



ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Κβαντικό Δίκτυο και Διαδίκτυο

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Τσίβος Χρήστος Μάριος (ΑΜ: 3119078)

Επιβλέπων: Ξενάκης Απόστολος, Καθηγητής

ΛΑΡΙΣΑ, Φεβρουάριος 2024



UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Quantum Network and Internet

BACHELOR THESIS

Tsivos Christos Marios (RN: 3119078)

Supervisor: *Xenakis Apostolos, Professor*

LARISSA, February 2024

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

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

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

Ο/Η Δηλών/ούσα

(Υπογραφή)

Ονοματεπώνυμο Φοιτητή/-ήτριας

Ημερομηνία

Τσίβος Χρήστος Μάριος

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων

Ξενάκης Απόστολος

Επίκουρος Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Μέλος 1ο

Σάββας Ηλίας

Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Μέλος 2ο

Ιατρέλλης Όμηρος

Επίκουρος Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης:

Περίληψη

Αυτή η πτυχιακή εργασία ασχολείται με την με την ανάλυση της κβαντικής μηχανικής , την ανασκόπηση των πρωτοκόλλων και λύσεων που θα προσφέρει το κβαντικό διαδίκτυο. Ειδικότερα ασχολείται με τις ιδιαιτερότητες που έχουν οι κβαντικές επικοινωνίες , τα μέρη που αποτελείται το κβαντικό δίκτυο και αναλύει τα συστήματα που είναι απαραίτητα για την λειτουργία του κβαντικού διαδικτύου. Τέλος στην πτυχιακή αυτή υλοποιείται το κβαντικό κύκλωμα πρωτοκόλλου BB84 με χρήση Python με σκοπό την ανάδειξη του τρόπου λειτουργίας του κβαντικού προγραμματισμού.

Abstract

This thesis deals with the analysis of quantum mechanics, reviewing the protocols and solutions that the quantum internet will offer. In particular, it deals with the peculiarities of quantum communications, the parts that make up the quantum network and analyzes the systems that are necessary for the operation of the quantum internet. Finally, in this thesis, the BB84 protocol quantum circuit is implemented using Python in order to demonstrate how quantum programming works.

Ευχαριστίες

Η παρούσα πτυχιακή εργασία ήθελε πολύ κόπο και χρόνο. Το ενδιαφέρον περιεχόμενο των κβαντικών δικτύων αλλά και η μαγεία του κβαντικού κόσμου με κατέστησε ικανό να ολοκληρώσω την εργασία.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου τον κύριο Ξενάκη Απόστολο για την βοήθειά του και τις ιδέες του, καθώς και όλους τους καθηγητές της σχολής για τις γνώσεις που μου παρείχαν αυτά τα χρόνια.

Ονοματεπώνυμο

Τσίβος Χρήστος Μάριος

Ημερομηνία

15/06/2024

Περιεχόμενα

ΠΕΡΙΛΗΨΗ	VII
ABSTRACT	IX
ΕΥΧΑΡΙΣΤΙΕΣ.....	XI
ΠΕΡΙΕΧΟΜΕΝΑ.....	XIII
1 ΕΙΣΑΓΩΓΗ	1
1.1 ΠΕΡΙ ΚΒΑΝΤΙΚΩΝ.....	1
1.2 ΟΡΙΣΜΟΙ	2
1.3 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ.....	5
2 ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ	9
2.1 ΚΒΑΝΤΙΚΗ ΜΗΧΑΝΙΚΗ	9
2.1.1 Χώρος Καταστάσεων και Αρχή Υπερθέσης.....	9
2.1.2 Single Qubit System	11
2.1.3 Multiple qubits.....	12
2.1.4 Bell States ή EPR.....	12
2.1.5 Κβαντική Εμπλοκή.....	13
2.2 ΚΒΑΝΤΙΚΟ ΔΙΚΤΥΟ.....	15
2.2.1 Κβαντικές πύλες	15
2.2.2 Κβαντικά πρωτόκολλα δικτύου.....	18
2.2.3 Μέρη κβαντικού δικτύου.....	25
2.3 ΚΒΑΝΤΙΚΟ ΔΙΑΔΙΚΤΥΟ	32
2.3.1 Εφαρμογές	32
2.3.2 Προβλήματα	36
2.3.3 Λύσεις.....	39
2.4 ΚΒΑΝΤΙΚΕΣ ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ.....	42
2.4.1 Κβαντική τηλεμεταφορά.....	43
2.4.2 Θεώρημα μη κλωνοποίησης.....	47
3 ΤΑ ΒΑΣΙΚΑ ΤΗΣ ΡΥΘΗΘΗ.....	51

3.1	ΤΙ ΕΙΝΑΙ Η PYTHON.....	51
3.1.1	Τι κάνει η Python και Πώς μπορεί να χρησιμοποιηθεί αυτή η γλώσσα προγραμματισμού;.....	52
3.1.2	Γιατί να χρησιμοποιήσουμε την Python	53
3.2	ΙΣΤΟΡΙΑ ΤΗΣ PYTHON.....	54
3.3	ΠΑΡΑΔΕΙΓΜΑΤΑ ΣΤΗΝ PYTHON.....	54
3.4	QISKIT, JUPITER NOTEBOOK, ANACONDA PYTHON.....	56
3.4.1	Πως συνεργάζονται.....	57
3.4.2	Εγκατάσταση Qiskit στο Jupyter Notebook	58
4	ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ.....	61
4.1	ΠΡΟΣΟΜΟΙΩΣΗ BB84 PROTOCOL ΣΕ ΚΒΑΝΤΙΚΟ ΥΠΟΛΟΓΙΣΤΗ.....	61
4.1.1	Πείραμα 1: Η κωδικοποίηση της Alice και η μέτρηση του Bob χρησιμοποιώντας την ίδια βάση.....	66
4.1.2	Πείραμα 2: Προσομοίωση του BB84 (χωρίς eavesdropping)	67
4.1.3	Πείραμα 3: Προσομοίωση του BB84 με επίθεση eavesdropping	69
5	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	73
	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	75

1 Εισαγωγή

1.1 Περί Κβαντικών

Το Διαδίκτυο έχει αλλάξει τον κόσμο με αμέτρητους τρόπους, συνδέοντας ανθρώπους και πληροφορίες όπως ποτέ άλλοτε. Ωστόσο, καθώς ο όγκος των δεδομένων που παράγουμε και μεταδίδουμε αυξάνεται εκθετικά, οι παραδοσιακές μέθοδοι αποθήκευσης και επεξεργασίας δεδομένων γίνονται όλο και πιο αμφισβητούμενες. Εδώ μπαίνει στο παιχνίδι η κβαντική δικτύωση, προσφέροντας ένα νέο σύνορο σε ασφαλή και αποτελεσματικά κρυπτογραφικά συστήματα.

Οι κβαντικοί υπολογιστές και η κβαντική επικοινωνία είναι δύο ταχέως αναπτυσσόμενοι τομείς στον κόσμο της επιστήμης των υπολογιστών και της τεχνολογίας των πληροφοριών. Οι κβαντικοί υπολογιστές έχουν τη δυνατότητα να φέρουν επανάσταση λύνοντας προβλήματα που οι κλασικοί υπολογιστές δεν μπορούν να λύσουν αποτελεσματικά.

Τα κβαντικά δίκτυα αποτελούν βασικό μέρος των κβαντικών επικοινωνιών, παρέχοντας τα μέσα για τη μετάδοση κβαντικών πληροφοριών σε μεγάλες αποστάσεις. Αυτά τα δίκτυα αναπτύσσονται επί του παρόντος και δοκιμάζονται για εφαρμογές που κυμαίνονται από την ασφαλή επικοινωνία έως τον καταναμημένο υπολογισμό.

Με τον όρο κβαντικό στη φυσική ή ένα κβάντο (πληθυντικός: κβάντα) είναι η μικρότερη ποσότητα οποιασδήποτε φυσικής οντότητας (φυσικής ιδιότητας) που εμπλέκεται σε μια αλληλεπίδραση. Ένα κβάντο είναι μια διακριτή ποσότητα ενέργειας ανάλογη σε μέγεθος με τη συχνότητα της ακτινοβολίας που αντιπροσωπεύει. Η θεμελιώδης αντίληψη ότι μια χημική ιδιότητα μπορεί να «κβαντιστεί» αναφέρεται ως «υπόθεση κβαντοποίησης».[1] Αυτό σημαίνει ότι το μέγεθος της φυσικής ιδιότητας μπορεί να λάβει μόνο διακριτές τιμές που αποτελούνται από ακέραια πολλαπλάσια ενός κβάντου. Για παράδειγμα, ένα φωτόνιο είναι ένα ενιαίο κβάντο φωτός ορισμένης συχνότητας (ή οποιαδήποτε άλλη μορφή ηλεκτρομαγνητικής ακτινοβολίας). Ομοίως, η ενέργεια ενός ηλεκτρονίου που είναι δεσμευμένο σε ένα άτομο είναι κβαντισμένη και μπορεί να υπάρχει μόνο σε ορισμένες διακριτές τιμές. (Τα άτομα και η ύλη γενικά είναι σταθερά επειδή τα ηλεκτρόνια

μπορούν να υπάρχουν μόνο σε διακριτά ενεργειακά επίπεδα μέσα σε ένα άτομο.) Η κβαντοποίηση είναι ένα από τα θεμέλια της πολύ ευρύτερης φυσικής της κβαντικής μηχανικής. Η κβαντοποίηση της ενέργειας και η επιρροή της στον τρόπο αλληλεπίδρασης της ενέργειας και της ύλης (κβαντική ηλεκτροδυναμική) είναι μέρος του θεμελιώδους πλαισίου για την κατανόηση και την περιγραφή της φύσης.

1.2 Ορισμοί

Κβαντικός υπολογισμός: Ο κβαντικός υπολογισμός χρησιμοποιεί κβαντικά bit ή αλλιώς qubits αντί για κλασικά bit για την αποθήκευση και την επεξεργασία πληροφοριών. Οι κβαντικοί υπολογιστές μπορούν να λύσουν προβλήματα που οι κλασικοί υπολογιστές δεν μπορούν να λύσουν αποτελεσματικά, όπως η προσομοίωση πολύπλοκων συστημάτων και η παραγοντοποίηση μεγάλων αριθμών.

Κβαντική επικοινωνία: Η κβαντική επικοινωνία είναι ένας τύπος επικοινωνίας που χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για τη μετάδοση πληροφοριών με ασφάλεια. Σε αντίθεση με την κλασική επικοινωνία, η οποία βασίζεται στην ανταλλαγή ενός κοινόχρηστου μυστικού κλειδιού, η κβαντική επικοινωνία χρησιμοποιεί κβαντική εμπλοκή για να διασφαλίσει ότι οι πληροφορίες που μεταδίδονται είναι ασφαλείς.

Κβαντικό δίκτυο: Το κβαντικό δίκτυο είναι ένας τύπος υποδομής δικτύου που παρέχει τα μέσα για τη μετάδοση κβαντικών πληροφοριών σε μεγάλες αποστάσεις. Βασίζεται στις αρχές της κβαντικής μηχανικής για να εξασφαλίσει την ασφάλεια και την ακεραιότητα των μεταδιδόμενων πληροφοριών. [Εικόνα 1].

Κβαντικό Διαδίκτυο: Το κβαντικό διαδίκτυο οραματίζεται ως ένα δίκτυο που θα επέτρεπε την εξαιρετικά ασφαλή επικοινωνία αξιοποιώντας αυτές τις κβαντικές ιδιότητες [Εικόνα 1].



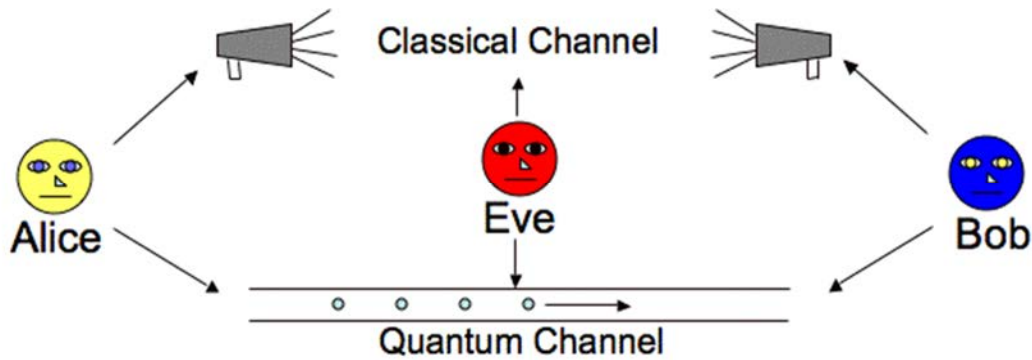
Εικόνα 1: Κβαντικό Δίκτυο-Διαδίκτυο

Ασφαλής Επικοινωνία: Η δυνατότητα ανίχνευσης κάθε προσπάθειας υποκλοπής της κβαντικής επικοινωνίας, καθώς η πράξη της μέτρησης διαταράσσει την κβαντική κατάσταση.

Κβαντική εμπλοκή: Η κβαντική εμπλοκή είναι ένα φαινόμενο όπου δύο ή περισσότερα σωματίδια συσχετίζονται με τέτοιο τρόπο ώστε η κατάσταση ενός σωματιδίου να επηρεάζει στιγμιαία την κατάσταση του άλλου, ανεξάρτητα από την απόσταση μεταξύ τους. Αυτή η ιδιότητα θα μπορούσε να αξιοποιηθεί για τη δημιουργία ασφαλών καναλιών επικοινωνίας.

Κβαντική υπέρθεση: Τα κβαντικά συστήματα μπορούν να υπάρχουν σε πολλές καταστάσεις ταυτόχρονα, γνωστές ως υπέρθεση. Στο πλαίσιο της κβαντικής επικοινωνίας, αυτό θα μπορούσε να χρησιμοποιηθεί για τη μετάδοση πολλαπλών τμημάτων πληροφοριών ταυτόχρονα.

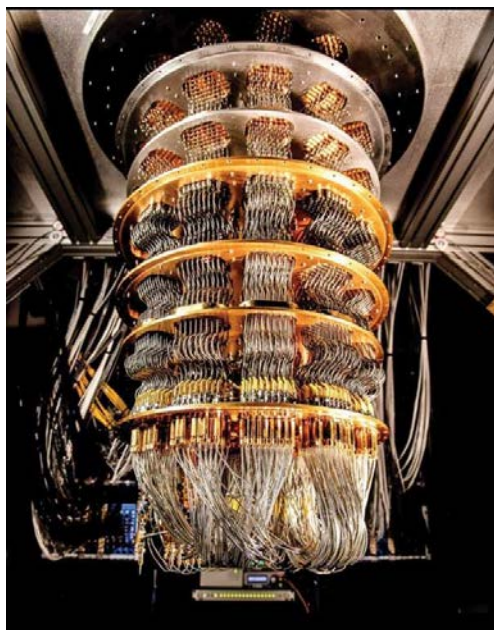
Διανομή Κβαντικού Κλειδιού (QKD): Το QKD είναι μια μέθοδος που χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για να ασφαλίσει την επικοινωνία επιτρέποντας σε δύο μέρη να παράγουν ένα κοινό τυχαίο μυστικό κλειδί. Αυτό το κλειδί μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων, διασφαλίζοντας το απόρρητο και την ασφάλεια της επικοινωνίας [Εικόνα 2].



Εικόνα 2: QKD

Κβαντική τηλεμεταφορά: Η κβαντική τηλεμεταφορά περιλαμβάνει τη μετάδοση κβαντικών πληροφοριών από τη μια θέση στην άλλη, χωρίς τη φυσική μεταφορά σωματιδίων. Βασίζεται στις αρχές της εμπλοκής και είναι μια πιθανή μέθοδος για ασφαλή κβαντική επικοινωνία.

Κβαντικός υπολογιστής: Ένας κβαντικός υπολογιστής είναι ένας υπολογιστής που χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για την εκτέλεση υπολογισμών. Σε αντίθεση με τους κλασικούς υπολογιστές που βασίζονται στα bits που μπορούν να είναι είτε 0 είτε 1, οι κβαντικοί υπολογιστές χρησιμοποιούν κβαντικά bits, ή qubits, τα οποία μπορούν να είναι ταυτόχρονα 0, 1 ή και κάποια συνδυασμός αυτών των δύο καταστάσεων λόγω του φαινομένου της κβαντικής υπερθέσης. Οι κβαντικοί υπολογιστές μπορούν να εκτελέσουν ορισμένους τύπους υπολογισμών σημαντικά πιο γρήγορα από τους κλασικούς υπολογιστές για συγκεκριμένα προβλήματα, όπως η παράλληλη αναζήτηση, οι παραγωγικοί αλγόριθμοι και η παροχή λύσεων σε κβαντικά προβλήματα. Ωστόσο, η ανάπτυξη και η διατήρηση σταθερών κβαντικών κυκλωμάτων και qubits αποτελούν μεγάλες προκλήσεις λόγω της κβαντικής αστάθειας. Κάποιες εφαρμογές των κβαντικών υπολογιστών περιλαμβάνουν την κρυπτογραφία, τον σχεδιασμό νέων υλικών, την προσομοίωση κβαντικών συστημάτων, και την επίλυση προβλημάτων σε επιστημονικούς τομείς όπως η χημεία και η βιολογία. Ωστόσο, οι κβαντικοί υπολογιστές είναι ακόμη σε πρώιμο στάδιο ανάπτυξης, και πολλά προβλήματα πρέπει να επιλυθούν προτού γίνουν πρακτικά και ευρέως διαθέσιμα [Εικόνα 3].



Εικόνα 3: Κβαντικός Υπολογιστής

1.3 Ιστορική αναδρομή

Το Διαδίκτυο έχει μεταμορφώσει τον κόσμο με τρόπο που λίγες άλλες τεχνολογίες έχουν, συνδέοντας ανθρώπους και πληροφορίες όπως ποτέ άλλοτε. Ωστόσο, με την ανάπτυξη της αποθήκευσης και της επεξεργασίας δεδομένων, το Διαδίκτυο αντιμετωπίζει προκλήσεις όσον αφορά την ασφάλεια και το απόρρητο. Εδώ μπαίνει στο παιχνίδι η κβαντική τεχνολογία, προσφέροντας νέες δυνατότητες για την ανάπτυξη πιο ασφαλών και αποτελεσματικών κρυπτογραφικών συστημάτων. Τα κβαντικά δίκτυα έχουν αναδειχθεί ως μια αναπτυσσόμενη τεχνολογία στον τομέα αυτό, με τη δυνατότητα να φέρουν επανάσταση στον τρόπο με τον οποίο επικοινωνούμε και μεταφέρουμε πληροφορίες.

Η κβαντική δικτύωση είναι ένα πεδίο έρευνας που διερευνά τη χρήση κβαντικών συστημάτων για επικοινωνία και επεξεργασία πληροφοριών. Περιλαμβάνει τη χρήση κβαντικών bit ή qubits, τα οποία είναι τα θεμελιώδη δομικά στοιχεία του κβαντικού υπολογισμού, για τη μετάδοση και επεξεργασία πληροφοριών. Σε αντίθεση με τα κλασικά bit, τα qubits μπορούν να υπάρχουν σε πολλές καταστάσεις ταυτόχρονα, γεγονός που τα καθιστά πιο ευέλικτα και ισχυρά. Αυτή η ιδιότητα είναι γνωστή ως υπέρθεση και είναι ένα από τα βασικά χαρακτηριστικά των κβαντικών συστημάτων. Η ιστορία της κβαντικής δικτύωσης μπορεί να εντοπιστεί στις αρχές της δεκαετίας του 1980, όταν ο Richard

Feynman, πρότεινε για πρώτη φορά την ιδέα της χρήσης κβαντικών συστημάτων για υπολογιστές και επικοινωνία. Ωστόσο, μόλις τη δεκαετία του 1990 αναπτύχθηκαν τα πρώτα πρωτόκολλα διανομής κβαντικών κλειδιών (QKD), τα οποία επέτρεψαν την ασφαλή επικοινωνία μέσω ενός μη ασφαλούς καναλιού. Επίσης το 1994 ο μαθηματικός Peter Shor κατασκεύασε τον αλγόριθμο του Shor ο οποίος σχεδιάστηκε ώστε να παρέχει επιτάχυνση σε γνωστούς αλγορίθμους παραγοντοποίησης μεγάλων σύνθετων αριθμών και έχει ξεπεράσει τον αλγόριθμο RSA στην κρυπτογραφία όσο αφορά την ασφάλεια. Το 2004, επιτεύχθηκε η πρώτη επίδειξη κβαντικής τηλεμεταφοράς, η οποία περιελάμβανε τη μεταφορά κβαντικών πληροφοριών μεταξύ δύο qubits σε απόσταση 600 μέτρων [2]. Έκτοτε, η κβαντική δικτύωση έχει σημειώσει σημαντική πρόοδο, με την ανάπτυξη νέων πρωτοκόλλων, τεχνολογιών και εφαρμογών. Το 2012 ιδρύθηκε το πρώτο κβαντικό δίκτυο, που συνδέει τρεις κόμβους στις αυστριακές πόλεις της Βιέννης και του Ίνσμπρουκ. Αυτό το δίκτυο χρησιμοποίησε το QKD για να δημιουργήσει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των κόμβων και απέδειξε τη σκοπιμότητα της κβαντικής επικοινωνίας σε μεγάλες αποστάσεις. Το 2017, Κινέζοι ερευνητές ανακοίνωσαν τη δημιουργία του πρώτου κβαντικού δορυφόρου στον κόσμο, που ονομάζεται Micius [Εικόνα 4: Micius], ο οποίος είναι ικανός να μεταδίδει κβαντικές πληροφορίες σε απόσταση έως και 1.200 χιλιομέτρων [3]. Αυτή η ανακάλυψη άνοιξε νέες δυνατότητες για την ανάπτυξη ασφαλών κβαντικών δικτύων σε παγκόσμια κλίμακα, με τη δυνατότητα σύνδεσης ανθρώπων και συσκευών σε όλο τον κόσμο χρησιμοποιώντας κβαντική τεχνολογία.



Εικόνα 4: Δορυφόρος Micius

Σήμερα, τα κβαντικά δίκτυα και το διαδίκτυο βρίσκονται ακόμη στα αρχικά στάδια ανάπτυξης, αλλά οι πιθανές εφαρμογές είναι τεράστιες. Τα κβαντικά δίκτυα θα μπορούσαν να χρησιμοποιηθούν για την παροχή ασφαλούς επικοινωνίας για κυβερνητικές υπηρεσίες, χρηματοπιστωτικά ιδρύματα και άλλους οργανισμούς που απαιτούν υψηλά επίπεδα ασφάλειας.

Συμπερασματικά, η εξέλιξη και η ιστορία των κβαντικών δικτύων και του διαδικτύου είναι ένα συναρπαστικό θέμα, το οποίο υπογραμμίζει τις δυνατότητες της κβαντικής τεχνολογίας να φέρει επανάσταση στον τρόπο με τον οποίο επικοινωνούμε και μεταφέρουμε πληροφορίες. Ενώ υπάρχουν ακόμη πολλές προκλήσεις που πρέπει να ξεπεραστούν, η πρόοδος που έχει σημειωθεί μέχρι στιγμής είναι απόδειξη της ευρηματικότητας και της δημιουργικότητας των ερευνητών και επιστημόνων σε όλο τον κόσμο. Καθώς η κβαντική τεχνολογία συνεχίζει να αναπτύσσεται, μπορούμε να περιμένουμε να δούμε νέες εφαρμογές και δυνατότητες να αναδύονται, οι οποίες θα διαμορφώσουν το μέλλον του Διαδικτύου και του κόσμου μας.

Οι απαρχές της επιστήμης των υπολογιστών μπορούν να αναχθούν στους αρχαίους αλγόριθμους όπως ο Αλγόριθμος του Ευκλείδη (περίπου 300 π.Χ.) και οι πρώιμες βαβυλωνιακές σφηνοειδείς πινακίδες (περίπου 2000 - 1700 π.Χ.). Ωστόσο, η επίσημη διάκριση της επιστήμης των υπολογιστών από άλλες επιστήμες όπως τα μαθηματικά και η μηχανική γίνεται σαφέστερη τον 19ο αιώνα. Στις αρχές έως τα μέσα του 19ου αιώνα, ο Charles Babbage σχεδίασε προγραμματιζόμενες υπολογιστικές μηχανές, όπως η Difference Engine (1822) και η Analytical Engine. Η σύγχρονη επιστήμη των υπολογιστών λέγεται συχνά ότι ξεκίνησε το 1936 όταν ο Alan Turing εισήγαγε την έννοια του καθολικού υπολογιστή. Η ανάπτυξη των ηλεκτρονικών υπολογιστών τη δεκαετία του 1940, ιδιαίτερα με την αρχιτεκτονική Von Neumann, έθεσε τα θεμέλια για τη σύγχρονη πληροφορική. Οι εξελίξεις στα μέσα του 20ου αιώνα, συμπεριλαμβανομένης της εφεύρεσης του τρανζίστορ το 1947 και των ολοκληρωμένων κυκλωμάτων το 1959, σημείωσαν μια ταχεία αύξηση της υπολογιστικής ισχύος. Η περίφημη παρατήρηση του Gordon Moore το 1965, γνωστή ως νόμος του Moore, προέβλεψε διπλασιασμό της πολυπλοκότητας του επεξεργαστή κάθε 18 μήνες. Ωστόσο, αυτή η τάση δείχνει σημάδια επιβράδυνσης καθώς τα εξαρτήματα φτάνουν σε ατομικό μέγεθος. Κοιτάζοντας το μέλλον του κβαντικού υπολογισμού είναι λαμπρό, όπου τα κβαντικά αποτελέσματα θα μπορούσαν να αξιοποιηθούν

για σημαντικά πιο ισχυρές υπολογιστικές δυνατότητες. Καθώς τα εξαρτήματα πλησιάζουν τα ατομικά μεγέθη, ο κβαντικός υπολογισμός μπορεί να προσφέρει νέες ευκαιρίες για προόδους πέρα από τους περιορισμούς του κλασικού υπολογισμού [4].

2 ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

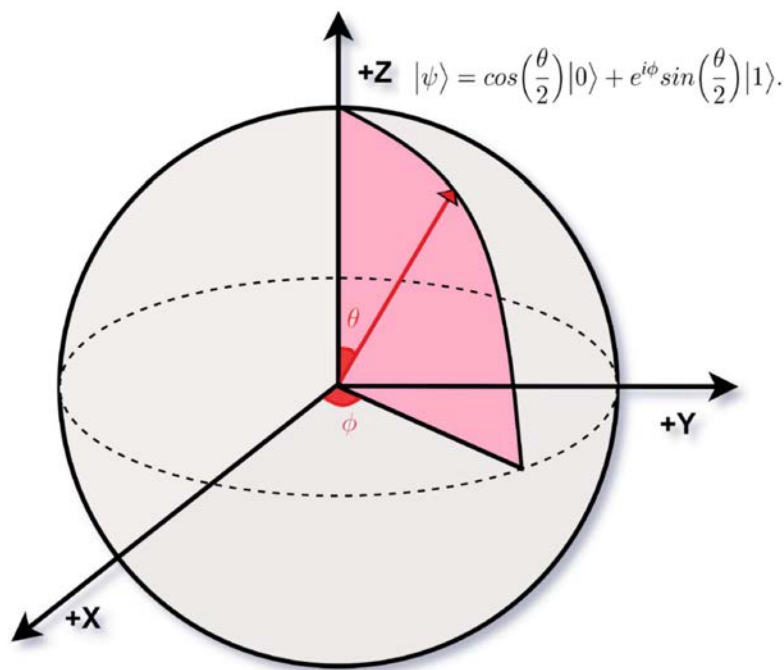
2.1 Κβαντική μηχανική

Η κβαντική μηχανική αυξάνεται σε σημαντικότητα στον σημερινό κόσμο καθώς πολλές εταιρίες κολοσσοί επενδύουν υπέρογκα ποσά για την έρευνα και ανάπτυξη νέων εφαρμογών πάνω στα κβαντικά συστήματα. Μερικά παραδείγματα είναι η κβαντική φυσική, η τεχνητή νοημοσύνη, εφαρμογές στην υγεία για ανάπτυξη εμβολίων ακόμη και στρατιωτικές εφαρμογές. Διατυπώνεται ως μαθηματικό πλαίσιο η σύνολο κανόνων για την ανάπτυξη φυσικών υποθέσεων εκμεταλλεύονται τις ιδιότητες της κβαντικής μηχανικής και δίνει την δυνατότητα ασφαλούς επικοινωνίας [5], μέσω κρυπτογράφησης One time Pad OTP [6].

