ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΒΙΟΪΑΤΡΙΚΗΣ

«ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΚΒΑΝΤΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ονοματεπώνυμο φοιτητή: Ανδρέας Ανδριόπουλος
Αριθμός μητρώου:14009
Επιβλέπων Καθηγητής: Ιωάννης Κανδαράκης, Ομότιμος Καθηγητής

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η πτυχιακή/διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
	Ιωάννης Κανδαράκης	Ομότιμος Καθηγητής	Kandarakis Ioannis Digitally signed by Kandarakis Ioannis Date: 2021.10.29 20:30:09 +03'00'
	Γεώργιος Φούντος	Καθηγητής	Georgios Fountos Digitally signed by Georgios Fountos Date: 2021.11.01 11:54:05 +02'00'
	Χρήστος Μιχαήλ	Επίκουρος Καθηγητής	Christos Michail Digitally signed by Christos Michail Date: 2021.11.01 10:17:07 +02'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ανδρέας Ανδριόπουλος του Νικολάου, με αριθμό μητρώου 14009 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Βιοϊατρικής, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου».

Ο Δηλών

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποτελεί μια μελέτη επί των διαφόρων τεχνολογιών στην Κβαντική Επικοινωνία. Ειδικότερα, αναλύονται τα πλεονεκτήματα που διαθέτει η χρήση κβαντικών τεχνολογιών έναντι των κλασικών τηλεπικοινωνιών, ενώ γίνεται αναφορά και στο πώς θα μπορούσαμε να υλοποιήσουμε τέτοιες τεχνικές.

Η δομή της εργασίας είναι η εξής: στο 1^{ο} κεφάλαιο γίνεται μια αναγκαία επισκόπηση των βασικών εννοιών της Κβαντομηχανικής. Ύστερα, στο 2^{ο} κεφάλαιο αναπτύσσονται τα βασικά της κβαντικής υπολογιστικής (qubits, κβαντικές πύλες κτλ.) και αφού παρατεθούν οι βασικές αυτές έννοιες, δίνουμε μια περιγραφή των στοιχειωδών περί Κβαντικής Κρυπτογραφίας και Κβαντικής Διανομής Κλειδιού. Στο 3^{ο} κεφάλαιο παραθέτουμε κάποιες πρώτες απόπειρες υλοποίησης συστημάτων κβαντικών υπολογιστών, ειδικότερα γίνεται λόγος για ιοντικούς κλωβούς (ion traps) και για την εφαρμογή NMR τεχνολογιών στην κβαντική υπολογιστική. Τέλος, το 4^{ο} κεφάλαιο αποτελεί μια επισκόπηση των πιο σύγχρονων τεχνολογιών στην Κβαντική Επικοινωνία. Συγκεκριμένα, αναφερόμαστε (i) σε ποικίλες εφαρμογές της κβαντικής οπτικής στις επικοινωνίες, (ii) στην δυνατότητα ανάπτυξης κβαντικού διαδικτύου, (iii) στο πρόγραμμα της CubeSat για την αξιοποίηση κβαντικών τεχνολογιών σε δορυφορικά συστήματα και (iv) την δυνατότητα εκτέλεσης κβαντικής επικοινωνίας σε κανάλια μηδενικής χωρητικότητας.

ABSTRACT

The present thesis comprises a study upon various technologies that stem from quantum communication. In particular, we analyze the advantages of quantum technologies over classical communication, while possible ways of applying said technologies are also examined.

The structure of this thesis is as follows: in Chapter 1 we overview some necessary theory of quantum mechanics. Then, in Chapter 2 we develop the fundamentals of quantum computing (qubits, quantum gates etc.) and once these fundamental terms have been develop, we give a description of the basics in quantum cryptography and quantum key distribution. In Chapter 3 we list several attempts that have been made for the implementation of quantum computing. In particular, we discuss ion traps and NMR technology applications in quantum computing. Finally, Chapter 4 comprises an overview of modern technologies in quantum communications. More specifically, we refer to (i) various applications of quantum optics in communications, (ii) the capability of developing quantum internet, (iii) the CubeSat program for utilization of quantum technologies in satellite systems and (iv)the capability of carrying out quantum communication through zero capacity channels.

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όσους συνέβαλλαν σε αυτή.

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου , κύριο Ιωάννη Κανδαράκη, για την εμπιστοσύνη που μου έδειξε, δίνοντας μου αυτό το θέμα, την επιστημονική του καθοδήγηση, τις υποδείξεις του, την επιμονή του και το αμείωτο ενδιαφέρον που έδειξε από την αρχή μέχρι το τέλος.

Επίσης, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για την στήριξή τους, την συμπαράσταση και την κατανόηση που έδειξαν σε όλη την διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

Κεφάλαιο 1^{ο} : Ανασκόπηση βασικής Κβαντομηχανικής.

1.1 Τελεστές, Εξίσωση Schrodinger

Ξεκινάμε την παρούσα εργασία παρουσιάζοντας κάποια στοιχεία της θεωρίας της Κβαντομηχανικής. Η Κβαντομηχανική αποσκοπεί, κατά κύριο λόγο, στη μελέτη της «μηχανικής» σε συστήματα αρκετά μικρά- ατομικής/υποατομικής κλίμακας- και των νόμων που διέπουν τα διάφορα φαινόμενα στην κλίμακα αυτή. Πιο αναλυτική μελέτη των ακολούθων μπορεί να βρεθεί στα [1],[2].

Η βασική διαφορά με την κλασική μηχανική είναι ότι με την πάροδο του χρόνου διαπιστώθηκε ότι η κατάλληλη προσέγγιση για τα μικρής κλίμακας συστήματα είναι η πιθανοθεωρητική, και άρα τα συστήματα αυτά διέπονται από τυχαιότητα και όχι από απόλυτα ντετερμινιστικούς νόμους. Στην βάση της Κβαντομηχανικής βρίσκεται ο λεγόμενος κυματοσωματιδιακός δυϊσμός, ότι δηλαδή κάθε σωματίδιο μπορεί να θεωρηθεί ότι αποτελεί συγχρόνως κύμα (και αντίστροφα). Για αυτό το κύμα, όμως, δεν αντιστοιχεί η γνωστή από την Κλασική Μηχανική κυματική εξίσωση, αλλά ο αντίστοιχος «νόμος» στην Κβαντομηχανική εκφράζεται με την εξίσωση του Schrödinger:

$$i\hbar\frac{\partial\Psi}{\partial t}(\boldsymbol{r},t) = -\frac{\hbar^2}{2m}\nabla^2\Psi(\boldsymbol{r},t) + V(\boldsymbol{r})\cdot\Psi(\mathbf{r},\mathrm{t}) \quad (1.1)$$

όπου η μιγαδική συνάρτηση Ψ είναι η λεγόμενη *κυματοσυνάρτηση* του συστήματος. Η ίδια η κυματοσυνάρτηση δεν έχει κάποια φυσική σημασία, αλλά το τετράγωνο του μέτρου της $|\Psi(\boldsymbol{r},t)|^2 = \Psi^*(\boldsymbol{r},t)\Psi(\boldsymbol{r},t)$ εκφράζει μια *πυκνότητα πιθανότητας*, δηλαδή λ.χ. στην περίπτωση της μιας διάστασης η πιθανότητα ένα σωματίδιο, που του αντιστοιχεί η κυματοσυνάρτηση Ψ, να βρεθεί στο διάστημα [a,b] θα είναι ίση με

$$\int_a^b |\Psi(x,t)|^2 dx$$

Όλα τα υπόλοιπα από εκεί και έπειτα περιστρέφονται γύρω από την κυματοσυνάρτηση. Αυτό σημαίνει, επι της ουσίας, ότι οποιοδήποτε φυσικό μέγεθος

που πιθανόν να μας ενδιαφέρει να μελετήσουμε – ορμή, ενέργεια, στροφορμή κλπ- μπορεί να αναπαρασταθεί ως τελεστής, ο οποίος δρα πάνω στην κυματοσυνάρτηση Ψ. Παραδείγματος χάριν, ο τελεστής της Χαμιλτονιανής $\widehat{H}$ αντιστοιχεί στην συνολική ενέργεια του συστήματος και η δράση του στην κυματοσυνάρτηση Ψ είναι $\widehat{H} = i\hbar\frac{\partial\Psi}{\partial t}$. Προφανώς αυτοί οι τελεστές δεν είναι ιδιαίτερα χρήσιμοι σε ό,τι αφορά εργαστηριακές μετρήσεις, αλλά οι πιθανές τιμές που μπορούμε να μετρήσουμε δεν είναι τίποτα άλλο παρά οι ιδιοτιμές του συγκεκριμένου τελεστή, δηλαδή είναι εκείνοι οι αριθμοί Ε για τους οποίους υπάρχει μια συνάρτηση Ψ με:

$$\widehat{H}\Psi = E\,\Psi$$

Οι αντίστοιχες Ψ λέγονται ιδιοσυναρτήσεις της ιδιοτιμής Ε ή και ιδιοκαταστάσεις του συστήματος. Ιδιαίτερο χαρακτηριστικό των κβαντομηχανικών συστημάτων αποτελεί το ότι την στιγμή που λαμβάνουμε μια μέτρηση, επέρχεται αυτό που ονομάζουμε κατάρρευση της κυματοσυνάρτησης. Αυτό, πρακτικά, σημαίνει ότι αν έχουμε μια κυματοσυνάρτηση Ψ η οποία να αναλύεται στις ιδιοκαταστάσεις Ψ_n , δηλ. γράφεται $\Psi = \sum_{n=1}^{\infty} c_n\Psi_n$ και μετρήσουμε λ.χ. την ενέργεια που αντιστοιχεί στην n-οστή κατάσταση, τότε η προηγούμενη κυματοσυνάρτηση παύει να περιγράφει το σύστημα, όλες οι άλλες ιδιοκαταστάσεις δεν συνεισφέρουν και η μοναδική κυματοσυνάρτηση που συνεισφέρει στην περιγραφή του συστήματος πλέον είναι η Ψ_n.

Για έναν τελεστή μπορούμε να κάνουμε κάποιες εκτιμήσεις ως προς την αναμενόμενη τιμή του και τη διασπορά (στατιστική διακύμανση) του κάθε τέτοιου τελεστή. Η μέση τιμή, για παράδειγμα, ενός κβαντομηχανικού τελεστή $\hat{A}$ θα είναι (εδώ θεωρούμε ότι μιλάμε για μια διάσταση):

$$\langle\hat{A}\rangle = \int_{-\infty}^{+\infty} \psi^*(x,t)\ \hat{A}\psi(x,t)dx \quad (1.2)$$

Ενώ αντίστοιχα ορίζεται και η αβεβαιότητα του τελεστή ως:

$$\Delta\hat{A} = \sqrt{\langle\left(\hat{A} - \langle\hat{A}\rangle\right)^2\rangle} = \sqrt{\langle\hat{A}^2\rangle - \left(\langle\hat{A}\rangle\right)^2} \quad (1.3)$$

Οι κβαντομηχανικοί τελεστές είναι συνήθως (αν όχι πάντα) ερμιτιανοί, δηλαδή ικανοποιούν την ιδιότητα:

$$(\psi, A\phi) = \int \psi^*\,\hat{A}\phi dx = \int \left(\hat{A}\phi\right)^*\phi dx = \left(\hat{A}\psi, \phi\right) \quad (1.4)$$

και σε αυτήν την περίπτωση ο $\hat{A} = \hat{A}^{\dagger}$, όπου ο $A^{\dagger}$ είναι ο συζυγής του $\hat{A}$.

Οι βασικοί κβαντομηχανικοί τελεστές ως προς τους οποίους συνήθως εκφράζονται οι υπόλοιποι είναι οι τελεστές της θέσης:

$$\hat{x} = x, \hat{y} = y, \hat{z} = z \ \ \textit{ή διανυσματικά}\ \hat{\boldsymbol{r}} = \boldsymbol{r} \quad (1.5)$$

και οι τελεστές της ορμής:

$$\widehat{p_x} = -i\hbar\frac{\partial}{\partial x}\ ,\widehat{p_y} = -i\hbar\frac{\partial}{\partial y}, \widehat{p_z} = -i\hbar\frac{\partial}{\partial z}\ \text{ ή διανυσματικά }\ \hat{\boldsymbol{p}} = -i\hbar\nabla \ (1.6)$$

Τότε, έχουμε λ.χ.:

-Τον τελεστή της Χαμιλτονιανής

$$\hat{H} = \hat{H}(\hat{\boldsymbol{r}}, \hat{p}) = \frac{\hat{p}^2}{2m} + V(\boldsymbol{r}) (1.7)$$

- Τον τελεστή της στροφορμής:

$$\hat{\boldsymbol{l}} = \hat{\boldsymbol{l}}(\hat{\boldsymbol{r}}, \hat{\boldsymbol{p}}) = \hat{\boldsymbol{r}} \times \hat{\boldsymbol{p}} = -i\hbar\boldsymbol{r} \times \nabla \ (1.8)$$

Σημαντική για την μελέτη των κβαντομηχανικών τελεστών είναι η έννοια του μεταθέτη. Αν $\hat{A}, \hat{B}$ δυο τελεστές, τότε ορίζουμε ως τον μεταθέτη τους να είναι:

$$\left[\hat{A}, \hat{B}\right] = \hat{A}\ \hat{B} - \ \hat{B}\ \hat{A}\ (1.9)$$

(Στην συνέχεια θα παραλείπουμε τα ˆ από τους τελεστές, οι οποίοι θα συμβολίζονται με χρήση κεφαλαίων γραμμάτων κατά κύριο λόγο). Κάποιες βασικές ιδιότητες των μεταθετών είναι οι εξής:

$$-[A, B] = -[B, A]\ (1.10)$$

$$-[A, B + C] = [A, B] + [A, C]\ (1.11)$$

$-[A, BC] = [A, B]C + B[A, C]$ (Γενικότερα, αν $A_1, A_2, \dots, A_n$ τότε $[A, A_1, \dots, A_i, \dots, A_n] = \sum_{i=1}^{n} A_1 \dots A_{i-1}[A, A_i]A_{i+1} \dots A_n$) (1.12)

Η έννοια του μεταθετή, μεταξύ άλλων, μας δίνει μια σημαντική πληροφορία για δυο φυσικά μεγέθη: το κατά πόσον ο μεταθέτης δυο κβαντομηχανικών τελεστών είναι 0 ή όχι μας δηλώνει το αν μπορούμε να μετρήσουμε ταυτόχρονα τιμές για τα αντίστοιχα φυσικά μεγέθη των τελεστών αυτών, χωρίς η μια μέτρηση να επηρεάζει την άλλη. Επιπλέον, μπορεί κανείς να εκφράσει τον ρυθμό μεταβολής μιας ποσότητας μέσω μεταθετών. Συγκεκριμένα, ισχύει ότι:

$$i\hbar\frac{d\langle A\rangle}{dt} = \langle[A, H]\rangle\ (1.13)$$

Αυτή η τελευταία σχέση μας δηλώνει ότι αν μια ποσότητα μετατίθεται με την Χαμιλτονιανή Η, τότε είμαστε σε θέση να πούμε ότι -κατά μέσο όρο- το μέγεθος που αντιστοιχεί στον τελεστή Α διατηρείται στο φυσικό σύστημα που μελετάμε. Επιπλέον, ισχύει το λεγόμενο θεώρημα του Ehrenfest, που μας λέει ότι οι μέσες τιμές των φυσικών μεγεθών –δηλαδή των αντιστοίχων τελεστών- υπακούουν στις ίδιες εξισώσεις με αυτές της κλασικής μηχανικής.

1.2 Αρχή της Αβεβαιότητας

Ανάμεσα στα γνωστά αποτελέσματα της θεωρίας της Κβαντομηχανικής είναι η λεγόμενη Αρχή της αβεβαιότητας θέσης-ορμής του Heisenberg:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \ (1.14)$$

Η ανισότητα αυτή εκφράζει το γεγονός ότι δεν μπορούμε να έχουμε πλήρως προσδιορισμένες την θέση ενός σωματιδίου και την ορμή του ταυτόχρονα, αλλά όταν αποκτάμε περισσότερη πληροφορία για το ένα μέγεθος, τόσο αυξάνεται η αβεβαιότητα για το άλλο. Γενικότερα, αν Α,Β δύο τελεστές που αντιστοιχούν σε κάποια φυσικά μεγέθη τα οποία είναι ασυμβίβαστα (αυτό σημαίνει ότι $[A, B] \neq 0$) τότε ισχύει ότι:

$$\Delta A \cdot \Delta B \geq \frac{1}{2} |\langle [A, B] \rangle| \ (1.15)$$

Εύκολα δείχνει κανείς ότι $[x, p] = i\hbar$, επομένως αντικαθιστώντας $A = x$ και $B = p$ στην τελευταία σχέση παίρνουμε την προαναφερθείσα μορφή της αρχής αβεβαιότητας θέσης-ορμής.

Αν επιλέξουμε, τώρα, στην γενική μορφή της αρχής της αβεβαιότητας $B = H$ τότε παίρνουμε:

$$\Delta A \cdot \Delta E \geq \frac{1}{2} |\langle [A, H] \rangle| = \frac{\hbar}{2} \left| \frac{d\langle A \rangle}{dt} \right| \ (1.16)$$

όπου συμβολίσαμε ΔΕ την αβεβαιότητα για την ενέργεια. Μπορούμε, αναδιατάσσοντας τους όρους να γράψουμε:

$$\frac{\Delta A}{|\frac{d\langle A \rangle}{dt}|} \Delta E \geq \frac{\hbar}{2} \ (1.17)$$

Ορίζοντας $\tau_A = \frac{\Delta A}{|\frac{d\langle A \rangle}{dt}|}$ να είναι ο *χαρακτηριστικός χρόνος εξέλιξης του συστήματος ως προς το μέγεθος Α* και παίρνοντας τ να είναι το ελάχιστο αυτών των χρόνων πάνω στα φυσικά μεγέθη του συστήματος, έχουμε ότι:

$$\tau \cdot \Delta E \geq \frac{\hbar}{2}$$

και αυτή η σχέση είναι γνωστή ως σχέση αβεβαιότητας χρόνου-ενέργειας. Το περιεχόμενο αυτής της σχέσης είναι το εξής: η δυνατότητα να εκτιμήσουμε σε ένα βαθμό την ενέργεια ενός κβαντομηχανικού συστήματος είναι αντιστρόφως ανάλογη του χρόνου που χρειάζεται για να παρουσιαστεί μια ουσιαστική μεταβολή στο σύστημα.

1.3 Φορμαλισμός Dirac

Ο συμβολισμός που εισήγαγε στην Κβαντομηχανική ο Paul Dirac αποτελεί μια γενίκευση της έννοιας των διανυσμάτων γραμμή και στήλη. Γράφουμε, αρχικά:

$$(\psi, \phi) = \langle \psi | \phi \rangle = \int \psi^*(x)\phi(x)dx \ (1.18)$$

Από τον συμβολισμό του εσωτερικού γινομένου με χρήση αγκυλών (brackets) θα θεωρούμε ως «διανύσματα στήλη» τα ket $|\psi\rangle$ και ως «διανύσματα γραμμή» τα bra $\langle\psi|$. Επομένως, το εσωτερικό γινόμενο δύο τέτοιων «διανυσμάτων» είναι σαν να παραθέτουμε το bra δίπλα στο αντίστοιχο ket για να σχηματιστεί το bracket. Αντίστοιχα, σε αυτόν τον συμβολισμό, γράφουμε για έναν τελεστή A:

$$\langle A \rangle = \langle \psi | A | \psi \rangle \ (1.19)$$

Αντίστοιχα, σε ένα σύστημα με ιδιοκαταστάσεις ψ_n ,συμβολίζοντας $|n\rangle$ το διάνυσμα που αντιστοιχεί στην ιδιοκατάσταση ψ_n, έχουμε ότι:

$$\psi = \sum_{n=1}^{\infty} c_n |n\rangle \ (1.20)(\alpha) \kappa \alpha \iota \ A = \sum_{n=1}^{\infty} a_n |n\rangle\langle n| \ (1.20)(\beta)$$

όπου a_n οι αντίστοιχες ιδιοτιμές του A στην n-οστή ιδιοκατάσταση.

1.4 Κβαντικά συστήματα πολλών σωμάτων

Μέχρι στιγμής έχουμε καλύψει την περίπτωση κβαντικών συστημάτων με ένα μόνο σωματίδιο. Στη συνέχεια θα επισημάνουμε πώς περιγράφονται τα συστήματα

πολλαπλών σωματιδίων. Αν λ.χ. αναφερόμαστε σε ένα σύστημα δύο σωμάτων που η κυματοσυνάρτηση του καθενός είναι ψ_a, ψ_β αντίστοιχα, τότε η κυματοσυνάρτηση του συστήματος θα είναι:

$$\psi_{\alpha\beta}(r_1, r_2) = \psi_\alpha(r_1)\psi_\beta(r_2) \ (1.21)$$

με τους α, β να είναι κβαντικοί αριθμοί που διατρέχουν ένα πλήρες σύνολο τιμών (δηλαδή οι ψ_α, ψ_β είναι δύο πλήρεις βάσεις μονοσωματιδιακών κυματοσυναρτήσεων). Έτσι, η γενική κατάσταση του συστήματος θα γράφεται σε μορφή επαλληλίας αυτών των καταστάσεων:

$$\psi = \sum_{\alpha,\beta} c_{\alpha\beta}\, \psi_{\alpha\beta}(r_1, r_2) = \sum_{\alpha,\beta} c_{\alpha\beta}\psi_\alpha(r_1)\psi_\beta(r_2) \ (1.22)$$

Με τέτοιες επαλληλίες γινομένων από μονοσωματιδιακές κυματοσυναρτήσεις κατασκευάζουμε την τυχούσα κατάσταση ενός συστήματος δύο σωματιδίων. Αν επαναφέρουμε, λοιπόν, τον συμβολισμό του Dirac και θεωρήσουμε τις μονοσωματιδιακές καταστάσεις των δύο σωματιδίων με τα ket $|\alpha\rangle, |\beta\rangle$ τότε η κατάσταση που αποτελεί το γινόμενο αυτών των δύο και περιγράφει την κοινή κατάσταση του συστήματος των δυο σωμάτων γράφεται ως:

$$|a, \beta\rangle = |\alpha\rangle|\beta\rangle$$

Σε κάποιες περιπτώσεις, αυτή η έκφραση είναι γνωστή και ως τανυστικό γινόμενο ή γινόμενο Kronecker των δύο μονοσωματιδιακών καταστάσεων και συμβολίζεται με $|a\rangle \otimes |\beta\rangle$. Χάριν απλότητος, δεν θα υιοθετήσουμε στη συνέχεια αυτών των συμβολισμό.

Στη συνέχεια θα αναπτύξουμε το πώς χειριζόμαστε αυτά τα αντικείμενα. Αν έχουμε, λ.χ., δυο τέτοια διανύσματα $|\alpha, \beta\rangle, |\alpha', \beta'\rangle$ τότε ισχύει ότι:

$$\langle\alpha, \beta|\alpha', \beta'\rangle = \langle\alpha|\alpha'\rangle\langle\beta|\beta'\rangle$$

Γενικότερα, αν έχουμε έναν κβαντομηχανικό τελεστή Α που δρα στις καταστάσεις του γινομένου, αυτός θα αναλύεται σε δύο συνιστώσες A_1, A_2 με τον A_1 να δρα στην κυματοσυνάρτηση του πρώτου σωματιδίου και τον A_2 στου δεύτερου. Συμβολίζουμε αντίστοιχα $A = A_1 \otimes A_2$ και ισχύει:

$$\langle\alpha, \beta|A|\alpha, \beta\rangle = \langle\alpha|A_1|\alpha\rangle\langle\beta|A_2|\beta\rangle$$

και φυσικά τα παραπάνω μπορούν να επεκταθούν και σε συστήματα σωμάτων περισσότερων των δύο.

1.5 Ο τελεστής πυκνότητας

Στην διαχείριση συστημάτων πολλαπλών σωμάτων ιδιαίτερο ρόλο παίζει ο λεγόμενος τελεστής πυκνότητας.

Όταν η κυματοσυνάρτηση ενός κβαντικού συστήματος μπορεί να περιγράφει από μια επαλληλία των ιδιοσυναρτήσεων τότε λέμε ότι αυτές οι επαλληλίες αποτελούν καθαρές καταστάσεις. Σε αυτήν την περίπτωση, δηλαδή αν η κυματοσυνάρτηση είναι $|\Psi\rangle = \sum_{n=1}^{\infty} c_n|\mathrm{n}\rangle$ τότε ο τελεστής πυκνότητας δίνεται από την:

$$\rho = |\Psi\rangle\langle\Psi| = \sum_n \sum_m c_n c_m^* |\mathrm{n}\rangle\langle\mathrm{m}| = \sum_n \sum_m \rho_{nm} |\mathrm{n}\rangle\langle\mathrm{m}| \quad (1.23)$$

Όπως φαίνεται από την τελευταία σχέση, μπορούμε να αναπαραστήσουμε τον ρ ως έναν πίνακα με στοιχεία τα ρ_{nm}. Τα διαγώνια στοιχεία αυτού του πίνακα πυκνότητας έχουν την εξής φυσική σημασία: ότι η πιθανότητα να βρεθεί το σύστημα στην κατάσταση $|\mathrm{n}\rangle|$ ισούται με ρ_{nn} . Για αυτό τα στοιχεία αυτά λέγονται και πληθυσμοί. Επίσης, ο τελεστής της πυκνότητας είναι ερμιτιανός και ισχύουν τα εξής:

$$Tr(\rho) = 1 \ (1.24)(\alpha) \ \kappa\alpha\iota \ |\rho_{mn}|^2 = \rho_{mm}^2 \rho_{nn}^2 (1.24)(\beta)$$

απ' όπου είναι σαφές ότι:

$$Tr(\rho^2) = 1 \ (1.25)(\alpha) \ \kappa\alpha\iota \ \rho^2 = \rho \ \ (1.25)(\beta)$$

Σε πολλές περιπτώσεις, όμως, ένα κβαντικό σύστημα δεν βρίσκεται σε καθαρή κατάσταση. Αυτό οφείλεται στο ότι ένα οποιοδήποτε κβαντικό σύστημα ενδεχομένως να αλληλοεπιδρά με άλλα, το οποίο οδηγεί στο φαινόμενο της κβαντικής διεμπλοκής ή συμπλοκής ή εναγκαλισμού (entanglement). Σε αυτές τις περιπτώσεις, το σύστημά μας είναι ένα μείγμα από καθαρές κβαντικές καταστάσεις, καθεμία εκ των οποίων διαθέτει τις δικές της ιδιοκαταστάσεις. Αν P_Ψ η πιθανότητα το σύστημα να βρεθεί σε μια από τις καθαρές καταστάσεις $|\Psi\rangle$, τότε ο τελεστής πυκνότητας δίνεται από την:

$$\rho = \sum_\Psi P_\Psi \, |\Psi\rangle\langle\Psi| \ (1.26)$$

Σαφώς ο ρ είναι ερμιτιανός, ενώ ο τελεστής θα είναι της μορφής:

$$\rho = \sum_\Psi \sum_{nm} P_\Psi \ c_n^\Psi (c_m^\Psi)^* |\mathrm{n}\rangle\langle\mathrm{m}| \quad (1.27)$$

Μια σημαντική διαφορά με πριν είναι ότι εδώ:

$$Tr(\rho) = \sum_\Psi P_\Psi \ \ (1.28)$$

Σημαντική διαφορά με πριν, επίσης, αποτελεί το γεγονός ότι ο ρ δεν είναι ταυτοδύναμος στην περίπτωση μείγματος, δηλαδή $\rho^2 \neq \rho$.

