

Αλγόριθμοι για επίτευξη ασφαλούς άμεσης κβαντικής επικοινωνίας

Πτυχιακή Εργασία



Τμήμα Πληροφορικής

Ιόνιο Πανεπιστήμιο

Στοιχεία Φοιτητή:

Οικονόμου Σταυρούλα Π2020171

Κέρκυρα, 2024

Επιβλέπων καθηγητής:

Θεόδωρος Ανδρόνικος

Επιτροπή:

Μιχαήλ Στεφανιδάκης

Ελένη Χριστοπούλου

Περιεχόμενα

[Περιεχόμενα](#)

[Περίληψη](#)

[Εισαγωγή](#)

[1. Κβαντικοί Υπολογιστές](#)

[1.1 Βασικές έννοιες](#)

[1.1.1 Κβαντικές Καταστάσεις και Qubits](#)

[1.1.2 Υπέρθωση \(Superposition\)](#)

[1.1.3 Μέτρηση \(Measurement\)](#)

[1.1.4 Κβαντικές Πύλες \(Quantum Gates\)](#)

[1.2 Κβαντική Κρυπτογραφία](#)

[1.3 Quantum Key Distribution](#)

[1.4 Αλγόριθμος BB84](#)

[2. Κβαντική Ασφαλής Άμεση Επικοινωνία](#)

[2.1 Διανομή Κβαντικού Κλειδιού Υψηλής Χωρητικότητας](#)

[2.1.1 Ασφάλεια Πρωτοκόλλου](#)

[2.2 Πρωτόκολλο Άμεσης Κβαντικής Επικοινωνίας με χρήση του Einstein-Podolsky-Rosen μπλοκ](#)

[2.2.1 Ασφάλεια Πρωτοκόλλου](#)

[2.3 Κβαντική Ασφαλής Άμεση Επικοινωνία βασισμένη σε μεμονωμένα σωματίδια](#)

[2.3.1 Ασφάλεια Έναντι Επιθέσεων](#)

[2.4 Κβαντική Ασφαλής Άμεση Επικοινωνία Ελεύθερου Χώρου](#)

[2.4.1 Βασικές Αρχές](#)

[2.4.2 Πρωτόκολλο DL04](#)

[2.4.3 Πρωτόκολλο RECON](#)

[2.4.4 Κβαντικό Πρωτόκολλο Χαμηλής Πιθανότητας Αναχαίτισης](#)

[2.4.5 Κβαντικό πρωτόκολλο ιδιωτικής επικοινωνίας χωρίς κλειδί](#)

[2.4.6 QSDC σε Πραγματικό Κβαντικό Κανάλι](#)

[2.5 Ελεύθερος Χώρος QSDC και Χαρακτηριστικά](#)

[2.5.1 Ζητήματα που προκύπτουν στο QSDC Ελεύθερου Χώρου](#)

[2.5.2 Στρατηγική Κωδικοποίησης Φωτονίων](#)

[2.5.3 Σκοπιμότητα δορυφορικού QSDC](#)

[2.5.4 CAID QSDC](#)

[3. Εξέλιξη της Κβαντικής Ασφαλούς Άμεσης Επικοινωνίας](#)

[3.1 Σχεδίαση Πρωτοκόλλων QSDC](#)

[3.2 Ασφάλεια Πρωτοκόλλου QSDC](#)

[3.3 Πειραματικές Υλοποιήσεις QSDC](#)

[3.4 Υβριδικό QSDC Δίκτυο](#)

[4. Συμπεράσματα](#)

[5. Αναφορές](#)

Περίληψη

Η συγκεκριμένη εργασία έχει ως επίκεντρο την επίτευξη ασφαλούς άμεσης κβαντικής επικοινωνίας και την εξοικείωση με τους αλγορίθμους που σχετίζονται με αυτή. Σε πρώτη φάση, γίνεται μια εισαγωγή αναφορικά με βασικές έννοιες του κβαντισμού όπως τα qubits, τα quantum gates καθώς και το QKD. Στη συνέχεια, αναλύεται μια πληθώρα αλγορίθμων από τις αρχές του κβαντισμού μέχρι και σήμερα, ενώ παράλληλα, γίνεται λόγος για την εξέλιξη του QSDC καθώς και πιθανές εφευρέσεις πάνω σε αυτόν τον τομέα. Στόχος της εργασίας είναι η ανάλυση της πορείας της ασφαλούς άμεσης κβαντικής επικοινωνίας καθώς και η περαιτέρω έρευνα για την εύρεση ενός βέλτιστου πρωτοκόλλου QSDC που θα χαρακτηρίζεται από πλήρη ασφάλεια ανεξαρτήτως των συνθηκών και των επιθέσεων που προκύπτουν.

Εισαγωγή

Ο κβαντικός υπολογισμός αποτελεί ένα αναδυόμενο πεδίο που χρησιμοποιεί αρχές της κβαντικής μηχανικής για την εκτέλεση υπολογιστικών εργασιών, συνδυάζοντας πτυχές της επιστήμης των υπολογιστών, της φυσικής και των μαθηματικών για την επίλυση πολύπλοκων προβλημάτων ταχύτερα από τους κλασικούς υπολογιστές.

Η ιδέα της κβαντικής μηχανικής για υπολογισμούς προτάθηκε πρώτη φορά από τον φυσικό Richard Feynman το 1982, υποδηλώνοντας ότι οι συμβατικοί υπολογιστές θα δυσκολεύονταν να προσομοιώσουν αποτελεσματικά τα κβαντικά συστήματα, ενώ ένα H/Y που θα ακολουθούσε τις αρχές της κβαντικής μηχανικής θα μπορούσε να εκτελέσει ορισμένους τύπους υπολογισμών πολύ ταχύτερα. Στη συνέχεια, κατά τη δεκαετία του 1990, εμφανίστηκαν οι πρώτοι κβαντικοί αλγόριθμοι και η πειραματική πρόοδος προς την υλοποίηση κβαντικών υπολογιστών, με ορισμένα κβαντικά μηχανήματα να ξεπερνούν τα κλασικά σε συγκεκριμένες εργασίες, παρόλο που βρίσκονται ακόμη σε πρώιμα στάδια.

Ταυτόχρονα, γίνεται λόγος για πρωτόκολλα κβαντικής διανομής κλειδιών (QKD), εστιάζοντας ιδιαίτερα στο πρωτόκολλο BB84 από τους Bennett & Brassard το 1984. ενώ αναλύεται το QKD και πως βασίζεται σε κβαντικές αρχές για την ασφαλή διανομή κλειδιών κρυπτογράφησης μεταξύ δύο μερών, της Alice και του Bob χρησιμοποιώντας κβαντικά κανάλια. Τέλος, περιγράφεται επίσης η πόλωση του φωτός στην κβαντική επικοινωνία και την κρυπτογραφία, τονίζοντας τον τρόπο με τον οποίο τα φωτόνια μπορούν να εμφανίσουν διαφορετικές πολωμένες καταστάσεις ζωτικής σημασίας για την κωδικοποίηση πληροφοριών ή τη διανομή κβαντικών κλειδιών.

Από την άλλη, η εξέλιξη της ανθρωπότητας και η ανάγκη για ασφαλή επικοινωνία οδήγησαν στην ανακάλυψη της κρυπτογραφίας, ενός τρόπου μετάδοσης πληροφοριών ώστε να παραμένουν ακατανόητες σε μη εξουσιοδοτημένα μέρη. Συγκεκριμένα, η κβαντομηχανική, μαζί με την κρυπτογραφία, προσφέρει δυνατότητες για ασφαλή διανομή κλειδιών, με συστήματα QKD όπως τα BB84, EPR και B92 που ενισχύουν την ασφάλεια της κβαντικής επικοινωνίας.

Στο κείμενο εισάγεται επίσης η έννοια της κβαντικής ασφαλούς άμεσης επικοινωνίας (QSDC) που βασίζεται σε μεμονωμένα σωματίδια. Ειδικότερα, εισάγεται μια νέα βάση Y και χρησιμοποιείται η λειτουργία Pauli I σε συνδυασμό με τη λειτουργία Z για την κωδικοποίηση μυστικών μηνυμάτων σε μεμονωμένα σωματίδια. Η συγκεκριμένη μέθοδος επιτρέπει την ευκολότερη εφαρμογή καθώς περιστρέφει μόνο τη φάση του σωματιδίου χωρίς να αλλάζει την πόλωσή του. Το QSDC επισημαίνεται ως βασική πτυχή της κβαντικής κρυπτογραφίας με διάφορες ερευνητικές προόδους κατά τη διάρκεια των ετών, όπως πρωτόκολλα που χρησιμοποιούν ζεύγη EPR για μετάδοση μηνυμάτων και κωδικοποίηση πληροφοριών σε φάσματα συχνοτήτων.

Τέλος, αναφέρεται επίσης ότι το QSDC είναι τελικά χρήσιμο σε πρακτικές εφαρμογές και μπορεί να επιτύχει υψηλό επίπεδο ασφάλειας επικοινωνίας όταν συνδυάζεται με κλασική ή μετα-κβαντική κρυπτογραφία. Σαφέστατα, η επίτευξη άνευ όρων ασφάλειας μας επιφυλάσσει πολλές προκλήσεις λόγω των πρακτικών ατελειών της συσκευής και την ανάγκη αντιμετώπισης των κενών ασφαλείας που μπορεί να προκύψουν.

1. Κβαντικοί Υπολογιστές

Η κβαντική υπολογιστική, αποτελεί ένα αναδυόμενο πεδίο, καθώς χρησιμοποιεί αρχές της κβαντικής μηχανικής για την εκτέλεση υπολογιστικών εργασιών. Πρόκειται για έναν πολυεπιστημονικό τομέα, που περιλαμβάνει πτυχές της επιστήμης των υπολογιστών, της φυσικής και των μαθηματικών ταυτόχρονα, έτσι ώστε να επιλυθούν πολύπλοκα προβλήματα ταχύτερα από έναν κλασικό Η/Υ. Η ιδέα της εκμετάλλευσης της κβαντικής μηχανικής για τον υπολογισμό προτάθηκε αρχικά από τον φυσικό Richard Feynman το 1982, όταν πρότεινε ότι οι συμβατικοί υπολογιστές θα αντιμετώπιζαν δυσκολίες στην προσομοίωση των κβαντικών συστημάτων αποτελεσματικά, αλλά ένας υπολογιστής που ακολουθούσε τις αρχές της κβαντικής μηχανικής θα μπορούσε πιθανότατα να εκτελέσει ορισμένους τύπους υπολογισμών πολύ πιο γρήγορα.

Στη συνέχεια, ο David Deutsch δημιούργησε μια θεωρητική βάση για ένα κβαντικό μηχάνημα Turing, καταλήγοντας στο συμπέρασμα ότι τα κβαντικά κυκλώματα είναι παγκόσμια και έτσι μπορούν να προσομοιώσουν οποιοδήποτε κλασικό αλγόριθμο. Έπειτα, κατά τη δεκαετία του 1990 ακολούθησαν και οι πρώτοι κβαντικοί αλγόριθμοι και οι πρώτες πειραματικές προόδους για την υλοποίηση κβαντικών υπολογιστών. Σήμερα, ενώ υπάρχουν κβαντικοί υπολογιστές που υπερβαίνουν τους κλασικούς σε συγκεκριμένες εργασίες, βρίσκονται ακόμα σε πρώιμα στάδια [1].