2.1.1 Χώρος Καταστάσεων και Αρχή Υπερθέσης

Είναι ένα απομονωμένο ή κλειστό σύστημα με qubits το οποίο συσχετίζεται με το πολύπλοκο χώρο Hilbert, γνωστό και ως χώρος καταστάσεων του συστήματος. Ένα μοναδικό διάνυσμα περιγράφει πλήρως το διάνυσμα κατάστασης ενός συστήματος στον χώρο των καταστάσεων. Ένα qubit είναι το απλούστερο κβαντικό μηχανικό σύστημα που μπορεί να αναπαρασταθεί γεωμετρικά από μια σφαίρα Bloch [Εικόνα 5]. Κάθε καθαρή κβαντική κατάσταση $|\psi\rangle$ μπορεί να αναπαρασταθεί από ένα σημείο στην επιφάνεια της σφαίρας Bloch με σφαιρικές συντεταγμένες θ ως πολική γωνία, δηλαδή η γωνία που κάνει μια γραμμή με τον άξονα Z, και ϕ ως αζιμουθιακή γωνία, δηλαδή η γωνία που κάνει η γραμμή με τον άξονα X [60]: $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$ όπου " $|\cdot\rangle$ " ονομάζεται "κετ-διάνυσμα" στη σημειογραφία του Dirac, που αναπαριστά φυσικά την καθαρή κβαντική κατάσταση του qubit. Η γωνία ϕ αναπαριστά τη φάση μιας κβαντικής κατάστασης $|\psi\rangle$. Κάθε ξεχωριστή κατάσταση στη σφαίρα Bloch αναπαρίσταται από ένα δισδιάστατο (2D) διάνυσμα, όπου $|0\rangle$ και $|1\rangle$ είναι τα βασικά διανύσματά του που είναι ορθογώνια μεταξύ

τους. Οι καταστάσεις που μπορούν να αναπαρασταθούν από ένα "κετ-διάνυσμα" γνωρίζονται ως καθαρές κβαντικές καταστάσεις. Συγκριτικά, οι μικτές καταστάσεις είναι μείγματα καθαρών καταστάσεων, με αποτέλεσμα πιθανολογικά αποτελέσματα όταν μετρούνται. Είναι ένα σύστημα με αδύναμη κατάσταση ή την οποία η κατάσταση της δεν καθορίζεται πλήρως, γραμμένη με απειροελάχιστους διαφορετικούς τρόπους ως πιθανά αποτελέσματα καθορισμένων καθαρών καταστάσεων [7], [8]. Η καθαρή κατάσταση, που δίνεται στην εξίσωση (1), κατά τη μέτρηση οδηγεί σε είτε την κατάσταση $|0\rangle$ είτε την κατάσταση $|1\rangle$, όπως απεικονίζεται από την ερμηνεία της Κοπεγχάγης [9].



Εικόνα 5: Σφαίρα Bloch: Γεωμετρική αναπαράσταση της καθαρής κβαντικής κατάστασης του qubit. Κάθε κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ μπορεί να αναπαρασταθεί στην επιφάνεια της σφαίρας όπου $\alpha = \cos(\theta/2)$ και $\beta = e^{i\phi} \sin(\theta/2)$.

Ενώ στην κλασική επικοινωνία η μετάδοση πληροφοριών λαμβάνει χώρα σε μορφή bits που παίρνουν τιμή είτε "0" είτε "1", η κβαντική επικοινωνία χρησιμοποιεί qubits που μπορούν να βρίσκονται σε υπέρθεση των δύο βασικών καταστάσεων ταυτόχρονα παίρνοντας τις τιμές "0" και "1" [10]. Το αποτέλεσμα της μέτρησης τέτοιων καταστάσεων δεν είναι καθορισμένο $|0\rangle$ ή καθορισμένο $|1\rangle$. Η αρχή της υπέρθεσης κατανοείται καλύτερα με τον οπτικό προσδιορισμό της πολικότητας ενός φωτονίου. Στα 45 μοίρες πολικότητας, ένα φωτόνιο είναι ταυτόχρονα κάθετα και οριζόντια πολωμένο, αναπαριστώντας και τις

δύο καταστάσεις ταυτόχρονα [11]. Ένα διάσημο παράδειγμα σκέψης της αρχής της υπέρθεσης είναι το παράδειγμα της γάτας του Shrödinger, όπου η γάτα, όπως ερμηνεύεται συνήθως, είναι ταυτόχρονα νεκρή και ζωντανή ως αποτέλεσμα τυχαίου γεγονότος που μπορεί ή δεν μπορεί να συμβεί.

2.1.2 Single Qubit System

Στην κλασσική επικοινωνία η πληροφορία κωδικοποιείται σε μορφή δυαδικού συστήματος. Το bit αναπαριστά τις πιθανές τιμές $|1\rangle$ ή $|0\rangle$. Αντίθετα στην κβαντική επικοινωνία χρησιμοποιούνται τα qubits όπου οι πιθανές τιμές των φωτονίων μπορεί να είναι 0 και 1 ταυτόχρονα καθώς βασίζεται στο two way qubit system. Η πόλωση του φωτονίου μπορεί να έχει σπιν πάνω ή κάτω και βρίσκεται είτε σε υπέρθεση είτε σε θέση βάσης. Ρίχνοντας δεσμίδες φωτός σε ένα ηλεκτρόνιο που συμβολίζεται με $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ μπορούμε να επηρεάσουμε το αποτέλεσμα της μέτρησής του δηλαδή από $|0\rangle$ και $|1\rangle$ να γίνει $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ σε κατάσταση υπέρθεσης. Οι μεταβλητές α και β είναι πολύπλοκοι αριθμοί που αναπαριστούν πιθανότητες, δηλαδή $|\alpha|^2$ είναι η πιθανότητα να λάβουμε $|\psi\rangle = 0$ ως αποτέλεσμα της μέτρησης στο qubit $|\psi\rangle$, και $|\beta|^2$ είναι η πιθανότητα να λάβουμε $|\psi\rangle = 1$ ως αποτέλεσμα της μέτρησης στο qubit $|\psi\rangle$. Πρέπει να ικανοποιείται η συνθήκη: $|\alpha|^2 + |\beta|^2 = 1$. Ένα κλασσικό bit είναι σαν ένα νόμισμα που οδηγεί σε συγκεκριμένα αποτελέσματα κορώνας ή γράμματος. Υποθέτοντας ένα qubit με $\alpha = \beta = \sqrt{1/2}$, θα βρίσκεται στην κατάσταση: $|\pm\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Αυτό δίνει αποτέλεσμα 0 με πιθανότητα 0,5 και αποτέλεσμα 1 με πιθανότητα 0,5, όταν μετριέται κατά τη διάρκεια της πάροδου του χρόνου. Αυτή η κατάσταση συχνά παίζει έναν ζωτικό ρόλο στην κβαντική επικοινωνία και συμβολίζεται ως $|+\rangle$ και $|-\rangle$. Παρόλο που το qubit έχει θεωρητικά τη δυνατότητα να μεταφέρει άπειρη πληροφορία, όλες οι κβαντικές καταστάσεις καταρρέουν σε μια μόνο κατάσταση 0 και 1 κατά τη μέτρηση, και ο λόγος για αυτό το χαρακτηριστικό είναι ακόμα άγνωστο.

2.1.3 Multiple qubits

Ένα διπλό σύστημα qubit παρουσιάζει τέσσερις υπολογιστικές βασικές καταστάσεις που συμβολίζονται ως $|00\rangle$, $|01\rangle$, $|10\rangle$ και $|11\rangle$. Η κβαντική κατάσταση για ένα ζεύγος qubits αναπαρίσταται από διανύσματα κατάστασης με τους αντίστοιχους συντελεστές ως:

$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. Όπως και στις συνθήκες που συζητήθηκαν για ένα μοναδικό qubit, τα αποτελέσματα της μέτρησης της εξίσωσης συμβαίνουν με πιθανότητες α_{00}^2 για $|00\rangle$, α_{01}^2 για $|01\rangle$, α_{10}^2 για $|10\rangle$ και α_{11}^2 για $|11\rangle$. Αν $x = 00, 01, 10$ ή 11 , η συνθήκη κανονικοποίησης δίνεται από τη σχέση $\sum_x |\alpha_x|^2 = 1$. Επομένως, είναι εμφανές ότι με την ενσωμάτωση πολλαπλών qubits, οι υπολογιστικές βασικές καταστάσεις αυξάνονται εκθετικά, παρέχοντας τη δυνατότητα για πολύπλοκους υπολογισμούς που ήταν προηγουμένως αδύνατοι με τους κλασικούς πόρους.

2.1.4 Bell States ή EPR

Ο όρος "EPR" προέρχεται από το παράδοξο που παρουσιάζουν οι Αϊνστάιν, Ποντόλσκι και Ρόζεν στο περίφημο άρθρο τους "Μπορεί μια κβαντομηχανική περιγραφή της φυσικής πραγματικότητας να θεωρηθεί ολοκληρωμένη;" [12]. Αυτό το παράδοξο ανέδειξε τις αντιφατικές ιδιότητες των καταστάσεων Bell. Σε ένα διπλό κβαντομηχανικό σύστημα, οι καταστάσεις Bell εκφράζονται μαθηματικά ως:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

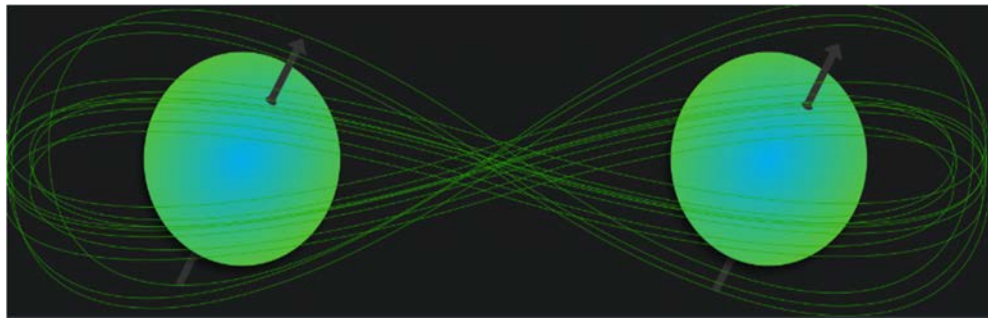
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Τα δύο σωματίδια σε αυτές τις καταστάσεις Bell ονομάζονται ζεύγη EPR και είναι υπεύθυνα για τη δημιουργία και διανομή της εμπλοκής, ειδικά στην περίπτωση της κβαντικής τηλεμεταφοράς, που είναι η κύρια λειτουργία της Κβαντικής Πληροφορίας. Τα ζεύγη EPR δημιουργούνται με διάφορες μεθόδους και αποστέλλονται στην Alice και Bob. Σε αυτή τη διάταξη, οποιαδήποτε μέτρηση στο

qubit της Alice θα δώσει το ίδιο αποτέλεσμα με μια μέτρηση στο qubit του Bob, καθιστώντας δικαιολογημένη την κοινή τους εμπλοκή μέσα στο ζεύγος EPR.

Μια κατάσταση Bell έχει το χαρακτηριστικό ότι, όταν μετριέται η κατάσταση του πρώτου qubit, έχουμε δύο δυνατά αποτελέσματα: 0 με πιθανότητα 1/2 και 1 με πιθανότητα 1/2, οδηγώντας σε καταστάσεις μετά τη μέτρηση $|00\rangle$ και $|11\rangle$, αντίστοιχα. Συνεπώς, αν μετρηθεί το δεύτερο qubit, θα έχουμε το ίδιο αποτέλεσμα με το πρώτο qubit. Αυτό εξηγεί την ενδιαφέρουσα συσχέτιση μεταξύ αυτών των δύο qubits. Ακόμα και εάν εφαρμοστούν κάποιες τοπικές λειτουργίες στο πρώτο ή το δεύτερο qubit, αυτές οι συσχετίσεις εξακολουθούν να υπάρχουν λόγω της εμπλοκής.

Ο John Bell επέκτεινε περαιτέρω το παράδοξο του EPR στο [13], δηλώνοντας ότι οι συσχετίσεις μέτρησης στην κατάσταση Bell είναι πολύ ισχυρότερες από οτιδήποτε εφικτό σε κλασικά συστήματα. Αυτό επιτρέπει την επεξεργασία πληροφοριών που πηγαίνει πολύ πέρα από όσα είναι δυνατά στον κλασικό κόσμο [Εικόνα 6].



Εικόνα 6: Εμπλοκή: Δύο σωματίδια A και B είναι συσχετισμένα μεταξύ τους, ακόμα και αν βρίσκονται σε μεγάλη απόσταση μεταξύ τους. Εάν γίνει οποιαδήποτε μέτρηση στο A με σπιν +45, τότε το ίδιο αποτέλεσμα αντανakλάται και στο B. Αυτό συμβαίνει λόγω του παράξοχου φαινομένου της κβαντικής εμπλοκής.

2.1.5 Κβαντική Εμπλοκή

Όπως φαίνεται στην [Εικόνα 6], είναι το φαινόμενο της συσχέτισης μεταξύ δύο ζευγαριών qubits, ακόμα και όταν αυτά είναι απομακρυσμένα μεταξύ τους. Σε αυτή τη συγκυρία, οποιαδήποτε τυχαία μέτρηση σε εμπλεκόμενα qubits θα δώσει

το ίδιο σύνολο τυχαίων αποτελεσμάτων [14]. Η έννοια της κβαντικής εμπλοκής, που υπαγορεύεται από τους νόμους της κβαντικής μηχανικής, αποτελεί βασική λειτουργικότητα για διάφορες εφαρμογές και δεν έχει αντίστοιχο στην κλασική επικοινωνία. Όπως συζητήθηκε προηγουμένως ένα ζεύγος EPR είναι ένα μέγιστα εμπλεκόμενο ζεύγος qubits που βρίσκονται σε υπερθέση. Η ανεξάρτητη μέτρηση αυτών των qubits οδηγεί σε τυχαία κατανομή του "1" και "0" με ίση πιθανότητα. Αυτό σημαίνει ότι η κατάσταση των εμπλεκόμενων qubits διαμορφώνεται αμέσως όταν το άλλο ζεύγος ενός εμπλεκόμενου qubit μετρηθεί. Η εμπλοκή δεν επιτρέπει καμία ανταλλαγή πληροφοριών μεταξύ απομακρυσμένων κόμβων, αντίθετα επιτρέπει μόνο την απόκτηση κοινών πληροφοριών. Για την ανταλλαγή πληροφοριών, τα qubits μπορούν να μεταδοθούν ανάμεσα σε απομακρυσμένους κόμβους χωρίς πραγματικά να τα στείλουμε από την πηγή στον προορισμό με το φαινόμενο της κβαντικής τηλεμεταφοράς [15], [16], το οποίο είναι θεμελιώδες για τα κβαντικά δίκτυα [17]. Μια άγνωστη κβαντική κατάσταση μπορεί επίσης να μεταδοθεί μέσω τηλεμεταφοράς από την πηγή στον προορισμό σε μεγάλες αποστάσεις με τη βοήθεια ζευγών EPR και τοπικών λειτουργιών.

Η έννοια της εμπλοκής αναγνωρίστηκε πρώτα από τον Einstein κ.ά. το 1935 [18] και το φαινόμενο της εμπλοκής προήλθε αρχικά από τον Schrödinger την ίδια χρονιά [19]. Επίσης, αποκαλείται ως "τρομακτική δράση σε απόσταση" από τον Einstein. Στη συνέχεια, ο Bohm έψαξε τα δύο κβαντικά σωματίδια που ήταν εμπλεκόμενα μεταξύ τους, τα οποία τώρα αποκαλούνται qubits [20]. Στη συνέχεια, ο Bell συνέχισε την έρευνά του [21] διατύπωσε ένα θεώρημα για το πειραματικό έλεγχο της ερώτησης για την τοπικότητα και την πραγματικότητα της εμπλοκής. Αυτή η εξέλιξη ενέπνευσε διάφορους ερευνητές να δημιουργήσουν εμπλεκόμενα σωματίδια στα εργαστήρια [22], [23], [24]. Μια σειρά από πειράματα που πραγματοποιήθηκαν το 2015 κάλυψαν όλες τις πειραματικές παραλείψεις που υπήρχαν προηγουμένως [25], [26], [27]. Η χρήση της εμπλοκής για επικοινωνία σε τεχνικές εφαρμογές δεν είναι σαφής, διότι η εμπλοκή αυτή καθαυτή δεν επιτρέπει τη μετάδοση πληροφοριών. Ωστόσο, μπορεί να βοηθήσει στη δημιουργία ενός εικονικού ασφαλούς καναλιού ή ενός κρυπτογραφικού καναλιού [28]. Συστήματα με πολλαπλά σωματίδια αναπαρίστανται από τον 2-διάστατο χώρο καταστάσεων. Παρατηρείται ότι, με την προσθήκη ενός μόνο qubit, οι υπολογιστικές βάσεις αυξάνονται εκθετικά, προσφέροντας χώρο για πολύπλοκους υπολογισμούς που εί-

ναι αδύνατοι στα κλασικά συστήματα επικοινωνίας. Ένα τέτοιο σύστημα περιγράφεται από το θεώρημα Greenberger–Horne–Zeilinger (GHZ) [29], το οποίο διαφέρει από το θεώρημα του Bell [30] όσον αφορά την καθοριστική φύση των προβλεπόμενων αποτελεσμάτων. Η εφαρμογή του θεωρήματος GHZ είναι ότι η πολλαπλή εμπλοκή σωματιδίων μπορεί να χρησιμοποιηθεί για την Κβαντική Διόρθωση Σφαλμάτων (QEC) [31]. Με αυτούς τους τρόπους αναπτύσσονται και αποδεικνύονται πλεονεκτήματα υψηλής διάστασης μπλεγμένων ζευγών EPR στη θεωρία της κβαντικής [32].

2.2 ΚΒΑΝΤΙΚΟ ΔΙΚΤΥΟ

2.2.1 Κβαντικές πύλες

Οι κβαντικές πύλες επιδρούν σε καταχωρητές που περιέχουν ένα ή και περισσότερα qubits (ή κβαντικές καταστάσεις). Καταχωρητές + Πύλες = Κβαντικά Κυκλώματα

Πύλες: • Hadamard (πύλη υπέρθεσης – super position)

• Identity (πύλη αδράνειας – identity gate)

• x (πύλη αντιστροφής)

Πύλη αδράνειας I

Επιδρά σε ένα qubit χωρίς να το επηρεάζει και συμβολίζεται ως: $I = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$

• Qiskit: qc.i(#n) όπου qc το όνομα της μεταβλητής που υποδηλώνει το κβαντικό κύκλωμα και #n είναι ο αριθμός του qubit που θέλουμε να επιδράσει η πύλη.

• Όταν μία πύλη(ες) επιδρά σε qubit(s) μαθηματικά το λύνουμε με το κλασσικό γινόμενο πινάκων (πάντα Πύλες x Κβαντική κατάσταση).

$$I |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1x1 + 0x0 \\ 0x1 + 1x0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$I |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1x0 + 0x1 \\ 0x0 + 1x1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$I |x\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1xa + 0xb \\ 0xb + 1xb \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = |x\rangle$$

Πύλη Hadamard H

Συμβολίζεται ως:

Το $H|0\rangle$, είναι το αποτέλεσμα της δράσης της πύλης αυτής σε εάν qubit που βρίσκεται στην κατάσταση $|0\rangle$ και $|1\rangle$ αντίστοιχα: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

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

$$H|x\rangle \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix} = \frac{1}{\sqrt{2}} ((a+b)|0\rangle + (a-b)|1\rangle)$$

Είναι αποδεκτή η κατάσταση διότι:

$$\left(\frac{1}{\sqrt{2}}\right)^2 [(a+b)^2 + (a-b)^2] = \frac{1}{2} (a^2 + b^2 + 2ab + a^2 + b^2 - 2ab) = \frac{1}{2} [2(a^2 + b^2)] = a^2 + b^2 = 1$$

Όταν ένα qubit βρίσκεται είτε στην κατάσταση που δίνεται από $H|0\rangle$ είτε στην κατάσταση που δίνεται από την $H|1\rangle$, η πιθανότητα να μετρήσουμε και να το βρούμε στην βασική κατάσταση 0 είναι ίση με την πιθανότητα να το βρούμε στην βασική κατάσταση 1. Φυσικά και οι δύο πιθανότητες είναι ίσες με 0,5.

Πύλη X

Λειτουργεί σαν την NOT σε κλασσικούς υπολογιστές και συμβολίζεται ως:

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

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

$$X|x\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0xa + 1xb \\ 1xa + 0xb \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$$

Παραδείγματα

Διαδοχική εφαρμογή πύλης Hadamard και X σε ένα καταχωρητή ενός qubit:

$$|0\rangle \rightarrow H \rightarrow X$$

$$|0\rangle \rightarrow H = H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |\psi\rangle$$

$$|\psi\rangle \rightarrow X = X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Εφαρμογή διαδοχικών πυλών Hadamard

Όταν εφαρμόζονται δύο διαδοχικές πύλες Hadamard αλληλοαναιρούνται και οδηγούν σε αβεβαιότητα, $H \rightarrow H \rightarrow |x\rangle = |x\rangle$

$$H|x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix}$$

$$H \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} a+b \\ a-b \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2a \\ 2b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = |x\rangle$$

Κβαντικές πύλες Pauli

Μία πολύ σημαντική ομάδα κβαντικών πυλών που δρουν σε ένα qubit είναι οι κβαντικές πύλες Pauli. Αυτές οι κβαντικές πύλες είναι σημαντικές διότι κάθε δυνατή κβαντική πύλη του ενός qubit μπορεί να συντεθεί από έναν γραμμικό συνδυασμό των πυλών Pauli και της πύλης αδράνειας. Δηλαδή, με τις πύλες αυτές μπορούμε να εκτελέσουμε όλες τις περιστροφές του διανύσματος κατάστασης ενός qubit στη σφαίρα Bloch. Οι κβαντικές πύλες Pauli συμβολίζονται με τα γράμματα X, Y και Z. Οι πύλες Pauli περιγράφονται αντίστοιχα από τους τελεστές X, Y και Z στους οποίους αντιστοιχούν οι παρακάτω πίνακες:

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

Η δράση της πύλης X σε ένα qubit είναι:

$$X|q_I\rangle = X(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle = |q_O\rangle$$

Η δράση της πύλης Y σε ένα qubit είναι:

$$Y|q_I\rangle = Y(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix} = -ib|0\rangle + ia|1\rangle = |q_O\rangle$$

Η δράση της πύλης Z σε ένα qubit είναι:

$$Z|q_I\rangle = Z(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle = |q_O\rangle$$

Οι ιδιότητες των κβαντικών πυλών Pauli φαίνονται συνοπτικά στον Πίνακα 3-4.

Πύλη πολλαπλών qubit CNOT

Στην πράξη, περισσότερα από ένα qubits εμπλέκονται στις υπολογιστικές διαδικασίες. Επομένως, η μελέτη των χειρισμών πάνω σε πολλαπλά qubits είναι σημαντική για την κατανόηση των ενδιαφερουσών πτυχών. Ένα πύλη ελέγχου-NOT (CNOT) είναι η ευρέως χρησιμοποιούμενη πύλη λογικής πολλαπλών, η οποία έχει το qubit-στόχο και το qubit ελέγχου ως τις εισόδους της πύλης CNOT. Εάν το qubit ελέγχου είναι 1, τότε το qubit-στόχο αντιστρέφεται στην έξοδο· εάν το qubit ελέγχου είναι 0, τότε το qubit-στόχο διατηρεί την αρχική του κατάσταση και συμβολίζεται με :

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

2.2.2 Κβαντικά πρωτόκολλα δικτύου

Κβαντική Διανομή κλειδιού (Quantum Key Distribution QKD)

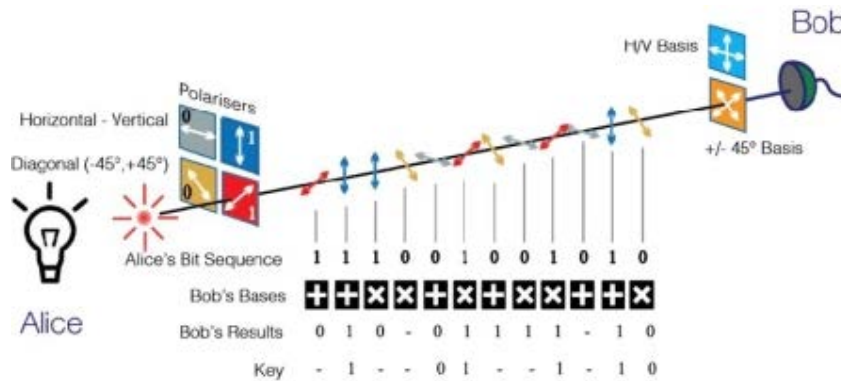
Σε κάθε τομέα της εποχής μας είτε είναι στρατιωτικές εφαρμογές, οικονομικές, ιδιωτικές εταιρίες, κρατικοί φορείς όλοι βασίζονται σε ένα δίκτυο για την διεκπεραίωση των καθημερινών τους εργασιών και την κοινή χρήση giga bytes δεδομένων. Η ασφάλεια είναι προτέρημα καθώς οποιασδήποτε μορφής επίθεσης λογοκλοπής είναι πιθανή σε ιδιωτικά

η σε δημοσιά κανάλια δικτύου. Τα συστήματα ασφαλείας χρησιμοποιούν κλασικά κρυπτογραφικά πρωτόκολλα για την ασφάλεια του απορρήτου βασίζονται στην επίλυση δύσκολων μαθηματικών προβλημάτων όπως η παραγοντοποίηση, λογάριθμοι δυσχαιρένοντας την προσπάθεια των κακόβουλων χρηστών (χάκερ) να υποκλέψουν στοιχεία διότι αφού η υπολογιστική ισχύ είναι ανεπαρκής ώστε να επιλύσει τα προβλήματα αυτά. Η κρυπτογραφία χωρίζεται σε συμμετρική, ασύμμετρη και υβριδική όπου μερικά κλειδιά χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Εάν χρησιμοποιείται το ίδιο κλειδί για τα δύο προαναφερθέντα τότε το σύστημα είναι γνωστό ως ιδιωτικό κλειδί κρυπτοσυστήματος. Από την άλλη το δημόσιο κλειδί κρυπτοσυστήματος χρησιμοποιεί δημόσιο κλειδί για την κρυπτογράφηση ιδιωτικό κλειδί για αποκρυπτογράφηση [33], [34]. Η ιδέα του δημοσίου κλειδιού προήλθε από τν Diffie and Hellman το 1976 [35]. Η πρώτη εφαρμογή έγινε από τους Rivest, Shamir, Adleman (RSA) το 1978 [36].

