονικά διεμπλεκόμενα ζευγάρια και έτσι να επεκταθεί σταδιακά η διεμπλοκή.



Εικόνα 2-5 Λειτουργία των quantum repeaters

2.4.2 Δημιουργία κόμβων κβαντικών επαναληπτών και οι ατέλειες τους

Σε αυτό το τμήμα θα αναφερθούμε στα τμήματα και τις τεχνικές που χρειάζονται για να δημιουργηθεί ένας κβαντικός επαναλήπτης καθώς και ατέλειες που παρουσιάζονται σε αυτά. Ωστόσο κατά την υλοποίηση τους μπορεί να παρουσιαστούν περισσότερες ατέλειες από αυτές που θα αναφερθούν.

- a) **Κβαντικό κανάλι:** Υποθέτουμε ότι τα φωτόνια ταξιδεύουν μέσω οπτικής ίνας. Οι απώλειες που δημιουργούνται από τα φωτόνια θεωρούνται οι κύριες πηγές ατελειών.
- b) **Πηγή διεμπλοκής:** Ο σκοπός της πηγής είναι να δημιουργήσει διεμπλοκή μεταξύ κβαντικών μνημών οι οποίες βρίσκονται σε L . Ιδανικά θα επιθυμούσαμε η πηγή να δημιουργεί πλήρη διεμπλοκή μεταξύ κβαντικών ζευγαριών Bell. Στην πράξη όμως είναι δύσκολο να δημιουργηθεί πλήρης διεμπλοκή και το πιθανότερο είναι να δημιουργηθεί έναν ποσοστό διεμπλοκής.

- c) **Ανιχνευτές:** Οι ανιχνευτές εντοπίζουν τα φωτόνια που στέλνονται στον κόμβο.
- d) **Πύλες:** Οι ατέλειες των πυλών εξαρτώνται σε μεγάλο βαθμό από την ποιότητα του κβαντικού μας κυκλώματος.
- e) **Κβαντικές πύλες:** Οι κβαντικές πύλες είναι ένα πολύ βασικό κομμάτι των κβαντικών επαναλυπτών διότι σε αυτές αποθηκεύεται η κβαντική πληροφορία. Ένα από τα βασικότερα προβλήματα που εμφανίζονται σε αυτές είναι ότι ένα φωτόνιο απελευθερώνεται όταν ένα σήμα διαβάσματος εφαρμοστεί στην κβαντική μνήμη. Πιο γενικά, τα συχνότερα σφάλματα που προκύπτουν έπειτα από την ολοκλήρωση των λειτουργιών διάβασμα, αποθήκευση και αποστολή των qubit είναι ότι αυτά παραμένουν άθικτα.
- f) **Απόσταση διεμπλοκής:** Είναι μια πιθανολογική διαδικασία η οποία απαιτεί τοπικές πύλες πολλών qubit αλλά και την χρήση κλασσικής επικοινωνίας. Στο πρωτόκολλο του Deutsch αναφέρεται η διαδικασία χρήσης αυτής της τεχνικής. Το πρωτόκολλο ξεκινάει με 2^k ζευγάρια qubits και μετά από k γύρους παράγεται ένα διεμπλεκόμενο ζευγάρι με μεγαλύτερη πιστότητα απότι είχε στην αρχή. Σε κάθε γύρω απαιτείται να χρησιμοποιηθούν δυο πύλες CNOT,κάθε μια εκτελείται σε δυο qubits τα οποία βρίσκονται στον ίδιο quantum repeater σταθμό. Στην μέθοδο της απόσταξης εντοπίζονται συνήθως δυο είδη σφαλμάτων. Το πρώτο είδος δημιουργείται λόγω των ατελειών που υφίστανται μέχρι στιγμής οι κβαντικές πύλες και δεν επιτρέπουν να επιτευχθεί η ιδανική πιστότητα. Ακόμη οι κβαντικές μνήμες καθώς και οι ανιχνευτές μειώνουν την πιθανότητα επιτυχίας της απόσταξης.
- g) **Εναλλαγή διεμπλοκής:** Η μέθοδος αυτή δημιουργήθηκε ώστε να γίνει εφικτή η αποστολή των qubit σε μεγαλύτερες αποστάσεις. Για να υλοποιηθεί αυτή η τεχνική χρησιμοποιούνται τα ζευγάρια Bell τα οποία δημιουργούνται μέσω ενός σταθμού που βρίσκεται μεταξύ δυο γειτονικών qubits. Σε αυτό το σημείο πρέπει να τονιστεί το γεγονός ότι για το τελευταίο στάδιο της διαδικασίας διανομής κβαντικού κλειδιού δεν είναι απαραίτητη για την εύρεση της περιστροφής του qubit τα αποτελέσματα της μέτρησης του Bell. Τα αποτελέσματα της περιστροφής μπορούν να συμπεριληφθούν στην κλασσική μεταεπεξεργασία.

2.4.3 Πλάνο δημιουργίας

Τώρα που αναλύθηκαν τα τμήματα που θα απαρτίζουν έναν κβαντικό επαναλήπτη σαν επόμενο βήμα θα πρέπει να αναφερθεί ο τρόπος που αυτά θα

πρέπει να συνδιαστούν ώστε να επιτευχθεί η επιθυμητή λειτουργία. Αρχικός στόχος των repeaters είναι να μπορούν να ανταπεξέλθουν στις απαιτήσεις των σημερινών εφαρμογών. Γι' αυτό το λόγο έχει δημιουργηθεί ένα πλάνο σχετικά με τα τεχνολογικά βήματα που πρέπει να γίνουν και χωρίζει τους quantum repeaters σε τρεις κατηγορίες:

1st Generation

Σε αυτή την κατηγορία η λειτουργία των repeaters στηρίζεται στους κβαντικούς επεξεργαστές οι οποίοι έχουν το μειονέκτημα ότι είναι πολύ επιρρεπείς στα σφάλματα. Το πρώτο μέρος της διαδικασίας ξεκινάει με την δημιουργία διαμπλεκόμενων συνδέσμων μεταξύ δυο γειτονικών κόμβων επαναληπτών. Όταν θα έχουν δημιουργηθεί αρκετοί συνδέσμοι εκτελείται η λεγόμενη κβαντική κάθαρση με την οποία γίνεται υψηλότερη η πιστότητα του συνδέσμου. Αφού η υψηλή πιστότητα μεταξύ των δυο γειτονικών κόμβων επικυρωθεί τότε γίνεται η σύνδεση μεταξύ τους μέσω του **entanglement swapping** για να μπορέσει να δωθεί σύνδεση διπλάσιας απόστασης από την αρχική. Σαν δεύτερο μέρος ξανά γίνεται μεταξύ των επόμενων δυο γειτονικών κόμβων η κάθαρση και το swapping για να δημιουργηθούν ακόμα μεγαλύτερης απόστασης σύνδεσμοι. Η διαδικασία αυτή συνεχίζεται έως ότου δημιουργηθεί η διεμπλοκή που απαιτείται μεταξύ της Alice και του Bob. Εάν η κάθαρση ή το swapping αποτύχει σε κάποιο στάδιο τότε η διαδικασία θα πρέπει να σταματήσει και να ξεκινήσει σε αυτό το τμήμα από το πρώτο μέρος.

2nd Generation

Στην προηγούμενη γενιά επαναληπτών χρειάστηκαν να χρησιμοποιηθούν οι πιθανοτικές διαδικασίες κάθαρση και swapping οι οποίες δημιουργούν μεγάλες καθυστερήσεις στο σύστημα μας λόγω του ότι χρειάζεται να γίνει αναμονή για διάδοση του κλασσικού σήματος μεταξύ των δυο κόμβων. Ένας τρόπος για να ξεπεραστούν τα προβλήματα είναι να αντικατεστηθούν οι πιθανοτικές διαδικασίες με ντετερμινιστικές. Για παράδειγμα στην διαδικασία entanglement swapping θα μπορούσε να χρησιμοποιηθεί ντετερμινιστική μέτρηση των ζευγαρίων Bell διότι μπορούν να υπάρξουν πύλες των δυο qubit που να μπορούν να υλοποιηθούν πιστά και αποτελεσματικά. Ακόμη, όσον αφορά τις δυσκολίες της κάθαρσης θα πρέπει να δημιουργηθούν συστήματα μιας κατεύθυνσης ώστε το qubit των διεμπλεκόμενων συνδέσμων να μπορέσει να ξανά χρησιμοποιηθεί χωρίς ανάγκη χρήσης κλασσικής επικοινωνίας μεταξύ των δυο κόμβων. Ένας τρόπος επίλυσης αυτού του προβλήματος είναι να χρησιμοποιηθούν κώδικες διόρθωσης σφάλματος. Ωστόσο η διόρθωση σφαλμάτων δημιουργεί σημαντικούς περιορισμούς στην ποιότητα των συνδέσμων διεμπλοκής που μπορούν να χρησιμοποιηθούν. Οπότε το πρόβλημα που έρχεται να αντιμετωπιστεί με την δεύτερη γενιά επαναληπτών είναι ο χρόνος επικοινωνίας μεταξύ δυο γειτονικών κόμβων. Με τους δυο προαναφερθέντες ντετερμινιστικούς μηχανισμούς δημιουργείται διεμπλεκόμενη σύνδεση σε 1 RRT(ο

χρόνος που χρειάζεται ένα φωτόνιο να διαδοθεί μεταξύ των δυο κόμβων και το κλασσικό κανάλι να αναγγείλει την σύνδεση), και πλεόν είναι εφικτή η σχεδίαση επαναληπτών όπου οι χρόνοι αποθήκευσης μνήμης περιορίζονται κατά πολύ. Παρόλο που είναι απαραίτητη η χρήση κλασσικού καναλιού(το οποίο καθυστερεί το σύστημα μας) η δεύτερη γενιά επαναληπτών βελτιώνει σημαντικά τον χρόνο επικοινωνίας σε σύγκριση με αυτή της πρώτης.

3rd Generation

Όπως αναφέρθηκε και προηγουμένως οι δεύτερης γενιάς κβαντικοί επαναλήπτες έχουν πολλούς περιορισμούς στην εκτέλεση λόγω του ότι χρειάζεται ένα κλασσικό μήνυμα να σταλεί ώστε να προαναγγελθεί η επιτυχημένη μετάδοση διεμπλοκής μεταξύ των δυο κόμβων. Ο λόγος αυτή της καθυστέρησης είναι ότι μέχρι να σταλεί το μήνυμα μέσω του κλασσικού καναλιού το qubit δεν μπορεί να δεχθεί περαιτέρω επεξεργασία. Οπότε σκοπός της τρίτης γενιάς είναι να μπορέσει να αποκλίσει τελείως την κλασσική επικοινωνία. Ο τρόπος για να γίνει αυτό είναι μπορέσει να κωδικοποιηθεί το κβαντικό σήμα ώστε να μπορέσει να σταλεί μέσω των δυο κόμβων χωρίς απώλειες. Με αυτό τον τρόπο θα στέλνεται μεταξύ των κόμβων η κβαντική πληροφορία κρυπτογραφημένη χρησιμοποιώντας qubits(φωτόνια) των οποίων η κωδικοποίηση θα στηρίζεται πάνω στην ανοχή τους στην απώλεια. Έτσι στην συνέχεια θα γίνεται διόρθωση σφάλματος και η πληροφορία θα αποκρυπτογραφείται και θα στέλνεται ακολουθώντας την ίδια διαδικασία στον επόμενο κόμβο. Αυτό θα συνεχιστεί έως ότου ο Bob λάβει το κβαντικό μήνυμα. Είναι σημαντικό να επισημανθεί ότι ο κώδικα ανοχής απώλειας έχει ανοχή λιγότερη από 50%, αλλά είναι αρκετό ώστε οι κάμβοι επαναληπτών να έχουν αρκετή απόσταση μεταξύ τους. Όπως γίνεται αντιληπτό με την Τρίτη γενιά επαναληπτών όχι μόνο θα υπάρξει τεράστια βελτίωση στις επικοινωνίες αλλά θα μπορέσουν να τεθούν σε λειτουργία ακόμη περισσότερες εφαρμογές.