1.1 Βασικές έννοιες

1.1.1 Κβαντικές Καταστάσεις και Qubits

Στην επιστήμη της κβαντομηχανικής, η κατάσταση ενός φυσικού συστήματος περιγράφεται από ένα διάνυσμα κατάστασης στον χώρο Hilbert $\mathcal{H}$. Ο χώρος Hilbert είναι ένας διανυσματικός χώρος σύνθετης αξίας που περιλαμβάνει κάθε πιθανή κατάσταση στην οποία μπορεί να κατοικεί ένα κβαντικό σύστημα. Ο γνωστός συμβολισμός “ket” που περιγράφει ένα διάνυσμα στον χώρο μιγαδικών αριθμών $\mathbb{C}^n$ και αντιπροσωπεύει μια καθαρή κβαντική κατάσταση συμβολίζεται ως:

$$|\psi\rangle = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \dots \\ a_n \end{bmatrix} \quad (1.1)$$

όπου το σύμβολο $|\cdot\rangle$ είναι ο συμβολισμός Dirac, ενός συμβόλου ψ για ένα διάνυσμα και έχουμε $a\psi \in C\psi$ που σχετίζεται με το άθροισμα του $|a|^2$ που ισούται με 1.

Ένα κλασικό bit μπορεί να βρεθεί σε δύο μόνο καταστάσεις, είτε 0 είτε 1, ενώ ένα qubit βρίσκεται σε πολλαπλές καταστάσεις ταυτόχρονα, δηλαδή μπορεί να είναι 0, 1 ή και τα δύο. Αυτό συμβαίνει λόγω της υπέρθεσης (superposition), όπου αποτελεί έναν γραμμικό συνδυασμό των $|0\rangle$ και $|1\rangle$ καταστάσεων. Ειδικότερα, αν ορίσουμε την υπέρθεση ως $|\psi\rangle$, προκύπτει ο παρακάτω τύπος

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.2)$$

Όπου α, β είναι μιγαδικοί αριθμοί και είναι της μορφής $z = x + iy$, όπου $i = \sqrt{-1}$. Ωστόσο, κατά τη μέτρηση, ένα qubit μπορεί να βρεθεί μόνο στην κατάσταση $|0\rangle$ ή $|1\rangle$ και σύμφωνα με την κβαντική μηχανική, το μέτρο εις το τετράγωνο των α, β μας δίνει την πιθανότητα εύρεσης του qubit στο state $|0\rangle$ ή $|1\rangle$. Δηλαδή:

$|\alpha|^2$: Πιθανότητα εύρεσης $|\psi\rangle$ στην κατάσταση $|0\rangle$

$|\beta|^2$: Πιθανότητα εύρεσης $|\psi\rangle$ στην κατάσταση $|1\rangle$

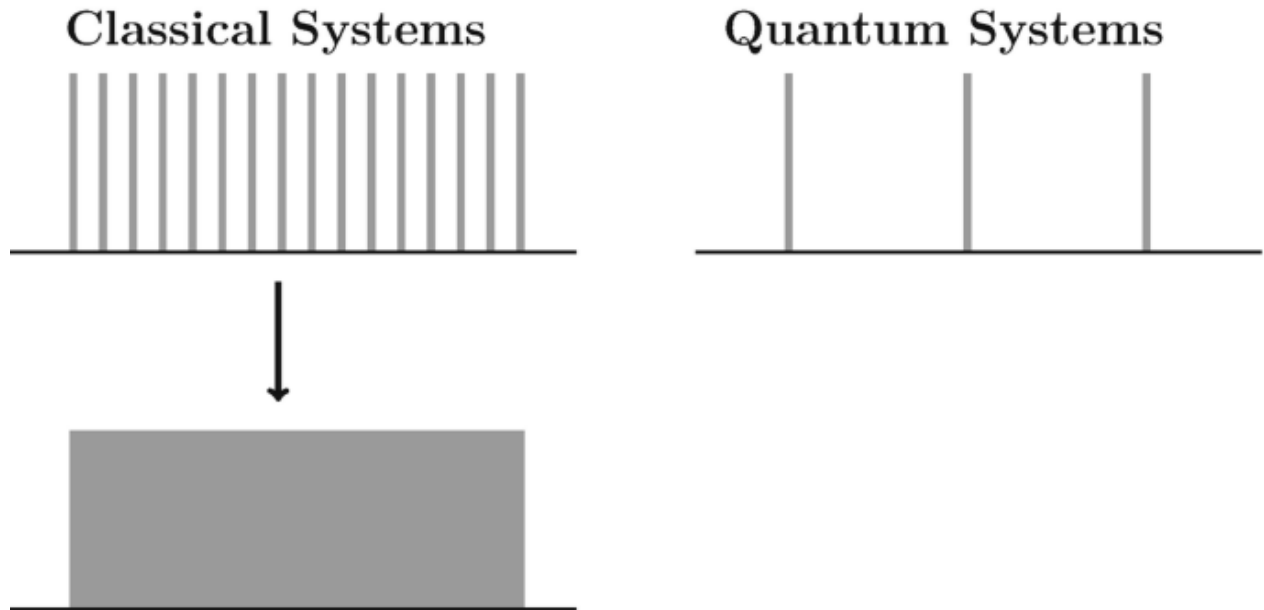
Επομένως, εφόσον υπάρχει ο περιορισμός λήψης ενός δεδομένου αποτελέσματος, ισχύει ο παρακάτω τύπος

$$|\alpha|^2 + |\beta|^2 = 1 \quad (1.3)$$

1.1.2 Υπέρθεση (Superposition)

Η κβαντική υπέρθεση αποτελεί ένα φαινόμενο το οποίο σχετίζεται άρρηκτα με τα κβαντικά συστήματα. Αυτά αποτελούνται από μικρά αντικείμενα όπως πυρήνες, ηλεκτρόνια, στοιχειώδη σωματίδια και φωτόνια, για τα οποία παρατηρείται η δυαδικότητα μεταξύ κύματος-σωματιδίου καθώς και άλλα μη κλασικά φαινόμενα. Για παράδειγμα, θα περίμενε κανείς ότι ένα αντικείμενο μπορεί να έχει μια αυθαίρετη ποσότητα κινητικής ενέργειας που κυμαίνεται από 0 έως άπειρα Joules, δηλαδή μια μπάλα του μπάσκετ θα ήταν δυνατό να εκτοξευθεί σε οποιαδήποτε ταχύτητα. Παρόλα αυτά, σύμφωνα με την κβαντομηχανική κάτι ανάλογο δεν ισχύει καθώς η ενέργεια της μπάλας είναι κβαντισμένη και περιορίζεται σε συγκεκριμένες τιμές. Ειδικότερα, ένα παράδειγμα κβαντισμού ενέργειας είναι όταν οι ενέργειες μπορούν να έχουν μόνο ακέραιες τιμές και όχι οποιουδήποτε άλλους αριθμούς μεταξύ τους. Σαφέστατα, το ανθρώπινο μάτι δεν μπορεί να διακρίνει τα κενά και για αυτόν τον λόγο στην κλασική

φυσική αντιμετωπίζονται ως συνεχή. Εάν όμως εστιάσουμε σε μικρότερα μεγέθη όπως παρατηρούμε στο παρακάτω σχήμα, το άτομο υδρογόνου είναι αρκετά μικρό ώστε τα κβαντικά φαινόμενα να είναι σημαντικά.



Εικόνα 1. Quantum Superposition (https://link.springer.com/chapter/10.1007/978-3-030-61601-4_1).

1.1.3 Μέτρηση (Measurement)

Η μέτρηση φυσικών παρατηρήσιμων στοιχείων συνδέεται άμεσα με την κβαντική μηχανική καθώς μπορεί να μας δείξει ποια αποτελέσματα μετρήσεων είναι δυνατά καθώς και ποια είναι η πιθανότητα λήψης κάθε αποτελέσματος από τη μέτρηση. Παράλληλα, ενώ η μέτρηση γενικά δεν έχει καμία επίδραση σε ένα σύστημα στην κλασική μηχανική, σε ένα κβαντομηχανικό σύστημα έχει βαθύ αντίκτυπο, μεταβάλλοντας την κατάσταση του με μη αναστρέψιμο τρόπο. Παίζει θεμελιώδη ρόλο σε κβαντικούς υπολογισμούς αφού κάποια στιγμή θα πρέπει να αντλήσουμε πληροφορίες από το υπολογιστικό σύστημα. Όταν ένα κβαντικό bit υπάρχει σε υπέρθεση των καταστάσεων $|0\rangle$ και $|1\rangle$ αποτελεί ένα ιδιαίτερο φαινόμενο, καθώς κατά τη μέτρηση, το Qubit καταλήγει σε μία από αυτές τις καταστάσεις. Το αποτέλεσμα αυτού του κατακερματισμού δεν μπορεί να προβλεφθεί με βεβαιότητα, ωστόσο, είναι δυνατό να προσδιοριστεί η πιθανότητα του κβαντικού bit να καταρρεύσει σε μια συγκεκριμένη κατάσταση [2].

Μια μέτρηση είναι μια διαδικασία κατά την οποία κάποιος έχει δύο ξεχωριστά

φυσικά συστήματα, που αντιπροσωπεύονται από δύο σύνολα δυναμικών τελεστών. Επιπλέον, η δυναμική εξέλιξη είναι τέτοια ώστε, δεδομένων ορισμένων συνθηκών στη συσκευή μέτρησης, ένας προσδιορισμός κάποιας ποσότητας που σχετίζεται με αυτή θα δώσει πληροφορίες για το σύστημα ενδιαφέροντος. Ταυτόχρονα, εφόσον γίνεται λόγος για αλληλεπίδραση δύο συστημάτων σε ορισμένες περιπτώσεις, οι πληροφορίες που λαμβάνονται είναι ίδιες με έναν προσδιορισμό, αλλά σε άλλες περιπτώσεις μπορεί να διαφέρουν σημαντικά. Έτσι, λόγω της ομοιότητας της κυματομηχανικής με την κλασική κυματοθεωρία έχει επίσης προκύψει η λανθασμένη εντύπωση ότι οι συνθήκες στην κβαντομηχανική είναι εξ ολοκλήρου ισοδύναμες με τις συνθήκες της κλασικής μηχανικής, δηλαδή τις αρχικές συνθήκες. Στην κλασική φυσική, όλες οι καταστάσεις μπορούν, με τη χρήση της εξίσωσης κίνησης, να χαρτογραφηθούν στις αρχικές. Εάν δηλαδή, κάποιος μετρήσει τη θέση τώρα και την ορμή δύο μέρες μετά, ή τα μετρήσει και τα δύο ταυτόχρονα δεν έχει καμία απολύτως διαφορά [3].

