Κβαντική Κρυπτογραφία & Πληροφορία

Ντιγκάρης Αλέξανδρος

1 Ιουνίου 2022

Περιεχόμενα

Κατάλογος Σχημάτων

1 Κβαντικοί υπολογιστές

1.1 Η έννοια του qubit

Στην θεωρία της πληροφορίας, η θεμελιώδης μονάδα μέτρησης θεωρείται το bit , παίρνοντας τιμές 0 και 1. Προέκταση αυτής της κλασσικής λογικής είναι το qubit , το οποίο μπορεί να βρεθεί σε μια υπέρθεση δύο καταστάσεων $|0\rangle, |1\rangle$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

(Σχ. 1.1)

με τα α, β να είναι μιγαδικοί αριθμοί. Έτσι λοιπόν το qubit περιγράφεται στον δισδιάστατο μιγαδικό διανυσματικό χώρο C^2 (Hilbert space) . Οι καταστάσεις είναι ορθοκανονικές μεταξύ τους, ενώ τα α, β ικανοποιούν την συνθήκη κανονικοποίησης:

$$|\alpha|^2 + |\beta|^2 = 1$$

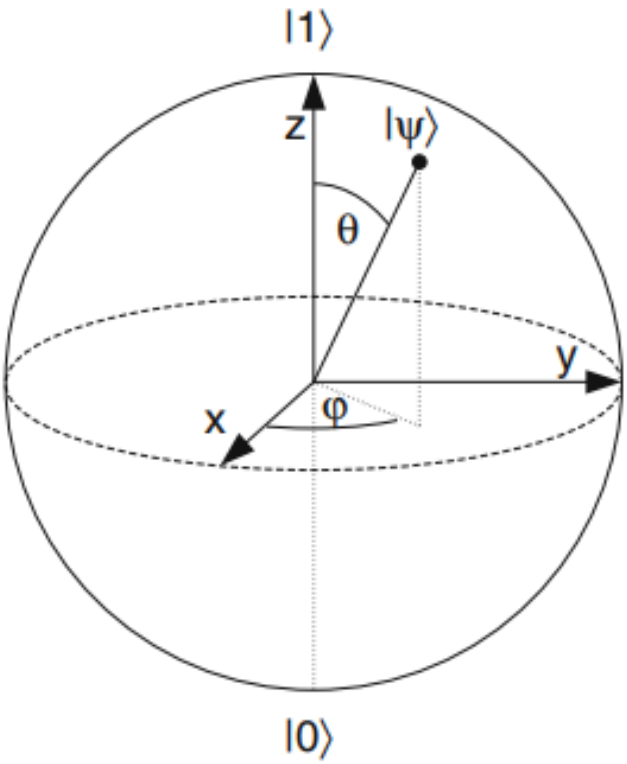
(Σχ. 1.2)

Έτσι η Σχ. 1.1 μπορεί να γραφεί ως

$$|\psi\rangle = cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}sin\frac{\theta}{2}\,|1\rangle$$

(Σχ. 1.3)

με ϑ, φ πραγματικούς αριθμούς



Σχήμα 1: Το qubit σαν διάνυσμα στην σφαίρα Bloch

Όλη η πληροφορία ενός qubit περιέχεται στις συνιστώσες α, β. Παρόλα αυτά η πληροφορία παραμένει κρυμμένη αλλά υπάρχουσα. Μόνο κατά την μέτρηση μιας κατάστασης, έχουμε απώλεια πληροφορίας. Από την Σχ. 1.1 παρατηρούμε ότι το qubit μπορεί να παρασταθεί και σαν διάνυσμα δύο συνιστωσών στην περιπτωσή μας. Η μορφή αυτή λέγεται διάνυσμα Bloch . Για $\theta = 0$ και $\theta = \pi$ έχουμε τις αμιγείς καταστάσεις $|0\rangle, |1\rangle$ αντίστοιχα. Η κυματοσυνάρτηση ενός qubit μπορεί να γραφεί με την μορφή:

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

(Σχ. 1.4)

ενώ για μια κυματοσυνάρτηση με δύο qubits θα είχαμε αντίστοιχα

$$|\psi\rangle = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

(Σχ. 1.5)

Έχοντας $\alpha, \beta \neq 0$, το qubit θα υπάρχει σαν υπέρθεση των $|0\rangle, |1\rangle$ (Σχ. 1.1). Με την παραπάνω λογική μπορούμε να θεωρήσουμε ότι η κατάσταση ενός qubit που δεν εμπίπτει στο κλασσικό χώρο (αυστηρά 0 ή 1), μπορεί να περιγραφεί σαν υπέρθεση των γινομένων της σχετικής φάσης με την μέτρηση. Για παράδειγμα:

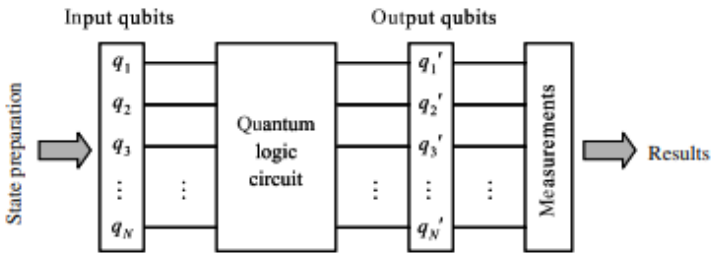
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

(Σχ. 1.6)

1.2 Κβαντικές πύλες

Η μονάδα επεξεργασίας ενός υπολογιστή επεξεργάζεται bits ανά μονάδες ή δυάδες, μέσω των λεγόμενων λογικών πυλών NOT και NAND . Οι πύλες NOT λαμβάνουνε bits ανά μονάδες, ενώ οι NAND ανά δυάδες. Οι πύλες αυτές είναι συνδεδεμένες σε ένα κύκλωμα, δρούνε πάνω στα bits και παράγουν ένα αποτέλεσμα (output) . Στην δικιά μας περίπτωση, μια συστοιχία από N qubits λαμβάνεται ως είσοδος (input) στο κύκλωμα των κβαντικών λογικών πυλών NOT και NAND . Οι πύλες παράγουν ως έξοδο μια καινούργια συστοιχία N' qubits , στα οποία τελείται μια μέτρηση και δίνουν ως τελικό αποτέλεσμα (output) , n bits . Το πλεονέκτημα που προσφέρουν οι κβαντικοί υπολογιστές είναι ότι τα N qubits στην είσοδο στην πραγματικότητα αντιπροσωπεύουν (βλέπε Σχ. 1.5), 2^N πακέτα πληροφορίας. Ακόμα και αν η επεξεργασία των λογικών πυλών γίνεται κβαντομηχανικά και το output είναι πεπερασμένο, το μέγεθος της πληροφορίας που μπορούμε να διοχετεύσουμε στον επεξεργαστή μας είναι τεράστιο!



Σχήμα 2: Η λειτουργία ενός κβαντικού επεξεργαστή

Πως όμως λειτουργούν οι λογικές πύλες. Αρχικά θα κάνουμε λόγο για τις πύλες επεξεργασίας ενός qubit την φορά. Η πύλη δέχεται ως είσοδο ένα qubit σε μια κατάσταση $|\psi\rangle$

και δίνουν ως έξοδο το ίδιο qubit σε μια κατάσταση $|\psi'\rangle$:

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \rightarrow |\psi'\rangle = \begin{pmatrix} c'_0 \\ c'_1 \end{pmatrix}$$

(Σχ. 1.7)

Επομένως μια single-qubit πύλη μπορεί να παρομοιαστεί σαν μια $N \times N$ μήτρα M που μετασχηματίζει ένα διάνυσμα Bloch N στοιχείων σε ένα καινούργιο διάνυσμα:

$$\begin{pmatrix} c'_0 \\ c'_1 \end{pmatrix} = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

(Σχ. 1.8)

Για τις λογικές πύλες θα πρέπει να ισχύει η αντιστρεπτότητα, δηλαδή:

$$MM^\dagger = I$$

(Σχ. 1.9)

Παραδείγματα single-qubit πυλών είναι η πύλη NOT η οποία εκτελεί μια περιστροφή π rad κατά τον x άξονα της σφαίρας Bloch και είναι γνωστή και σαν bit-flip τελεστής:

$$X \cdot q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix}$$

(Σχ. 1.10)

η πύλη Z ή αλλιώς phase-flip τελεστής, η οποία εκτελεί μια περιστροφή π rad κατά τον z άξονα της σφαίρας Bloch :

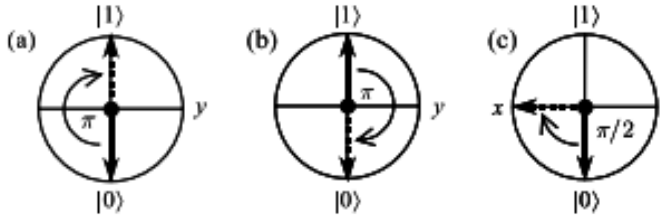
$$Z \cdot q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_0 \\ -c_1 \end{pmatrix}$$

(Σχ. 1.11)

και η πύλη Hadamard η οποία εκτελεί μια περιστροφή π rad κατά τον z άξονα και στην συνέχεια μια περιστροφή $\pi/2$ rad κατά τον y άξονα της σφαίρας Bloch :

$$H \cdot q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} \frac{c_0+c_1}{\sqrt{2}} \\ \frac{c_0-c_1}{\sqrt{2}} \end{pmatrix}$$

(Σχ. 1.12)



Σχήμα 3: Αποτελέσματα single-qubit πυλών στο διάνυσμα Bloch

Τέλος ο πίνακας-τελεστής iY εκτελεί ταυτόχρονα bit και phase flip:

$$iY = Z \cdot X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

(Σχ. 1.13)

ώστε

$$iY\,|0\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

$$iY\,|1\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

(Σχ. 1.14)

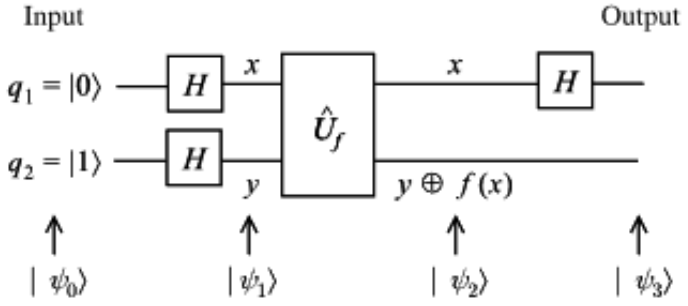
Όσον αφορά τις two-qubit πύλες, η πιο συνηθής περίπτωση είναι αυτή της CU (controlled unitary) πύλης. Η πύλη αυτή δέχεται δύο qubits , ένα control που δεν δέχεται τροποποίηση και ένα target που δέχεται έναν μοναδιακό μετασχηματισμό. Το control δεν αλλάζει αλλά λειτουργεί σαν διακόπτης στο τι αλλαγή θα δεχθεί το target . Παράδειγμα τέτοιου τύπου πύλης είναι η CNOT πύλη όπου εκτελεί έναν μετασχηματισμό NOT στο qubit q_2 αν το qubit q_1 είναι ίσο με $|1\rangle$:

$$U_{CNOT}\,|\psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{11} \\ c_{10} \end{pmatrix}$$

(Σχ. 1.15)