Δεδομένου ότι τα κρυπτοσυστήματα δημόσιου κλειδιού είναι αργά, χρησιμοποιούνται συστήματα που συνδυάζουν ιδιωτικό και δημόσιο κλειδί τα οποία προσφέρουν σημαντικά πλεονεκτήματα ταχύτητας [37]. Σε κρυπτοσυστήματα δημόσιου κλειδιού, χωρίς να γνωρίζουν το μυστικό κλειδί ένα μήνυμα δεν μπορεί να αποκωδικοποιηθεί, ενισχύοντας έτσι την ασφάλεια των συστημάτων. Δυστυχώς, τα κρυπτοσυστήματα ιδιωτικού κλειδιού υποφέρουν από πρόβλημα διανομής με ασφαλή τρόπο. Το QKD παρέχει εξαιρετική ασφάλεια έναντι των χάκερς και παρέχει λύσεις σε βασικά προβλήματα διανομής χρησιμοποιώντας κβαντική κρυπτογραφία [38] με τους ακόλουθους στόχους.

- Αρχικά, ο αποστολέας Alice και Bob μοιράζονται ένα μυστικό/ιδιωτικό κλειδί μεταξύ τους, χωρίς η Eve να το γνωρίζει.
- Στη συνέχεια, αυτό το κλειδί διανέμεται από την Alice στον Bob μέσω ενός ασφαλές κβαντικού καναλιού. Η ασφάλεια αυτού του κλειδιού εξαρτάται από το γεγονός ότι οποιαδήποτε απόπειρα υποκλοπής ή κατασκοπείας από την Eve θα διαταράξει την κατάσταση των βασικών qubits, εκθέτοντας έτσι την προσπάθειά του/της. Ως εκ τούτου, είναι αδύνατο η Eve να αντιγράψει τις πληροφορίες χωρίς να εντοπιστεί.
- Η Alice και ο Bob πρέπει να είναι σε θέση να πιστοποιήσουν την αυθεντικότητα του μηνύματος, προκειμένου να αποτραπεί η κλοπή του από την Eve πέρνοντας έτσι την θέση της Alice είτε του Bob. Αυτή η εργασία μπορεί να είναι επιτευχθεί με κβαντικά πρωτόκολλα ελέγχου ταυτότητας όπως [39], [40], [41]. Εάν αυτό το

επίπεδο ελέγχου ταυτότητας (αυθεντικότητας) μπορεί να επιτευχθεί, το QKD μπορεί να παρέχει αποδεδειγμένη ασφάλεια έναντι σε απεριόριστες επιθέσεις, κάτι το οποίο είναι σχεδόν αδύνατο με τα κλασικά κρυπτογραφικά πρωτόκολλα ανταλλαγής κλειδιών [Εικόνα 7].



Εικόνα 7: Αναπαράσταση του πρωτοκόλλου QKD

Βήματα για την πραγματοποίηση του QKD

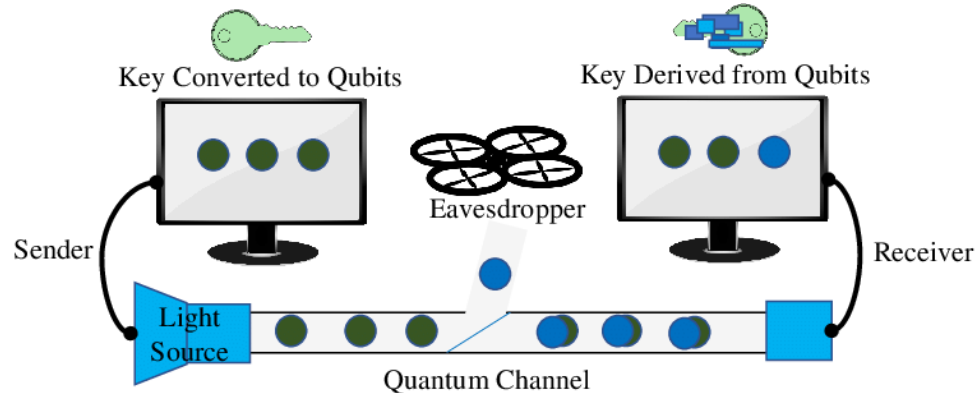
- 1) Key Protocols : Για την ασφάλεια και την ακεραιότητα των δεδομένων, τα σύστημα τα qkd λειτουργούν σε δύο στάδια. Στο πρώτο στάδιο παράγεται τυχαία ακολουθία bit γνωστή ως κλειδί η οποία μπορεί να είναι αποτέλεσμα ορισμένης δυαδικής λειτουργίας που εκτελείται στα δεδομένα ώστε να μεταδοθεί.
- 2) Στο δεύτερο στάδιο, το παραγόμενο κβαντικό κλειδί αποστέλλεται στον προορισμό με ασφαλή τόπο σε σχέση με το κλασικό κανάλι το οποίο μπορεί να αποκωδικοποιηθεί χρησιμοποιώντας το ίδιο ιδιωτικό κλειδί.
- 3) Ένα κρυπτογραφικό πρωτόκολλο που χρησιμοποιείται στα κλασικά συστήματα είναι το OTP, το οποίο έχει αποδειχθεί ότι είναι ασφαλές στην κβαντική τεχνολογία [42]. Κανένας αλγόριθμος δεν θα είναι σε θέση να αποκτήσει το κλειδί που παράγεται κβαντικά τυχαία. Μερικά από τα πρωτόκολλα είναι:

Πρωτόκολλο OTP

Το OTP είναι από τις πιο παλιές κλασικές κρυπτογραφικές μεθόδους από το 1882 και εφευρεθεί από τον Frank Miller [43]. Είναι απλό αλλά αποτελεσματικό κρυπτοσύστημα ιδιωτικού κλειδιού. Η ασφάλεια του OTP δεν μπορεί να παραβιαστεί

χωρίς την γνώση του κοινόχρηστου κλειδιού γι' αυτό και το ξέρουν μόνο η Alice και ο Bob (ιδιωτικό κλειδί). Εάν η πληροφορία υποκλαπεί από την Eve, τότε η Alice και ο Bob θα μάθουν για την κατασκοπεία αυτή ως αποτέλεσμα οι πληροφορίες που θα παραχθούν να είναι άκυρες. Τα δεδομένα είναι κρυπτογραφημένα από μια δυαδική λειτουργία σε δεδομένα και κλειδιά bits. Τα αποτελέσματα αυτής της λειτουργίας στέλνονται στον Bob, ο οποίος με την σειρά του αποκωδικοποιεί την πληροφορία χρησιμοποιώντας την ίδια δυαδική λειτουργία στα ληφθέντα δεδομένα bits, αποκτώντας έτσι την πρωτότυπη πληροφορία με την βοήθεια ενός κοινόχρηστου κλειδιού έχοντας τα ακόλουθα χαρακτηριστικά:

- 1) Το κλειδί που δημιουργείται πρέπει να χρησιμοποιείται μόνο μια φορά. Δεν μπορεί να επαναχρησιμοποιείται να είναι στην αρχική του μορφή. Ακόμη και ένα μέρος αυτού του κλειδιού δεν θα πρέπει να επαναχρησιμοποιηθεί διότι θέτει σε κίνδυνο την ασφάλεια του συστήματος.
- 2) Το μήκος του κλειδιού πρέπει να είναι τουλάχιστον όσο τα δεδομένα που θα σταλούν, έτσι ώστε ακόμα κι αν η Eve επιτεθεί στο κανάλι δεν τα καταφέρνει.
- 3) Το κλειδί πρέπει να μοιραστεί με την Alice και τον Bob με μυστικό τρόπο έτσι ώστε μόνο οι δύο τους να έχουν στην κατοχή τους το κλειδί αυτό.



Εικόνα 8: OTP

Δεδομένου ότι το OTP [Εικόνα 8], απαιτεί το μήκος του κλειδιού να είναι στο τουλάχιστον όσο ο όγκος των δεδομένων που πρέπει να μεταδοθούν καθίσταται μη πρακτικό για να χρησιμοποιηθεί σε αρκετές περιπτώσεις. Ως εκ τούτου, υπάρχει ανάγκη εξερεύνησης και εκμετάλλευσης της ιδιοκτησίας της εμπλοκής, για τη δημιουργία κβαντικής κρυπτογράφησης vernam cipher [44] και άλλα πρωτόκολλα για την ενίσχυση της ασφάλειας [45].

Πρωτόκολλο BB84

Αυτό το πρωτόκολλο είναι από τις πιο δημοφιλής μεθόδους που χρησιμοποιούνται στην κβαντική κρυπτογραφία. Εφευρέθηκε από δύο φυσικούς τους Charles H. Bennett και Gilles Brassard, στην IBM το 1984 [46]. Μέσω μιας πρωτότυπης ιδέας του Wiesner το 1970 αλλά η έρευνα του δεν μπόρεσε να δημοσιευθεί την ίδια χρονιά το 1983 [47]. Σε αυτό το πρωτόκολλο τα φωτόνια που μεταφέρουν qubits αποστέλλονται στον Bob, ο οποίος πραγματοποιεί μέτρηση στα φωτόνια που λαμβάνει. Μερικά από τα φωτόνια αυτά χάνονται λόγω αποσύνδεσης μερικά φτάνουν και άλλα χάνονται.

Basis		0	1		
		$\oplus$	$\uparrow$	$\rightarrow$	Horizontal/Vertical basis
		$\otimes$	$\nearrow$	$\searrow$	Diagonal basis

Data bits of Alice	0	1	0	0	1	0	1	1	0	0	1	1	1	0
Assigned basis	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Alice's photon polarization	$\uparrow$	$\searrow$	$\nearrow$	$\uparrow$	$\searrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\nearrow$
Bob's random basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$
Bob's photon polarization	$\rightarrow$	$\searrow$	$\uparrow$	$\searrow$	$\searrow$	$\uparrow$	$\rightarrow$	$\uparrow$	$\searrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\rightarrow$
Bob's receiving bits	1	1	0	1	1	0	1	0	1	0	0	0	1	1
Alice and Bob then reveal their basis to each other over an authenticated public channel.														
Sifted Key		1			1	0				0			1	

11001

Εικόνα 9: Πρωτόκολλο BB84

Από όλα τα φωτόνια που ανιχνεύονται μερικά από τα bits έχουν την μορφή κλειδιού και τα υπόλοιπα θα γίνουν αντιληπτά από την Eve και θα πάρει όλες τις πληροφορίες που χρειάζεται ώστε να ολοκληρώσει τον σκοπό της δηλαδή την κατασκοπεία. Η Alice κωδικοποιεί την πληροφορία η οποία είναι κοινόχρηστη μόνο με τον Bob. Εάν αυτή η πληροφορία αποκωδικοποιείται χρησιμοποιώντας διαφορετική βάση από αυτή της Alice τότε η μέτρηση θα διαταράξει την κατάσταση των φωτονίων ου φέρουν τα qubits. Σε αυτήν την περίπτωση η Eve θα μετρήσει την πληροφορία με διαφορετική βάση η οποία αλλάζει την κατάσταση των qubits, αποκαλύπτοντας έτσι την κατάσταση του, με τον Bob να απορρίπτει αυτά τα bits. Το πρωτόκολλο BB84 είναι βασισμένο στην επικοινωνία σειρών από qubits τα οποία στέλνονται από την Alice στον Bob και αποθηκεύονται στα

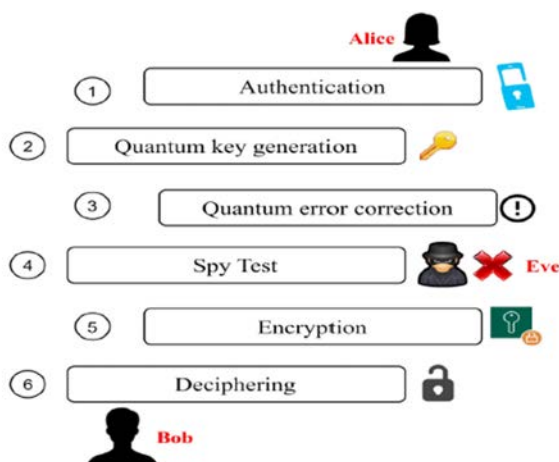
φωτόνια που αντιπροσωπεύονται από τις καταστάσεις πόλωσης. Συνήθως η επικοινωνία μεταξύ της Alice και του Bob γίνεται μέσω των κβαντικών καναλιών αλλά το πιο διαδεδομένο είναι οι οπτικές ίνες. Η Alice μπορεί να χρησιμοποιήσει κάθετη ή οριζόντια ή διαγώνια βάση πόλωσης για κωδικοποίηση των πληροφοριών, π.χ., $|\uparrow\rangle$ για κάθετη βάση, $|\rightarrow\rangle$ για οριζόντια βάση, για διαγώνια βάση. Οι καταστάσεις $|\uparrow\rangle = |0\rangle$ και $|\rightarrow\rangle = |1\rangle$ να αντιπροσωπεύονται από $\oplus$. Οι καταστάσεις $|\downarrow\rangle = |0\rangle$ και $|\leftarrow\rangle = |1\rangle$ αντιπροσωπεύονται από $\otimes$. Το πρωτόκολλο εκτελείται ως εξής:

- 1) Οι κβαντικές καταστάσεις κωδικοποιούνται χρησιμοποιώντας τα δεδομένα των bits της Alice με την βάση $\oplus$ and $\otimes$ και τυχαίων κλασικών bit 0 ή 1. Η Alice στέλνει την κωδικοποιημένη κβαντική κατάσταση στον Bob μέσω κάποιου καναλιού το οποίο συνήθως είναι ευάλωτο σε επιθέσεις από την Eve. Τα κωδικοποιημένα δεδομένα είναι σε μορφή $m|\uparrow\rangle, |\rightarrow\rangle$.
- 2) Στη συνέχεια, ο Bob χρησιμοποιεί μια τυχαία βάση για τη μέτρηση των qubits που λαμβάνονται με βάση $\oplus$ και $\otimes$ όπως φαίνεται στην [Εικόνα 9]. Αυτή είναι η τελευταία κβαντική πράξη που πραγματοποιήθηκε σε αυτό το πρωτόκολλο.
- 3) Ο Μπομπ τότε αναγνωρίζει στην Αλίκη τα qubits που έχει λάβει μέσω δημόσιου καναλιού.
- 4) Η Alice και ο Bob αποκαλύπτουν τη βάση που χρησιμοποιήθηκε για την κωδικοποίηση του qubit δεδομένων μέσω ενός δημόσιου καναλιού. Όταν επιλέγουν και οι δύο την ίδια βάση, τα αντίστοιχα μετρούμενα bit διατηρούνται και αυτά τα δεδομένα θα αποτελέσουν το κλειδί. Αν επιλέξουν μια διαφορετική βάση τότε τα bit θα απορριφθούν και αυτή η διαδικασία είναι γνωστή ως sifting.
- 5) Στη συνέχεια, η παρουσία της Eve ελέγχεται με την αποκάλυψη ένας τυχαίου αριθμού bit που κωδικοποιείται από την Alice. Αν τα bits που ανιχνεύονται από τον Bob είναι τα ίδια, τότε δεν υπάρχουν παρεμβολές από την Eve και τα υπόλοιπα bit χωρίς σφάλματα ονομάζονται κλειδιά κρυπτογράφησης.

Πρωτόκολλο Ekert

Αυτό το πρωτόκολλο λαμβάνει υπόψη την εμπλοκή φωτονίων που φέρουν qubits, προτάθηκε το 1991 από τον Artur Ekert [28]. Η πρώτη εφαρμογή αυτού του πρωτοκόλλου

επιτεύχθηκε από τον Anton Zeilinger και η ομάδα του το 1999 σε μικρή απόσταση 360 m [48]. Από την ίδια ομάδα, η πρώτη μεταφορά χρημάτων μέσω κβαντικής κρυπτογραφίας επιδείχθηκε το 2004 [49]. Αυτό το πρωτόκολλο εκτελείται σε 6 βήματα όπως φαίνεται παρακάτω στην [Εικόνα 10].



Εικόνα 10: 6 βήματα της διαπλοκής του πρωτοκόλλου Ekert

- 1) Πρώτα, πρέπει να ρυθμιστεί ένα πιστοποιημένο κανάλι, που μπορεί να είναι κλασικής ή κβαντικής φύσης, μεταξύ της Αλίκης και του Bob και πρέπει να σιγουρευτούν δεν υπάρχει περίπτωση η Eve να πάρει θέση ένας από αυτούς. Αυτό το κανάλι είναι ανοιχτό σε υποκλοπές.
- 2) Στη συνέχεια, αποστέλλεται ένα ζεύγος EPR εμπλεκόμενων φωτονίων στην Alice και στον Bob, των οποίων η μέτρηση έχει ως αποτέλεσμα τιμές 0 ή 1. Η Alice και ο Bob φιλτράρουν εκείνα τα bit που δείχνουν σαφείς συσχετίσεις (σημαντικά κομμάτια) από αυτά χωρίς σαφείς συσχετισμούς (μη ουσιαστικά bits). Για αυτό, η ανάγκη για κλασικό κανάλι είναι απαραίτητη.
- 3) Στη συνέχεια, η διαδικασία ενίσχυσης απορρήτου [50] χρησιμοποιείται για τη διόρθωση των σφαλμάτων μέτρησης.

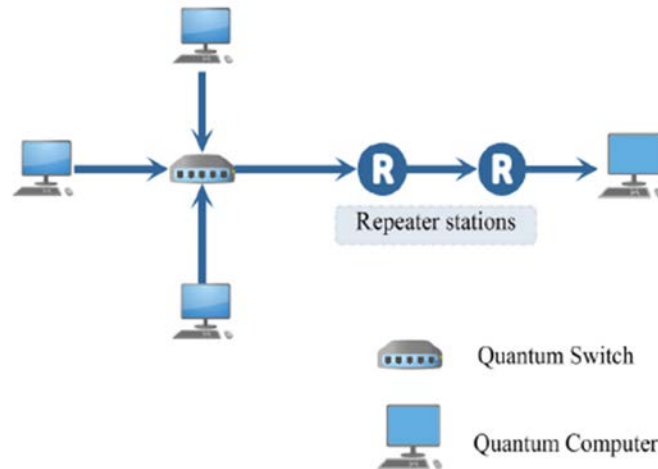
- 4) Η ασφάλεια του δικτύου εξαρτάται από το εάν η κατάσταση είναι μέγιστη μπλεγμένη ή όχι, διαφορετικά η αποσυναγωγή γίνεται εμπόδιο στην επικοινωνία. Η απόπειρα επίθεσης της Eve μπορεί να εντοπιστεί με την ανισότητα του Bell [51]. Εάν αυτή η ανισότητα δεν παραβιαστεί, τότε μπορεί να νομίζουμε ότι υπάρχει επίθεση από eavesdropping ή οι πληροφορίες που κοινοποιούνται έχουν κάποια τεχνικά προβλήματα. Ως αποτέλεσμα, οποιαδήποτε επιτυχημένη επίθεση από την Eve μπορεί να εντοπιστεί αμέσως και ελέγχεται η λειτουργικότητα του συστήματος.
- 5) Το κβαντικό κλειδί, λαμβάνοντας υπόψη τα σχετικά bits, χρησιμοποιείται για μια συμμετρική διαδικασία όπως για OTP και αποστέλλονται μέσω κανονικού Διαδικτύου.
- 6) Μετά από αυτό, ο Bob λαμβάνει τα δεδομένα που είναι κρυπτογραφημένα σε ένα κρυπτογραφημένο κείμενο και το αποκρυπτογραφεί με το αυτοαπαράγόμενο ιδιωτικό κλειδί. Αυτό συμπληρώνει το πρωτόκολλο Ekert με αποτέλεσμα τη δημιουργία ενός ασφαλούς κλειδιού.

2.2.3 Μέρη κβαντικού δικτύου

Κβαντικοί επαναλήπτες

Οι κβαντικοί επαναλήπτες αποτελούν αναπόσπαστα εξαρτήματα του Κβαντικού Δικτύου [Εικόνα 11], διευκολύνοντας τη μετάδοση της κβαντικής πληροφορίας σε μεγάλες αποστάσεις. Προτείνονται από τον Jurgen Briegel το 1998 [52] για την αντιμετώπιση του προβλήματος απώλειας φωτονίων σε κβαντικές επικοινωνίες μεγάλων αποστάσεων.

Στα κλασσικά δίκτυα, το πρόβλημα επιλύεται χρησιμοποιώντας κλασσικούς επαναλήπτες που αντιγράφουν το πληροφορίες μετά από τακτά χρονικά διαστήματα για ενίσχυση. Ωστόσο, στην περίπτωση της κβαντικής επικοινωνίας, λόγω του θεωρήματος της μη-κλωνοποίησης [53], οι πληροφορίες που μεταφέρονται σε qubits δεν μπορούν να αντιγραφούν, καθώς οι κλασσικοί επαναλήπτες δεν είναι κατάλληλοι για επικοινωνία. Οι επαναλήπτες [54] αυτοί έχουν εξελιχθεί και κατηγοριοποιούνται σε τρεις γενιές.



Εικόνα 11: Κβαντικοί επαναλήπτες: Αυτοί οι επαναλήπτες (σταθμοί) χρησιμοποιούνται σε μικρές αποστάσεις ώστε να μπορεί να δημιουργηθεί εμπλοκή μεταξύ ενδιάμεσων κόμβων και τελικά μεταξύ ακραίων κόμβων που απέχουν μεγάλη απόσταση μεταξύ τους. Εδώ, οι κβαντικού διακόπτες χρησιμοποιούνται επίσης για τη μετάδοση πληροφοριών μεταξύ των ακραίων κόμβων, διασχίζοντας κανάλια σε υπέρθεση διαφορετικών τάξεων.

Η πρώτη γενιά κβαντικών επαναληπτών συνδέει δύο απομακρυσμένους κόμβους μικρής απόστασης. Κάθε σταθμός επαναλήπτη πρέπει να δέχεται, να επεξεργάζεται και να μεταδίδει την πληροφορία. 1) Το μπλέξιμο των qubits παίρνει μέρος, 2) Ανταλλαγή των qubit, 3) Διόρθωση σφαλμάτων [55]. Ένα αρνητικό της 1^{ης} γενιάς είναι ότι χρειάζονται πολλές κλασσικές πληροφορίες για την διόρθωση σφαλμάτων το οποίο προκαλεί φόρτο στο δίκτυο.

Η δεύτερη γενιά κβαντικών επαναληπτών εφαρμόζει την τεχνική της μονής διαδρομής κλασσικής επικοινωνίας για την διόρθωση των qubits [56],[57],[58]. Έτσι ο χρόνος αναμονής [154] για την διόρθωση των qubit δεν χρειάζεται αλλά χρειάζεται αμφίδρομη επικοινωνία ώστε να μειωθούν τυχόν λάθη που προκύπτουν.

Η Τρίτη γενιά κβαντικών επαναληπτών βασίζεται στην αμφίδρομη επικοινωνία η οποία αντικαθίσταται από μονή μετάδοση σήματος με τη χρήση συγκεκριμένων κωδικών που αντέχουν την απώλεια πληροφορίας [56],[59],[60],[61]. Η πληροφορία αποκωδικοποιείται σε qubits όπου φωτόνια ταξιδεύουν μέσα από το κανάλι επικοινωνίας. Ο παραλήπτης λαμβάνει τα qubits ύλης σε πριν γίνει η διόρθωση σφαλμάτων, ενώ στη δεύτερη γενιά δεν χρειάζεται. Τα qubit ύλης δεν απαιτούνται για να χρησιμεύουν ως κβαντικές μνήμες όπως στην πρώτη και δεύτερη γενιά το 2014 και αυτό το σύστημα χαρακτηρίστηκε ως πλήρως ανεκτικό σε σφάλματα [62].

Η μεγάλη ζήτηση κλασσικών qubits για κβαντικούς επαναλήπτες οδήγησε στην ανάπτυξη οπτικών κβαντικών επαναληπτών τα τελευταία χρόνια [54] [63] [64] [65] με τη χρήση του πρωτοκόλλου DLCZ [66]. Το οποίο ονομάστηκε από τον Duan [67], Ιδιαίτερα, μέσα από σύνολα κβαντικών μνημών και γραμμικών οπτικών τεχνικών, διευκολύνει τη διατήρηση ισχυρής σύζευξης ανάμεσα στα φωτόνια και τις μνήμες που αποδεικνύονται πλεονεκτικές σε επικοινωνία κβαντικών πληροφοριών σε μεγάλη απόσταση [68]. Η ιδέα είναι να δημιουργηθεί εμπλοκή μεταξύ δύο ζευγαριών qubit, καθένα καλύπτοντας μια μικρή απόσταση και στη συνέχεια θα γίνεται πάλι εμπλοκή δύο ζευγαριών qubits μέχρι να φτάσει στον τερματικό κόμβο.

Entanglement Swapping: Σε αυτήν τη διαδικασία, η προβολή της κατάστασης δύο σωματιδίων γίνεται σε μια εναλλαγή εμπλοκής (entanglement swapping), για την απόκτηση συνολικής εμπλοκής. Επιτυγχάνεται μέσω εκτέλεσης ειδικής Μέτρησης Bell (BSM), η οποία δεν απαιτεί ουσιαστικά άμεση συνεργασία μεταξύ των δύο σωματιδίων. Μια τέτοια μέτρηση θα οδηγήσει αυτόματα στην κατάρρευση της κατάστασης των υπόλοιπων δύο σωματιδίων σε μια εναλλαγή εμπλοκής. Δεν είναι τίποτα λιγότερο από την κβαντική τηλεμεταφορά των κβαντικών καταστάσεων. Πολλές διαδικασίες τηλεμεταφοράς πραγματοποιούνται από πολλούς σταθμούς επαναλήπτη, δημιουργώντας έτσι έναν κβαντικό κανάλι για τη μετάδοση της πληροφορίας μεταξύ των άκρων κόμβων που είναι φυσικά απομακρυσμένοι χιλιάδες χιλιόμετρα [69], [70], [71].

Κβαντικά κανάλια επικοινωνίας

Το κβαντικό διαδίκτυο είναι ένα δίκτυο που παρουσιάζει εγγενή ασφάλεια και θα υλοποιηθεί συνδυαστικά με τον κλασικό Διαδίκτυο, όπου οι άκροι θα συνδέονται μέσω κλασικών και κβαντικών καναλιών. Δημιουργείται ένα συνεχές κβαντικό κανάλι μέχρι να συνδεθούν όλοι οι άκροι, όπως φαίνεται στην [Εικόνα 12].



Εικόνα 12: Το κβαντικό δίκτυο λειτουργεί σε συνεργία με το κλασσικό

Τόσο η κλασική πληροφορία όσο και η κβαντική πληροφορία μπορούν να σταλούν μέσω των κβαντικών καναλιών. Όπως φαίνεται στην τηλεμεταφορά κβαντικών δεδομένων $|\Phi_D\rangle$, τα ζεύγη EPR που δημιουργούνται διανέμονται στην Άλις και το Μπομπ μέσω ενός κβαντικού καναλιού. Αυτό το κανάλι μπορεί να είναι ένα κανάλι ελεύθερου χώρου για την αποστολή κβαντικών πληροφοριών σε μεγάλες αποστάσεις ή μπορεί να είναι κανάλια βασισμένα σε ίνες, τα οποία μπορούν να χρησιμοποιηθούν για τη μετάδοση κβαντικών πληροφοριών σε σχετικά μικρότερες αποστάσεις. Πόσο αποτελεσματικά μπορεί να διανεμηθεί μια ενθάρρυνση εξαρτάται από τη δυνατότητα του καναλιού και τη διαδικασία διανομής ενθάρρυνσης, που περιορίζεται κυρίως από την απώλεια φωτονίων στο κανάλι που κλιμακώνεται εκθετικά σε μια συνηθισμένη κατάσταση. Η χωρητικότητα του καναλιού επιβάλλει τη δυνατότητα του καναλιού να παραδίδει την πληροφορία από την Άλις στον Μπομπ με τρόπο αξιόπιστο και ανακτήσιμο.