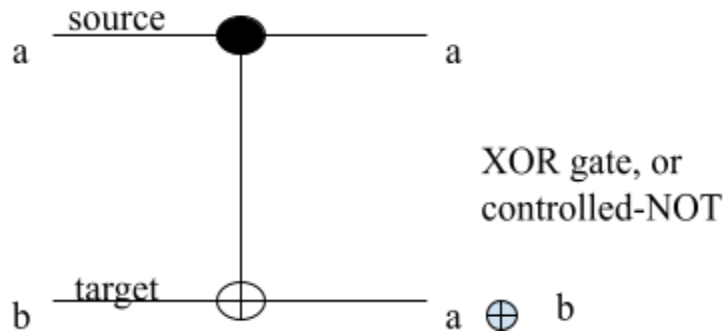
1.1.4 Κβαντικές Πύλες (Quantum Gates)

Το πιο κοινό μοντέλο υπολογισμού για κβαντικούς υπολογιστές είναι το μοντέλο κβαντικού κυκλώματος. Όπως και σε έναν κλασικό υπολογιστή, αυτό το μοντέλο έχει μία κβαντική πύλη που μετατρέπει το qubit εισόδου. Μια ακολουθία πυλών μπορεί να περιγραφεί πλήρως προσδιορίζοντας πως η υπολογιστική βάση, δηλαδή $\{|0\rangle, |1\rangle\}$ μετασχηματίζεται από τη λειτουργία μιας κβαντικής πύλης. Εν ολίγης, μία κβαντική πύλη αποτελεί έναν τελεστή που δρα σε qubits. Η αναστρέψιμη πύλη XOR (Controlled-NOT Gate) αποτελεί μια από τις κυριότερες κβαντικές πύλες καθώς λειτουργεί πάνω σε δύο qubits, ένα ελέγχου και ένα qubit στόχο. Ειδικότερα η πύλη CNOT:

- Αφήνει το qubit ελέγχου χωρίς να υπάρχει καμία μεταβολή και εκτελεί μια πύλη Pauli-X στο qubit στόχο όταν το qubit ελέγχου είναι σε κατάσταση $|1\rangle$.
- Αφήνει το qubit στόχο χωρίς να υπάρχει καμία μεταβολή όταν το qubit ελέγχου είναι σε κατάσταση $|0\rangle$.

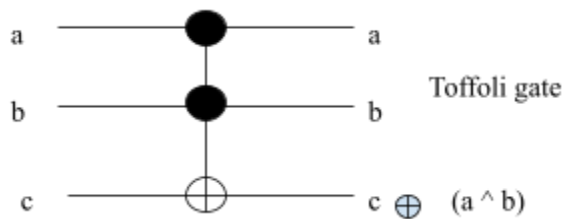
Κατά τη διάρκεια της δεκαετίας του 1970, ο Tom Toffoli, διερεύννησε πως θα μπορούσε να γίνει αναστρέψιμος υπολογισμός στην παραδοσιακή γλώσσα των λογικών πυλών Boole. Ειδικότερα, έδειξε ότι ένα σύνολο τροποποιημένων πυλών θα μπορούσε να χρησιμοποιηθεί στη θέση των παραδοσιακών λογικών πυλών Boole, όπως AND, OR, κλπ. Μια από αυτές, η οποία αποδείχθηκε ότι ήταν κεντρικής σημασίας στο επόμενο έργο κβαντικής πύλης είναι η πύλη που φαίνεται στην παρακάτω εικόνα. Η συγκεκριμένη πύλη γνωστή και ως αναστρέψιμη πύλη XOR ή πύλη ελεγχόμενου-NOT, έχει την ιδιότητα που υποδεικνύεται, δηλαδή το b bit μετατρέπεται στο XOR, ενώ το bit

είναι αμετάβλητο. Η απλή διατήρηση του bit κάνει την πύλη αναστρέψιμη ενώ η είσοδος είναι μια μοναδική συνάρτηση της εξόδου.



Εικόνα 2. Αναστρέψιμη πύλη XOR ή πύλη ελεγχόμενου-NOT.

Ταυτόχρονα, η πύλη XOR δεν είναι καθολική για Boolean υπολογισμούς, καθώς μια καθολική λογική πύλη είναι αυτή από την οποία μπορεί κανείς να συναρμολογήσει ένα κύκλωμα το οποίο θα αξιολογήσει οποιαδήποτε αυθαίρετη συνάρτηση Boole. Ειδικότερα, στη συνηθισμένη (μη αναστρέψιμη) λογική Boole, το NAND αποτελεί μια επιλογή για την καθολική πύλη. Ακόμη, ο Toffoli αναζήτησε μια άλλη αναστρέψιμη πύλη που θα μπορούσε να παίζει το ρόλο μιας καθολικής πύλης για αναστρέψιμα κυκλώματα. Η ανακάλυψή του είναι αυτό που ονομάζεται “Πύλη Toffoli” (Toffoli Gate) που φαίνεται στην παρακάτω εικόνα. Συγκεκριμένα, η πύλη απαιτεί τρία bit, και είναι εύκολο να αποδειχθεί ότι οποιαδήποτε καθολική αναστρέψιμη λογική πύλη boolean πρέπει να έχει τουλάχιστον τρία bit. Ουσιαστικά, αυτή είναι μια πύλη AND στην οποία αποθηκεύονται και τα δύο bit εισόδου, δηλαδή τα bit a, b παραμένουν αμετάβλητα, ενώ το bit c , εναλλάσσεται από τα a, b [4].



Εικόνα 3. Three-bit Toffoli gate.

1.2 Κβαντική Κρυπτογραφία

Η κρυπτογραφία είναι ένας τομέας εφαρμογών που παρέχει απόρρητο, αυθεντικοποίηση και εμπιστευτικότητα στους χρήστες. Ένας σημαντικός τομέας είναι αυτός της ασφαλούς επικοινωνίας, με στόχο να επιτρέπει την εμπιστευτική επικοινωνία μεταξύ διαφορετικών μερών, έτσι ώστε κανένας μη εξουσιοδοτημένος χρήστης να μην έχει πρόσβαση στο περιεχόμενο των μηνυμάτων. Με ανάλογο τρόπο, η κρυπτογράφηση RSA χρησιμοποιεί δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό, με βάση τη δημιουργία μεγάλων πρώτων αριθμών που είναι δύσκολο να υπολογιστούν. Η διαδικασία κρυπτογράφησης RSA περιλαμβάνει την επιλογή πρώτων αριθμών, τη δημιουργία προϊόντων και τη δημιουργία δημόσιων και ιδιωτικών κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Ο αλγόριθμος RSA χρησιμοποιεί την παρακάτω διαδικασία για την δημιουργία δημοσίων και ιδιωτικών κλειδιών:

- Επιλογή δύο μεγάλων πρώτων αριθμών, p και q .
- Πολλαπλασιασμός των αριθμών για την εύρεση του $n = p * q$, όπου n είναι ο συντελεστής κρυπτογράφησης και αποκρυπτογράφησης.
- Επιλογή ενός αριθμού e , όπου $e < n$ και ο n είναι σχετικά πρώτος στο $(p - 1) * (q - 1)$, δηλαδή το e και η παραπάνω σχέση δεν έχουν κανένα κοινό παράγοντα παρά μόνο το 1.
- Αν $n = p * q$, τότε το δημόσιο κλειδί είναι $\langle e, n \rangle$ και με αυτό μπορεί να κρυπτογραφηθεί ένα μήνυμα απλού κειμένου m . Η εύρεση κρυπτογραφημένου κειμένου από το απλό κείμενο γίνεται με τον ακόλουθο τύπο: $C = m^e \bmod n$, όπου εδώ το m πρέπει να είναι μικρότερο από το n .
- Για να προσδιορίσουμε το ιδιωτικό κλειδί, χρησιμοποιούμε τον ακόλουθο τύπο για τον υπολογισμό του d έτσι ώστε: $D_e \bmod \{(p - 1) * (q - 1)\} = 1$.
- Το ιδιωτικό κλειδί είναι $\langle d, n \rangle$ και μπορεί να χρησιμοποιηθεί στην αποκρυπτογράφηση ενός κρυπτογραφημένου κειμένου.
- Τέλος, για τον υπολογισμό απλού κειμένου m από το κρυπτογραφημένο κείμενο χρησιμοποιείται ο ακόλουθος τύπος: $m = c^d \bmod n$.

Η κβαντική κρυπτογραφία είναι ένας τομέας ο οποίος περιλαμβάνει τη χρήση της κβαντικής μηχανικής για τη δημιουργία ασφαλούς επικοινωνίας μέσω της διανομής κλειδιών, η οποία βασίζεται στους νόμους της φυσικής, ενώ παράλληλα προσφέρει πλεονεκτήματα έναντι των παραδοσιακών μεθόδων δημιουργώντας κλειδιά που είναι πιο δύσκολο να σπάσουν. Επιπλέον, χρησιμοποιεί την κβαντική μηχανική για να δημιουργήσει μυστικά κλειδιά μέσω μιας μεθόδου που ονομάζεται διανομή κβαντικών κλειδιών (QKD). Το QKD περιλαμβάνει τη χρήση τόσο ενός δημόσιου κλασικού καναλιού όσο και ενός κβαντικού καναλιού για την αποστολή κρυπτογραφημένων μηνυμάτων, με μεμονωμένα φωτόνια σε διαφορετικές καταστάσεις πόλωσης να

χρησιμοποιούνται για τη διανομή κλειδιών.

Η θεμελιώδης αρχή της κβαντικής μηχανικής, ότι η μέτρηση διαταράσσει μια κβαντική κατάσταση, αξιοποιείται στο QKD, καθιστώντας δύσκολη την υποκλοπή μηνυμάτων χωρίς ανίχνευση. Η κβαντική κρυπτογραφία προσφέρει μια πολλά υποσχόμενη εναλλακτική λύση στις παραδοσιακές μεθόδους κρυπτογράφησης, ειδικά ενόψει των πιθανών απειλών που θέτει ο κβαντικός υπολογιστής στην κρυπτογράφηση RSA καθώς έχει αποδειχθεί ότι η ασφάλειά της μπορεί να τεθεί σε κίνδυνο σύμφωνα με τον αλγόριθμο του Shor [5].

1.3 Quantum Key Distribution

Ως γνωστόν η ασφάλεια των περισσότερων παραδοσιακών κρυπτογραφικών συστημάτων βασίζεται στην πολυπλοκότητα των μαθηματικών αλγορίθμων και στον ανέφικτο χρόνο που απαιτείται για τη διακοπή τους. Ωστόσο, αυτή η ασφάλεια μπορεί να τεθεί σε κίνδυνο εάν η διαδικασία για τη διανομή μυστικών κλειδιών είναι αδύναμη. Το 1994 ο Peter Shor εισήγαγε έναν αλγόριθμο που παράγει αποτελεσματικά μεγάλους ακέραιους αριθμούς χρησιμοποιώντας αρχές κβαντικού υπολογισμού, θέτοντας μια πιθανή απειλή για τη συμβατική κρυπτογραφία. Η διανομή κβαντικού κλειδιού αποτελεί μια νέα τεχνολογία ασφάλειας που εξαρτάται από τους νόμους της κβαντικής μηχανικής για να μοιράζεται το μυστικό κλειδί και να παρέχει άνευ όρων ασφάλεια. Παράλληλα το QKD, έχει μια νέα ικανότητα που δεν ανήκει στη συμβατική τεχνική κρυπτογραφίας, δηλαδή την ικανότητα ανίχνευσης της παρουσίας κακόβουλου χρήστη. Επιπλέον, σε θεωρητικό επίπεδο το QKD έχει αποδειχθεί ότι προσφέρει επικοινωνία που είναι άνευ όρων ασφαλής με βάση τους νόμους της κβαντικής μηχανικής και παρακάτω αναλύονται μερικά πρωτόκολλα βασισμένα στο Quantum Key Distribution.



Εικόνα 4. Block Diagram ενός QKD συστήματος (<https://ieeexplore.ieee.org/document/8527822>).