1.3 Κβαντικοί αλγόριθμοι

Ο πρώτος αλγόριθμος που χρησιμοποιήθηκε για να αναδείξει την υπεροχή του κβαντικού υπολογιστή σε σχέση με το κλασσικό ανάλογο ήταν ο αλγόριθμος του Deutsch . Ο αλγόριθμος δέχεται ως είσοδο δύο qubits σε καθορισμένη κατάσταση με το πρώτο αρχικοποιημένο στην $|0\rangle$ και το δεύτερο στην $|1\rangle$ αντίστοιχα. Τα qubits αυτά δέχονται μετασχηματισμό Hadamard , μεταβάλλοντας την καταστάση τους σε $|\psi_{11}\rangle$ και $|\psi_{21}\rangle$ αντίστοιχα. Το αποτέλεσμα καθορίζεται μέσω ενός μοναδιακού μετασχηματισμού ως balanced ή constant και ως μια νέα κατάσταση $|\psi_2\rangle$ περνά από έναν δεύτερο μετασχηματισμό Hadamard προτού εξέλθει σαν τελική κατάσταση $|\psi_3\rangle$. Η παραπάνω διαδικασία μπορεί να παρασταθεί μαθηματικά ως:



Σχήμα 4: Αλγόριθμος Deutsch

$$|\psi_0\rangle = |0,1\rangle = |0\rangle\,|1\rangle = |\psi_{01}\rangle\,|\psi_{02}\rangle$$

$$|\psi_{11}\rangle = H \cdot q_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\psi_{21}\rangle = H \cdot q_2 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

(Σχ. 1.16)

Επομένως η καταστάση $|\psi\rangle$ στην είσοδο του μοναδιακού μετασχηματισμού θα είναι:

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

(Σχ. 1.17)

Ο μοναδιακός μετασχηματισμός θα επιδράσει μόνο στην $|\psi_{21}\rangle$ κατάσταση επιχειρώντας modular-2 $f(x)$ $(\oplus f(x))$ πρόσθεση. Το αποτέλεσμα θα είναι η κατάσταση:

$$|\psi_2\rangle = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle)$$

(Σχ. 1.18)

Στην περίπτωση ενός constant αποτελέσματος θα ισχύει $f(0) = f(1)$ ενώ για balanced αποτελέσματα θα έχουμε $f(1) = 1 \oplus f(0)$, με τις τελικές καταστάσεις να γράφονται ως:

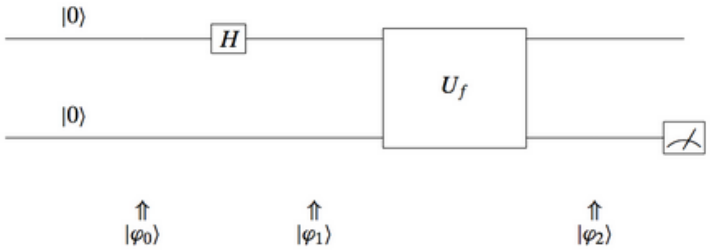
$$|\psi_3\rangle^{constant} = \frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |1 \oplus f(0)\rangle)$$

$$|\psi_3\rangle^{balanced} = \frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |1 \oplus f(0)\rangle)$$

(Σχ. 1.19)

Για παράδειγμα ένα πρόγραμμα που θα διασφάλιζε την ύπαρξη δύο τιμών (0 και 1) κατά την ρίψη ενός νομίσματος θα εκτελούσε δύο μετρήσεις ενώ ένας κβαντικός υπολογιστής μόνο μία, γνωρίζοντας αντίστοιχα αν το αποτέλεσμα είναι balanced ή constant . Στην γενική περίπτωση ένας κλασσικός υπολογιστής χρειάζεται $2^{n-1}+1$ επαναλήψεις.

Σε μια διαφορετική λογική, ο αλγόριθμος του Deutsch μπορεί να διαμορφωθεί ως:



Σχήμα 5: Αλγόριθμος Deutsch σε μια διαφορετική όψη

όπου:

$$|\phi_0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|\phi_1\rangle = |H \cdot 0, 0\rangle = \left| \frac{|0\rangle + |1\rangle}{\sqrt{2}}, 0 \right\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$|\phi_2\rangle = \frac{|x, y \oplus f(x)\rangle + |x, y \oplus f(x)\rangle}{\sqrt{2}} = \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} = \frac{|0, 0 \oplus 1\rangle + |1, 0 \oplus 0\rangle}{\sqrt{2}}$$

$$\Rightarrow |\phi_2\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

(Σχ. 1.20)

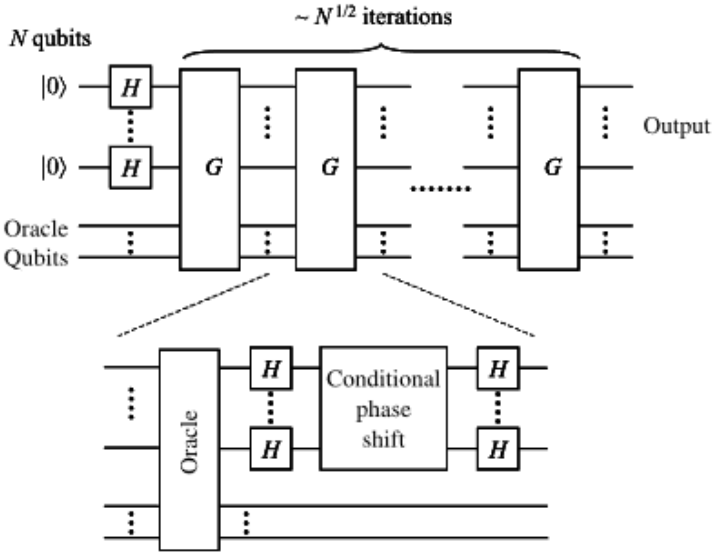
Ένας άλλος αλγόριθμος είναι ο αλγόριθμος του Grover ή αλλιώς κβαντικής αναζήτησης. Ο αλγόριθμος αυτός μπορεί να δράσει σε μια οποιαδήποτε ανοργάνωτη μη δομημένη βάση δεδομένων. Εάν για παράδειγμα η βάση δεδομένων χρησιμοποιεί σαν πρωτεύων κλειδί

το ονοματεπώνυμο του χρήστη και δίνει πληροφορίες για την διεύθυνση οικίας του και το τηλεφωνό του, έχει αποδειχθεί από τους C. Bennett, Bernstein και Brassard ότι για μια βάση N σειρών - δεδομένων, ένας κβαντικός υπολογιστής θέλει $\sqrt{N}$ πράξεις εύρεσης με τον κλασσικό να χρειάζεται με ψάξει κατά μέσο όρο $\frac{N}{2}$ των δεδομένων ώστε να έχει 50% πιθανότητα εύρεσης της ζητούμενης πληροφορίας. Αν και η επιτάχυνση που προσφέρει ο αλγόριθμος του Grover είναι τετραγωνικής (quadratic) φύσεως, συνεχίζει να έχει πολλές εφαρμογές σε ένα ευρύ φάσμα αλγορίθμων. Επομένως για μια βάση δεδομένων 10^6 σειρών, ένας κβαντικός υπολογιστής θέλει 10^3 πράξεις ενώ ο κλασσικός $5 \cdot 10^5$. Το σημαντικό χαρακτηριστικό του αλγορίθμου αυτού είναι η λύση του προβλήματος της αντιστροφής συναρτήσεων (function inversion) που χρησιμοποιείται ευρέως στην κρυπτογραφία. Για μια γνωστή συνάρτηση $y = f(x)$ για την οποία κατασκευάζουμε μια βάση δεδομένων με όλα τα πιθανά output της, έχοντας ως δείκτη σειράς το input x. Ο αλγόριθμος του Grover χρειάζεται μόνο $\sqrt{N}$ επαναλήψεις ώστε να βρει το δωσμένο y_0 και συνεπώς το input x_0 που του αντιστοιχεί. Εξισώνοντας τώρα τον αριθμό των δεδομένων με μια συστοιχία N qubits έχουμε:

$$2^N = N_{data}$$

(Σχ. 1.21)

Συνεπώς χρησιμοποιώντας για παράδειγμα μόνο 100 qubits μπορούμε να διαχειριστούμε μέχρι και έναν όγκο $\sim 10^{30}$ δεδομένων!



Σχήμα 6: Αλγόριθμος Grover

Ο τρόπος λειτουργίας του αλγορίθμου είναι ο εξής. Κάθε qubit αρχικοποιείται στην κατάσταση $|0\rangle$ και δέχεται μετασχηματισμό Hadamard . Έτσι οδηγούμαστε σε μια κατάσταση

γινομένων:

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^N (|0\rangle_1 + |1\rangle_1) \cdot (|0\rangle_2 + |1\rangle_2) \cdots (|0\rangle_N + |1\rangle_N)$$

(Σχ. 1.22)

Η κατάσταση αυτή περνάει από $\sqrt{N}$ μετασχηματισμούς Grover μέχρι να δώσει το τελικό αποτέλεσμα με πιθανότητα $\simeq 1$. Ο μετασχηματισμός Grover διακρίνεται από συγκεκριμένα βήματα. Αρχικά ενάς μοναδιακός τελεστής εν ονόματι oracle δρα σαν ένα μαύρο κουτί και σημαδεύει την λύση ως:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

ή αλλιώς

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

(Σχ. 1.23)

με $f(x) = 0$ αν η ζητούμενη πληροφορία δεν είναι η λύση και $f(x) = 1$ στην αντίθετη περίπτωση.

Για να αποσαφηνήσουμε την λειτουργία του oracle παρατίθεται το παρακάτω παράδειγμα. Έστω μια συστοιχία με ένα qubit αρχικοποιημένη σε κατάσταση $|1\rangle$ και $|x\rangle$ η input κατάσταση κάθε φορά. Τότε θα έχουμε:

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

$$U_f(|x\rangle \otimes H |1\rangle) = \frac{1}{\sqrt{2}}(U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle)$$

$$\Rightarrow U_f(|x\rangle \otimes H |1\rangle) = \frac{1}{\sqrt{2}}(|x\rangle |0 \oplus f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle)$$

$$\Rightarrow U_f(|x\rangle \otimes H\,|1\rangle) = \begin{cases} \frac{1}{\sqrt{2}}(-\,|x\rangle\,|0\rangle + |x\rangle\,|1\rangle) & f(x) = 1 \\ \\ \frac{1}{\sqrt{2}}(|x\rangle\,|0\rangle - |x\rangle\,|1\rangle) & f(x) = 0 \end{cases}$$

$$\Rightarrow U_f(|x\rangle \otimes H\,|1\rangle) = (-1)^{f(x)}\,|x\rangle \otimes H\,|1\rangle$$

(Σχ. 1.24)

Με άλλα λόγια το input μας κωδικοποιείται με μια αλλαγή φάσης του qubit υπό συνθήκη $f(x)$ (conditional phase shift) .