Τα βήματα της κβαντικής επικοινωνίας μέσω των κβαντικών καναλιών διαφέρουν από την επικοινωνία μέσω των κλασικών καναλιών σε πολλούς τρόπους. Στον κβαντικό κανάλι, η επικοινωνία της κβαντικής πληροφορίας λαμβάνει χώρα σε τρεις διαφορετικές φάσεις:

- Φάση κωδικοποίησης καναλιού, όπου η αποστολέας Άλις κωδικοποιεί ή προετοιμάζει την κβαντική κατάσταση που θα σταλεί στον προορισμό Μπομπ, έτσι ώστε η κωδικοποιημένη πληροφορία να αντισταθμίζει το θόρυβο στο κανάλι [72], [73].

- Η επόμενη φάση είναι η φάση εξέλιξης της κβαντικής πληροφορίας, όπου η κβαντική πληροφορία τοποθετείται στο κβαντικό κανάλι, που αντιστοιχεί την πληροφορία στον παραλήπτη Μπομπ.
- Το τελικό στάδιο είναι η φάση αποκωδικοποίησης, που περιλαμβάνει την αποκωδικοποίηση της κβαντικής πληροφορίας από τον προορισμό Μπομπ. Εδώ η ληφθείσα κβαντική κατάσταση, περιλαμβάνοντας την ακριβή πληροφορία, μπορεί να είναι μια υπερθετική κατάσταση ή μια κατάσταση που κατέχει κάποιο θόρυβο. Αυτή η κατάσταση μετριέται στη συνέχεια από τον Μπομπ, λαμβάνοντας υπόψη τις διαδικασίες διόρθωσης σφαλμάτων.

1) Κανάλια ελεύθερου ή κενού χώρου

Είναι οπτικά κανάλια βασισμένα στο πρωτόκολλο QKD [74] [75] , έχουν εφαρμοστεί από [76] , [77] , [78] το Zeilinger group στους Κανάριους νήσους σε απόσταση 144 χιλιομέτρων. Υπόσχεται ότι η επικοινωνία θα γίνεται χωρίς σφάλματα σε μεγάλες αποστάσεις. Το πλεονέκτημα του ελεύθερου χώρου είναι ότι τα φωτόνια διατηρούν την πληροφορία άθικτη αλλά αυτό γινόταν σε απόσταση μέχρι 30 χιλιομέτρων καθώς οι διαταράξεις στην ατμόσφαιρα έκαναν τα φωτόνια να χάνουν την πληροφορία. Έτσι η Κίνα [79] δημιούργησε τρόπους όπως την οπτική-μεταεπεξεργασία [80], ισχυρότερες καταστάσεις [81] και πρωτόκολλα QKD που κωδικοποιούνται από το OAM modes [82], τρόποι λειτουργίας όπου η πληροφορία ταξίδεψε 1000 χιλιόμετρα στον διαστημικό σταθμό [83] καθιστώντας δυνατή την κβαντική επικοινωνία σε τεράστιες αποστάσεις.

2) Κανάλια Βασισμένα σε Οπτικές Ίνες

Εκτός από τους συνδέσμους ελεύθερου χώρου, οι οποίοι παίζουν ένα ζωτικό ρόλο στην κβαντική επικοινωνία μεγάλων αποστάσεων, οι οπτικές ίνες είναι πιο ελκυστικές λόγω της τεχνολογικής τους υπεροχής σε σχέση με το κλασσικό δίκτυο [Εικόνα 13].



Εικόνα 13: Οπτική Ίνα

Εδώ, τα qubit που μεταφέρουν πληροφορίες μεταδίδονται από την Άλις στον Μπομπ μέσω οπτικών καναλιών στις ίνες. Μια τυπική ίνα μονής λειτουργίας αποτελείται από έναν πυρήνα και ένα επίστρωμα που μεταφέρει το φως. Η συνολική εσωτερική ανάκλαση καθοδηγεί το φως κατά μήκος του πυρήνα της ίνας λόγω της διαφοράς στο δείκτη διάθλασης. Αυτοί οι καθοδηγητικοί κύλινδροι κατασκευάζονται άμεσα με πυρίτιο [84] ή σε αγωγούς όπως το αλουμίνιο [85]. Υπάρχουν διάφορα είδη ινών διαθέσιμα για την εξάπλωση των καταστάσεων των κβαντικών. Μεταξύ αυτών, οι ίνες μονής λειτουργίας έχουν έναν μικρότερο πυρήνα που διατηρεί το φως πιο σφιχτά, επομένως καλύτερα κατάλληλες για τα ακριβή περιβάλλοντα των πειραμάτων των κβαντών [86]. Σε ένα τέτοιο πείραμα, δημιουργείται ενθάρρυνση σε απόσταση 300 χλμ μέσω οπτικού καναλιού ίνας [87]. Τα κανάλια βασισμένα σε ίνες έχουν το πλεονέκτημα ότι τα περιβαλλοντικά στοιχεία δεν είναι σημαντικά μέσα στα κανάλια ίνας, διατηρώντας έτσι τη συνεκτικότητα των φωτονίων. Αντίθετα, υποφέρει από προβλήματα διατήρησης πολικοποίησης και οπτικής απόσβεσης που περιορίζουν την απόσταση επικοινωνίας σε μερικές εκατοντάδες χιλιόμετρα [88], [89], [90].

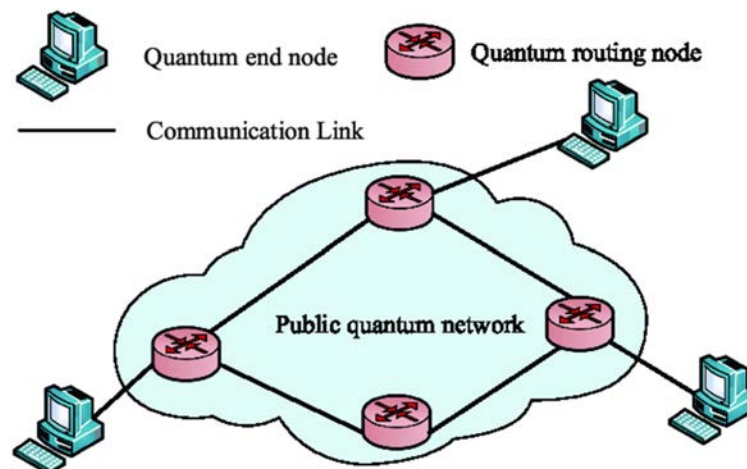
Κβαντικές Μνήμες

Οι κβαντικές μνήμες είναι μέρος των κβαντικών επικοινωνιών, οι οποίες χρειάζονται για την αποθήκευση και την επεξεργασία qubits που στέλνονται με φωτόνια υψηλής πιστότητας [91]. Λειτουργούν μαζί με του κβαντικούς επαναλήπτες σαν εργαλείο συγχρονι-

σμού επέκτασης της κβαντικής επικοινωνίας [92]. Μια έρευνα που ασχολείται με ανάπτυξη κβαντικών μηνυμάτων είναι το πρότζεκτ Qubit Applications [93]. Για την επίτευξη μακρινής επικοινωνίας οι κβαντικές μήμες μετατρέπουν τα qubits από φως σε ύλη και χρησιμοποιούνται επίσης για συγχρονισμό. Η επικοινωνία καθίσταται εφικτή μέσω του ελεύθερου χώρου και των οπτικών ινών [94]. Οι μήμες αυτές χρησιμοποιούν ουδέτερα άτομα, ώστε να επιτρέπεται η αποθήκευση, η λειτουργικότητα και η ανάκτηση των φωτονίων που βρίσκονται σε εμπλοκή [95].

Τερματικοί κόμβοι

Οι τερματικοί κόμβοι [Εικόνα 14] αποτελούν το πιο σημαντικό προαπαιτούμενο στα κβαντικά δίκτυα καθώς χρησιμοποιούνται όλα τα στοιχεία που αναλύσαμε παραπάνω για να επιτευχθεί η κβαντική επικοινωνία. Δηλαδή αυτοί οι κόμβοι καθίστανται λειτουργική με την βοήθεια συνεργασίας των κβαντικών υπολογιστών, κβαντικών επαναληπτών. Κβαντικών μηνυμάτων και των κλασικών υπολογιστών. Η πιστότητα μπορεί να βελτιωθεί με πολλαπλά qubits στους τερματικούς κόμβους κάνοντας έτσι μια μικρής κλίμακα επικοινωνίας για τους κβαντικούς υπολογιστές. Αυτοί οι κόμβοι έχουν διάφορες λειτουργίες όπως από τη χρήση του πρωτοκόλλου QKD μέχρι την διανομή κβαντικού υπολογισμού. Τελικά για να γίνει πραγματικότητα το κβαντικό δίκτυο πρέπει οι τερματικοί κόμβοι να παρέχουν αξιόπιστη αποθήκευση των κβαντικών καταστάσεων [96], καθώς η εφαρμογή του θα γίνεται στο φυσικό επίπεδο του κβαντικού δικτύου [97].



Εικόνα 14: Τερματικοί κόμβοι και η σύνδεση με το κβαντικό δίκτυο

2.3 ΚΒΑΝΤΙΚΟ ΔΙΑΔΙΚΤΥΟ

2.3.1 Εφαρμογές

Το κβαντικό διαδίκτυο είναι ένα αχανές πεδίο με τεράστιες δυνατότητες σε πολλές εφαρμογές [97]. Με την τωρινή τεχνολογία δεν μπορούμε να προβλέψουμε ακριβώς τις τεχνολογίες που θα μας προσφέρει, αλλά αυτήν η τεχνολογία αναπτύσσεται με ραγδαίους ρυθμούς αναπτύσσοντας εφαρμογές που θα αναλύσουμε παρακάτω όπως της ασφαλούς επικοινωνίας, συγχρονισμού ρολογιών, τυφλού υπολογισμού .

A. Ασφαλής επικοινωνία

Η ασφαλής επικοινωνία [Εικόνα 15], αποτελεί το βασικό προαπαιτούμενο για την σημερινή εποχή. Υπάρχουν πολυάριθμες εφαρμογές που βασίζονται στην μεταφορά δεδομένων μέσω του διαδικτύου όπως τραπεζικές συναλλαγές, αγορά και πώληση μετοχών, αγορά προϊόντων μέσω του διαδικτύου , στρατιωτικές ακόμη και εθνικές εφαρμογές οι οποίες μέσω του κβαντικού πρωτοκόλλου QKD θα διατηρούν την ιδιωτικότητα τους άθικτη [98]. Η παραδοσιακή κλασική επικοινωνία στον σύγχρονο κόσμο χρησιμοποιεί διάφορα πρωτόκολλα κρυπτογράφησης, όπως η ανταλλαγή κλειδιών Diffie-Hellman [99] και τα πρωτόκολλα RSA [100], σε ισότοπους ηλεκτρονικού εμπορίου. Ωστόσο, αυτά τα πρωτόκολλα μπορεί να υποκείμενα σε αποκρυπτογράφηση από μελλοντικούς πλήρης κβαντικούς υπολογιστές, θέτοντας σε κίνδυνο όλα τα συστήματα ασφαλείας. Ωστόσο, με τη χρήση της Κβαντικής Πληροφορίας (QI) και πρωτοκόλλων ασφαλείας όπως το Quantum Key Distribution (QKD) [101], το θεώρημα της μη κλωνοποίησης και η κβαντική τηλεμεταφορά διακόπτουν το σύστημα και ανιχνεύουν κατά την εκτέλεση την παραβίαση διατηρώντας το απόρρητο των συστημάτων. Η έρευνα στον τομέα του QKD έχει διεξαχθεί εκτενώς και έχει εφαρμοστεί με επιτυχία σε αποστάσεις που καλύπτουν από λίγα εκατοντάδες χιλιόμετρα [102], [103], [104] έως χιλιάδες χιλιόμετρα με την εκτόξευση του δορυφόρου Micius από επιστήμονες από την Κίνα [105].

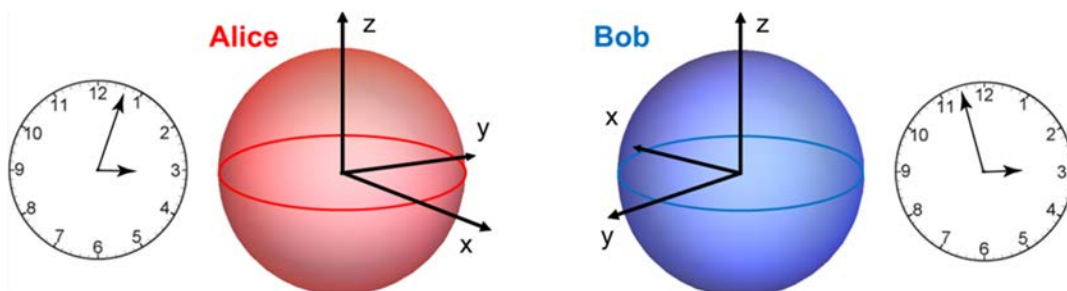


Εικόνα 15: Ασφαλής Επικοινωνία

Το Διαδίκτυο των Πραγμάτων (IoT) είναι κρίσιμο για πολλές εφαρμογές [106], [107], [108], και η προστασία των δεδομένων σε αυτές τις εφαρμογές είναι ζωτικής σημασίας. Τα συστήματα ασφαλείας που βασίζονται σε συμβατικά κρυπτογραφικά πρωτόκολλα αντιμετωπίζουν κίνδυνο από τους μελλοντικούς κβαντικούς υπολογιστές που αναπτύσσονται ήδη. Οι κβαντικές επιθέσεις [109], όπως οι ατομικές, συλλογικές ή γενικές επιθέσεις με τη χρήση του κβαντικού υπολογισμού, επηρεάζουν τα κρυπτοσυστήματα με δημόσια κλειδιά. Η ασφάλεια του IoT θα επωφεληθεί από την κβαντική κρυπτογραφία, που λειτουργεί βασιζόμενη σε κβαντικά θεωρήματα και μπορεί να εφαρμοστεί σε ασύρματες και οπτικές επικοινωνίες, απαραίτητες για την ασφάλεια των συστημάτων IoT. Οι μετα-κβαντικοί κρυπτοσυστήματα IoT έχουν εξεταστεί [110] και μπορούν να ενισχύσουν την ασφάλεια σε πολλούς τομείς που εξαρτώνται από συσκευές IoT με περιορισμένους πόρους και μπαταρίες. Η μετα-κβαντική κρυπτογραφία αναφέρεται σε πρωτόκολλα που αντιστέκονται σε κβαντικές επιθέσεις και μπορεί να επηρεάσει διάφορες εφαρμογές του IoT, όπως την άμυνα και δημόσια ασφάλεια, βιομηχανία, έξυπνη υγεία, κ.ά. Συνεπώς, η μετάβαση από τα κλασικά πρωτόκολλα σε κβαντικά είναι ουσιώδης για τη συνολική ασφάλεια των δεδομένων.

Β. Συγχρονισμός ρολογιών

Ένα σημαντικό ζήτημα σε πολλές πρακτικές εφαρμογές των σύγχρονων τεχνολογιών είναι η ακριβής χρονοκράτηση και συγχρονισμός των ρολογιών σε όλον τον κόσμο. Λόγω του ακριβούς συγχρονισμού των ρολογιών, όλες οι επιστημονικές εφαρμογές που εξαρτώνται από το χρονικό συγχρονισμό εμφανίζουν ελάχιστα σφάλματα. Αυτές οι εφαρμογές περιλαμβάνουν το σύστημα ποσοτικής θέσης [111], συγχρονισμός γεννητριών ηλεκτρικής ενέργειας που τροφοδοτούν εθνικά δίκτυα ηλεκτρικής ενέργειας, συγχρονισμός μεταφοράς δεδομένων και χρηματοοικονομικές συναλλαγές, μακρινές γραμμές τηλεσκοπίων και καταναμεμημένος υπολογισμός κβαντικού υπολογισμού. Ωστόσο, αυτά τα συστήματα πλοήγησης, όπως το GPS, υφίστανται απειλή ασφαλείας γνωστή ως απομίμηση [112], [113]. Για τον συγχρονισμό των ρολογιών, απαιτούνται τεχνικές διασταύρωσης που συνδέουν απομακρυσμένους κβαντικούς κόμβους με ρολόγια που πρέπει να συνδεθούν σε ένα κβαντικό δίκτυο [114], [115]. Ένα καταναμεμημένο δίκτυο κβαντικών περιορισμένων ρολογιών, χωρισμένων από μεγάλες αποστάσεις, μπορεί να θεωρηθεί ως ένα τελικό ρολόι, όπου όλα τα μέλη σε διάφορες χώρες μπορούν να συγχωνεύσουν τους πόρους τους και να επιτύχουν συνεκτικά υψηλότερη σταθερότητα του ρολογιού. Με αυτόν τον τρόπο, μπορούν να διανείμουν αυτήν τη διεθνή χρονική κλίμακα σε όλους σε πραγματικό χρόνο. Η καταναμεμημένη αρχιτεκτονική επιτρέπει σε κάθε μέλος του δικτύου να επωφελείται από τη σταθερότητα του τοπικού σήματος ρολογιού χωρίς να χάνει την κυριαρχία του ή να διαπραγματεύεται την ασφάλεια. Κβαντικοί αλγόριθμοι απαιτούνται για την αντιμετώπιση του προβλήματος του Κβαντικού Συγχρονισμού Ρολογιών (QCS). Απαιτείται η ελαχιστοποίηση της διαφοράς χρόνου, μεταξύ δύο χωριστών ρολογιών με το ελάχιστον δυνατό αριθμό πόρων επικοινωνίας. Ο χρόνος μπορεί να υπολογιστεί με ακρίβεια και εξαρτάται από τη σταθερότητα της συχνότητας του ρολογιού και την αβεβαιότητα του χρόνου παράδοσης των μηνυμάτων που στέλνονται μεταξύ των δύο ρολογιών που χωρίζονται από μεγάλη απόσταση [Εικόνα 16].



Εικόνα 16: Αβεβαιότητα συγχρονισμού ρολογιών μεταξύ Alice και Bob

Επί του παρόντος, αναπτύσσονται πρωτόκολλα για τη μέτρηση του χρόνου με μεγαλύτερες ακρίβειες. Κάποια πρωτόκολλα εμφανίζουν ακρίβειες καλύτερες από 100 νανοδευτερόλεπτα για ρολόγια που χωρίζονται από περισσότερα από 8000 χιλιόμετρα [311]. Με την πρόοδο σε αυτά τα πρωτόκολλα, όπως το Ticking Qubit Handshake (TQH), όπως συζητείται στο [116], μπορεί να αυξηθεί αυτή η ακρίβεια στα 100 πικοδευτερόλεπτα. Αυτό επιτρέπει τον συγχρονισμό του ρολογιού που δεν εξαρτάται από τις αβεβαιότητες στον χρόνο παράδοσης μηνυμάτων μεταξύ των ρολογιών.

Γ. Τυφλός υπολογισμός

Η Τυφλή Κβαντική Υπολογιστική (Blind Quantum Computation - BQC) είναι μια άλλη εφαρμογή της Κβαντικής Πληροφορίας (QI) που σχετίζεται με την ασφάλεια ενός χρήστη. Με αυτόν τον τρόπο, η ιδιωτικότητα του δεν διαρρέεται σε έναν κβαντικό υπολογιστή που συμμετέχει στην υπολογιστική διαδικασία [117]. Η τεχνολογία για την κατασκευή ενός κβαντικού υπολογιστή κινείται με γρήγορους ρυθμούς, αλλά μόνο λίγα κέντρα στον κόσμο μπορεί να το χρησιμοποιήσουν λόγω της ανωτερότητάς του και του κόστους. Όπως και στο σημερινό σύστημα ενοικίασης υπερυπολογιστών, οι χρήστες μπορεί να λαμβάνουν περιορισμένα δικαιώματα πρόσβασης. Υποθέτουμε ότι μια χρήστης, η Alice, θέλει περιορισμένη πρόσβαση σε έναν κβαντικό υπολογιστή και μοιράζεται ευαίσθητες πληροφορίες για υπολογισμό. Το αποτέλεσμα αυτού του υπολογισμού στέλνεται πίσω στην Alice μέσω του κλασικού καναλιού. Σε αυτήν την περίπτωση, εάν η Alice θέλει το αποτέλεσμα του υπολογισμού χωρίς να αποκαλύπτει τις ευαίσθητες πληροφορίες της, πρέπει να χρησιμοποιήσει ένα πρωτόκολλο BQC. Αυτό επιτρέπει σε οποιονδήποτε χρήστη να αλληλεπιδρά με έναν κβαντικό υπολογιστή χωρίς να αποκαλύπτει τις ευαίσθητες πληροφορίες του σε οποιονδήποτε άλλον (για παράδειγμα, τον Bob) που έχει πρόσβαση στον κβαντικό υπολογιστή [118], [119]. Πρόσφατα, οι ηλεκτρονικές πληρωμές έχουν γίνει κυρίαρχες σε σχεδόν κάθε τομέα λόγω των ιστότοπων ηλεκτρονικού εμπορίου. Ωστόσο, η ασφάλειά τους απειλείται από την εμφάνιση κβαντικών υπολογιστών στην αγορά. Πρόσφατα, βασισμένο στο BQC, ένα σύστημα αξιολόγησης ασφάλειας ηλεκτρονικών πληρωμών χρησιμοποιείται για την αξιολόγηση της ασφάλειας των δικτυακών συναλλαγών, εγγυώνται την ασφάλεια [120]. Το BQC προτάθηκε αρχικά από τον Chaum το 1983 [121] και πρωτοδιατυπώθηκε από τον Childs το 2001 [122],

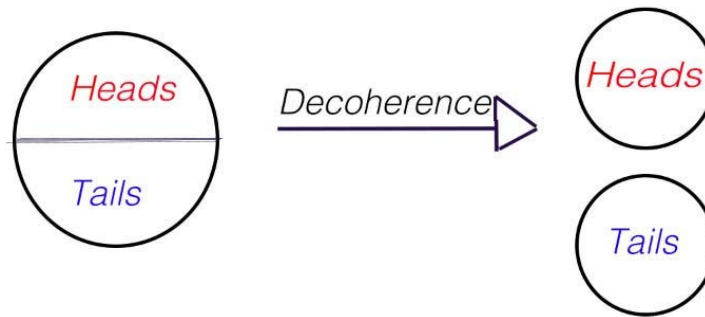
όπου η κρυπτογράφηση προστατευόταν με OTP χρησιμοποιώντας το μοντέλο κυκλώματος, έτσι ώστε ο διακομιστής με πλήρως εξοπλισμένο κβαντικό υπολογιστή να διατηρεί τις πληροφορίες ιδιωτικές χωρίς να μαθαίνει τίποτα για αυτές. Το πρωτόκολλο που πρότειναν οι Arrighi και Salvail το 2006 [123] απαιτεί από την Alice να προετοιμάζει και να μετρά την πολυκβαντική μπλεγμένη κατάσταση. Επιπλέον, είναι ευαίσθητο στον έλεγχο, πράγμα που σημαίνει ότι, εάν ο πλήρως εξοπλισμένος κβαντικός υπολογιστής δεν διστάζει να αποκαλυφθεί, μπορεί να αποκτήσει πληροφορίες. Σε ένα τέτοιο πρωτόκολλο, απαιτούνταν ένας κβαντικός υπολογιστής σταθερού μεγέθους με πρόσβαση σε μνήμη κβαντικού τύπου για την Alice [124]. Ένα πρωτόκολλο χρησιμοποιώντας το μοντέλο μιας κατεύθυνσης [125] διατυπώθηκε το 2009 από τους Broadbent κ.ά, όπου η Alice χρειάζεται μόνο έναν κλασικό υπολογιστή και μια κβαντική συσκευή μικρής κλίμακας που θα χρησιμοποιείται για τους υπολογισμούς της χρησιμοποιώντας τυχαία περιστραμμένες μόνο σταθερές qubit. Επομένως, αυτό το πρωτόκολλο είναι απόλυτα ασφαλές και η είσοδος και η έξοδος της Alice διατηρούνται εμπιστευτικές. Η ασφάλεια αυτού του πρωτοκόλλου επιδεικνύεται πειραματικά σε ένα οπτικό σύστημα [126]. Αυτή η έρευνα έχει εμπνεύσει πολλούς άλλους ερευνητές να υλοποιήσουν πιο ανθεκτικά πρωτόκολλα τυφλής κβαντικής υπολογιστικής. Συνεπώς, στο μέλλον, η Κβαντική Πληροφορία θα χρησιμοποιήσει δαπανηρούς και ισχυρούς κβαντικούς υπολογιστές στο υπολογιστικό cloud νέφος, κυρίως καταχωρημένους από μεγάλες τεχνολογικές εταιρείες. Ωστόσο, εκτός από την παροχή ασφάλειας και ιδιωτικότητας στα δεδομένα του χρήστη, το BQC θα ελέγχει επίσης εάν ο υπολογισμός εκτελείται από έναν κβαντικό επεξεργαστή και όχι από κάποια απάτη.

2.3.2 Προβλήματα

Σε αυτό το κεφάλαιο παρουσιάζουμε τα προβλήματα και τις προκλήσεις με τις οποίες θα έρθει αντιμέτωπο το κβαντικό δίκτυο. Αρχικά θα παρουσιάσουμε με το πρόβλημα της αποσυννοχής έπειτα τις επιπτώσεις της αποσυννοχής στην κβαντική τηλεμεταφοράς, μπλεξίματος και το πρόβλημα της πτώσης των κβαντικών καταστάσεων όταν μετριοούνται.

Α Αποσυνοχή

Η κβαντική επικοινωνία καθίσταται δυνατή με τη μετάδοση κβαντικών καταστάσεων από την Άλις στο Μπομπ μέσω του ελεύθερου χώρου ή οπτικών ινών [127]. Στην φυσική, δύο κύματα έχουν συνοχή, εφόσον διατηρούν σταθερή φάση σχέσης μεταξύ τους. Ωστόσο, περιβαλλοντικοί παράγοντες και η ευαισθησία των φωτονίων που μεταφέρουν τα qubits οδηγούν σε αποσυνοχή, με αποτέλεσμα οι κβαντικές καταστάσεις να χάνουν τις ιδιότητές τους και να υιοθετούν χαρακτηριστικά της κλασικής φυσικής με την πάροδο του χρόνου [Εικόνα 17].



Εικόνα 17: Αποσυνοχή

Για να διατηρήσουν τις ιδιότητές των φωτονίων που περιέχουν την πληροφορία τους θα πρέπει να είναι τελείως απομονωμένες από το περιβάλλον κάτι που αποτελεί πρόκληση με την τρέχουσα τεχνολογία των κβαντικών συστημάτων. Η αποσυνοχή είναι μια αναστρέψιμη διαδικασία που επηρεάζει τις διαδικασίες επικοινωνίας, όπως η τηλεμεταφορά και η εμπλοκή των καταστάσεων qubits. Η αξιοπιστία της τηλεμεταφοράς μετρίεται με τον κβαντικό συντελεστή, με μεγαλύτερες ατέλειες που προκαλούν χαμηλότερο συντελεστή. Οι χρόνοι αποσύνθεσης υποδηλώνουν πόσον καιρό τα qubits μπορούν να παραμένουν συσχετισμένα χωρίς απώλεια πληροφοριών και εξαρτώνται από την τεχνολογία των qubits. Για παράδειγμα, τα υπεραγωγικά κυκλώματα έχουν χρόνο αποσύνθεσης 100 μικροδευτερολέπτων των qubits [128], [129], ενώ μεγαλύτερος χρόνος αποσύνθεσης έχει καταγραφεί με παγιδευμένα ιόντα. Η αξιοπιστία της τηλεμεταφοράς μετρίεται με την κβαντική πιστότητα η οποία θεωρείται ως μορφή αξίας, όσο μεγαλύτερες είναι οι ατέλειες λόγω της αποσυνοχής, τόσο μικρότερη η πιστότητα. κλασικές τεχνικές διατηρούν την κβαντική πληροφορία έναντι στην

αποσυννοχή [130]. Συνήθως το πρόβλημα μπορεί να ξεπεραστεί με την απόσταξη εμπλοκής η οποία χρειάζεται επιπλέον επίπεδα επεξεργασίας των qubit.