Σκοπός μέχρι στιγμής ήταν να μπορέσουν να επικοινωνήσουν η Alice με τον Bob μέσω ενός καναλιού. Στην πραγματικότητα όμως η Alice και ο Bob θα είναι μέλη ενός πολύ μεγαλύτερου και πολύπλοκου κβαντικού δικτύου του οποίου δεν θα γνωρίζουν την ακριβή του τοπολογία. Έτσι εάν κάποιος θελήσει να εδραιώσει μια σύνδεση σε όλο το δίκτυο κόμβων επαναληπτών μεταξύ της Alice και του Bob ταυτόχρονα με αυτούς τότε θα πρέπει η Alice και ο Bob να χαρτογραφήσουν μια διαφορετική διαδρομή ώστε να μπορέσουν να επικοινωνήσουν. Συνοψίζοντας, θα μπορούσε ένα κβαντικό δίκτυο χρησιμοποιώντας κβαντικούς επαναλήπτες να αντικαταστήσει στο μέλλον ολοκληρωτικά το σημερινό κλασσικό δίκτυο.

Κεφάλαιο 3^ο

3.1 Παραγωγή και μετάδοση κβαντικών κλειδιών

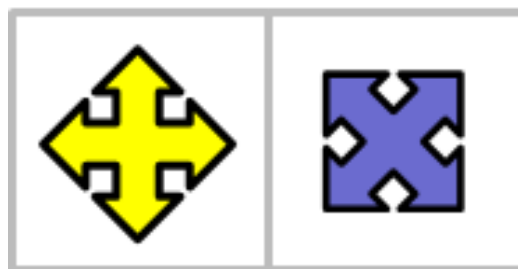
Εισαγωγή

Σκοπός της κρυπτογραφίας είναι η ανάπτυξη , η μελέτη και η χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης ώστε να αποκρυφθούν τα περιεχόμενα μηνυμάτων. Ο Stephen Wiesner εκμεταλλεύτηκε την αδυναμία διακλάδωσης των qubits και δημιούργησε την κβαντική κωδικοποίηση για την δημιουργία κβαντικών χρημάτων τα οποία είναι αδύνατο να πλαστογραφηθούν. Η λειτουργία είναι η εξής:





Η κωδικοποίηση στο πρωτόκολλο αυτό στηρίζεται στον τρόπο πόλωσης των qubits. Δηλαδή η τράπεζα θα δώσει μια επιταγή που θα αποτελείται από μια σειρά qubits (0 ή 1) και κάθε ένα ξεχωριστά από αυτά θα πολωθεί τυχαία με έναν από τους δυο παρακάτω τρόπους:

A) Ευθύγραμμη πόλωση στην οποία τα φωτόνια που αποτελούν τα qubits θα είναι γραμμικώς πολωμένα σε γωνίες 180° ή 90° δηλαδή 1 ή 0 αντίστοιχα.

B) Διαγώνια πόλωση ή βάση Hadamard στην οποία ουσιαστικά θα δημιουργηθεί υπέρθεση στην κατάσταση των φωτονίων και ανάλογα εάν το qubit ήταν 0 ή 1 θα γίνει $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ή $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ και η πόλωση τους θα είναι στις 45° ή 135° αντίστοιχα.



Εικόνα 3-1 Φίλτρα πόλωσης

0		
1		

Εικόνα 3-2 Αντιστοιχία πολώσεων με bit

Σύμφωνα με τα παραπάνω αντιλαμβανόμαστε ότι ανάλογα με την τιμή του κάθε qubit και το φίλτρο στο οποίο θα το προετοιμάσει η τράπεζα, αυτό θα σταλθεί υπό συγκεκριμένες μοίρες.

Qubits	Φίλτρο	Μοίρες
0		90°
1		180°
0		45°
1		135°

Εικόνα 3-3 πίνακας συσχέτισης qubit με φίλτρα και μοίρες

Οι περιπτώσεις που προκύπτουν στον παραλείπτη σε περίπτωση που τοποθετήσει είτε το σωστό είτε το λάθος φίλτρο είναι οι εξής:

1^η) Εάν το qubit έχει πολωθεί με την ευθύγραμμη πόλωση (οριζόντια ή κάθετα) και μετρηθεί με αυτή τότε θα βρεθεί ο σωστός αριθμός.

2^η) Εάν το qubit έχει πολωθεί με την διαγώνια πόλωση και μετρηθεί με αυτή τότε θα βρει τον σωστός αριθμός.

3^η) Εάν το qubit έχει πολωθεί με την ευθύγραμμη πόλωση αλλά μετρηθεί με την διαγώνια τότε είναι σαν ο παραλείπτη να έχει δημιουργεί υπέρθεση στο qubit και έτσι όταν θα κάνει την μέτρηση θα έχει 50% πιθανότητες λάβει το qubit με την σωστή τιμή και 50% όχι.

4^η) Παρόμοια με την 3^η περίπτωση εάν ο αποστολέας πολώσει το qubit με διαγώνια πόλωση και δεν μετρηθεί με αυτή τότε ο παραλήπτης έχει 50% πιθανότητες να πετύχει την σωστή τιμή.

Όπως είναι λογικό μόνο η τράπεζα μπορεί να γνωρίζει τι είδους φίλτρο έχει τοποθετήσει σε κάθε qubit και έτσι εάν κάποιος επίδοξος προσπαθήσει να το αποκρυπτογραφήσει στην τύχη τότε θα έχει 50% πιθανότητα για κάθε qubit να πετύχει το σωστό φίλτρο. Και αν αυτός βάλει το λάθος φίλτρο τότε θα έχει πάλι 50% πιθανότητες να πετύχει το σωστό αποτέλεσμα. Εάν λοιπόν υποθέσουμε ότι θα έχουμε 20 αριθμούς τότε η πιθανότητα να πετύχει κάθε φίλτρο σωστό είναι της μορφής $1/2^n$, όπου για $n=20$ οι πιθανότητες είναι λιγότερες από 1:1000000.

3.2 Πρωτόκολλο BB84

Λειτουργία

Πάνω στην λειτουργία που αναφέρθηκε προηγουμένως στηρίχθηκαν Charles Bennett και Gilles Brassard το 1984 και πρότειναν το πρωτόκολλο BB84. Το πρωτόκολλο αυτό χρησιμοποιείται μόνο για την ασφαλή αποστολή του κλειδιού της κρυπτογράφησης και όχι για το κρυπτογραφημένο περιεχόμενο. Παρακάτω θα δοθεί ένα παράδειγμα στο οποίο αναλύονται τα βήματα τα οποία θα πρέπει να ακολουθήσουν δυο χρήστες η Alice και ο Bob ώστε έχουν πρόσβαση μόνο οι δυο τους στο κρυπτογραφικό κλειδί.

Βήμα 1^ο: Η Alice δημιουργεί μια τυχαία συμβολοσειρά η οποία αποτελείται από n bits

Βήμα 2^ο: Η Alice για κάθε bit δημιουργεί ένα αντίστοιχο qubit και το πολώνει με έναν από τους δυο τρόπους που αναφέρθηκαν πιο πάνω

Βήμα 3^ο: Η Alice στέλνει τα πολωμένα qubit στον Bob (ένα κάθε φορά)

Βήμα 4^ο: Ο Bob όταν λαμβάνει κάθε qubit το μετράει τυχαία με έναν από τους δυο τρόπους και ανακοινώνει στο δημόσιο κανάλι ότι τα έλαβε

Βήμα 5^ο: Στην συνέχεια όταν ο Bob ολοκληρώσει την παραλαβή και την μέτρηση όλων των qubits η Alice ανακοινώνει τον τρόπο πόλωσης που χρησιμοποίησε σε κάθε qubit αλλά όχι την τιμή που είχαν αυτά.

Βήμα 6^ο: Ο Bob κρατάει τα qubit που μέτρησε με την ίδια βάση που έστειλε η Alice. Στην συνέχεια ανακοινώνει στην Alice ποιά qubit έδωσε (δηλαδή δεν τα μέτρησε με την ίδια βάση) ώστε να τα διώξουν. Εάν ο αριθμός των qubits που μετρήθηκε με την ίδια βάση δεν ξεπερνάει μια τιμή που τέθηκε τότε το πρωτόκολλο απορρίπτεται και ξεκινάει από την αρχή. Η τιμή αυτή επιλέγεται να είναι τέτοια ώστε να μην υπάρξει πρόβλημα εάν έχουν γίνει όλα τα βήματα σωστά και δεν έχει παρέμβει κάποιος τρίτος στο σύστημα.

Βήμα 7^ο: Η Alice επιλέγει τυχαία κάποια από τα εναπομείναντα bits και ανακοινώνει στον Bob ποια επέλεξε αλλά όχι την τιμή τους. Στο συγκεκριμένο σημείο έχουν ένα κλειδί το οποίο ονομάζεται **ακατέργαστο κλειδί (raw key)**

Βήμα 8^ο: Στο σημείο αυτό η Alice και ο Bob θέλουν να διαπιστώσουν αν η Eve έχει προσπαθήσει να υποκλέψει το κβαντικό κλειδί. Έτσι επιλέγουν κάποια qubits από το ακατέργαστο κλειδί και εάν όλα είναι στην κατάσταση που έστειλε η Alice τότε συμπεραίνουν ότι δεν έχει γίνει προσπάθεια υποκλοπής. Αν όμως έστω και ένα είναι διαφορετικό τότε συμπεραίνουν ότι η Eve προσπάθησε να υποκλέψει το κβαντικό κλειδί και καλό θα ήταν να επαναλάβουν το BB84

Βήμα 9^ο: Τέλος εάν μέχρι αυτό το σημείο δεν έχει υπάρξει καμία επιπλοκή τότε με τα εναπομείναντα bits από το ακατέργαστο κλειδί δημιουργείται το **κβαντικό κλειδί**.

Όπως αναφέραμε παραπάνω μεταξύ του Bob και της Alice μπορεί να προκύψουν τυχαία κβαντικά λάθη τα οποία μπορεί να πηγάζουν είτε από θόρυβο του κβαντικού συστήματος είτε από την δράση τρίτου (της λεγόμενης Eve). Αυτό θα οδηγήσει στην μη απόλυτη συσχέτιση μεταξύ των κλειδιών μετατόπισης των επικοινωνούντων πλευρών, αλλά και στο ανεπιθύμητο αποτέλεσμα να κατέχει η Eve ένα ποσοστό του κλειδιού. Για να αποκλειστεί αυτή η πιθανότητα εφαρμόζονται αλγόριθμοι διόρθωσης κβαντικών σφαλμάτων και ενίσχυσης της ιδιωτικότητας, αφού η Alice και ο Bob εκτιμήσουν την κβαντική πληροφορία που απέκτησε η Eve κατά την διαδικασία διανομής του κλειδιού. Αυτό το ποσοστό πληροφορίας πρέπει να είναι κάτω από ένα συγκεκριμένο κατώφλι, προκειμένου να θεωρείται ασφαλής η περαιτέρω χρήση του κλειδιού.