Η βασική χρήση του τελεστή πυκνότητας είναι η ακόλουθη: σε καθαρές καταστάσεις, έχουμε αναφέρει ότι η μέση τιμή ενός τελεστή υπολογίζεται με την βοήθεια των ιδιοκαταστάσεων. Ο αντίστοιχος υπολογισμός για ένα μείγμα γίνεται με την βοήθεια του τελεστή πυκνότητας. Ειδικότερα, ισχύει ότι:

$$< A > = Tr(\rho A)$$

Επιπλέον, μπορεί να δείξει κανείς ότι ο τελεστής πυκνότητας ικανοποιεί την εξίσωση:

$$\frac{\partial}{\partial t}\rho = -i[H, \rho] (1.29)$$

που στην περίπτωση καθαρής κατάστασης, δεν είναι παρά η εξίσωση του Schrödinger. Η εξίσωση αυτή λέγεται εξίσωση von Neumann/Liouville και αποτελεί άλλη μια ένδειξη του ότι σε συστήματα πολλαπλών σωμάτων, αν γνωρίζουμε τον τελεστή πυκνότητας, μπορούμε να περιγράψουμε ολόκληρο το σύστημα.

1.6 Εικόνα του Heisenberg

Μεταξύ άλλων, ο φορμαλισμός του Dirac έχει το προτέρημα ότι μας επιτρέπει να αλλάζουμε εύκολα την αναπαράσταση του φυσικού συστήματος σε αυτήν που μας βολεύει περισσότερο. Αν U ένας μοναδιαίος τελεστής – δηλαδή τέτοιος ώστε $U^\dagger U = I$ με I να είναι ο ταυτοτικός τελεστής- θέτοντας $|\psi'\rangle = U|\psi\rangle$ και για τον τυχαίο τελεστή A θέτοντας $A' = UAU^\dagger$ έχουμε μια διαφορετική περιγραφή του φυσικού συστήματος η οποία, όμως, αφήνει αναλλοίωτα τα βασικά μεγέθη (μέσες τιμές, αβεβαιότητες). Για παράδειγμα:

$$\langle A' \rangle = \langle \psi' | A' | \psi' \rangle = \langle \psi | U^\dagger A' U | \psi \rangle = \langle \psi | A | \psi \rangle = A \ (1.30)$$

Μπορεί να δείξει κανείς ότι η μετάβαση από την μια περιγραφή στην άλλη αφήνει αναλλοίωτες και τις μεταθετικές σχέσεις μεταξύ τελεστών. Αυτό είναι σημαντικό, διότι μπορούμε να προσεγγίσουμε το ίδιο σύστημα υπό μια διαφορετική οπτική.

Ειδικότερα, αν θεωρήσουμε τον τελεστή $U = e^{i\hbar Ht}$ παίρνουμε την λεγόμενη περιγραφή της κβαντομηχανικής κατά Heisenberg.Ισχύει γενικά ότι:

$$|\psi(t)\rangle = e^{-i\hbar Ht}|\psi(0)\rangle \ (1.31)$$

Άρα, για τις νέες καταστάσεις θα είναι:

$$\left|\psi_H\right\rangle = e^{i\hbar Ht}\left|\psi(t)\right\rangle = |\psi(0)\rangle \ (1.32)$$

δηλαδή σε αυτήν την θεώρηση, δεν υπάρχει χρονική μεταβολή της κυματοσυνάρτησης, αλλά η χρονική εξέλιξη του συστήματος μεταφέρεται στους τελεστές. Έτσι, αν Α ένας τελεστής, τότε:

$$A_H(t) = e^{iHt}Ae^{-iHt} \ (1.33)$$

Κεφάλαιο 2ο : Θεωρία Κβαντικής Υπολογιστικής/Κβαντικής Επικοινωνίας

2.1.Εισαγωγή

Έχοντας θέσει πλέον τα θεμέλια, μπορούμε να προβούμε στην ανάλυση του κυρίως θέματος αυτής της εργασίας. Η Κβαντική Επικοινωνία και η Κρυπτογραφία

στηρίζονται στην έννοια του κβαντικού υπολογιστή, που αποτελεί έναν υπολογιστή ο οποίος δεν διαθέτει ως βασική μονάδα εγγραφής και επεξεργασίας της πληροφορίας στο δυαδικό σύστημα λ.χ. μια μαγνητική ψηφίδα μνήμης, αλλά ένα κβαντικό σύστημα. Η διαφορά με έναν κλασικό υπολογιστή είναι ότι ο τελευταίος έχει μόνο δυο επιτρεπτές καταστάσεις, το 0 και το 1. Αντίθετα, σε έναν κβαντικό υπολογιστή υπάρχει η δυνατότητα να βρίσκεται σε οποιαδήποτε επαλληλία αυτών των δύο καταστάσεων. Ειδικότερα για κβαντικούς υπολογιστές, παραπέμπουμε στα [2],[3],[4]

Όπως γνωρίζουμε ήδη, το ελάχιστο κομμάτι μνήμης σε έναν συμβατικό υπολογιστή είναι το bit (binary digit). Στους κβαντικούς υπολογιστές- όπως αναφέραμε ήδη- η θέση μνήμης αποκτά κβαντικό χαρακτήρα, γίνεται δηλαδή ένα κβαντικό σύστημα δύο σωμάτων. Αν συμβολίσουμε με $|0\rangle, |1\rangle$ τις δυο βασικές καταστάσεις, τότε οποιαδήποτε υλοποιήσιμη κατάσταση σε αυτό το σύστημα αποτελεί έναν συνδυασμό αυτών των δυο βασικών, δηλαδή θα είναι της μορφής:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ (2.1)$$

όπου τα $|\alpha|^2, |\beta|^2$ αντιπροσωπεύουν τις πιθανότητες η συγκεκριμένη θέση μνήμης να βρίσκεται στις καταστάσεις $|0\rangle$ και$|1\rangle$ αντίστοιχα. Έτσι, στους κβαντικούς υπολογιστές, όταν αναφερόμαστε για την μονάδα πληροφορίας, θα την ονομάζουμε qubit (κατ' αντιστοιχία με την κλασική περίπτωση).

Φυσικά (αντίστοιχα με τον συνήθη υπολογιστή) ένας κβαντικός υπολογιστής δεν διαθέτει μνήμη αποτελούμενη από ένα μόνο qubit. αλλά από πολλά τοποθετημένα σε κοντινή απόσταση μεταξύ τους, με τρόπο ώστε να είναι δυνατός ο ανεξάρτητος έλεγχός τους με κατάλληλα εξωτερικά πεδία. Αν υποθέσουμε, για απλότητα, ότι ο κβαντικός υπολογιστής μας έχει δύο qubits, τότε οι δυνατές καταστάσεις του συστήματος θα είναι οι :

$$|00\rangle = |0\rangle|0\rangle, |10\rangle = |1\rangle|0\rangle, |01\rangle = |0\rangle|1\rangle \text{ και } |11\rangle = |1\rangle|1\rangle$$

Έτσι, η γενική κατάσταση της μνήμης – ή του καταχωρητή (register)- θα περιγράφεται ως:

$$|\psi\rangle = c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle + c_{11}|11\rangle \ (2.2)$$

όπου τα τετράγωνα των μέτρων c_{ab} εκφράζουν τις πιθανότητες να βρεθούμε στις αντίστοιχες καταστάσεις.

Αν, γενικά, ο κβαντικός υπολογιστής διαθέτει N θέσεις μνήμης, το τυχόν στοιχείο της υπολογιστικής βάσης – κατά αναλογία με την περίπτωση των 2 qubits- θα είναι της μορφής:

$$|x\rangle = |x_1 \dots x_N\rangle = |x_1\rangle \dots |x_N\rangle$$

όπου τα $x_1, \dots, x_N$ είναι οι δυαδικές μεταβλητές για την κάθε θέση μνήμης- το κάθε qubit. Έτσι, η γενική κβαντική κατάσταση της μνήμης θα γράφεται:

$$|\psi\rangle = \sum_x c_x|x\rangle = \sum_{x_1,\dots,x_N} c_{x_{1,\dots,x_N}}|x_1, \dots, x_N\rangle \quad (2.3)$$

με $\sum_x |c_x|^2 = 1$. Σε αυτό το σημείο φαίνεται και μια ουσιαστική διαφορά με τους κλασικούς υπολογιστές. Το πλήθος των βασικών διανυσμάτων σε έναν κβαντικό υπολογιστή με N qubits είναι $D = 2^N$. Ακόμη και αν έχουμε ένα σχετικά μικρό πλήθος από qubits –λ.χ. N=200- το οποίο να είναι ασήμαντο για έναν συνηθισμένο υπολογιστή, το πλήθος αυτών των βασικών διανυσμάτων είναι τεράστιο. Στο παράδειγμά μας για N=200 ισχύει ότι $D = 2^{200} \simeq 10^{87}$, που είναι αριθμός μεγαλύτερος από τον αριθμό των υλικών σωματιδίων όλου του ορατού σύμπαντος. Φαίνεται, λοιπόν, ότι ακόμη και με αυτό το μικρό σχετικά πλήθος από qubits, ένας κβαντικός υπολογιστής μπορεί να επιφορτιστεί την επεξεργασία πληροφορίας αντίστοιχης των 2^{200} Bits, κάτι το οποίο μοιάζει ανέφικτο για τους κλασικούς υπολογιστές. Αυτή η τεράστια ανωτερότητα σε υπολογιστική δύναμη οφείλεται στο ότι όταν ένας κβαντικός υπολογιστής εκτελεί κάποιους υπολογισμούς, τους εκτελεί «παράλληλα» και για τις δύο τιμές της δυαδικής μεταβλητής του κάθε qubit, εφόσον έχουμε επαλληλία των καταστάσεων $|0\rangle, |1\rangle$ σε κάθε qubit. Εφόσον κατά τη διάρκεια αυτών των υπολογισμών δεν γίνεται καμία μέτρηση (για να καταρρεύσει η αρχική κυματοσυνάρτηση και να περιοριστούμε σε ακριβώς μια απ' τις δυο βασικές καταστάσεις σε κάποιο qubit), οι δυο αυτές βασικές καταστάσεις θα εξακολουθούν να υφίστανται συγχρόνως σε όλα τα qubit.

Αυτό, όμως, έχει και ένα μειονέκτημα: ακριβώς αυτή η ταυτόχρονη συνύπαρξη όλων αυτών των διαφορετικών βασικών καταστάσεων δεν μας δίνει μονοσήμαντα μια απάντηση, εφόσον όλες αυτές οι βασικές καταστάσεις υπάρχουν συγχρόνως και άρα αποτελούν όλες πιθανές εξόδους του υπολογιστή. Αυτό το πρόβλημα, όμως, μπορεί να παρακαμφθεί σε αρκετές περιπτώσεις. Πολλές φορές το μόνο που μας ενδιαφέρει είναι να πάρουμε ένα output της μορφής ΝΑΙ-ΟΧΙ. Μπορούμε, λοιπόν, σε αυτή την περίπτωση να καταχωρήσουμε το αποτέλεσμα στο πρώτο qubit της μνήμης. Αν το αποτέλεσμα είναι ΝΑΙ το qubit θα επιστρέφει- ως μέρος της αλγοριθμικής διαδικασίας- την κατάσταση $|0\rangle$ ενώ για την κατάσταση ΟΧΙ θα επιστρέφει την κατάσταση $|1\rangle$. Το μόνο, λοιπόν, που χρειάζεται είναι να μετρήσουμε το συγκεκριμένο qubit και αυτό θα μας δώσει την επιθυμητή απάντηση.

Αν, τώρα, δεν είμαστε βέβαιοι για το αποτέλεσμα που μετρήσαμε, μπορούμε να επαναλάβουμε το πρόγραμμα όσο χρειαστεί και να επαναλάβουμε τη μέτρηση ώστε να περιορίσουμε το ενδεχόμενο σφάλματος σε ένα ανεκτό επίπεδο.

Αναφέρουμε, επίσης, τις λεγόμενες καταστάσεις Bell οι οποίες ορίζονται:

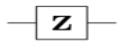
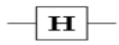
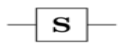
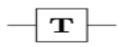
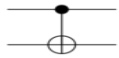
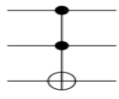
$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,, |B_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), |B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |B_{11}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (2.4)$$

Για καταστάσεις δύο qubits οι καταστάσεις Bell συνθέτουν μια βάση. Εύκολα επαληθεύεται, επίσης, ότι οι καταστάσεις Bell είναι ορθογώνιες μεταξύ τους και κανονικοποιημένες, δημιουργώντας έτσι μια ορθοκανονική βάση στον χώρο των καταστάσεων του συστήματος αυτών των δύο qubits.

2.2. Κβαντικές πύλες

Η λειτουργία ενός κβαντικού υπολογιστή στηρίζεται στην πραγματοποίηση κατάλληλων χειρισμών πάνω στα qubits που συγκροτούν τη μνήμη του ή τον καταχωρητή του όπως λέγεται. Επειδή, όμως, τα qubits είναι κβαντικά αντικείμενα θα πρέπει η επεξεργασία τους να γίνεται σύμφωνα με τις προβλεπόμενες από την κβαντική θεωρία διεργασίες: την μοναδιαία εξέλιξη μέσω της εξίσωσης του Schrödinger που προκαλείται κυρίως με την δράση κατάλληλων ηλεκτρομαγνητικών παλμών και την διαδικασία μέτρησης, που διέπετε από την αρχή της κατάρρευσης του διανύσματος κατάστασης. Επειδή, όμως, εκτός από ειδικές περιπτώσεις, η μέτρηση εκτελείται στο τέλος της υπολογιστικής διαδικασίας, οι δυνατοί χειρισμοί επί των qubits θα πρέπει να είναι υποχρεωτικά μοναδιαίοι . Οι πράξεις αυτές είναι οι κβαντικές πύλες (κατ'αναλογίαν με τις λογικές πύλες των κλασικών υπολογιστών). Είναι σημαντικό να επισημάνουμε εξ αρχής ένα βασικό γεγονός επί του οποίου στηρίζεται όλο το κυκλωματικό μοντέλο των υπολογιστών (είτε κλασικών ή κβαντικών): αρκεί ένας μικρός αριθμός στοιχειωδών πυλών για να υλοποιηθεί μέσω αυτών –έστω κατά προσέγγιση- οποιοσδήποτε μοναδιαίος μετασχηματισμός επί του συνόλου των qubits του καταχωρητή. Ειδικότερα, αρκεί ένας μικρός αριθμός πυλών που δρουν μόνο πάνω σε ένα qubit σε συνδυασμό με μία μόνο πύλη που δρα σε δύο qubit.

Κάθε μονοδυφιακή πύλη δρα επί της τυχαίας κατάστασης η οποία είναι της μορφής $\alpha|0\rangle + \beta|1\rangle$, για αυτό και μπορεί να αναπαρασταθεί με την μορφή πίνακα – ο οποίος μάλιστα θα είναι μοναδιαίος. Ακολούθως παρουσιάζονται κάποιες βασικές κβαντικές πύλες:

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

ΒΑΣΙΚΕΣ ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ ΚΑΙ ΟΙ ΑΝΤΙΣΤΟΙΧΟΙ ΠΙΝΑΚΕΣ (ΠΗΓΗ: WIKIPEDIA)

και εκτός αυτών έχουμε και την μονάδα, η οποία συμβολίζεται με I στο κύκλωμα και της αντιστοιχεί ο ταυτοτικός πίνακας. Όσον αφορά την δράση αυτών των πυλών πάνω σε ένα qubit, έχουμε τα εξής:

-Για την πύλη Hadamard: Έχουμε ότι

$$H\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}|0\rangle + |1\rangle\\|0\rangle - |1\rangle\end{pmatrix} \equiv \begin{pmatrix}|+\rangle\\|-\rangle\end{pmatrix} \quad (2.5)$$

με τον ρόλο αυτής της πύλης να είναι να δημιουργήσει ισοβαρείς επαλληλίες των βασικών καταστάσεων $|0\rangle, |1\rangle$.

- Για την πύλη X:

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

Η πύλη X, δηλαδή, αναστρέφει την κατάσταση του qubit αλλάζοντας τα 0 και 1. Είναι, δηλαδή, το ανάλογο της κλασικής πύλης NOT. Θα συμβολίζουμε την δράση αυτής της πύλης ως:

$$X|x\rangle = |\bar{x}\rangle$$

όπου x=0 ή 1 και $\bar{x}$= 1 ή 0 στις αντίστοιχες περιπτώσεις το ανεστραμμένο είδωλό της δυαδικής μεταβλητής x. Αντίστοιχα μπορεί κανείς να υπολογίσει και την δράση των πυλών όπως οι Y,Z,S.

Έπειτα αναφερόμαστε σε κβαντικές πύλες που δρουν σε δύο qubits. Η βασική τέτοια πύλη είναι η Controlled not ή CNOT όπως θα την συμβολίσουμε στην συνέχεια. Η δράση της περιγράφεται ως εξής:

$$CNOT|0\rangle|y\rangle = |0\rangle|y\rangle \; και \; CNOT|1\rangle|y\rangle = |1\rangle|\bar{y}\rangle$$

Η δράση της πύλης CNOT κάνει το εξής: αν το πρώτο qubit βρίσκεται στην κατάσταση $|0\rangle$ τότε η πύλη CNOT δεν μεταβάλλει το δεύτερο qubit, ενώ αν το πρώτο είναι στην κατάσταση $|1\rangle$ τότε η πύλη CNOT αναστρέφει το δεύτερο. Το πρώτο qubit, λοιπόν, παίζει τον ρόλο του qubit ελέγχου (control qubit), ενώ το δεύτερο είναι το qubit-στόχος (target qubit) και σε αυτόν τον τρόπο δράσης οφείλεται η ονομασία της πύλης. Η δράση της πύλης CNOT πάνω στην τυχούσα κατάσταση $|x, y\rangle$ να γραφτεί :

$$CNOT|x, y\rangle = |x, y \oplus x\rangle \; (2.6)$$

όπου το σύμβολο $\oplus$ είναι η πρόσθεση modulo 2, δηλαδή η συνήθης πρόσθεση δύο ακεραίων με «αφαίρεση» των πολλαπλασίων του δύο από το άθροισμα. Έτσι, το αποτέλεσμα θα είναι πάντα 0 ή 1 και άρα πρόκειται για το κατάλληλο είδος πρόσθεσης για ένα δυαδικό σύστημα που μόνο τα ψηφία 0 και 1 είναι δεκτά.

Μια θεμελιώδης νέα δυνατότητα που μας παρέχει η πύλη CNOT είναι η σύμπλεξη καταστάσεων που ήταν ασύμπλεκτες πριν την δράση της. Αν θεωρήσουμε, για παράδειγμα, την κατάσταση:

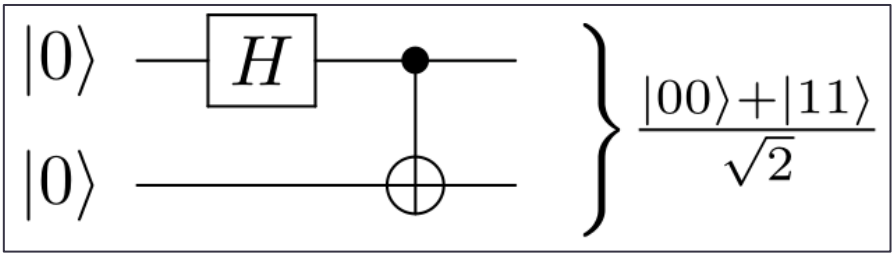
$$|\psi_{in}\rangle = (\alpha|0\rangle + \beta|1\rangle)|1\rangle$$

τότε η δράση της πύλης CNOT επί αυτής της κατάστασης θα είναι:

$$CNOT|\psi_{in}\rangle = \alpha|0\rangle|1\rangle + \beta|1\rangle|0\rangle$$

Παρατηρούμε, δηλαδή, ότι ενώ η αρχική κατάσταση ήταν ασύμπλεκτη, η τελική κατάσταση –κατόπιν δράσης της CNOT- είναι συμπλέκτη κατάσταση αφού δεν μπορεί να γραφεί ως γινόμενο καταστάσεων των δύο βασικών qubit αλλά μόνο ως γραμμικός συνδυασμός τέτοιων γινομένων. Ειδικότερα, αν θέσουμε $\alpha = \beta = \frac{1}{\sqrt{2}}$ η μετασχηματισμένη κατάσταση που παίρνουμε δρώντας μέσω της CNOT δεν είναι παρά η κατάσταση Bell $|B_{01}\rangle$. Σημειωτέων ότι όλες οι καταστάσεις Bell μπορούν να δημιουργηθούν κατά κάποιο ανάλογο τρόπο, μέσω ενός κυκλώματος της ακόλουθης

μορφής (αντίστοιχα τροποποιούμε τις αρχικές καταστάσεις και για τις υπόλοιπες καταστάσεις Bell):



ΔΙΑΤΑΞΗ ΓΙΑ ΤΗΝ ΔΗΜΙΟΥΡΓΙΑ ΚΑΤΑΣΤΑΣΕΩΝ BELL (ΠΗΓΗ: WIKIPEDIA)

Δηλαδή, η διαδικασία που ακολουθούμε είναι η εξής: παίρνουμε το πρώτο qubit και αφήνουμε μια πύλη Hadamard να δράσει πάνω στην κατάσταση στην οποία βρίσκεται αυτό. Στην συνέχεια, χρησιμοποιούμε το αποτέλεσμα αυτής της διεργασίας ως ένα control qubit, με το δεύτερο qubit να παίζει τον ρόλο του target qubit. Εφαρμόζοντας εν τέλει την πύλη CNOT σε αυτά τα δύο τελευταία qubit παίρνουμε μια από τις καταστάσεις Bell.

Γενικότερα, μπορούμε να ορίσουμε την ελεγχόμενη πύλη που αντιστοιχεί σε οποιαδήποτε μονοδυφιακή πύλη από αυτές που ορίσαμε. Αν U είναι μια μονοδυφιακή πύλη, τότε το ελεγχόμενο αντίστοιχό της θα είναι:

$$CU\ (|0\rangle|y\rangle) = |0\rangle|y\rangle\ και\ CU(|1\rangle|y\rangle) = |1\rangle|Uy\rangle$$

Αν, δηλαδή, το πρώτο qubit βρίσκεται στην κατάσταση $|0\rangle$ τότε το target qubit δεν μεταβάλλεται, ενώ αν το control qubit (δηλ. το 1ο) βρίσκεται στην κατάσταση $|1\rangle$ τότε εφαρμόζουμε την κβαντική πύλη U στο target qubit.

Υπάρχει ένα άλλο είδος πύλης η οποία δεν είναι δυνατό να δημιουργηθεί σε έναν κβαντικό υπολογιστή και αυτή είναι η πύλη της αντιγραφής (κατ'αναλογίαν με τους κλασικούς υπολογιστές). Πράγματι, ας υποθέσουμε ότι υπάρχει η δυνατότητα κατασκευής μιας τέτοιας πύλης και έστω ότι U είναι ο μοναδιαίος τελεστής που της αντιστοιχεί. Τότε η δράση αυτού του τελεστή θα είναι η εξής: σε ένα κβαντικό σύστημα, θα παίρνει την κατάσταση $|\psi\rangle|\varphi\rangle$ και θα την στέλνει στην $|\psi\rangle|\psi\rangle$. Τότε, όμως, για δυο γραμμικά ανεξάρτητες καταστάσεις $|\psi_1\rangle, |\psi_2\rangle$ θα είναι:

$$U(c_1|\psi_1\rangle + c_2|\psi_2\rangle)|\phi\rangle = c_1(U|\psi_1\rangle|\phi\rangle) + c_2(U|\psi\rangle|\phi\rangle) = c_1|\psi_1\rangle|\psi_1\rangle + c_2|\psi_2\rangle|\psi_2\rangle$$
$$\neq (c_1|\psi_1\rangle + c_2|\psi_2\rangle)(c_1|\psi_1\rangle + c_2|\psi_2\rangle) (2.8)$$

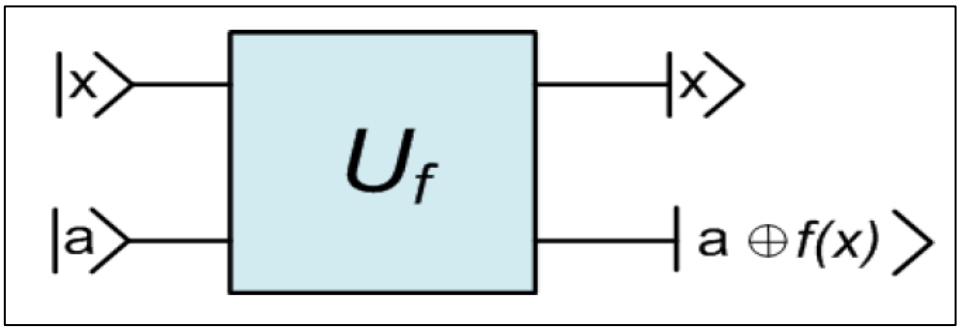
δηλαδή δεν ικανοποιείται η ίδια σχέση που προσδιορίζει την U για μια επαλληλία καταστάσεων. Επομένως δεν μπορεί να υπάρξει πύλη η οποία να αντιγράφει την τυχούσα κβαντική κατάσταση σε ένα σύστημα από qubits ενός κβαντικού υπολογιστή. Ωστόσο, αυτό δεν σημαίνει ότι γενικά η διαδικασία αντιγραφής είναι ανέφικτη. Αν η κατάσταση που θέλουμε να αντιγράψουμε μας είναι γνωστή, τότε κατασκευάζοντας κατάλληλη μετρητική διαδικασία μπορούμε να αντιγράψουμε αυτήν την κατάσταση όπως περιεγράφηκε προηγουμένως. Αυτό είναι σαφές και από

φυσική σκοπιά, αφού αν μπορούσαμε να αντιγράψουμε όσες φορές θέλαμε μια άγνωστη κατάσταση, θα μπορούσαμε ύστερα να εκτελέσουμε μετρήσεις πάνω στα αντίγραφα για να αντλήσουμε πληροφορία για την πρωτότυπη κατάσταση, αφήνοντάς την άθικτη. Αυτό σαφώς και δεν είναι εφικτό λόγω του αξιώματος της Κβαντομηχανικής που αφορά την μέτρηση σε κβαντικά συστήματα.