Ας πάρουμε το παράδειγμα μιας βάσης τεσσάρων δεδομένων ($N_{data} = 4$), άρα και 2 qubits . Τότε θα έχουμε:

$$|\psi_1\rangle = \Big(\frac{1}{\sqrt{2}}\Big)^2 (|0\rangle_1 + |1\rangle_1) \cdot (|0\rangle_2 + |1\rangle_2)$$

$$\Rightarrow |\psi_1\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\Rightarrow |\psi_1\rangle = (1/2, 1/2, 1/2, 1/2)$$

(Σχ. 1.25)

Έστω η ζητούμενη πληροφορία είναι η $|10\rangle$:

$$\Rightarrow |\psi_1\rangle' = (1/2, 1/2, -1/2, 1/2)$$

(Σχ. 1.26)

Τέλος υπολογίζουμε το μέσο πλάτος πιθανότητας:

$$(+1/2 + 1/2 - 1/2 + 1/2) \cdot \frac{1}{4} = 1/4$$

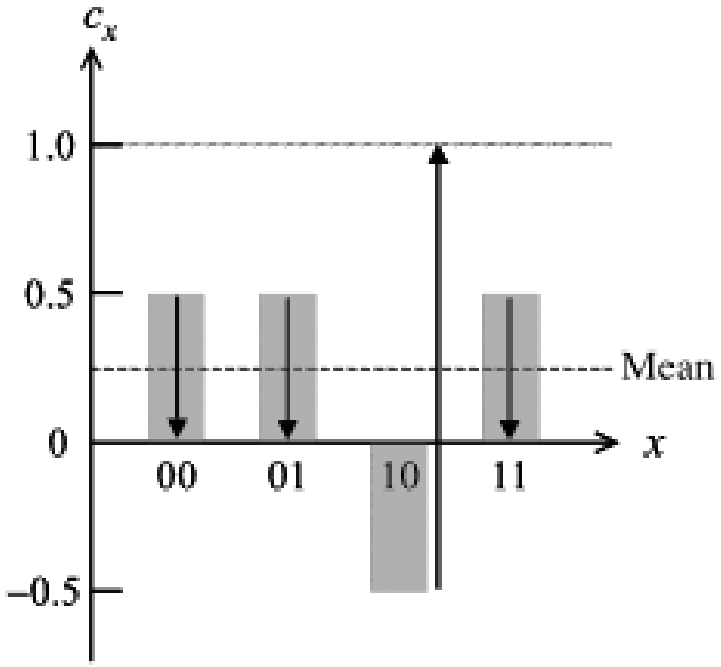
(Σχ. 1.27)

Αντιστρέφουμε τώρα το πλάτος πιθανότητας της κάθε κατάστασης, σε σχέση με το μέσο πλάτος και έχουμε εν τέλει:

$$|\psi_2\rangle = (0, 0, 1, 0)$$

(Σχ. 1.28)

όπου η ζητούμενη πληροφορία ($|10\rangle$) έχει τώρα πιθανότητα εύρεσης 1.



Σχήμα 7: Αντιστροφή πλάτους ως προς τον μέσο

Ο μοναδιακός μετασχηματισμός U_f μπορεί να γραφεί και ως $U_f = 2\,|\psi\rangle\,\langle\psi| - I$ δηλαδή σαν έναν τελεστή που διατηρεί αναλλοίτες όλες τις καταστάσεις εκτός από εκείνες που είναι κάθετες στην $|\psi\rangle$. Με χρήση αυτού του τελεστή μπορούμε να αποδείξουμε την αντιστροφή

γύρω από την μέση τιμή:

$$(2\left|\psi\right\rangle\left\langle\psi\right| - I)\sum_k a_k\left|k\right\rangle =$$

$$= 2\sum_k(\left\langle\psi|a_k|\psi\right\rangle\left|k\right\rangle - a_k)\left|k\right\rangle$$

$$= 2\sum_k\langle a\rangle\left|k\right\rangle - \sum_k a_k\left|k\right\rangle$$

$$= \sum_k\Big(2\langle a\rangle - a_k\Big)\left|k\right\rangle$$

(Σχ. 1.29)

Επομένως για $\langle a\rangle = 1/4$ και $a_k = 1/2$ έχουμε:

$$2\cdot\frac{1}{4} - \frac{1}{2} = \frac{1}{2} - \frac{1}{2} = 0$$

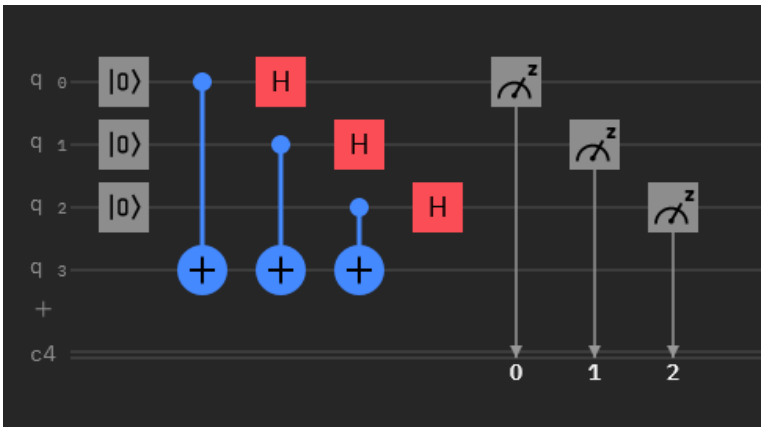
(Σχ. 1.30)

ενώ για την ζητούμενη κατάσταση με $\langle a\rangle = 1/4$ και $a_k = -1/2$ θα έχουμε:

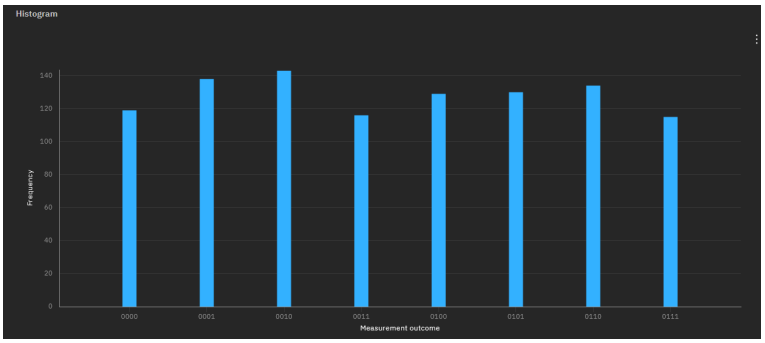
$$2\cdot\frac{1}{4} - (-\frac{1}{2}) = \frac{1}{2} + \frac{1}{2} = 1$$

(Σχ. 1.31)

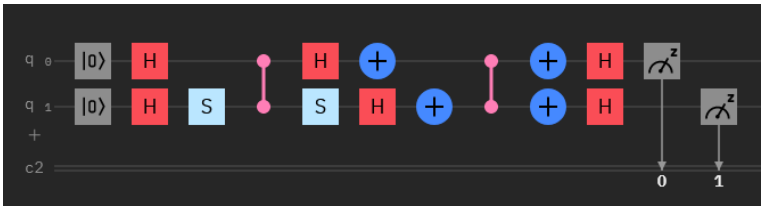
Μπορούμε να προσομοιώσουμε τους αλγόριθμους Deutsch και Grover στο framework της IBM Quantum , παίρνοντας τα παρακάτω αποτελέσματα:



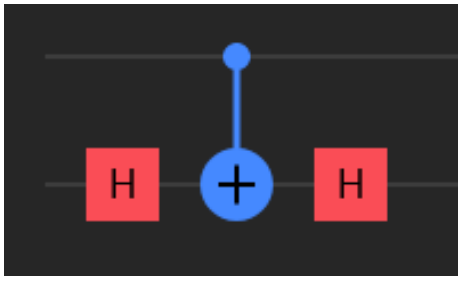
Σχήμα 8: Ο αλγόριθμος Deutsch στην balanced του μορφή



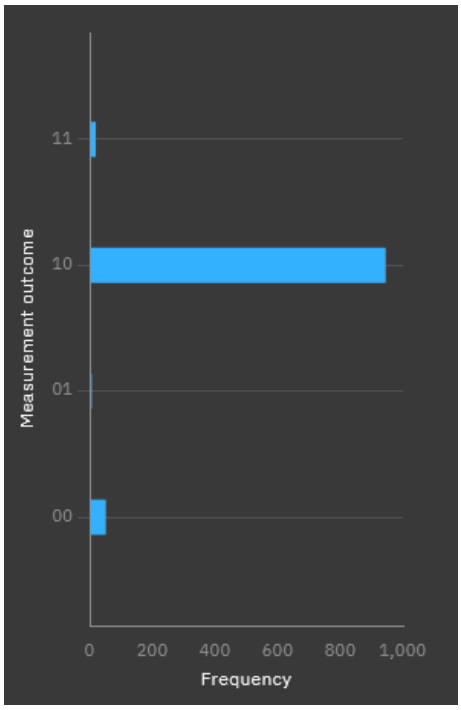
Σχήμα 9: Ισάξια (balanced) πιθανότητα για κάθε μια από τις καταστάσεις



Σχήμα 10: Ο αλγόριθμος Grover



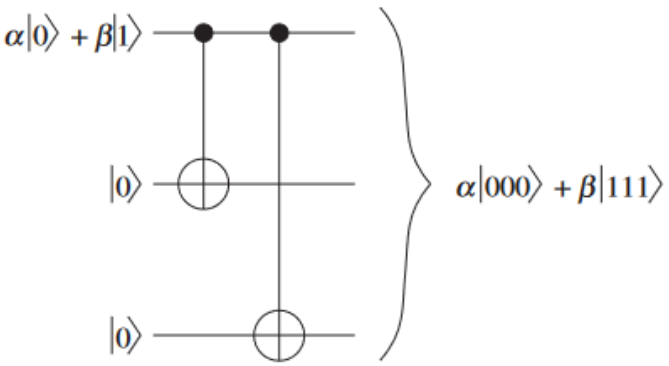
Σχήμα 11: Ο μετασχηματισμός oracle



Σχήμα 12: Η τελική κατανομή πιθανοτήτων για την περίπτωση της εύρεσης της $|10\rangle$

Ένα ακόμα μειονέκτημα των κλασσικών υπολογιστών είναι στην προσομοίωση κβαντομηχανικών συστημάτων, για παράδειγμα συστήματα με 50 άτομα. Σε ένα κβαντικό υπολογιστή αυτό λύνεται με χρήση 50 qubits ενώ σε έναν κλασσικό με $2^{50} \simeq 10^{15}$ bits .

Όσον αφορά την διόρθωση λαθών στους κβαντικούς υπολογιστές, μπορούμε να δούμε πρώτα το κλασσικό ανάλογο στο οποίο οι τιμές 0 και 1 σε δύο bits είναι τόσο διαφορετικές μεταξύ τους, ώστε η πιθανότητα κάποια θερμική ή μηχανική ή εξωγενής αλληλεπίδραση να επηρρεάσει τις καταστάσεις των δύο bits είναι αμελητέα. Το ίδιο πράγμα δεν ισχύει όμως για ένα κβαντομηχανικό σύστημα. Εκεί κάποιος θερμικός ή μηχανικός θόρυβος μπορεί να αλλάξει τις καταστάσεις των qubits και να δημιουργήσει λάθη.

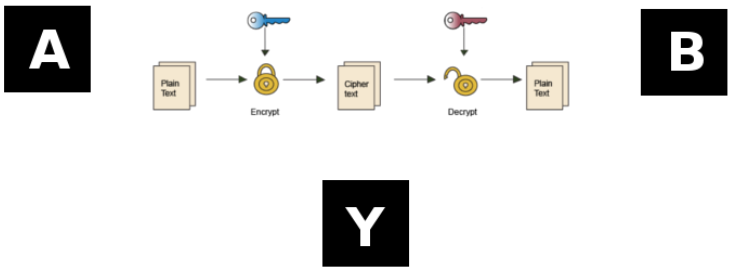


Σχήμα 13: Διόρθωση σφάλματος για bit-flip για ένα qubit , με χρήση άλλων δύο

2 Ορισμός της κρυπτογραφίας

Η κρυπτογραφία είναι μια επιστήμη που σκοπός της είναι η απόκρυψη της πληροφορίας, αποθηκευμένης σε μορφή μηνύματος, από κάποιο τρίτο πρόσωπο ή μέσο. Η αποδοτικότητα της κρυπτογραφείας έγκειται στην ασφάλεια κατά την μετάδοση αλλά και κατά την επεξεργασία του μηνύματος. Πρόκειται για μια περιζήτητη επιστήμη που βρίσκει εφαρμογές στην προστασία και μεταφορά δεδομένων μεγάλων εταιριών, των στρατιωτικών και κυβερνητικών δυνάμεων μιας χώρας κλπ.