Στην παραπάνω εικόνα φαίνεται ένα σύστημα QKD, αποτελούμενο από τον αποστολέα (Alice), τον παραλήπτη (Bob), τον κακόβουλο χρήστη (Eve) και δύο κανάλια: το κβαντικό και το δημόσιο. Το κβαντικό κανάλι χρησιμοποιείται για τη μετάδοση και την ανταλλαγή πληροφοριών μυστικού κλειδιού με τη μορφή κβαντικών bit (qubits). Ταυτόχρονα, το δημόσιο κανάλι χρησιμοποιείται για τη μετάδοση των qubits και τη διαπραγμάτευση του κοινού μυστικού κλειδιού. Οι δύο κυριότεροι τύποι μέσων που εφαρμόζονται μέσω του συστήματος QKD είναι η οπτική ίνα και ο ελεύθερος χώρος [6].

Η υλοποίηση του QKD χωρίζεται σε τέσσερις κύριες διαδικασίες:

- Ανταλλαγή ακατέργαστου κλειδιού
- Key sifting
- Key distillation
- Usable key size

Στην ανταλλαγή ακατέργαστου κλειδιού, τα δύο μέρη ανταλλάσσουν qubits σε ένα μη αξιόπιστο κανάλι και έπειτα γίνεται η κωδικοποίησή τους χρησιμοποιώντας συγκεκριμένες καταστάσεις πόλωσης σωματιδίων φωτός. Σε αντίθεση με την κλασική επικοινωνία, όπου οι πληροφορίες κωδικοποιούνται χρησιμοποιώντας επίπεδα ηλεκτρικής τάσης ή παλμούς λέιζερ, η κβαντική επικοινωνία βασίζεται στις ιδιότητες των φωτονίων. Δηλαδή, κάθε qubit προετοιμάζεται με 0 είτε με 1 και τα επίπεδα πόλωσής τους μετρώνται για να εξαχθεί το ακατέργαστο κλειδί. Τέλος, αξίζει να σημειωθεί ότι τα qubits δεν μπορούν να κλωνοποιηθούν ή να διαχωριστούν χωρίς την εισαγωγή ανιχνεύσιμων διαταραχών, εξασφαλίζοντας έτσι την ασφάλεια που βασίζεται στους φυσικούς νόμους.

Η ανταλλαγή ακατέργαστου κλειδιού (key shifting) αναφέρεται σε τεχνικές που χρησιμοποιούνται κατά τη διάρκεια της διαδικασίας δημιουργίας κλειδιών για την ενίσχυση της ασφάλειας και τη μείωση του κινδύνου υποκλοπής. Μερικές προσεγγίσεις για την ανταλλαγή ακατέργαστων κλειδιών αποτελούν οι Αλγόριθμοι Ακατέργαστων Κλειδιών Συνεχούς Μεταβλητής (CV-QKD) αλλά και η Διαφορική Μετατόπιση Φάσης Κβαντικής Διανομής Κλειδιών.

Με ανάλογο τρόπο, το key distillation αποτελεί μια κρίσιμη φάση στη διαδικασία του QKD, κατά την οποία εξασφαλίζεται ότι το τελικό κοινό μυστικό κλειδί μεταξύ των δύο μερών, είναι ασφαλές και ταυτόσημο, παρά την παρουσία θορύβου και πιθανών υποκλοπών. Τέλος, το key distillation αποτελείται από τα βήματα της διαλογής, διόρθωσης σφαλμάτων, εκτίμηση παραμέτρων και ενίσχυση απορρήτου. Η τελευταία κατηγορία για την υλοποίηση του QKD αποτελείται από το συμμετρικό μήκος κλειδιού (Usable key size), το οποίο δεν αποτελεί σταθερό αριθμό αλλά εξαρτάται από δύο παράγοντες:

1. Επίπεδο ασφάλειας: Όσο υψηλότερη είναι η ασφάλεια που απαιτείται τόσο μεγαλύτερο χρειάζεται να είναι το κλειδί.

2. Χαρακτηριστικά κβαντικού καναλιού: Οι απώλειες μετάδοσης όπως και ο θόρυβος που υπάρχει στο κανάλι μπορούν να μειώσουν το μήκος του χρησιμεύσιμου κλειδιού.

1.4 Αλγόριθμος BB84

Σύμφωνα με τις παραπάνω διαδικασίες λοιπόν οι Bennett και Brassard το 1984, υλοποίησαν το πρώτο πρωτόκολλο διανομής κβαντικού κλειδιού, το οποίο χρησιμοποιεί την κωδικοποίηση των κλασικών bits σε qubits, δηλαδή κβαντικά συστήματα δύο επιπέδων. Πρόκειται για το πρώτο πρωτόκολλο κβαντικής κρυπτογραφίας το οποίο εξηγούσε τη χρήση της κατάστασης πόλωσης των φωτονίων για την μετάδοση των πληροφοριών ενός μυστικού κλειδιού μέσω ενός κβαντικού καναλιού επικοινωνίας. Αυτό το πρωτόκολλο είναι γνωστό ως BB84 και κατηγοριοποιείται ως βάση προετοιμασίας και μέτρησης του πρωτοκόλλου QKD.

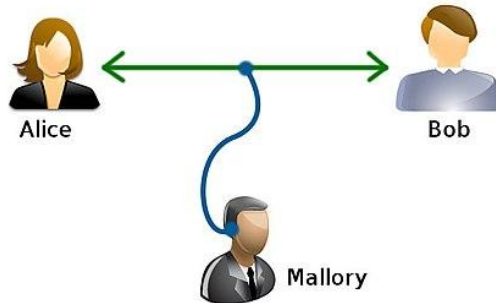
Ειδικότερα, η Alice και ο Bob επιθυμούν να δημιουργήσουν ένα μυστικό κλειδί εξ αποστάσεως και για να το καταφέρουν αυτό, έχουν πρόσβαση σε δύο κανάλια: το πρώτο αποτελεί ένα κλασικό κανάλι από το οποίο οι δύο χρήστες μπορούν να στέλνουν μηνύματα και να επικοινωνούν έχοντας πρώτα ταυτοποιηθεί. Σε αυτή τη περίπτωση ένας κακόβουλος χρήστης όπως η Eve (Eavesdropper) μπορεί παράλληλα να ακούσει όλη τη συνομιλία χωρίς όμως να έχει τη δυνατότητα να αλλάξει τα μηνύματα που αποστέλλονται. Το δεύτερο, είναι το κβαντικό κανάλι, το οποίο επιτρέπει στην Alice και τον Bob να στέλνουν κβαντικά σήματα, μια δραστηριότητα υψηλού κινδύνου καθώς σε αυτή τη περίπτωση ο κακόβουλος χρήστης μπορεί να εκτελέσει οποιαδήποτε πράξη στην πληροφορία που αποστέλλεται.

Το BB84 περιλαμβάνει δύο βασικά μέρη: τη φάση της κβαντικής μετάδοσης, κατά την οποία οι χρήστες (Alice, Bob) προετοιμάζουν, αποστέλλουν και μετρούν τις κβαντικές καταστάσεις. Ενώ το δεύτερο μέρος, αποτελεί τη φάση μετά την επεξεργασία που είναι καθαρά κλασικό, καθώς η Alice και ο Bob επικοινωνούν μόνο στο κλασικό κανάλι για να μετατρέψουν τα bit strings από την πρώτη φάση σε ασφαλή κλειδιά.

Η πόλωση του φωτός αναφέρεται στον προσανατολισμό των ηλεκτρομαγνητικών κυμάτων που απαρτίζουν το φως. Τα φωτόνια έχουν τη δυνατότητα να εμφανίζουν διαφορετικές πολωμένες καταστάσεις, που περιγράφουν την κατεύθυνση ταλάντωσης του ηλεκτρικού πεδίου σε σχέση με την κατεύθυνση κίνησης του φωτονίου. Επομένως, η παραπάνω ιδιότητα καθίσταται χρήσιμη στην κβαντική επικοινωνία και κρυπτογραφία για την κωδικοποίηση πληροφοριών ή την κατανομή κβαντικών κλειδιών αντίστοιχα.

Το πρωτόκολλο BB84 χρησιμοποιεί τέσσερις κβαντικές καταστάσεις που προετοιμάζονται τυχαία από τον αποστολέα (Alice) σε μία από τις δύο βάσεις για τη μετάδοση πληροφοριών στον δέκτη (Bob). Οι τέσσερις κβαντικές καταστάσεις είναι οι εξής:

1. $|0\rangle$ και $|1\rangle$ στην ευθύγραμμη βάση (βάση-X), όπου $|0\rangle = (1,0)$ και $|1\rangle = (0,1)$
2. $|+\rangle$ και $|-\rangle$ στην διαγώνια βάση (βάση-Y), όπου $|+\rangle = (1/\sqrt{2})(1, 1)$ και $|-\rangle = (1/\sqrt{2})(1, -1)$



Εικόνα 5. Κλασικό Παράδειγμα Επικοινωνίας μεταξύ Alice, Bob και Mallory ([Alice and Bob | Detailed Pedia](#)).

Στην εικόνα 3, παρατηρούμε τη διαδικασία επικοινωνίας μεταξύ της Alice και του Bob με τον Mallory να είναι ο πιθανός εισβολέας που μπορεί να επιχειρήσει να υποκλέψει την επικοινωνία τους. Έτσι, το BB84 αποτελείται από τα παρακάτω βήματα:

1. Η Alice δημιουργεί μια τυχαία ακολουθία bit και κωδικοποιεί κάθε bit σε μια τυχαία επιλεγμένη κατάσταση πόλωσης χρησιμοποιώντας μία από τις δύο βάσεις, είτε ευθύγραμμη είτε διαγώνια.
2. Η Alice στέλνει τα κωδικοποιημένα φωτόνια στον Bob μέσω του κβαντικού καναλιού.
3. Ο Bob επιλέγει τυχαία μια από τις δύο βάσεις για να μετρήσει την πόλωση κάθε φωτονίου που λαμβάνει από την Alice.
4. Ο Bob μετρά κάθε φωτόνιο και καταγράφει τα αποτελέσματα είτε ως 0 είτε ως 1.
5. Μετά τη μετάδοση, η Alice και ο Bob αποκαλύπτουν δημόσια τις βάσεις που χρησιμοποίησαν για κάθε bit πάνω από το κλασικό κανάλι.
6. Η Alice και ο Bob απορρίπτουν τα κομμάτια όπου οι βάσεις δεν συμπίπτουν.
7. Τα υπόλοιπα bits σχηματίζουν το κλειδί.
8. Για τη διασφάλιση της ασφάλειας του κλειδιού η Alice και ο Bob πραγματοποιούν μια δοκιμή για να ανιχνεύσουν τυχόν πιθανές υποκλοπές συγκρίνοντας ένα υποσύνολο του κλειδιού τους σε σχέση με το κλασικό κανάλι.
9. Τέλος, χρησιμοποιούνται τεχνικές διόρθωσης σφαλμάτων και ενίσχυσης απορρήτου για να εξαγάγουν ένα πιο σύντομο, αλλά ασφαλές, κοινόχρηστο μυστικό κλειδί.