2.3. Μερικοί αλγόριθμοι για κβαντικούς υπολογιστές

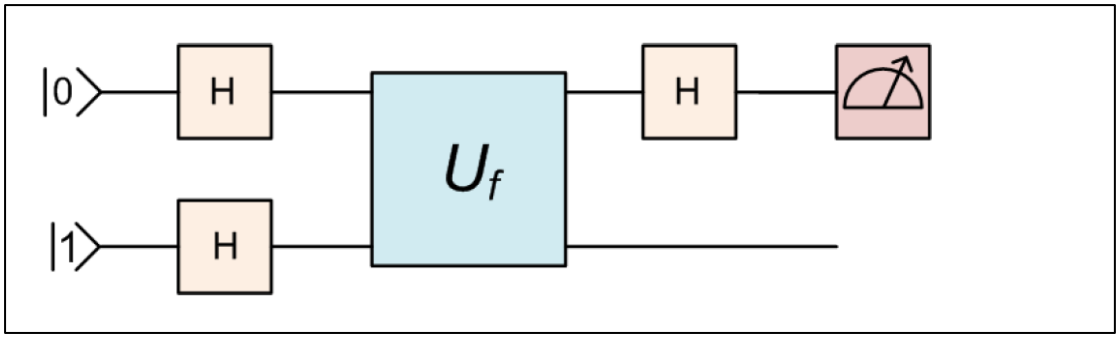
Θα περιγράψουμε στην παρούσα ενότητα κάποιους αλγορίθμους που στηρίζονται στην αρχιτεκτονική του κβαντικού (αποκλειστικά) υπολογιστή. Το απλούστερο παράδειγμα τέτοιου αλγορίθμου είναι ο αλγόριθμος του Deutsch.

Ο εν λόγω αλγόριθμος λύνει το εξής πρόβλημα: Έστω $f:\{0,1\}\to\{0,1\}$. Για κάθε τέτοια συνάρτηση υπάρχουν δύο περιπτώσεις: είτε η f είναι σταθερή και άρα $f(0)=f(1)$ είτε η f δεν είναι σταθερή και τότε $f(0)\neq f(1)$. Ένας κλασικός υπολογιστής θα χρειαζόταν δύο υπολογισμούς για να αποφανθεί για το αν μια τέτοια f είναι σταθερή ή όχι. Το ιδιαίτερο με τον αλγόριθμο του Deutsch είναι ότι μπορεί να μας δώσει απάντηση με έναν μόνο υπολογισμό. Προτού αναπτύξουμε τον αλγόριθμο, παραθέτουμε το ακόλουθο κύκλωμα:



Ο ΤΕΛΕΣΤΗΣ U_f (ΠΗΓΗ: Ι. ΚΑΡΑΦΥΛΛΙΔΗΣ, «ΚΒΑΝΤΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ»)

Το κύκλωμα αυτό περιλαμβάνει έναν καταχωρητή με δύο qubits, με το πρώτο να είναι το $|a\rangle$ και το δεύτερο το $|x\rangle$.Αν $f:\{0,1\}\to\{0,1\}$, με έναν συνδυασμό από κβαντικές πύλες που αναπαρίστανται από τον μοναδιαίο τελεστή U_f δρούμε πάνω στα qubits, αφήνοντας το δεύτερο (το $|x\rangle$) αμετάβλητο και «στέλνοντας» το πρώτο qubit στο $|a\oplus f(x)\rangle$. Κάθε f δίνει και διαφορετικό U_f. Έχοντας αυτό κατά νου, παρουσιάζουμε ακολούθως το κύκλωμα για τον αλγόριθμο του Deutsch:



ΔΙΑΤΑΞΗ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ DEUTSCH (ΠΗΓΗ: Ι.ΚΑΡΑΦΥΛΛΙΔΗΣ, «ΚΒΑΝΤΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ»)

Η περιγραφή του αλγορίθμου είναι η εξής: θεωρούμε δύο qubits με αρχικές καταστάσεις $|1\rangle, |0\rangle$ για το πρώτο και το δεύτερο qubit αντίστοιχα. Η κατάσταση του καταχωρητή, σε αυτήν την περίπτωση, θα είναι $|01\rangle$. Ύστερα, δρουν οι πύλες Η σε κάθε ένα από τα δύο qubits. Μετά εφαρμόζουμε την πύλη U_f που περιγράψαμε παραπάνω. Για το δεύτερο qubit εφαρμόζουμε πάλι μια πύλη Hadamard και μετράμε το συγκεκριμένο qubit. Στο τέλος, αν μετρηθεί η κατάσταση $|0\rangle$, τότε η συνάρτηση f είναι σταθερή, αλλιώς αν μετρηθεί η κατάσταση $|1\rangle$ η f δεν είναι σταθερή.

2.4. Κβαντική Κρυπτογραφία-Κβαντική Επικοινωνία

Ως γνωστόν, η Κρυπτογραφία και στο κλασικό της πλαίσιο αφορά την ασφαλή ανταλλαγή μηνυμάτων ανάμεσα σε δυο ανθρώπους , αλλά και τον τρόπο με τον οποίο μπορεί αυτή η ασφάλεια να παραβιαστεί. Η θεμελιώδης διαφορά που υπεισέρχεται σε ένα κβαντικό σύστημα είναι ότι δεν μπορεί κανείς να «κρυφακούσει» και ακόμη κι αν συνέβαινε κάτι τέτοιο, δεν γίνεται μια τέτοια ενέργεια να περάσει απαρατήρητη. Αυτό γιατί αν χρησιμοποιήσουμε ένα κβαντικό κανάλι επικοινωνίας, αυτό θα βρίσκεται σε μια κατάσταση η οποία θα αποτελεί μια επαλληλία θεμελιωδών καταστάσεων. Αν, λοιπόν, κάποιος προσπαθήσει να παρεισφρήσει μέσα στο κανάλι αυτό, η ενέργεια αυτή αποτελεί ένα είδος μέτρησης, επομένως η αρχική κατάσταση του καναλιού καταρρέει.

Προκύπτει, λοιπόν, στο κβαντομηχανικό πλαίσιο το εξής πρόβλημα: αν δυο άνθρωποι πρόκειται να συμφωνήσουν για ένα ιδιωτικό κλειδί στο κανάλι επικοινωνίας, πώς θα διανεμηθεί αυτό το κλειδί; Η απάντηση δίνεται από το λεγόμενο σύστημα ιδιωτικού κλειδιού (ή όπως αλλιώς λέγεται, κώδικας του Vernam).

Αν οι Α,Β συμφωνούν να έχουν στην κατοχή τους ένα ιδιωτικό κλειδί υπό τη μορφή μιας τυχαίας αλληλουχίας από 0 και 1, τουλάχιστον τόσο μακράς όσο και το μήνυμα που θα ανταλλάξουν, έχοντας συμφωνήσει στο κλειδί η κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος είναι πολύ εύκολη. Αφού γραφεί και το ίδιο το μήνυμα σε δυαδική μορφή , ο αποστολέας (Α) κρυπτογραφεί προσθέτοντάς του ψηφίο προς ψηφίο το συμφωνημένο κλειδί (η πρόσθεση είναι modulo 2) και το

αποστέλλει στον παραλήπτη του (Β). Ο Β, μόλις παραλάβει το μήνυμα, ξαναπροσθέτει το κλειδί και επειδή η διπλή πρόσθεση modulo 2 αυτοαναιρείται, το τελικό μήνυμα θα ταυτίζεται με το αρχικό. Το βασικό πρόβλημα σε αυτή την περίπτωση, όμως, είναι η ασφάλεια του κλειδιού: πώς μπορούν οι Α,Β να συμφωνήσουν και να κοινοποιήσει ο ένας στον άλλο το κλειδί του μηνύματος με τέτοιον τρόπο ώστε κανένας «παρείσακτος» να μην έχει πρόσβαση στο κλειδί;

Με βάση τα όσα είπαμε παραπάνω, βέβαια, προκύπτει και ένα άλλο βασικό ερώτημα: χρειάζεται η χρήση κλειδιού για το μήνυμα; Η απάντηση, βεβαίως, είναι καταφατική. Παρ ’ό,τι κάποιος που μπορεί να κρυφακούσει θα πραγματοποιήσει μέτρηση για το κβαντικό σύστημα του καναλιού επικοινωνίας, υπάρχει το θέμα ότι οι μετρήσεις που θα κάνει μπορεί να είναι οι σωστές αναφορικά με το μήνυμα και άρα δεν θα μείνουν ίχνη αυτής της παραβίασης του καναλιού. Επομένως, βλέπουμε ότι είναι ασφαλέστερο να χρησιμοποιήσουμε κλειδί για την μεταφορά του μηνύματός μας.

Το ζήτημα της μεταφοράς κλειδιού σε ένα κβαντικό κανάλι επικοινωνίας αφορά στην λεγόμενη κβαντική διανομή κλειδιού (Quantum Key Distribution, Q.K.D.). Δυο τρόποι με τους οποίους υλοποιείται αυτή η διαδικασία είναι τα πρωτόκολλα BB84 (Bennet& Brassard, 1984) και EPR, που στηρίζονται στην χρήση κατάλληλων συμπλεκτών καταστάσεων .

Αρχικά, η ιδέα για το BB84 είναι η εξής απλή: αν ο Α στείλει στον Β, μέσω του κβαντικού καναλιού που έχουν στην διάθεσή τους, μια αλυσίδα από 2^N qubits, όπου Ν το μέγιστο μήκος των μηνυμάτων που συνήθως ανταλλάσσουν, ο Α προετοιμάζει τα qubits σε δύο διαφορετικές μετρητικές κατευθύνσεις. Μπορούμε να θεωρήσουμε λ.χ. ότι τα qubits είναι γραμμικά πολωμένα φωτόνια και το κβαντικό κανάλι επικοινωνίας μια οπτική ίνα. Σε αυτό το σύστημα οι καταστάσεις $|0\rangle, |1\rangle$ αντιστοιχίζονται συνήθως με τις δυο ορθογώνιες καταστάσεις γραμμικής πόλωσης $|x\rangle, |y\rangle$. Για την μέτρηση αυτών των qubits μας αρκεί μόνο ένας γραμμικός πολωτής, π.χ. κατά τον άξονα x. Αν το φωτόνιο περνάει από τον πολωτή, σημαίνει ότι βρίσκεται στην κατάσταση $|x\rangle$ και άρα ο καταγραφέας μας σημειώνει 0, ενώ αν δεν περνάει θα βρίσκεται στην κατάσταση $|y\rangle$ και άρα ο καταγραφέας μας θα σημειώνει 1. Αγνοώντας τυχόν ατέλειες του καναλιού και επακόλουθες λανθασμένες αναγνώσεις, το σύστημα είναι αξιόπιστο διότι τα υποστελλόμενα qubits είναι καθαρές ιδιοκαταστάσεις $|x\rangle$ ή $|y\rangle$ και όχι καταστάσεις επαλληλίας . Με βάση τα όσα περιγράφουμε, όμως, ο Α θα πρέπει να αξιοποιήσει και μια δεύτερη κατάσταση π.χ. σε 45 μοίρες από τον άξονα x. Έτσι έχουμε μια δεύτερη κατεύθυνση προετοιμασίας των φωτονίων, οπότε ο Α μπορεί να επιλέγει τυχαία κάποια κατεύθυνση πόλωσης για κάθε φωτόνιο και να τα στέλνει στον Β. Έτσι, αν το φωτόνιο βρίσκεται στην $|x\rangle$ ή $\tau\eta\nu\ |u\rangle$ (τα $|u\rangle, |v\rangle$ αντιστοιχούν στην δεύτερη κατεύθυνση πόλωσης) θα αποδίδουμε την τιμή 0, ενώ για την δεύτερη κατεύθυνση δηλ. αν είναι $|y\rangle$ ή $|v\rangle$ την τιμή 1. Ύστερα, ο Β μετράει τα πολωμένα φωτόνια επιλέγοντας πάλι τυχαία τις κατευθύνσεις μέτρησης για το καθένα και αποδίδει τις τιμές 0 και 1 στις αντίστοιχες

περιπτώσεις. Με αυτήν την διαδικασία που περιγράψαμε, ο Α και ο Β δεν βλέπουν τα σωστά γράμματα μόνο στις θέσεις που χρησιμοποίησαν τον ίδιο μετρητή και οι συμπτώσεις αυτές θα είναι Ν από το συνολικό 2Ν. Το μόνο που απομένει είναι οι Α,Β να χρησιμοποιήσουν ένα κλασικό κανάλι επικοινωνίας, να συγκρίνουν τις κατευθύνσεις των πολωτών τους για καθένα από τα διαδοχικά ψηφία της αλυσίδας μήκους 2Ν που έχουν καταγράψει και να κρατήσουν τελικά μόνο εκείνα τα ψηφία για τα οποία χρησιμοποιήθηκαν ταυτόσημοι πολωτές.

Παρατηρούμε εδώ ότι δεν μας ενδιαφέρει η μυστικότητα της επικοινωνίας στο κλασικό κανάλι, διότι η μόνη πληροφορία που θα μπορούσε κανείς να εξάγει είναι σε πόσα ψηφία συμφωνούν οι Α και Β, αλλά χωρίς να είναι γνωστές οι καταστάσεις αυτών των ψηφίων. Επίσης, αν κάποιος παρεμβληθεί στη γραμμή για να μετρήσει ταυτόχρονα τα φωτόνια που ταξιδεύουν στον Β, δεν θα μπορέσει πάλι να «σπάσει τον κώδικα». Ο λόγος είναι ο εξής: αρχικά ο ξένος στο κανάλι επικοινωνίας δεν έχει την δυνατότητα- όπως επισημάνθηκε νωρίτερα- να αντιγράψει πλήρως το μήνυμα για να κάνει τις απαραίτητες μετρήσεις. Αν παρεμβληθεί στην γραμμή, θα πρέπει να μετρήσει τα φωτόνια συγχρόνως με τον Β και να μετρήσει με τον ίδιο τρόπο τα φωτόνια όπως και ο Β, ενώ ταυτόχρονα φροντίζει τα φωτόνια να συνεχίζουν το ταξίδι τους προς τον Β, αλλιώς ο Β θα διαπιστώσει έλλειμα φωτονίων και θα ακυρώσει την διαδικασία. Ακόμη και έτσι, αν ο παραβάτης του καναλιού επικοινωνίας θα έχει μετρήσει 2Ν φωτόνια και στα Ν/4 εξ αυτών οι μετρήσεις θα έχουν γίνει δεκτές – δηλαδή οι Α,Β θα συμφωνούν για τον άξονα μέτρησης- αλλά τα ψηφία του Β θα είναι διαφορετικά από του Α. Αυτό μπορεί να συμβεί, διότι ενώ οι Α,Β έχουν επιλέξει τον ίδιο άξονα, αν ο παραβάτης έχει χρησιμοποιήσει άλλον άξονα, το φωτόνιο που θα φτάσει στον Β θα βρίσκεται σε κατάσταση επαλληλίας και άρα υπάρχει 50% πιθανότητα να βρεθεί σε κατάσταση διαφορετική απ' ό,τι προετοίμασε ο Α και άρα να δώσει λάθος ψηφίο στον Β. Αν, λοιπόν, οι Α,Β διαπιστώσουν ότι τα κλειδιά τους είναι διαφορετικά στο 25% των ψηφίων τους, μπορούν να επιλέξουν ένα τυχαίο δείγμα μήκους m – ο καθένας από τη δική του αλυσίδα- και να συγκρίνουν λ.χ. μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου τα ψηφία τους. Αν το ποσοστό εκείνων που διαφέρουν είναι περίπου m/4 τότε έχει υπάρξει παρεμβολή και η διαδικασία εναλαμβάνεται μέχρις ότου να είναι σαφές ότι δεν έχει υπάρξει παραβίαση του καναλιού επικοινωνίας.

Από την άλλη, με το πρωτόκολλο EPR μπορούμε να δείξουμε ότι η χρήση συμπλεκτών φωτονίων απλοποιεί το προηγούμενο πρωτόκολλο καθιστώντας παράλληλα ασφαλέστερη την διαδικασία διανομής του κλειδιού. Το νέο πρωτόκολλο δουλεύει ως εξής: ύστερα λ.χ. από ένα τηλεφώνημα του Α ένα τρίτο πρόσωπο σε ένα ενδιάμεσο σημείο της γραμμής επικοινωνίας, ο Ε, παράγει ζεύγη συμπλεκτών φωτονίων στην κατάσταση:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle|x\rangle + |y\rangle|y\rangle) (2.9)$$

και τα αφήνει να ταξιδέψουν προς τις δύο αντίθετες κατευθύνσεις της γραμμής όπου βρίσκονται οι Α και Β. Αν λ.χ. ο Α μετράει νωρίτερα αυτά τα φωτόνια μέσω του πολωτή κατά τον άξονα x , ο καταγραφέας του θα σημειώνει 0 αν το φωτόνιο περάσει και 1 αν δεν περάσει. Έτσι, όμως, λόγω της συμπλοκής των φωτονίων, ο Β θα λαμβάνει φωτόνια που κάθε φορά δεσμεύονται στην ίδια κατάσταση πόλωσης με τα αντίστοιχα που λαμβάνει ο Α και έτσι καταγράφει την ίδια αλυσίδα ψηφίων όπως και ο Α. Έτσι έχει ολοκληρωθεί η διανομή του κλειδιού.

Αναφορικά με την ασφάλεια του κλειδιού, ακόμη και εκείνος που δημιουργεί τα σύμπλεκα φωτόνια – δηλαδή ο Ε- δεν μπορεί να γνωρίζει τίποτα για τα επιμέρους φωτόνια, αφού καθένα από αυτά –λόγω του παραπάνω τύπου για την κατάσταση $|\psi\rangle -$ βρίσκεται ταυτόχρονα και στην κατάσταση $|x\rangle$ και στην $|y\rangle$. Αν επιχειρήσει να το μάθει, μετρώντας την πόλωση του ενός ή του άλλου, θα καταστραφεί η σύμπλεξή τους και αυτό μπορεί να ελεγχθεί εύκολα. Χρειάζεται απλώς οι Α,Β να πάρουν ένα τυχαίο δείγμα από m ζεύγη και να μετρήσουν τις πολώσεις τους σε μια κοινή κατεύθυνση που την αλλάζουν τυχαία από ζεύγος σε ζεύγος. Αν η σύμπλεξη δεν έχει καταστραφεί τότε οι μετρήσεις τους θα είναι απόλυτα συσχετισμένες. Αν, όμως, η σύμπλεξη έχει καταστραφεί, τότε η συσχέτιση θα είναι πρακτικά μηδενική. Θα περιορίζεται στις ελάχιστες περιπτώσεις που η κοινή κατεύθυνση του πολωτή τους ήταν η ίδια με την κατεύθυνση μέτρησης που επέλεξε ο Ε. Έτσι, οι Α,Β θα πρέπει να φροντίσουν ώστε να τους αποσταλούν N+m αντί για N σύμπλεκα ζεύγη, ώστε να μπορούν να πραγματοποιήσουν τον έλεγχο σύμπλεξης και να αγνοήσουν μετά εκείνα που χρησιμοποιήθηκαν για αυτόν τον σκοπό.

Κεφάλαιο 3ο : Πρώτα βήματα στην Κβαντική Τεχνολογία

3.1. Εισαγωγή

Επισημάναμε ήδη ότι η κβαντική υπολογιστική παρέχει πολλές νέες δυνατότητες, με του κβαντικούς υπολογιστές να έχουν σαφώς ανώτερη υπολογιστική δύναμη από τους κλασικούς, ενώ παράλληλα η ανταλλαγή πληροφοριών σε ένα κβαντικό κανάλι επικοινωνίας είναι πιο ασφαλής από την αντίστοιχη κλασική περίπτωση. Παρ ’όλα αυτά υπάρχει λόγος που αυτά τα οφέλη δεν έχουν γίνει ακόμη ευρέως αντιληπτά, και αυτός είναι ότι παρότι είναι σαφές το θεωρητικό πλαίσιο των κβαντικών υπολογιστών –μέχρι ενός βαθμού- είναι σημαντικά δύσκολη η υλοποίησή της και η δημιουργία qubits, καταχωρητών κλπ. Η δυσκολία έγκειται στο ότι για να λειτουργήσει ένας κβαντικός υπολογιστής θα πρέπει να μπορεί να διατηρηθεί η συμφωνία φάσης στις καταστάσεις επαλληλίας των qubits τουλάχιστον για όσο διαρκεί ο υπολογισμός. Ωστόσο, ο καταχωρητής δεν λειτουργεί στο κενό. Είναι ένα μικροσκοπικό κβαντικό σύστημα που αλληλοεπιδρά με ένα πολύ μεγαλύτερο περιβάλλον, συμπλέκεται μαζί του και ως αποτέλεσμα αυτής της σύμπλεξης υφίσταται απώλεια συμφωνίας η οποία καταστρέφει τις επαλληλίες και μαζί μ ’αυτές όλα τα αναμενόμενα πλεονεκτήματα έναντι του κβαντικού υπολογιστή. Το φαινόμενο αυτό της «αποσυμφώνησης» (decoherence) λόγω σύμπλεξης (entanglement) με το περιβάλλον είναι το αδύναμο σημείο του κβαντικού υπολογιστή και αυτό θα πρέπει να υπερνικήσουμε για να επιτύχουμε τον επιθυμητό στόχο μας.

3.2. Ιοντικοί κλωβοί

Επιθυμούμε, λοιπόν, να βρούμε τρόπους να απομονώσουμε το σύστημα του κβαντικού υπολογιστή από το περιβάλλον του, ούτως ώστε να αποφευχθεί το decoherence. Μια προσέγγιση στην λύση αυτού του προβλήματος είναι η μέθοδος του ιοντικού κλωβού (ion trap method), η οποία προτάθηκε για πρώτη φορά από τους

I.Cirac και P. Zoller [6] για την δημιουργία μιας κβαντικής πύλης C-NOT. Η ιδέα είναι η ακόλουθη: εφόσον θέλουμε να απομονώσουμε το σύστημα των qubits από το περιβάλλον του, το τοποθετούμε σε έναν θάλαμο κενού. Αν, όμως, τα qubits είναι ουδέτερα άτομα, δεν θα μπορούν να παραμένουν αιωρούμενα – και μάλιστα σε σταθερές θέσεις- μέσα στον κενό χώρο. Για αυτό, λοιπόν, είναι πιο ωφέλιμο να αξιοποιήσουμε ιόντα αντί ουδέτερων ατόμων και μάλιστα να χρησιμοποιήσουμε κατάλληλα ηλεκτρικά ή/και μαγνητικά για τη «στήριξή» τους σε συγκεκριμένες ευσταθείς θέσεις. Ο ιοντικός κλωβός, λοιπόν, αποτελεί μια ΗΜ διάταξη που παγιδεύει ιόντα σε ελεγχόμενες θέσεις στον κενό χώρο. Μια τέτοια διάταξη – η οποία αρχικά είχε άλλη χρησιμότητα- είναι γνωστή ως (γραμμικός) κλωβός του Paul, που μάλιστα απέφερε το βραβείο Nobel στον δημιουργό της. Αυτή η διάταξη εγκλωβίζει ιόντα πάντα σε μια γραμμή, αποτρέποντας την κίνησή τους σε κάθε εγκάρσια κατεύθυνση. Επειδή, όμως, τα ιόντα απωθούνται και η κίνησή τους πάνω στην ευθεία εγκλωβισμού είναι ελεύθερη, θα πρέπει να τροποποιήσουμε την διάταξη περαιτέρω για να είναι σταθερή. Αυτό επιτυγχάνεται με την τοποθέτηση δυο θετικά φορτισμένων πλακών κάθετων στον άξονα του κλωβού. Έτσι, η απώθηση από τις πλάκες και η μεταξύ άπωση των ιόντων θα έχουν ως αποτέλεσμα την διαμόρφωση μιας σταθερής διάταξης.

Ως προς τον φυσικό φορέα των qubits, αυτός θα είναι τα ίδια τα ιόντα. Ένα δημοφιλές τέτοιο ιόν είναι το βηρύλλιο (Be^+) αλλά επίσης το ασβέστιο (Ca^+), το μαγνήσιο(Mg^+) και το στρόντιο(Sr^+), καθώς και άλλα άτομα κατά προτίμηση από την ομάδα των αλκαλικών γαιών. Μεταξύ άλλων, λόγω του ότι διαθέτουν μια κατάλληλη συστάδα σταθμών πάνω από τη θεμελιώδη που μπορούν να διεγερθούν εύκολα με διαθέσιμες δέσμες λέιζερ, ενώ στη συστάδα αυτών των σταθμών περιλαμβάνεται και μία με μεγάλο χρόνο ζωής (της τάξεως του sec) που είναι ιδιαίτερα πρόσφορη ως κατάσταση $|1\rangle$ του qubit, δίπλα στην θεμελιώδη κατάσταση του ιόντος που είναι η αυτονόητη επιλογή για την κατάσταση $|0\rangle$. Όσο για τις υπόλοιπες στάθμες της συστάδας, δεν εμπλέκονται άμεσα στην λειτουργία του υπολογιστή, αλλά είναι σημαντική η συμβολή τους σε άλλες διεργασίες, όπως η ψύξη των ιόντων σε χαμηλές θερμοκρασίες – της τάξης $10^{-6}K$ - που απαιτούνται προκειμένου να γίνει δυνατή αυτή η λειτουργία.