Η κρυπτογραφεία αποτελείται από πέντε βασικά στοιχεία: τον πομπό, τον δέκτη, το μήνυμα, τον υποκλοπέα και έναν κρυπτογραφικό μηχανισμό. Ο πομπός δημιουργεί ένα μήνυμα και το κρυπτογραφεί μέσω κάποιου μηχανισμού. Το μήνυμα μεταφέρεται στον δέκτη είτε μέσω ενός ιδιωτικού είτε μέσω ενός δημόσιου καναλιού. Ο δέκτης λαμβάνει το μήνυμα και το αποκρυπτογραφεί. Αν το μήνυμα μεταφέρθηκε μέσω δημοσίου καναλιού, υπάρχει ο κίνδυνος η πορεία του μηνύματος να ανακοπτεί από ένα τρίτο πρόσωπο, έναν υποκλοπέα. Ο υποκλοπέας αν έχει στην κατοχή του τον μηχανισμό κρυπτογράφησης, μπορεί όχι μόνο να διαβάσει το μήνυμα, αλλά και να το μεταβάλλει, ώστε να στείλει παραποιημένο και ίσως κακόβουλο περιεχόμενο στον δέκτη.



Σχήμα 14: Η χρήση κλειδιών στην κρυπτογραφία

2.1 Μηχανισμοί κρυπτογράφησης & κλειδιά

Οι μηχανισμοί κρυπτογράφησης ποικίλουν και είναι συνήθως μαθηματικές συναρτήσεις ή αλγόριθμοι. Η πιο σύγχρονη μορφή κρυπτογράφησης σήμερα, γίνεται με την χρήση δημόσιων και ιδιωτικών κλειδιών. Το μήνυμα μεταφράζεται αρχικά σε μια μη-αναγνωρίσιμη σειρά χαρακτήρων είτε αριθμών, το λεγόμενο κρυπτογράφημα. Αμέσως μετά, διακρίνουμε δύο μεθόδους.

Σύμφωνα με την μία, το κρυπτογράφημα συνενώνεται με ένα ιδιωτικό κλειδί και αποστέλλεται στον δέκτη. Ο δέκτης με την χρήση του ίδιου κλειδιού, μεταφράζει το κρυπτογράφημα. Αυτή η μέθοδος είναι επικίνδυνη, καθώς με την χρήση του ίδιου κλειδιού, μπορεί να εμφανιστούν μοτίβα, έτσι ώστε ο υποκλοπέας να μπορέσει να βρει το μυστικό κλειδί και να αποκρυπτογραφήσει τα επερχόμενα μηνύματα.

Η δεύτερη μέθοδος χρησιμοποιεί κάθε φορά διαφορετικό δημόσιο κλειδί, το οποίο δημιουργείται με μια μονόδρομη μη-αντιστρεπτή συνάρτηση. Ακόμα και αν ο υποκλοπέας γνωρίζει το κλειδί, η αντιστροφή της κατασκευής του απαιτεί τόσο μεγάλο χρονικό διάστημα που είναι πρακτικά ανθρωπίνως αδύνατο να πραγματοποιηθεί. Έτσι λοιπόν το κρυπτογράφημα

συνενώνεται με ένα δημόσιο κλειδί, του οποίου ο δημιουργός-αλγόριθμος είναι γνωστός. Η πληροφορία που παράγεται, μεταφέρεται στον δέκτη, ο οποίος με χρήση ενός ιδιωτικού κλειδιού, το οποίο δεν είναι γνωστό στους υπόλοιπους, μεταφράζει την πληροφορία στο αρχικό μήνυμα. Ακολουθούν τα παρακάτω παραδείγματα:

α) χρήση του ίδιου ιδιωτικού κλειδιού

Ας υποθέσουμε ότι κωδικοποιούμε την αλφάβητο σαν χαρακτήρες 5 bits . Έστω το μήνυμα που θέλουμε να μεταφέρουμε, είναι το "QUANTUM ". Αρχικά, η πρώτη κωδικοποίηση του θα μας δώσει "10001101010000101110101001010101101", που είναι και το κρυπτογράφημα μας. Έστω ότι το ιδιωτικό κλειδί μας θα είναι το "00110011011110100010001011000111001". Σημειώνουμε εδώ ότι το μήκος του κλειδιού οφείλει να είναι ίσο με το σύνολο των χαρακτήρων του μηνύματος. Αμέσως μετά, συνενώνουμε το κρυπτογράφημα με το κλειδί μέσω modular-2 πρόσθεσης. Έτσι θα έχουμε "10111110001110001100100010010010100", το οποίο είναι και η τελική μορφή του κρυπτογραφήματος που θα αποσταλλεί στον Β. Στην συνέχεια, ο Β θα πραγματοποιήσει modular-2 αφαίρεση μεταξύ του τελικού κρυπτογραφήματος και του ιδιωτικού κλειδιού, όντας ο μόνος που γνωρίζει το κλειδί, πέρα από τον Α. Το αποτέλεσμα της αφαίρεσης αυτής, δεν είναι κανένα αλλό παρά το αρχικό μήνυμα "QUANTUM " γραμμένο σε 5-bit χαρακτήρες.

β) χρήση διαφορετικού δημοσίου κλειδιού

Ως παράδειγμα θα φέρουμε τον αλγόριθμο RSA . Αρχικά παίρνουμε δύο πρώτους αριθμούς, έστω $x = 3$ και $y = 11$. Το γινόμενο τους είναι $c = 33$. Υπολογίζοντας τώρα την συνάρτηση $\phi(c) = (x-1)\cdot(y-1) = 20$, θα επιλέξουμε έναν θετικό ακέραιο a, ώστε $1 < a < \phi(c)$, έστω $a = 7$.

Επομένως το δημόσιο κλειδί θα είναι το $(a, c) = (7, 33)$.

Για να υπολογίσουμε τώρα το ιδιωτικό κλειδί, θα πρέπει να βρούμε έναν θετικό ακέραιο ώστε να ισχύει $(b \cdot a) mod(\phi(c)) = 1$. Βρίσκουμε $b = 3$.

Άρα το ιδιωτικό κλειδί είναι το $(b, c) = (3, 33)$.

Έστω λοιπόν ότι ο Α θέλει να αποστείλει το μήνυμα "Η " στον Β. Εφόσον ο αλγοριθμός μας δουλεύει αριθμητικά, μετατρέπουμε το "Η " σε "8". Για να σχηματιστεί το κρυπτογράφημα, υπολογίζουμε την τιμή $8^a mod c = 2$ κάνοντας χρήση του δημοσίου κλειδιού. Άρα το τελικό μήνυμα που θα αποσταλλεί στον Β, θα είναι "2" ή αλλιώς "Β ". Ο Β τώρα, για να αποκρυπτογραφήσει το μήνυμα, θα υπολογίσει την τιμή $2^b mod c = 8$ χρησιμοποιώντας το ιδιωτικό κλειδί.

2.2 Αδυναμίες της σύγχρονης κρυπτογραφίας

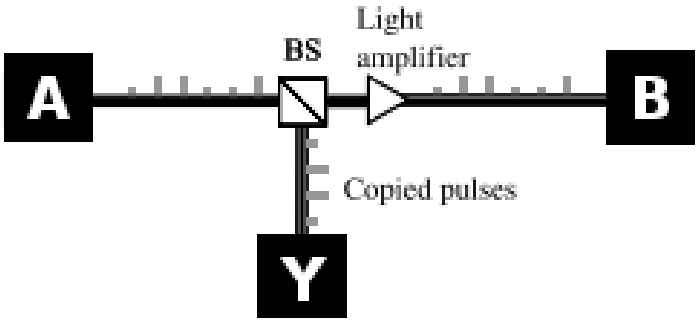
Καμία κρυπτογράφηση δεν είναι απόρθητη. Κάθε κρυπτογράφηση μπορεί να σπάσει είτε μέσω της εμφάνισης μοτίβων στο κρυπτογράφημα (συχνότητα ορισμένων χαρακτήρων σε σχέση με τους υπόλοιπους, βλέπε κώδικας Morse), είτε μέσω υποκλοπής του κλειδιού από τρίτον.

Μια διείσδυση ή μια υποκλοπή είναι αρκετή για να καταστρέψει ολόκληρο το κρυπτοσύστημα με το οποίο ανταλλάσουν πληροφορίες σημαντικά πρόσωπα και υπηρεσίες.

2.3 Κβαντική κρυπτογραφία

Τα ατελείωτα αδιέξοδα πάνω στις προσπάθειες να σβήσουν οι αδυναμίες της κλασσικής προσέγγισης της κρυπτογραφείας, έρχεται να λύσει η κβαντομηχανική. Η μέθοδος ασφαλούς μετάβασης του ιδιωτικού κλειδιού με χρήση της κβαντομηχανικής, ονομάζεται κβαντική διανομή κλειδιού και μπορεί να πραγματοποιηθεί με δύο τρόπους. Ο πρώτος πατάει πάνω στις κβαντομηχανικές αρχές που διέπουν τις μετρήσεις σε απομονωμένα σωματίδια, ενώ ο δεύτερος περιστρέφεται γύρω από τις ιδιότητες των διεμπλεγμένων καταστάσεων. Προς το παρών θα δούμε αναλυτικά την πρώτη τεχνική.

Ας δούμε ένα παράδειγμα για να αποσαφηνίσουμε καλύτερα το φαινόμενο. Έστω αρχικά η κλασσική περίπτωση όπου ο A και ο B ανταλλάσουν πληροφορία με την μορφή φωτεινών παλμών, μέσω μιας οπτικής ίνας. Οι μεγάλου πλάτους ισχυροί παλμοί αντιστοιχούν σε 1 bit , ενώ οι μηδενικού πλάτους και ασθενείς παλμοί αντιστοιχούν σε 0 bit . Στην περίπτωση αυτή, ο υποκλοπέας Υ μπορεί μέσω ενός διαχωριστή δέσμης να υποκλέψει την πληροφορία και μετά χρησιμοποιώντας έναν ενισχυτή πλάτους να αφήσει την πληροφορία να σταλθεί στον B, ακέραια και χωρίς να δώσει κάποια ένδειξη ότι κάποιος την υποκλέπτει.



Σχήμα 15: Το κλασσικό μοντέλο κρυπτογραφίας

Στην κλασσική προσέγγιση λοιπόν, ο B αδυνατεί να γνωρίζει αν η πληροφορία υποκλέπτεται ή όχι και έτσι το κρυπτοσύστημα κρίνεται εξ αρχής μη-ασφαλές και επικίνδυνο. Το παραπάνω σενάριο στην κβαντομηχανική απαγορεύεται λόγω του θεωρήματος της μη-κλωνοποίησης (non-cloning theory) . Σύμφωνα με το θεώρημα αυτό, είναι αδύνατο να δημιουργήσουμε ένα ανεξάρτητο και πανομοιότυπο αντίγραφο μιας οποιαδήποτε τυχαίας κβαντικής κατάστασης.

Ας υποθέσουμε ότι έχουμε δύο διακριτές κβαντικές καταστάσεις $|\psi\rangle, |\phi\rangle$ οι οποίες δεν είναι ορθογώνιες:

$$\langle\phi|\psi\rangle \neq 0$$

(Σχ. 2.1)

Αν υποθέσουμε ότι η κλωνοποίηση θα γίνει με χρήση του μοναδιακού τελεστή U, ο οποίος αντιγράφει την εισαγόμενη κατάσταση $|\psi\rangle, |\phi\rangle$ σε μια κατάσταση $|s\rangle$ όπως φαίνεται παρακάτω:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

(Σχ. 2.2)

Παίρνωντας λοιπόν το εσωτερικό γινόμενο έχουμε το εξής:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

(Σχ. 2.3)

το οποίο αληθεύει μόνο αν οι $|\psi\rangle, |\phi\rangle$,είναι η ίδια κατάσταση ή είναι ορθογώνιες. Επομένως δεν γίνεται να επιτευχθεί κλωνοποίηση εφόσον κάνουμε λόγο για μη-ορθογώνιες καταστάσεις.