Για την διασφάλιση της μέγιστης πιθανής ασφάλειας του κλειδιού που δημιουργείται μέσω του πρωτοκόλλου BB84, η Alice και ο Bob διενεργούν με σχολαστικό τρόπο μια κεντρική δοκιμή που έχει σχεδιαστεί για την ανίχνευση πιθανών υποκλοπών. Αυτό περιλαμβάνει μια προσεκτική σύγκριση ενός τυχαία επιλεγμένου υποσυνόλου του κλειδιού σε σχέση με το κλασικό κανάλι. Έτσι, η Alice γνωστοποιεί το επιλεγμένο υποσύνολο στον Bob, ο οποίος στη συνέχεια το εξετάζει προσεκτικά σε σχέση με το δικό του, μοιράζοντας άμεσα τα αποτελέσματα με την Alice. Μια ουσιαστική συσχέτιση μεταξύ των υποσυνόλων υποδηλώνει την απουσία ενός κακόβουλου χρήστη στο κβαντικό κανάλι, επιβεβαιώνοντας την ασφάλεια του κλειδιού.

Από την άλλη πλευρά, η έλλειψη επικοινωνίας υποδηλώνει πιθανή υποκλοπή, προκαλώντας άμεσο τερματισμό του πρωτοκόλλου. Η συγκεκριμένη δοκιμή που ονομάζεται “ένισχυση απορρήτου”(privacy amplification) αποτελεί αναπόσπαστο κομμάτι της διαφύλαξης της διανομής κλειδιού. Η ακρίβεια της γνησιότητας του κλειδιού εξαρτάται από το αν η Alice και ο Bob μέτρησαν στις ίδιες βάσεις, με αποτέλεσμα να υπάρχει 100% ακρίβεια, ή εάν επιλέχθηκαν διαφορετικές βάσεις μειώνοντας έτσι την ακρίβεια στο 50%. Ουσιαστικά το BB84 δίνει τη δυνατότητα σε δύο μέρη να δημιουργήσουν ένα κοινό μυστικό κλειδί σε ένα μη ασφαλές κανάλι, εναρμονίζοντας κατ’ αυτόν τον τρόπο τις αρχές της κβαντικής μηχανικής με την κλασική επικοινωνία [7].

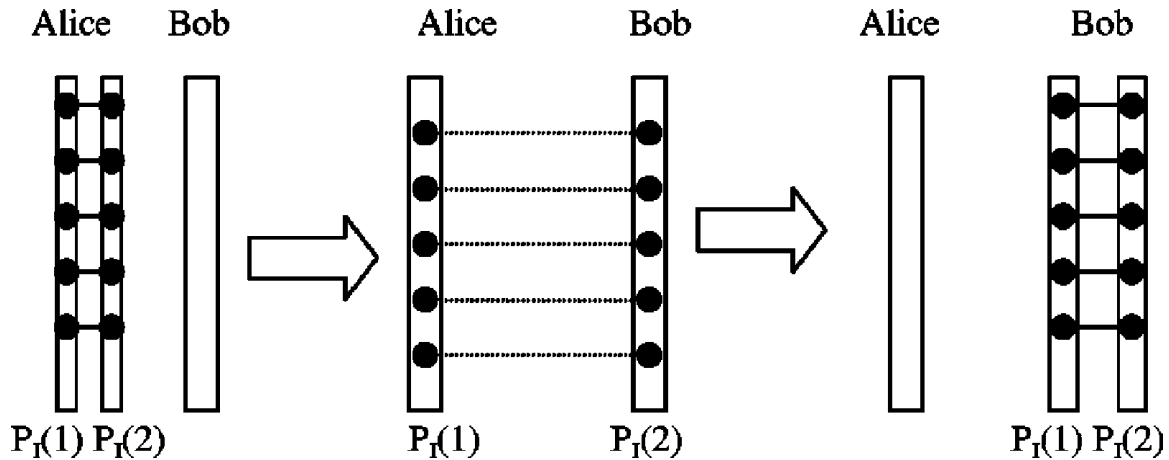
2. Κβαντική Ασφαλής Άμεση Επικοινωνία

2.1 Διανομή Κβαντικού Κλειδιού Υψηλής Χωρητικότητας

Η εξέλιξη του ανθρώπινου είδους σε συνδυασμό με τις πολυάριθμες γλώσσες οδήγησε στην ανάγκη ασφαλούς επικοινωνίας και μετάδοση μηνυμάτων με εχεμύθεια από το ένα άτομο στο άλλο. Έτσι, ανακαλύφθηκε η κρυπτογραφία, ένας τρόπος διάδοσης πληροφοριών, ώστε να είναι ακατανόητες για όσους δεν προορίζονται να έχουν πρόσβαση στο μήνυμα. Ένας από τους γνωστότερους τρόπους κρυπτογράφησης αποτελεί το κρυπτοσύστημα δημοσίου κλειδιού, καθώς η ασφάλειά του εξαρτάται από την υψηλή πολυπλοκότητα των μαθηματικών πράξεων.

Ωστόσο, η ανάπτυξη του κβαντικού υπολογισμού και συγκεκριμένα ο αλγόριθμος του Shor, για την παραγοντοποίηση μεγάλων αριθμών, αποτελεί ήδη μεγάλη απειλή σε τέτοιου είδους κρυπτοσυστήματα. Η κβαντομηχανική αποτελεί πλέον μια από τις μεγαλύτερες ανακαλύψεις του 20^{ου} αιώνα, ενώ η συνδυαστική προσέγγιση του κβαντισμού με την κρυπτογραφία μπορεί να βοηθήσει στην ασφαλή διανομή του κλειδιού για την επίτευξη ασφαλούς κβαντικής επικοινωνίας. Ειδικότερα, τέτοια σχήματα διανομής κβαντικών κλειδιών (QKD) είναι τα BB84, EPR και B92.

Παρακάτω αναλύεται ένα πρωτόκολλο που χρησιμοποιεί ζεύγη EPR για τη διανομή κλειδιού μεταξύ της Alice και του Bob, που περιλαμβάνει μετρήσεις με βάση την αρχή του Bell καθώς και ελέγχους υποκλοπής. Το συγκεκριμένο πρωτόκολλο είναι υπεύθυνο για την ασφάλεια έναντι των επιθέσεων από πιθανούς κακόβουλους χρήστες όπως η Eve (eavesdropper), καθώς τους εμποδίζει από το να αποκτήσουν χρήσιμες πληροφορίες. Ειδικότερα, η Alice παράγει EPR ζεύγη, ο Bob επιλέγει ένα υποσύνολο για μέτρηση και γίνονται επακόλουθοι έλεγχοι για τη διασφάλιση της ασφαλούς διανομής κλειδιού. Παράλληλα, η ασφάλεια του συστήματος έγκειται στην ικανότητά του να ανιχνεύει απόπειρες υποκλοπής, διασφαλίζοντας την ακεραιότητα των διανεμημένων κλειδιών.



Εικόνα 6. Αναπαράσταση του QKD πρωτοκόλλου (<https://journals.aps.org/pr/abstract/10.1103/PhysRevA.65.032302>).

Όπως φαίνεται στην παραπάνω απεικόνιση, κατά τη διάρκεια της μετάδοσης της δεύτερης ακολουθίας σωματιδίων, η Eve δεν μπορεί να έχει πρόσβαση στα ζεύγη EPR και ως εκ τούτου δεν μπορεί να κλέψει το κλειδί. Η δράση της προκαλεί απλώς αναστάτωση στο κλειδί, που στην πραγματικότητα αποτελεί ένα είδος καταστροφής. Επίσης, ο δεύτερος έλεγχος υποκλοπής έχει σχεδιαστεί για την ανίχνευση αυτού. Στην πράξη, αυτή η διαδικασία συνδυάζεται με τη διαδικασία ενίσχυσης της ιδιωτικότητας στο στάδιο επεξεργασίας του QKD.

2.1.1 Ασφάλεια Πρωτοκόλλου

Αρχικά, όσον αφορά την επίθεση με άμεση μέτρηση από την Eve (eavesdropper) υπάρχει ασφάλεια, καθώς σε αυτή την περίπτωση ανακόπτεται η πρώτη ακολουθία σωματιδίων, γίνονται μετρήσεις πάνω σε αυτά και η Eve στέλνει ξανά την μετρημένη ακολουθία στον Bob. Λόγω της συγκεκριμένης μέτρησης, όλα τα ζεύγη EPR, με τη μια ακολουθία σωματιδίων να κατέχεται από την Alice και την άλλη από τον Bob, καταστρέφονται. Κατά τη διάρκεια της πρώτης διαδικασίας ελέγχου υποκλοπής, η καταστροφή της Eve δεν είναι ανιχνεύσιμη επειδή η μέτρηση του Bob θα αποφέρει ακριβώς τα ίδια αποτελέσματα με εκείνα της Eve, συνεπώς θα υπάρχει ομοιότητα και με τα αποτελέσματα της Alice.

Ωστόσο, κατά τη διάρκεια του δεύτερου ελέγχου υποκλοπής, η δράση της Eve εντοπίζεται πιο εύκολα. Από τη στιγμή λοιπόν, που τα ζεύγη EPR έχουν καταρρεύσει, ο Bob θα έχει μόνο το 50% των πιθανοτήτων να επιτύχει το σωστό αποτέλεσμα όταν χρησιμοποιεί τη Bell-basis μέτρηση για να διαβάσει τα ζεύγη EPR. Συμπερασματικά, το ποσοστό λάθους (error rate) φτάνει έως το 50% και μπορεί εύκολα να εντοπιστεί, ενώ η Eve δεν μπορεί να λάβει χρήσιμες πληροφορίες από αυτή την καταστροφική επίθεση.

Ταυτόχρονα, το συγκεκριμένο πρωτόκολλο είναι εξίσου ασφαλές ως προς τις επιθέσεις αναχαίτισης-εκ νέου αποστολής (intercept-resend attack). Έστω ότι η Eve παρεμποδίζει την ακολουθία σωματιδίων $\{P_i(2), i=1, \dots, N\}$ και τη διατηρεί, αλλά δεν μπορεί να κάνει μια μέτρηση με βάση το θεώρημα του Bell, αφού δεν κατέχει την άλλη ακολουθία σωματιδίων. Για να την αποκτήσει, πρέπει να στείλει μια ψεύτικη ακολουθία στον Bob, ώστε εκείνος να ειδοποιήσει την Alice.

Βέβαια, αυτό μπορεί να εντοπιστεί άμεσα κατά τον πρώτο έλεγχο υποκλοπής, καθώς ο Bob επιλέγει τυχαία ένα υποσύνολο σωματιδίων και τα μετρά. Στη συνέχεια, ενημερώνει την Alice αναφορικά με το ποια σωματίδια έχει μετρήσει έτσι ώστε να κάνει και εκείνη την ίδια διαδικασία. Έπειτα, μοιράζονται και οι δύο τα αποτελέσματά τους και τα συγκρίνουν δημόσια. Εάν λοιπόν η ακολουθία του Bob είναι η ψεύτικη που έστειλε η Eve, τότε τα μισά αποτελέσματα δεν θα συμπίπτουν με εκείνα της Alice, έχοντας ως αποτέλεσμα τον εύκολο εντοπισμό της Eve.