Δεν μας φτάνουν, όμως, αυτά για να λειτουργήσει μια συλλογή από qubits ως κβαντικός υπολογιστής, αλλά χρειάζεται να εξετάσουμε την αλληλεπίδρασή τους. Στην περίπτωση της ιοντικής αλυσίδας, το αποτέλεσμα της αλληλεπίδρασης των ιόντων της είναι οι συλλογικές τους ταλαντώσεις καθορισμένης συχνότητας, δηλαδή αυτό που ονομάζουμε κανονικούς τρόπους ταλάντωσης. Αυτές είναι στην ουσία τους πανομοιότυπες με τις ταλαντώσεις μια αλυσίδας μαζών συνδεδεμένων με ελατήρια ή μιας αντίστοιχης αλυσίδας συζευγμένων εκκρεμών. Ο πρώτος τέτοιος τρόπος ταλάντωσης – αυτός με την χαμηλότερη συχνότητα- αντιστοιχεί στην ομοιόμορφη κίνηση δεξιά και αριστερά όλων των μαζών του συστήματος, χωρίς συμπίεση ή

τέντωμα των συνδετικών «ελατηρίων». Στην περίπτωση της ιοντικής αλυσίδας, αυτός ο τρόπος συλλογικής ταλάντωσης – γνωστός και ως κοινός τρόπος (common mode)- λαμβάνει χώρα γύρω από το ελάχιστο του δυναμικού που δημιουργούν στο κέντρο της σχετικής διάταξης οι ομόσημα φορτισμένες πλάκες στα άκρα της.
Εφόσον τα ιόντα της αλυσίδας αποτελούν μικροσκοπικά αντικείμενα, οι ταλαντώσεις τους θα είναι κβαντωμένες με χαρακτηριστικό κβάντο ενέργειας $\hbar\omega$ όπου ω η συχνότητα του συγκεκριμένου τρόπου ταλάντωσης. Για πολύ μακρές αλυσίδες- ή και για στερεά σώματα- οι ταλαντώσεις αυτές δεν είναι παρά ηχητικά κύματα, οπότε τα σχετικά κβάντα διαθέτουν και ορμή εκτός από ενέργεια και θα είναι, επομένως, τα ηχητικά ανάλογα των φωτονίων. Θα είναι, δηλαδή, σωμάτια-φορείς του ηχητικού πεδίου και για αυτό τα αποκαλούμε και φωτόνια.

Σύμφωνα με τα προηγούμενα, η πλήρης περιγραφή της ιοντικής αλυσίδας θα επιτυγχάνεται μέσω διανυσμάτων της μορφής:

$$|\Psi\rangle = |\mathrm{x}_1 \dots x_n\rangle|\bar{n}\rangle \ (3.1)$$

όπου οι $x_i, i = 1, \dots, N$ οι δυαδικές μεταβλητές που προσδιορίζουν την εσωτερική κβαντική κατάσταση του κάθε ιόντος, ενώ το ket $|\bar{n}\rangle$ περιγράφει την κατάσταση της συλλογικής τους κίνησης με τον ακέραιο αριθμό $\bar{n}$ που δηλώνει το πλήθος των κβάντων (ή φωτονίων) του βασικού τρόπου ταλάντωσης που είναι παρόντα στη συγκεκριμένη κατάσταση. Παρ ‘ότι θεωρητικά η συλλογική κίνηση του συστήματος μπορεί να διαθέτει όλες τις καταστάσεις $|\bar{0}\rangle, |\bar{1}\rangle, |\bar{2}\rangle, \dots, |\bar{n}\rangle$ θα εστιάσουμε το ενδιαφέρον μας στις δυο πρώτες. Η κατάσταση $|\bar{0}\rangle$ αντιστοιχεί στην κίνηση μηδενικού σημείου της αλυσίδας και η δεύτερη $|\bar{1}\rangle$ στην παρουσία ενός φωνονίου.
Ειδικότερα , αν N=2 τότε η κατάσταση ελάχιστης ενέργειας της αλυσίδας θα είναι η:

$$|00\rangle|\bar{0}\rangle = |0\rangle|0\rangle|\bar{0}\rangle \ (3.2)$$

και αυτήν θα θεωρήσουμε ως αφετηρία των κβαντομηχανικών χειρισμών που θα περιγράψουμε ακολούθως. Το κύριο ζήτημα είναι να δούμε πώς πραγματοποιούνται φυσικά οι διάφορες κβαντικές πύλες που αποτελούν τα θεμελιώδη δομικά στοιχεία του υπολογιστή. Για τις μονοδυφιακές πύλες το ζήτημα είναι απλό. Οποιαδήποτε εξ αυτών μπορεί να υλοποιηθεί με τη δράση πάνω στο κάθε συγκεκριμένο ιόν μιας πολύ εστιασμένης δέσμης λέιζερ κατάλληλης διάρκειας και με τη συχνότητα ω_0 που αντιστοιχεί στην ηλεκτρονιακή μετάβαση $|0\rangle \rightarrow |1\rangle$.

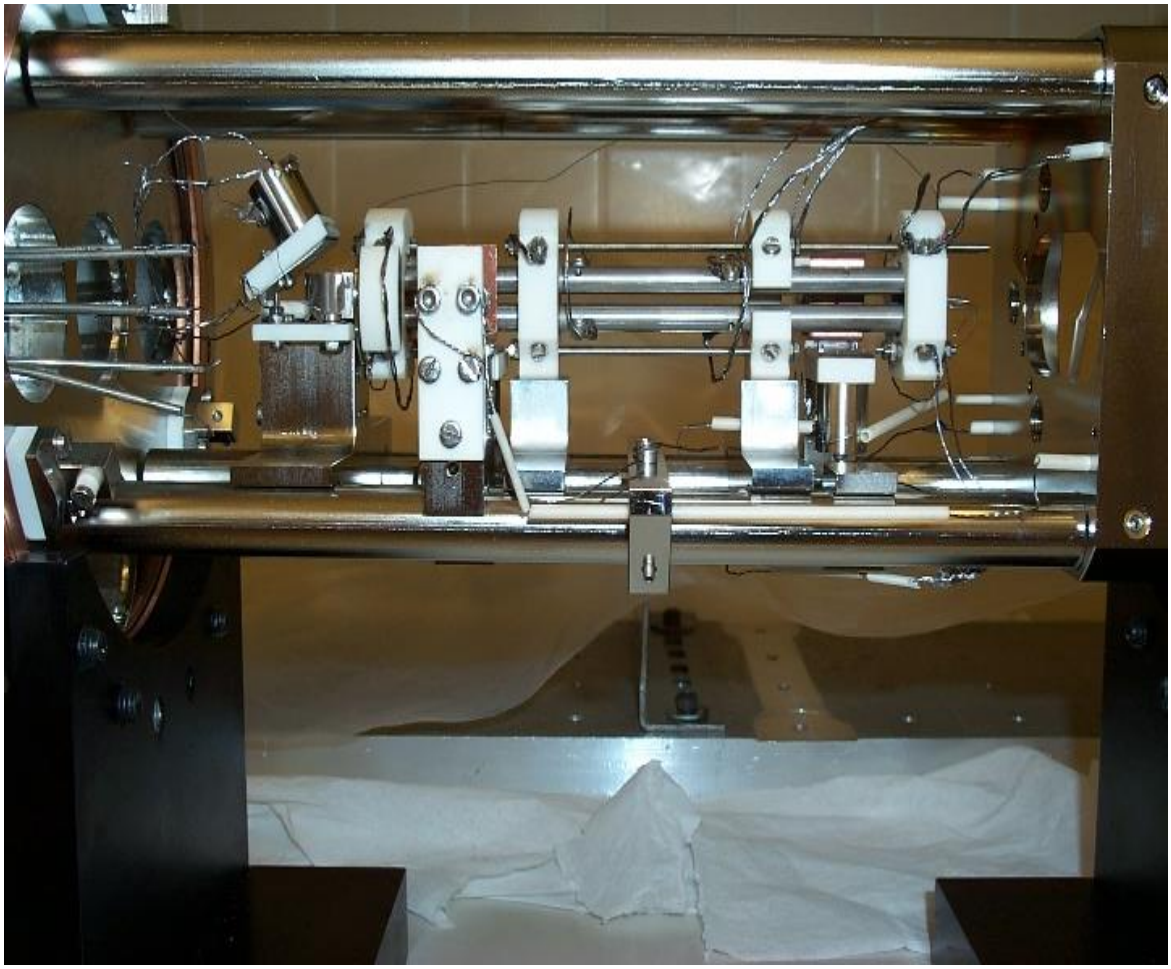
Σημειωτέον ότι η διεγερμένη στάθμη που αντιστοιχεί στην κατάσταση $|1\rangle$ είναι αρκετά μακρόβια (της τάξης του δευτερολέπτου) και ως εκ τούτου έχει μικρό φασματικό εύρος. Έτσι, η δράση του λέιζερ κοντά στον συντονισμό υπόκειται στις λεγόμενες ταλαντώσεις Rabi. Μια «συντονισμένη» δέσμη λέιζερ πάνω σε κάθε ιόν μπορεί να το φέρει σε οποιαδήποτε κατάσταση της μορφής $c_0(t)\ |0\rangle + c_1(t)\ |1\rangle$ και

πρέπει ύστερα να υπολογίσουμε εμείς τον χρόνο δράσης ώστε η επαλληλία αυτή να είναι η επιθυμητή. Οπότε, έχουμε αρχικά τους παλμούς π που φέρνουν το ιόν στην κατάσταση $|1\rangle$ αν ξεκινούσε στην κατάσταση $|0\rangle$ ή στην $|0\rangle$ αν ήταν αρχικά στην $|1\rangle$. Επίσης, έχουμε τους παλμούς π/2 που φέρνουν το εκάστοτε ιόν σε ισοβαρή επαλληλία, δηλαδή σε επαλληλία της μορφής:

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

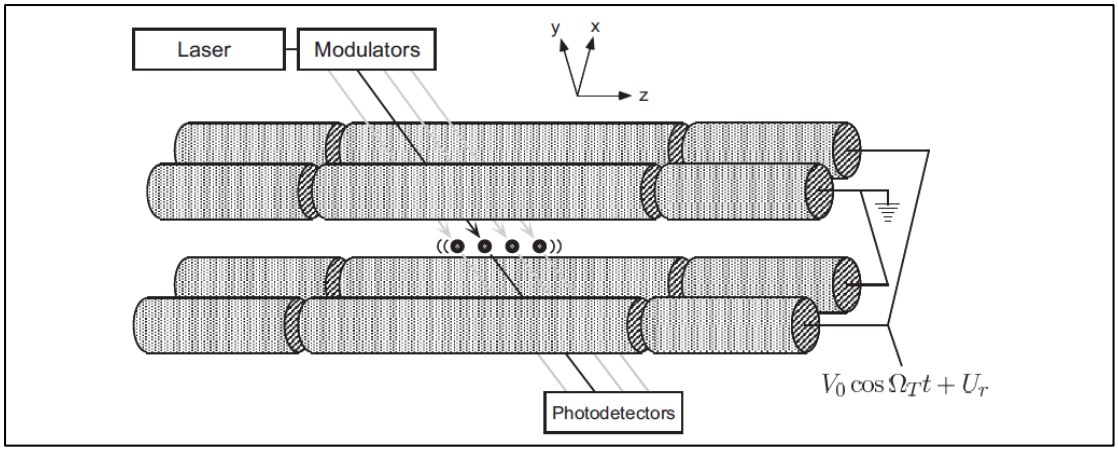
αν η αρχική του κατάσταση ήταν $|0\rangle$ ή $|1\rangle$. Οι παλμοί τύπου π αντιστοιχούν, φυσικά, στην πύλη X και οι παλμοί π/2 στην κβαντική πύλη Hadamard. Όλα τα παραπάνω εξαρτώνται από την διεύθυνση πόλωσης της δέσμης σε συνδυασμό με τους κβαντικού αριθμούς της κατάσταση $|1\rangle$. Ακόμη και έτσι, όμως, με τρόπο όμοιο με πριν μπορούμε να κατασκευάσουμε αντίστοιχα οποιαδήποτε απλή (μονοδυφιακή πύλη). Με έναν ελαφρώς πιο σύνθετο τρόπο υλοποιείται σε αυτό το πλαίσιο και η πύλη CNOT.

3.3. Ο κλωβός Paul



ΕΙΚΟΝΑ 3.: ΓΡΑΜΜΙΚΟΣ ΙΟΝΤΙΚΟΣ ΚΛΩΒΟΣ (ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΟΥ ΚΑΛΓΚΑΡΙ, ΠΗΓΗ: WIKIPEDIA)

Θα επεκταθούμε, τώρα, στο πώς επιτυγχάνεται ο μηχανισμός παγίδευσης των ιόντων που περιγράψαμε προηγουμένως. Σε έναν γραμμικό κλωβό Paul βρίσκονται τέσσερα παράλληλα ηλεκτρόδια (στις κορυφές ενός τετραγώνου, σε εγκάρσια τομή), τα οποία τροφοδοτούνται από δύο πόλους μιας πηγής ραδιοσυχνοτήτων ($f \simeq$ $λίγα\ MHz$) και όλη η διάταξη βρίσκεται σε υψηλό κενό ($\simeq 10^{-8} Pa$). Ο άξονας εγκλωβισμού είναι ο άξονας συμμετρίας του κλωβού και τα ιόντα που παγιδεύονται εκεί ελέγχονται από μια δέσμη λέιζερ μέσω κατάλληλου παραθύρου. Παράλληλα, η ανάγνωσή τους γίνεται με μια κατάλληλη δέσμη και έναν σχετικό ανιχνευτή. Σε αυτήν την διάταξη, λοιπόν, λόγω της ραγδαίας εναλλαγής στις πολικότητες των δύο ζευγών ηλεκτροδίων, οι αλλεπάλληλες «απόπειρες» διαφυγής ενός ιόντος προς το ένα ή το άλλο από τα εκάστοτε ελκτικά γι' αυτό ηλεκτρόδια «ματαιώνονται» διαρκώς. Αυτό έχει ως αποτέλεσμα, πρακτικά, την ενεργό παγίδευσή του στο κέντρο της διάταξης.



ΕΙΚΟΝΑ 3.2:ΔΙΑΤΑΞΗ ΓΡΑΜΜΙΚΟΥ ΚΛΩΒΟΥ: 4 ΙΟΝΤΑ ΠΑΓΙΔΕΥΜΕΝΑ ΑΝΑΜΕΣΑ ΣΕ ΔΥΟ ΖΕΥΓΗ ΚΥΛΙΝΔΡΙΚΩΝ ΗΛΕΚΤΡΟΔΙΩΝ (ΠΗΓΗ:M.A. NIELSEN, I.L. CHUANG, "QUANTUM COMPUTATION AND QUANTUM INFORMATION")

Από μαθηματικής σκοπιάς, η μελέτη του προβλήματος ανάγεται στην αναζήτηση ευσταθών λύσεων της εξίσωσης:

$$x''(t) + (k_0 + k_1 \cos(\omega t))x(t) = 0 \ (E\xi. Matthews) (3.3)$$

Η τελευταία εξίσωση μπορεί να ιδωθεί και ως το χρονικό ανάλογο της μονοδιάστατης εξίσωσης Schrödinger:

$$\psi''(x) + (\varepsilon - U_0 \cos(kx))\psi(x) = 0 \ (3.4)$$

μέσα στο περιοδικό δυναμικό $U(x) = U_0 \cos(kx)$. *Για δεδομένο U(x), η ύπαρξη ευσταθών λύσεων αυτής της διαφορικής εξίσωσης είναι δυνατή μόνο για ορισμένες ζώνες τιμών του ε που είναι οι γνωστές ενεργειακές ζώνες των ηλεκτρονίων μέσα σε ένα κρυσταλλικό στερεό, δηλαδή σε ένα περιοδικό δυναμικό. Πλήρως ανάλογα, για δεδομένο «δυναμικό»* $k_1 \cos(\omega t)$ στην εξ. Matthews –δηλαδή για δεδομένο πλάτος και συχνότητα της πηγής ραδιοσυχνοτήτων- θα υπάρχουν ευσταθείς λύσεις (δηλαδή λύσεις που παγιδεύουν το ιόν) μόνο όταν η παράμετρος k_0 (η ένταση της πρόσθετης πηγής συνεχούς τάσης) πέφτει σε ορισμένες ζώνες τιμών. Έτσι, βλέπουμε ότι η κατασκευή ενός γραμμικού ιοντικού κλωβού είναι περίπλοκο ζήτημα, διότι προϋποτίθεται η εκλογή των σχετικών παραμέτρων μέσα σε κατάλληλα διαστήματα τιμών και η προσθήκη μιας συνιστώσας συνεχούς τάσης σε ένα από τα δύο ζεύγη ηλεκτροδίων υπαγορεύεται από την ανάγκη μεγαλύτερης ευχέρειας στην επιλογή αυτών των τιμών.

Παρ 'ότι ο κλωβός Paul αποτελεί ένα χρήσιμο εργαλείο, δεν είναι τέλειο, μιας και κατά τη λειτουργία του αναπτύσσονται παράσιτα ηλεκτρικά πεδία, αφενός λόγω του λεγόμενου θορύβου Johnson (που οφείλεται στην τυχαία θερμική κίνηση των ηλεκτρονίων μέσα στους αγωγούς) και αφετέρου λόγω μικροανωμαλιών στις επιφάνειες των ηλεκτροδίων. Αυτό έχει ως αποτέλεσμα την ανεπιθύμητη θέρμανση των ιόντων.

Εντούτοις, η λειτουργία ενός κβαντικού υπολογιστή ιοντικού κλωβού δεν φαίνεται να απειλείται λόγω αυτού του φαινομένου. Αρκετά πειράματα έχουν δείξει ότι το ενδεχόμενο της εσωτερικής υπερθέρμανσης είναι ελέγξιμο ή τουλάχιστον δεν επέρχεται τόσο γρήγορα ώστε να διακυβεύεται ένας υπολογισμός σε εξέλιξη.

3.4. Πυρηνικός Μαγνητικός Συντονισμός

Τα συστήματα πυρηνικών σπιν του είδους που συζητήσαμε στην προηγούμενη παράγραφο θα μπορούσαν να είναι ιδανικά για την κβαντική υπολογιστική αν οι συζεύξεις σπιν με σπιν ήταν μεγάλες και ελέγξιμες. Το βασικό ελάττωμα ενός κβαντικού υπολογιστή ιοντικού κλωβού είναι η αδυναμία της εκ φωτονίου μετριασμένης σύζευξης σπιν με σπιν και η επιρρέπεια αυτής της τεχνικής σε decoherence. Ένας τρόπος περιορισμού του προβλήματος θα μπορούσε να είναι η παγίδευση μορίων αντί ατόμων – η αλληλεπίδραση Fermi μέσω μαγνητικών δίπολων και ηλεκτρονίων μεταξύ γειτονικών πυρήνων θα παρείχαν ισχυρές φυσιολογικές συζεύξεις. Ωστόσο, λόγω των πολλών τρόπων ταλάντωσής τους, τα μόρια δεν μπορούν να παγιδευτούν και να ψυχθούν εύκολα. Έτσι, η οπτική «χειραγώγηση» και ανίχνευση πυρηνικών σπιν σε παγιδευμένα μόρια δεν έχει επιτευχθεί παρά μόνο σε εξαιρετικές περιπτώσεις.

Από την άλλη, η απευθείας χειραγώγηση και ανίχνευση των πυρηνικών καταστάσεων σπιν με χρήση ηλεκτρομαγνητικών κυμάτων ραδιοσυχνοτήτων είναι ένα αρκετά ανεπτυγμένο πεδίο που λέγεται «Πυρηνικός μαγνητικός συντονισμός» (Nuclear Magnetic Resonance). Οι τεχνικές αυτές χρησιμοποιούνται ευρέως στην χημεία, για παράδειγμα, για την μέτρηση ιδιοτήτων υγρών, στερεών και αερίων, για τον προσδιορισμό της δομής των μορίων και την απεικόνιση υλικών και ακόμη σε βιολογικά συστήματα. Αυτές οι εφαρμογές οδήγησαν στην σημαντική εξέλιξη της NMR τεχνολογίας, επιτρέποντας τον έλεγχο και την παρατήρηση από δεκάδες έως και εκατοντάδες, ακόμη και χιλιάδες πυρήνων σε ένα πείραμα.

Παρ ‘όλα αυτά, ανακύπτουν δύο σημαντικά ζητήματα στην χρήση NMR για κβαντική υπολογιστική. Αρχικά, λόγω του ότι η πυρηνική μαγνητική ροπή είναι πολύ μικρή, απαιτείται μεγάλο πλήθος μορίων ($\approx 10^8$) για την παραγωγή μετρήσιμου σήματος επαγωγής. Ένα μόριο μόνο του μπορεί να είναι καλός κβαντικός υπολογιστής, αλλά πώς μπορεί να ισχύει το ίδιο για ένα σύνολο από μόρια; Ειδικότερα, η έξοδος μιας NMR μέτρησης είναι ένας μέσος πάνω από τα σήματα των μορίων. Μπορεί να έχει νόημα αυτός ο μέσος από κβαντικούς υπολογιστές; Δεύτερον, οι τεχνικές NMR εφαρμόζονται κατά κύριο λόγο σε φυσικά συστήματα που βρίσκονται σε θερμοκρασία δωματίου, όπου η ενέργεια σπιν $\hbar\omega$ είναι πολύ μικρότερη του $k_B T$. Έτσι, η αρχική κατάσταση των σπιν είναι σχεδόν παντελώς τυχαία. Η παραδοσιακή κβαντική υπολογιστική απαιτεί το σύστημα να ετοιμάζεται

σε καθαρή κατάσταση. Πώς μπορεί, λοιπόν, ο υπολογισμός να εκτελείται σε ένα σύστημα το οποίο βρίσκεται σε μεικτή κατάσταση υψηλής εντροπίας;

Λύσεις σε αυτά τα δύο προβλήματα έχουν καταστήσει την NMR προσέγγιση αρκετά ελκυστική μέθοδο για την εφαρμογή κβαντικών υπολογισμών, παρά τους περιορισμούς που ανακύπτουν λόγω της θερμικής φύσης των τυπικών συστημάτων. Όπως και να 'χει, αυτή η προσέγγιση έχει χρησιμεύσει στην αντιμετώπιση διαφόρων σχετικών προβλημάτων γενικότερα: για παράδειγμα, τεχνικές ελέγχου ρεαλιστικών Χαμιλτονιανών για την εκτέλεση αυθαίρετων μοναδιαίων μετασχηματισμών, μεθόδους χαρακτηρισμού και παράκαμψης του decoherence (και συστηματικών σφαλμάτων) και θεωρήσεις που προκύπτουν με την συνάθροιση συνιστωσών για την υλοποίηση πλήρων κβαντικών αλγορίθμων σε πλήρη συστήματα.

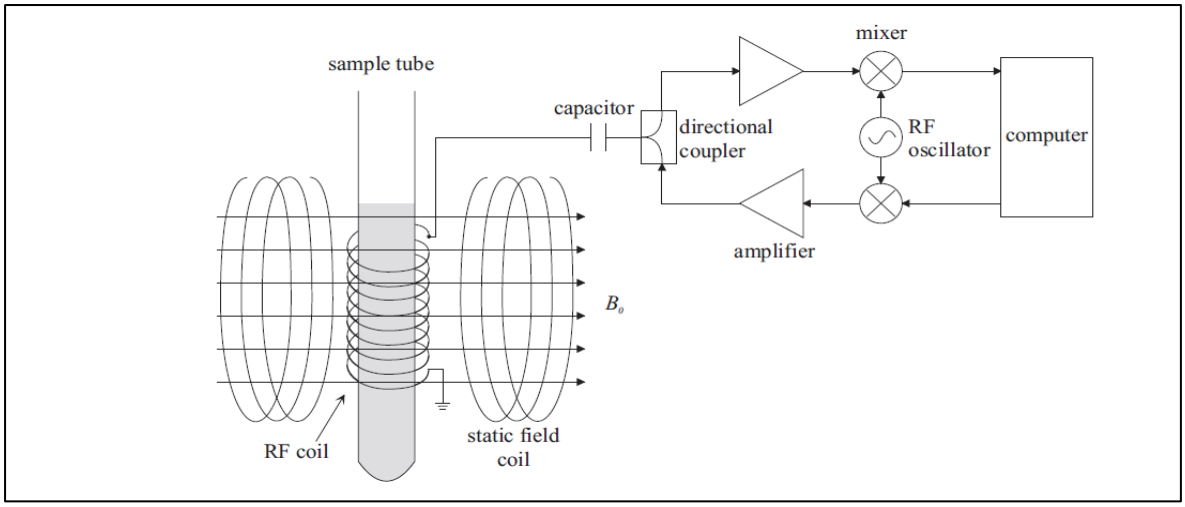
Μια διάταξη που να απορρέει από αυτήν την τεχνολογία είναι η εξής: τα δύο βασικά μέρη ενός παλλόμενου NMR συστήματος για υγρά δείγματα (σε αυτά θα εστιάσουμε) είναι το δείγμα και το φασματοσκόπιο NMR. Ένα τυπικό μόριο που μπορεί να χρησιμοποιηθεί θα περιέχει n το πλήθος πρωτόνια με σπιν ½ (άλλοι πιθανοί πυρήνες είναι ^{13}C, ^{19}F, ^{15}N, ^{31}P) και παράγει σήμα NMR συχνότητας γύρω στα 500MHz όταν τοποθετείται σε ένα μαγνητικό πεδίο περίπου 11.7 Tesla. Οι συχνότητες των διαφορετικών πυρήνων εντός του μορίου μπορεί να διαφέρουν από μερικά kHz μέχρι μερικές εκατοντάδες kHz λόγω των διαφορών στα τοπικά μαγνητικά πεδία. Τα μόρια διαλύονται μέσα σε ένα διαλύτη, μειώνοντας την συγκέντρωση στον βαθμό που οι ενδομοριακές αλληλεπιδράσεις θεωρούνται αμελητέες, αφήνοντας ένα σύστημα που μπορεί να περιγράφει ως ένα σύνολο από n qubit κβαντικών «υπολογιστών».

Το φασματοσκόπιο κατασκευάζεται από ηλεκτρονικά ραδιοσυχνοτήτων και έναν μεγάλο υπεραγώγιμο μαγνήτη, μέσα στην οπή του οποίου τοποθετούμε σε γυάλινο σωλήνα το δείγμα. Εκεί, το στατικό μαγνητικό πεδίο B_0 κατά τη διεύθυνση $\hat{z}$ τροποποιείται κατάλληλα ώστε να είναι ομοιόμορφο πάνω από περίπου $1cm^3$. Η ύπαρξη ορθογωνίων σελών ή πηνίων Helmholtz στο εγκάρσιο επίπεδο επιτρέπουν την ανάπτυξη μικρών, ταλαντευόμενων μαγνητικών πεδίων κατά τις $\hat{x}$ και $\hat{y}$ διευθύνσεις. Τα πεδία αυτά ενεργοποιούνται και απενεργοποιούνται με ραγδαίους ρυθμούς για την διαμόρφωση των πυρηνικών καταστάσεων σπιν. Τα ίδια πηνία αποτελούν, επίσης, μέρος κυκλωμάτων που χρησιμοποιούνται για την ανίχνευση σημάτων ραδιοσυχνοτήτων που παράγονται από τους προπορευόμενους πυρήνες (όπως ένας περιστρεφόμενος μαγνήτης επάγει εναλλασσόμενο ρεύμα σε ένα κοντινό του πηνίο).