Ο υποκλοπέας στην προκειμένη περίπτωση χρειάζεται πρώτα να γνωρίζει αν οι καταστάσεις ειναι ορθογώνιες ή όχι, ώστε να επιχειρήσει να τις υποκλέψει και να τις κλωνοποιήσει προς τον Β. Παρόλα αυτά, οποιαδήποτε προσπάθεια για απόσπαση πληροφορίας από το σύστημα, διαταράσσει το σύστημα επομένως ειδοποιεί τους Α, Β ότι το κανάλι παρακολουθείται. Ο Β λαμβάνοντας υπόψιν αυτό, θα απορρίψει το μήνυμα και θα ζητήσει εκ νέου αποστολή από τον Α. Επομένως, η κβαντομηχανική δεν αποτρέπει τον υποκλοπέα να αποσπάσει το μήνυμα, αλλά ενημερώνει τον πομπό και τον δεκτή για την ύπαρξη του υποκλοπέα.

2.4 Το πρωτόκολλο BB84

Το πρωτόκολλο BB84 είναι ιστορικά το πρώτο πρωτόκολλο κβαντικής διανομής κλειδιού. Η όλη ιδέα βασίζεται στο ότι όπως στην κλασσική περίπτωση, ο Α στέλνει το μήνυμα με μορφή φωτεινών παλμών 0 και 1, στην δικιά μας υπόθεση ο Α μπορεί τώρα να καθορίσει και την πόλωση που θα έχουν οι παλμοί αυτοί. Διακρίνουμε δύο πολωτικές βάσεις: την $\oplus$ δηλαδή πολωμένο είτε κατά $0°$ είτε κατά $90°$ στον άξονα διέλευσης, και την $\otimes$ δηλαδή πολωμένο είτε κατά $45°$ είτε κατά $135°$ στον άξονα διέλευσης. Με άλλα λόγια το φωτόνιο μας μπορεί να υπάρξει με τις επόμενες τέσσερις καταστάσεις:

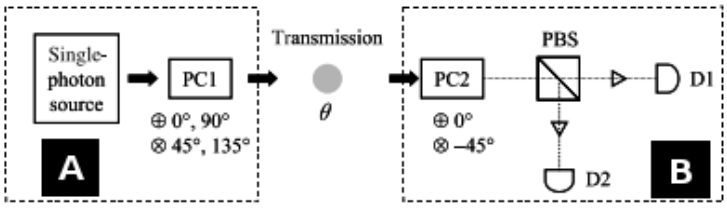
$$|1\rangle^{0°} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|0\rangle^{90°} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|+\rangle^{45°} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|-\rangle^{135°} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

(Σχ. 2.4)



Σχήμα 16: Το πρότυπο BB84

Ο τρόπος που λειτουργεί το πρωτόκολλο BB84 είναι ο εξής: ο Α στέλνει ένα σύνολο φωτονίων στον Β, με το κάθε φωτόνιο πολωμένο κατά την επιλογή του Α. Η πόλωση γίνεται συνήθως μέσω της ηλεκτροπτικής συσκευής "Pockel's cell ", η οποία περιστρέφει το

διάνυσμα πόλωσης σύμφωνα με το εφαρμόζον δυναμικό. Ο Β λαμβάνει τα φωτόνια χρησιμοποιώντας κάθε φορά αυθαίρετη επιλογή βάσεων. Τα φωτόνια εισέρχονται αρχικά στο Pockel's cell του Β και ανάλογα την βάση που επέλεξε, οδηγούνται μέσω ενός διαχωριστή δέσμης σε έναν από τους δύο ανιχνευτές. Ο D1 υποδέχεται φωτόνια σε $|1\rangle$ ή $|+\rangle$ καταστάσεις, ενώ ο D2 τις υπόλοιπες δύο. Επειδή έχουμε να κάνουμε με δύο βάσεις, αυτό σημαίνει ότι ο Β κατά μέσο όρο, θα έχει μαντέψει το μισό πλήθος των φωτονίων σωστά. Μαντεύοντας σωστά ένα φωτόνιο, ανακτά και από ένα bit πληροφορίας που του έστειλε ο Α. Στην αντίθετη περίπτωση, ανακτά ένα τυχαίο bit . Αμέσως μετά, ο Α και ο Β συνομιλούν μέσω ενός δημοσίου καναλιού και αποκαλύπτουν τι βάσεις χρησιμοποίησαν για το κάθε φωτόνιο, χωρίς να αποκαλύψουν την πληροφορία του κάθε φωτονίου. Στην συνέχεια ο Β εκπέμπει στον Α ένα υποσύνολο (sample) των bits με την σωστή βάση, ώστε ο Α να ελέγξει αν υπήρξε υποκλοπέας κατά την μετάδοση και η κατάσταση των bit διαταράχθηκε. Αν διαπυστωθεί ότι δεν υπήρξε παραβίαση, τότε το υπόλοιπο σύνολο των σωστών bits θα χρησιμοποιηθεί σαν ιδιωτικό κλειδί για τους Α και Β.

Υποθέτοντας ότι ο Α και ο Β μοιράζονται μεταξύ τους πολλά μέγιστως κβαντικά διεμπλεγμένα qubits , με κατάσταση της Σχ. 1.6. Γνωρίζουμε ότι τα qubits με τέτοια κατάσταση έχουν πιθανότητα 50% να δώσουν μέτρηση 0 και άλλη 50% να δώσουν μέτρηση 1.

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

(Σχ. 2.5)

Αν ο Α ή ο Β μετράνε είτε σε Q (0° ή 90°) είτε σε Z (45° ή 135°) όπου Q και Z οι πίνακες Pauli , τότε μετράνε σωστά με πιθανότητα 50%. Αν μετρήσουν την ίδια παρατήρηση με σωστή βάση και οι δύο, τότε θα ισχύει η παρακάτω συνθήκη

$$X \otimes X = Z \otimes Z$$

(Σχ. 2.6)

Αν τώρα υποθέσουμε ότι ο υποκλοπέας επηρεάζει την διεμπλοκή των Α και Β, τότε η κοινή διεμπλεγμένη κατάσταση των Α, Β και Υ θα είναι

$$|\phi_{ABU}\rangle = \frac{1}{\sqrt{2}}(|00_{AB}\rangle\,|u_{00}\rangle + |01_{AB}\rangle\,|u_{01}\rangle + |10_{AB}\rangle\,|u_{10}\rangle + |11_{AB}\rangle\,|u_{11}\rangle)$$

(Σχ. 2.7)

Εάν τώρα κάθε ζευγάρι qubit των A και B ικανοποιεί την Σχ. 2.6, τότε η Σχ. 2.5 μπορεί να γραφεί ως

$$|\phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00_{AB}\rangle + |11_{AB}\rangle)\,|u\rangle$$

$$\rightarrow |\phi_{ABY}\rangle = |\phi_{AB}\rangle\,|u\rangle$$

(Σχ. 2.8)

Επομένως τα ζευγάρια των A, B δεν θα συσχετίζονται με τον Υ και σαν αποτέλεσμα δεν θα μπορεί ο Υ να αποκτήσει πληροφορίες επηρρεάζοντας το σύστημα. Όσο περισσότερο διεμπλεγμένοι είναι οι A και B μεταξύ τους, τόσο λιγότερο μπορεί ο Υ να διεμπλακεί με τον A είτε με τον B αντίστοιχα.

2.5 Ανάλυση σφαλμάτων στην κρυπτογραφία

Ας υποθέσουμε ότι ο Υ υποκλέπτει τα εισερχόμενα φωτόνια. Ο Υ μπορεί στην συνέχεια να αποστείλει ένα νέο φωτόνιο στον B, αλλά αφού δεν γνωρίζει ούτε ο Υ την βάση που χρησιμοποίησε ο A, θα πρέπει κάθε φορά να μαντεύει. Επομένως ο Υ θα αποστέλνει με επιτυχία 50%, φωτόνια στον B. Έτσι λοιπόν, αφού και ο B μαντεύει σωστά με επιτυχία 50%, η πιθανότητα σφάλματος μπορεί να οριστεί χονδρικά ως:

$$P_{error} = P^{Y}_{wrongbasis} \times P^{B}_{wrongbasis} = 50\% \times 50\% = 25\%$$

(Σχ. 2.9)

Με άλλα λόγια, ένας ρυθμός σφάλματος $\geq 25\%$ μπορεί να γίνει εύκολα ανιχνεύσιμος κατά την ανάλυση του A και να ξεσκαρτάρουνε τα δύο μέλη τις ανταλλαγμένες πληροφορίες.

Συνοψίζοντας, θα πρέπει να τονίσουμε και την περίπτωση που ο Υ υποκλέπτει τα bits του A, τα οποία δεν θα φτάσουν ποτέ στον B και στην συνέχεια συνομιλεί με τον A παριστάνοντας τον B. Αυτός ο τύπος παραβίασης αντιμετωπίζεται με την κλασσική τεχνική της επαλήθευσης ταυτότητας (identity verification) .

2.6 Διόρθωση των σφαλμάτων

Έκτος από τα σφάλματα που προκύπτουν από την παρέμβαση του υποκλοπέα, μπορεί να προκύψουν και σφάλματα τυχαίας φύσεως που δημιουργούν πρόβλημα στην επικοινωνία Α και Β. Τέτοια σφάλματα είναι η απαλοιφή φωτονίων, η διπλοθλαστικότητα (birefringence) και οι σκοτεινές μετρήσεις των ανιχνευτών (dark counts) . Το συστήμα μας πρέπει να παίρνει μέτρα ώστε να αντιλαμβάνεται και να καταπολεμά τέτοια σφάλματα.

Αρχικά θα κάνουμε λόγο για την απαλοιφή φωτονίων. Απαλοιφή μπορεί να συμβεί λόγω απορρόφησης ή σκέδασης ενός φωτονίου καθώς μεταφέρεται στον Β. Για την διόρθωση αυτού του σφάλματος, θα πρέπει ο Α και ο Β να κρατάνε αρχείο για τους χρόνους κατά τους οποίους έλαβαν τα φωτόνια. Οι χρόνοι αυτοί θα πρέπει να ανακοινωθούν και από τα δύο μέλη κατά την ανάλυση σφάλματος.

Ένα δεύτερο είδος σφάλματος είναι η διπλοθλαστικότητα. Αυτό σημαίνει ότι αν ένα φωτόνιο ταξιδεύει μέσα από διπλοθλαστικό μέσο, ενδέχεται αλλάξει η πολωσή του. Έτσι ο Β ενώ θα έχει διαλέξει την σωστή βάση, θα καταγράφει λάθος αποτέλεσμα. Για την διόρθωση αυτού του τύπου σφάλματος, θα πρέπει ο Α να χρησιμοποιήσει κλασσικές τακτικές ελέγχου, όπως το parity check .

Ένα τρίτο είδος σφάλματος είναι οι σκοτεινές μετρήσεις (dark counts) . Ένα φωτόνιο ξεκινώντας από τον Α, μπορεί να μην φτάσει ποτέ με ακρίβεια στον Β. Ωστόσο ένας από τους ανιχνευτές του Β, μπορεί να καταγράψει μια μέτρηση, η οποία είναι εσφαλμένη και οφείλεται είτε σε θερμικό θόρυβο είτε σε ελλάτωμα του ανιχνευτή. Και αυτός ο τύπος σφάλματος λύνεται όπως και η διπλοθλαστικότητα.