B. Ατέλεις Κβαντική Τηλεμεταφορά

Οι ατέλειες είναι παρούσες σε όλους τους τύπους επικοινωνίας, και η κβαντική επικοινωνία δεν αποτελεί εξαίρεση. Αυτές οι ατέλειες πηγάζουν από την αποσυννοχή, όπως το αναλύσαμε στην προηγούμενη παράγραφο. Η κβαντική επικοινωνία αντιμετωπίζει πρόβλήματα από περιβαλλοντικές αλληλεπιδράσεις με αποτέλεσμα την απώλεια φωτονίων που μεταφέρουν τα qubits. Η αποσυννοχή επηρεάζει επίσης τη διαδικασία κβαντικής τηλεμεταφοράς καθώς και τη διαδικασία δημιουργίας και διανομής των qubits. Ωστόσο, άλλες λειτουργίες που εφαρμόζονται στις κβαντικές καταστάσεις της διαδικασίας κβαντικής τηλεμεταφοράς εισάγουν επιπλέον ατέλειες στο τηλεμεταφερόμενο qubit [131]. Αυτές οι κβαντικές ατέλειες έχουν πολλαπλασιαστικό χαρακτήρα, συνεπώς, μπορεί να θεωρηθεί ότι αυτό το φαινόμενο μοιάζει περισσότερο με τα κλασικά εφέ ξεθωριάσματος παρά με τον κλασικό πρόσθετο θόρυβο που προκαλείται από τη βραδυκίνηση των ηλεκτρονίων [132]. Εξελίζεις σε ερευνητικό επίπεδο στοχεύουν στο να μοντελοποιήσουν ακριβώς τις κβαντικές ατέλειες, λαμβάνοντας υπόψη τις διάφορες επιδράσεις των ατελειών στη διαδικασία κβαντικής τηλεμεταφοράς [133].

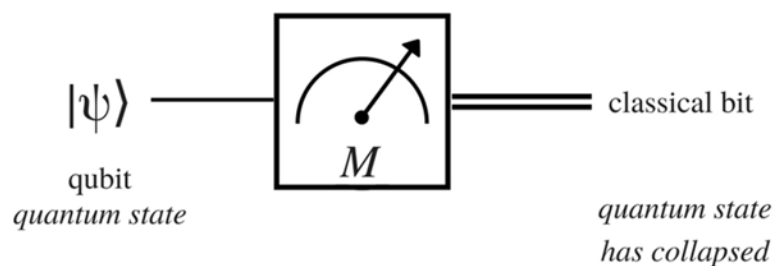
Γ. Πολυπλοκότητα σχεδιασμού Υλοποίηση Δικτύου Αξιοπιστών Επαναληπτικών

Σε αντίθεση με την κλασική επικοινωνία όπου υπάρχουν δεδομένα σε πακέτα αποστέλλονται μαζί με αντίγραφα του ίδιου, σε περίπτωση που τα δεδομένα χαθούν ή δεχθούν επίθεση, είναι αδύνατο στην κβαντική επικοινωνία να αντιγράψουμε τα qubits λόγω των ιδιοτήτων του θεωρήματος του της μη-κλωνοποίησης no-cloning theorem [133]. Αυτό θέτει ορισμένες αυστηρές προκλήσεις σχεδιασμού, οι οποίες αυξάνουν την πολυπλοκότητα του σχεδιασμού του λειτουργικού δικτύου στο κβαντικό διαδίκτυο. Αν μιλάμε για κλασικούς κωδικούς διόρθωσης σφαλμάτων, δεν μπορούν να εφαρμοστούν άμεσα στην κβαντική επικοινωνία, γιατί δεν είναι δυνατή η εκ νέου μετάδοση των qubits. Επομένως, απαιτούνται κωδικοί διόρθωσης σφαλμάτων quantum error correction (QEC) [134] και πρέπει να υπάρχουν λειτουργίες δικτύου να σχεδιαστεί ανάλογα κάνοντας το σύστημα πολύπλοκο. Τέτοιος η πολυπλοκότητα του σχεδιασμού είναι παρούσα σε κάθε επίπεδο του σχεδιασμού του κβαντικού διαδικτύου έναρξης- μετάβασης από το επίπεδο

λειτουργικότητας διόρθωσης σφαλμάτων στο επίπεδο ελέγχου πρόσβασης μέσου και ανακάλυψης διαδρομής, με πρωτόκολλα όπως το CQ^2 [135], [136].

Α. Μέτρηση κβαντικών καταστάσεων

Ένα qubit μπορεί να βρίσκεται σε υπέρθεση των δύο καταστάσεων και μετρώντας την κατάσταση του qubit καταρρέει σε μια από τις δύο καταστάσεις. Αυτό σημαίνει ότι πριν την μέτρηση η ποσότητα πληροφορίας που βρίσκεται μέσα στο qubit είναι άγνωστη. Αυτό το πρόβλημα μπορεί να χαρακτηριστεί ως παράδοξο της γάτας του Schrödinger [19]. Μια γάτα μπορεί να είναι ζωντανή και νεκρή ταυτόχρονα χάρις την υπέρθεση. Σε αυτήν την μέτρηση πάντα η γάτα θα είναι είτε ζωντανή είτε νεκρή. Το αποτέλεσμα των πιθανοτήτων χαρακτηρίζεται ακόμη ως άλυτο πρόβλημα και εγκυμονεί πολλές κρυμμένες πληροφορίες μέσα σε αυτό το παράδοξο μέχρι και σήμερα [Εικόνα 18].



Εικόνα 18: Μέτρηση κατάστασης qubit

2.3.3 Λύσεις

Α Επανάσταση των κβαντικών επεξεργαστών

Οι μελλοντικές κβαντικές τεχνολογίες θα χρειαστούν κβαντικούς υπολογιστές με ισχυρές υπολογιστικές ικανότητες ώστε να επιτευχθεί η κβαντική επανάσταση. Θα μπορέσουν να επιλύσουν προβλήματα που πρακτικά είναι αδύνατο να επιλυθούν με τους σημερινούς υπερυπολογιστές. Το κβαντικό δίκτυο θα γίνεται ολοένα και πιο ισχυρό λόγω των αυξανόμενων αριθμών των qubits στους τερματικούς κόμβους. Για να συμβαδίσουμε

με αυτό το δεδομένο οι κβαντικοί επεξεργαστές με διπλά ψηφία εξελίσσονται και αναπτύσσονται χαράζοντας έτσι τον νέο κβαντικό διαδικτυακό κόσμο. Αυτή η ανάπτυξη θα βοηθήσει στο να ενισχύσει την οικονομία του κόσμου, την υγεία, εταιρίες cloud βάσεις δεδομένων θα είναι πολύτιμες. Επίσης, οι κβαντικοί υπολογιστές θα συνδέονται μεταξύ τους μέσω της καθαρής διαπλοκής και η επικοινωνία θα γίνει χρησιμοποιώντας κβαντική τηλεμεταφορά. Η κβαντική πληροφορία μπορεί επίσης να βοηθήσει στη δικτύωση υπολογιστών για ακόμα μεγαλύτερη απόδοση.

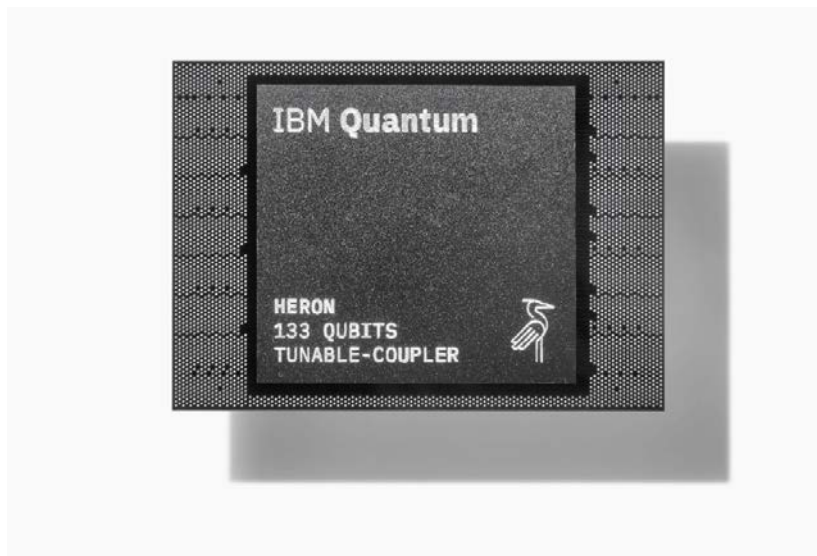
B. Υλοποίηση Δικτύου Αξιοπίστων Επαναληπτικών

Το δίκτυο επαναλήπτη παίζει σημαντικό ρόλο στη σύγχρονη δικτύωση και ως εκ τούτου, πολλά θεωρητικά και πρακτικά έχουν καθιερωθεί έρευνες [137], [138], ακόμα κι αν βρίσκονται ακόμη σε στάδιο ανάπτυξης [139], [140]. Η υλοποίηση δικτύων επαναλήπτη απαιτεί έναν αριθμό ενδιάμεσων αραιοί κόμβοι που είναι μπλεγμένοι μεταξύ τους έτσι ώστε η εμπλοκή δημιουργείται μεταξύ δύο μακρινών ακραίων κόμβων με το φαινόμενο-entanglement swapping. Κάθε ζεύγος γειτονικών κόμβων επαναλήπτη ανταλλάσσει τα κρυπτογραφημένα κλειδιά που χρησιμοποιούν QKD που επιτρέπει στους μακρινούς κόμβους να δημιουργούν διαγράφουν τα δικά τους κλειδιά με την υπόθεση ότι οι κόμβοι πρέπει να είστε αξιοπίστοι. Όμως, μέχρι πρόσφατα στην εργασία του Μπρίστολ [141], η εμπιστοσύνη- Οι ελεύθεροι κόμβοι αποδεικνύονται επίσης κλιμακωτοί σε ένα κβαντικό επίπεδο πόλης δίκτυο που χρησιμοποιεί QKD που βασίζεται σε εμπλοκή. Έτσι, αξιοπίστο Η υπόθεση των κόμβων μπορεί να αποφευχθεί με τρεις τρόπους, πρώτον με χρήση του QKD που βασίζεται σε εμπλοκή [142], συσκευή μέτρησης εκκρεμής QKD [143], [144], [145], επικοινωνία πολλαπλών διαδρομών τεχνικές όπως η κωδικοποίηση κβαντικού δικτύου [146] και με χρήση των κβαντικών αναμεταδοτών. Ωστόσο, οι αξιοπίστοι επαναλήπτες είναι ένα καυτό θέμα που θα υλοποιηθεί με αξιοπίστους κόμβους για να ξεπεραστούν οι περιορισμοί απόστασης μεταξύ των κόμβων.

Γ. Ενσωμάτωση των qubits με άλλες τεχνολογίες

Πολλοί ισχυροί υπολογιστές που φτιάχτηκαν χρησιμοποιούν διαφορετικά συστήματα όπως bits, νευρώνες και qubits για τους υπολογισμούς. Ο υπερυπολογιστής που φτιάχτηκε από την IBM, έχει μέγιστη απόδοση 200.000 teraflops [147] και είναι το πιο ισχυρό μηχάνημα στον κόσμο το οποίο είναι χτισμένο πάνω σε bits και νευρώνες. Αυτός υπολογιστής έχει την δυνατότητα να επιλύει σύνθετα προβλήματα τα οποία σχετίζονται με την

τεχνητή νοημοσύνη. Τέλος είναι πάρα πολύ γρήγοροι, πράγμα που βοηθάει στο να αποφορτίζεται πολύ εύκολα από διάφορα υπολογιστικά προβλήματα που έρχεται αντιμέτωπη η επιστήμη. Οι νευρώνες μπορούν επίσης να συνδυαστούν με qubits και μπορούν να κατασκευάσουν έναν κβαντικό υπολογιστή με αλγόριθμους μηχανικής μάθησης νευρώνων με δυνατότητες πολλαπλάσιες σε σχέση με τον κλασσικό υπολογιστή. Τα qubits μαζί με τα bits μπορούν να συνδυασθούν για την δημιουργία κβαντικών επεξεργαστών, τα οποία έχουν την δυνατότητα να κάνουν κλασσικούς υπολογισμούς. Η IBM άλλη μια φορά προτοπώρησε στον τομέα και πρόσφατα τον Δεκέμβριο του 2023 ανέπτυξε νέας γενιάς κβαντικό επεξεργαστή τον HERON [148] με ισχύ 133 qubits [Εικόνα 19]. Οπότε η έρευνα των επιστημόνων εστιάζει στους πιθανούς συνδυασμούς των bits, qubits και των νευρώνων ώστε να δημιουργηθούν νέες κβαντικές τεχνολογίες όπως οι κβαντικοί υπολογιστές και ισχυρότεροι επεξεργαστές που θα φέρουν την επανάσταση στον νέο κβαντικό κόσμο.

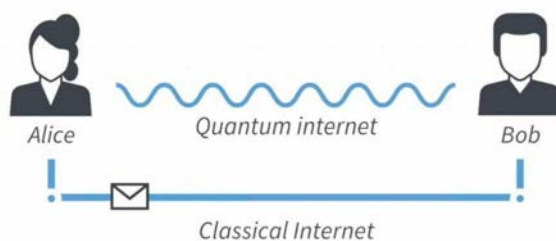


Εικόνα 19: Κβαντικός επεξεργαστής IBM HERON 2ης γενιάς

Δ. Η συνύπαρξη του κβαντικού και κλασσικού διαδικτύου

Το κβαντικό δίκτυο θα γίνει εφικτό όταν δορυφόροι οι οποίοι θα κατασκευαστούν από εταιρίες και θα σχηματίσουν τον δρόμο για εμπλοκή μεγάλων αποστάσεων με χρήση του πρωτοκόλλου QKD. Θα χρειαστούν νέες οπτικές ίνες αναβαθμισμένες που να συμβαδίζουν με τις αρχές της κβαντικής μηχανικής για την ανταλλαγή κλασσικών δεδομένων

που θα χρειαστούνε για την κβαντική τηλεμεταφορά [149]. Το πρωτόκολλο QKD θα χρειαστεί επίσης κλασικά κανάλια για την απόκτηση πληροφοριών, την ασφάλιση τους ώστε να μειωθούν οι θόρυβοι και οι καθυστερήσεις στα κανάλια επικοινωνίας [150]. Ένα πλήρες ασφαλισμένο πρωτόκολλο QKD βασισμένο σε κανάλια θα συνδέει κλασσικές συσκευές όπως κινητά, τάμπλετ, έξυπνα ρολόγια, δορυφόρους, έξυπνα οχήματα, έξυπνα σπίτια με απόλυτη ασφάλεια. Το κβαντικό σύννεφο ή cloud θα υπάρχει και θα είναι απολύτως ασφαλές και θα παρέχει ιδιωτικότητα των δεδομένων του κάθε χρήστη. Οπότε το κβαντικό διαδίκτυο θα συνυπάρχει με το κλασσικό διαδίκτυο σε ένα κόσμο γεμάτο από εφαρμογές με ανεγάζδιαστη ασφάλεια [Εικόνα 20].



Εικόνα 20: Συνεργασία κβαντικού και κλασσικού διαδικτύου

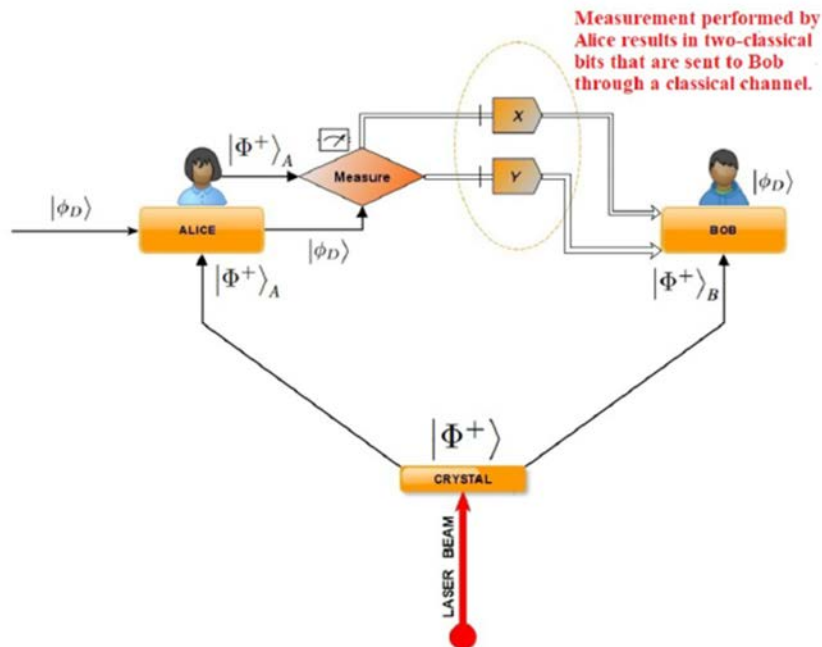
2.4 ΚΒΑΝΤΙΚΕΣ ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ

Το Κβαντικό Διαδίκτυο είναι ένα σύστημα που αποτελείται από διάφορες λειτουργίες που απαιτούνται για την επικοινωνία πληροφοριών μεταξύ απομακρυσμένων κόμβων ενός δικτύου. Σε αυτήν την ενότητα, θα επικεντρωθούμε σε διάφορες λειτουργίες του Κβαντικού Διαδικτύου όπως η κβαντική τηλεμεταφορά, κβαντικά κανάλια, κβαντικοί επαναλήπτες, κβαντικές μνήμες, Κβαντική Διασφάλιση Κλειδιών (QKD) και τερματικοί κόμβοι.

2.4.1 Κβαντική τηλεμεταφορά

Η κβαντική τηλεμεταφορά αποτελεί ένα σύστημα για τη μετάδοση qubits εντός ενός δικτύου κβαντικής επικοινωνίας χωρίς τη φυσική μεταφορά του σωματιδίου που αποθηκεύει το qubit. Η έννοια της τηλεμετάδοσης qubits ξεκίνησε με τον σημαντικό έργο που παρουσιάστηκε στο "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" [151]. Πρωτοεξετάστηκε πειραματικά από την ομάδα του Anton Zeilinger το 1997 με την επιτυχημένη μετάδοση κβαντικών οπτικών καταστάσεων [152]. Ταυτόχρονα, η ομάδα του Sandu Popescu πειραμάτισε με επιτυχία τη φωτονική τηλεμεταφορά το 1998 [153]. Η απόσταση της τηλεμετάδοσης 55 μέτρων επετεύχθη υπό εργαστηριακές συνθήκες από τον Ελβετό ερευνητή Nicolas Gisin και την ομάδα του το 2003 [154], επαληθεύθηκε στο εμπορικό δίκτυο τηλεπικοινωνιών της Swisscom με βάση την οπτική ίνα το 2007 [155]. Αργότερα, το 2004, ερευνητές από την Ινσμπρούκ και τις ΗΠΑ κατάφεραν να τηλεμεταφέρουν ατομικές καταστάσεις για πρώτη φορά [156], ακολουθούμενοι από μια Αυστριακή ομάδα υπό τον Anton Zeilinger που επέτυχε απόσταση 600 μέτρων μέσω οπτικής ίνας πάνω από τον ποταμό Δούναβη [157]. Αυτή η απόσταση βελτιώθηκε σε 1,3 χιλιόμετρα στο [158]. Σημαντικές πειραματικές προόδους στα δίκτυα κβαντικής τηλεμεταφοράς έχουν βελτιώσει την απόσταση σε ευθεία σε 8,2 χιλιόμετρα [159] και 100 χιλιόμετρα [160].

Μια μεγαλύτερη απόσταση - 144 χιλιόμετρα μεταξύ των νησιών La Palma και Tenerife - της τηλεμεταφοράς επετεύχθη από μια ομάδα του Anton Zeilinger το 2012 χρησιμοποιώντας ένα κανάλι ελεύθερου χώρου [161]. Με τις προόδους στην τεχνολογία δορυφόρων, η τηλεμετάδοση σε απόσταση μεγαλύτερη των 1200 χιλιομέτρων έχει πραγματοποιηθεί με επιτυχία με τον εκτοξευτή του δορυφόρου Micius από την ομάδα του Jian-Wei Pan και της Κίνας [162].



Εικόνα 21: Κβαντική Τηλεμεταφορά: Η Alice κρατά την κατάσταση του ζεύγους $|\Phi^+\rangle_A$ και ο Bob κρατά την κατάσταση $|\Phi^+\rangle_B$. Η μέτρηση της κατάστασης Bell και των δεδομένων του qubit ως ζεύγος $|\phi_D\rangle |\Phi^+\rangle_A$ τελειώνει από την Alice με το αποτέλεσμα να ανακτάται σε κλασσικά bits X και Y όπως φαίνονται παραπάνω. Πειράζοντας τα X και Y που στέλνονται στον Bob, η αρχική κατάσταση της $|\phi_D\rangle$ ανακτάται.

- 1) Σύνδεσμος κβαντικού καναλιού, για τη δημιουργία συνδεδεμένου ζευγαριού EPR και τη διανομή του μεταξύ των κόμβων πηγής και προορισμού.
- 2) Σύνδεσμος κλασσικού καναλιού, για τη μετάδοση δύο κλασσικών bit από έναν κόμβο πηγής σε έναν κόμβο προορισμού για την αποστολή του αποτελέσματος μέτρησης του qubit πηγής.

Η κβαντική τηλεμετάδοση δεν είναι απλή για εφαρμογή, πράγμα που επιφέρει αποδοτική επικοινωνία και πιστότητα του συστήματος. Ωστόσο, ταυτόχρονα, εμπλέκει διαδικασίες λόγω απώλειας φωτονίων στο περιβάλλον ή αποδοτική επεξεργασία της τηλεμετάδοσης. Συνεπώς, η τεχνολογία που επιλέγεται για την κβαντική τηλεμετάδοση παίζει έναν ισχυρό ρόλο στη βελτίωση της αξιοπιστίας του συστήματος και στη μείωση της αποδοτικότητας [163]. Η διαδικασία της τηλεμετάδοσης αρχίζει με τον κόμβο πηγής Alice που

κατέχει ένα άγνωστο qubit δεδομένων $|\varphi_D\rangle = \alpha|0\rangle + \beta|1\rangle$, και ένα ζευγάρι EPR που μοιράζεται μεταξύ της Alice και του Bob. Ας υποθέσουμε το ζευγάρι Bell να είναι $|\Phi^+\rangle$. Το qubit του ζευγαριού Bell, στο οποίο η Alice κρατάει το qubit που συμβολίζεται ως $|\Phi^+\rangle_A$ και το άλλο ζευγάρι qubit που κρατάει ο Bob συμβολίζεται ως $|\Phi^+\rangle_B$. Η διαδικασία της τηλεμετάδοσης μεταξύ της Alice και του Bob είναι ως εξής:

1) Η κατάσταση Bell $|\Phi^+\rangle$ προετοιμάζεται από την Alice και τον Bob, έτσι ώστε καθένας από αυτούς να κρατάει το qubit αυτού του ζευγαριού EPR. Η Alice κρατάει την κατάσταση $|\Phi^+\rangle_A$ και ο Bob κρατάει την κατάσταση $|\Phi^+\rangle_B$ του ζευγαριού.

2) Ταυτόχρονα, η κατάσταση που πρόκειται να τηλεμεταφερθεί, δηλαδή $|\varphi_D\rangle$, αποκτάται από την Alice.

3) Η μέτρηση της κατάστασης Bell και του qubit δεδομένων ως ένα ζευγάρι $|\varphi_D\rangle|\Phi^+\rangle_A$ πραγματοποιείται από την Alice και το αποτέλεσμα της μέτρησης, αποθηκευμένο σε δύο κλασικά bit, στέλνεται στον προορισμό του Bob μέσω του κλασικού συνδέσμου.

4) Ο Bob επεξεργάζεται τα ληφθέντα κλασικά bit και εφαρμόζει διορθώσεις στην κατεύθυνση X ή Z ανάλογα.

5) Τέλος, η κατάσταση qubit του Bob $|\Phi^+\rangle_B$ κρατάει τώρα την ίδια κατάσταση κβαντικής με την κατάσταση $|\varphi_D\rangle$ της Alice. Αυτό ολοκληρώνει τη διαδικασία της τηλεμετάδοσης του qubit δεδομένων μεταξύ των τελικών κόμβων της Alice και του Bob.

Κατά τη διάρκεια της διαδικασίας μέτρησης, η σύνδεση του ζευγαριού EPR καταστρέφεται, επομένως πρέπει να σημειωθεί ότι για τηλεμετάδοση ενός άλλου qubit δεδομένων, πρέπει να δημιουργηθεί και να διανεμηθεί άλλο ζευγάρι EPR. Επομένως, μπορεί να διαπιστωθεί ότι η κβαντική συγκέντρωση είναι ένα σημαντικό κβαντικό αποτέλεσμα, καθώς είναι θεμελιώδης προϋπόθεση για τη μετάδοση του σωματιδίου που αποθηκεύει το qubit. Είναι ζωτικής σημασίας να εξεταστούν οι τεχνολογίες για τη δημιουργία και διανομή των qubits. Δεδομένου ότι η Alice και ο Bob αντιπροσωπεύουν απομακρυσμένους κόμβους, η δημιουργία σύνδεσης που λαμβάνει χώρα σε ένα μέρος πρέπει να συμπληρώνεται με τη δυνατότητα διανομής της σύνδεσης, μεταφέροντας το συνδεδεμένο qubit προς τον προορισμό. Λαμβάνοντας υπόψη αυτό, είναι πολύ πιθανό να υιοθετηθούν φωτόνια ως παροχή εν σύνδεσης [164]. Ο λόγος για αυτήν την επιλογή βρίσκεται στα πλεονεκτήματα που προσφέρουν τα φωτόνια για τη διανομή εν σύνδεσης [165], μαζί με το ελάχιστο αλληλεπίδραση με το περιβάλλον, το ομαλό έλεγχο με βασικά οπτικά εξαρτήματα καθώς και την υψηλή ταχύτητα χαμηλών απωλειών μετάδοσης σε απομακρυσμένους κόμβους.

Μαθηματικές Λεπτομέρειες: Για λόγους σαφήνειας, ας αναλύσουμε τις μαθηματικές λεπτομέρειες της διαδικασίας τηλεμεταφοράς της κβαντικής. Η είσοδος είναι το κβιτιδιακό κατάσταση $|\varphi D\rangle$ που πρόκειται να μεταφερθεί από την Alice στον Bob. Απαιτούνται ζεύγη EPR της κατάστασης Bell $|\Phi+\rangle$ να βρίσκονται στην κατοχή και της Alice και του Bob.