Τέλος, μια ακόμη περίπτωση κατά την οποία το πρωτόκολλο παραμένει ασφαλές είναι η επίθεση αδιαφανούς στρατηγικής (opaque attack strategy). Ειδικότερα, στόχος της Eve είναι να παρεμποδίζει κάθε σήμα και να το μετρά. Εάν λαμβάνει αποτέλεσμα, αφήνει το σήμα να μεταδοθεί, ενώ σε διαφορετική περίπτωση το καταστρέφει εντελώς. Παρόλα αυτά, στο συγκεκριμένο σχήμα είναι αδύνατον να χρησιμοποιηθεί αυτή η στρατηγική αφού η Alice στέλνει στον Bob μόνο μία αλληλουχία σωματιδίων τη φορά, γεγονός που την καθιστά άχρηστη χωρίς την άλλη ακολουθία. Εν ολίγης, το παραπάνω πρωτόκολλο επιτυγχάνει υψηλό ποσοστό αποτελεσματικότητας, ξεπερνώντας άλλα πρωτόκολλα όπως το BB84 και το EPR, καθώς η ικανότητα του συστήματος να διανέμει μυστικά κλειδιά σε πολλούς χρήστες και η κοινή δυνατότητα διανομής κλειδιών το κάνει να ξεχωρίζει από τα υπόλοιπα [8].

2.2 Πρωτόκολλο Άμεσης Κβαντικής Επικοινωνίας με χρήση του Einstein-Podolsky-Rosen μπλοκ

Η Κατανομή Κβαντικού Κλειδιού ή εναλλακτικά QKD, αναπτύσσεται με ταχύ ρυθμό, ειδικά μετά την εφεύρεση του αλγορίθμου BB84 τη δεκαετία του 1980, ενώ ταυτόχρονα, έγινε η διάκριση διαφόρων QKD σχημάτων, τα οποία μπορούν να χωριστούν σε δύο κατηγορίες: τα ντετερμινιστικά και τα μη ντετερμινιστικά. Ειδικότερα, το χαρακτηριστικό των μη ντετερμινιστικών σχημάτων είναι ότι ο αποστολέας (Alice) επιλέγει με τυχαίο τρόπο δύο σελ από measuring bases έτσι ώστε να παραχθούν τουλάχιστον δύο ειδών καταστάσεις και στη συνέχεια να αποσταλούν στον παραλήπτη (Bob). Έπειτα, ο Bob, επιλέγει τυχαία ένα από τα δύο σελ βάσεων για τη μέτρηση των καταστάσεων. Σε αυτή τη περίπτωση, υπάρχει μόνο μία συγκεκριμένη πιθανότητα ότι η Alice και ο Bob θα επιλέξουν τις ίδιες βάσεις (measuring bases). Συνεπώς, η Alice δεν μπορεί να προσδιορίσει ποια τιμή bit θα λάβει ο Bob, προτού γίνει ανταλλαγή κλασικών

πληροφοριών. Ωστόσο, σε ένα ντετερμινιστικό σχήμα, η Alice και ο Bob επιλέγουν την ίδια βάση για τις μετρήσεις τους έτσι ώστε να καταλήξουν στα ίδια αποτελέσματα εφόσον το κβαντικό κανάλι δεν διαταραχθεί.

Μία ασφαλής άμεση επικοινωνία συνεπάγεται τη μετάδοση σημαντικών μηνυμάτων απευθείας, χωρίς να προηγηθεί η δημιουργία τυχαίου κλειδίου για την κρυπτογράφηση τους. Έτσι, είναι απαραίτητο να ικανοποιούνται δύο απαιτήσεις. Αρχικά, τα μηνύματα πρέπει να διαβάζονται απευθείας από τον νόμιμο παραλήπτη (Bob), όταν αυτός λαμβάνει τις κβαντικές καταστάσεις χωρίς καμία πρόσθετη κλασική πληροφορία να χρειάζεται μετά τη μετάδοση. Κατά δεύτερον, τα ήδη κωδικοποιημένα μηνύματα μέσα στις κβαντικές καταστάσεις δεν πρέπει να διαρρέουν ακόμα κι αν ένας κακόβουλος χρήστης εισέλθει στο κανάλι, διότι εφόσον η Eve (eavesdropper), αποκτήσει πρόσβαση τόσο στο κανάλι όσο και στα μηνύματα, η μετάδοσή τους καθίσταται πολύ δύσκολη έως και αδύνατη.

Παρακάτω θα αναλυθεί ένα Quantum Secure Direct Communication σχήμα με τη χρήση των EPR ζευγών. Ένα ζεύγος EPR μπορεί να βρεθεί σε μια από τις παρακάτω καταστάσεις Bell:

$$\bullet \quad |\Phi^+\rangle = (1/\sqrt{2})(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \quad (2.1)$$

$$\bullet \quad |\Phi^-\rangle = (1/\sqrt{2})(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B) \quad (2.2)$$

$$\bullet \quad |\Psi^+\rangle = (1/\sqrt{2})(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) \quad (2.3)$$

$$\bullet \quad |\Psi^-\rangle = (1/\sqrt{2})(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) \quad (2.4)$$

Το QSDC περιλαμβάνει την Alice και τον Bob οι οποίοι προετοιμάζουν ζεύγη EPR σε καταστάσεις Bell, μεταδίδουν ακολουθίες ζευγών EPR, εκτελούν ελέγχους ασφαλείας, κωδικοποιούν μηνύματα και διορθώνουν σφάλματα. Με αυτόν τον τρόπο το πρωτόκολλο διασφαλίζει την ασφάλεια ελέγχοντας για υποκλοπή στη μετάδοση της ακολουθίας C. Επομένως, θα μαθευτεί άμεσα εάν υπάρχει κάποιος κακόβουλος χρήστης στην κβαντική γραμμή, ενώ ταυτόχρονα, η Eve (eavesdropper) δεν μπορεί να διαβάσει τις πληροφορίες, ακόμη και αν αποκτήσει πρόσβαση σε μία από τις ακολουθίες, διότι είναι αδύνατον να γνωστοποιηθούν πληροφορίες ενός σωματιδίου από ένα ζεύγος EPR μόνο. Συνεπώς, καμία πληροφορία δεν μπορεί να διαρρεύσει στην Eve και η χωρητικότητα είναι αρκετά υψηλή αφού κάθε EPR ζεύγος φέρει δύο bit κλασικής πληροφορίας.

2.2.1 Ασφάλεια Πρωτοκόλλου

Παράλληλα, το QSDC πρωτόκολλο βασίζεται σε EPR ζεύγη και έτσι η ασφάλειά του είναι όμοια με εκείνη των πεπλεγμένων φωτονίων. Ειδικότερα, η απόδειξη των παραπάνω γίνεται με βάση την ασφάλεια για τη μετάδοση της ακολουθίας C. Αν δηλαδή, η Alice και ο Bob δεν μπορούσαν να εντοπίσουν την Eve κατά τη μετάδοση της ακολουθίας C, η Eve θα μπορούσε με ευκολία να συλλάβει τα δύο φωτόνια σε κάθε EPR ζεύγος και να κάνει μετρήσεις με βάση τον Bell έτσι ώστε να διαβάσει το μυστικό μήνυμα.

Στο συγκεκριμένο πρωτόκολλο, η μετάδοση και ο έλεγχος ασφαλείας της ακολουθίας C είναι παρόμοια με τις διαδικασίες στο πρωτόκολλο BBM92, όπου ένα ζεύγος EPR αποστέλλεται στην Alice και το άλλο στον Bob. Σε αυτήν την περίπτωση τα σωματίδια της ακολουθίας M διατηρούνται με ασφάλεια στην τοποθεσία της Alice καθώς πριν ελέγξει την υποκλοπή, η Εύα δεν έχει πρόσβαση στα σωματίδια της ακολουθίας M. Επομένως, η ασφάλεια μετάδοσης για την ακολουθία C απλώς μειώνεται στην ασφάλεια του πρωτοκόλλου BBM92 QKD και έτσι συμπεραίνουμε ότι το QSDC είναι ασφαλές.

Σε περίπτωση που η Εύα μπορεί να συλλέξει μόνο ένα φωτόνιο σε κάθε ζεύγος EPR, τότε η λήψη πληροφοριών καθίσταται αδύνατη. Αντιθέτως, ο τρόπος με τον οποίο είναι εφικτή η υποκλοπή, είναι η προσποίηση του Bob ότι έλαβε την ακολουθία C και να σταλεί στον ίδιο μία ψεύτικη ακολουθία. Αν η Alice και ο Bob δεν αντιληφθούν την παραπάνω πράξη, αυτόματα η Eve δύναται να διακόψει την ακολουθία M και να αποκρυπτογραφήσει τις πληροφορίες που φέρουν τα EPR ζεύγη. Μόνο όταν δηλαδή η Alice και ο Bob διαπιστώσουν ότι δεν υπάρχει παρακολούθηση από τρίτους, μεταδίδουν την ακολουθία M.

Σαφέστατα, οι παραπάνω αποδείξεις βασίζονται σε ιδανικές καταστάσεις και δεν λαμβάνουν υπόψη τον θόρυβο στην μετάδοση. Σε ένα κανάλι χαμηλού θορύβου, η απώλεια φωτονίων θα είναι μικρή και η Eve θα αυξήσει είτε το ποσοστό σφάλματος είτε την απώλεια σήματος. Έτσι η ασφάλεια της ακολουθίας C θα είναι εξασφαλισμένη εάν η Alice και ο Bob κάνουν τον πρώτο έλεγχο υποκλοπής και αναλύσουν το ποσοστό σφάλματος και την αποτελεσματικότητα. Αντιθέτως εάν η απώλεια κβαντικού καναλιού είναι αρκετά υψηλή προκύπτουν τα εξής προβλήματα:

- Ασφάλεια μετάδοσης της ακολουθίας C, που απαιτεί από την Alice και τον Bob να μοιράζονται μια ακολουθία πεπλεγμένων καταστάσεων.
- Απώλεια ακολουθίας M.

Χωρίς μέτρηση ο Bob δεν μπορεί να βεβαιωθεί εάν λαμβάνει τα σωματίδια ή όχι στην ακολουθία C και η Alice πρέπει να κωδικοποιήσει όλα τα σωματίδια στην ακολουθία M. Έτσι, η υποκλοπή της Eve δεν μπορεί να ανιχνευθεί εάν συλλάβει μερικά από τα σωματίδια της ακολουθίας και στείλει τα άλλα στον Bob με ένα καλύτερο κβαντικό

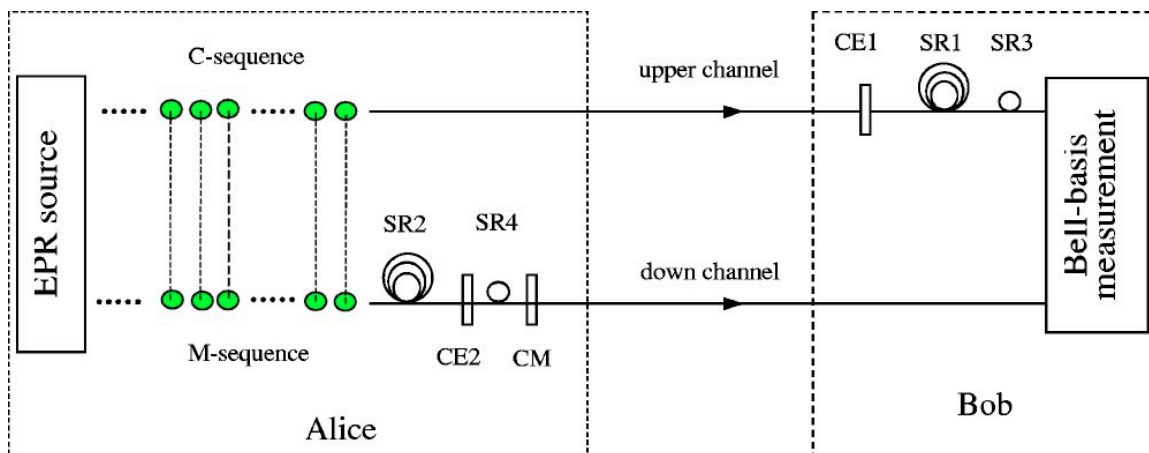
κανάλι με το οποίο δεν αυξάνεται η απωλεστική απόδοση όλων των φωτονίων. Με αυτόν τον τρόπο, η Eve παρεμποδίζει την ακολουθία M και κάνει μέτρηση Bell για να λάβει ένα μέρος του μυστικού μηνύματος.