Τέλος, η εμφάνιση όλων αυτών των τυχαίων και συστηματικών σφαλμάτων σημαίνει ότι ο Α θα πρέπει να κοινοποιεί περισσότερα bits πληροφορίας με τον Β και να συγκρίνει τα αποτελέσματα. Επομένως, το πλήθος των bits που αποστέλνει ο Α κάθε φορά, θα πρέπει να έχει ένα ανάλογο μέγεθος που να επιτρέπει την περαιτέρω ανάλυση των σφαλμάτων που θα προκύψουν. Το μέγεθος των απαιτούμενων bits που θα χρησιμοποιηθούν για την διόρθωση των σφαλμάτων, μπορούμε να το καθορίσουμε εύκολα, εφαρμόζοντας το λεγόμενο θεώρημα Shannon's noisy channel coding theorem . Σύμφωνα με το οποίο, το απαιτούμενο πλήθος των bits που θα χρησιμοποιήσει ο Α για διόρθωση, θα είναι:

$$N_{correction} = N \cdot [-\epsilon log_2 \epsilon - (1-\epsilon) log_2 (1-\epsilon)]$$

(Σχ. 2.10)

όπου N το συνολικό πλήθος των αποσταλλούμενων bits και ϵ η πιθανότητα σφάλματος

Βλέπουμε εδώ ότι όσο αυξάνει το ϵ τόσα περισσότερα bits πληροφορίας πρέπει να αχρηστέψουμε, ώστε να απαλοίψουμε το σφάλμα. Στην πράξη, μπορούμε να ανεχτούμε ένα επίπεδο σφάλματος, αρκεί να παραμένει μικρότερο αυτού που εισάγει ο υποκλοπέας. Παρόλα αυτά, βλέπουμε ότι ανάλογα την αρχιτεκτονική του συστήματος, η απόδοση αποστολής πληροφορίας θα πέφτει, λόγω της ύπαρξης τέτοιων σφαλμάτων.

2.7 Πηγές μονών φωτονίων

Βασική απαίτηση της κβαντικής κρυπτογραφείας είναι ο Α να στέλνει ένα φωτόνιο την φορά. Αν ο Α αποστείλει παραπάνω από ένα φωτόνια κάθε φορά, υπάρχει κίνδυνος ο Υ να πάρει κρίσιμες πληροφορίες για το σύστημα. Για παράδειγμα, αν από τον Α φύγουν δύο φωτόνια, ο Υ έχει 50% πιθανότητα να επιλέξει λάθος βάση. Σε περίπτωση επιλογής λάθος βάσης, και τα δύο φωτόνια θα καταλήξουν στους ανιχνευτές του Υ. Επομένως ο Υ θα αντιληφθεί ότι χρησιμοποιεί λάθος βάση. Η λάθος αυτή μέτρηση και παρέμβαση του Υ δεν θα φτάσει ποτέ στον Β, με αποτέλεσμα ο ρυθμός σφάλματος του Υ να μειώνεται με το περιστατικό.

Μια μέθοδος εκπομπής μονών φωτονίων είναι η μείωση της οπτικής ισχύος ενός laser , έτσι ώστε ο μέσος όρος εκπομπής να είναι κοντά στο 0.1 επομένως να ακολουθεί κατανομή Poisson . Αυτή η λύση αν και βολική, δεν είναι αξιόπιστη. Για παράδειγμα ένα laser που λειτουργεί στα 800 nm με συχνότητα 4 MHz, αν μειώσουμε την ισχύ του στα 0.1 pW, θα έχουμε:

$P(0) = \frac{0.1^0}{0!}e^{-0.1} = 90.48\%$ πιθανότητα για μηδενική εκπομπή φωτονίου

$P(1) = \frac{0.1^1}{1!}e^{-0.1} = 9.05\%$ πιθανότητα για εκπομπή ενός φωτονίου

$P(\geq 2) = 1 - (P(0) + P(1)) = 0.47\%$ για εκπομπή δύο και περισσότερων φωτονίων

(Σχ. 2.11)

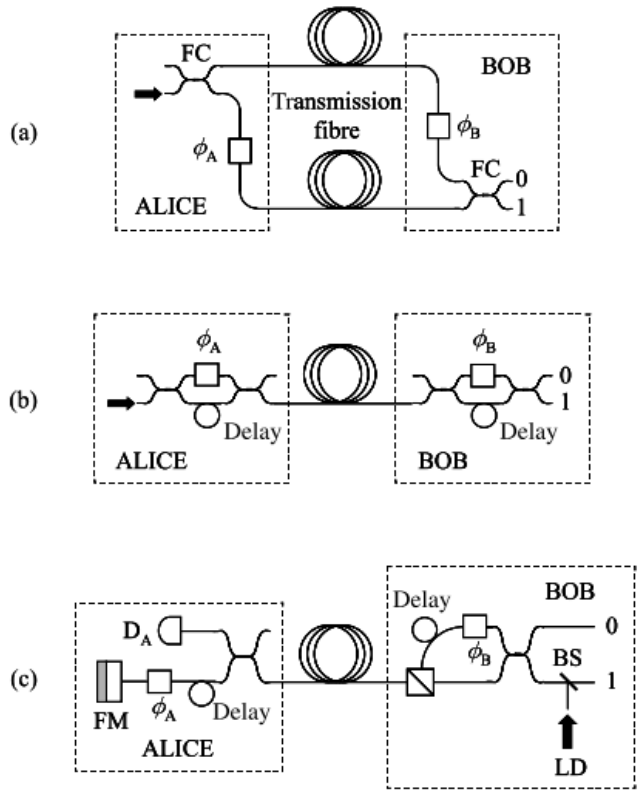
3 Εφαρμοσμένη κβαντική κρυπτογραφία

Στην πράξη, η κβαντική κρυπτογραφεία μπορεί να εφαρμοστεί με δύο τρόπους, είτε με ελεύθερη διάδοση στον χώρο (free space) είτε με διάδοση με οπτικές ίνες. Στην free space εκδοχή, ο Α και ο Β κάνουν χρήση ισχυρών τηλεσκοπίων, παραλληλοποιώντας τα εισερχόμενα και εξερχόμενα φωτόνια ώστε να μην υπάρξουν απώλειες στους ανιχνευτές λόγω περίθλασης. Σαν παράδειγμα αναφέρουμε την free space διάδοση από τους Bennett και Brassard το 1992, όπου με laser 550 nm μετέδωσαν φωτόνια σε ακτίνα 32 cm. Στην σημερινή εποχή, με μήκη κύματος 600-900 nm, επιτυγχάνουμε μετάδοση έως και 23 km. Με αύξηση του μήκου κύματος, οι απώλειες λόγω της τυρβώδης ροής του αέρα (turbulence) μικραίνουν. Τέλος, τα εισαγόμενα σφάλματα λόγω του φωτός του υπόβαθρου (Ήλιος, Σελήνη, φώτα πόλεως κλπ.) μπορεί να αποφευχθεί με χρήση κατάλληλων φίλτρων στους ανιχνευτές.

Όσον αφορά την κβαντική κρυπτογραφεία μέσω οπτικών ινών, η δέσμη δεν παρεκλίνει δηλαδή αφαιρεί την ανάγκη παράλληλων τηλεσκοπίων και το σύστημα είναι ελεγχόμενο χωρίς την παρουσία τυρβωδών ροών κλπ. Παρόλα αυτά, η χρήση οπτικών ινών εισάγει δύο σημαντικά προβλήματα. Η πρώτη δυσκολία είναι ότι κατά την διάδοση η ισχύς του φωτονίου μειώνεται, γεγονός που μπορεί να δώσει λάθος ή καθόλου αποτελέσματα στον Β. Το φωτόνιο μπορεί να μην ανιχνευθεί ποτέ από τον Β ή η ισχύς του να μειωθεί τόσο ώστε να αλλάξει η τιμή του bit που αντιπροσωπεύει. Μια επιπλέον δυσκολία είναι ότι οι οπτικές ίνες είναι εν γένει διπλοθλαστικές, πράγμα που κάνει την χρήση κρυπτογραφικών πρωτόκολλων με χρήση πολωμένων φωτονίων, δύσκολη.

Κρίνοντας ότι η χρήση οπτικών ινών είναι πιο ελεγχόμενη και έμπιστη σε σχέση με την ελεύθερη διάδοση, οι αδυναμίες αυτές στις οπτικές ίνες που αναφέραμε πριν, μπορούν να διορθωθούν. Όσον αφορά την απώλεια κατά την διάδοση, σχετίζεται ισχυρά με το μήκος κύματος που χρησιμοποιείται. Κατά βάση στις οπτικες ίνες χρησιμοποιούνται τα 850, 1300 και 1550 nm. Τα 850 nm εμφανίζουν τις μεγαλύτερες απώλειες, παρόλα αυτά, οι επιλέγοντας τα 1300 και 1550 nm δεν προτείνεται. Αυτό γιατί, φωτόνια μήκους 850 nm ανιχνεύονται με χαμηλό σχετικά θόρυβο, με χρήση ανιχνευτών μονοφωτονικών φωτοδιόδων (SPAD) από πυρίτιο. Αντίθετα, φωτόνια 1300 και 1550 nm ανιχνεύονται από SPAD με μικρότερο ενεργειακό χάσμα (band gap) , όπως ανιχνευτές γερμανίου ή InGaAs . Τετοιου είδους ανιχνευτές εμφανίζουν μεγάλο πλήθος σκοτεινών σημείων (dark counts) , γεγονός που αυξάνει τα σφάλματα.

Τέλος λόγω των θερμικών και μηχανικών αλλαγών που υπόκεινται οι οπτικές ίνες σε μεγάλες αποστάσεις, έχουμε την εμφάνιση της διπλοθλαστικότητας στο υλικό. Έτσι λοιπόν είναι καλύτερο να αφήσουμε τα πολωτικά πρότυπα και να γίνει χρήση διαφορετικού είδους προτύπων. Ένα τέτοιο πρότυπο είναι η κωδικοποίηση οπτικής φάσης (optical phase encoding) , στην οποία ένα συμβολόμετρο Mach-Zehnder χρησιμοποιείται για να κωδικοποιήσει τα μεταδιδόμενα φωτόνια, αλλάζοντας τους την οπτική τους φάση από τον Α στον Β. Τα φωτόνια φεύγουν από τον Α μέσω ενός συζευκτή ίνας. Αν η σχετική διαφορά φάσης είναι $[0, \pi]$ τότε το φωτόνιο ταξιδεύει μέσω της δεύτερης γραμμής του συζευκτή και ερμηνεύεται στην συνέχειά από τον Β σαν φωτεινός ή σκοτεινός κροσσός αντίστοιχα. Στην περίπτωση σχετικής διαφοράς φάσεως $[\pi/2, 3\pi/2]$, το φωτόνιο θα εξέλθει με πιθανότητα 50%, επομένως το πρότυπο είναι αντίστοιχο με αυτό του πολωτικού BB84 . Συμβολόμετρα χρησιμοποιούνται πολλών ειδών.



Σχήμα 17: Τα διάφορα πρότυπα κβαντικής κρυπτογραφίας οπτικής φάσης

Το πιο απλό είδος περιλαμβάνει μια συστοιχία συζευκτών ίνας με τις αντίστοιχες συνδέσεις να συμπεριλαμβάνουν μια συσκευή αλλαγής φάσης. Σε μια πιο σύνθετη μορφή, η σύνδεση που δεν ορίζει αλλαγή φάσης, επιβάλλει μια χρονική καθυστέρηση στο μεταδιδόμενο φωτόνιο. Η εισαγωγή αυτού του μηχανισμού γίνεται για την απαλοιφή της περίπτωσης εκείνης που τα φωτόνια θα επιλέξουν την μικρότερη ή την μεγαλύτερη διαδρομή διάδοσης. Η απαλοιφή αυτή γίνεται ώστε οι διαφορές φάσεως να είναι αυτές που ορίζει το πρότυπο οπτικής φάσης. Μια τελευταία παραλλαγή συμβολόμετρου είναι η παρακάτω. Ένας πολυφωτονικός παλμός στέλνεται μέσω μιας διόδου laser από τον B, διασχίζει έναν διαχωριστή δέσμης με χαμηλή ανακλαστικότητα προς τον A. Τα φωτόνια αυτά φτάνουν στον A και ανακλούνται μέσω μιας συλλογής ενός καθρέφτη και μιας πλάκας καθυστέρησης φάσης π/4 (Faraday mirror) απ΄όπου αναμορφώνονται σε δέσμες μονών φωτονίων και εκπέμπονται πίσω στον B. Αυτό το σύστημα ανάδρασης που χρησιμοποιείται, αφαιρεί την όποια διπλοθλαστικότητα στην οποία υπόκειται το σήμα μας. Τέλος, το συμβολόμετρο εκτελεί την ίδια διαδικασία μετάδοσης από τον A στον B, όπως και στις προηγούμενες περιπτώσεις. Αυτό το μοτίβο κρυπτογραφίας ονομάζεται και plug-and-play και είναι υπεύθυνο για τις μεταδόσεις σε αποστάσεις της τάξεως των km.