Ένα τυπικό πείραμα ξεκινά με μια μακρά περίοδο αναμονής στην οποία οι πυρήνες δύνανται να θερμανθούν μέχρι την ισορροπία. Αυτό μπορεί να απαιτεί αρκετά λεπτά για καλά προετοιμασμένα υγρά δείγματα. Υπό έλεγχο ενός (κλασικού) υπολογιστή, παλμοί ραδιοκυμάτων εφαρμόζονται για να επιτύχουν τον επιθυμητό μετασχηματισμό στην κατάσταση των πυρήνων. Οι ενισχυτές παλμών υψηλής ισχύος ύστερα απενεργοποιούνται ακαριαία και ένας ευαίσθητος προ-ενισχυτής

ενεργοποιείται, για να μετρήσει την τελική κατάσταση των σπιν. Η έξοδος, που καλείται αποσύνθεση ελεύθερης επαγωγής(free induction decay), μετασχηματίζεται κατά Fourier για την απόκτηση ενός φάσματος συχνοτήτων με κορυφές των οποίων οι περιοχές είναι συναρτήσεις των καταστάσεων σπιν.

Υπάρχουν αρκετά σημαντικά πρακτικά ζητήματα τα οποία οδηγούν σε εμφανείς ατέλειες. Επί παραδείγματι, χωρικές ανομοιογένειες στο στατικό μαγνητικό πεδίο οδηγούν τους πυρήνες σε διαφορετικά σημεία των πεδίων να προπορεύονται σε διαφορετικές συχνότητες. Αυτό διευρύνει γραμμές στο φάσμα. Μια ακόμη μεγαλύτερη πρόκληση αποτελεί η ομοιογένεια του πεδίου ραδιοσυχνοτήτων, το οποίο δημιουργείται από ένα πηνίο που πρέπει να είναι κάθετο στον B_0 μαγνήτη. Αυτός ο γεωμετρικός περιορισμός και η απαίτηση του να διατηρείται συγχρόνως ψηλή B_0 ομοιογένεια συνήθως αναγκάζει το πεδίο ραδιοσυχνοτήτων να είναι ανομοιογενές και να παράγεται από ένα μικρό πηνίο, οδηγώντας έτσι σε ατελή έλεγχο του πυρηνικού συστήματος. Επίσης, ο συγχρονισμός των παλμών και η ευστάθεια ισχύος, φάσης και συχνότητας είναι σημαντικά ζητήματα. Ωστόσο, σε αντίθεση με τους ιοντικούς κλωβούς, λόγω χαμηλών συχνοτήτων, είναι πιο εύκολα εφικτός ο έλεγχος αυτών των παραμέτρων.



ΕΙΚΟΝΑ 3.3: ΔΙΑΤΑΞΗ ΕΝΟΣ " NMR ΚΒΑΝΤΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ" (ΠΗΓΗ:M.A. NIELSEN, I.L. CHUANG, "QUANTUM COMPUTATION AND QUANTUM INFORMATION")

Με βάση την διάταξη που περιγράψαμε παραπάνω, έχουν πραγματοποιηθεί πειράματα στα οποία έχει επιτευχθεί τοπογραφία επίδειξης καταστάσεων (χρησιμεύει στην απασφαλμάτωση (debugging)), η υλοποίηση στοιχειωδών κβαντικών πυλών και η υλοποίηση ενός κβαντικού αλγορίθμου αναζήτησης. Είναι ενδιαφέρον το ότι αυτή η τεχνοτροπία για την υλοποίηση κβαντικού υπολογιστή έχει υπάρξει επιτυχής στην υλοποίηση κβαντικών αλγορίθμων και διεργασιών κβαντικής πληροφορίας σε συστήματα έως και 7 qubits.

Ωστόσο, υπάρχουν σημαντικοί περιορισμοί που προκύπτουν από τις χρονικές, χωρικές και λογικές τεχνικές τιτλοφόρησης (labeling) που βρίσκονται στην καρδιά αυτής της μεθόδου. Επίσης, μια θεμελιώδης αδυναμία της μεθόδου έγκειται στην

χρήση μορίων ως κβαντικούς υπολογιστές. Η δομή των μορίων παίζει τον ρόλο της αρχιτεκτονικής του υπολογιστή, καθορίζοντας ποια ζεύγη- ή ποιες ομάδες- από qubits αλληλοεπιδρούν μεταξύ τους (κατ' αντιστοιχία, οι παλμοί ραδιοσυχνοτήτων λειτουργούν ως το λογισμικό). Δεν είναι, βέβαια, απαραίτητο όλα τα qubits να είναι καλά συνδεδεμένα. Αυτό είναι διπλά σημαντικό, μιας και οι αλληλεπιδράσεις δεν μπορούν να απενεργοποιηθούν, εκτός αν επαναληφθεί η εστίαση. Επιπρόσθετα, η πρόσβασή μας στα qubits επιτυγχάνεται βάσει των συχνοτήτων τους, αλλά αυτό γίνεται ολοένα και πιο δύσκολο καθώς το πλήθος των πυρήνων αυξάνεται. Υπάρχει λύση για αυτό, που είναι η χρήση αρχιτεκτονικής cellular automata style, όπως στην μονοδιάστατη αλυσίδα X-A-B-C-A-B-C-...-A-B-C-Y στην οποία τα άκρα της αλυσίδας είναι καθορισμένα, ενώ το μέσο της συντίθεται από μια επαναλαμβανόμενη κανονική ακολουθία. Σε αυτήν την αρχιτεκτονική, μόνο διακεκριμένα γράμματα μπορούν να είναι διευθυνσιοδοτούμενα και φαίνεται, ενδεχομένως, ότι είναι ένα αρκετά περιοριστικό υπολογιστικό μοντέλο. Ωστόσο, έχει δειχθεί ότι στην πραγματικότητα είναι καθολικό, με μονάχα πολυωνυμική επιβράδυνσης (slowdown). Η ακριβής ποσότητα της επιβράδυνσης που απαιτείται θα είναι, φυσικά, σημαντική στην εκτέλεση διεργασιών όπως ένας κβαντικός αλγόριθμος αναζήτησης, που έχει μόνο επιτάχυνση (speedup) της τάξης της τετραγωνικής ρίζας.

Κλείνοντας αυτή την συζήτηση του μοντέλου NMR κβαντικής υπολογιστικής, θα λέγαμε ότι ενώ πρόκειται για ένα κάθε άλλο παρά ιδανικό μοντέλο στην πράξη και ενώ διαθέτει τα προαναφερθέντα μειονεκτήματα, μπορεί να αξιοποιηθεί για την δοκιμή αλγορίθμων και την επίδειξη βασικών τεχνικών που άλλες υλοποιήσεις θα πρέπει να εφαρμόσουν για την πραγματοποίηση ενός κβαντικού υπολογισμού. (Λεπτομερέστερη ανάλυση των παραπάνω αλλά και άλλων πιθανών υλοποίησεων κβαντικών υπολογιστών μπορεί να βρεθεί στο 7^{ο} κεφάλαιο του [7]).

Κεφάλαιο 4ο : Η Κβαντική Επικοινωνία σήμερα

Ύστερα από την επισκόπησή μας πάνω στις πρώτες προσπάθειες ανάπτυξης κβαντικής τεχνολογίας, μεταξύ άλλων και στο κομμάτι της επικοινωνίας, προχωράμε στην αναφορά σε πιο πρόσφατες εξελίξεις.

4.1. Το μέλλον της Κβαντικής Επικοινωνίας

Πρόσφατα εισήχθη στην αγορά η τεχνολογία του 5G προσφέροντας ήδη πολλές νέες προοπτικές. Γίνεται έρευνα, παράλληλα, για την ανάπτυξη του 6G, η οποία θα έχει τελειοποιηθεί πιθανώς περί το 2030. Παρ 'όλα αυτά, το 5G έχει εμφανίσει προβλήματα σε ό,τι αφορά την κίνηση (traffic) των δικτύων, τα οποία αναμένεται να οξυνθούν πολύ περισσότερο στο 6G. Το φάσμα των συχνοτήτων θα πρέπει να επεκταθεί για να συμπεριλαμβάνει της τάξης των 30-300Ghz αλλά επιπέδου TerraHertz (0.3-10 THz) ούτως ώστε να επιτυγχάνονται ταχύτητες TerraBits-ανά δευτερόλεπτο. Για αυτό θα αποκτήσει μεγαλύτερη σημασία για αυτά τα μελλοντικά ζητήματα η συμπερίληψη οπτικών υποδομών σε συστήματα THz, για την αξιοποίηση των απεριόριστων δυνατοτήτων των πρώτων. Ακόμη περισσότερο, φαίνεται να επωφελείται η τεχνολογία και από τις εξελίξεις στην κβαντική οπτική.

Η Κβαντική Οπτική (Q.O.) είναι κλάδος της Φυσικής που αναπτύσσεται απ' την δεκαετία του 70. Το πλεονέκτημα του να καταφύγουμε στην κβαντική οπτική από ότι σε κλασικές τεχνοτροπίες είναι ότι μπορούμε να μεταφέρουμε και να χειριστούμε οπτικά σήματα με εξαιρετικά πολλούς βαθμούς ελευθερίας. Η επιρροή της κβαντικής οπτικής δεν σταματάει, βέβαια, εκεί στις σύγχρονες τεχνολογίες, αλλά συνεισφέρει επίσης και σε ζητήματα παρατηρήσεων με πολλαπλά τηλεσκόπια, ενώ αξιοποιείται με τέτοιο τρόπο ώστε να εξασφαλίζουμε ότι ένα σύστημα που μας ενδιαφέρει είναι πράγματι κβαντικό.

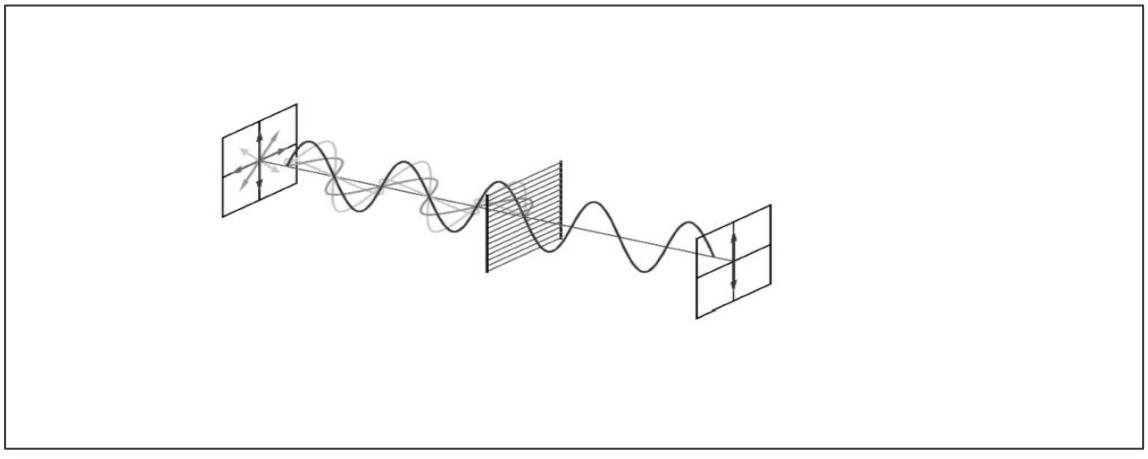
Με αφορμή αυτήν την τεχνοτροπία, ενδιαφερόμαστε να μελετήσουμε το κατά πόσον είναι εφικτή η κβαντική οπτική επικοινωνία (Quantum Optical Communications/ Q.O.C.) (Πηγή για το συγκεκριμένο εδάφιο: [8])

4.2. Ειδικότερα για την Κβαντική Οπτική:

Η Κβαντική Οπτική απασχολείται με την μελέτη φαινομένων που αφορούν στην αλληλεπίδραση κβάντων ενός ηλεκτρομαγνητικού πεδίου (λ.χ. τα φωτόνια μιας δέσμης φωτός) με την ύλη (δηλαδή με άτομα και μόρια). Στην μελέτη αυτή συμπεριλαμβάνεται η μελέτη «της σωματιδιακής φύσης» των φωτονίων και ως εκ τούτου των αντίστοιχων ιδιοτήτων τους, και η εξέταση μέσω πειράματος κβαντομηχανικών φαινομένων που φαίνεται να αντιβαίνουν με την διαίσθησή μας, όπως η κβαντική σύμπλεξη ή η τηλεμεταφορά.

Η μελέτη της κβαντικής οπτικής αρχικά ήταν εστιασμένη σε απλές μη-κλασικές καταστάσεις του φωτός, όπως μονά φωτόνια, συμπιεσμένες καταστάσεις, δίδυμες οπτικές δέσμες και καταστάσεις τύπου Einstein-Podolsky-Rosen (EPR). Σε ποιο ώριμο στάδιο, η κβαντική οπτική έχει θίξει κβαντικές καταστάσεις με πολλαπλούς κβαντικούς βαθμούς ελευθερίας (δηλαδή είτε χωρικούς ή χρονικούς, συχνότητας κ.ά.). Αυτό δημιουργεί ολοένα και περισσότερες προοπτικές αξιοποίησης της Κβαντικής Οπτικής μελλοντικά στις Τηλεπικοινωνίες. Στην πραγματικότητα, οποιαδήποτε μορφή έχει ένα ηλεκτρομαγνητικό πεδίο μπορεί να θεωρηθεί ως ένας ξεχωριστός κβαντικός βαθμός ελευθερίας και ανάλογα με τον ρυθμό μετάδοσης, ο άξονας της ταλάντωσης σε μια ηλεκτρομαγνητική μετάδοση μπορεί να έχει πολλούς διαφορετικούς προσανατολισμούς από την κατεύθυνση μετάδοσης. Για παράδειγμα, όταν υπάρχει μόνο εγκάρσια συνιστώσα για το ηλεκτρικό πεδίο, αυτό είναι φυσικά εγκάρσιο στην κατεύθυνση διάδοσης ενώ το μαγνητικό πεδίο είναι ορθό σε αυτήν (Αντίστοιχα όταν η διάδοση του μαγνητικού πεδίου είναι εγκάρσια).

Διαφορετικά σύνολα από τέτοιους ρυθμούς μας επιτρέπουν να θεωρήσουμε την ίδια κβαντική κατάσταση από διαφορετικές σκοπιές: μια κατάσταση μπορεί από μια οπτική γωνία να θεωρείται συμπλεγμένη, ενώ σε άλλη ότι είναι παραγοντοποιημένη. Μπορούμε, λοιπόν, με χρήση τεχνικών μη γραμμικής οπτικής, να διαμορφώνουμε κατά το δοκούν τα κβαντικά πεδία όχι μόνο επιλέγοντας τους ρυθμούς που υπεισέρχονται, αλλά βελτιστοποιώντας και την χωροχρονική τους μορφής. Με άλλα λόγια, τα qubits μπορούν να κωδικοποιηθούν στους βαθμούς ελευθερίας ενός φωτονίου λ.χ. της πόλωσής του, δηλαδή της κατεύθυνσης των ταλαντώσεων του ηλεκτρικού πεδίου.



ΕΙΚΟΝΑ 4.1:ΠΑΡΑΔΕΙΓΜΑ ΠΟΛΩΣΗΣ ΦΩΤΟΣ (ΠΗΓΗ: A. MANZALINI, ""QUANTUM COMMUNICATIONS IN FUTURE NETWORKS AND SERVICES)

Επιπλέον, η τροχιακή στροφορμή του φωτός θεωρείται πολλά υποσχόμενος επιπλέον βαθμός ελευθερίας για την πολυπλεξία δεδομένων σε οπτικές ίνες, στην νανοκλίμακα κλπ. Η τροχιακή στροφορμή αυτή αναπαριστά την συνιστώσα της

στροφορμής μιας δέσμης φωτός που είναι ανεξάρτητη από το πεδίο χωρικής κατανομής και όχι της πόλωσης. Έχει δειχθεί ότι η τροχιακή στροφορμή μπορεί να χρησιμοποιηθεί σε χαμηλές ραδιοσυχνότητες και δεν περιορίζεται στην οπτική εύρος συχνοτήτων.

4.3. Κβαντική Οπτική Επικοινωνία (QOC0

Η Κβαντική Οπτική Επικοινωνία, πάλι, εκμεταλλεύεται την ιδέα της χρήσης των φωτονίων ως «ιπτάμενα» qubits, με σκοπό την μεταφορά qubits από έναν φυσικό κβαντικό πομπό σε έναν φυσικό κβαντικό δέκτη. Τα πλεονεκτήματα χρήσης αυτών των αιωρούμενων qubits συμπεριλαμβάνουν την ασθενή αλληλεπίδραση με το περιβάλλον (ελαττώνοντας έτσι τον κίνδυνο για decoherence), έλεγχο με τυπικές οπτικές συνιστώσες και μεταδόσεις υψηλών ταχυτήτων και χαμηλών απωλειών μέσω οπτικών και ράδιο-καναλιών. Παραθέτουμε, στη συνέχεια, ορισμένα παραδείγματα εφαρμογών που προκύπτουν από τα όσα αναφέραμε έως τώρα:

- Με τις αυξανόμενες ανάγκες για bandwidth, τα THz συστήματα επικοινωνιών αναμένεται να αποκτήσουν μεγαλύτερη σημασία. Η ενσωμάτωση των THz συστημάτων μέσω κβαντικών οπτικών δικτύων θα είναι σημαντική στην συμπλήρωση των πλεονεκτημάτων των ραδιοδικτύων με τις απεριόριστες δυνατότητες των συστημάτων οπτικής μετάδοσης. Αυτή η ενσωμάτωση απαιτεί καινοτόμες μεθόδους επεξεργασίας σημάτων, κάτι στο οποίο η κβαντική τεχνολογία μπορεί να βοηθήσει. Έχει δημιουργηθεί διάταξη [7] στην οποία ένας ασύρματος σύνδεσμος επετεύχθη στον οποίο ενσωματώθηκε απρόσκοπτα σε φωτονικό δίκτυο, συμπληρώνοντας την ευθεία οπτική/THz μετατροπή σε ευθεία THz/οπτική μετατροπή στον THz δέκτη. Ο ασύρματος αυτός σύνδεσμος λειτουργεί σε φέρουσα συχνότητα 0.2885 THz με μέγιστη τιμή γραμμής 50Gbits/s και γέφυρες μήκους 16 μέτρων. Το THz σήμα παράγεται από THz/οπτική μετατροπή σε UTC φωτοδίοδο. Στον δέκτη, το THz σήμα μετατρέπεται στο οπτικό φάσμα με χρήση ultra-broadband plasmonic-organic hybrid modulator.

- Οι Κβαντικές Οπτικές Τεχνολογίες μπορούν να βρουν πολλά υποσχόμενες εφαρμογές και στο κομμάτι των δικτύων πρόσβασης σε υποδομές τηλεπικοινωνιών. Σε ένα παράδειγμα τέτοιας αρχιτεκτονικής για ένα κβαντικό δίκτυο πρόσβασης [10] στο οποίο εκτελείται κβαντική διανομή κλειδιού μεταξύ πολλαπλών χρηστών πάνω σε 1x64 παθητικό οπτικό διαχωριστή. Σε downstream configuration, ένας κβαντικός πομπός τοποθετείται στον κόμβο του δικτύου. Το μεταδιδόμενο κβαντικό κλειδί κατευθύνεται τυχαία σε κάποιον απ’ τους κβαντικούς δέκτες μέσω ενός παθητικού οπτικού διαχωριστή δέσμης. Κάθε χρήστης χρειάζεται έναν μόνο ανιχνευτή φωτονίων και το κλειδί διανέμεται τυχαία. Σε upstream configuration χρειάζεται ένας

μόνο ανιχνευτής στον κόμβο του δικτύου. Οι κβαντικοί πομποί μοιράζονται αυτόν τον ανιχνευτή διασφαλίζοντας ότι φτάνουν φωτόνια στον δέκτη μόνο από έναν πομπό τη φορά.

Ένα άλλο ενδιαφέρον παράδειγμα υλοποίησης κβαντικού δικτύου πρόσβασης [11] αποτελεί η ανάπτυξη μιας peer-to-peer υπηρεσίας πολυμέσων μέσω μονάδων οπτικού δικτύου (Optical Network Units). Ειδικότερα, η πρόταση υποστηρίζει ευθεία κβαντική και κλασική επικοινωνία ONU-NU χρησιμοποιώντας N:N διαχωριστή. Η κβαντική διανομή κλειδιού ανάμεσα σε ONU και τερματισμό οπτικής γραμμής (Optical Line Termination) μπορεί να εκτελεστεί κανονικά και δύναται να υποστηρίξει 64 ONUs χάρη στην λογική ανάθεση μηκών κύματος διαφορετικών σημάτων.

- Τα κβαντικά σωματίδια μπορούν να διαδίδονται ταυτόχρονα σε πολλαπλές χωροχρονικές τροχιές. Αυτό προσφέρει την δυνατότητα ανάπτυξης κβαντικών συσκευών που λέγονται κβαντικοί διακόπτες, στους οποίους η χρονική σειρά των καναλιών επικοινωνίας ελέγχεται από έναν κβαντικό βαθμό ελευθερίας που αναπαρίσταται, λ.χ, από ένα qubit ελέγχου. Αρκετές υλοποιήσεις του κβαντικού διακόπτη έχουν δοκιμαστεί πειραματικά, με το qubit ελέγχου να αναπαρίσταται από βαθμούς ελευθερίας της πόλωσης ή της τροχιακής στροφορμής.

- Θεωρείται, γενικά, ότι η βασανιστική υπόσχεση μιας μαζικής διάδοσης κβαντικών υπολογιστικών συστημάτων στην αγορά και αντίστοιχων υπηρεσιών βρίσκεται ακόμη πολύ μακριά για τους εξής λόγους: προβλήματα θορύβου και decoherence, ανάγκη για αξιόπιστες τεχνικές διόρθωσης σφαλμάτων κλπ. Η χρήση κβαντικής οπτικής για την ανάπτυξη κβαντικών υπολογιστικών συστημάτων μας φέρνει ένα βήμα πιο κοντά σε αυτό τον στόχο. Τα κβαντικά υπολογιστικά συστήματα που βασίζονται στην κβαντική οπτική μπορούν να εξελίξουν την τωρινή υπολογιστική τεχνολογία με χρήση φωτονίων ως φορείς πληροφορίας. Υπάρχουν, λ.χ., παραδείγματα [12] συνιστωσών, συμπεριλαμβανομένων διορθώσεων σφαλμάτων σε μοτίβα φωτονίων, οπτικές κβαντικές μνήμες και αλγορίθμους και πρωτόκολλα. Συνεχίζοντας στην ίδια κατεύθυνση, το LASOLV αποτελεί ένα πολύ καλό παράδειγμα υπολογιστή που στηρίζεται σε φωτονικές τεχνολογίες ανεπτυγμένες από την NTT. Ειδικότερα, το LASOLV είναι μια συνεκτική μηχανή Ising (Coherent Ising Machine) , η οποία χρησιμοποιεί ένα μοντέλο Ising βασισμένο σε φωτονικές τεχνολογίες για την επίλυση προβλήματα συνδυαστικής βελτιστοποίησης. Στην πραγματικότητα, υπάρχει μεγάλο κομμάτι δουλειάς που περιγράφει την υλοποίηση Ising υπολογιστικής με παγίδευση ατόμων, μονών φωτονίων, κυκλωμάτων υπεραγωγών, νανομαγνητών κ.α. Άλλο ενδιαφέρον παράδειγμα [13] αποτελεί η πρόταση

και η πειραματική επιβεβαίωση μεθόδου χρήσης της χωρικής διαμόρφωσης του φωτός για τον προσδιορισμό της θεμελιώδους κατάστασης μιας Ising Χαμιλτονιανής. Η μήτρα φάσης σε έναν χωρικό διαμορφωτή φωτός (Spatial Light Modulator) δρα ως ένα πλέγμα από χιλιάδες σπιν, οι αλληλεπιδράσεις των οποίων κυβερνώνται από την δεσμευμένη οπτική ένταση στο μακρινό πεδίο και μπορεί να προγραμματιστεί με διαμόρφωση του πλάτους της εισόδου. Ανάδραση από το πεδίο εντοπισμού επιτρέπει την χωρική κατανομή φάσης να εξελίσσεται προς το ελάχιστο από τα επιλεγμένα μοντέλα σπιν.

Η τεχνητή νοημοσύνη αποτελεί ένα από τα πιο πολλά υποσχόμενα πεδία εφαρμογής της υπολογιστικής με χρήση κβαντικής οπτικής. Είναι γνωστό ότι οι έως τώρα προταθείς λύσεις για A.I. είναι εξαιρετικά κοστοβόρες (από άποψη πόρων) αλλά και χρονοβόρες. Στην πραγματικότητα, τα σύγχρονα Deep Neural Networks, όπως και άλλα A.I. μοντέλα, στηρίζονται σε τρανζίστορ που λειτουργούν βάση της άλγεβρας Boole για την εκτέλεση μεγάλου πλήθους υπολογισμών σε τεράστια σύνολα δεδομένων. Τροχοπέδη αποτελεί το ότι τα τσιπ σετ ηλεκτρονικά δεν εξελίσσονται με τον ίδιο ρυθμό όπως οι λύσεις για λογισμικό για A.I. Είναι ευρέως γνωστό ότι η τρέχουσα τάση κατανάλωσης ενέργειας δεν είναι βιώσιμη μακροπρόθεσμα: χρειάζεται μια καινοτομία εάν πρόκειται να εξελιχθεί η αγορά των εφαρμογών του A.I. Σημειώνεται ότι η βάση της λειτουργίας ενός Deep Neural Network(D.N.N.), κάθε στρώμα υψηλότερου επιπέδου μαθαίνει αυξανόμενα πιο αφηρημένα υψηλού επιπέδου χαρακτηριστικά, δίνοντας μια χρήσιμη αναπαράσταση των χαρακτηριστικών των χαμηλότερων στρωμάτων. Αυτή η ομοιότητα μας υποδεικνύει το ενδεχόμενο οι αρχές των νευρικών δικτύων αυτών να βρίσκονται βαθιά ριζωμένες στην κλασική θεωρία πεδίου και στην κβαντική οπτική. Αυτή η σκοπιά προσφέρει, ενδεχομένως, την επιβεβαίωση ότι ο τρόπος να παρακάμψουμε τα προαναφερθέντα εμπόδια είναι η χρήση υπολογιστικών συστημάτων κβαντικής οπτικής τα οποία είναι σημαντικά πιο γρήγορα και λιγότερο κοστοβόρα ενεργειακά από τα τωρινά. Λαμβάνουμε υπόψη ότι οι πράξεις που κάνει ένα D.N.N. είναι κατά κύριο λόγο πολλαπλασιασμοί πινάκων, καθώς επίσης και το ότι κυκλώματα κβαντικής οπτικής μπορούν να κάνουν πολύ πιο γρήγορα τέτοιες πράξεις σε σχέση με τα κλασικά αντίστοιχα συστήματα επεξεργασίας. Η υπολογιστική κβαντική οπτικής επιτρέπει τον υπολογισμό ενός τέτοιου πολλαπλασιασμού να γίνει σε ένα CPU clock cycle (ανεξαρτήτως μεγέθους των πινάκων), ενώ τα ηλεκτρονικά τσιπς χρειάζονται τουλάχιστον μερικές εκατοντάδες clock cycles για να εκτελέσουν την ίδια πράξη. Ήδη γίνεται έρευνα και ανάπτυξη τέτοιων τεχνολογιών. Παραδείγματος χάριν [14] έχει πραγματοποιηθεί η μελέτη ενός πλήρως-οπτικού περ θλαστικού DNN: το πρωτότυπο απαρτίζεται από μια σειρά από περ θλαστικά στρώματα όπου κάθε σημείο (το ισοδύναμο ενός

νευρώνα) δρα ως μια δευτερεύουσα πηγή ενός ηλεκτρομαγνητικού κύματος κατευθυνόμενου προς το επόμενο στρώμα.