Προκειμένου να αποφευχθεί η επίθεση στην ακολουθία C και να μοιραστεί μια ακολουθία ζευγών EPR με ασφάλεια, ο Bob είναι αναγκαίο να πραγματοποιήσει εναλλαγή κβαντικής διεμπλοκής στα σωματίδια που λαμβάνει πρώτα και στη συνέχεια να λάβει ένα υποσύνολο της ακολουθίας C σωματιδίων που μπλέκονται με την αλληλουχία της Alice. Έτσι, αν υπάρχουν πράγματι σωματίδια εκεί, η εναλλαγή θα πετύχει, διαφορετικά θα υπάρχει αποτυχία και με αυτόν τον τρόπο η λειτουργία εναλλαγής εδώ χρησιμεύει ως ανίχνευση ύπαρξης σωματιδίων.

Ταυτόχρονα, για να επιτύχουμε τη βελτιωμένη ασφάλεια και αποτελεσματικότητα του παραπάνω σχεδίου είναι απαραίτητη η προσωρινή αποθήκευση της ακολουθίας επαλήθευσης των φωτονίων. Έτσι είναι εφικτός ο έλεγχος για υποκλοπή προτού ληφθεί η πραγματική ακολουθία δεδομένων (ακολουθία M) και αυτό επιτυγχάνεται με συσκευές αποθήκευσης φωτός και οπτικές καθυστερήσεις. Οπότε σύμφωνα με την τεχνική ηλεκτρομαγνητικής επαγόμενης διαφάνειας, η ακολουθία C των φωτονίων, είναι εφικτό να αποθηκευτεί για ένα μικρό χρονικό διάστημα έως ότου ολοκληρωθεί ο έλεγχος υποκλοπής και η μεταφορά της M αλληλουχίας.

Από την άλλη πλευρά, η χρήση οπτικών καθυστερήσεων αποτελεί ένα καλά ανεπτυγμένο τεχνολογικό επίτευγμα καθώς, αντί να γίνει παραγωγή των EPR ζευγών ταυτόχρονα, μπορούμε να παράγουμε μια χρονικά διατεταγμένη ακολουθία ζεύγους EPR. Στο παρακάτω σχήμα παρατηρούμε μια ακολουθία EPR, όπου παράγεται στην τοποθεσία της Alice, και έτσι το ένα φωτόνιο μετά το άλλο αποστέλλεται στην τοποθεσία του Bob μέσω της άνω γραμμής και έπειτα η αντίστοιχη M ακολουθία αποστέλλεται μέσω της κάτω γραμμής μετάδοσης. Στη συνέχεια, όταν η ακολουθία C φτάσει στον Bob, ο ίδιος διαλέγει με τυχαίο τρόπο μερικά φωτόνια για έλεγχο υποκλοπής, γίνεται η τυχαία μέτρηση αυτών και τέλος ανακοινώνονται οι θέσεις, η βάση μέτρησης και τα αποτελέσματα των επιλεγμένων φωτονίων.

Εφόσον τα αποτελέσματα γνωστοποιηθούν στην Alice, εκτελείται μία ακόμη μέτρηση ίδιας βάσης με εκείνη του Bob στα αντίστοιχα φωτόνια της ακολουθίας M . Έτσι, εάν το ποσοστό σφάλματος είναι κάτω από ένα προκαθορισμένο όριο, τότε το κβαντικό κανάλι παραμένει ασφαλές. Ακόμη, κατά τη διάρκεια μετάδοσης της ακολουθίας M , χρησιμοποιούνται μερικά τυχαία επιλεγμένα φωτόνια έτσι ώστε να γίνει έλεγχος στον ρυθμό σφαλμάτων μετάδοσης, ενώ στα ίδια φωτόνια εφαρμόζεται μια λειτουργία που επιλέγεται επίσης τυχαία. Επομένως, εφόσον ο Bob λάβει τα ζεύγη δειγματοληψίας και τα συνδυάσει με εκείνα της Alice, μπορεί να ανακτήσει αυτές τις πράξεις χρησιμοποιώντας μέτρηση Bell.



Εικόνα 7. Σχήμα QSDC με χρήση οπτικών καθυστερήσεων (<https://arxiv.org/pdf/quant-ph/0308173>).

Συμπερασματικά το παραπάνω σχήμα μοιάζει περισσότερο με ένα πρωτόκολλο διανομής κβαντικού κλειδιού, καθώς μόλις ο Bob λάβει την ακολουθία επαλήθευσης, μαζί με την Alice δημιουργούν ένα κοινό κλειδί μιας χρήσης μετρώντας τα σωματίδια τους χρησιμοποιώντας μια τυχαία επιλεγμένη βάση, η οποία αποτελεί παραλλαγή του πρωτοκόλλου Ekert91 και του BB84. Η σημαντική διαφορά μεταξύ της κβαντικής άμεσης επικοινωνίας (QDC) και της κατανομής κβαντικού κλειδιού (QKD) είναι ότι το σχήμα QDC δεν απαιτεί την καθιέρωση ενός κλασικού κλειδιού αλλά ενός εγγενούς κβαντικού μηχανικού πόρου όπως τα κοινά ζεύγη EPR. Επομένως, με την ανάπτυξη αποτελεσματικής πηγής EPR και συσκευής μέτρησης καταστάσεων Bell, η κβαντική άμεση επικοινωνία καθίσταται ευκολότερη στην πραγματοποίηση και μπορεί να ευνοηθεί σε συγκεκριμένες εφαρμογές [9].

2.3 Κβαντική Ασφαλής Άμεση Επικοινωνία βασισμένη σε μεμονωμένα σωματίδια

Σε αυτή την ενότητα θα αναλυθεί ένα σύστημα κβαντικής ασφαλούς άμεσης επικοινωνίας το οποίο βασίζεται σε μεμονωμένα σωματίδια. Συγκεκριμένα, γίνεται ο ορισμός μιας νέας βάσης Y (Y -basis) που διαφέρει από τις βάσεις Z και X στο BB84. Έπειτα, γίνεται χρήση της λειτουργίας Pauli I συνδυαστικά με τη λειτουργία Z , για την κωδικοποίηση του μυστικού μηνύματος στα μεμονωμένα σωματίδια. Το κύριο πλεονέκτημα αυτής της λειτουργίας είναι ότι γίνεται περιστροφή μόνο της φάσης του σωματιδίου και δεν αλλάζει η πόλωση του, με αποτέλεσμα η εφαρμογή του να είναι πιο εύκολη.

Η κβαντική ασφαλής άμεση επικοινωνία (QSDC) αποτελεί σημείο αιχμής στον κλάδο της κβαντικής κρυπτογραφίας και αυτό φαίνεται από τις διάφορες έρευνες που γίνονται αδιάλειπτα κατά το πέρασμα των χρόνων. Ειδικότερα:

- (2002) Long και Liu: Πρώτο πρωτόκολλο QSDC με χρήση ζεύγους EPR για μετάδοση μηνύματος.
- (2004) Deng και Long: Πρώτο πρωτόκολλο QSDC σωματιδίου σύμφωνα με το οποίο το μήνυμα κωδικοποιείται μέσω ενιαίων πράξεων στα μεμονωμένα σωματίδια.
- (2016) Hu και άλλοι: Παραλλαγή του πρωτοκόλλου των Deng και Long, όπου οι πληροφορίες κωδικοποιούνται στο φάσμα συχνοτήτων ενός μπλοκ.
- (2018) Niu και άλλοι: Χρήση πυκνής λειτουργίας κωδικοποίησης των ζευγών EPR έτσι ώστε το QSDC να είναι ανεξάρτητο από τη συσκευή μέτρησης, που μπορεί να εξαλείψει τα κενά ασφαλείας που σχετίζονται με αυτή, ενισχύοντας σημαντικά την ασφάλεια.
- (2020) Zhou και άλλοι: Πρώτο ανεξάρτητο από τη συσκευή QSDC όπου γίνεται συνδυασμός της γραμμικής ενίσχυσης χωρίς θόρυβο.

Σε αυτό το πρωτόκολλο, ορίζεται μία νέα βάση Y , η οποία είναι αμερόληπτη ως προς τη βάση Z και X που είχαμε δει στο BB84. Στη συνέχεια, σύμφωνα με την πράξη Pauli Z έχουμε:

$$\sigma = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (2.5)$$

Παράλληλα, είναι σαφές ότι η λειτουργία Z χρειάζεται μόνο να περιστρέφει τη φάση του σωματιδίου, ενώ η λειτουργία Y να περιστρέφει τόσο την πόλωση όσο και τη φάση του. Επομένως, η υλοποίηση της Z είναι ευκολότερη από εκείνη της Y . Συγκριτικά λοιπόν με το σχήμα του Deng, ο αποστολέας του μηνύματος στο παρόν πρωτόκολλο, δηλαδή η Alice, θα χρειαστεί λιγότερο εξοπλισμό και πόρους, γεγονός που το καθιστά ακόμη πιο πρακτικό. Παρακάτω φαίνονται οι τέσσερις ενιαίες πράξεις Pauli:

- I πράξη: $\sigma = |0\rangle\langle 0| + |1\rangle\langle 1|$ (2.6)
- X πράξη: $\sigma = |0\rangle\langle 1| + |1\rangle\langle 0|$ (2.7)
- Z πράξη: $\sigma = |0\rangle\langle 0| - |1\rangle\langle 1|$ (2.8)
- Y πράξη: $i\sigma = |0\rangle\langle 1| - |1\rangle\langle 0|$ (2.9)

Εάν υποθέσουμε ότι η Alice επιθυμεί να στείλει ένα μήνυμα στον Bob μέσω της κβαντικής ασφαλούς άμεσης επικοινωνίας, τότε η μεθοδολογία έχει ως εξής. Σε πρώτη φάση ο Bob παράγει με τυχαίο τρόπο μερικά σωματίδια από τις βάσεις X και Y και τα

αποστέλλει στην Alice. Έπειτα, εκείνη επιλέγει τυχαία κάποια από τα σωματίδια που έλαβε ως “σωματίδια ελέγχου” και μετρά το καθένα από αυτά σύμφωνα με τις βάσεις X ή Y. Στη συνέχεια, η Alice μεταφέρει στον Bob τα αποτελέσματα των μετρήσεων και εκείνος μπορεί να καταλάβει αν έχει υπάρξει υποκλοπή ανάλογα με το ποσοστό σφάλματος. Έτσι, αν υπάρχει υποψία κλοπής ο Bob, λέει στην Alice να διακόψει τη διαδικασία και να ξεκινήσει από την αρχή, εναλλακτικά το πρωτόκολλο συνεχίζεται κανονικά.