Από τα παραπάνω προκύπτει ότι το πρωτόκολλο BB84 απαιτεί τα δύο επικοινωνούντα μέρη να είναι σε θέση να υπολογίζουν το ποσοστό πληροφορίας που κατέχει ο υποκλοπέας. Αυτό είναι εξαιρετικά δύσκολο, δεδομένου ότι ο ρυθμός λαθών που καθορίζει το συγκεκριμένο ποσοστό, δεν προέρχεται μόνο από τη δράση του υποκλοπέα, αλλά και από τις κατασκευαστικές ατέλειες του κβαντικού συστήματος (θόρυβος των ανιχνευτών φωτονίων, λάθη στον έλεγχο της πόλωσης, απώλειες φωτονίων κατά τη διάδοσή τους στις οπτικές ίνες) ή ακόμη και από τον θόρυβο του περιβάλλοντος. Ωστόσο, έχει αποδειχτεί ότι η διανομή κβαντικού κλειδιού είναι απολύτως ασφαλής.

Κβαντικό Κύκλωμα

Για την περιγραφή του κβαντικού κυκλώματος του πρωτοκόλλου BB84 θα χρησιμοποιήσουμε την ορθοκανονική βάση $\{|0\rangle, |1\rangle\}$ ως αντίστοιχη του φίλτρου «+» και η ορθοκανονική βάση $\{|+\rangle, |-\rangle\}$ ως αντίστοιχη του φίλτρου «x». Το κβαντικό κύκλωμα του πρωτοκόλλου BB84 φαίνεται στην παρακάτω εικόνα.



Εικόνα 3-4. Το κβαντικό κύκλωμα του πρωτοκόλλου BB84

Στην είσοδο του κυκλώματος (στα αριστερά) είναι με μεριά του αποστολέα ενώ στα δεξιά του παραλήπτη. Στο σχήμα φαίνεται το σύστημα με το οποίο γίνεται η παραγωγή κλειδιού και περιλαμβάνει ένα qubit στην κατάσταση $|0\rangle$ στο οποίο μπορούν να δράσουν οι κβαντικές πύλες Hadamard και X. Τα κλασσικά bits q και a λειτουργούν ως εξής:

- Όταν το q βρίσκεται στην κατάσταση $\ll 1 \gg$ τότε η πύλη X επενεργεί στο κύκλωμα και μετατρέπει το qubit από $|0\rangle$ σε $|1\rangle$. Ενώ εάν το q βρίσκεται στην κατάσταση $\ll 0 \gg$ τότε η πύλη X δεν ενεργοποιείται και έτσι το qubit της εισόδου παραμένει $|0\rangle$. Με αυτό το τρόπο δίνεται η δυνατότητα στην Alice να μπορεί να ελέγξει αν το qubit που θα αποστείλει θα είναι $|0\rangle$ ή $|1\rangle$.
- Η λειτουργία του bit a είναι όμοια με αυτή το bit q με την διαφορά ότι όταν το a τεθεί $\ll 1 \gg$ τότε στο κύκλωμα επεμβαίνει η πύλη Hadamard. Με το bit αυτό επιλέγεται ποιά ορθοκανονική βάση θα επιλεγεί. Εάν είναι 0 επιλέγεται η βάση $\{|0\rangle, |1\rangle\}$, ενώ εάν είναι 1 η $\{|+\rangle, |-\rangle\}$. Για την τιμή που θα λάβει αυτό το bit εφαρμόζεται συνήθως μια γεννήτρια ψευδοτυχαίων αριθμών.

q	a	$ \psi\rangle$
0	0	$ 0\rangle$
1	0	$ 1\rangle$
0	1	$ +\rangle$
1	1	$ -\rangle$

Πίνακας. Η κατάσταση του qubit $|\psi\rangle$ το οποίο αποστέλλεται για όλους τους συνδυασμούς των bits q και a .

Το qubit μεταφέρεται μέσω το κβαντικού καναλιού προς την δεξιά πλευρά του κυκλώματος την οποία και θεωρούμε πλευρά του Bob. Στο σύστημα αυτό του παραλήπτη υπάρχει μόνο μια πύλη η Hadamard η οποία ελέγχεται με το bit b . Σε αυτό το σημείο αντίστοιχα με προηγουμένως όταν το bit b είναι 1 τότε η πύλη Hadamard επενεργεί στο κύκλωμα ενώ όταν είναι 0 παραμένει ανενεργή. Με αυτό τον τρόπο δίνεται η δυνατότητα στον Bob να επιλέξει τι είδους φίλτρο θα χρησιμοποιήσει σε κάθε qubit. Η τιμή αυτού του bit είναι τυχαία για κάθε qubit το οποίο παραλαμβάνεται και για την παραγωγή του μπορεί να χρησιμοποιηθεί μία γεννήτρια ψευδοτυχαίων αριθμών. Με το bit αυτό αποφασίζεται αν η μέτρηση του $|\psi\rangle$ θα γίνει στην ορθοκανονική βάση $\{|+\rangle, |-\rangle\}$ ($b=1$) ή στην ορθοκανονική βάση $\{|0\rangle, |1\rangle\}$ ($b=0$).

q	a	$ \psi\rangle$	b	Κλειδί
0	0	$ 0\rangle$	0	$ 0\rangle$
0	0	$ 0\rangle$	1	
1	0	$ 1\rangle$	0	$ 1\rangle$
1	0	$ 1\rangle$	1	
0	1	$ +\rangle$	0	
0	1	$ +\rangle$	1	$ 0\rangle$
1	1	$ -\rangle$	0	
1	1	$ -\rangle$	1	$ 1\rangle$

Πίνακας. Η κατάσταση του qubit $|\psi\rangle$ το οποίο μετρίεται για όλους τους συνδυασμούς των bits q, a και b.

Μετά την μετάδοση του qubit $|\psi\rangle$ το κβαντικό κανάλι κλείνει και ανοίγει ένα κλασικό κανάλι για την σύγκριση των κλασικών bits a και b. Αν είναι ίδια, τότε το qubit θα αποτελέσει μέρος του κβαντικού κλειδιού, αν όχι θα απορριφθεί. Τέλος στον παραπάνω πίνακα παρουσιάζεται η κατάσταση του qubit $|\psi\rangle$ για κάθε δυνατή κατάσταση των κλασικών bit q, a και b. Με κόκκινο χρώμα έχουν μαρκιαστεί οι περιπτώσεις των τριών αριθμών οι οποίες θα απορριπτούν (δηλαδή αυτές όπου $a \neq b$).

3.3 Κώδικας BB84

3.3.0.Εισαγωγή

Βήμα 1^ο: Εγκατάσταση προγράμματος anaconda

Αρχικά για να γίνει προσομοίωση ενός κβαντικού υπολογιστή σε έναν κλασικό υπολογιστή θα πρέπει να γίνει εγκατάσταση του προγράμματος anaconda. Μέσω αυτού του προγράμματος μας δίνεται η δυνατότητα να καλέσουμε κατάλληλες βιβλιοθήκες και να προσομοιώσουμε έναν κβαντικό υπολογιστή σε επίπεδο παλμών, κυκλωμάτων αλλά και εφαρμογών.

Βήμα 2º: Εισαγωγή κατάλληλων βιβλιοθηκών

Έχοντας λοιπόν εγκαταστήσει το `anaconda` καλούμε τις απαραίτητες βιβλιοθήκες. Η πρώτη και βασικότερη βιβλιοθήκη είναι η `qiskit`. Με την βοήθεια της `qiskit` μπορούμε να έχουμε πρόσβαση στον τρόπο λειτουργίας ενός κβαντικού υπολογιστή και να επεξεργαστούμε τα qubits όπως εμείς επιθυμούμε. Στην συνέχεια την βιβλιοθήκη `numpy` διότι θα χρειαστούν οι συνάρτησεις τυχαιότητας ώστε τα qubit που θα στείλει η Alice στον Bob αλλά και οι βάσεις να επιλεγούν τυχαία.

```
In [1]: from qiskit import *|
        from numpy.random import randint
```

3.3.1.Πλευρά της Alice

Βήμα 1º : Δημιουργία bit, βάσεων

Με την συνάρτηση `random` δημιουργούνται **100** τυχαίοι αριθμοί (0 ή 1) οι οποίοι είναι τα bit που θα θέλει η Alice να στείλει στον Bob. Στην συνέχεια τοποθετούνται σε μία λίστα που ονομάστηκε **'Alice_bits'** ώστε να μπορέσει σε επόμενο βήμα στο καθένα από αυτά να επενεργήσει μια βάση. Όπως αναφέραμε και παραπάνω σε κάθε qubit θα πρέπει να ενεργήσει μια βάση (ευθύγραμμη ή διαγώνια). Η επιλογή της βάσης γίνεται τυχαία και συμβολίζεται με "0" η ευθύγραμμη και με "1" η διαγώνια. Στην συνέχεια οι βάσεις αποθηκεύονται σε μια λίστα η οποία ονομάζεται **'Alice_bases'**. Θα πρέπει να τονιστεί ότι σε αυτό το σημείο δεν έχει γίνει ακόμη χρήση κβαντικού υπολογιστή. Το μόνο που έχει συμβεί είναι ότι έχουν δημιουργηθεί 2 λίστες από τις οποίες η μια εμπεριέχει την ακολουθία των δυαδικών αριθμών που η Alice επιθυμεί να στείλει στον Bob και η άλλη λίστα εμπεριέχει την κωδικοποίηση (0 ή 1) αναλόγως με το ποιά βάση επιλέγει η Alice κάθε φορά να επενεργήσει σε κάθε qubit. Όπως είναι λογικό δεν γίνεται κάθε φορά που ο χρήστης επιθυμεί να τρέξει το πρόγραμμα να δίνει 100 δυαδικούς αριθμούς και 100 βάσεις. Για αυτό τον λόγο έχει χρησιμοποιηθεί η εντολή `randint` η οποία βρίσκεται μέσα σε έναν βρόγχο και για 100 επαναλήψεις αναπαράγει τυχαία τους αριθμούς (0 ή 1) και τους αποθηκεύει κατάλληλα στις λίστες.

```
#####ALICE PART#####
np.random.seed()
n= 100

#random generation of alice bits
Alice_bits=[]
for i in range(n):
    Alice_bits.append(randint(0,2))

#random generation of alice bases
## Base X is 0 and base Z is 1
Alice_bases=[]
for i in range(n):
    Alice_bases.append(randint(0,2))
```

Βήμα 2º: Προετοιμασία των qubits της Alice

Στην συνέχεια δημιουργείται η συνάρτηση “**alice_prepetation**” η οποία παίρνει σαν ορίσματα το bit που θέλει να στείλει η Alice και την βάση που αυτή θέλει να τοποθετήσει στο qubit. Στην συνέχεια η συνάρτηση αυτή δημιουργεί qubit και του δίνει την αντιστοιχη τιμή ($|0\rangle$ ή $|1\rangle$) ανάλογα με την τιμή του εκάστοτε bit. Έπειτα, ανάλογα με τη βάση που “επέλεξε” στο προηγούμενο βήμα η Alice να τοποθετήσει, θα δράσει σε αυτό η αντίστοιχη πύλη.

```
#####FUNCTIONS#####
##The creation of qc depending on alice base
def alice_preperation(alice_bit, alice_base):
    qc = QuantumCircuit(1,1)
    #Base X
    if alice_base == 0:
        if alice_bit == 0:
            pass
        else:
            qc.x(0) #Pauli_gate X
    #Base Z
    else:
        if alice_bit == 0:
            qc.h(0)
        else:
            qc.x(0)
            qc.h(0)
    qc.barrier()
    return qc
```

1^η Περίπτωση: Εάν η βάση που επιλέχθηκε είναι ευθύγραμμη (δηλ. 0) και το bit είναι και αυτό 0 τότε το qubit παραμένει όπως είναι (δεν επιδράει καμία πύλη πάνω στο qubit).