- Άλλο πιθανό πεδίο εφαρμογών, το οποίο είναι πάλι πολλά υποσχόμενο, είναι η χρήση μέτα-υλικών (metamaterials) στον χώρο των τεχνολογιών πληροφορίας και επικοινωνίας και στις τηλεπικοινωνίες π.χ. στην ανάπτυξη έξυπνων ράδιο-περιβαλλόντων (εσωτερικού ή εξωτερικού χώρου).

  Τα metamaterials (MM) είναι υλικά που εμπεριέχουν διάφορα στοιχεία στο εσωτερικό τους (λ.χ. μέταλλα ή διηλεκτρικά υλικά διαφόρων σχημάτων και διαστάσεων) τα οποία είναι σχεδιασμένα και τεχνητά κατασκευασμένα για να διαχειρίζονται και να κατευθύνουν ηλεκτρομαγνητικά κύματα. Παραδείγματα ενσωματωμένων αντικειμένων (inclusions) σε τέτοια υλικά συμπεριλαμβάνουν στοιχεία σκέδασης και νάνο-αντηχεία. Αυτά τα στοιχεία είναι κατάλληλα τοποθετημένα (σε ένα μικρό κλάσμα του μήκους κύματος): όταν ένα ηλεκτρομαγνητικό προσπίπτει σε ένα MM, τα τοπικά πεδία σκεδάζονται από τα εσωτερικά συστατικά του MM και παρεμβάλλονται, προκαλώντας έτσι μια αλλαγή στην αρχική κατανομή του ηλεκτρομαγνητικού πεδίου. Αυτές οι ιδιότητες ήδη χρησιμοποιούνται για την ανάπτυξη λειτουργιών «έξυπνης κεραίας» και επεξεργασίας ηλεκτρομαγνητικών κυμάτων.

  Metasurfaces (MS) είναι δυσδιάστατα MM. Τα MS φτιάχνονται, πάλι, από οποιαδήποτε περιοδικά δυσδιάστατα inclusions το πάχος και η περιοδικότητα των οποίων είναι μικρά σε σχέση με το μήκος του ηλεκτρομαγνητικού μήκους κύματος: λόγω της δυσδιάστατης φύσης τους τα MS καταλαμβάνουν περιορισμένο φυσικό χώρο και επιδεικνύουν χαμηλές απώλειες όπως τα φωτόνια κινούνται σε κάθετη σε επίπεδο κατεύθυνση. Είναι, μάλιστα, εφικτό να αναπτυχθεί MS που να δείχνει δείκτες διάθλασης που δεν υπάρχουν στην φύση (λ.χ. κοντά στο 0 ή αρνητικούς δείκτες διάθλασης).

  Αναμένεται ότι τα MS θα βρουν εφαρμογή σε ποικίλα προβλήματα, όπως η κάλυψη ραδιοσυχνοτήτων σε περιοχές που δεν καλύπτονται καλά μέσω εγκατάστασης βάσεων, ανάπτυξη έξυπνων ραδιοκυματικά περιβάλλοντα, εφαρμογές ολογραφικής ασφάλειας, μαθηματικές πράξεις ή πολλαπλασιασμούς πινάκων με χρήση τεχνητής νοημοσύνης (π.χ. με οπτικό μετασχηματισμό Fourier), εντοπισμός και αναγνώριση εικόνων κλπ.

  Η MS αναλογική υπολογιστική μπορεί να χρησιμοποιηθεί στην εκτέλεση μαθηματικών πράξεων (όπως χωρική παραγώγιση, ολοκλήρωση ή συνέλιξη) απευθείας χρησιμοποιώντας το προφίλ ενός προσπίπτοντος κύματος καθώς διαδίδεται κατά μήκος αυτών των blocks.

- Μια μελλοντική εφαρμογή: Λέμε ότι ένας ψηφιακός δίδυμος (digital twin) είναι η ψηφιακή αναπαράσταση των στοιχείων και των χαρακτηριστικών πραγμάτων, όπως μηχανημάτων, συστημάτων, διαδικασιών παραγωγής ή ακόμη και ανθρώπων. Η πρωτοβουλία Digital Twin Computing (DTC) στοχεύει στην επέκταση της παραπάνω ιδέας του ψηφιακού διδύμου επεκτείνοντας και αναβαθμίζοντας επικοινωνίες και αλληλεπιδράσεις στον κυβερνοχώρο. Για παράδειγμα, η πλατφόρμα DTC απαρτίζεται από τέσσερα στρώματα: (1)το Cyber/φυσικό στρώμα αλληλεπίδρασης που συλλέγει τα πραγματικά δεδομένα που απαιτούνται για την γένεση του ψηφιακού διδύμου και παρέχει ανάδραση (feedback) στον πραγματικό κόσμο μέσω των εφαρμογών. (2)το στρώμα ψηφιακού διδύμου που παράγει και διατηρεί τα ψηφιακά δίδυμα χρησιμοποιώντας δεδομένα που λαμβάνει από το προηγούμενο στρώμα.
  (3) το στρώμα παρουσίασης ψηφιακού κόσμου που παρέχει το πλαίσιο επίκλησης digital twin λειτουργιών που θα αξιοποιούν τους ψηφιακούς διδύμους απ’ το στρώμα (2).
  (4) το στρώμα εφαρμογής για την ανάπτυξη DTC εφαρμογών χρησιμοποιώντας το στρώμα (3).

  Πλήρως ανάλογα, θα μπορούσε να αναπτυχθεί μια αντίστοιχη κβαντική εκδοχή των παραπάνω, ο «κβαντικός οπτικός δίδυμος» (quantum optical twin, Q.O.T), που θα αξιοποιεί τέσσερα αντίστοιχα με τα προηγούμενα στρώματα. Το τελευταίο θα ήταν εφικτό με την αξιοποίηση QOC τεχνολογιών καθιστώντας δυνατή την μεταφορά, αποθήκευση και επεξεργασία ψηφιακής αλλά ακόμη και κβαντικής πληροφορίας.

  Θα μπορούσαμε να ορίσουμε το QOT ως το κβαντικό ομοίωμα μιας ζωντανής ή μη φυσικής οντότητας, που μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς: κβαντικό ομοίωμα σημαίνει απλώς ότι αναπτύσσεται με χρήση τεχνολογιών κβαντικής οπτικής (ακόμη και σε συνδυασμό με κλασικές τεχνολογίες).

  Το QOT ως έννοια διαφέρει σημαντικά απ’ το κλασικό ψηφιακό δίδυμο για τον ίδιο λόγο που η κβαντική πληροφορία διαφέρει ουσιαστικά από την κλασική. Ενώ η θεμελιώδης μονάδα πληροφορίας στην κλασική πληροφορία είναι το bit, στην κβαντική πληροφορία η αντίστοιχη μονάδα είναι το qubit που κωδικοποιείται με φωτόνια. Όπως έχουμε αναφέρει, τα φωτόνια-qubit είναι σωματίδια ελεύθερα από decoherence για τα οποία οι αντίστοιχες λειτουργίες που εκτελούνται γίνονται με ευκολότερο τρόπο από την αξιοποίηση ηλεκτρονιακών qubit σε υπεραγώγιμα chipsets.

  Μια μελλοντική «Έξυπνη πόλη» αποτελεί μια πρόκληση όπου το QOT θα μπορούσε να συνεισφέρει ουσιαστικά, καθώς το ολοένα αυξανόμενο επίπεδο πολυπλοκότητας των σύγχρονων πόλεων θα απαιτεί επίλυση, σε –σχεδόν- πραγματικό χρόνο, προβλημάτων συνδυαστικής και local vs global

βελτιστοποίησης με πολλαπλούς περιορισμούς. Για παράδειγμα, μπορούμε να φανταστούμε κάθε έξυπνο αμάξι εξοπλισμένο με A.I. συστήματα ικανά να λύσουν προβλήματα τοπικής μεταφοράς ανιχνεύοντας διαρκώς το έξυπνο ραδιοκυματικό περιβάλλον (π.χ. αλληλοεπιδρώντας με MS) για να προσδιορίσουν την καλύτερη διαδρομή για να φτάσει κανείς στον προορισμό του ή αν το αυτοκίνητο θα πρέπει να σταματήσει ή να επιταχύνει σε μια διασταύρωση. Τέτοιες τοπικές αποφάσεις ίσως δεν είναι οι βέλτιστες σε μεγάλη κλίμακα, οπότε το QOT σε αυτή την περίπτωση θα μπορούσε να βελτιστοποιήσει την συνολική κίνηση της πόλης στέλνοντας στους οδηγούς των αυτοκινήτων προτάσεις για την βελτιστοποίηση του χρόνου ταξιδιού ή για την αποφυγή κίνησης ή ατυχημάτων.

Το QOT ενός ανθρώπου αποτελεί την επέκταση των τωρινών ψηφιακών βοηθών ή των έξυπνων προσωπικών βοηθών και των ψηφιακών διδύμων. Μπορεί να ειπωθεί ως μια κβαντική οντότητα ικανή να ψηφιοποιεί έναν άνθρωπο και να δρα εκ μέρους του στον κβαντικό χώρο, εκμεταλλευόμενη τις δυνατότητες κβαντικής τεχνητής νοημοσύνης για την επίλυση πολύπλοκων προβλημάτων. Δεν μπορούμε να περιμένουμε να λύνουμε περίπλοκα προβλήματα βελτιστοποίησης σε πραγματικό χρόνο με τους κλασικούς ψηφιακούς υπολογιστές σε ζητήματα χρόνου επεξεργασίας και απαιτήσεων κατανάλωσης ενέργειας. Για αυτό και η κβαντική υπολογιστική τεχνολογία μπορεί να κάνει την διαφορά.

4.4. Κβαντικό Διαδίκτυο (Quantum Internet)

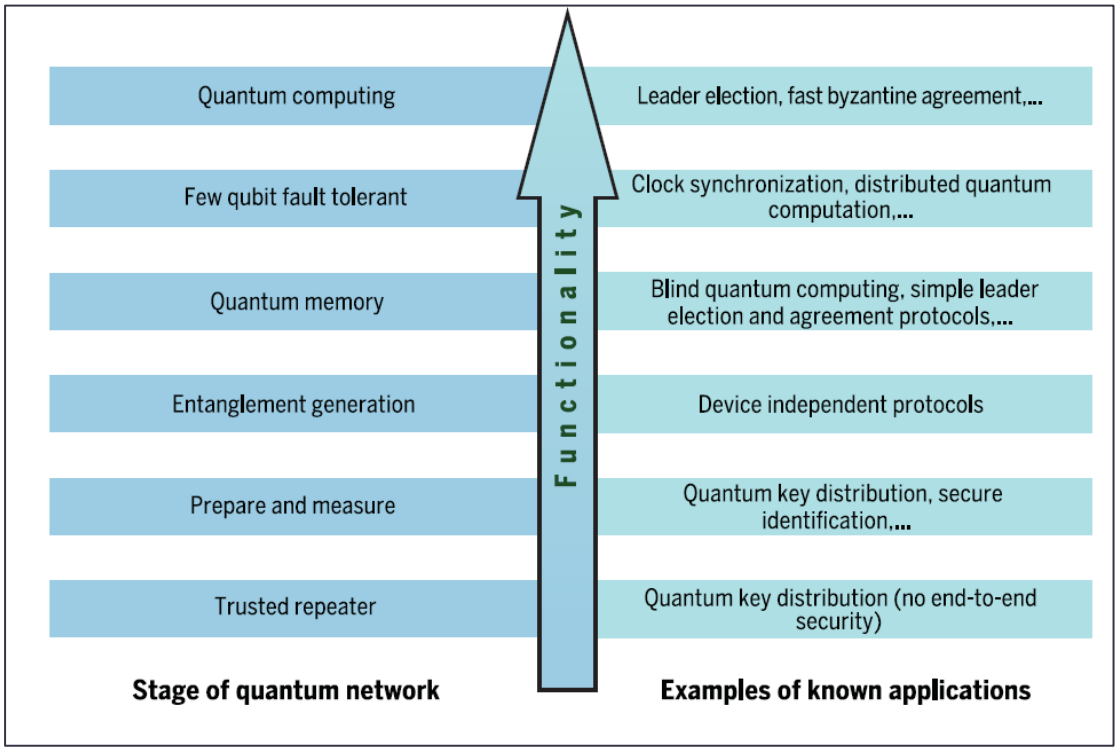
Είναι γεγονός ότι η δημιουργία και η ανάπτυξη του διαδικτύου απετέλεσε γεγονός με εξαιρετικά σημαντικό αντίκτυπο στον κόσμο. Ο σκοπός του κβαντικού διαδικτύου θα είναι, αντίστοιχα, να αξιοποιηθεί σε ζητήματα που το κλασικό ανάλογό του αδυνατεί να ανταπεξέλθει. Έτσι, το κβαντικό διαδίκτυο θα μπορούσε να συμπληρώνει το διαδίκτυο του σήμερα με χρήση κβαντικής επικοινωνίας, ενώ θεωρείται από κάποιους ότι όλες οι επικοινωνιακές ανάγκες μας θα καλύπτονται πλήρως από κβαντικά κανάλια [15] . Όπως έχουμε ήδη αναφέρει, μια σημαντική διαφοροποίηση του κβαντικού διαδικτύου από το κλασικό ανάλογό του είναι η κβαντική διανομή κλειδιού, η οποία καθιστά ασφαλέστερες τις τηλεποικωνίες υπό το κβαντομηχανικό πρίσμα. Εντούτοις, οι εφαρμογές του κβαντικού διαδικτύου δεν σταματάνε εκεί, αλλά υπάρχουν πολλές ακόμη που επιτυγχάνουν εκεί που το τωρινό διαδίκτυο αποτυγχάνει. Τέτοιες εφαρμογές είναι, για παράδειγμα, η ασφαλής πρόσβαση σε απόμακρους κβαντικούς υπολογιστές, ακριβέστερος συγχρονισμός ρολογιών και επιστημονικές εφαρμογές όπως ο συνδυασμός φωτός από μακρινά τηλεσκόπια για την βελτίωση παρατηρήσεων. Καθώς η ανάπτυξη του κβαντικού διαδικτύου συνεχίζεται, άλλες χρήσιμες εφαρμογές πιθανώς να εμφανιστούν στο μέλλον.

Εκ πρώτης όψεως, ίσως φαίνεται ότι το εγχείρημα δημιουργίας του κβαντικού διαδικτύου είναι δυσκολότερο από την δημιουργία ενός μεγάλης κλίμακας κβαντικού υπολογιστή. Εξάλλου, μπορούμε να φανταζόμαστε σε πλήρη αναλογία με το κλασικό διαδίκτυο, ότι η τελική εκδοχή ενός κβαντικού διαδικτύου απαρτίζεται από πλήρεις, λειτουργικούς κβαντικούς υπολογιστές που μπορούν να ανταλλάσσουν έναν αυθαίρετο αριθμό από qubits. Ευτυχώς, όπως υποδεικνύουν αρκετά πρωτόκολλα κβαντικών δικτύων, δεν είναι απαραίτητη η υλοποίηση μεγάλων κβαντικών υπολογιστών. Μια κβαντική συσκευή με ένα μόνο qubit στο άκρο της είναι ήδη αρκετή για αρκετές εφαρμογές. Επιπλέον, τα σφάλματα στα πρωτόκολλα του κβαντικού διαδικτύου συχνά μπορούν να αντιμετωπιστούν με χρήση κλασικών παρά κβαντικών τεχνικών διόρθωσης σφαλμάτων, επιβάλλοντας λιγότερες απαιτήσεις στον έλεγχο και την ποιότητα των qubits απ’ ότι στην περίπτωση ενός μεγάλου κβαντικού υπολογιστή. Ο λόγος που η αντίστοιχη «φιλοσοφία» του κβαντικού διαδικτύου μπορεί να ξεπεράσει τις δυνατότητες του κλασικού με τόσα, σημαντικά λιγότερα μέσα είναι επειδή τα πλεονεκτήματα των κβαντικών πρωτοκόλλων βασίζονται εξ ολοκλήρου στις εγγενώς κβαντικές ιδιότητες όπως η κβαντική σύμπλεξη, η οποία μπορεί να αξιοποιηθεί με μόλις μερικά qubits. Αντίθετα, ένας κβαντικός υπολογιστής πρέπει να διαθέτει περισσότερα qubits που μπορούν να προσομοιωθούν σε έναν κλασικό υπολογιστή για να προσφέρει ένα υπολογιστικό πλεονέκτημα. Δεδομένων των προκλήσεων που ανακύπτουν στην ανάπτυξη ενός κβαντικού διαδικτύου, είναι χρήσιμο να σκεφτούμε το τι δυνατότητες χρειάζονται για να επιτύχουμε συγκεκριμένες κβαντικές εφαρμογές και τι τεχνολογία χρειάζεται για την υλοποίησή τους.

Η υλοποίηση κβαντικού διαδικτύου απαιτεί σημαντική ανάπτυξη των κβαντικών αναμεταδοτών, όπως επίσης και των end nodes. Είναι σαφές ότι βραχυπρόθεσμα, μπορεί κανείς να βελτιστοποιήσει και τα δύο σχετικά ανεξάρτητα. Δηλαδή, μπορεί κανείς να φανταστεί ένα κβαντικό διαδίκτυο που αξιοποιεί σχετικά απλά end nodes αλλά που χρησιμοποιεί αναμεταδότες αρκετά ισχυρούς που να καλύπτουν μεγάλες αποστάσεις. Ομοίως, ένα κβαντικό διαδίκτυο στο εγγύς μέλλον θα μπορούσε να βελτιστοποιηθεί για μικρότερες αποστάσεις (λ.χ. παν-ευρωπαϊκά), ενώ θα χρησιμοποιεί πολύ πιο ισχυρά end nodes ικανά να εφαρμόζουν ένα μεγάλο σύνολο από πρωτόκολλα. Ιδανικά, αυτοί οι σχεδιασμοί μπορούν να εξασφαλίσουν προς τα εμπρός συμβατότητα για την επίτευξη του τελικού στόχου ενός πλήρως ανεπτυγμένου, παγκόσμιου κβαντικού διαδικτύου.

Περιγράφουμε, αρχικά, τις φάσεις της ανάπτυξης του κβαντικού διαδικτύου με γνώμονα την λειτουργικότητα. Κάθε διαδοχικό τέτοιο στάδιο διακρίνεται από την αυξανόμενη λειτουργικότητα, με τίμημα την αυξανόμενη πειραματική δυσκολία. Λέμε ότι μια πειραματική υλοποίηση έχει φτάσει ένα συγκεκριμένο στάδιο μόνο όταν η λειτουργικότητα αυτού του σταδίου και όλων των προηγουμένων είναι διαθέσιμη στα end nodes αυτού του δικτύου. Κρίσιμη στη διάκριση ανάμεσα στα στάδια είναι το ότι επακόλουθο προσφέρει μια θεμελιωδώς καινούργια λειτουργικότητα που δεν

είναι διαθέσιμη στο προηγούμενο στάδιο αντί απλά να βελτιώνει παραμέτρους ή να προσφέρει «και άλλο από το ίδιο» αυξάνοντας των αριθμό των qubits. Χάριν απλότητας, τα στάδια και οι έλεγχοι που περιγράφονται ακολούθως αφορούν συστήματα που προετοιμάζουν και μεταδίδουν qubits, αλλά είναι εφικτό να αναφερθούμε σε αυτές τις δυο εργασίες όταν εμπλέκονται qubits (κβαντικά συστήματα υψηλότερων διαστάσεων) ή συνεχείς μεταβλητές. Για κάθε στάδιο περιγράφουμε κάποιο από τα πρωτόκολλα εφαρμογών που είναι ήδη γνωστά και μπορούν να υλοποιηθούν με την λειτουργικότητα που παρέχεται σε αυτό το στάδιο.



ΕΙΚΟΝΑ 4.2:ΤΑ ΣΤΑΔΙΑ ΑΝΑΠΤΥΞΗΣ ΤΟΥ ΚΒΑΝΤΙΚΟΥ ΔΙΑΔΙΚΤΥΟΥ (ΠΗΓΗ: S. WEHNER, D.ELKOUSS, R. HANSON, "QUANTUM INTERNET: A VISION FOR THE ROAD AHEAD")

Είναι εύκολα αντιληπτό το ότι ένα απλό πρωτόκολλο, ή καλύτερα θεωρητική ανάλυση, μπορεί να βρεθεί στο μέλλον που να λύνει το ίδιο πρόβλημα με λιγότερες απαιτήσεις επί της λειτουργικότητας. Έτσι, παράλληλα με τις αποθαρρυντικές προκλήσεις στις προσπάθειες υλοποίησης του κβαντικού διαδικτύου, υπάρχουν και οι προκλήσεις για τους προγραμματιστές κβαντικού λογισμικού για την σχεδίαση πρωτοκόλλων που υλοποιούν ευκολότερα μια διεργασία σε κάποιο στάδιο. Αυτές οι παράμετροι μπορούν να εκτιμηθούν χρησιμοποιώντας μια σειρά από απλούς ελέγχους, που μας επιτρέπουν να πιστοποιούμε την επίδοση μιας πειραματικής εφαρμογής που επιτυγχάνει κάποιο συγκεκριμένο στάδιο, όπως επίσης και την επίδοση πρωτοκόλλων που εξαρτώνται από τις παραμέτρους αυτές.

- Δίκτυα αξιόπιστων αναμεταδοτών (Trusted repeater networks)

Το πρώτο στάδιο διαφέρει σημαντικά από τα υπόλοιπα, μιας και δεν επιτρέπει end-to-end μεταδόσεις των qubits. Παρ ‘όλα αυτά, από τεχνολογικής άποψης, τα δίκτυα αξιόπιστων αναμεταδοτών μπορούν να χρησιμεύσουν ως εφαλτήριο για την ανάπτυξη του κβαντικού διαδικτύου, δίνοντας ώθηση στην ανάπτυξη υποδομών και σε μηχανικές εξελίξεις. Ανάλογα με την υποκείμενη τεχνολογία, οι αξιόπιστοι αναμεταδότες μπορούν να αναβαθμιστούν σε πραγματικούς κβαντικούς αναμεταδότες. Ειδικότερα, ένα δίκτυο αξιόπιστων αναμεταδοτών έχει τουλάχιστον δύο end nodes και μια ακολουθία από συνδέσμους σε μικρές αποστάσεις που συνδέουν κοντινούς ενδιάμεσους αναμεταδοτικούς κόμβους. Κάθε ζεύγος διπλανών κόμβων χρησιμοποιεί κβαντική διανομή κλειδιού για την ανταλλαγή κλειδιών κρυπτογράφησης. Αυτά τα ανά ζεύγη κλειδιά επιτρέπουν στα end nodes να γεννούν το δικό τους κλειδί, δεδομένου ότι όλοι οι ενδιάμεσοι κόμβοι είναι αξιόπιστοι. Ένα πρώτο βήμα αναβάθμισης τέτοιων δικτύων θα μπορούσε να είναι μια διαδικασία κβαντικής διανομής κλειδιού ανεξάρτητης της συσκευής μέτρησης, που αποτελεί ένα πρωτόκολλο που είναι ασφαλές ακόμη και με αναξιόπιστες συσκευές μέτρησης που εφαρμόζεται με τυπικές οπτικές συνιστώσες και πηγές. Αυτό το πρωτόκολλο ήδη αξιοποιεί κάποια συστατικά που είναι χρήσιμα και για μετέπειτα στάδια, όπως μετρήσεις Bell δύο φωτονίων.

-Δίκτυα προετοιμασίας και μέτρησης(Prepare and measure networks)

Αυτό το στάδιο είναι το πρώτο που προσφέρει end-to-end κβαντική λειτουργικότητα. Επιτρέπει end-to-end κβαντική διανομή κλειδιού χωρίς την ανάγκη χρήσης ενδιάμεσων αναμεταδοτικών κόμβων και ήδη επιτρέπει μια σειρά από πρωτόκολλα για άλλες ενδιαφέρουσες διεργασίες. Αυτό το στάδιο επιτρέπει σε κάθε κόμβο να προετοιμάσει μια μονοδυφιακή κατάσταση και να μεταδώσει την κατάσταση που προκύπτει σε οποιονδήποτε άλλο κόμβο, ο οποίος μετά θα την μετρήσει. Στην περίπτωση που ένα σήμα ότι το qubit έχει χαθεί μπορεί να γεννηθεί. Για παράδειγμα, κόμβος- δέκτης μπορεί να αγνοήσει φαινόμενα μη ανίχνευσης και να συμπεράνει ότι αυτά τα qubits έχουν χαθεί. Αν ο πομπός μπορεί να προετοιμάσει μια συνεπλεγμένη κατάσταση από δύο qubits, τότε αυτό το στάδιο συμπεριλαμβάνει και την ειδική περίπτωση όπου ο πομπός μεταδίδει το πρώτο και το δεύτερο qubit σε δύο διαφορετικούς κόμβους του δικτύου (ή σε έναν άλλο κόμβο και στον εαυτό του). Τέτοια κατανομή σύμπλεξης μπορεί να επιλεγεί εκ των υστέρων.