- Η καθολική κατάσταση της Alice και του Bob αναπαρίσταται από το $|\psi D\rangle$, το οποίο είναι τονικό γινόμενο του $|\varphi D\rangle$ και του $|\Phi+\rangle$ δοθέντος από: $|\psi D\rangle = |\varphi D\rangle \otimes |\Phi+\rangle$

Εδώ, το $\otimes$ αναπαριστά τονικό γινόμενο, $|\varphi D\rangle$ είναι η κατάσταση του κβιτιδίου δεδομένων, και $|\Phi+\rangle$ είναι η κατάσταση Bell. Η καθολική κατάσταση $|\psi D\rangle$ αποτυπώνει τη συνδυασμένη κατάσταση του κβαντικού σωματιδίου και της κατάστασης Bell για τη διαδικασία της τηλεμεταφοράς.

Έτσι έχουμε :

$$|\psi D\rangle = a|0\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta|1\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Και στη συνέχεια

$$|\psi D\rangle = \frac{a|000\rangle + a|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$$

Στη συνέχεια η Alice εφαρμόζει CNOT στα qubits που κατέχει το $|10\rangle$ αντιστοιχεί στο $|11\rangle$ και το αποτέλεσμα είναι:

$$|\psi D\rangle \geq \frac{(a|000\rangle + a|011\rangle + \beta|100\rangle + \beta|111\rangle)}{\sqrt{2}}$$

Έπειτα η Alice εφαρμόζει την πύλη Hadamard στο $|\varphi D\rangle$ όπου το $|0\rangle$ αντιστοιχεί

σε $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ και το $|1\rangle$ σε $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ με αποτέλεσμα:

$$|\psi D\rangle = \frac{(\alpha|000\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle)}{2}$$

Τέλος έχουμε:

$$|\psi D\rangle = \frac{(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle))}{2}$$

- Στη συνέχεια, η Alice εφαρμόζει τη συνδυασμένη μέτρηση στο ζεύγος των qubits που κατέχει και έχει πιθανότητα 25% να πάρει κάθε ένα από τα συνδυασμούς $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
- Το αποτέλεσμα της μέτρησης της Alice επηρεάζει αμέσως την κατάσταση του qubit του Bob, ανεξαρτήτως της απόστασης μεταξύ τους, καθώς τα ζεύγη είναι συγκεκριμένα.
- Ο Bob μπορεί να ανακτήσει την αρχική κατάσταση του κβαντικού σωματιδίου $|\Phi_D\rangle$ μετά από τη χειρισμό των κλασικών ψηφίων, που λαμβάνει μέσω κλασικού συνδέσμου, έχοντας τις πληροφορίες από τη μέτρηση της Alice.
- Εάν το αποτέλεσμα της μέτρησης της Alice είναι $|00\rangle$, τότε η κατάσταση του κβαντικού σωματιδίου του Bob είναι $\alpha|0\rangle + \beta|1\rangle$. Έτσι, το qubit του Bob ακολουθεί την αρχική κβαντική κατάσταση $|\Phi_D\rangle$ και δεν απαιτείται καμία επιπλέον λειτουργία. Εάν η συνδυασμένη μέτρηση της Alice είναι $|01\rangle$, το αποτέλεσμα της μέτρησης του Bob είναι $\alpha|1\rangle + \beta|0\rangle$. Έτσι, ο Bob ανακτά την αρχική κβαντική κατάσταση $|\Phi_D\rangle = \alpha|0\rangle + \beta|1\rangle$ εφαρμόζοντας τη λειτουργία Pauli-X. Παρόμοια, για τη μέτρηση της Alice $|10\rangle$ και $|11\rangle$, ο Bob ανακτά ξανά την αρχική κατάσταση εφαρμόζοντας συγκεκριμένες λειτουργίες πυλών. Αυτό ολοκληρώνει με επιτυχία τη διαδικασία της τηλεμεταφοράς κβαντικών σωματιδίων μεταξύ της Alice και του Bob.
- Μετά από όλα αυτά, μπορεί να συμπεραθεί ότι η διαδικασία της τηλεμεταφοράς υπακούει στην ταχύτητα του φωτός, διατηρώντας έτσι τη θεωρία της σχετικότητας.

2.4.2 Θεώρημα μη κλωνοποίησης

Αυτό το θεώρημα, το οποίο διατυπώθηκε πρώτα από τους Wootters, Zurek και Deiks το 1982 [166], δηλώνει ότι η κβαντική κατάσταση οποιασδήποτε σωματιδίου που μεταφέρει ένα qubit σε ένα κβαντικό κανάλι δεν μπορεί ούτε να αντιγραφεί, ούτε να ενισχυθεί, ούτε να κλωνοποιηθεί, κάνοντάς το έτσι ένα αξιόπιστο και ασφαλές μέσο επικοινωνίας. Οποιαδήποτε προσπάθεια αντιγραφής της θα ανιχνευθεί, ενεργοποιώντας περαιτέρω το πρωτόκολλα QKD [167]. Ωστόσο, ταυτόχρονα, το Θεώρημα μη κλωνοποίησης ή No-Cloning εμποδίζει τα qubits να σταλούν σε μεγάλες αποστάσεις μέσω ενίσχυσης ή αποστολής αντιγράφων των qubits, όπως γίνεται στην κλασική επικοινωνία, για την αποτελεσματική ανίχνευση bits χωρίς απώλεια πληροφοριών. Για αυτόν τον σκοπό, μελετώνται οι κβαντικοί επαναλήπτες για την επίλυση του προβλήματος της επικοινωνίας qubits

σε μεγάλες αποστάσεις, που είναι η καίρια λειτουργία που απαιτείται για την πλήρη κλίμακα του κβαντικού Διαδικτύου.

Για κάθε άγνωστη κβαντική κατάσταση $|\psi\rangle$, δεν υπάρχει μια μοναδική πράξη U που μπορεί να αντιγράψει αυτή την κατάσταση, δηλαδή δεν υπάρχει U τέτοια ώστε

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle, \text{ για όλες τις δυνατές καταστάσεις } |\psi\rangle.$$

Απόδειξη: Ας υποθέσουμε ότι θέλουμε να αντιγράψουμε το $|\psi\rangle = \alpha|0\rangle + b|1\rangle$ όπου φυσικά ισχύει $\alpha^2 + b^2 = 1$

Έστω ότι υπάρχει κάποια (άγνωστη) κβαντική πύλη η οποία προφανώς επιδρά σε 2 qubits (θέλουμε να αντιγράψουμε το πρώτο στο δεύτερο) τέτοια ώστε $U|\psi 0\rangle \rightarrow |\psi\psi\rangle$.

$$U|00\rangle \rightarrow |00\rangle \text{ και } U|10\rangle \rightarrow |11\rangle$$

$$\text{Όμως: } |\psi\psi\rangle = |\psi\rangle \otimes |\psi\rangle = \begin{pmatrix} \alpha \\ b \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ b \end{pmatrix} = \begin{pmatrix} \alpha\alpha \\ \alpha b \\ b\alpha \\ bb \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha b \\ b\alpha \\ b^2 \end{pmatrix} = \alpha^2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} +$$

$$\alpha b \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + b\alpha \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + b^2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} =$$

- $\alpha^2|00\rangle + \alpha b|01\rangle + b\alpha|10\rangle + b^2|11\rangle$
- Όμως: $U(|\psi\rangle \otimes |0\rangle) = U(\alpha|0\rangle + b|1\rangle \otimes |0\rangle) =$
- $U(\alpha|0\rangle \otimes |0\rangle) + U(b|1\rangle \otimes |0\rangle) = \alpha|00\rangle + b|11\rangle$ αλλά
- $\alpha|00\rangle + b|11\rangle \neq \alpha^2|00\rangle + \alpha b|01\rangle + b\alpha|10\rangle + b^2|11\rangle$

Δηλαδή παίρνουμε δύο διαφορετικά αποτελέσματα αντιγραφής (κλωνοποίησης) εάν απλά χρησιμοποιήσουμε διαφορετική μαθηματική προσέγγιση. Φυσικά αυτό είναι αδύνατο και κατά συνέπεια δεν υπάρχει τρόπος αντιγραφής (κλωνοποίησης) μίας άγνωστης κβαντικής κατάστασης.

3 Τα βασικά της Python

Σε αυτό το κεφάλαιο θα κάνουμε μια μικρή εισαγωγή στην γλώσσα προγραμματισμού Python, πως μπορούμε να την χρησιμοποιήσουμε καθώς και να την εγκαταστήσουμε. Επειδή δεν είναι εφικτό να τρέξουμε κβαντικά προγράμματα σε κανονικό υπολογιστή θα χρησιμοποιήσουμε το Jupiter Notebook. Το οποίο είναι ένα πρόγραμμα που μας βοηθάει να τρέξουμε την python μέσα στο περιβάλλον του notebook τρέχοντας έτσι με τη βοήθεια του το κβαντικό πρόγραμμα. Θα ακολουθήσουμε και μερικά παραδείγματα πάνω στην python για την καλύτερη εμπέδωση της .

3.1 Τι είναι η Python

Η Python [168], [Εικόνα 22], είναι μια δυναμική γλώσσα προγραμματισμού υψηλού επιπέδου, γενικής χρήσης και τα μοντέρνα χαρακτηριστικά της την κάνουν κατάλληλη ως πρώτη γλώσσα προγραμματισμού. Κατατάσσεται σταθερά ως μία από τις πιο δημοφιλείς γλώσσες προγραμματισμού. Σχεδιάστηκε κυρίως για αναγνωσιμότητα, την κομψότητα, την ευ-χρηστία της καθώς και την απλότητα του συντακτικού της καθώς επιτρέπει στους προ-γραμματιστές να δημιουργήσουν μικρότερο κώδικα σε σχέση με άλλες γλώσσες προ-γραμματισμού, όπως είναι η java και η C++.



Εικόνα 22: Python

Αυτή η γλώσσα προγραμματισμού είναι αντικειμενοστραφής, δηλαδή ο τρόπος και οι τεχνικές προγράμματος, μέσω μια δομής δεδομένων του είναι αυτόνομη με δικά της χαρακτηριστικά. Η Python διαθέτει μεταγλωττιστές (compilers) και διερμηνευτές (interpreters) για να επεξεργάζεται τη μετατροπή του κώδικα σε «γλώσσα μηχανής» ώστε να εκτελεστεί από τον Η/Υ (στην περίπτωση της Python η επεξεργασία πραγματοποιείται από διερμηνευτή). Θεωρείται μια γλώσσα προγραμματισμού απλή, ισχυρή και μεσαίου επιπέδου.

Η Python είναι επεκτάσιμη και ενσωματωμένη. Αν χρειαζόμαστε ένα σημαντικό κομμάτι κώδικα να «τρέχει» πολύ γρήγορα ή αν πρέπει να έχουμε ένα κομμάτι ενός αλγορίθμου που να μην είναι ανοικτό, τότε μπορούμε να προγραμματίσουμε εκείνο το κομμάτι σε C ή C++ και στη συνέχεια να το χρησιμοποιήσουμε από το Python πρόγραμμά μας. Αξίζει να σημειωθεί ότι η αναγνωσιμότητα στον προγραμματισμό σημαίνει η ευκολία με την οποία ένας χρήστης μπορεί να κατανοήσει το σκοπό, τον έλεγχο της ροής και τη λειτουργία του πηγαίου κώδικα. Είναι πολύ σημαντική λόγω του γεγονός ότι οι προγραμματιστές αντί να συντάσσουν καινούργιο κώδικα, αφιερώνουν πολύ χρόνο προσπαθώντας να κατανοήσουν, να επαναχρησιμοποιήσουν και τροποποιήσουν τον κώδικα, που πολλές φορές μπορεί να τους οδηγήσει σε σφάλματα.

3.1.1 Τι κάνει η Python και Πώς μπορεί να χρησιμοποιηθεί αυτή η γλώσσα προγραμματισμού;

- Η Python χρησιμοποιείται για τη δημιουργία διαδικτυακών εφαρμογών (web applications) καθώς και την ανάπτυξη λογισμικού για τη δημιουργία διάφορων εργασιών.
- Η Python είναι εφικτό να συνδεθεί με συστήματα βάσεων δεδομένων (database systems), να διαβάσει ή και να τροποποιεί αρχεία.
- Η Python μπορεί να διαχειριστεί αρχεία μεγάλου όγκου δεδομένων.
- Η Python είναι δυνατόν να εκτελέσει πολύπλοκες μαθηματικές πράξεις
- Η Python μπορεί να χρησιμοποιηθεί για ταχύτερη δημιουργία πρωτοτύπων ή σε συνδυασμό για ανάπτυξη λογισμικού έτοιμου για παραγωγή.

3.1.2 Γιατί να χρησιμοποιήσουμε την Python

- Μόνο η Python μέχρι σήμερα διαθέτει βιβλιοθήκες που επιτρέπουν τον κβαντικό προγραμματισμό , οι οποίες αναπτύχθηκαν από πολύ μεγάλες εταιρίες όπως η IBM, Google κλπ.
- Η Python διαθέτει διερμηνέα (interpreter) αλλά και μεταγλωττιστή (compiler) ταυτόχρονα. Μπορεί να χρησιμοποιηθεί σε διαφορετικές πλατφόρμες όπως Windows, Linux, Mac, Raspberry, κ.λπ., γι' αυτό και αποτελεί την πιο χρησιμοποιούμενη γλώσσα προγραμματισμού σήμερα.
- Είναι ελεύθερου λογισμικού ανοικτού κώδικα, δηλαδή μπορούμε να διανείμουμε ελεύθερα αντίγραφα αυτού του λογισμικού, να διαβάσουμε τον πηγαίο κώδικα, να πραγματοποιήσουμε αλλαγές σε αυτό καθώς και να χρησιμοποιήσουμε «κομμάτια» του κώδικα σε νέα δωρεάν προγράμματα. Βασίζεται στην ιδέα μιας κοινότητας που μοιράζεται τη γνώση και έτσι βελτιώνεται συνεχώς.
- Η σύνταξή της είναι απλή, είναι κατάλληλη για αρχάριους και έμπειρους προγραμματιστές, μοιάζει με την αγγλική γλώσσα με επιρροή από τα μαθηματικά, γι' αυτό και η εκμάθησή της είναι κατανοητή και γρήγορη.
- Η Python προτείνεται ως μια πολύ καλή σύγχρονη γλώσσα με στοιχεία Διαδικτύου για μαθητές Γυμνασίου και Λυκείου, που αρχίζουν να μαθαίνουν προγραμματισμό H/Y.
- Παρέχει τη δυνατότητα να γράφονται προγράμματα σε λιγότερες γραμμές κώδικα συγκριτικά με άλλες γλώσσες προγραμματισμού.
- Διαθέτει τεράστια ποικιλία από βιβλιοθήκες που διευκολύνουν ιδιαίτερα πολλές εργασίες.
- Η Python εκτελείται σε ένα σύστημα διερμηνέα (compiler) γρήγορα, συνεπώς μόλις συνταχθεί ο κώδικας εκτελείται αμέσως.
- Είναι ταυτόχρονα διαδικαστική, αντικειμενοστραφής αλλά και συναρτησιακή.

Γνωστές Εμπορικές Εφαρμογές Γραμμένες σε Python:

- YouTube
- Facebook
- Dropbox
- Google (Μεγάλη χρήση της σε βασικές εφαρμογές)

- Instagram
- Bit Torrent (Προηγούμενη Έκδοση)
- Second Life

3.2 Ιστορία της Python

Η Python δημιουργήθηκε από τον Guido van Rossum και κυκλοφόρησε για πρώτη φορά το 1991. Δίνει προτεραιότητα στην αναγνωσιμότητα και την ευκολία χρήσης. Η γλώσσα εξελίχθηκε μέσω εκδόσεων όπως η Python 2 και η Python 3, με την Python 3 να εισάγει σημαντικές βελτιώσεις αλλά να προκαλεί προβλήματα συμβατότητας προς τα πίσω. Η Python απέκτησε μια τεράστια κοινότητα και δημοτικότητα στην ανάπτυξη του ιστού, την επιστήμη δεδομένων, την τεχνητή νοημοσύνη και πολλά άλλα. Η συνταξιοδότηση του Guido van Rossum το 2018 οδήγησε σε ένα μοντέλο διακυβέρνησης με γνώμονα την κοινότητα. Η Python παραμένει μια ευέλικτη και ευρέως χρησιμοποιούμενη γλώσσα προγραμματισμού.

3.3 Παραδείγματα στην Python

Print Statements:

1) Print()

Η συνάρτηση `print()` χρησιμοποιείται για την εμφάνιση εξόδου στην κονσόλα. Μπορείτε να παρέχετε τιμές, μεταβλητές ή εκφράσεις μέσα στις παρενθέσεις. Η έξοδος θα εμφανιστεί στην οθόνη.

```
print("Hello, World!")
```

2) Variables and Data Types Μεταβλητές και τύποι δεδομένων:

Οι μεταβλητές χρησιμοποιούνται για την αποθήκευση δεδομένων. Στην Python, μπορείτε να εκχωρήσετε τιμές σε μεταβλητές χωρίς να προσδιορίσετε ρητά τους τύπους δεδομένων τους. Η Python συνάγει αυτόματα τον τύπο δεδομένων με βάση την εκχωρημένη τιμή.

```
age = 25 # Integer
height = 5.9 # Float
name = "John" # String
is_student = True # Boolean
```

3) Αριθμητικές πράξεις:

Η Python υποστηρίζει διάφορες αριθμητικές πράξεις για αριθμούς όπως πρόσθεση, αφαίρεση, πολλαπλασιασμό και διαίρεση.

```
a = 10
b = 5
addition = a + b
subtraction = a - b
multiplication = a * b
division = a / b
```

4) Οι συμβολοσειρές Strings είναι ακολουθίες χαρακτήρων. Περικλείονται είτε σε μονά είτε σε διπλά εισαγωγικά.

```
message = "Hello, Python!"
```

5) Οι λίστες Lists είναι ταξινομημένες συλλογές που μπορούν να αποθηκεύσουν πολλές τιμές, ακόμη και διαφορετικών τύπων, σε μία μόνο μεταβλητή.

```
numbers = [1, 2, 3, 4, 5]
names = ["Alice", "Bob", "Charlie"]
```

6) Conditional Statements

Οι δηλώσεις υπό όρους σας επιτρέπουν να λαμβάνετε αποφάσεις στον κώδικά σας. εάν χρησιμοποιούνται δηλώσεις για τον έλεγχο συνθηκών και την εκτέλεση διαφορετικών μπλοκ κώδικα με βάση το αν η συνθήκη είναι True ή False.

```
if age >= 18:
    print("You are an adult.")
else:
    print("You are a minor.")
```

7) Loops Βρόχοι:

Οι βρόχοι χρησιμοποιούνται για την επανάληψη ενός μπλοκ κώδικα πολλές φορές. for οι βρόχοι επαναλαμβάνονται σε μια ακολουθία (όπως μια λίστα), ενώ ενώ οι βρόχοι συνεχίζονται μέχρι να ικανοποιηθεί μια συγκεκριμένη συνθήκη.

```
for number in numbers:
    print(number)
count = 0
while count < 5:
    print("Count:", count)
    count += 1
```

8) Functions Λειτουργίες:

Οι συναρτήσεις είναι επαναχρησιμοποιήσιμα μπλοκ κώδικα που μπορούν να κληθούν με διαφορετικές εισόδους. Βοηθούν στην οργάνωση και τη διαμόρφωση κώδικα.

```
def greet(name):  
    print("Hello, ", name)  
greet("Alice")
```

9) Lists and Dictionaries: Λίστες και λεξικά:

Οι λίστες είναι συλλογές στοιχείων, ταξινομημένων με βάση το ευρετήριό τους.

Τα λεξικά, από την άλλη πλευρά, αποθηκεύουν στοιχεία ως ζεύγη κλειδιού-τιμής.

Μπορείτε να χρησιμοποιήσετε ένα κλειδί για πρόσβαση στην αντίστοιχη τιμή.

```
fruits = ["apple", "banana", "orange"]  
person = {"name": "John", "age": 30}
```

10) Comments Σχόλια:

Τα σχόλια χρησιμοποιούνται για να εξηγήσουν τον κώδικα και να τον κάνουν πιο κατανοητό. Στην Python, τα σχόλια μιας γραμμής συμβολίζονται με # και τα σχόλια πολλαπλών γραμμών μπορούν να γραφτούν χρησιμοποιώντας τριπλά εισαγωγικά (''' ή """).

```
# This is a single-line comment  
'''  
This is a multi-line comment.  
It can span multiple lines.  
'''
```

3.4 QISKIT, JUPITER NOTEBOOK, ANACONDA PYTHON

Το Anaconda, το Jupyter Notebook και το Qiskit είναι όλα εργαλεία που χρησιμοποιούνται συνήθως στον τομέα των κβαντικών υπολογιστών και της επιστήμης της κβαντικής πληροφορίας. Ας αναλύσουμε το καθένα από αυτά:

Anaconda:

Το Anaconda είναι μια διανομή της γλώσσας προγραμματισμού Python ειδικά σχεδιασμένη για την επιστήμη των δεδομένων και την επιστημονική πληροφορική. Έρχεται με έναν διαχειριστή πακέτων που ονομάζεται Conda, ο οποίος απλοποιεί τη διαδικασία εγκατάστασης, διαχείρισης και ενημέρωσης διαφόρων βιβλιοθηκών και πακέτων. Χρησιμοποιείται ευρέως στην κοινότητα της επιστήμης δεδομένων λόγω της ευκολίας διαχείρισης πακέτων και της υποστήριξής του για επιστημονικές βιβλιοθήκες. Η εγκατάσταση της γίνεται από την επίσημη σελίδα: <https://www.anaconda.com/>

Jupyter Notebook:

Το Jupyter Notebook είναι μια εφαρμογή web ανοιχτού κώδικα που επιτρέπει την δημιουργία και τον μοιρασμό εγγράφων που περιέχουν κώδικα, εξισώσεις, απεικονίσεις και αφηγηματικό κείμενο. Υποστηρίζει διάφορες γλώσσες προγραμματισμού, αλλά χρησιμοποιείται ευρέως στην κοινότητα της Python. Τα σημειωματάρια μπορούν να χρησιμοποιηθούν για ανάλυση δεδομένων, μηχανική μάθηση και για διαδραστικούς υπολογιστές. Με τα σημειωματάρια Jupyter, δίνεται η δυνατότητα να εκτέλεσης κβαντικής προσομοίωσης σε κώδικα Qiskit για την εκτέλεση κβαντικών προγραμμάτων. Η εγκατάσταση της γίνεται από την επίσημη σελίδα: <https://jupyter.org/>

Qiskit:

Το Qiskit είναι ένα πακέτο ανάπτυξης λογισμικού κβαντικών υπολογιστών ανοιχτού κώδικα που αναπτύχθηκε από την IBM. Παρέχει εργαλεία για εργασία με κβαντικά κυκλώματα, αλγόριθμους και συσκευές υλικού. Το Qiskit είναι γραμμένο σε Python και μπορεί να χρησιμοποιηθεί στα σημειωματάρια Jupyter. Επιτρέπει στους χρήστες να σχεδιάζουν και να προσομοιώνουν κβαντικά κυκλώματα, να εκτελούν κβαντικούς αλγόριθμους σε προσομοιωτές, ακόμη και να τους εκτελούν σε πραγματικό κβαντικό υλικό που παρέχεται από την IBM Quantum Experience.

3.4.1 Πως συνεργάζονται

Το Qiskit είναι ένα πακέτο κιτ ανάπτυξης λογισμικού ανοιχτού κώδικα (SDK) για εργασία με κβαντικούς υπολογιστές σε επίπεδο κυκλωμάτων, παλμών και αλγορίθμων. Το Qiskit ιδρύθηκε από την IBM Research για να επιτρέψει την ανάπτυξη λογισμικού για

την υπηρεσία κβαντικού υπολογιστικού νέφους, IBM Quantum Experience.[2][3], συμπεριλαμβανομένων προσομοιωτών και πραγματικών κβαντικών συσκευών. Παρέχει εργαλεία για τη δημιουργία και το χειρισμό κβαντικών προγραμμάτων και την εκτέλεσή τους σε πρωτότυπες κβαντικές συσκευές στην IBM Quantum Platform ή σε προσομοιωτές σε τοπικό υπολογιστή. Ακολουθεί το μοντέλο κυκλώματος για καθολικούς κβαντικούς υπολογισμούς και μπορεί να χρησιμοποιηθεί για οποιοδήποτε κβαντικό υλικό (προς το παρόν υποστηρίζει υπεραγωγία qubits και παγιδευμένα ιόντα)[1]. Μέσω του Qiskit εκτελούμε τα κβαντικά κυκλώματά σας σε συσκευές IBM Quantum απευθείας από ένα Notebook Jupyter. Για την πρόσβαση στο Qiskit Quantum Experience θα πρέπει να δημιουργήσουμε λογαριασμό στο site: <https://quantum.ibm.com/> και αφού μας δοθεί το μοναδικό id token θα είμαστε έτοιμοι να τρέχουμε κβαντικά προγράμματα σε python. Στην πραγματικότητα όταν τρέχουμε ένα πρόγραμμα σε python στο Jupiter notebook αφού πατήσουμε shift-enter για να δούμε το αποτέλεσμα , με την βοήθεια του api id token μας δεσμεύουμε έναν κβαντικό υπολογιστή της IBM με σκοπό να τρέξει το πρόγραμμα και στη συνέχεια στέλνει τα αποτελέσματα των προγραμμάτων που θα γράψαμε οπτικοποιούμενα με την βοήθεια του Jupiter Notebook στην οθόνη μας.

3.4.2 Εγκατάσταση Qiskit στο Jupiter Notebook

- Προετοιμασία για το τρέξιμο προγραμμάτων
- Ανοίγουμε το Jupiter notebook
- Ανοίγουμε νέο παράθυρο new Python file
- Εκτελούμε την εντολή `import qiskit` (για την εισαγωγή του qiskit) και shift-enter
- Εκτελούμε την εντολή `qiskit.__qiskit_version__` για τον έλεγχο της έκδοσης
- Αφού γνωρίζουμε το μοναδικό μας API TOKEN του λογαριασμού μας της IBM
- Εκτελούμε: `from qiskit import IBMQ`
- Εκτελούμε: `IBMQ.save_account(' εδώ γράφουμε τον κωδικό του API TOKEN ' )`
- Συνδεθήκαμε !

4 Πρακτικό μέρος

4.1 Προσομοίωση BB84 protocol σε κβαντικό υπολογιστή

Σε αυτό το κεφάλαιο αναλύονται τα βήματα για την ανάπτυξη του κώδικα, ο κώδικας της εφαρμογής του πρωτοκόλλου BB84 σε γλώσσα Python και η αναπαρίσταται το αποτέλεσμα της. Θα αναλύσουμε τρία πειράματα 1^ο: Η κωδικοποίηση της Alice και η μέτρηση του Bob χρησιμοποιώντας την ίδια βάση, 2^ο: Προσομοίωση του BB84 χωρίς την Eve να εφαρμόζει τεχνική επίθεσης eavesdrop, 3^ο Προσομοίωση του BB84 με την Eve να κάνει επίθεση με την τεχνική eavesdropping.

-Αρχικά θα πρέπει να ανοίξουμε το Jupiter Notebook και από εκεί να επιλέξουμε “New” και “Python 3” (ipykernel).

-Στη συνέχεια θα δημιουργήσουμε δύο text files στο Jupiter Notebook παντώντας “New” και “Text File”. Θα γράψουμε τον κώδικα στο καθένα και ύστερα θα τα αποθηκεύσουμε σε μορφή “.py”.