2^η Περίπτωση: Εάν η βάση είναι ευθύγραμμη αλλά το bit είναι 1 τότε θα πρέπει να επενεργήσει η πύλη “x”. Η πύλη “x” ή αλλιώς Pauli αλλάζει την κατάσταση του qubit από 0 σε 1 ή αντίστροφα. Δηλαδή:

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

3^η Περίπτωση: Σε περίπτωση που η βάση είναι διαγώνια (δηλ. 1) και το bit είναι 0 τότε στο qubit θα επενεργήσει η πύλη “h” (Hadamard). Η πύλη Hadamard δημιουργεί υπέρθεση στο qubit και έτσι αυτό έχει 50% πιθανότητες να είναι 1 και 50% πιθανότητες να είναι 0. Η κατάσταση που θα δημιουργηθεί θα είναι:

- $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

4^η Περίπτωση: Στην τελευταία περίπτωση η βάση είναι διαγώνια (δηλ. 1) και το bit είναι 1, τότε στο qubit θα επενεργήσουν οι πύλες “x” και στην συνέχεια η “h”. Η κατάσταση που θα δημιουργηθεί θα είναι:

- $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Τέλος η σύναρτηση μας επιστρέφει το προετοιμασμένο qubit το οποίο και σε επόμενο βήμα θα σταλεί στον Bob.

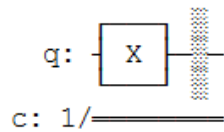
Βήμα 4^ο : Δημιουργία κωδικοποιημένου μηνύματος

Έχοντας λοιπόν δημιουργήσει η σύναρτηση “alice_preparation” καλείται για κάθε ένα bit ξεχωριστά και το κάθε προετοιμασμένο qubit που επιστρέφεται αποθηκεύεται στην λίστα **code_message**.

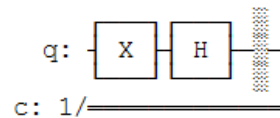
```
#Base placement on alice qubits
code_message= []
for i in range(n):
    code_message.append(alice_preparation(Alice_bits[i], Alice_bases[i]))
#for i in range(n):
    #code_message[0].draw(output='mpl')
```

Στις παρακάτω εικόνες παρουσιάζονται σχηματικά οι βάσεις που τοποθέτησε η Alice στα δυο πρώτα qubits της.

```
code_message[0].draw()
```



```
code_message[1].draw()
```



3.3.2.Πλευρά του Bob

Βήμα 1º: Δημιουργία βάσεων του Bob

Με την σειρά του ο Bob δημιουργεί τις δικές του τυχαίες βάσεις ώστε να μπορέσει να τις συγκρίνει με αυτές της Alice. Αφού τις δημιουργήσει καλεί την συνάρτηση **measure_code** η οποία παίρνει σαν ορίσματα τις βάσεις του Bob και το **code_message** που του έστειλε η Alice. Σε περίπτωση που παρεμβάλεται στο σύστημα η Eve τότε στην συνάρτηση αυτή αντί για το **code_message** της Alice θα πρέπει να τοποθετηθεί το **Eve_results**. Για να είναι πιο ρεαλιστικό η Eve παρεμβάλεται μέσω την μεταβλητής **rand** η οποία παίρνει τυχαία την τιμή 0 ή 1 μέσω της εντολής **randint**. Σε περίπτωση που το **rand = 1** η Eve θα παρεμβληθεί στην επικοινωνία αλλιώς εάν **rand = 0** η Eve δεν θα παρεμβληθεί. Θα γίνει εκτενέστερη ανάλυση στο “**βήμα 3º : Eve_part**” για την διαδικασία που θα πρέπει να ακολουθηθεί σε περίπτωση που επέμβει η Eve στο σύστημα.


```
#####BOB_PART#####
##Bob random bases
Bob_bases=[]
Bob_results = []
Bob_key= []
for i in range(n):
    Bob_bases.append(randint(0,2))
##Compare Bobs bases with the bases alice sended
##Two cases
if rand == 1: #If Eve interfere
    for j in range(n):
        Bob_results.append(measure_code(Bob_bases[j], Eve_results[j]))
else: ##If Eve do not interfere
    for j in range(n):
        Bob_results.append(measure_code(Bob_bases[j], code_message[j]))
```

Βήμα 2º: Μέτρηση των qubits

Η συνάρτηση που καλεί ο Bob είναι η `measure_code` και παρουσιάζεται στην παρακάτω εικόνα. Σε αυτή ανάλογα με την βάση που χρησιμοποίησε ο Bob θα πρέπει να γίνουν και οι αντίστοιχες ενέργειες. Έαν `bob_bases = 0` τότε θα γίνει απλά μέτρηση του qubit και εάν `bob_bases = 1` τότε θα πρέπει πρώτα να επέμβει η πύλη Handamard και στην συνέχεια να γίνει η μέτρηση. Αφού γίνει λοιπον η μέτρηση το αποτέλεσμα αποθηκεύεται και η συνάρτηση επιστρέφει το αποτέλεσμα που θα είναι ο αριθμός 0 ή 1. Το αποτέλεσμα αυτό αποθηκεύεται στην συνέχεια στην λίστα **Bob_results**.

```
##It applies to the coded message the bases that bob choose
def measure_code (bob_bases, code_message):
    measured_bit =[]
    if bob_bases == 0:
        code_message.measure(0,0)
    else:
        code_message.h(0)
        code_message.measure(0,0)
    aer_sim = Aer.get_backend('aer_simulator')
    qobj = assemble(code_message, shots=1, memory=True)
    result = aer_sim.run(qobj).result()
    measured_bit = int(result.get_memory()[0])
    return measured_bit
```

3.3.3.Πλευρά της Eve

Βήμα 1º: Επέμβαση της Eve

Όπως αναφέρθηκε και παραπάνω η Eve μέσω της συνάρτησης randint δρα στο σύστημα τυχαία (εάν randint = 0 δεν δράει εάν randint= 1 δράει)

```
#####EVE_PART#####
##Eve operates randomly
##If random number = 1 Eve operates
rand = randint(0,2)
if rand == 1:
    Eve_bases=[]
    Eve_results = []
    for i in range(n):
        Eve_bases.append(randint(0,2))
##Compare Bobs bases with the bases alice sended
    for j in range(n):
        Eve_results.append(Eve_interference(Eve_bases[j], code_message[j]))
```

Όπως φαίνεται και στην παραπάνω εικόνα η Eve δημιουργεί τυχαία βάσεις με τον ίδιο τρόπο που δημιούργησε και η Alice. Έπειτα παίρνει το code_message που έστειλε η Alice και τις βάσεις που δημιούργησε και χρησιμοποιεί την συνάρτηση **Eve_interference** η οποία θα παρουσιάσεται παρακάτω.

Βήμα 2º: Μέτρηση και προετοιμασία των qubit

Η διαδικασία που επιτελεί αυτή η συνάρτηση είναι παρόμοια με αυτή που χρησιμοποιεί ο Bob (measure_code) με την διαφορά ότι η Eve θα πρέπει στο τέλος της μέτρησης της να ξανά προετοιμάσει τα qubit που μέτρησε. Για να συμβεί αυτό καλείται η συνάρτηση alice_preperation που χρησιμοποίησε η Alice για να προετοιμάσει τα qubit της. Αφού γίνει αυτή η διαδικασία επιστρέφεται η τιμή του κάθε bit και αποθηκεύεται στην λίστα Eve_results και αυτή με την σειρά της στέλνεται στο Bob αντί για το code_message της Alice.

```

##When Eve insert
def Eve_interference(eve_bases, code_message):
    measured_bit = []
    if eve_bases == 0:
        code_message.measure(0,0)
    else:
        code_message.h(0)
        code_message.measure(0,0)
    aer_sim = Aer.get_backend('aer_simulator')
    qobj = assemble(code_message, shots=1, memory=True)
    result = aer_sim.run(qobj).result()
    measured_bit = int(result.get_memory()[0])
    return alice_preperation(measured_bit, eve_bases)

```

3.3.4. Παραγωγή κβαντικών κλειδιών

Για να γίνει η παραγωγή του κλειδιού θα πρέπει να συγκρίνουν η Alice και ο Bob τις βάσεις που χρησιμοποίησαν μέσω ενός κλασικού καναλιού. Καλώντας και οι δυο τη συνάρτηση **remove_bases** για κάθε μια περίπτωση ξεχωριστά διώχνουν τα bit στα οποία χρησιμοποίησαν διαφορετική βάση ώστε να συγκρίνουν αυτά που μέτρησαν με την ίδια βάση. Επειδή το σύστημα μας θεωρείται ότι δεν έχει σφάλματα λόγω θορύβου θα πρέπει εάν δεν έχει παρέμβει η Eve όλα τα qubit που μετρήθηκαν με την ίδια βάση να δώσουν τα ίδια αποτελέσματα και στους δυο.

```

#####Checking bases #####
##Alice Key
Alice_key = []
Bob_key=[]
for i in range(n):
    #Alice key
    if remove_bases(Alice_bases[i], Bob_bases[i], Alice_bits[i]) != None:
        Alice_key.append(remove_bases(Alice_bases[i], Bob_bases[i], Alice_bits[i]))

    #Bob_key
    if remove_bases(Alice_bases[i], Bob_bases[i], Bob_results[i]) != None:
        Bob_key.append(remove_bases(Alice_bases[i], Bob_bases[i], Bob_results[i]))

##It removes bases that are different
def remove_bases (alice_bases, bob_bases, bit):
    if alice_bases == bob_bases:
        return bit

```

3.3.5.Έλεγχος κλειδιού

Τέλος να γίνεται έλεγχος εάν το κλειδί της Alice είναι ίδιο με του Bob εάν όχι τότε έχει παρέμβει κάποιος τρίτος στο σύστημα (Eve) και ο κώδικας μας εμφανίζει το μήνυμα "The key is safe" ενώ εάν έχει παρέμβει στο σύστημα η Eve θα εμφανίζει "Error: Alice and Bob have different keys"

```
safe = 1
##Test if the protocol works properly
for i in range(len(Alice_key)):
    if Alice_key[i] != Bob_key[i]:
        print('Error: Alice and Bob have different keys')
        safe = 0
        break
if safe == 1:
    print('The key is safe')
```

Κεφάλαιο 4^ο

4.1.Πρωτόκολλο E91

Εισαγωγή

Η κρυπτογραφία όπως προαναφέρθηκε αποτελεί την βάση της ασφαλούς επικοινωνίας. Έχοντας αυτό σαν στόχο στα τέλη του 1991 ο επιστήμονας Ekert πρότεινε ένα πρωτόκολλο κρυπτογραφίας το οποίο να στηρίζεται στην κβαντική διεμπλοκή. Εμπνευσμένος από το δημοσιευμένο άρθρο EPR paradox του Einstein-Podolsky-Rosen δημιούργησε το E91 protocol. Όπου "E" είναι το αρχικό του ονόματος Ekert και 91 η χρονιά ανακάλυψης του πρωτοκόλλου.