Αυτού του είδους η λειτουργικότητα προετοιμασίας και μέτρησης που μόλις περιγράψαμε δεν είναι ισοδύναμη με την μετάδοση αυθαίρετων qubit κατά μήκος ενός δικτύου. Η τελευταία απαιτεί την δυνατότητα μεταφοράς μιας άγνωστης κατάστασης (που ο πομπός δεν γνωρίζει πώς να προετοιμάσει) ντετερμινιστικά στον δέκτη- δηλαδή δεν υπάρχει εκ των υστέρων επιλογή κατά τα φαινόμενα ανίχνευσης.

Αυτό το στάδιο είναι ήδη επαρκές για την υλοποίηση πρωτοκόλλων για αρκετές ενδιαφέρουσες κρυπτογραφικές διεργασίες, αρκεί η πιθανότητα απώλειας (p) και οι ανακρίβειες κατά την μετάδοση (ε_T) και κατά την μέτρηση (ε_M) είναι αρκετά μικρά. Η πιο γνωστή τέτοια διεργασία είναι η κβαντική διανομή κλειδιού, η οποία παρέχει μια λύση στην διεργασία γένεσης ενός ασφαλούς κλειδιού κρυπτογράφησης ανάμεσα σε δύο μακρινούς end nodes. Υπάρχουν πρωτόκολλα κβαντικής διανομής κλειδιού που μπορούν να υλοποιηθούν με μονοδυφιακές προετοιμασίες και μετρήσεις με ανοχή σε κάποια ποσότητα εκ των υστέρων επιλογών. Για γνωστό πρωτόκολλα σε αυτό το στάδιο, η συνθήκη $\varepsilon_T + \varepsilon_M \leq 0.11$ είναι επαρκής και μπορεί να εκτιμηθεί ελέγχοντας μόνο ένα μικρό αριθμό καταστάσεων.

-Δίκτυα διανομής σύμπλεξης (Entanglement distribution networks)

Το τρίτο στάδιο επιτρέπει end-to-end δημιουργία κβαντικής σύμπλεξης με ντετερμινιστικό ή και με άλλους τρόπους, όπως επίσης και τοπικές μετρήσεις. Τα end nodes δεν απαιτούν κβαντική μνήμη σε αυτό το στάδιο.

Ο όρος «ντετερμινιστική δημιουργία σύμπλεξης» (deterministic entanglement generation) αναφέρεται στο γεγονός ότι η διαδικασία επιτυγχάνει με πιθανότητα (σχεδόν) ένα. Η heralding δημιουργία σύμπλεξης είναι μια ελαφρώς ασθενέστερη μορφή της ντετερμινιστικής στην οποία σηματοδοτούμε την επιτυχή δημιουργία σύμπλεξης με ένα ενδεχόμενο που είναι ανεξάρτητο της (άμεσης) μέτρησης των συνεπλεγμένων qubits. Εδώ, η δημιουργία σύμπλεξης είναι ντετερμινιστική, δεδομένου ενός τέτοιου σήματος επιτυχίας. Ειδικότερα, αυτό απαγορεύει εκ των υστέρων επιλογές για ανίχνευση ενδεχομένων που μετράνε τα συνεπλεγμένα qubits.

Η κυριότερη πρόοδος σε αντίθεση με το προηγούμενο στάδιο είναι ότι σε αυτό είναι εφικτή η υλοποίηση πρωτοκόλλων ανεξαρτήτων από την συσκευή, στα οποία οι κβαντικές συσκευές είναι κατά πολύ αναξιόπιστες. Ειδικότερα, η ιδέα της ανεξαρτησίας συσκευών μοντελοποιεί τα end nodes ως κάποιου είδους μαύρα κουτιά, στα οποία μπορούμε να δώσουμε κλασικές οδηγίες για την εκτέλεση συγκεκριμένων μετρήσεων και να πάρουμε τα αντίστοιχα αποτελέσματα που προκύπτουν από τις μετρήσεις. Δεν είναι εξασφαλισμένη η πραγματική κβαντική κατάσταση ή οι μετρήσεις που εκτελούνται από την συσκευή, όπου η συσκευή μπορεί να κατασκευάζεται από κάποιον παρείσακτο. Το κλασικό λογισμικό που χρησιμοποιείται για τον έλεγχο τέτοιων κβαντικών συσκευών είναι αξιόπιστο και υποτίθεται ότι η κβαντική συσκευή απλά επιδεικνύει συμπεριφορά εισόδου/εξόδου. Συγκεκριμένα, οι συσκευές μπορούν να καταγράφουν τις εισόδους και τις εξόδους τους, αλλά δεν μπορούν να μεταδώσουν το κλειδί στον παρείσακτο. Χαμηλά σφάλματα προετοιμασίας και μέτρησης τέτοια ώστε $\varepsilon_P + \varepsilon_M \leq 0.057$ είναι αρκετά για να εξασφαλίσουν την εφαρμοσιμότητα κβαντικής διανομής κλειδιού, στην οποία

ικανές και αναγκαίες συνθήκες για τις παραμέτρους να εφαρμόσουν γενικές διεργασίες σε αυτό το στάδιο είναι άγνωστες.

-Δίκτυα κβαντικής μνήμης (Quantum memory networks)

Το επόμενο στάδιο διακρίνεται από την δυνατότητα για τα end nodes να έχουν τοπική μνήμη ενώ παράλληλα επιτρέποντας καθολικό τοπικό έλεγχο. Αυτό επιτρέπει την εφαρμογή αρκετά πιο περίπλοκων πρωτοκόλλων που απαιτούν προσωρινή αποθήκευση μιας κβαντικής κατάστασης κατά τη διάρκεια περαιτέρω κβαντικών ή κλασικών επικοινωνιών. Παραδείγματα αποτελούν πρωτόκολλα για την επίλυση διεργασιών κατανεμημένων συστημάτων. Αυτό το στάδιο υποδεικνύει επίσης την δυνατότητα εκτέλεσης «απόσταξης» σύμπλεξης και την δημιουργία πολυσωματιδιακών σύμπλεκτων καταστάσεων από δυσωματιδιακή σύμπλεξη, εκμεταλλεύοντας την δυνατότητα για τοπική μνήμη και τοπικό έλεγχο. Σημαντική διαφορά από το προηγούμενο στάδιο είναι ότι πλέον είναι δυνατή η μεταφορά αγνώστων qubit από έναν κόμβο του δικτύου σε έναν άλλο- παραδείγματος χάριν, με χρήση ντετερμινιστικής τηλεμεταφοράς. Αυτή η δυνατότητα δεν εξασφαλίζεται από το προηγούμενο στάδιο: η ύπαρξη τεχνολογίας που μπορεί να χρησιμοποιηθεί για την ντετερμινιστική αναμετάδοση qubit σε μεγάλες αποστάσεις μέσω κβαντικής διόρθωσης σφαλμάτων σε μεγάλη κλίμακα υποδηλώνει την τεχνολογική δυνατότητα υλοποίησης καλής τοπικής κβαντικής μνήμης. Μια σημαντική παράμετρος στην εφαρμογή πρωτοκόλλων είναι ο αριθμός γύρων επικοινωνίας k, δηλαδή ο αριθμός των φορών που ανταλλάσσεται πληροφορία μεταξύ δύο end nodes κατά τη διάρκεια του πρωτοκόλλου. Για την υλοποίηση χρήσιμων πρωτοκόλλων εφαρμογών, ο χρόνος αποθήκευσης t θα πρέπει να συγκριθεί με τον χρόνο επικοινωνίας στο δίκτυο αντί για τον απόλυτο χρόνο. Αυτό σημαίνει ότι τα δίκτυα κόμβων που είναι μακριά μεταξύ τους χρειάζονται πράγματι να παρουσιάζουν μεγαλύτερους χρόνους μνήμης για να επιτύχουν αυτό το στάδιο, και η ποιότητα της μνήμης είναι χρονοεξαρτώμενη. Το ότι αυτός ο χρόνος t σχετίζεται με τον μέγιστο χρόνο που απαιτείται για δύο κόμβους να επικοινωνήσουν οφείλεται στο ότι ένα στάδιο επιτυγχάνεται μόνο όταν η λειτουργικότητα είναι διαθέσιμη σε οποιουσδήποτε δύο κόμβους του δικτύου, ακόμη και αν αυτοί οι δυο είναι οι πιο μακρινοί μεταξύ τους.

Η διαθεσιμότητα κβαντικών μνημών και ντετερμινιστικής μετάδοσης qubits επιτρέπει την χρήση πολλών νέων πρωτοκόλλων σε αυτό το στάδιο. Αρχικά, για να είναι ασφαλής η χρήση τέτοιων υπολογιστών- χωρίς, δηλαδή, την αποκάλυψη της φύσης ή του αποτελέσματος του υπολογισμού τους- είναι δυνατή η εκτέλεση ασφαλούς υποβοηθούμενου κβαντικού υπολογισμού ή «τυφλού» κβαντικού υπολογισμού. Έτσι, μια απλή κβαντική συσκευή που είναι ικανή να προετοιμάσει και να μετρήσει qubits είναι αρκετή για την εκτέλεση υπολογισμών σε έναν μεγάλης κλίμακας κβαντικό υπολογιστή ούτως ώστε ο κβαντικός υπολογιστής να μην μπορεί να αποκτήσει πληροφορία για το πρόγραμμα ή το αποτέλεσμα. Το ότι χρειαζόμαστε

έναν μεγάλης κλίμακας κβαντικό υπολογιστή δεν σημαίνει ότι ένα δίκτυο κβαντικής υπολογιστικής απαιτείται για την εκτέλεση τέτοιων πρωτοκόλλων. Χρειαζόμαστε απλώς ένα κβαντικό διαδίκτυο που επιτρέπει την επικοινωνία ενός client με τον διακομιστή.

Άλλες διεργασίες στο κομμάτι της Κρυπτογραφίας αποτελούν εργαλεία όπως πρωτόκολλα διαμοιρασμού κλασικών ή κβαντικών μυστικών, συμπεριλαμβανομένων επαληθεύσιμων σχημάτων μοιρασμού μυστικών και ανώνυμων μεταδόσεων. Αυτό το στάδιο, επίσης, προσφέρει και άλλες ενδιαφέρουσες δυνατότητες πέραν των κρυπτογραφικών. Για παράδειγμα, υπάρχουν προτάσεις που εκμεταλλεύονται την σύμπλεξη σε μεγάλες αποστάσεις για την επέκταση του baseline στα τηλεσκόπια, για την βελτίωση του συγχρονισμού των ρολογιών κ.ά. Ανάλογα με τις απαιτήσεις που έχουμε από έναν τέτοιο συγχρονισμό, τα προτεινόμενα πρωτόκολλα μπορούν να υλοποιηθούν με χρήση κβαντικής μνήμης ή few-qubit fault-tolerant δίκτυα.

Αναγκαίες και ικανές απαιτήσεις των παραμέτρων για την επίλυση των προαναφερθέντων διεργασιών δεν είναι ακόμη γνωστές. Είναι, επίσης, αντιληπτό ότι μια βελτιωμένη ανάλυση λαμβάνοντας υπόψη το αν η ντετερμινιστική διανομή qubit είναι απαραίτητη, ή αν αρκεί η εκ των υστέρων επιλεγμένη διανομή qubits, μπορεί να ωθήσει κάποια απ’ τα πρωτόκολλα σε χαμηλότερο στάδιο.

-Few-qubit fault-tolerant networks

Αυτό το στάδιο διαφέρει απ΄την απαίτηση οι τοπικές διαδικασίες να πραγματοποιούνται με κάποια ανοχή σε σφάλματα, κάτι το οποίο αποτελεί μεγαλύτερη πρόκληση. Η ανοχή σφαλμάτων δεν είναι αναγκαία για αρκετά πρωτόκολλα του κβαντικού διαδικτύου, αλλά το να είναι διαθέσιμα τέτοια πρωτόκολλα θα επέτρεπε την εκτέλεση τοπικών κβαντικών υπολογισμών σε υψηλό βάθος κυκλώματος όπως επίσης και αυθαίρετη επέκταση (θεωρητικά, έστω) του χρόνου αποθήκευσης για την εκτέλεση πρωτοκόλλων με αυθαίρετο αριθμό γύρων επικοινωνίας.

Το ότι αναφερόμαστε σε λίγα qubits (few qubits) αφορά το γεγονός ότι ο αριθμός των qubits που είναι διαθέσιμος είναι ακόμη μικρός για να προσομοιώνονται αποτελεσματικά τα end nodes σε κλασικούς υπολογιστές. Αυτό δεν σημαίνει ότι ολόκληρο το δίκτυο μπορεί να προσομοιωθεί αποτελεσματικά ή ότι θα μπορούσαν να υπάρξουν ισοδύναμα κλασικά πρωτόκολλα, και αυτό διότι οι επιδράσεις της σύμπλεξης δεν μπορούν να αναπαραχθούν κλασικά.

Η πρόσβαση σε fault-tolerant πύλες επιτρέπει τον υψηλότερης ακριβείας συγχρονισμό ρολογιών και πρωτόκολλα που απαιτούν πολλούς γύρους επικοινωνίας και υψηλό βαθμό κυκλώματος για να είναι χρήσιμη. Αυτό συμπεριλαμβάνει τον κατανεμημένο κβαντικό υπολογισμό όπως και εφαρμογές για πλήρη κβαντικά υπολογιστικά δίκτυα, περιορισμένα σε λίγα qubits. Αυτό θα μπορούσε να έχει μεγάλο πρακτικό ενδιαφέρον, ιδιαίτερα σε εφαρμογές στον χώρο των κατανεμημένων

συστημάτων, αλλά σε ό,τι αφορά την υλοποίηση κβαντικών αλγορίθμων σε κβαντικούς υπολογιστές, η ισχύς του να έχουμε περιορισμένο αριθμό από qubits στην διάθεσή μας είναι ενδιαφέρον ζήτημα για διερεύνηση.

-Δίκτυα κβαντικής υπολογιστικής(Quantum computing networks)

Το τελικό στάδιο αναφέρεται σε κβαντικούς υπολογιστές που μπορούν να ανταλλάσσουν αυθαίρετα κβαντική επικοινωνία. Το καινούργιο στοιχείο σε αυτό το στάδιο αφορά στο ότι προσφέρονται πλέον λύσεις σε υπολογιστικά προβλήματα που δεν μπορούν πλέον να λυθούν αποτελεσματικά με κλασικούς υπολογιστές.

Είναι σαφές ότι σε αυτό το στάδιο του κβαντικού διαδικτύου είναι δυνατή λίγο-πολύ η εφαρμογή οποιοδήποτε πρωτοκόλλου. Οι μικρής κλίμακας εκδοχές πρωτοκόλλων που ακολουθούν μπορούν να υλοποιηθούν επίσης και στο few-qubit fault-tolerant στάδιο και περαιτέρω ανάπτυξη μπορεί να οδηγήσει σε περίτεχνα πρωτόκολλα και ανάλυση που να τα τοποθετεί σε χαμηλότερα στάδια.

Αρχικά, θα εστιάσουμε και πάλι στην Κρυπτογραφία. Σε αυτό το στάδιο, είναι εφικτό το στρίψιμο νομισμάτων με αυθαίρετα μικρή μεροληψία. Μπορούμε, επίσης, να λύνουμε καθαρά κβαντικής διεργασίες, όπως ασφαλή multiparty κβαντικούς υπολογισμούς, και έτσι σχηματίζεται μια επέκταση της κλασικής αξιολόγησης ασφαλούς λειτουργίας στο κβαντικό πλαίσιο. Κλασικά, αυτό σημαίνει ότι ο κόμβος j διατηρεί ένα input string x_j και όλοι οι n κόμβοι υπολογίζουν από κοινού το $y = f(x_1, \dots, x_n)$. Ο στόχος είναι οι κακοήθεις κόμβοι να μην μπορούν να συμπεράνουν τίποτα παραπάνω για τα inputs x_j των «καλών» κόμβων απ' ότι παρατηρώντας την έξοδο y. Ένα παράδειγμα αυτού του προβλήματος είναι η ασφαλής ψηφοφορία, όπου το $x_j \in \{0,1\}$ αντιστοιχεί στην επιλογή ανάμεσα σε έναν από δύο πιθανούς υποψηφίους και f είναι η συνάρτηση πλειοψηφίας. Η κβαντική εκδοχή αυτού επιτρέπει κάθε ομάδα (party) να διατηρεί μια κβαντική κατάσταση $|\Psi_j\rangle$ ως είσοδο, και οι ομάδες από κοινού επιθυμούν να υπολογίσουν μια κβαντική διεργασία U.

Στην συνέχεια, στρέφουμε την προσοχή μας σε κατανεμημένα συστήματα τα οποία διαμορφώνονται από μερικές υπολογιστικές συσκευές που είναι συνδεδεμένες, στις οποίες αναφερόμαστε στην καθομιλουμένη με τον όρο «cloud». Πολλές προκλήσεις προκύπτουν στον συντονισμό και τον έλεγχο τέτοιων συστημάτων που ενδεχομένως να μην είναι τόσο οικείες σε έναν φυσικό. Ένα απλό παράδειγμα: ας θεωρήσουμε ότι μια τραπεζική συναλλαγή καταγράφεται εφεδρικά σε αρκετούς backup servers. Αν ένας ή περισσότεροι αποτύχουν κατά το update, ενδέχεται να δείχνουν ασυνεπή δεδομένα (λ.χ. 1 εκατομμύριο ευρώ εναντίον 0). Πρωτόκολλα για την επίτευξη συμφωνίας μεταξύ επεξεργαστών αναπτύσσονται ευρέως στην πράξη- για παράδειγμα το σύστημα Chubby της Google. Εκτός του χώρου του διαδικτύου αυτού καθαυτού, άλλα παραδείγματα αποτελούν την αξιοπιστία σε smart grids, συστήματα ελέγχου πτήσεων και πίνακες αισθητήρων.

Αυτό το πεδίο δεν είναι προς το παρόν εξίσου ανεπτυγμένο στο κβαντικό του ανάλογο, ωστόσο κάποια πρωτόκολλα είναι γνωστό ότι καταδεικνύουν πως το κβαντικό διαδίκτυο προσφέρει πολλές δυνατότητες για την επίλυση προβλημάτων σε κατανεμημένα συστήματα, κατά πολύ πιο αποδοτικό τρόπο απ' ότι είναι εφικτό κλασικά. Διαισθητικά, ο λόγος που η Κβαντική Επικοινωνία μπορεί να βοηθήσει την επίλυση τέτοιων προβλημάτων είναι ότι η σύμπλεξη επιτρέπει τον συντονισμό ανάμεσα σε μακρινούς μεταξύ τους επεξεργαστές με τρόπο σημαντικά πιο αποδοτικό απ' ότι μπορεί να επιτευχθεί κλασικά. Ένα από τα πιο εκπληκτικά παραδείγματα «κβαντικού» πλεονεκτήματος σε κατανεμημένα συστήματα μπορεί να βρεθεί για την διεργασία του byzantine agreement. Ο στόχος εδώ είναι να επιτραπεί σε n επεξεργαστές να συμφωνούν σε ένα κοινό bit, ενώ ένα κλάσμα εξ αυτών μπορεί να είναι ελαττωματικό. Ο όρος «byzantine» αναφέρεται στο εξαιρετικά απαιτητικό μοντέλο των αυθαίρετα συσχετισμένων σφαλμάτων, στο οποίο οι ελαττωματικοί επεξεργαστές ουσιαστικά συμπράττουν στην παρεμπόδιση του πρωτοκόλλου. Μπορεί να δειχθεί ότι σε κάποια συστήματα, υπάρχει ένα κβαντικό πρωτόκολλο που λύνει αυτήν την διεργασία με χρήση ενός σταθερού αριθμού γύρων κβαντικής επικοινωνίας, ενώ η ποσότητα κλασικής πληροφορίας είναι της τάξης $O(\sqrt{\frac{n}{logn}})$, όπου n το πλήθος των επεξεργαστών. Το σχετικό πρωτόκολλο απαιτεί αρκετά qubits, απαιτώντας έτσι λειτουργικότητα του τελικού σταδίου του κβαντικού διαδικτύου.
Ο στόχος της εκλογής «αρχηγού» είναι η εκλογή ενός «ηγετικού» επεξεργαστή από ένα πλήθος κατανεμημένων επεξεργαστών, που είναι ένα σημαντικό εργαλείο λ.χ. για να αποφασίσουμε ποιος επεξεργαστής θα αξιοποιήσει κάποιον συγκεκριμένο πόρο. Αυτή η διεργασία αποτελεί ιδιαίτερα μεγάλη πρόκληση σε ένα ανώνυμο δίκτυο, στο οποίο κανένας κόμβος δεν έχει αναγνωριστικό. Σε αυτό το πλαίσιο, δεν υπάρχει ακριβής κλασικός αλγόριθμος για εκλογή αρχηγού σε γενικές τοπολογίες δικτύων, ενώ κβαντικά η επίλυση αυτού του προβλήματος είναι εφικτή.

Τέλος, αυτό το στάδιο επιτρέπει την επίλυση κατανεμημένων υπολογιστικών διεργασιών μέσω μετάδοσης σε κάποιες περιπτώσεις ακόμη και εκθετικά λιγότερων qubits σε σχέση με τα κλασικά bits. Ωστόσο, αυτά τα πρωτόκολλα απαιτούν γενικά μεγάλο αριθμό από qubits σε κάθε end node για την επίτευξη σημαντικού πλεονεκτήματος. Συγκεκριμένες παραλλαγές τέτοιων πρωτοκόλλων με περιορισμούς ενέργειας μπορούν να υλοποιηθούν και σε χαμηλότερα στάδια. Τέλος, η παρουσία σύμπλεξης επιφέρει και νέα ζητήματα ασφαλείας για υπάρχοντα κλασικά πρωτόκολλα, απαιτώντας περαιτέρω ανάλυση.

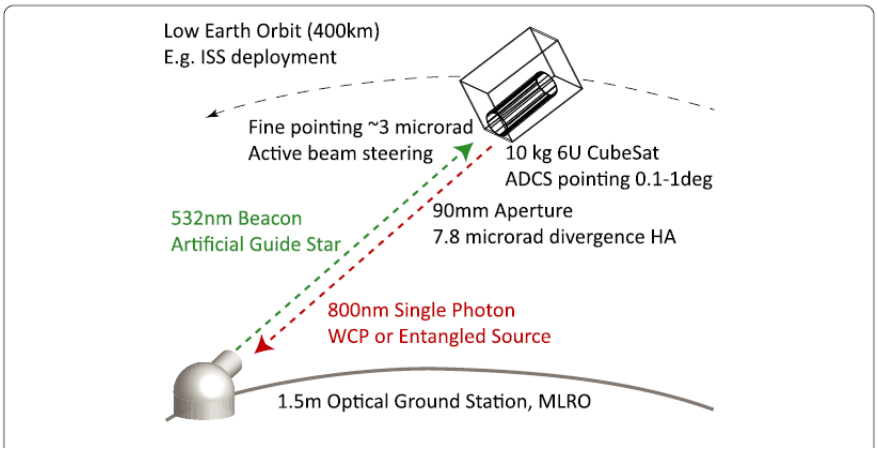
Η παρούσα κατάσταση στο πειραματικό κομμάτι για κβαντικά δίκτυα μεγάλων αποστάσεων είναι στο χαμηλότερο στάδιο με αρκετά εμπορικά συστήματα για κβαντική διανομή κλειδιού στην αγορά. Τα πρώτα εκτεταμένα δίκτυα αξιόπιστων αναμεταδοτών έχουν ήδη εφαρμοσθεί σε μητροπολιτικές αποστάσεις, ενώ η εφαρμογή σε μεγάλες αποστάσεις έχει ολοκληρωθεί πρόσφατα. Η υλοποίηση του πρώτου σταδίου με end-to-end κβαντική λειτουργικότητα – δίκτυα προετοιμασίας

και μέτρησης- σε μεγάλες αποστάσεις απαιτεί την χρήση κβαντικών αναμεταδοτών για την γεφύρωση μεγάλων αποστάσεων μέσω αποθήκευση ενδιάμεσων qubits ή διόρθωσης σφαλμάτων, όπως επίσης απαιτούνται routers για την προώθηση κβαντικών καταστάσεων στον επιθυμητό κόμβο. Αρκετά πρόσφατα πειράματα έχουν επιδείξει στοιχεία που ανήκουν σε αυτό και σε υψηλότερα στάδια σε ό,τι αφορά μικρές αποστάσεις, υποδεικνύοντας ότι είναι προσιτά και τα δίκτυα υψηλότερης λειτουργικότητας. Λεπτομερέστερα για αυτά τα πειράματα παραπέμπουμε στο [13].

4.5. Το πρόγραμμα της CubeSat

Τα τελευταία χρόνια η CubeSat έχει αναπτύξει ένα πρόγραμμα για την ανάπτυξη τεχνολογιών Κβαντικής Επικοινωνίας σε δορυφόρους [17]. Συγκεκριμένα, σκοπός του προγράμματος είναι αφενός η –ασφαλέστερη όπως είδαμε- κβαντική διανομή κλειδιού και αφετέρου η επίτευξη σύμπλεξης μεταξύ εδάφους και διαστήματος.

Παρακάτω φαίνεται η ιδέα για τις επιχειρήσεις CONOPS. Στόχος είναι η αποστολή κβαντικών σημάτων στο επίπεδο ενός φωτονίου από μια πλατφόρμα σε τροχιά σε κάποιο δέκτη στο έδαφος.