1ο αρχείο κώδικα: BB84Test.py

```
import numpy as np
from qiskit import QuantumCircuit, Aer
from qiskit.visualization import plot_histogram
## Για την αναπαράσταση
from IPython.display import display
# Δημιουργία κβαντικού κυκλώματος
qc = QuantumCircuit(1,1)
# Η Alice κωδικοποιεί το qubit
qc.barrier()
# Ο Bob λαμβάνει το qubit και κάνει μέτρηση
qc.measure(0,0)
# Σχεδίαση και προσομοίωση κυκλώματος
display(qc.draw())
aersim = Aer.get_backend('aer_simulator')
job = aersim.run(qc, shots=1000)
counts = job.result().get_counts()
print("Total counts:", counts)
plot_histogram(counts)
```

Κώδικας: κβαντικό κύκλωμα του BB84.

Αρχικά εισάγουμε την βιβλιοθήκη numpy για αριθμητικούς υπολογισμούς και κάποιες κλάσεις για την αναπαράσταση και οπτικοποίηση του κβαντικού κυκλώματος. Έπειτα

δημιουργούμε ένα κβαντικό κύκλωμα (qc)= QuantumCircuit(1, 1) με ένα qubit και ένα κλασικό bit. Το πρώτο όρισμα είναι ο αριθμός των qubit και το δεύτερο όρισμα είναι ο αριθμός των κλασικών bit. Στη συνέχεια η Alice κωδικοποιεί το qubit , εισάγοντας ένα φράγμα στο κβαντικό κύκλωμα. Είναι ένα οπτικό βοήθημα για τον διαχωρισμό διαφορετικών τμημάτων του κυκλώματος. Ο Bob προσθέτει μια πράξη μέτρησης στο κβαντικό κύκλωμα. Μετρά το qubit (qubit 0) και αποθηκεύει το αποτέλεσμα στο κλασικό bit (bit 0). Τέλος αναπαριστούμε το κύκλωμα με το display.

Aer.get_backend('aer_simulator'): Ανακτά το backend του προσομοιωτή Aer για προσομοίωση κβαντικού κυκλώματος.

aersim.run(qc , shots=1000): Εκτελεί το κβαντικό κύκλωμα qc στον προσομοιωτή για 1000 (μετρήσεις).

job.result().get_counts(): Ανακτά τα αποτελέσματα των μετρήσεων και τις συχνότητές τους από τα αποτελέσματα της προσομοίωσης.

2ο αρχείο κώδικα: BB84.py

```
from numpy.random import randint
import numpy as np
from qiskit import QuantumCircuit, transpile, Aer
from qiskit.providers.aer import QasmSimulator
from qiskit.visualization import plot_histogram
## Για την αναπαράσταση
from IPython.display import display
np.random.seed(seed=23)
n = 4
four_times_n = 4 * n
def encode_message(bits, bases):
    message = []
    for i in range(four_times_n):
        qc = QuantumCircuit(1,1)
        if bases[i] == 'V': # Ετοιμασία qubit στην κατεύθυνση V το οποίο είναι η βάση Z
            if bits[i] == 0:
                pass
            else:
                qc.x(0)
        else: # Ετοιμασία του qubit στην κατεύθυνση H το οποίο είναι η βάση X
            if bits[i] == 0:
                qc.h(0)
            else:
                qc.x(0)
                qc.h(0)
        qc.barrier()
        message.append(qc)
    return message
def measure_message(message, bases):
    backend = Aer.get_backend('aer_simulator')
```

```

measurements = []
for q in range(four_times_n):
    if bases[q] == 'V': # Μέτρηση στην V κατεύθυνση
        message[q].measure(0,0)
    else: # Μέτρηση στην H κατεύθυνση
        message[q].h(0)
        message[q].measure(0,0)
    aer_sim = Aer.get_backend('aer_simulator')
    job = aer_sim.run(message[q], shots=1, memory=True)
    measured_bit = int(job.result().get_memory()[0])
    measurements.append(measured_bit)
return measurements
def remove_garbage(a_bases, b_bases, bits):
    same_basis_bits = []
    for q in range(four_times_n):
        if a_bases[q] == b_bases[q]:
            # Επιλέγουμε το bit εάν χρησιμοποιούν την ίδια βάση
            same_basis_bits.append(bits[q])
    return same_basis_bits
## Step 1
# Η Alice παράγει bits
alice_bits = list(randint(2, size=four_times_n))
print("Alice bits: \n", alice_bits)

## Step 2
# Δημιουργία πίνακα ώστε να δούμε πια qubits
# κωδικοποιούνται και με ποιες βάσεις
#alice_bases = list( map(lambda bit: 'V' if bit == 0 else 'H', randint(2,
size=four_times_n))
)
dir = ['V', 'H']
alice_bases = list( map(lambda bit: dir[bit], randint(2, size=four_times_n)) )
print("Alice bases: \n", alice_bases)
message = encode_message(alice_bits, alice_bases)
## Step 3
# Αποφασίζουμε σε ποια βάση θα κάνουμε την μέτρηση:
bob_bases = list( map(lambda bit: dir[bit], randint(2, size=four_times_n))
print("Bob bases: \n", bob_bases)
bob_results = measure_message(message, bob_bases)
print("Bob results: \n", bob_results)
## Step 4
alice_bits_samebasis = remove_garbage(alice_bases, bob_bases, alice_bits)
bob_bits_samebasis = remove_garbage(alice_bases, bob_bases, bob_results)
# print("Bob's same-basis bits :\n", bob_bits_samebasis)
## Step 5: Το μέγεθος των bits όπου η Alice και ο Bob χρησιμοποιούν την ίδια βάση είναι
το πολύ 2 * n.

```

Κώδικας: Προσομοίωση του πρωτοκόλλου BB84 QKD, όπου η Alice δημιουργεί τυχαία bits, τα κωδικοποιεί σε κβαντικές καταστάσεις, ο Bob επιλέγει τυχαίες βάσεις για μέτρηση και αργότερα συγκρίνουν τα αποτελέσματά τους για να δημιουργήσουν ένα ασφαλές κλειδί.

Αρχικά εισάγουμε βιβλιοθήκες για την παραγωγή αριθμητικών πράξεων, για τον κβαντικό υπολογισμό μέσω του qiskit αλλά και για την αναπαράσταση του κώδικα.

- `np.random.seed(seed=23)`: Ορίζει έναν σταθερό σπόρο για τη δημιουργία τυχαίων αριθμών για να διασφαλίσει την αναπαραγωγικότητα.

- `four_times_n = 4 * n`: Συνολικός αριθμός bit/qubit, που είναι 16 σε αυτήν την περίπτωση, $n = 4$: Αριθμός qubits που θέλει να στείλει η Alice.
- `encode_message`: Μια λίστα για την αποθήκευση των κβαντικών κυκλωμάτων που αντιπροσωπεύουν τα κωδικοποιημένα qubits.

Η συνάρτηση επαναλαμβάνεται μέσα από κάθε bit και την αντίστοιχη βάση του.

Για κάθε qubit: Εάν η βάση είναι 'V' (Κάθετη ή Z-βάση), προετοιμάζει το qubit στην κατάσταση $|1\rangle$ εάν το bit είναι 1. Διαφορετικά, παραμένει στην κατάσταση $|0\rangle$.

Εάν η βάση είναι «H» (οριζόντια ή βάση X), προετοιμάζει το qubit σε μια υπέρθεση χρησιμοποιώντας την πύλη Hadamard ($|+\rangle$ ή $|-\rangle$ καταστάσεις).

- `measure_message`: Μια λίστα για την αποθήκευση των αποτελεσμάτων των μετρήσεων. Η συνάρτηση επαναλαμβάνεται μέσω κάθε qubit και της αντίστοιχης βάσης του.

Για κάθε qubit: Εφαρμόζει μια μέτρηση στην επιλεγμένη βάση. Προσομοιώνει τη μέτρηση και ανακτά το μετρούμενο bit. Το μετρούμενο bit προσαρτάται στη λίστα μετρήσεων.

- `same_basis_bits`: Μια λίστα για την αποθήκευση των bit που μέτρησαν η Alice και ο Bob χρησιμοποιώντας την ίδια βάση.
- `randint(2, size=four_times_n)`: Δημιουργεί έναν πίνακα `four_times_n` τυχαίων ακεραίων μεταξύ 0 (συμπεριλαμβανομένου) και 2 (αποκλειστικά), που αντιπροσωπεύουν τα bit που θέλει να στείλει η Alice.
- Η Alice δημιουργεί μια τυχαία ακολουθία bit για αποστολή στον Bob.
- Η Alice επιλέγει τυχαία μια βάση ('V' ή 'H') για κάθε bit για να κωδικοποιήσει τα qubits της.
- Ο Bob επιλέγει τυχαία βάσεις για να μετρήσει τα qubits που έλαβε από την Alice.
- Τα qubits μετρώνται από τον Bob και τα αποτελέσματα των μετρήσεων αποθηκεύονται.
- Τόσο η Alice όσο και ο Bob φιλτράρουν τα bits που μετρώνται σε διαφορετικές βάσεις, διατηρώντας μόνο τα bits που μετρώνται στην ίδια βάση.
- Ο μέγιστος αριθμός bit που μπορούν να συμφωνήσουν (μετρούμενος στην ίδια βάση) είναι το πολύ « $2 * n$ », όπου το « n » αντιπροσωπεύει τον αριθμό των

qubits που έστειλε η Alice, δημιουργώντας ένα κοινό κλειδί ασφαλείας μεταξύ τους.

Συνοπτικά:

Η Alice δημιουργεί τυχαία bit και τα κωδικοποιεί σε qubits, στέλνει τα qubits στον Bob. Ο Bob επιλέγει τυχαίες βάσεις για να μετρήσει τα qubits. Alice και ο Bob απορρίπτουν τα κομμάτια όπου χρησιμοποιούσαν διαφορετικές βάσεις. Αυτή η διαδικασία στοχεύει να δημιουργήσει ένα κοινό μυστικό κλειδί μεταξύ της Alice και του Bob για ασφαλή επικοινωνία.

Στην κβαντομηχανική, μια βάση αναφέρεται σε ένα σύνολο κβαντικών καταστάσεων που χρησιμοποιούνται για την αναπαράσταση άλλων καταστάσεων μέσω γραμμικών συνδυασμών. Η επιλογή της βάσης είναι κρίσιμη καθώς καθορίζει τον τρόπο με τον οποίο αναπαρίσταται και μετράται μια κβαντική κατάσταση. Στο πλαίσιο του πρωτοκόλλου BB84 Quantum Key Distribution (QKD), χρησιμοποιούνται συνήθως οι βάσεις 'V' (Κάθετη ή Z-βάση) και 'H' (Οριζόντια ή X-βάση).

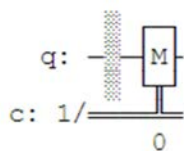
Κάθετη βάση ('V' ή Z-βάση): Σε αυτή τη βάση, οι καταστάσεις αντιπροσωπεύονται από τις ιδιοκαταστάσεις του τελεστή Pauli Z, οι οποίες συμβολίζονται ως $|0\rangle$ και $|1\rangle$. Αυτές οι καταστάσεις αντιστοιχούν στην υπολογιστική βάση σε έναν κβαντικό υπολογιστή.

Οριζόντια βάση («H» ή X-βάση): Σε αυτή τη βάση, οι καταστάσεις αντιπροσωπεύονται από τις ιδιοκαταστάσεις του τελεστή Pauli X. Οι καταστάσεις σε αυτή τη βάση συμβολίζονται ως $|+\rangle$ και $|-\rangle$, που είναι υπερθέσεις των καταστάσεων $|0\rangle$ και $|1\rangle$.

Ο όρος "κατεύθυνση" στο πλαίσιο των κβαντικών βάσεων αναφέρεται στον προσανατολισμό ή τον άξονα κατά μήκος του οποίου μετράται η κβαντική κατάσταση. Για παράδειγμα, στο πρωτόκολλο BB84, τα 'V' και 'H' αντιπροσωπεύουν διαφορετικούς προσανατολισμούς ή κατευθύνσεις στις οποίες μετρώνται τα qubits. Αντιστοιχούν σε διαφορετικές βάσεις μέτρησης που χρησιμοποιούνται από την Alice και τον Bob για την κωδικοποίηση και την αποκωδικοποίηση των κβαντικών πληροφοριών με ασφάλεια.

4.1.1 Πείραμα 1: Η κωδικοποίηση της Alice και η μέτρηση του Bob χρησιμοποιώντας την ίδια βάση

• Στο κελί, πληκτρολογούμε: `%load BB84Test.py` και κάνουμε κλικ στην "Εκτέλεση" για να φορτώσουμε ένα απλό πρόγραμμα. Σε αυτό το πρόγραμμα, η Alice προετοιμάζει και στέλνει ένα qubit με τιμή 0 στην κατακόρυφη κατεύθυνση στον Bob. Ο Bob μετρά το qubit με την ίδια κατεύθυνση. Η διαδικασία είναι όπως στο διάγραμμα παρακάτω αφού εκτελέσουμε την εντολή: `%run BB84Test.py`



- Σημείωση ότι οι διακεκομμένες γραμμές που χρησιμοποιούνται εδώ είναι απλώς ένδειξη του χωρισμού της εργασίας μεταξύ της Alice και του Bob.

Υποθέτουμε ότι η Άλις κωδικοποιεί το qubit στην οριζόντια κατεύθυνση αντί για την κατακόρυφη κατεύθυνση. Δηλαδή, εφαρμόζει την πύλη Hadamard στο qubit. Επίσης ο Μπομπ μετρά το qubit στην οριζόντια κατεύθυνση:

Τροποποιούμε τον κώδικα:

```
%load BB84Test.py

import numpy as np
from qiskit import QuantumCircuit, Aer
from qiskit.visualization import plot_histogram
## Η αναπαράσταση
from IPython.display import display

# Δημιουργία κβαντικού κυκλώματος
qc = QuantumCircuit(1, 1)

# Η Alice κωδικοποιεί το qubit με χρήση πύλης Hadamard
qc.h(0)
qc.barrier()

# Ο Bob λαμβάνει το qubit και κάνει μέτρηση με την ίδια βάση εφαρμόζοντας πύλη Hadamard
qc.h(0)
qc.measure(0, 0)

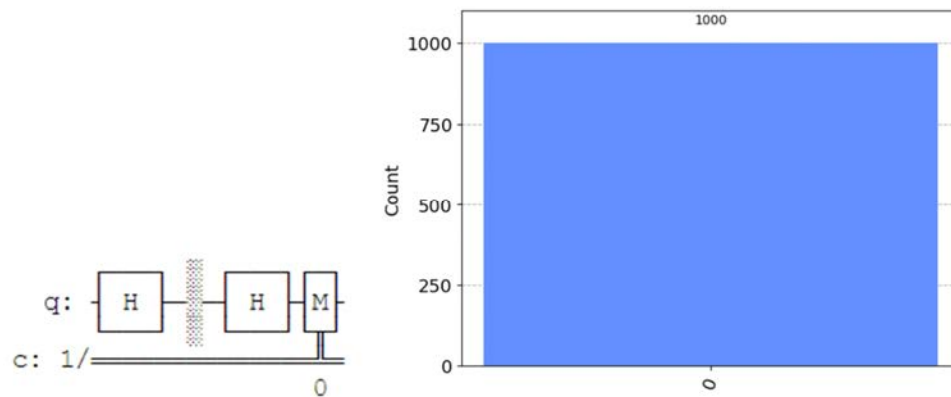
# Σχεδίαση και προσομοίωση κυκλώματος
display(qc.draw())

aersim = Aer.get_backend('aer_simulator')
job = aersim.run(qc, shots=1000)
counts = job.result().get_counts()
print("Total counts:", counts)
```

```
plot_histogram(counts)
```

Σε αυτόν τον τροποποιημένο κώδικα, η πύλη H (`qc.h(0)`) εφαρμόζεται στο qubit, υποδεικνύοντας ότι η Alice κωδικοποιεί το qubit στην οριζόντια κατεύθυνση και ο Bob μετρά το qubit στην οριζόντια κατεύθυνση από προεπιλογή.

Έχουμε σαν αποτέλεσμα:



Total counts: {'0': 1000}

Οπότε το αποτέλεσμα είναι ότι η Alice και ο Bob χρησιμοποιούν την ίδια βάση εφαρμόζοντας την πύλη Hadamard στην οριζόντια κατεύθυνση. Όπως φαίνεται στο διάγραμμα μετά από 1000 μετρήσεις το αποτέλεσμα που δόθηκε ήταν 0.

4.1.2 Πείραμα 2: Προσομοίωση του BB84 (χωρίς eavesdropping)

-Αρχικά φορτώνουμε το αρχείο με τον κώδικα: `%load BB84.py`

-Στη συνέχεια το εκτελούμε με την εντολή: `%run BB84.py`

Παίρνουμε τα εξής αποτελέσματα:

```
Alice bits:
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
Alice bases:
['H', 'V', 'H', 'V', 'H', 'H', 'H', 'V', 'V', 'H', 'V', 'H', 'H', 'V', 'V', 'H']
Bob bases:
['H', 'H', 'H', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'V']
Bob results:
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
```

Η Alice και ο Bob επιλέγουν τις μισές κοινές βάσεις και τα συγκρίνουν σε μια κρυπτογραφημένη γραμμή, αλλά για απλότητα επιλέγουμε το πρώτο μισό της ακολουθίας ως δείγματα bits.

-Για να έχουμε πάρουμε το μέγεθος της δειγματοληψίας των bits θα εκτελέσουμε τον ακόλουθο κώδικα προσθέτοντάς τον ακριβώς από κάτω από το τέλος του κώδικα του αρχείου BB84.py.

```
sample_size = len(alice_bits_samebasis) // 2
alice_sample = alice_bits_samebasis[0:sample_size]
bob_sample = bob_bits_samebasis[0:sample_size]
print("sample size:", sample_size)
print("alice_sample = ", alice_sample)
print(" bob_sample = " , bob_sample)
print(bob_sample == alice_sample)
```

Με αποτέλεσμα:

Alice bits:

```
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
```

Alice bases:

```
['H', 'V', 'H', 'V', 'H', 'H', 'H', 'V', 'V', 'H', 'V', 'H', 'H', 'V', 'V', 'H']
```

Bob bases:

```
['H', 'H', 'H', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'V']
```

Bob results:

```
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
```

sample size: 4 # Το μέγεθος του δείγματος είναι 4, πράγμα που σημαίνει ότι η επόμενη σύγκριση βασίζεται στα πρώτα 4 bit τόσο από την Alice όσο και από τον Bob για να ελεγχθεί αν ταιριάζουν.

alice_sample = [1, 0, 0, 1]

bob_sample = [1, 0, 0, 1]

True

- Είναι True που υποδεικνύει ότι τα δείγματα από την Alice και τον Bob ταιριάζουν. Αυτό σημαίνει ότι για αυτά τα 4 qubits, η Alice και ο Bob χρησιμοποίησαν τις ίδιες βάσεις (είτε "H" είτε "V") τόσο για την κωδικοποίηση όσο και για τη μέτρηση, και πήραν τα ίδια αποτελέσματα. Άρα η Alice και ο Bob μπορούν να χρησιμοποιήσουν το άλλο μισό της ακολουθίας bit ως το κλειδί.

Στο πρωτόκολλο διανομής κβαντικού κλειδιού BB84, τα "V" και "H" αναφέρονται σε δύο διαφορετικές βάσεις που χρησιμοποιούνται για την κωδικοποίηση και τη μέτρηση qubits.

1. V (Κάθετη) Βάση: Σε αυτή τη βάση, τα qubits κωδικοποιούνται χρησιμοποιώντας την κάθετη και οριζόντια πόλωση φωτονίων. Συγκεκριμένα, ένα qubit μπορεί να κωδικοποιηθεί είτε ως $|0\rangle$ (κάθετη πόλωση) είτε ως $|1\rangle$ (οριζόντια πόλωση).
2. H (Οριζόντια) Βάση: Σε αυτή τη βάση, τα qubits κωδικοποιούνται χρησιμοποιώντας τις διαγώνιες πολώσεις των φωτονίων, δηλαδή τις πολώσεις 45 μοιρών και 135 μοιρών. Ένα qubit μπορεί να κωδικοποιηθεί είτε ως $|+\rangle$ (πόλωση 45 μοιρών) είτε ως $|-\rangle$ (πόλωση 135 μοιρών).

Όταν η Alice στέλνει ένα qubit στον Bob, επιλέγει τυχαία να το κωδικοποιήσει είτε στη βάση V είτε σε H. Ομοίως, όταν ο Bob μετρά το qubit που λαμβάνει από την Alice, επιλέγει τυχαία να το μετρήσει είτε στη βάση V είτε σε H. Εάν και οι δύο χρησιμοποιούν την ίδια βάση (είτε V είτε H), ο Bob θα μπορεί να προσδιορίσει σωστά την κατάσταση του qubit. Ωστόσο, εάν χρησιμοποιούν διαφορετικές βάσεις, η μέτρηση του Bob θα είναι τυχαία και δεν θα μπορεί να προσδιορίσει σωστά την κατάσταση του qubit.

Αυτή η αρχή αποτελεί τη βάση της ασφάλειας στο πρωτόκολλο BB84. Συγκρίνοντας τις επιλεγμένες βάσεις τους για κάθε qubit σε ένα δημόσιο κανάλι (χωρίς να αποκαλύπτουν τις πραγματικές τιμές qubit), η Alice και ο Bob μπορούν να αναγνωρίσουν και να απορρίψουν τυχόν μετρήσεις όπου χρησιμοποιούσαν διαφορετικές βάσεις, αφήνοντας μόνο τις μετρήσεις όπου χρησιμοποιούσαν την ίδια βάση. Αυτές οι μετρήσεις αντιστοίχησης μπορούν στη συνέχεια να χρησιμοποιηθούν για τη δημιουργία ενός ασφαλούς κοινόχρηστου κλειδιού.

4.1.3 Πείραμα 3: Προσομοίωση του BB84 με επίθεση eavesdropping

Θα συμπληρώσουμε τον κώδικα ανάμεσα από τα #Step 2 και #Step 3 και θα γράψουμε την τεχνική eavesdropping που θα κάνει η Eve. Δηλαδή θα δημιουργεί πρώτα μια τυχαία επιλογή βάσης bit. Έπειτα θα μετράει το κάθε qubit με μια τυχαία παραγόμενη βάση και τέλος θα κωδικοποιεί το μήνυμα με τυχαία βάση και θα στέλνει το μήνυμα στον Bob. Επίσης θα εκτυπώσουμε και το ποσοστό της διαφωνίας συγκρίνοντας κάθε αντίστοιχο bit μεταξύ της Alice και του Bob.

```
## Ανάμεσα από τα Steps 2 and 3 (Eve's eavesdropping)
## Δημιουργία τυχαίας επιλογής βάσης για κάθε of bit της Eve
eve_bases = List(map(lambda bit: dir[bit], randint(2, size=four_times_n)))
print("Eve bases: \n", eve_bases)

# Μέτρηση των qubits της Eve που στάλθηκαν από την Alice
eve_results = measure_message(message, eve_bases)
print("Eve results: \n", eve_results)

# Η Eve κωδικοποιεί το μήνυμα ξανά σύμφωνα με την τυχαία επιλογή βάσης
eve_message = encode_message(eve_results, eve_bases)

# Ο Bob λαμβάνει τα qubits από την Eve και εφαρμόζει μέτρηση
bob_results_after_eve = measure_message(eve_message, bob_bases)
print("Bob results after Eve: \n", bob_results_after_eve)
```

```
# Ποσοστό διαφωνίας μεταξύ της Alice και του Bob
disagreement_percentage = sum(a != b for a, b in zip(alice_sample, bob_sample)) /
sample_size * 100

# Εκτύπωση ποσοστού
print("Percentage of disagreement between Alice and Bob:
{:.2f}%".format(disagreement_percentage))
```

-Αφού συμπληρώσουμε τον κώδικα ανάμεσα από τα Steps 2 και 3 στο BB84.py και το αποθηκεύσουμε

-Φορτώνουμε τον κώδικα με την εντολή: %load BB84.py

-Τρέχουμε τον κώδικα με την εντολή: %run BB84.py

Με αποτέλεσμα:

```
Alice bits:
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
Alice bases:
['H', 'V', 'H', 'V', 'H', 'H', 'H', 'V', 'V', 'H', 'V', 'H', 'H', 'V', 'V', 'H']
Eve bases:
['H', 'H', 'H', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'H', 'H', 'V', 'V']
Eve results:
[1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1]
Bob results after Eve:
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1]
Bob bases:
['V', 'H', 'V', 'V', 'V', 'H', 'H', 'V', 'V', 'H', 'V', 'V', 'V', 'H', 'V', 'V']
Bob results:
[0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1]
sample size: 4
alice_sample = [1, 0, 1, 1]
bob_sample = [1, 0, 0, 0]
False
Το ποσοστό διαφωνίας της Alice και του Bob είναι: 50.00%
```

-Το ποσοστό διαφωνίας είναι το ποσοστό απόκλισης μέτρησης των bits της Alice και του Bob και χρησιμεύει ως δείκτης πιθανής υποκλοπής ή παρεμβολής στην κβαντική επικοινωνία. Ένα χαμηλό ποσοστό διαφωνίας υποστηρίζει την πεποίθηση ότι η Alice και ο Bob μοιράζονται ένα μυστικό κλειδί με ασφάλεια, ενώ ένα υψηλότερο ποσοστό όπως το αποτέλεσμα 50.00 % μπορεί να απαιτήσει περαιτέρω ανάλυση και μέτρα ασφαλείας καθώς ελλοχεύει ο κίνδυνος κλοπής μέσω eavesdropping. Όμως όπως ανάλυσουμε και στα προηγούμενα κεφάλαια με το πρωτόκολλο του QKD και το No-cloning theorem καθίσταται αδύνατο η αντιγραφή του κλειδιού και όταν γίνει η επίθεση η μέτρηση θα κατάρρευση ειδοποιώντας τους χρήστες ότι έγινε επίθεση εξού και το αποτέλεσμα μας False.

5 Συμπεράσματα

Στην πτυχιακή αυτήν, έχουμε συζητήσει για το κβαντικό δίκτυο και διαδίκτυο καθώς και τις τεχνολογικές προόδους που καλύπτουν τις βασικές έννοιες για την κατανόηση αυτής της νέας τεχνολογίας. Έχουμε αναλύσει την βασική φυσική που υποκρύπτεται σε αυτήν την τεχνολογία καθώς και την ασυναγώνιστη ασφάλεια και ιδιωτικότητα που προσφέρει χάρις στο θεώρημα της μη-κλωνοποίησης και της τηλεμεταφοράς, βασισμένα στους νόμους της κβαντικής μηχανικής. Επίσης πρωτόκολλα όπως η κατανομή κλειδιού QKD, BB84, OTP, Ekert είναι το μέλλον του κβαντικού διαδικτύου διότι θα προσφέρουν ασφάλεια βασιζόμενο πάνω σε αυτά και θα επιτρέπει τον δικτυακό συνδυασμό κλασικών και κβαντικών κόμβων που βρίσκονται απόμακρα. Η πιο σημαντική και προκλητική απαίτηση για το κβαντικό διαδίκτυο είναι η κβαντική τηλεμεταφορά βασισμένη στην δημιουργία και διανομή αλληλεπίδρασης μεταξύ ενός δικτύου κόμβων που βρίσκονται σε μακρινές αποστάσεις. Για τον σκοπό αυτό, χρησιμοποιούνται κβαντικοί επαναλήπτες που δημιουργούν την αλληλεπίδραση μεταξύ μακρινών κόμβων με τη βοήθεια ανταλλαγής διαμεσολαβητικών κόμβων, όπου η κβαντική πληροφορία αποθηκεύεται σε τοπικές κβαντικές μνήμες. Η κβαντική πληροφορία είναι εύθραυστη, πράγμα που σημαίνει ότι περιβαλλοντικά φαινόμενα όπως η αποσυνέχεια, όπου η κβαντική πληροφορία χάνεται με τον χρόνο, θα επηρεάσουν αρνητικά την κβαντική επικοινωνία. Λόγω της αποσυνέχειας, οι κβαντικές καταστάσεις χάνουν τις ιδιότητές τους και εισέρχονται στον κόσμο της κλασικής φυσικής. Επομένως, η υλοποίηση της τεχνολογίας του κβαντικού διαδικτύου θα συνοδευτεί από πολλές σχεδιαστικές προκλήσεις και πολυπλοκότητες. Τέλος αναπτύχθηκε πρόγραμμα προσομοίωσης του πρωτοκόλλου BB84 σε γλώσσα προγραμματισμού python, με την βοήθεια του Qiskit και του Jupiter Notebook και του Anaconda Python. Αναπτύχθηκαν τα σενάρια της λειτουργίας του BB84 μεταξύ δύο ατόμων καθώς και η λειτουργία του με σενάριο επίθεσης από κάποιον τρίτο στο οποίο το σύστημα καταρρέει και ενημερώνει τους χρήστες ότι κάποιος προσπαθεί να υποκλέψει την πληροφορία. Ως εκ τούτου, θα απαιτηθούν πολυάριθμες προσπάθειες που θα ανοίξουν το δρόμο για την υλοποίηση ενός πλήρως ανεπτυγμένου κβαντικού διαδικτύου. Έχει επιτευχθεί μια σπουδαία επιτυχία από την έναρξη των κβαντικών δορυφόρων που έχουν επιτύχει την κατανομή κβαντικών κλειδιών μεταξύ δύο απομακρυσμένων εδαφικών σταθμών, κάτι που

έχει ενθαρρύνει διάφορες ερευνητικές ομάδες να επιταχύνουν τις προσπάθειές τους για την κατασκευή ενός πλήρους κβαντικού διαδικτύου στο άμεσο μέλλον.