Σε σύγκριση με το BB84 protocol στο οποίο η Alice προετοιμάζει τα qubits με τις κατάλληλες βάσεις και στην συνέχεια τα στέλνει στο Bob, το E91 protocol χρησιμοποιεί EPR ζεύγη κατά την επικοινωνία. Τα ζεύγη συνήθως δημιουργούνται από μια πηγή η οποία βρίσκεται στο ενδιάμεσο της απόστασης του Bob και της Alice η οποία και στέλνει στον καθένα από ένα διεμπλεκόμενο qubit. Όμως το πρόβλημα που παρουσιάζεται βρίσκεται στην δυσκολία διατήρησης της διεμπλοκής μεταξύ των δυο διεμπλεκόμενων ζευγών. Με άλλα λόγια το E91 πρωτόκολλο είναι πολύ πιο δύσκολο να εφαρμοστεί από το BB84 πρωτόκολλο.

Το αρχικό πρόβλημα που παρουσιάστηκε στο πρωτόκολλο E91 ήταν πως δεν υπήρχε μηχανισμός ώστε να μπορέσει να εντοπιστεί ο βαθμός ιδιοκτητικότητας που έχουν τα ζεύγη φωτονίων αλλά ούτε και μπορούσε να γίνει διόρθωση σφαλμάτων. Έτσι από τον Ekert ήρθε στην επιφάνεια η ανακάλυψη ότι η CHSH inequality (που μέχρι τότε χρησιμοποιούνταν μόνο για κλασσικά προβλήματα) δίνει συγκεκριμένα αποτελέσματα όταν υπήρχαν ζεύγη φωτονίων τα οποία δεν παραβιάζονται.

Ωστόσο, κατά την θεωρητική ανάλυση του πρωτοκόλλου δεν λαμβάνεται υπόψη η παρουσία-παρεμβολή της Eve και αγνοούνται τα σφάλματα λόγω θορύβου κάτι το οποίο δεν μπορεί να αγνοηθεί κατά το πρακτικό κομμάτι. Για εφαρμογές σε πραγματικό περιβάλλον θα πρέπει να ληφθούν υπόψη όλοι οι παράμετροι.

Έχοντας λοιπόν σαν εργαλείο την CHSH inequality το πρωτόκολλο E91 εκμεταλλεύεται τις ιδιότητες της χρησιμοποιώντας τον βαθμό παραβίασης που προσφέρει αυτή η ανισότητα σαν έλεγχο του κλειδιού. Ο λόγος ο οποίος η ανισότητα αυτή μπορεί να συνεισφέρει στον έλεγχο του κλειδιού εμπνεύστηκε από μια έννοια που ονομάζεται *monogamy of entanglement* ή αλλιώς μονογαμία της διεμπλοκής. Πιο αναλυτικά όταν σε ένα ζεύγος διεμπλοκόμενων φωτονίων αλληλεπιδράσει ένα ακόμη φωτόνιο (για παράδειγμα ένα φωτόνιο σταλμένο από την Eve) τότε αυτή η ανισότητα παρουσιάζει τιμές μικρότερες από τις επιθυμητές.

Παρόλο που το πρωτόκολλο BB84 και το E91 χρησιμοποιούν διαφορετικούς κβαντικούς μηχανισμούς κατά την υλοποίηση τους στην ουσία και τα δυο σχετίζουν την ασφάλεια του κλειδιού τους με βάση το σφάλμα που παρουσιάζει ο μηχανισμός τους. Για αυτό το λόγο και τα δυο πρωτόκολλα θεωρούνται ισοδύναμα και η διεμπλοκή θεωρείται απλά σαν ένας ακόμη τρόπος συσχέτισης δυο κόμβων.

CHSH ανισότητα

Η ιδέα πως η πληροφορία σε ένα κβαντικό σύστημα μπορούσε να μοιραστεί μεταξύ σωματιδίων ακαριαία, και γρηγορότερα από την ταχύτητα του φωτός, βρισκόταν σε αντίφαση με την αρχή της τοπικότητας. Ήταν κάποιοι φυσικά που πίστευαν ότι αντί τα σωματίδια να έχουν μόνο την ικανότητα διεμπλοκής και της ακαριαίας μετάδοσης της πληροφορίας, πρέπει να διαθέτουν και κάποιες "κρυφές μεταβλητές" οι οποίες θα μπορούσαν κατά την διεμπλοκή να αποδώσουν κάποιες πληροφορίες σχετικά με τα σωματίδια. Αυτή ήταν μια ντετερμινιστική οπτική γωνία η οποία υποστήριζε ότι οι ιδιότητες ενός κβαντικού συστήματος (spin, θέση, πόλωση, κ.α) είναι προκαθορισμένες και οι τιμές έχουν δημιουργηθεί ανεξαιρέτως εάν έχει γίνει μέτρηση ή όχι. Φυσικά η κβαντική θεωρία υποστηρίζει ότι οι ιδιότητες

του κβαντικού συστήματος δεν είναι προκαθορισμένες και πως η τιμές δεν έχουν δημιουργηθεί μέχρις ότου γίνει η μέτρηση.

Στα μισά περίπου του 20^{ου} αιώνα, ένα φυσικός ονόματι John Bell δημοσίευσε ένα άρθρο στο οποίο παρουσίασε μια μαθηματική διατύπωση για την αρχή τοπικότητα βασισμένος στην ύπαρξη κρυφών μεταβλητών. Η μαθηματική διατύπωση είναι μια ανισότητα η οποία μπορεί να εφαρμοστεί σε μικροσκοπικό επίπεδο. Ωστόσο κάθε φορά που πήγαινε να εφαρμοστεί σε ένα κβαντικό σύστημα αυτή αποτύγχανε να επιφέρει τα επιθυμητά αποτελέσματα. Έτσι με την σειρά τους και στηριζόμενοι σε αυτή την μαθηματική διατύπωση ο John Clauser, Michael Horne, Abner Shimony, και Richard Hol δημιούργησαν την CHSH inequality η οποία και πήρε το όνομα της από τα αρχικά τους. Η CHSH ανισότητα ορίζεται από μια παράμετρο "S" για την οποία θα πρέπει να ισχύει $|S| \leq 2$ και

$$S = E(\alpha, \beta) + E(\alpha', \beta) - E(\alpha, \beta') + E(\alpha', \beta')$$

Οι όροι $E(\alpha, \beta)$, $E(\alpha', \beta)$ κ.λ.π, είναι η κβαντική συσχέτιση μεταξύ σωματιδιακών ζεύγων, και ορίζεται ως μια προσδοκώμενη τιμή που θα πρέπει να παράγει το αποτέλεσμα του πειράματος και παράγονται από τον τύπο:

$$E(\alpha, \beta) = \frac{n_{00} - n_{01} - n_{10} + n_{11}}{n_{00} + n_{01} + n_{10} + n_{11}}$$

Όπου η είναι η πιθανότητα ο συνδιασμός των πολώσεων α, β να παράγει το αποτέλεσμα 00, 01, 10 ή 11.

Ο υπολογισμός του S απαιτεί 16 διαφορετικούς προσανατολισμούς πόλωσης. Για τα α , α' , β και β' θα επιλεγούν οι γωνίες 0°, 45°, 22.5° και 67.5° αντίστοιχα. Ακόμη θα πρέπει να κρατήσουμε τις τιμές όπου ο πολωτής A διατηρεί τις γωνίες 0°, 45°, 90° και 135° ενώ παράλληλα ο πολωτής B αυξάνει την τιμή της πόλωσης του από 0° έως 360° κατά 10° κάθε φορά.

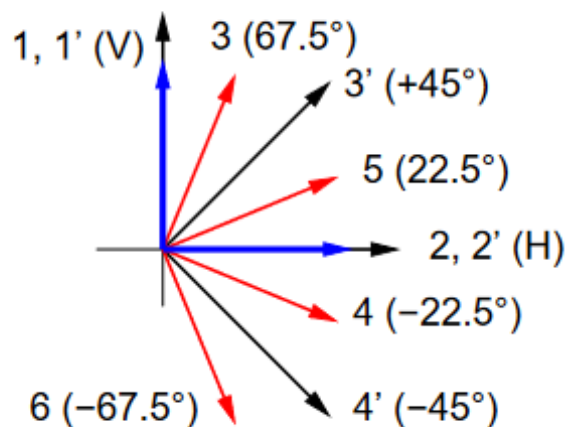
Μια ακόμα σημαντική παράμετρος του πειράματος είναι η ορατότητα (V). Η ορατότητα αποτελεί την μέτρηση της συσχέτισης των πόλωσης μεταξύ 2 διεμπλεκόμενων φωτονίων. Αυτή καθορίζεται από την μέγιστη τιμή της ποσότητα S: $S_{\max} \leq 2\sqrt{2}V$ όπου $V \leq 0.71$ και υπολογίζεται από την σχέση:

$$\frac{C_{\max} - C_{\min}}{C_{\max} + C_{\min}}$$

Πειραματικά για να επιβεβαιωθεί παραβίαση στα ζευγάρια Bell, θα πρέπει το S να είναι μικρότερο από 2 και η ορατότητα (V) να είναι μικρότερη από 0.71.

Λειτουργία πρωτοκόλλου E91

Αφού έγινε ανάλυση της CHSH ανισότητας σειρά έχει η διαδικασία που ακολουθείτε ώστε να υλοποιηθεί το πρωτόκολλο E91. Η ιδέα για την υλοποίηση του πρωτοκόλλου είναι να χρησιμοποιηθούν τρεις βάσεις πόλωσης a, b, c στην πλευρά της Alice και δυο βάσεις πόλωσης a', b' στην πλευρά του Bob. Όλες μαζί δίνουν 10 διαφορετικές περιπτώσεις αφού κάθε πόλωση έχει δυο πιθανές ορθογώνιες πολώσεις. Στην παρακάτω εικόνα παρουσιάζονται τα διαφορετικά είδη πολώσεων όπου με χρώμα είναι οι καταστάσεις a, b, c και με μαύρο οι a', b' .



Έτσι τα βήματα που ακολουθούνται για την υλοποίηση του πρωτοκόλλου είναι τα εξής:

Βήμα 1°: Μια πηγή δημιουργεί ένα EPR ζευγάρι φωτονίων για παράδειγμα $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, και στέλνει το ένα σωματίδιο στην Alice ($|\psi^+\rangle_1$) και το δεύτερο σωματίδιο στον Bob ($|\psi^+\rangle_2$).

Βήμα 2°: Η Alice και ο Bob τυχαία επιλέγουν μια βάση από τις προαναφερθείσες ώστε να μετρήσουν το σωματίδιο που έλαβαν.