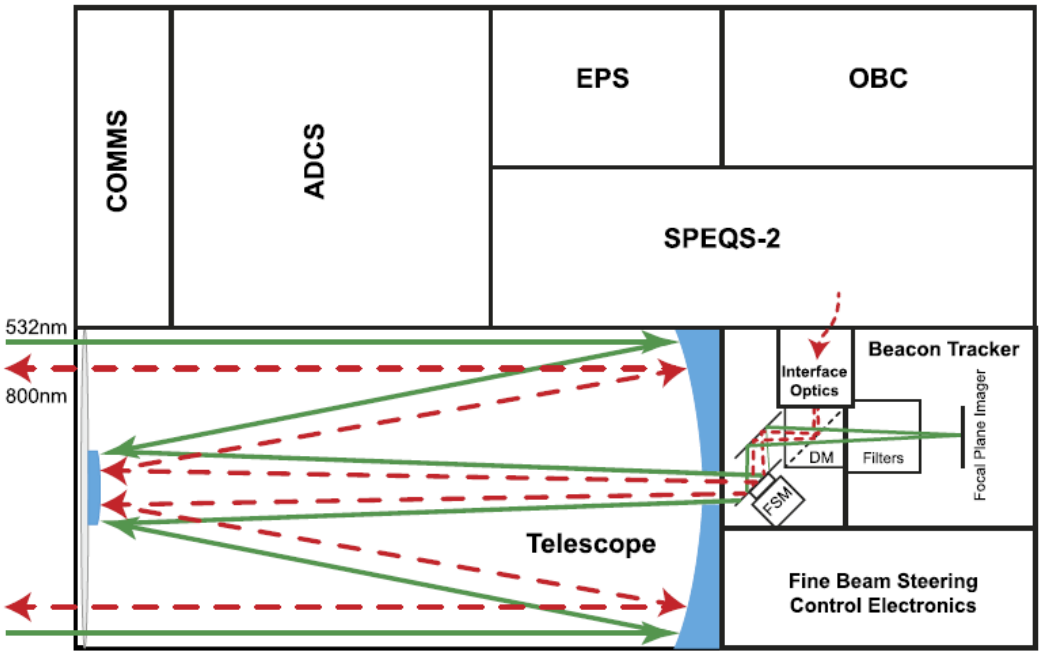


ΕΙΚΟΝΑ 4.3(ΠΗΓΗ:D. KL OI ET AL., "CUBESAT QUANTUM COMMUNICATIONS MISSION")

Ο αντίστοιχος δορυφόρος θα εκτοξευόταν από τον διεθνή διαστημικό σταθμό σε χαμηλή κυκλική τροχιά γύρω από την Γη. Ο σταθμός που θα παρακολουθούσε τον δορυφόρο στην επιφάνεια της Γης θα ήταν ο Matera Laser Rangefinding Observatory του πανεπιστημίου της Πάντοβα, λειτουργώντας ως οπτικός σταθμός εδάφους (Ο.Σ.Ε.).Ο Ο.Σ.Ε. θα μετέδιδε ένα ισχυρό beacon καθοδήσης στα 532nm επιτρέποντας στον δορυφόρο να αποκτήσει και να ξεκινήσει να παρακολουθεί την επιθυμητή θέση. Ο ανιχνευτής του beacon είναι ευθυγραμμισμένος με το εξερχόμενο σήμα φωτονίων και επιτρέπει την ακρίβεια στον προσδιορισμό της κατεύθυνσης διορατικότητας του τηλεσκοπίου μετάδοσης. Το σήμα σφάλματος από τον ανιχνευτή beacon χρησιμοποιείται για την καθοδήγηση ενός ταχέως περιστρεφόμενου καθρέφτη για την κατεύθυνση φωτονίων του σήματος προς τον Ο.Σ.Ε. Το fine-pointing σύστημα λαμβάνει υπόψιν την εκτροπή ταχύτητας με point-ahead διόρθωση. Μια κβαντική

πηγή πάνω στον δορυφόρο παρέχει μονο-φωτονικού επιπέδου σήματα που ανιχνεύονται από τον Ο.Σ.Ε. Μια εναλλάξιμη πηγή strong/weak συνεπούς παλμού επιτρέπει και στα δύο την δυνατότητα χαρακτηρισμού την απόδοση σημαδέματος και του free-space καναλιού, καθώς επίσης και κβαντική διανομή κλειδιού. Μια πηγή συμπλεγμένων φωτονίων θα επέτρεπε την κατανομή της σύμπλεξης μεταξύ διαστήματος και εδάφους, με ένα ζεύγος φωτονίων να μετράται επί του δορυφόρου και ύστερα τα αποτελέσματα συγκρίνονται με το αντίστοιχο ζεύγος στο έδαφος.

Η δομή του δορυφόρου είναι όπως φαίνεται ακολούθως:



ΕΙΚΟΝΑ 4.4:ΔΙΑΤΑΞΗ ΔΟΡΥΦΟΡΟΥ(ΠΗΓΗ:D. KL OI ET AL., "CUBESAT QUANTUM COMMUNICATIONS MISSION")

Το μισό της διάταξης αφιερώνεται σε οπτική μετάδοσης, περιλαμβάνοντας ένα τηλεσκόπιο, ανιχνευτή beacon, καθοδηγητή δεσμών, και οπτική διεπαφή με την κβαντική πηγή. Ηλιακά πάνελ πάνω στον δορυφόρο θα παρείχαν ενέργεια την οποία το σύστημα πλατφόρμας EPS θα αποθήκευε και θα διένειμε. Οι επικοινωνίες διαχειρίζονται από UHF, S-band και X-band ραδιοσυστήματα. Το ADCS αποτελείται από ανιχνευτές της Γης, του Ήλιου και των αστέρων, magnetorquers και 3-axis momentum wheels. Το OBC διαχειρίζεται τις λειτουργίες του συστήματος. Η επεξεργασία δεδομένων εκτελείται από τον υπολογιστή της αποστολής ως κομμάτι του φορτίου της πηγής συμπλεγμένων φωτονίων (SPEQS-2).

4.6. Κβαντικά κανάλια μηδενικής χωρητικότητας

Οι εξελίξεις στον χώρο της Κβαντικής Επικοινωνίας δεν σταματάνε σε αυτά που μέχρι στιγμής έχουμε παρουσιάσει. Ένα άλλο παράδειγμα σχετικών προόδων στον κλάδο είναι η επίτευξη κβαντικής επικοινωνίας με χρήση καναλιών μηδενικής χωρητικότητας [14]. Γενικώς, το βασικό πρόβλημα σε κινητές, διαδικτυακές και δορυφορικές επικοινωνίες είναι η μετρίαση και διόρθωση του θορύβου. Ο Shannon έδωσε μια συστηματική θεωρία ανάλυσης της παρουσίας θορύβου, κάνοντας πιθανοθεωρητικές υποθέσεις επί της φύσης του θορύβου. Μοντελοποιώντας ένα θορυβώδες κανάλι N ως μια πιθανοθεωρητική απεικόνιση από τα σήματα εισόδου σε σήματα εξόδου, η χωρητικότητα C(N) του N ορίζονται ως το πλήθος των bits που δύναται να μεταδοθεί ανά χρήση καναλιού, με τα σφάλματα να εξαφανίζονται καθώς αυξάνει το πλήθος των μεταδόσεων. Η χωρητικότητα υπολογίζεται μέσω της σχέσης $C(N) = \max_{\mathrm{X}} I(X;Y)$ όπου η μεγιστοποίηση γίνεται πάνω από τις τυχαίες μεταβλητές X στην είσοδο του καναλιού, Y είναι η αντίστοιχη έξοδος της εισόδου X, ενώ I(X,Y)=H(X)+H(Y)-H(X,Y) είναι η από κοινού πληροφορία που ποσοτικοποιεί την συσχέτιση ανάμεσα σε είσοδο και έξοδο. Η ποσότητα $H(X) = -\sum_x p_x \log_2 p_x$ είναι η κατά Shannon εντροπία και ποσοτικοποιεί το πόσο ακριβώς τυχαία είναι η X. Η χωρητικότητα, με μονάδες bits ανά χρήση καναλιού, είναι το βασικό φράγμα ανάμεσα στους ρυθμούς επικοινωνίας που είναι εφικτοί και σε εκείνους που δεν είναι, δίνοντας μια καθοδήγηση στην σχεδίαση τεχνικών διόρθωσης σφαλμάτων.

Μια θεμελιώδης πρόβλεψη της φόρμουλας της χωρητικότητας είναι ότι τα μόνα κανάλια με μηδενική χωρητικότητα είναι ακριβώς εκείνα στα οποία η είσοδος και η έξοδος είναι πλήρως ασυσχέτιστες. Επιπλέον, αν υποθέσουμε ότι έχουμε πρόσβαση συγχρόνως σε δύο θορυβώδη κανάλια N_1, N_2 τότε $C(N_1 \times N_2) = C(N_1) + C(N_2)$. Η προσθετικότητα της χωρητικότητας μας δείχνει ότι είναι ένα εγγενές μέτρο των ιδιοτήτων μετάδοσης πληροφορίας του καναλιού.

Τα κβαντικά δεδομένα είναι μια ιδιαίτερα ευαίσθητη μορφή πληροφορίας και είναι ιδιαίτερα επιρρεπής στις επιδράσεις του θορύβου. Όπως έχουμε ήδη τονίσει, η Κβαντική Επικοινωνία μας εξασφαλίζει απεριόριστα ασφαλή επικοινωνία και ένας κβαντικός υπολογιστής επιταχύνει σημαντικά τους διάφορους υπολογισμούς, οπότε μας ενδιαφέρει ιδιαίτερα το να «θωρακίσουμε» τα κβαντικά δεδομένα από θόρυβο. Ένα κβαντικό κανάλι N μοντελοποιεί την φυσική διαδικασία που προσθέτει θόρυβο μέσα σε ένα κβαντικό σύστημα μέσω αλληλεπίδρασης με ένα μη παρατηρήσιμο περιβάλλον, γενικεύοντας το μοντέλο του Shannon και επιτρέποντας μια πιο ακριβή απεικόνιση της υποκείμενης φυσικής. Σε αυτό το πλαίσιο, είναι φυσικό να αναρωτηθούμε πώς μπορούμε να βρούμε την χωρητικότητα ενός κβαντικού καναλιού για μετάδοση κβαντομηχανικής πληροφορίας και το κατά πόσον υπάρχει για αυτήν μια απλή φόρμουλα όπως αυτή του Shannon.

Η απάντηση σε αυτό το ερώτημα μπορεί να δοθεί με την έννοια της συνεπούς πληροφορίας:

$$Q^{(1)}(N) = \max_{\rho^A} H(B) - H(E) \quad (4.1)$$

Οι εντροπίες μετρούνται στις καταστάσεις που επάγονται στην έξοδο και στο περιβάλλον από την κατάσταση εισόδου ρ^A, όπου H(B) είναι η εντροπία von Neumann τις κατάστασης ρ^B κατά την έξοδο. Η συνεπής πληροφορία διαφέρει από την από κοινού πληροφορία. Η διαφορά σχετίζεται με το θεώρημα της μη κλωνοποίησης.

Η πιο γνωστή έκφραση της κβαντικής χωρητικότητας δίνεται από την «κανονικοποίηση» της $Q^{(1)}$:

$$Q(N) = \lim_{n\to\infty} \frac{Q^{(1)}(N^{\times n})}{n} \quad (4.2)$$

Με το σύμβολο $N^{\times n}$ εννοούμε n αντίγραφα του n. Η ασυμπτωτική φύση αυτής της έκφρασης μας αποτρέπει από τον καθορισμό της κβαντικής χωρητικότητας ενός καναλιού κατά ουσιαστικό τρόπο, ενώ καθίσταται δύσκολη η ανακάλυψη των γενικών της ιδιοτήτων. Σε αντίθεση με την χωρητικότητα κατά Shannon, όπου η κανονικοποίηση είναι περιττή, εδώ δεν μπορεί να παραληφθεί. Ως εκ τούτου, ακόμη και φαινομενικά απλά ερωτήματα, όπως το να προσδιορίσουμε από την περιγραφή ενός καναλιού το αν μπορούμε να το χρησιμοποιήσουμε για αποστολή κβαντικής πληροφορίας, είναι προς το παρόν απροσδιόριστο. Στην πραγματικότητα, η απάντηση σε αυτό το ερώτημα εξαρτάται από το γενικό πλαίσιο: υπάρχουν ζεύγη καναλιών μηδενικής χωρητικότητας που μαζί παράγουν θετική κβαντική χωρητικότητα. Από αυτό συνάγουμε ότι η κβαντική χωρητικότητα δεν είναι προσθετική και έτσι η κβαντική χωρητικότητα δεν προσδιορίζει πλήρως την ικανότητα ενός καναλιού να μεταφέρει κβαντική πληροφορία.

Παρ ‘ότι ο πλήρης χαρακτηρισμός των μηδενικής χωρητικότητας καναλιών είναι άγνωστος, ορισμένες κλάσεις τέτοιων καναλιών μας είναι γνωστές. Μια τέτοια κλάση απαρτίζεται από κανάλια με κοινή κβαντική κατάσταση για έξοδο και περιβάλλον που είναι συμμετρική κάτω από εναλλαγή. Αυτά τα «συμμετρικά κανάλια» διαφέρουν αρκετά από τα μηδενικής χωρητικότητας κανάλια του Shannon, αφού παρουσιάζουν συσχετίσεις μεταξύ εισόδου και εξόδου. Ωστόσο, από μόνα τους δεν είναι χρήσιμα στην κβαντική επικοινωνία επειδή η συμμετρία υποδεικνύει ότι οποιαδήποτε χωρητικότητα θα οδηγούσε στην παραβίαση του θεωρήματος μη κλωνοποίησης. Μια άλλη κλάση καναλιών μηδενικής χωρητικότητας είναι τα λεγόμενα «κανάλια Horodecki», τα οποία παράγουν αρκετά ασθενώς συμπλεγμένες καταστάσεις που ικανοποιούν μια συνθήκη που λέγεται θετική μερική μετάθεση.

Μολονότι κανάλια από την μια ή την άλλη εξ αυτών των κλάσεων δεν μπορούν να συνδυαστούν για την πιστή μεταφορά κβαντικών δεδομένων, είναι δυνατό κάποιες φορές να καταλήξουμε σε θετική κβαντική χωρητικότητα όταν συνδυάσουμε ένα κανάλι από κάθε κλάση. Για την περιγραφή αυτού του

φαινομένου, εισάγουμε τις έννοιες της «ιδιωτικής χωρητικότητας» (private capacity) και της «βοηθούμενης χωρητικότητας» (assisted capacity).

Η ιδιωτική χωρητικότητα $P(N)$ ενός κβαντικού καναλιού N είναι ο ρυθμός στον οποίο μπορεί να χρησιμοποιηθεί το κανάλι για την αποστολή κλασικών δεδομένων, με τρόπο ώστε η μετάδοση να είναι ασφαλής απέναντι σε όποιον παρείσακτο έχει πρόσβαση στο περιβάλλον του καναλιού. Αυτή η χωρητικότητα σχετίζεται άμεσα με τα πρωτόκολλα κβαντικής διανομής κλειδιού και μπορεί να δειχθεί ότι πρόκειται ουσιαστικά για την κανονικοποίηση της «ιδιωτικής πληροφορίας»:

$$P^{(1)}(N) = \max_{X,\rho_x^A}(I(X;B) - I(X;E)) \quad (4.3)$$

όπου η μεγιστοποίηση γίνεται επί των κλασικών τυχαίων μεταβλητών X και των κβαντικών καταστάσεων ρ_x^A της εισόδου του N ανάλογα με την τιμή x της X.

Για να βρούμε άνω φράγμα της κβαντικής χωρητικότητας η «βοηθούμενη χωρητικότητα» έχει εισαχθεί εκεί που επιτρέπεται ελεύθερα η χρήση αυθαίρετων συμμετρικών καναλιών για την υποβοήθηση κβαντικών επικοινωνιών σε ένα δοθέν κανάλι. Αν με $\mathcal{A}$ συμβολίζουμε ένα συμμετρικό κανάλι μη φραγμένης διάστασης (το ισχυρότερο τέτοιο κανάλι), τότε η βοηθούμενη χωρητικότητα $Q_{\mathcal{A}}(N)$ ενός κβαντικού καναλιού ικανοποιεί:

$$Q_{\mathcal{A}}(N) = Q(N \times \mathcal{A}) = Q^{(1)}(N \times \mathcal{A}) (4.4)$$

Επειδή η διάσταση της εισόδου στο $\mathcal{A}$ είναι μη φραγμένη, δεν μπορούμε να εκτιμήσουμε αυτήν την χωρητικότητα γενικά. Ωστόσο, μας βοηθάει να συμπεράνουμε κάποια πράγματα για πεπερασμένης διάστασης κανάλια.

Ενώ τα κανάλια Horodecki έχουν μηδενική κβαντική χωρητικότητα, είναι γνωστά παραδείγματα τέτοιων καναλιών με μη μηδενική ιδιωτική χωρητικότητα. Το ένα από τα δύο μηδενικής χωρητικότητας κανάλια το συνδυάζουμε για να έχει θετική από κοινού χωρητικότητα και είναι αυτό που λέμε «ιδιωτικό κανάλι Horodecki» N_H και το άλλο είναι το συμμετρικό κανάλι $\mathcal{A}$. Τα βασικό εργαλείο μας είναι η ακόλουθη νέα σχέση ανάμεσα στις χωρητικότητες του καναλιού N:

$$\frac{1}{2}P(N) \leq Q_{\mathcal{A}}(N) (4.5)$$

δηλαδή η βοηθούμενη χωρητικότητα ενός καναλιού είναι τουλάχιστον το μισό της ιδιωτικής χωρητικότητας. Συνεπάγεται ότι οποιοδήποτε ιδιωτικό κανάλι Horodecki N_H έχει θετική βοηθούμενη χωρητικότητα και άρα δύο μηδενικής χωρητικότητας κανάλια $N_H, \mathcal{A}$ ικανοποιούν:

$$Q_{\mathcal{A}}(N_H) = Q(N_H \times \mathcal{A}) > 0 \ (4.6)$$

Παρ ‘ότι η κατασκευή μας συμπεριλαμβάνει συστήματα με μη φραγμένη διάσταση, μπορεί να δειχθεί ότι ένα ιδιωτικό κανάλι Horodecki μπορεί να

συνδυαστεί με ένα πεπερασμένο συμμετρικό κανάλι για να δώσουν θετική κβαντική χωρητικότητα. Ειδικότερα, υπάρχει τέτοιο κανάλι που δρα ως σύστημα τεσσάρων επιπέδων. Το κανάλι αυτό δίνει θετική κβαντική χωρητικότητα όταν συνδυάζεται με ένα μικρό συμμετρικό κανάλι- ένα κανάλι διαγραφής 50% $\mathcal{A}_e$ με τεσσάρων επιπέδων είσοδο που τις μισές φορές μεταφέρει την κατάσταση εισόδου στην έξοδο, αλλιώς δίνει το μήνυμα στον δέκτη ότι έχει πραγματοποιηθεί διαγραφή. Μπορεί να δειχθεί ότι ο παράλληλος συνδυασμός αυτών των καναλιών έχει κβαντική χωρητικότητα μεγαλύτερη από 0.01.

Κατόπιν αυτής της συζήτησης, ανακύπτει κατά φυσιολογικό τρόπο το ερώτημα του κατά πόσον είναι εφικτή η μεταφορά πληροφορίας. Με κβαντικά δεδομένα, η απάντηση θα ήταν «εξαρτάται». Αν πάρουμε τα ιδιωτικά κανάλια Horodecki και τα συμμετρικά κανάλια μεμονωμένα, κανένα από τα δυο δεν είναι χρήσιμα στην μεταφορά κβαντικής πληροφορίας, το καθένα για διαφορετικούς λόγους. Εντούτοις, κάθε κανάλι έχει την δυνατότητα να ενεργοποιήσει το άλλο, αναιρώντας επί της ουσίας τον λόγο που το άλλο έχει μηδενική χωρητικότητα. Δεν υπάρχει ανάλογο φαινόμενο στην κλασική θεωρία. Ενδεχομένως κάθε κανάλι να μεταφέρει διαφορετική, αλλά κατά μια έννοια συμπληρωματική πληροφορία. Σε αυτήν την περίπτωση, μπορεί να ποσοτικοποιηθεί ουσιωδώς αυτή η πληροφορία; Υπάρχουν άλλα ζεύγη μηδενικής χωρητικότητας καναλιών που παρουσιάζουν αυτήν την συμπεριφορά; Υπάρχουν τριάδες τέτοιων καναλιών αντίστοιχα;

Πέραν της προσθετικότητας, τα ευρήματα αυτά απαντούν σε δύο ανοικτά ερωτήματα αναφορικά με την κβαντική χωρητικότητα. Αρχικά, η κβαντική χωρητικότητα δεν είναι κυρτή συνάρτηση του καναλιού. Η κυρτότητα της χωρητικότητας σημαίνει ότι ένα πιθανοθεωρητικό μείγμα δύο καναλιών δεν έχει ποτέ μεγαλύτερη χωρητικότητα απ’ ότι το αντίστοιχο μέσο των χωρητικοτήτων δύο μεμονωμένων καναλιών. Η παραβίαση της κυρτότητας οδηγεί σε κάτι ενάντιο της διαίσθησής μας, όπου μπορεί να είναι ωφέλιμο να ξεχάσουμε ποιο κανάλι χρησιμοποιείται. Επιπλέον, υπάρχουν κανάλια με αυθαίρετα μεγάλο κενό ανάμεσα στα $Q^{(1)}$- αυτό λέγεται «hashing rate»- και την κβαντική χωρητικότητα . Ήταν συνεπές με προηγούμενα αποτελέσματα το να θεωρήσουμε ότι τα Q,$Q^{(1)}$ είναι ίσα έως μικρών διορθώσεων. Πλέον, όμως, είναι γνωστό ότι δεν έχουν έτσι τα πράγματα και υπάρχουν ενδείξεις για το ότι το hashing rate είναι ένα υπερβολικά απαισιόδοξο κατώφλι ως προς το οποίο μετράται η απόδοση πρακτικών διεργασιών διόρθωσης σφαλμάτων.

Είδη αυτής της υπερενεργοποίησης είναι γνωστά στο multiparty πλαίσιο, όπου μερικά διαχωρισμένα σωματίδια επικοινωνούν μέσω ενός κβαντικού καναλιού με πολλαπλές εισόδους ή εξόδους και εικάζεται ότι αντίστοιχα συμπεριφέρεται και ένα κβαντικό κανάλι βοηθούμενο από κλασική επικοινωνία ανάμεσα σε πομπό και δέκτη. Αυτές οι περιπτώσεις είναι αρκετά περίπλοκες, για αυτό και δεν αποτελεί έκπληξη το να παρουσιάζουν κάποια «εξωτική» συμπεριφορά. Αντιθέτως, το πρόβλημα της άνευ θορύβου κβαντικής επικοινωνίας με θορυβώδη κβαντικά κανάλια είναι μια απ’ τις πιο απλές και πιο

φυσικές διεργασίες στο κβαντομηχανικό πλαίσιο. (Για μια πιο εκτενή ανάλυση καναλιών μηδενικής χωρητικότητας, παραπέμπουμε στο [18])

Σύνοψη-Συμπεράσματα

Είδαμε ότι ο χώρος της Κβαντικής Υπολογιστικής και της Κβαντικής Επικοινωνίας είναι αρκετά πλούσιος ερευνητικά, μιας και είναι πολλές οι προκλήσεις που παρουσιάζονται για την περαιτέρω ανάπτυξη τέτοιων τεχνολογιών. Είναι ακόμη αβέβαιο, λ.χ., το πότε θα έχουμε έναν μεγάλης κλίμακας κβαντικό υπολογιστή ο οποίος να λειτουργεί ικανοποιητικά. Παρά το γεγονός ότι έχουν γίνει και στο παρελθόν προσπάθειες προς αυτή την κατεύθυνση, δεν έχει δοθεί ακόμη μια καθοριστική λύση. Εντούτοις, έχει γίνει ήδη εκτενής έρευνα – παρουσιάσαμε μόνο ένα σχετικά μικρό μέρος της- για την ανάπτυξη και την προσπάθεια ενσωμάτωσης αυτής της τεχνολογίας στην καθημερινότητά μας, με ποίκιλλες εφαρμογές να περιλαμβάνουν την καινούργια γενιά τηλεπικοινωνιών, τη Δορυφορική Επικοινωνία και πολλά ακόμη. Έτσι, παρά το γεγονός ότι υπάρχουν πολλές δυσκολίες για την άμεση αξιοποίηση κβαντικών τεχνοτροπιών στην καθημερινότητά μας, η ασύγκριτη αποδοτικότητά τους αποτελεί κίνητρο για να υπερνικήσουμε αυτές τις δυσκολίες.

Βιβλιογραφία

[1] Σ. Τραχανάς: «Κβαντομηχανική Ι», 2005, Πανεπιστημιακές Εκδόσεις Κρήτης

[2] Σ. Τραχανάς: «Κβαντομηχανική ΙΙ», 2016, Πανεπιστημιακές Εκδόσεις Κρήτης

[3] M. Pavic: «Quantum Computation and Quantum Communication,Theory and Experiments», 2006, Springer Science&Business Media, Inc,

[4]Ι. Καραφυλλίδης, «Κβαντική Υπολογιστική», 2015, Εκδόσεις Κάλλιπος

[5]D. P. DiVincenzo, "The Physical Implementation of Quantum Computation". Fortschritte der Physik, 2000, 48 (9–11):771–783, arXiv:quant-ph/0002077

[6] J. I. Cirac, P. Zoller "Quantum Computations with Cold Trapped Ions". Physical Review Letters, 1995, 74 (20): 4091–4094.

[7] M.Nielsen, I.Chuang, ”Quantum Computation and Quantum Information” Cambridge, 2010, Cambridge University Press. doi:10.1017/CBO9780511976667

[8] A. Manzalini, “Quantum Communications in Future Networks and Services” Quantum Rep, 2020, 2: 221-232. https://doi.org/10.3390/quantum2010014

[9] S. Ummethala, T. Harter, K. Koehnle, Z. Li, S. Muehlbrandt, Y. Kutuvantavida, Y P. Marin-Palomo, J. Schaefer, A. Tessmann, S.K. Garlapati, et al. «THz-to-optical conversion in wireless communications using an ultra-broadband plasmonic modulator» Nat. Photonics, 2019, 13: 519–524.

[10] B. Fröhlich, J.F. Dynes, M. Lucamarini, A.W. Sharpe, Z. Yuan, A.J. Shields «A quantum access network» Nature, 2013, 501: 69–72.

[11] C.Cai, Y. Sun, J. Niu, Y. Ji, «A Quantum Access Network Suitable for Internetworking Optical Network Units», IEEE Access, 2019, 7: 92091–92099.

[12] F. Flamini, N. Spagnolo, F. Sciarrino «Photonic quantum information processing: A review». Rep. Prog. Phys. 2018, 82, 016001.

[13] D. Pierangeli, G. Marcucci, C. Conti «Large-scale photonic Ising machine by spatial light modulation». Phys. Rev. Lett. 2019, 122, 213902.

[14] X. Lin, Y. Rivenson, N.T. Yardimci, M. Veli, Y. Luo, M. Jarrahi, A. Ozcan «All-optical machine learning using diractive deep neural networks» Science, 2018, 361: 1004–1008.

[15] S.Wehner, D.Elkouss, R.Hanson «Quantum Internet: A vision for the road ahead», Science Magazine, 2018, 362,6412

[16] D. Castelvecchi, «The quantum internet has arrived (and it hasn't)». Nature, 2018, 554, 289–292

[17] D.K.Oi, A.Ling, G. Vallone et al. "CubeSat quantum communications mission". EPJ Quantum Technol. 2017, 4: 6. https://doi.org/10.1140/epjqt/s40507-017-0060-1

[18] G. Smith, J. Yard, "Quantum Communication with Zero-Capacity Channels", Science Magazine, 2008, 321: 1812 - 1815, arXiv:0807.4935