Αυτό το back-and-forth μεταξύ αδυναμιών των οπτικών ινών και της υπάρχουσας τεχνολογίας, διαμορφώνει ένα πλαίσιο κατά το οποίο κρυπτογραφικά συστήματα λειτουργούν στα 850 nm με μεγάλη ταχύτητα, ενώ συστήματα με ίνες 1300 και 1550 nm να φτάνουν χαμηλότερες ταχύτητες του αναμενόμενου. Μέχρι στιγμής, ο μεγαλύτερος ρυθμός μετάδοσης κβαντικών bits που έχει επιτευχθεί προς το παρών - λαμβάνοντας υπόψιν τα απαιτούμενα bits για διόρθωση σφάλματος - στα 100,000 bits/second , ταξιδεύοντας σε ίνες 850 nm κατά μήκος 4.2 km.

4 Οι καταστάσεις Bell

Η χβαντική διεμπλοκή είναι ένα φυσικό φαινόμενο κατά το οποίο ένα ζεύγος σωματιδίων παράγεται με τέτοιο τρόπο ώστε η χβαντική κατάσταση του ενός να μην μπορεί να περιγράφει ανεξάρτητα από την κατάσταση του άλλου. Τα δύο σωματίδια συνηπάρχουν σε μια ολική κοινή κατάσταση με το ένα απόλυτα εξαρτημένο από το άλλο. Παράδειγμα τέτοιων καταστάσεων είναι οι λεγόμενες καταστάσεις Bell , οι οποίες μπορούν να διατυπωθούν μαθηματικά ως εξής:

$$\psi_0 = |0\rangle\,|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}$$

$$\Rightarrow \psi_0 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

(Σχ. 4.1)

και

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

(Σχ. 4.2)

Επομένως:

$$\psi_1 = H\,|00\rangle$$

$$\Rightarrow \psi_1 = \frac{1}{\sqrt{2}} \begin{pmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{pmatrix} \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$\Rightarrow \psi_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\psi_2 = CNOT \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\Rightarrow \psi_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\Rightarrow \psi_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

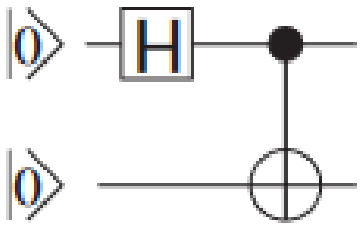
$$\Rightarrow \psi_2 = \frac{1}{\sqrt{2}} \Big(|00\rangle + |11\rangle \Big)$$

(Σχ. 4.3)

Με άλλα λόγια:

$$\psi_2 = C_{10} H_1 \psi_0$$

(Σχ. 4.4)



Σχήμα 18: Το κβαντικό κύκλωμα που μας δίνει τις καταστάσεις Bell

Παίρνοντας διαφορετικά σετ αρχικοποιημένων καταστάσεων $|0\rangle$ και $|1\rangle$, μπορούμε να καταλήξουμε στις τέσσερις ακόλουθες καταστάσεις Bell :

$$\left|\Phi^{+}\right\rangle_{12} = \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_1 \left|0\right\rangle_2 + \left|1\right\rangle_1 \left|1\right\rangle_2 \Big)$$

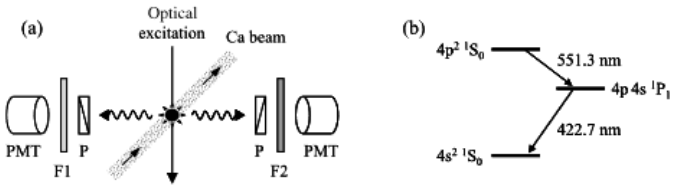
$$\left|\Phi^{-}\right\rangle_{12} = \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_1 \left|0\right\rangle_2 - \left|1\right\rangle_1 \left|1\right\rangle_2 \Big)$$

$$\left|\Psi^{+}\right\rangle_{12} = \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_1 \left|1\right\rangle_2 + \left|1\right\rangle_1 \left|0\right\rangle_2 \Big)$$

$$\left|\Psi^{-}\right\rangle_{12} = \frac{1}{\sqrt{2}}\Big(\left|0\right\rangle_1 \left|1\right\rangle_2 + \left|1\right\rangle_1 \left|0\right\rangle_2 \Big)$$

(Σχ. 4.5)

Δημιουργία διεμπλεγμένων φωτονίων μπορεί να προκύψει πειραματικά εύκολα με έκχυση ατομών ασβεστίου με στάθμη ελάχιστης ενέργειας στα $4s^2\ {}^1S_0$, και διεγείρωντας αρχικά με υπεριώδης ακτινοβολία την δέσμη στην στάθμη $3d4p\ {}^1P_1$ και στην συνέχεια εκπέμποντας στην τελική κατάσταση $4p^2\ {}^1S_0$. Δύο ανιχνευτές στημένοι σε αντίθετες κατευθύνσεις εντοπίζουν την εκπομπή των διεπμλεγμένων φωτονίων. Στο πείραμα που εκτέλεσαν οι Kocher και Commins το 1967, ένα νέφος ατόμων ασβεστίου διεγείρθηκε έως την κατάσταση στάθμης $4p^2\ {}^1S_0$, μέσω απορρόφησης υπεριωδών φωτονίων από μια λυχνία υδρογόνου. Τα φωτόνια λειτουργούσαν σε ένα μήκος κύματος 227.5 nm. Σε μετέπειτα πειράματα, χρησιμοποιήθηκαν φωτόνια μήκους 406 και 581 nm με χρήση λυχνίας laser .



Σχήμα 19: Πειραματική διάταξη για επίτευξη καταστάσεων Bell

Οι αρχικές και τελικές καταστάσεις του νέφους ασβεστίου έχουν σύνθετη στροφορμή $J = 0$ και σταθερό parity . Τις δεκαετίες του 1980 και 1990 χρησιμοποιήθηκε μια οπτική τεχνική μη-γραμμικών κρυστάλλων με όνομα down-conversion , όπου από ένα φωτόνιο υψηλής ενέργειας εκπεμπόμενο με laser και συχνότητα ω_0, μετατρέπεται σε ένα ζεύγος διεμπλεγμένων φωτονίων με συχνότητες ω_1 και ω_2 αντίστοιχα.

$$\omega_0 = \omega_1 + \omega_2$$

$$k_0 = k_1 + k_2$$

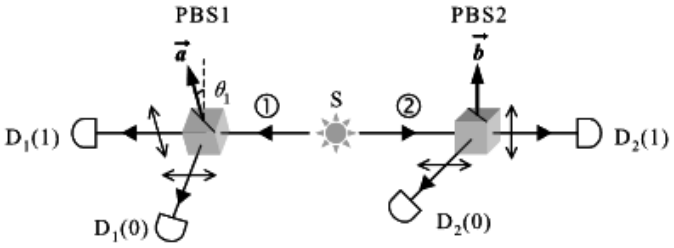
(Σχ. 4.6)

Οι σχέσεις αυτές είναι απόρροια των αρχών διατήρησης ενέργειας και ορμής και υπογραμμίζουν την ανάγκη τα μέτωπα κύματος του laser να είναι συμφασικά. Η τεχνική down-conversion καλείται εκφυλισμένη όταν $\omega_1 = \omega_2$ και μη-εκφυλισμένη όταν δεν ισχύει η παραπάνω σχέση. Ένα γενικό πρόβλημα με τους μη-γραμμικούς κρυστάλλους είναι η διαφοροποίηση του δείκτη διάθλασης σε σχέση με την συχνότητα του φωτός. Παρόλα αυτά λόγω της διπλοθλαστικότητας που διακρίνει αυτό το είδος των κρυστάλλων, η εμφάνιση της διάθλασης λόγω διαφορετικών συχνοτήτων εξισορροπείται από την εξάρτηση του δείκτη διάθλασης από την κατεύθυνση πόλωσης του φωτονίου. Έτσι επιτυγχάνουμε στατιστικά επαρκές πλήθος συμφασικών κυμάτων στον κρύσταλλο που θα μας εξασφαλίζουν την διατήρηση των νόμων ορμής και ενέργειας και επομένως την διεμπλοκή των παραγόμενων φωτονίων.

4.1 Η ανισότητα Bell

Η μεγαλύτερη απόρροια της ύπαρξης διεμπλεγμένων καταστάσεων είναι η εισαγωγή της έννοιας της μη-τοπικότητας. Το γεγονός ότι μετρώντας την κατάσταση του ενός φωτονίου μας δίνει απευθείας την κατάσταση και του δεύτερου, όσο και αν απομακρύνουμε τα δύο φωτόνια μεταξύ τους, η μετάδοση της πληροφορίας από το ένα στο άλλο μοιάζει ακαριαία. Αυτό σημαίνει ότι οι κβαντικοί νόμοι δεν συγκεντρώνονται μέσα σε ένα συγκεκριμένο χώρο, αλλά ισχύουν ανεξαρτήτως τόπου και θέσης μέτρησης. Για παράδειγμα, ο Einstein με αφορμή το

EPR paper θέλησε να αντικρούσει την άποψη της Κοπεγχάγης περί ισχύος της πιθανοκρατικής φύσης της κβαντομηχανικής. Ο Einstein θεώρησε ότι αντί για μια πιθανοκρατική αρχή, φαινόμενα όπως τα μικροσκοπικά (κβαντικής φύσεως) οφείλονται στην ύπαρξη κρυφών τοπικών μεταβλητών, για τις οποίες αδυνατούμε να κάνουμε μετρήσεις ή να τις προσεγγίσουμε. Η πρόταση αυτή του Einstein απορρίφθηκε μετά από τις μελέτες του John Bell το 1964. Ο Bell κατέληξε στο συμπέρασμα ότι τα κβαντικά συστήματα αλληλεπιδρούν μη-τοπικά.