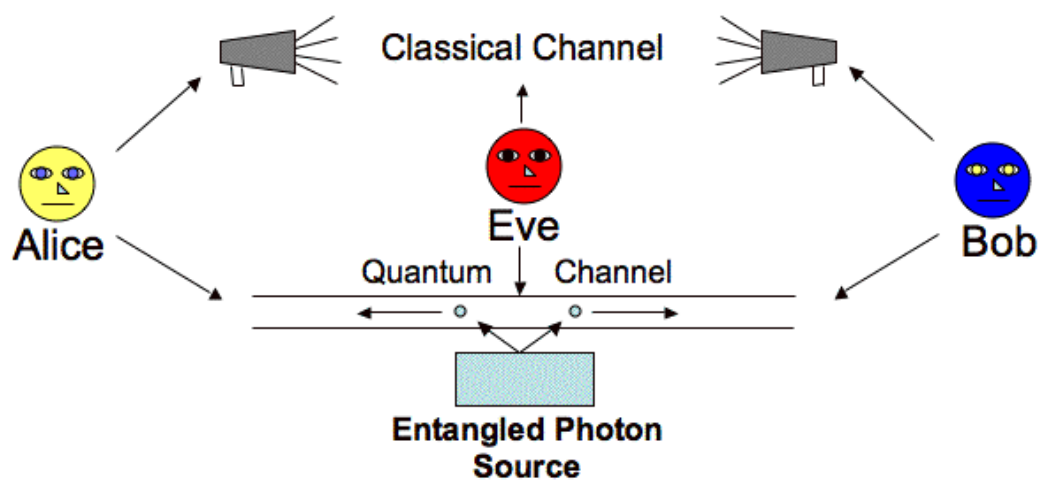
Βήμα 3°: Καταγράφουν το αποτέλεσμα της μέτρησης τους και μέσω ενός κλασσικού καναλιού επικοινωνούν οι δυο πλευρές σχετικά με το ποια βάση χρησιμοποίησε ο καθένας.

Βήμα 4°: Η Alice και ο Bob γνωρίζουν τις βάσεις που κάθε πλευρά χρησιμοποίησε για κάθε qubit και έτσι χωρίζουν σε δυο ομάδες τα αποτελέσματα. Η πρώτη ομάδα ονομάζεται **raw key** qubits G_k και χρησιμοποιείται για την παραγωγή του κλειδιού. Σε αυτή την ομάδα οι βάσεις που χρησιμοποιήθηκαν είναι η a από την μεριά της Alice και η a' από την μεριά του Bob. Αυτές οι δυο βάσεις είναι

πανομοιότυπες και αντιστοιχούν στην οριζόντια- κάθετη πόλωση και έτσι οδηγούν σε συσχετιζόμενα αποτελέσματα. Σε κάθε άλλη περίπτωση βάσεων τα αποτελέσματα αποθηκεύονται στην δεύτερη ομάδα η οποία ονομάζεται ομάδα δόλωμα ή αλλιώς decoy qubits G_d .

Βήμα 5°: Σε αυτό το σημείο θα επιλεγεί ένας συνδυασμός βάσεων που χρησιμοποιήθηκαν, από την ομάδα των decoy qubits τέτοιος ώστε να ικανοποιείται κάθε φορά η CHSH ανισότητα. Όπως προαναφέρθηκε η CHSH ανισότητα στηρίζεται στον τύπο:

$$S = E(b, a') + E(b, b') + E(c, a') - E(c, b'), \text{ όπου } S \geq 2$$



Εικόνα 4-1 Κβαντική κρυπτογραφία πρωτόκολλο E91

Βήμα 6°: Στην συνέχεια εάν ο συντελεστής S είναι μεταξύ 2 και $\sqrt{2}$ τότε δεν υπάρχει παραβίαση του συστήματος από κάποιο τρίτο πρόσωπο (Eve) ενώ εάν το S είναι μικρότερο του 2 τότε λέμε ότι υπάρχει παραβίαση του συστήματος. Σε περίπτωση λοιπόν που υπάρχει παραβίαση το πρωτόκολλο σταματάει και η διαδικασία ξεκινάει από την αρχή ενώ εάν δεν υπάρχει παραβίαση τότε σαν κλειδί χρησιμοποιείται το ακατέργαστο κλειδί που αναφέρθηκε προηγουμένως και η επικοινωνία ξεκινάει.

Θόρυβος στο πρωτόκολλο E91

Μια διευκρίνιση που θα πρέπει να δωθεί είναι πως σε πραγματικό περιβάλλον τα σφάλματα και οι προσπάθειες παρεμβολής τρίτων δεν μπορούν να εξαληφθούν σε μια επικοινωνίας. Το ενδεχόμενο να προκαλεί σφάλμα (ber) επικοινωνίας μόνο η Eve υπάρχει μόνο σε ένα ιδανικό περιβάλλον, όπου και μπορούμε να πούμε με σιγουριά ότι εάν το σφάλμα είναι διάφορο του μηδενός

($\text{ber} \neq 0$) τότε σίγουρα υπάρχει παρεμβολή τρίτου. Ωστόσο, εάν λάβουμε υπόψην το σφάλμα τότε αυτό προκαλείται και από την παρεμβολή της Eve αλλά και από τον θόρυβο του συστήματος. Δηλαδή θα υπάρχει σφάλμα ακόμη και εαν δεν υπάρχει παρεμβολή από κάποιον τρίτο, το οποίο σημαίνει ότι το αρχικό E91 πρωτόκολλο δεν μπορεί να χρησιμοποιηθεί σε περιβάλλον με θόρυβο. Γιαυτό οι μηχανισμοί για το εαν υπάρχει θόρυβος σε ένα κβαντικό κανάλι θα πρέπει να βελτιωθούν ώστε να προστατευτεί η πληροφορία. Στην διαδικασία της κβαντικής επικοινωνίας το επίπεδο σφάλματος του Bit που προκαλείται από θόρυβο μπορεί να φανεί μόνο ως ber_0 , και το ber_0 είναι πάντα σταθερό και αμετάβλητο. Αν υπάρξει παρεμβολή της Eve τότε το επίπεδο ber_i θα αυξηθεί και θα γίνει μεγαλύτερο από το ber_0 . Οποιοσδήποτε και εαν είναι ο λόγος που προκλήθηκε αυτή η κατάσταση, η Alice και ο Bob αποφασίζουν ότι το κανάλι δεν είναι ασφαλές και διακόπτουν την επικοινωνία τους.

Το αρχικό πρωτόκολλο E91 χρησιμοποιεί μια ομάδα δόλωμα G_d για να ανιχνεύσει την παρεμβολή τρίτων. Ωστόσο σε αυτή την διπλωματική θα χρησιμοποιηθεί το **raw key** για να αναλυθεί το επίπεδο σφάλματος των qubit που προκλήθηκε από την Eve και όχι από τον θόρυβο.

Κατά την διαδικασία ανάλυσης της ασφάλειας του συστήματος μια λογική υπόθεση είναι πως στο σύστημα υπάρχει συνεχώς θόρυβος. Παρόλο που η πραγματική τιμή του θορύβου είναι μεταβλητή, η μέγιστη ή η μέση τιμή θορύβου μπορεί να διεξαχθεί. Για να διασφαλιστεί όμως η ασφάλεια στο πρωτόκολλο E91 θα πρέπει να λειφθεί υπόψην η μέγιστη τιμή.

Ο θόρυβος σε ένα περιβάλλον με θόρυβο θα δημιουργήσει τα ίδια αποτελέσματα σε κάθε σωματίδιο στο οποίο οποίο επενεργούν φίλτρα. Το αποτέλεσμα θα είναι σε κάθε σωματίδιο που επενεργεί φίλτρο να εκτρέπεται κατά μια γωνία θ αριστερά ή δεξιά. Τα αποτελέσματα αυτής της περιστροφής φαίνονται στον παρακάτω πίνακα.

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Υπό την επιρροή του θορύβου στην περιστροφή οι κβαντικές καταστάσεις γίνονται:

$$\begin{aligned} |0\rangle &\rightarrow \cos\theta|0\rangle + \sin\theta|1\rangle \\ &= \frac{\cos\theta + \sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta - \sin\theta}{\sqrt{2}}|-\rangle \end{aligned}$$

$$\begin{aligned} |1\rangle &\rightarrow -\sin\theta|0\rangle + \cos\theta|1\rangle \\ &= \frac{\cos\theta - \sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta + \sin\theta}{\sqrt{2}}|-\rangle \end{aligned}$$

$$|+\rangle \rightarrow \frac{\cos \theta - \sin \theta}{\sqrt{2}}|0\rangle + \frac{\cos \theta + \sin \theta}{\sqrt{2}}|1\rangle$$

$$= \cos \theta |+\rangle - \sin \theta |-\rangle$$

$$|+\rangle \rightarrow \frac{\cos \theta + \sin \theta}{\sqrt{2}}|0\rangle - \frac{\cos \theta - \sin \theta}{\sqrt{2}}|1\rangle$$

$$= \cos \theta |-\rangle - \sin \theta |+\rangle$$

Όταν δεν υπάρχει θόρυβος τότε το $\theta = 0$, και οι τέσσερις κβαντικές καταστάσεις δεν θα αλλάξουν. Όσο μεγαλύτερη είναι η επίδραση του θορύβου τόσο μεγαλύτερη είναι η πιθανότητα να αλλάξει η κβαντική κατάσταση σε άλλη κατάσταση. Γιαυτό το επίπεδο του θορύβου (ϵ) μπορεί να περιγραφεί σαν ένα αποτέλεσμα που μπορεί να δημιουργηθεί μόνο από θόρυβο και η τιμή του πρέπει να αναλύεται προσεκτικά.

Όταν το επίπεδο του θορύβου (ϵ) υπολογιστεί δεν θα αλλάξει κατά την διάρκεια του πρωτοκόλλου E91. Η παρεμβολή της Ene θα δημιουργήσει διαφορετικό σφάλμα στο qubit (ber_i) το οποίο θα πρέπει να ικανοποιεί τον τύπο $ber_i \geq \epsilon$.

Στόχος είναι να βρεθεί η σχέση μεταξύ του σφάλματος του qubit (ber_i) και του επιπέδου του σφάλματος ϵ . Με άλλα λόγια, θα πρέπει να βρούμε την μαθηματική συσχέτιση μεταξύ ber_i και θ . Στο πρακτικό κομμάτι όπου η Ene παρεμβάλεται στο σύστημα επικοινωνίας πρέπει να αναλυθεί πόση πληροφορία μπορεί να υποκλέψει η Ene. Όπως είναι εύκολα αντιληπτό η Ene δεν μπορεί να διαβάσει το μυστικό μήνυμα εάν δεν έχει ολόκληρο το κλειδί. Δηλαδή εάν η πληροφορία που δέχεται η Ene είναι $I < 1$, υποδηλώνει πως η Ene μπορεί να έχει υπό την κατοχή της μόνο ένα μέρος του κλειδιού και πως δεν μπορεί να διαβάσει το μυστηκό κλειδί, τότε το πρωτόκολλο E91 είναι ασφαλές.