Βιβλιογραφία

- [1] Wiener,N.(1966). Differential Space, Quantum Systems, and Predtion. Cambridge, Massachusetts: The Massachusetts Institute of Technology Press
- [2] https://en.wikipedia.org/wiki/Quantum_teleportation
- [3] https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale
- [4] The Temple of Quantum Computing by Riley T. Perry , April 29, 2006
- [5] Y. Kanamori, S.-M. Yoo, W. Pan, and F. T. Sheldon, “A Short Survey On Quantum Computers,” International Journal of Computers and Applications, vol. 28, no. 3, pp. 227–233, Jul. 2006.
- [6] A. K. Pati, “Minimum classical bit for remote preparation and measurement of a qubit,” Physical Review A, vol. 63, no. 1, p. 014302, Dec. 2000
- [7] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” Reviews of Modern Physics, vol. 92, no. 2, p. 025002, May. 2020.
- [8] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, “Quantum Internet: Networking Challenges in Distributed Quantum Computing,” IEEE Network, Jan. 2019.
- [9] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” Natuwissenschaften, vol. 23, no. 49, pp. 823–828, Dec. 1935
- [10] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of the International Conference on Computers, Systems and Signal Processing, Dec. 1984
- [11] R. Van Meter, “Quantum Networking and Internetworking,” IEEE Network, vol. 26, no.4, pp. 59–64, Aug. 2012.
- [12] E. Hagley, X. Maitre, G. Nogues, C. Wunderlich, M. Brune, J.-M. Raimond, and S. Haroche, “Generation of Einstein-Podolsky-Rosen Pairs of Atoms,” Physi

cal Review Letters, vol. 79, no. 1, p. 1, Jul. 1997.

- [13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, p. 1895, Mar. 1993.
- [14] H. J. Kimble, “The quantum internet,” *Nature*, vol. 453, no. 7198, pp. 1023–1030, Jun. 2008
- [15] R. Valivarthi, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel et al., “Quantum teleportation across a metropolitan fibre network,” *Nature Photonics*, vol. 10, no. 10, pp. 676–680, Sep. 2016.
- [16] D. Bohm, “A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I,” *Physical Review*, vol. 85, no. 2, p. 166, Jan. 1952.
- [17] J. Freedman and J. F. Clauser, “Experimental Test of Local Hidden Variable Theories,” *Physical Review Letters*, vol. 28, no. 14, p. 938, Apr. 1972.
- [18] E. Hagley, X. Maitre, G. Nogues, C. Wunderlich, M. Brune, J.-M. Raimond, and S. Haroche, “Generation of Einstein-Podolsky-Rosen Pairs of Atoms,” *Physical Review Letters*, vol. 79, no. 1, p. 1, Jul. 1997.
- [19] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” *Physical Review*, vol. 47, no. 10, p. 777, May. 1935.
- [20] A. Aspect, J. Dalibard, and G. Roger, “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers,” *Physical Review Letters*, vol. 49, no. 25, p. 1804, Dec. 1982.
- [21] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, p. 1895, Mar. 1993.
- [22] Z. Ou and L. Mandel, “Violation of Bell’s Inequality and Classical Probability in a Two-Photon Correlation Experiment,” *Physical Review Letters*, vol. 61, no. 1, p. 50, Jul. 1988.
- [23] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenber, R. F. Vermeulen, R. N. Schouten, C. Abellán et al., “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature*, vol. 526, no. 7575, pp. 682–686, Oct. 2015.

- [24] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán et al., “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons,” *Physical Review Letters*, vol. 115, no. 25, p. 250401, Dec. 2015.
- [25] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman et al., “Strong Loophole-Free Test of Local Realism,” *Physical Review Letters*, vol. 115, no. 25, p. 250402, Dec. 2015.
- [26] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going Beyond Bell’s Theorem,” in *Bell’s Theorem, Quantum Theory and Conceptionsof the Universe*. Springer, 1989, pp. 69–72.
- [27] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, vol. 52, no. 4, p. R2493, Oct. 1995.
- [28] A. K. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” *Physical review letters*, vol. 67, no. 6, p. 661, Aug. 1991.
- [29] M. Erhard, M. Krenn, and A. Zeilinger, “Advances in high-dimensional quantum entanglement,” *Nature Reviews Physics*, vol. 2, no. 7, pp. 365– 381, Jun. 2020.
- [30] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, p. 1895, Mar. 1993.
- [31] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.
- [32] S. Stenholm and P. J. Bardroff, “Teleportation of N-dimensional states,” *Physical Review A*, vol. 58, no. 6, p. 4373, Dec. 1998.
- [33] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [34] A. W. Dent, “Hybrid Cryptography,” *IACR Cryptol. ePrint Arch.*, vol. 2004, p. 210, Jun. 2004.
- [35] G. Zeng and G. Guo, “Quantum authentication protocol,” *arXiv preprint quant-ph/0001046*, Jan. 2000.
- [36] H. N. Barnum, “Quantum secure identification using entanglement and catalysis,” *arXiv preprint quant-ph/9910072*, May. 1999.

- [37] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, “Quantum identification system,” *Physical Review A*, vol. 60, no. 1, p. 149, Jul. 1999
- [38] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, Nov. 1964
- [39] C. H. Bennett and G. Brassard, “The dawn of a new era for quantum cryptography : The experimental prototype is working !” *ACM Sigact News*, vol. 20, no. 4, pp. 78–80, Oct. 1989
- [40] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, “KaaS: Key as a Service over Quantum Key Distribution Integrated Optical Networks,” *IEEE Communications Magazine*, vol. 57, no. 5, pp. 152–159, May. 2019
- [41] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, “MultiTenant Provisioning for Quantum Key Distribution Networks With Heuristics and Reinforcement Learning: A Comparative Study,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 946–957, Jun. 2020.
- [42] H. Murray, J. Horgan, J. F. Santos, D. Malone, and H. Siljak, “Implementing a Quantum Coin Scheme,” in *2020 31st Irish Signals and Systems Conference (ISSC)*. IEEE, Aug. 2020, pp. 1–7.
- [43] S. Wiesner, “Conjugate Coding,” *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.
- [44] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.- Q. Cai, W.- Y. Liu, S.-L. Li et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, vol. 582, no. 7813, pp. 501–505, Jun. 2020.
- [45] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, “Observation of Three-Photon Greenberger-HorneZeilinger Entanglement,” *Physical Review Letters*, vol. 82, no. 7, p. 1345, Feb. 1999.
- [46] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, Nov. 1964
- [47] T. Beth, J. Müller-Quade, and R. Steinwandt, “Cryptanalysis of a practical quantum key distribution with polarization-entangled photons,” *Quantum Information & Computation*, vol. 5, no. 3, pp. 181–186, May. 2005.
- [48] A. Aspect, “Bell’s inequality test: more ideal than ever,” *Nature*, vol. 398, no. 6724, pp. 189–190, Mar. 1999.

- [49] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in Workshop on the Theory and Application of Cryptographic Techniques. Springer, Jul. 1993, pp. 410–423.
- [50] S. J. Lomonaco, "A QUICK GLANCE AT QUANTUM CRYPTOGRAPHY," *Cryptologia*, vol. 23, no. 1, pp. 1–41, Jun. 199.
- [51] M. Mehic, M. Niemiec, H. Siljak, and M. Voznak, "Error Reconciliation in Quantum Key Distribution Protocols," in *Reversible Computation: Extending Horizons of Computing: Selected Results of the COST Action IC1405*. Springer Nature, 2020, p. 222.
- [52] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside Quantum Repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, Jan. 2015.
- [53] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels," *Physical Review Letters*, vol. 76, no. 5, p. 722, Jan. 1996.
- [54] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li et al., "Long-Distance Entanglement Purification for Quantum Communication," *Physical Review Letters*, vol. 126, no. 1, p. 010503, Jan. 2021.
- [55] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Physical Review A*, vol. 79, no. 3, p. 032325, Mar. 2009.
- [56] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. Hollenberg, "Surface Code Quantum Communication," *Physical Review Letters*, vol. 104, no. 18, p. 180503, May. 2010.
- [57] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, no. 1, pp. 1–7, Apr. 2015.
- [58] F. Rozpedek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, "Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission," *Physical Review A*, vol. 99, no. 5, p. 052330, May. 2019.
- [59] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photonics*, vol. 6, no. 11, pp. 777–781, Oct.

2012.

[60] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, “Quantum communication without the necessity of quantum memories,” *Nature Photonics*, vol. 6, no. 11, pp. 777–781, Oct. 2012.

[61] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, “Quantum repeaters based on two species trapped ions,” *New Journal of Physics*, vol. 21, no. 7, p. 073002, Jul. 2019.

[62] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, “Ultrafast and Fault-Tolerant Quantum Communication across Long Distances,” *Physical Review Letters*, vol. 112, no. 25, p. 250501, Jun. 2014.

[63] J. Dias and T. C. Ralph, “Quantum repeaters using continuous-variable teleportation,” *Physical Review A*, vol. 95, no. 2, p. 022312, Feb. 2017.

[64]] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics,” *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.

[65] C. Chou, S. Polyakov, A. Kuzmich, and H. Kimble, “Single-Photon Generation from Stored Excitation in an Atomic Ensemble,” *Physical Review Letters*, vol. 92, no. 21, p. 213601, May. 2004.

[66] S. Santra, S. Muralidharan, M. Lichtman, L. Jiang, C. Monroe, and V. S. Malinovsky, “Quantum repeaters based on two species trapped ions,” *New Journal of Physics*, vol. 21, no. 7, p. 073002, Jul. 2019.

[67] C. H. van der Wal, M. D. Eisaman, A. André, R. L. Walsworth, D. F. Phillips, A. S. Zibrov, and M. D. Lukin, “Atomic Memory for Correlated Photon States,” *Science*, vol. 301, no. 5630, pp. 196–200, Jul. 2003.

[68] A. Kuzmich, W. Bowen, A. Boozer, A. Boca, C. Chou, L.-M. Duan, and H. Kimble, “Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles,” *Nature*, vol. 423, no. 6941, pp. 731–734, Jun. 2003.

[69] D. Bohm, “A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I,” *Physical Review*, vol. 85, no. 2, p. 166, Jan. 1952.

[70] T. Northup and R. Blatt, “Quantum information transfer using photons,” *Nature Photonics*, vol. 8, no. 5, p. 356, Apr. 2014.

- [71] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, M. A. M. Izhar, S. X. Ng, and L. Hanzo, "Towards the Quantum Internet: Generalised Quantum Network Coding for Large-Scale Quantum Communication Networks," *IEEE Access*, vol. 5, pp. 17 288–17 308, Aug. 2017.
- [72] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, no. 1, p. 43, Jan. 2002.
- [73] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. Tapster, and J. Rarity, "A step towards global key distribution," *Nature*, vol. 419, no. 6906, pp. 450–450, Oct. 2002.
- [74] D. M. Benton, P. M. Gorman, P. R. Tapster, and D. M. Taylor, "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications*, vol. 283, no. 11, pp. 2465–2471, Jun. 2010.
- [75] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New Journal of Physics*, vol. 11, no. 4, p. 045007, Apr. 2009.
- [76] . Gorbachev and A. Trubilko, "Quantum teleportation of EinsteinPodolsky-Rosen pair with the help of crossroads three particle state," *Zhurnal Eksperimental'noj i Teoreticheskoy Fiziki*, vol. 118, no. 5, pp. 1036–1040, 2000.
- [77] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger et al., "Experimental verification of the feasibility of a quantum channel between space and Earth," *New Journal of Physics*, vol. 10, no. 3, p. 033038, Mar. 2008.
- [78] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of LaguerreGaussian laser modes," *Physical Review A*, vol. 45, no. 11, p. 8185, Jun. 1992.
- [79] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Physics*, vol. 16, no. 10, pp. 1418–1438, Oct. 2006.
- [80] J. R. G. Alonso and T. A. Brun, "Protecting orbital-angular-momentum photons from decoherence in a turbulent atmosphere," *Physical Review A*, vol. 88, no. 2, p. 022326, Aug. 2013.
- [81] M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaeck,

M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba et al., “Long-Distance Free-Space Distribution of Quantum Entanglement,” *Science*, vol. 301, no. 5633, pp. 621–623, Aug. 2003.

[82] S. Zhao, J. Leach, L. Gong, J. Ding, and B. Zheng, “Aberration corrections for free-space optical communications in atmosphere turbulence using orbital angular momentum states,” *Optics Express*, vol. 20, no. 1, pp. 452–461, Dec. 2012.

[83] J. Ballato, T. Hawkins, P. Foy, R. Stolen, B. Kokuoz, M. Ellison, C. McMillen, J. Reppert, A. Rao, M. Daw et al., “Silicon optical fiber,” *Optics Express*, vol. 16, no. 23, pp. 18 675–18 683, Oct. 2008.

[84] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors,” *Nature Photonics*, vol. 1, no. 6, pp. 343–348, Jun. 2007.

[85] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuousvariable quantum key distribution by controlling excess noise,” *Scientific Reports*, vol. 6, no. 1, pp. 1–9, Jan. 2016.

[86] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang et al., “Measurement-DeviceIndependent Quantum Key Distribution Over a 404 km Optical Fiber,” *Physical Review Letters*, vol. 117, no. 19, p. 190501, Nov. 2016.

[87] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka et al., “Field test of quantum key distribution in the Tokyo QKD Network ,” *Optics Express*, vol. 19, no. 11, pp. 10 387–10 409, May. 2011.

[88] L. Ma, O. Slattery, and X. Tang, “Optical Quantum Memory and its Applications in Quantum Communication Systems,” *Journal of Research of the National Institute of Standards and Technology*, vol. 125, Jan. 2020.

[89] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, “Quantum Search Algorithms for Wireless Communications,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, Nov. 2018.

[90] C. Simon, M. Afzelius, J. Appel, A. B. de La Giroday, S. Dewhurst, N. Gisin, C. Hu, F. Jelezko, S. Kröll, J. Müller et al., “Quantum memories,” *The European Physical Journal D*, vol. 58, no. 1, pp. 1–22, Apr. 2010.

- [91] L.-M. Duan and C. Monroe, “Colloquium: Quantum networks with trapped ions,” *Reviews of Modern Physics*, vol. 82, no. 2, p. 1209, Apr. 2010.
- [92] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, “Inside Quantum Repeaters,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, Jan. 2015.
- [93] D.-S. Ding, “Raman Quantum Memory of Photonic Polarized Entanglement,” in *Broad Bandwidth and High Dimensional Quantum Memory Based on Atomic Ensembles*. Springer, Dec. 2018, pp. 91–107.
- [94] S. Bose, P. Knight, M. Plenio, and V. Vedral, “Proposal for Teleportation of an Atomic State via Cavity Decay,” *Physical Review Letters*, vol. 83, no. 24, p. 5158, Dec. 1999.
- [95] P. Vernaz-Gris, K. Huang, M. Cao, A. S. Sheremet, and J. Laurat, “Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble,” *Nature Communications*, vol. 9, no. 1, pp. 1–6, Jan. 2018.
- [96] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, Oct. 2018.
- [97] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, May. 2020.
- [98] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.
- [99] G.-L. Long and X.-S. Liu, “Theoretically efficient high-capacity quantum-key-distribution scheme,” *Physical Review A*, vol. 65, no. 3, p. 032302, Feb. 2002.
- [100] Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin et al., “Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km,” *Physical Review Letters*, vol. 124, no. 7, p. 070501, Feb. 2020.
- [101] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, “Generalized Privacy Amplification,” *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

- [102] C. S. Yoon, M. S. Kang, J. I. Lim, and H. J. Yang, “Quantum signature scheme based on a quantum search algorithm,” *Physica Scripta*, vol. 90, no. 1, p. 015103, Dec. 2014.
- [103] G. Gao, “Two quantum dialogue protocols without information leakage,” *Optics Communications*, vol. 283, no. 10, pp. 2288–2293, May. 2010.
- [104] C. Zheng and G. Long, “Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,” *Science China Physics, Mechanics & Astronomy*, vol. 57, no. 7, pp. 1238–1243, Jul. 2014.
- [105] S. Pirandola and S. Mancini, “Quantum teleportation with continuous variables: A survey,” *Laser Physics*, vol. 16, no. 10, pp. 1418–1438, Oct. 2006.
- [106] M. Mosca, A. Tapp, and R. de Wolf, “Private Quantum Channels and the Cost of Randomizing Quantum Information,” arXiv preprint quantph/0003101, Mar. 2000.
- [107] T. M. Fernández-Caramés, “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, Jul. 2019.
- [108] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, “A Review on Internet of Things for Defense and Public Safety,” *Sensors*, vol. 16, no. 10, p. 1644, Oct. 2016.
- [109] P. Fraga-Lamas, T. M. Fernández-Caramés, and L. Castedo, “Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways,” *Sensors*, vol. 17, no. 6, p. 1457, Jun. 2017.
- [110] M. Abadi, J. Feigenbaum, and J. Kilian, “On hiding information from an oracle,” *Journal of Computer and System Sciences*, vol. 39, no. 1, pp. 21–50, Aug. 1989.
- [111] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, “Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network,” *Physical Review Letters*, vol. 78, no. 16, p. 3221, Apr. 1997.
- [112] S. Perseguers, G. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, and A. Acín, “Distribution of entanglement in large-scale quantum networks,” *Reports on Progress in Physics*, vol. 76, no. 9, p. 096001, Sep. 2013.
- [113] I. L. Chuang, “Quantum Algorithm for Distributed Clock Synchronization,” *Physical Review Letters*, vol. 85, no. 9, p. 2006, Aug. 2000.
- [114] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi,

“Experimental Satellite Quantum Communications,” *Physical Review Letters*, vol. 115, no. 4, p. 040502, Jul. 2015.

[115] D. A. Lidar and T. A. Brun, *Quantum Error Correction*. Cambridge University Press, 2013.

[116] R. Van Meter and S. J. Devitt, “The Path to Scalable Distributed Quantum Computing,” *Computer*, vol. 49, no. 9, pp. 31–42, Sep. 2016.

[117] A. C.-C. Yao, “Interactive Proofs For Quantum Computations,” in *International Symposium on Algorithms and Computation*. Springer, Apr. 2003, pp. 1–1.

[118] R. Raussendorf and H. J. Briegel, “A One-Way Quantum Computer,” *Physical Review Letters*, vol. 86, no. 22, p. 5188, May. 2001.

[119] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal Blind Quantum Computation,” in *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, 2009, pp. 517–526.

[120] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, “Demonstration of Blind Quantum Computing,” *Science*, vol. 335, no. 6066, pp. 303–308, Jan. 2012.

[121] J. C. Corbett, J. Dean, M. Epstein, A. Fikes, C. Frost, J. J. Furman, S. Ghemawat, A. Gubarev, C. Heiser, P. Hochschild et al., “Spanner: Google’s Globally Distributed Database,” *ACM Transactions on Computer Systems (TOCS)*, vol. 31, no. 3, pp. 1–22, Aug. 2013.

[122] S. Duan, S. Cong, and Y. Song, “A survey on quantum positioning system,” *International Journal of Modelling and Simulation*, pp. 1–19, Mar. 2020.

[123] J. S. Warner and R. G. Johnston, “GPS Spoofing Countermeasures,” *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[124] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, P. M. Kintner et al., “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Sep. 2008, pp. 2314–2325.

[125] J. S. Warner and R. G. Johnston, “GPS Spoofing Countermeasures,” *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

- [126] N. Hinkley, J. A. Sherman, N. B. Phillips, M. Schioppo, N. D. Lemke, K. Beloy, M. Pizzocaro, C. W. Oates, and A. D. Ludlow, “An Atomic Clock with 10–18 Instability,” *Science*, vol. 341, no. 6151, pp. 1215–1218, Sep. 2013.
- [127] J. Williamson, “Brownian motion of electrons,” *Journal of Physics A: General Physics*, vol. 1, no. 6, p. 629, Nov. 1968.
- [128] V. G. Cerf and R. E. Ichniowski, “A Protocol for Packet Network Intercommunication,” *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 2, pp. 71–82, May. 2005.
- [129] G. Fournier, *The Quantum Internet: Ultrafast and Safe from Hackers*. Springer Nature, 2020.
- [130] D. Collins, N. Gisin, and H. De Riedmatten*, “Quantum relays for long distance quantum cryptography,” *Journal of Modern Optics*, vol. 52, no. 5, pp. 735–753, Feb. 2005.
- [131] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Dec. 1984.
- [132] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus et al., “Using quantum key distribution for cryptographic purposes: A survey,” *Theoretical Computer Science*, vol. 560, pp. 62–81, Dec. 2014.
- [133] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, May. 2020.
- [134] https://en.wikipedia.org/wiki/Quantum_error_correction
- [135] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Loncaric, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling et al., “A trusted node-free eight-user metropolitan quantum communication network,” *Science Advances*, vol. 6, no. 36, Sep. 2020.
- [136] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, Oct. 2018.
- [137] H.-K. Lo, M. Curty, and B. Qi, “Measurement-Device-Independent Quantum Key Distribution,” *Physical Review Letters*, vol. 108, no. 13, p. 130503, Mar. 2012.

- [138] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You et al., “Measurement-DeviceIndependent Quantum Key Distribution over Untrustful Metropolitan Network,” *Physical Review X*, vol. 6, no. 1, p. 011024, Mar. 2016.
- [139] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, “Measurement DeviceIndependent Quantum Key Distribution over asymmetric channel and unstable channel,” *Scientific Reports*, vol. 8, no. 1, pp. 1–7, Dec. 2018.
- [140] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “Quantum Network Coding,” in *Annual Symposium on Theoretical Aspects of Computer Science, STACS 2007*. Springer, 2007, pp. 610– 621.
- [141] D. A. Lidar, I. L. Chuang, and K. B. Whaley, “Decoherence-Free Subspaces for Quantum Computation,” *Physical Review Letters*, vol. 81, no. 12, p. 2594, Sep. 1998.
- [142] D. Suter and G. A. Álvarez, “Colloquium: Protecting quantum information against environmental noise,” *Reviews of Modern Physics*, vol. 88, no. 4, p. 041001, Oct. 2016.
- [143] C. P. Koch, “Controlling open quantum systems: tools, achievements, and limitations,” *Journal of Physics: Condensed Matter*, vol. 28, no. 21, p. 213001, May. 2016.
- [144] L. Viola, E. Knill, and S. Lloyd, “Dynamical Decoupling of Open Quantum Systems,” *Physical Review Letters*, vol. 82, no. 12, p. 2417, Mar. 1999.
- [145] L. Viola and S. Lloyd, “Dynamical suppression of decoherence in twostate quantum systems,” *Physical Review A*, vol. 58, no. 4, p. 2733, Oct. 1998.
- [146] S. L. Braunstein and P. Van Loock, “Quantum information with continuous variables,” *Reviews of Modern Physics*, vol. 77, no. 2, p.13, Jun. 2005.
- [147] <https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two>
- [148] <https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility>
- [149] D. W. Leung, “Quantum vernam cipher,” *Quantum Information & Computation*, vol. 2, no. 1, pp. 14–34, Dec. 2002.
- [150] A. I. Nurhadi and N. R. Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey,” in *2018 4th International Conference on Wireless and Telematics (ICWT)*. IEEE, Nov. 2018, pp. 1–5.

- [151] D. Bohm, "A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I," *Physical Review*, vol. 85, no. 2, p. 166, Jan. 1952.
- [152] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental Demonstration of Four-Photon Entanglement and HighFidelity Teleportation," *Physical Review Letters*, vol. 86, no. 20, p. 4435, May. 2001.
- [153] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu et al., "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, Dec. 2020.
- no. 2, pp. 398–403, Jan. 2007.
- [154] M. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. Itano, J. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri et al., "Deterministic quantum teleportation of atomic qubits," *Nature*, vol. 429, no. 6993, pp. 737–739, Jun. 2004.
- [155] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, "Quantum teleportation across the danube," *Nature*, vol. 430, no. 7002, pp. 849–849, Aug. 2004.
- [156] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang et al., "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, no. 7410, pp. 185–188, Aug. 2012.
- [157] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek et al., "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, Jun. 2007.
- [158] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman et al., "Strong Loophole-Free Test of Local Realism," *Physical Review Letters*, vol. 115, no. 25, p. 250402, Dec. 2015.
- [159] R. Valivarthi, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel et al., "Quantum teleportation across a metropolitan fibre network," *Nature Photonics*, vol. 10, no. 10, pp. 676–680, Sep. 2016.
- [160] S. L. Braunstein and H. J. Kimble, "Teleportation of ContinuousQuantum Variables," *Physical Review Letters*, vol. 80, no. 4, p. 869, Jan. 1998.

- [161] V. Gorbachev and A. Trubilko, “Quantum teleportation of EinsteinPodolsky-Rosen pair with the help of crossroads three particle state,” *Zhurnal Eksperimental’noj i Teoreticheskoy Fiziki*, vol. 118, no. 5, pp.1036–1040, 2000.
- [162] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li et al., “Ground-to-satellite quantum teleportation,” *Nature*, vol. 549, no. 7670, pp. 70–73, Aug. 2017.
- [163] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Reviews of Modern Physics*, vol. 92, no. 2, p. 025002, May. 2020.
- [164] A. Armour, M. Blencowe, and K. Schwab, “Quantum Dynamics of a Cooper-Pair Box Coupled to a Micromechanical Resonator,” *Physical Review Letters*, vol. 88, p. 148301, 2002.
- [165] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, “Experimental quantum teleportation,” *Nature*, vol. 390, no. 6660, pp. 575–579, Dec. 1997.
- [166] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
- [167] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, Nov. 1964.
- [168] <https://el.wikipedia.org/wiki/Python>
- [169] Quantum Internet—Applications, Functionalities,Enabling Technologies, Challenges, and Research Directions
- [170] Κβαντική Υπολογιστική ΙΩΑΝΝΗΣ ΚΑΡΑΦΥΛΛΙΔΗΣ Καθηγητής Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Δ.Π.Θ.