Σχήμα 20: Το πείραμα του Bell

Αρχικά θεώρησε μια πηγή δύο συσχετισμένων φωτονίων που προσλαμβάνονται από ανιχνευτές με μοναδιαίους άξονες πόλωσης $\vec{a}$ και $\vec{b}$ αντίστοιχα. Τα παραγόμενα φωτόνια μπορούν να είναι πολωμένα είτε οριζόντια (1) είτε κάθετα (0). Θεωρούμε τις βάσεις οριζόντιας και κάθετης πόλωσης ότι συμπίπτουν με τους κοινούς άξονες αναφοράς x, y των ανιχνευτών. Επομένως οι πιθανότητες για τα προσδοκούμενα ζευγάρια καταστάσεων πόλωσης των δύο φωτονίων, θα είναι:

$$P_{11}(\theta_a, \theta_b) = \frac{1}{2} cos^2(\theta_a - \theta_b) = 0.25$$

$$P_{10}(\theta_a, \theta_b) = \frac{1}{2} sin^2(\theta_a - \theta_b) = 0.25$$

$$P_{01}(\theta_a, \theta_b) = \frac{1}{2} sin^2(\theta_a - \theta_b) = 0.25$$

$$P_{00}(\theta_a, \theta_b) = \frac{1}{2} cos^2(\theta_a - \theta_b) = 0.25$$

(Σχ. 4.7)

Ενώ στην ειδική περίπτωση όπου $\theta_a = \theta_b = \theta$, θα έχουμε:

$$P_{11}(\theta, \theta) = 0.5$$

$$P_{10}(\theta, \theta) = 0$$

$$P_{01}(\theta, \theta) = 0$$

$$P_{00}(\theta, \theta) = 0.5$$

(Σχ. 4.8)

Μπορούμε να υπολογίσουμε το στατιστικό S:

$$E = \frac{P_{11} + P_{00} - P_{10} - P_{01}}{P_{11} + P_{00} + P_{10} + P_{01}}$$

$$S = E(\theta_a, \theta_b) - E(\theta_a, \theta'_b) + E(\theta'_a, \theta_b) + E(\theta'_a, \theta'_b)$$

(Σχ. 4.9)

Θα βρούμε ότι ισχύει η παρακάτω ανισότητα:

$$-2 \leq S \leq 2$$

(Σχ. 4.10)

Θεωρώντας τις παρακάτω τιμές για τις γωνίες θ_i:

$$\theta_a = 0^\circ$$

$$\theta'_a = 45^\circ$$

$$\theta_b = 22.5^\circ$$

$$\theta'_b = 67.5^\circ$$

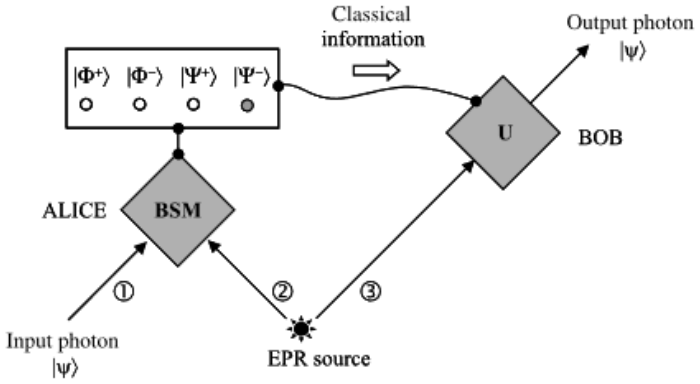
(Σχ. 4.11)

Βρίσκουμε ότι $S = 2\sqrt{2}$, πράγμα που παραβιάζει την (Σχ. 4.10). Στατιστικά λοιπόν, η ανισότητα Bell παραβίαζεται!

4.2 Κβαντική τηλεμεταφορά

Η επιβεβαίωση της μη-τοπικότητας στα κβαντικά συστήματα από τον John Bell έθεσε τα θεμέλια για την έννοια της κβαντικής τηλεμεταφοράς. Η ουσία πίσω από το φαινόμενο είναι η μεταφορά μιας κατάστασης $|\psi\rangle$ από έναν τόπο σε έναν άλλο, χωρίς την άμεση ανταλλαγή qubits . Ένα φωτόνιο q_1 εισάγεται σαν είσοδος με μια κατάσταση $|\psi\rangle$ από έναν αποστολέα Α και εξέρχεται σαν ένα δεύτερο φωτόνιο q_2 με την ίδια ακριβώς κατάσταση $|\psi\rangle$ στον παραλήπτη Β.

Σε αυτό το σημείο θα πρέπει να θυμηθούμε ότι οι κβαντικές καταστάσεις δεν αντιγράφονται ούτε η ύλη τηλεμεταφέρεται. Το φαινόμενο της κβαντικής τηλεμεταφοράς πραγματεύεται την τηλεμεταφορά της κβαντικής πληροφορίας από μια θέση σε μια άλλη. Τέλος η σχετικότητα απογορεύει την μετάδοση πληροφορίας με ταχύτητα μεγαλύτερης του φωτός.



Σχήμα 21: Διάταξη κβαντικής τηλεμεταφοράς

Στο παραπάνω σχήμα φαίνεται η διαγραμματική αναπαράσταση της τηλεμεταφοράς μιας κατάστασης $|\psi\rangle$ ενός φωτονίου (1), με χρήση ενός διεμπλεγμένου ζεύγους φωτονίων (2) και (3). Το φωτόνιο (1) εισέρχεται ως είσοδος σε μια τυχαία κατάσταση:

$$|\psi\rangle_1 = c_0\,|0\rangle + c_1\,|1\rangle$$

(Σχ. 4.12)

Ενώ το διεμπλεγμένο ζεύγος (2,3) ορίζουν την κοινή κατάσταση $Bell$:

$$|\psi\rangle_{23} = \frac{1}{\sqrt{2}}\Big(\,|0\rangle_2\,|1\rangle_3 - |1\rangle_2\,|0\rangle_3\,\Big)$$

(Σχ. 4.13)

η οποία παράγεται με την χρήση της τεχνικής down-conversion που συζητήσαμε παραπάνω.

Η ολική κυματοσυνάρτηση των τριών φωτονίων θα δίνεται από το γινόμενο των παραπάνω δύο:

$$|\psi\rangle_{123} = |\psi\rangle_1\,|\psi\rangle_{23}$$

$$\Rightarrow |\psi\rangle_{123} = \frac{1}{\sqrt{2}}\Big(c_0\,|0\rangle_1\,|0\rangle_2\,|1\rangle_3 - c_0\,|0\rangle_1\,|1\rangle_2\,|0\rangle_3 + c_1\,|1\rangle_1\,|0\rangle_2\,|1\rangle_3 - c_1\,|1\rangle_1\,|1\rangle_2\,|0\rangle_3\,\Big)$$

(Σχ. 4.14)

η οποία με χρήση των τεσσάρων καταστάσεων Bell (Σχ. 4.5) μπορεί να γραφεί ως:

$$|\psi\rangle_{123} = \tfrac{1}{2}\Big[\, |\Phi^+\rangle_{12}\,(c_0\,|1\rangle_3 - c_1\,|0\rangle_3) + |\Phi^-\rangle_{12}\,(c_0\,|1\rangle_3 + c_1\,|0\rangle_3) + |\Psi^+\rangle_{12}\,(-c_0\,|0\rangle_3 + c_1\,|1\rangle_3) - |\Psi^-\rangle_{12}\,(c_0\,|0\rangle_3 + c_1\,|1\rangle_3)\Big]$$

(Σχ. 4.15)

Αμέσως μετά ο Α πραγματοποιεί μια μέτρηση Bell στο ζεύγος (1,2) ώστε να πάρει μια από τις τέσσερις πιθανές καταστάσεις Bell . Για παράδειγμα, αν ο Α μετρήσει το (1,2) στην κατάσταση $|\Phi^+\rangle_{12}$, τότε το φωτόνιο (3) θα πρέπει να βρίσκεται στην κατάσταση:

$$|\psi\rangle_3 = c_0\,|1\rangle_3 - c_1\,|0\rangle_3$$

(Σχ. 4.16)

Επομένως επικοινωνώντας ο Α στον Β για το ποια μέτρηση έλαβε, ο Β γνωρίζει την πληροφορία που κουβαλά το (3) χωρίς να χρειαστεί να το μετρήσει με κάποιο τρόπο. Τέλος, για να αποκτήσει ο Β την ολική πληροφορία του εισαχθέντος φωτονίου (1), εκτελεί έναν μοναδιακό μετασχηματισμό στο φωτόνιο (3). Στην περιπτωσή μας, ο μετασχηματισμός θα είναι ο παρακάτω:

$$U q_3 = q_1$$

$$\Rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -c_1 \\ c_0 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

(Σχ. 4.17)

Μπορούμε διαπυστώσουμε ότι ο μοναδιακός μετασχηματισμός σε αυτή την περίπτωση είναι η επίδραση μιας Z και μιας X πύλης:

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

(Σχ. 4.18)

5 Παράρτημα

Τρεις πολυχρησιμοποιημένοι πίνακες είναι οι 2×2 πίνακες Pauli :

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

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

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

Ως εσωτερικό γινόμενο ορίζουμε:

$$\langle \phi | \psi \rangle = (\alpha_1^* \dots \alpha_n^*) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Ως εξωτερικό γινόμενο ορίζουμε:

$$|\psi\rangle \langle \phi| = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \cdot (b_1^* \dots b_n^*)$$

Ως γινόμενο τανυστών ορίζουμε:

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{pmatrix}$$

όπου A $m \cdot n$ πίνακας και B $p \cdot q$ πίνακας

Η εξέλιξη ενός κλειστού κβαντικού συστήματος περιγράφεται από τον μοναδιακό μετασχηματισμό. Για μια κατάσταση $|\psi\rangle$ σε χρόνο t_0 και μια κατάσταση $|\psi'\rangle$ σε χρόνο $t - t_0$ θα ισχύει:

$$|\psi'\rangle = U\,|\psi\rangle$$

Δεδομένου κάποιων τελεστών μέτρησης M, μπορούμε να ορίσουμε την πιθανότητα πριν μια μέτρηση, να συμβεί ένα γεγονός m ως:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

και την κατάσταση του συστήματος μετά από αυτή, ως:

$$|\psi_m\rangle = \frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

Οι τελεστές μέτρησης θα πρέπει να ικανοποιούν την συνθήκη:

$$\sum_m M_m^\dagger M_m = 1$$

ενώ στην δικιά μας περίπτωση, τα αποτελέσματα των μετρήσεων θέλουμε να είναι είτε 0 είτε 1, άρα διακρίνουμε δύο τελεστές μέτρησης:

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Για τους παραπάνω τελεστές θα ισχύουν:

$$M_0^\dagger = M_0^2 = M_0$$

$$M_1^\dagger = M_1^2 = M_1$$

Έχοντας ένα *qubit* με κατάσταση (Σχ. 1.1), αν λόγου χάρη θέλουμε την πιθανότητα μια μέτρηση να μας δώσει 0, τότε:

$$p(0) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|M_0|\psi\rangle = (\alpha^*\beta^*)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$p(0) = (\alpha^*\beta^*)\begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \alpha^*\alpha = |\alpha|^2$$

με κατάσταση:

$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}}{\sqrt{|\alpha|^2}} = \frac{\begin{pmatrix} \alpha \\ 0 \end{pmatrix}}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle$$

Ομοίως για μέτρηση που θα μας δώσει 1 θα έχουμε:

$$p(1) = |\beta|^2$$

και

$$|\psi'\rangle = \frac{\beta}{|\beta|}|1\rangle$$

Καθώς όμως από την Σχ. 1.6 για την κατάσταση $|+\rangle$ ή την κατάσταση $|-\rangle$ θα έχουμε ότι:

$$p(0) = p(1) = |\alpha|^2 = |\beta|^2 = \frac{1}{2}$$

άρα

$$|\psi_0'\rangle = \frac{\frac{1}{\sqrt{2}}}{\left|\frac{1}{\sqrt{2}}\right|}|0\rangle = |0\rangle$$

και

$$|\psi_1'\rangle = \frac{\frac{1}{\sqrt{2}}}{\left|\frac{1}{\sqrt{2}}\right|}|1\rangle = |1\rangle$$

6 Βιβλιογραφία

1. Quantum Optics An Introduction, Mark Fox
2. The Physics of Quantum Information, Dirk Bouwmeester & Artur Ekert
3. Quantum Computer Science An Introduction (N. David Mermin)
4. Quantum Cryptography From Key Distribution to Conference Key Agreement by Federico Grasselli
5. Cryptography Algorithms A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols (Massimo Bertaccini)
6. Applied Quantum Cryptography (C. Kollmitzer (auth.), Christian Kollmitzer etc.)
7. An introduction to quantum computing (Phillip Kaye, Raymond Laflamme, Michele Mosca)