4.2 Κώδικας πρωτοκόλλου E91

Εισαγωγή συναρτήσεων

Σαν πρώτο βήμα θα πρέπει να καλεστούν οι κατάλληλες συναρτήσεις ώστε να μπορέσει να γίνει προσομοίωση κβαντικού υπολογιστή σε κλασσικό υπολογιστή. Για να γίνει αυτό θα πρέπει να καλέσουμε διάφορες συναρτήσεις από την βιβλιοθήκη της rython την qiskit. Ακόμη θα πρέπει να χρησιμοποιηθεί η εντολή `IBMQ.load_account` ώστε να γίνει εφικτή η πρόσβαση στο σύστημα και στον προσομοιωτή που παρέχει η IBM Quantum. Έτσι το σύστημα μπορεί να αλληλεπιδράσει και να ανακτήσει εργασίες που συσχετίζονται με την εκτέλεση κβαντικών κυκλωμάτων.

```

from qiskit import *
import numpy as np
from random import randint
%matplotlib inline
from qiskit.tools.visualization import plot_histogram
import matplotlib.pyplot as plt
IBMQ.load_account()
simulator = Aer.get_backend('aer_simulator')

```

Δημιουργία διεμπλοκής

Έχοντας λοιπόν τις κατάλληλες βιβλιοθήκες σειρά έχει η δημιουργία μιας συνάρτησης η οποία θα έχει τον ρόλο της πηγής που θα δημιουργεί EPR ζεύγη. Η συνάρτηση αφού δημιουργήσει διεμπλοκή σε δυο qubit θα επιστρέφει το κβαντικό κύκλωμα.

```

#####Step_1#####
#Creation of entanglement
def creation_of_qubits():
    qc = QuantumCircuit(2,2)
    qc.h(0)
    qc.cx(0,1)
    qc.barrier()
    return qc

```

Δημιουργία των βάσεων Alice&Bob

Όπως αναφέραμε και παραπάνω η Alice και ο Bob θα πρέπει να επιλέγουν τυχαία την βάση που θα χρησιμοποιήσουν κάθε φορά. Για να γίνει πρακτικά αυτό θα πρέπει να χρησιμοποιηθεί η εντολή randint η οποία θα παράγει για την Alice τυχαία αριθμούς από το 1 έως το 3 και για τον Bob από το 1 έως το 2. Ανάλογα λοιπόν με το ποιος αριθμός θα επιλεγεί κάθε φορά θα χρησιμοποιείται και η κατάλληλη βάση. Οι βάσεις που μπορεί να επιλέξει η Alice είναι τρεις. Η πρώτη βάση είναι η I (αδράνειας) η οποία δεν επηρεάζει κάπως το qubit και το αφήνει ως

έχει. Η δεύτερη βάση που θα χρησιμοποιηθεί στο παρών παράδειγμα επεμβαίνει με τέτοιο τρόπο στο qubit ώστε να το στρέψει κατά -22.5° και αντίστοιχα η Τρίτη κατά -66.5° . Από την άλλη ο Bob θα πρέπει να επιλέξει ανάμεσα σε δυο βάσεις εκ των οποίων η πρώτη είναι η Hadamard και η δεύτερη στρέφει την κατάσταση του qubit κατά 45° . Στην συνέχεια γίνεται μέτρηση των δυο qubit και η συνάρτηση επιστρέφει το κβαντικό κύκλωμα που υλοποιήθηκε αφού επέμβηκαν οι βάσεις, αλλά και τις βάσεις που χρησιμοποιήθηκαν για τα δυο αυτά qubit.

```
#####Step_2#####
###Creation of Alice and Bob basis
def apply_filters(qc):
    rand_A, rand_B = randint(1,3), randint(1,2)
    ###Alice Basis###
    if rand_A == 1:
        qc.i(0)
    elif rand_A == 2:
        qc.ry(-22.5,0)
    elif rand_A == 3:
        qc.ry(-67.5,0)
    ###Bob Basis###
    if rand_B == 1:
        qc.h(1)
    elif rand_B == 2:
        qc.ry(45, 1)
    qc.measure(range(2),range(2))
    return qc,rand_A, rand_B
```

Έλεγχος βάσεων και δημιουργία κλειδιού

Σε αυτό το σημείο θα πρέπει να γίνει έλεγχος των βάσεων που χρησιμοποίησαν σε κάθε περίπτωση η Alice και ο Bob. Χρησιμοποιείται ένας βρόγχος ο οποίος κάνει 100 επαναλήψεις. Σε κάθε επανάληψη καλούνται οι συναρτήσεις που αναφέρθηκαν προηγουμένως οι οποίες επιτελούν τις λειτουργίες που αναφέρθηκαν παραπάνω. Ο αριθμός επαναλήψεων είναι τυχαίος και όσο μεγαλύτερος είναι τόσο πιο ασφαλές θα είναι το κλειδί, αφού η ανισότητα CHSH που θα αναφερθεί και στην συνέχεια θα έχει περισσότερα δείγματα. Στο κομμάτι αυτό του κώδικα γίνει θεωρητικά η συνεννόηση μεταξύ ενός κλασσικού καναλιού μεταξύ της Alice και του Bob σχετικά με το πια βάση χρησιμοποίησαν. Ανάλογα με

το πια βάση χρησιμοποίησε ο καθένας κάθε φορά το αντίστοιχα αποτέλεσμα της μέτρησης των qubits θα αποθηκευτεί σε διαφορετική λίστα. Έαν λοιπόν οι βάσεις είναι η I της Alice και η Hadamard του Bob τότε τα αποτελέσματα φυλάσσονται σε μια λίστα η οποία εάν το σύστημα δεν έχει παραβιαστεί εν τέλη θα είναι και το κλειδί της επικοινωνίας τους. Εάν όμως δεν είναι ο συνδιασμός αυτών των δυο βάσεων που επέλεξαν οι δυο πλευρές τότε ανάλογα με την επιλογή που έγινε θα αποθηκευτούν τα αποτελέσματα σε διαφορετικές λίστες. Ο λόγος που πρέπει να συμβεί αυτό είναι διότι το απαιτεί η CHSH ανισότητα ο τύπος της οποίας είναι:

$$S = E(b, a') + E(b, b') + E(c, a') - E(c, b')$$

Όπως φαίνεται από τον τύπο θα πρέπει για κάθε δείγμα του S να υπάρχουν 4 περιπτώσεις βάσεων

```
for i in range(100):
    qc, base_A, base_B = apply_filters(creation_of_qubits())
    if base_A == 1:
        secret_key.append(qc)
    elif base_A == 2 and base_B == 1:
        test_key1.append(qc)
    elif base_A == 2 and base_B == 2:
        test_key2.append(qc)
    elif base_A == 3 and base_B == 1:
        test_key3.append(qc)
    elif base_A == 3 and base_B == 2:
        test_key4.append(qc)
```

Αφού λοιπόν τελειώσει η λειτουργία του βρόγχου και αποθηκευτούν τα αποτελέσματα στις εκάστοτε λίστες σειρά έχει να δημιουργηθεί μια ακόμη λίστα στην οποία θα ταξινομούνται με την σειρά τα στοιχεία κάθε λίστας **test_key**:

```
compare = [len(test_key1), len(test_key2), len(test_key3), len(test_key4)]

for i in range(min(compare)):
    test_key.append(test_key1[i])
    test_key.append(test_key2[i])
    test_key.append(test_key3[i])
    test_key.append(test_key4[i])
```

Με τις εντολές που παρουσιάζονται στην παρακάτω εικόνα γίνεται προσομοίωση του κβαντικού υπολογιστή. Πιο αναλυτικά για κάθε στοιχείο της λίστας test_key γίνεται προσομοίωση και μας δίνεται το πιθανοτικό αποτέλεσμα που θα είχε αυτό το στοιχείο εάν έτρεχε σε κβαντικό υπολογιστή. Η προσομοίωση αυτή γίνεται για

κάθε στοιχείο 1024 φορές και από αυτές μας δίνεται ένα αποτέλεσμα πόσες φορές προέκυψε $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

```
result_ideal = simulator.run(test_key).result()
res = result_ideal.get_counts()
```

Η εντολή `result_ideal.get_counts()` επιστρέφει μια λίστα η οποία περιέχει μέσα λεξικά στα οποία το κλειδί είναι το αποτέλεσμα της κάθε μέτρησης και σαν τιμή η φορές που αυτό προέκυψε από τις 1024 δοκιμές που έγιναν.

```
print(res)
```

```
[{'10': 386, '01': 377, '11': 135, '00': 126}, {'01': 248, '11': 276, '10': 264, '00': 236},
```

Υπολογισμός CHSH

Για τον υπολογισμό της CHSH ανισότητας δημιουργήθηκε η συνάρτηση **`compute_chsh_witness`** η οποία δέχεται σαν όρισμα την λίστα `res`. Η συνάρτηση αυτή προσομοιώνει την λειτουργία της εξίσωσης:

$$S = E(b, a') + E(b, b') + E(c, a') - E(c, b')$$

Όπως αναφέραμε και προηγουμένως η λίστα `res` περιέχει ταξινομημένα ανά τετράδες τις περιπτώσεις που χρησιμοποιήθηκαν οι βάσεις όπως παρουσιάζονται από τον παραπάνω τύπο. Για παράδειγμα το πρώτο λεξικό της λίστας περιέχει τα αποτελέσματα της μέτρησης που έγιναν όταν η Alice χρησιμοποίησε την βάση b και ο Bob την βάση a' . Έτσι δημιουργείται μια λούπα η οποία αυξάνεται με βήμα 4 και κάθε φορά επιλέγονται τα εκάστοτε 4 λεξικά για επεξεργασία. Σε αυτό το σημείο θα πρέπει να αναφερθεί ότι το $E(a,b)$ υπολογίζεται από τον τύπο:

$$E(a,b) = \frac{n_{00}-n_{01}-n_{10}+n_{11}}{n_{00}+n_{01}+n_{10}+n_{11}}$$

Έτσι από το κάθε λεξικό θα προστίθονται οι φορές που το αποτέλεσμα ήρθε 00 ή 11 και θα αφαιρούνται οι φορές που αυτό ήρθε 01 ή 10 και στο τέλος θα διαιρείται όλο αυτό με το συνολικό αριθμό δηλαδή το 1024. Στην παρακάτω εικόνα παρουσιάζεται ο κώδικας για την διαδικασία που περιγράφηκε.

```
def compute_chsh_witness(res):
    CHSH = []
    for i in range(0, len(res), 4):
        chsh = 0
        for key, values in res[i].items():
            if key == '11' or key == '00':
                chsh -= values
            else:
                chsh += values
        for key, values in res[i+1].items():
            if key == '11' or key == '00':
                chsh -= values
            else:
                chsh += values
        for key, values in res[i+2].items():
            if key == '11' or key == '00':
                chsh -= values
            else:
                chsh += values
        for key, values in res[i+3].items():
            if key == '11' or key == '00':
                chsh += values
            else:
                chsh -= values
        CHSH.append(chsh/1024)
    return CHSH

CHSH1_ideal = compute_chsh_witness(res)
```

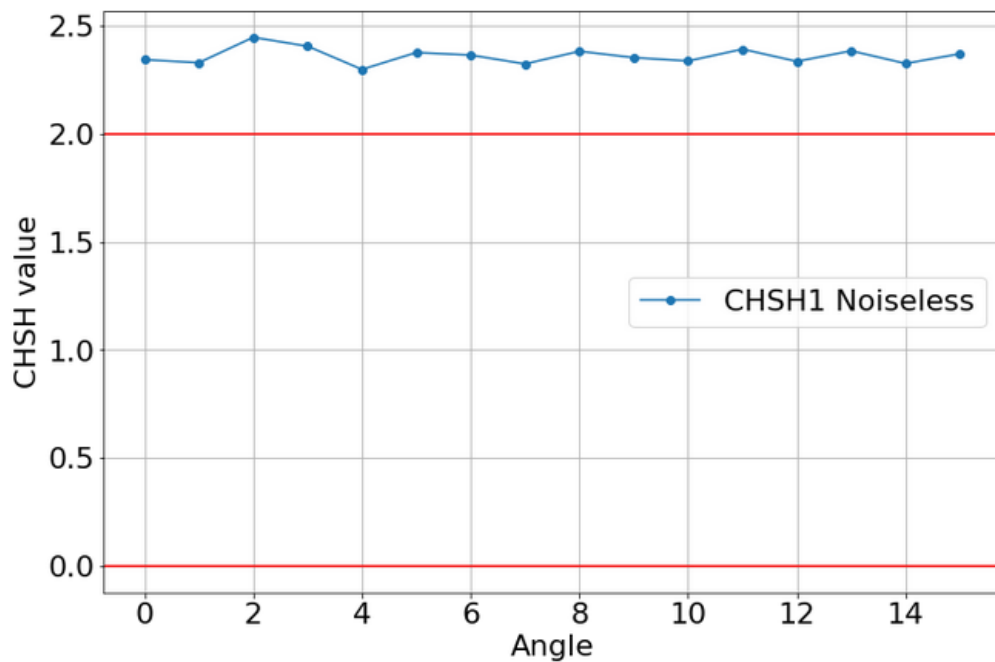
Διάγραμμα CHSH

Στο διάγραμμα που φαίνεται παρακάτω παρουσιάζονται τα αποτελέσματα της CHSH ανισότητας. Όπως είναι λογικό λόγω του ότι δεν υπάρχει παρέμβαση από κάποιον τρίτο στο σύστημα (Eve) τα αποτελέσματα κυμαίνονται από 2 έως $\sqrt{2}$ οπότε μπορούμε με σιγουριά να πούμε πως τα EPR ζεύγη έχουν πλήρη διεμπλοκή.

```
samples=[]
for i in range(len(CHSH1_ideal)):
    samples.append(i)
plt.figure(figsize=(12,8))
plt.rcParams.update({'font.size': 22})
plt.plot(samples,CHSH1_ideal,'o-',label = 'CHSH1 Noiseless')

plt.grid(which='major',axis='both')
plt.legend()
plt.axhline(y=2, color='r', linestyle='-')
plt.axhline(y=0, color='r', linestyle='-')
plt.xlabel('Angle')
plt.ylabel('CHSH value')
```

Text(0, 0.5, 'CHSH value')



Συμπεράσματα

Στην παρούσα διπλωματική παρουσιάστηκε το θεωρητικό υπόβαθρο της παραγωγής και μετάδοσης κβαντικών κλειδιών και αναλύθηκαν εκτενέστερα δυο κβαντικά πρωτόκολλα τα BB84 και E91. Η υλοποίηση των πρωτοκόλλων μας δίνει μια καλή εικόνα για την κβαντική κρυπτογραφία καθώς και για τους τρόπους με τους οποίους μπορούμε να εκμεταλευτούμε τις ιδιότητες και τους νόμους που η κβαντική φυσική μας παρέχει. Με την δημιουργία των δυο πρωτοκόλλων στον κβαντικό προσομοιωτή qiskit μπόρεσε να αποδειχθεί ότι η κβαντική κρυπτογραφία μπορεί να παρέχει μια απόλυτη και πλήρως ασφαλή επικοινωνία μεταξύ των χρηστών της. Σε αντίθεση με την κλασσική κρυπτογραφία η οποία έπειτα από εκτενή παρακολούθηση των μηνυμάτων και με την χρήση κατάλληλων αλγορίθμων η επικοινωνία μπορεί να παραβιαστεί, η κβαντική κρυπτογραφία με την χρήση των δυο αυτών πρωτοκόλλων εγγυάται την ασφάλεια της πληροφορίας στηριζόμενη σε κβαντικούς νόμους που διέπουν τα qubit και οι οποίοι καθιστούν αδύνατο την παρέμβαση τρίτου χωρίς να γίνει αντιληπτός στο σύστημα επικοινωνίας. Βέβαια οι υποδομές που χρειάζονται για να υλοποιηθεί ένα τέτοιο παγκόσμιο δίκτυο επικοινωνίας βρίσκονται ακόμα σε αρκετά πρώιμο στάδιο και απαιτούνται αρκετές τεχνολογικές βελτιώσεις ώστε ο εξοπλισμός να παρουσιάζει σφάλματα κάτω από το επιθυμητό όριο.

Προοπτικές

Για την υλοποίηση των πρωτοκόλλων χρησιμοποιήθηκε ένα ηλεκτρονικό περιβάλλον προσομοίωσης κβαντικών υπολογιστών το οποίο παρέχει με αρκετή ακρίβεια τις λειτουργίες ενός κβαντικού υπολογιστή. Σαν επόμενο βήμα της διπλωματικής θα ήταν ο αλγόριθμος που έχει υλοποιηθεί να δομικαστεί σε έναν πραγματικό υπολογιστή και να μετρηθούν πραγματικοί χρόνοι και σφάλματα. Αυτό α επιφέρει αλλαγές διότι μεταξύ την επικοινωνία δυο κβαντικών υπολογιστών μέσω ενός κβαντικού δικτύου θα υπάρχουν σφάλματα τα οποία θα πρέπει να λειφθούν υπόψη ώστε να τροποποιηθεί κατάλληλα ο κώδικας με βάσει αυτά και έτσι να υπάρχει μια σωστή και ασφαλεί επικοινωνία. Ακόμη θα μπορούσε στο πρωτόκολλο E91 να γίνουν δοκιμές με την παρέμβαση τρίτου στην επικοινωνία κάτι το οποίο με έναν κλασσικό προσομοιωτή δεν μπορούσε να υλοποιηθεί καθώς δεν υπάρχουν σωστά αποτελέσματα στα σφάλματα που λαμβάναμε.

Βιβλιογραφία

- [1] Bennett, C. H. et al. Teleporting an unknown quantum state via dual classic and Einstein–Podolsky–Rosen 1993.
- [2]Ιωάννης Καραφυλλίδης. Κβαντική Υπολογιστική. Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και βοηθήματα «Κάλλιπος» www.kallipos.gr, 2015.
- [3]Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. Physical Review Letters, 85(2):441–444, Jul 2000.
- [4]H. Lo. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410):2050–2056, Mar 1999.
- [5]John Watrous. Lecture notes in quantum computation, March 2006.
- [6] Daniel Gottesman, Hoi-Kwong Lo, Norbert Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices, 2002.
- [7]S. van Enk and Christopher Fuchs. Quantum state of an ideal propagating laser field. Physical review letters, 88:027902, 02 2002.
- [8] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. Physical Review Letters, 94(23), Jun 2005.
- [9] Xiongfeng Ma. Quantum cryptography: theory and practice, 2008.
- [10] Xiongfeng Ma. Security of quantum key distribution with realistic devices, 2005.
- [11] M. Nielsen, I. Chuang , “Quantum Computation and Quantum Information, Cambridge, 2000.
- [12] E. E. Rosinger, “Basics of Quantum Computation (Part 1)”, arXiv: quant-ph/0407064, vol.1, 8 Jul. 2004.
- [13] Anders K. H. Bengtsson, “Quantum computation: A computer science perspective”, rXiv: quantph/0511274, vol.1, 30 Nov. 2005.
- [14] Riley T. Perry. “The Temple of Quantum Computing”, April 29, 2006.
- [15] Phillip R. Kaye, Raymond Laflamme and Michele Mosca, “An Introduction to Quantum Computing”, 2007.
- [16] Ahn C., Wiseman H.M., Milburn G.J., “Quantum error correction for continuously detected errors”, 2003.

- [17] Bing Qi, Li Qian, Hoi-Kwong Lo, "A brief introduction of quantum cryptography for engineers, Wiley– VCH".
- [18] Will f., What are quantum repeaters, January 25.
- [19]Wu D.(2012) Research on quantum information network architecture and routing technology based on quantum repeater. <http://www.cnki.net>.
- [20] Liu Z.J. (2015) Research on Switching Technology in Quantum Multiuser Communication Network . <http://www.cnki.net>.
- [21] Wu Z.B. (2009) Analysis of Quantum Key Distribution Network. Optical Communication Research, 2: 22-24.
- [22] Hou B.G. (2013) Research on Topology Structure and Routing Algorithm of Quantum Key Distribution Network. <http://www.cnki.net>..
- [23]Peng H.(2014) Research on Grover routing algorithm in wireless self-organizing quantum communication network. Journal of Zhejiang University of Technology, 6: 612-615.
- [24]Wang Z. (2015) Research on security of quantum key distribution system under detection efficiency mismatch. <http://www.cnki.net>.
- [25] Stephen Wiesner, *Conjugate Coding*, Sigact News, 15, (1983)pg. 78.
- [26] W.K. Wootters and W.H. Zurek, *A Single Quantum cannot be Cloned*, Nature 299 (1982), pp. 802–803.
- [27] G. Brassard and L. Salvail, *Secret key reconciliation by public discussion*, Advances in Cryptology, Eurocrypt 93 Proc (1993). Pg. 410-423 .
- [28]William J. Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto, Inside Quantum Repeaters. IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 21, NO. 3, MAY/JUNE 2015.
- [29] Silvestre Abruzzo, Sylvia Bratzik, Nadja K. Bernardes, Hermann Kampermann, Peter van Loock and Dagmar Bruß, Quantum repeaters and quantum key distribution: Analysis of secret-key rates. 17 May 2013.
- [30]M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information". Cambridge University Press, 2005
- [31]V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," Phys. Rev. A, vol.54, pp. 1844–1852, Sep 1996.
- [32]Magnus Rådmark, "Photonic quantum information and experimental tests of foundations of quantum mechanics", 2010.

- [33]Gottesman, D., and I. L. Chuang, Nature _London_ 402390, 1999.
- [34]Phillip R. Kaye, Raymond Laflamme and Michele Mosca, "An Introduction to Quantum Computing", 2007.
- [35] Κωνσταντίνος Γ. Βαλάλης, "Κβαντικοί Υπολογισμοί και Γραμμικοί Οπτικοί Κβαντικοί Υπολογιστές", Nov 2011.
- [36] Leilei Li, Hengji Li, Chaoyang Li, Xiubo Chen, Yan Chang,Yuguang Yang⁴ and Jian Li, "The security analysis of E91 protocol in collective-rotation noise channel", International Journal of Distributed Sensor Networks, 2018.
- [37] Bell J S 1964 Physics 1 195-200
- [38]J.F. Clauser; M.A. Horne; A. Shimony; R.A. Holt (1969), "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett., 23 (15): 880–4
- [39] qutools. (2013). Entanglement Demonstrator: User's and Operation Manual [Attached in this webpage]
- [40] Violation of Bell's Inequality Lab Manual, 2016. [Attached in this webpage]
- [41] Li J, Li N, Li LL, et al. One step quantum key distribution based on EPR entanglement. 2016.
- [42]Ekert AK. Quantum cryptography based on Bell's theorem. Physical Review Letters 1991.
- [43]Zhiyong Z, Yanbo W, Min H, et al. Intercept-resent eavesdropping in polarization-drift quantum cryptography. 2016.
- [44]Παναγιώτης Γρηγοριάδης. Κβαντικοί υπολογιστές και κβαντική υπολογισσιμότητα. Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλίας, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών. Βόλος 2020.
- [45]Shor P. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994.
- [46] Hayward M. Quantum Computing and Shor's Algorithm. 2015
- [47]Γεώργιο Κάππος. Κβαντικοί υπολογιστές θεωρία, υλοποιήσεις και σύγχρονες εφαρμογές.Διπλωματική εργασία, Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Πληροφορικής. Θεσσαλονίκη 2016.
- [48]Physicsgg, <https://physicsgg.me>. 14/08/2012
- [49] Τραχανάς Σ. Κβαντομηχανική II. Πανεπιστημιακές Εκδόσεις Κρήτης; 2016