Σε δεύτερη φάση, η Alice εκτελεί μία από τις δύο πράξεις $\sigma = |0\rangle\langle 0| + |1\rangle\langle 1|$ (2.6), $\sigma = |0\rangle\langle 0| - |1\rangle\langle 1|$ (2.8) στα σωματίδια ανάλογα με το μήνυμα, δηλαδή εάν το bit του μηνύματος είναι 0, εκτελεί το (2.6), αλλιώς εάν είναι 1 εκτελεί το (2.8), και στέλνει ξανά τα υπόλοιπα σωματίδια πίσω. Εφόσον ο Bob τα λάβει, κάνει τις απαραίτητες μετρήσεις με τις αρχικές βάσεις για να εμφανιστεί το μήνυμα. Ειδικότερα, εάν το αποτέλεσμα της μέτρησης είναι ίδιο με την αρχική κατάσταση, τότε το bit είναι 0, διαφορετικά το bit του μηνύματος είναι 1. Τέλος, ζητείται από την Alice να δημοσιεύσει μερικά κομμάτια του μηνύματος για να ελεγχθεί η ασφάλεια και τα υπόλοιπα θα παραμείνουν ως το μυστικό μήνυμα.

2.3.1 Ασφάλεια Έναντι Επιθέσεων

Οι πιθανότητες να γίνει κάποια επίθεση υποκλοπής σε αυτό το σχήμα είναι ελάχιστες, αλλά όχι μηδαμινές και για αυτόν τον λόγο θα έπρεπε να ληφθούν τα κατάλληλα μέτρα. Για παράδειγμα, η Eve(eavesdropper) μπορεί να ανακτήσει τα σωματίδια που έστειλε ο Bob και να στείλει ξανά τα πλαστά σωματίδια στην Alice. Αφού η Alice εκτέλεσε τις απαραίτητες λειτουργίες και έστειλε πίσω τα σωματίδια, η Eve τα ανακτά για ακόμη μια φορά και στη θέση τους στέλνει τα πλαστά στον Bob. Σε αυτήν την περίπτωση η eavesdropper γνωρίζει τις βάσεις των πλαστών σωματιδίων και έτσι μπορεί να αποκτήσει πρόσβαση στο αρχικό μήνυμα.

Σε αυτό το πρωτόκολλο αναλύσαμε παραπάνω ότι εφόσον η Alice λάβει τα σωματίδια θα επιλέξει μερικά από αυτά ως “σωματίδια ελέγχου”, θα τα μετρήσει και θα στείλει στον Bob τα αποτελέσματα και εκείνος θα υπολογίσει το ποσοστό σφαλμάτων για να κρίνει εάν υπάρχει υποκλοπή. Έτσι, εάν η Eve πραγματοποιήσει επίθεση, δεν θα γνωρίζει τη βάση σωματιδίου που στέλνει ο Bob και θα είναι αδύνατο να δημιουργήσει πλαστά σωματίδια. Με αυτόν τον τρόπο, το ποσοστό σφάλματος θα υπερβεί την κατώτατη τιμή και θα βρεθεί η επίθεση.

Τα τελευταία χρόνια, έχει αναπτυχθεί αρκετά ο κλάδος της κβαντικής κρυπτογραφίας και ειδικότερα η κβαντική ασφαλής άμεση επικοινωνία. Το παραπάνω πρωτόκολλο αφορά τη χρήση μεμονωμένου σωματιδίου και τη λειτουργία Pauli Z, δηλαδή ορίζουμε μια νέα βάση Y διαφορετική από τις Z και X και χρησιμοποιούμε τη λειτουργία Z για την κωδικοποίηση του μυστικού μηνύματος στα σωματίδια. Η Pauli Z

θεωρείται πιο εύχρηστη στην εφαρμογή καθώς περιστρέφει μόνο τη φάση του σωματιδίου χωρίς να αλλάζει η πόλωση του. Συχνά, η πόλωση μπορεί να αλλάξει με την άσκηση υψηλής τάσης ενώ η αλλαγή φάσης μπορεί να υλοποιηθεί από έναν διαμορφωτή χαμηλής τάσης, και έτσι το συγκεκριμένο σχήμα καθίσταται πιο πρακτικό από τα υπάρχοντα πρωτόκολλα [10].

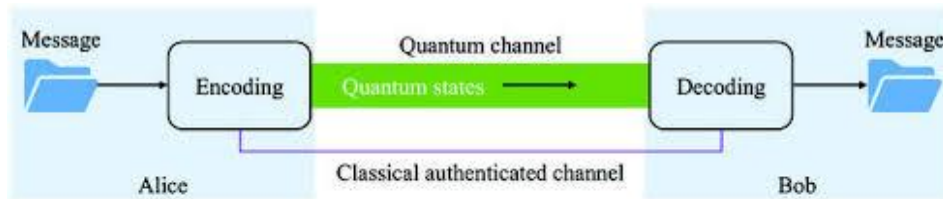
2.4 Κβαντική Ασφαλής Άμεση Επικοινωνία Ελεύθερου Χώρου

Οι έρευνες των τελευταίων ετών έχουν δείξει ότι ο κβαντισμός μπορεί να απειλήσει διάφορους αλγόριθμους υψηλής κρυπτογράφησης, καθώς στον τομέα της κρυπτογραφίας, ο μόνος αλγόριθμος που έχει αποδειχθεί απόλυτα ασφαλής είναι το One-Time-Pad. Επομένως, όσον αφορά ιδιωτικές πληροφορίες με μακροχρόνιες απαιτήσεις εμπιστευτικότητας, υπάρχει ο κίνδυνος του κακόβουλου χρήστη να αποθηκεύσει το κρυπτογραφημένο κείμενο και να περιμένει ένα χρονικό διάστημα για την αποκρυπτογράφηση του, όπου πιθανότατα να υπάρχουν νέες μέθοδοι και ταχύτερος εξοπλισμός όπως οι κβαντικοί υπολογιστές. Πλέον αποτελούν μια από τις μεγαλύτερες και πιο ρεαλιστικές απειλές για τις ασφαλείς επικοινωνίες που βασίζονται στην κλασική κρυπτογραφία, παρά το γεγονός ότι ακόμη και σήμερα δεν είναι πλήρως προσβάσιμες στον καθημερινό χρήστη.

2.4.1 Βασικές Αρχές

Το QSDC αποτελεί ένα σχέδιο για την επίτευξη ασφαλούς επικοινωνίας με τη χρήση κβαντικών καταστάσεων. Ο αποστολέας μηνυμάτων, δηλαδή η Alice κωδικοποιεί τα μηνύματα απλού κειμένου στις κβαντικές καταστάσεις, τα οποία έπειτα, μεταδίδονται στον δέκτη Bob μέσω ενός κβαντικού καναλιού. Με αυτόν τον τρόπο, ο Bob λαμβάνει τα μηνύματα μέσω αποκωδικοποίησης, δηλαδή μετρώντας τις λαμβανόμενες κβαντικές καταστάσεις. Έτσι, επιτυγχάνεται ασφαλής επικοινωνία χωρίς να απαιτείται εκ των προτέρων διανομή μυστικών κλειδιών. Ένα κλασικό κανάλι ελέγχου ταυτότητας είναι απαραίτητο για το QSDC για την ολοκλήρωση της ανίχνευσης υποκλοπής και τη διόρθωση σφαλμάτων. Η ασφάλεια του, βασίζεται στις αρχές της κβαντικής φυσικής, καθιστώντας αδύνατο για έναν κακόβουλο χρήστη να υποκλέψει οποιαδήποτε χρήσιμη πληροφορία που σχετίζεται με το μήνυμα. Μέσω του QSDC μπορούν να μεταδοθούν πολλές μορφές πληροφοριών όπως κείμενο, φωνή, βίντεο, ενώ παράλληλα, εάν χρησιμοποιείται για τη μετάδοση μυστικού κλειδιού, μπορεί να πραγματοποιηθεί τόσο η

διανομή όσο και η διαπραγμάτευση του τυχαίου μυστικού κλειδιού. Παρακάτω φαίνεται η υλοποίηση του QSDC πρωτοκόλλου.



Εικόνα 8. Υλοποίηση QSDC (https://www.researchgate.net/figure/Illustration-of-the-QSDC-scheme_fig1_368741948).

2.4.2 Πρωτόκολλο DL04

Ένα εξίσου σημαντικό πρωτόκολλο είναι το DL04 που υλοποιήθηκε από τους Deng και Long το 2004 χρησιμοποιώντας μεμονωμένα φωτόνια για μετάδοση πληροφοριών και αποτελείται από τα εξής βήματα:

1. Προετοιμασία καταστάσεων και μετάδοση. Ο Bob ετοιμάζει μια ακολουθία από qubits που περιέχει N μεμονωμένα φωτόνια και την στέλνει στην Alice.
2. Ανίχνευση υποκλοπής. Η Alice επιλέγει τυχαία μερικά φωτόνια που έλαβε από τον Bob για ανίχνευση υποκλοπής και κάθε φωτόνιο στο υποσύνολο μετράται είτε σε βάση Z είτε σε X . Ο Bob λαμβάνει τα αποτελέσματα των μετρήσεων και αν ο ρυθμός σφάλματος bit είναι μικρότερος από το κατώφλι, συνεχίζεται η διαδικασία, εναλλακτικά η μετάδοση απορρίπτεται.
3. Κωδικοποίηση πληροφοριών. Η Alice κωδικοποιεί το μυστικό μήνυμα στα υπόλοιπα μεμονωμένα φωτόνια και τα επιστρέφει στον Bob. Για την εκτίμηση της αξιοπιστίας της δεύτερης μετάδοσης η Alice επιλέγει τυχαία μερικά φωτόνια για την κωδικοποίηση σε 0 και 1.
4. Μέτρηση. Μετά την παραλαβή των φωτονίων, ο Bob διαβάζει τα κλασικά κομμάτια πληροφοριών που είναι κωδικοποιημένα από την Alice σύμφωνα με τις βάσεις προετοιμασίας του. Τέλος, ανακοινώνονται οι θέσεις των φωτονίων και η Alice με τον Bob κάνουν τις απαραίτητες μετρήσεις και εφόσον ο ρυθμός σφάλματος bit είναι μικρότερος από το κατώφλι, τότε η μετάδοση είναι επιτυχής.

2.4.3 Πρωτόκολλο RECON

Ένα πρωτόκολλο QSDC ενός φωτονίου βασιζόμενο στο One-Time-Pad, προτάθηκε το 2004 και ονομάζεται RECON και έχει τα ακόλουθα βήματα:

1. Κοινή χρήση μυστικού κλειδιού. Η Alice και ο Bob δημιουργούν δύο αμοιβαία κοινά μυστικά κλειδιά εκ των προτέρων.
2. Προετοιμασία αλληλουχίας μηνύματος και δοκιμής. Η Alice προετοιμάζει μια ακολουθία δυαδικών τυχαίων αριθμών μήκους $n\ell$ και τους εισάγει τυχαία σε μια άλλη ακολουθία μυστικών μηνυμάτων που πρόκειται να μεταδοθεί.
3. Προετοιμασία καταστάσεων. Η Alice επικαλείται την ακολουθία μυστικού κλειδιού μεγέθους $2(n\ell + n\ell)$ για να παρασκευάσει μεμονωμένα φωτόνια.
4. Κωδικοποίηση πληροφοριών. Η Alice κωδικοποιεί τη δυαδική ακολουθία δοκιμής μηνυμάτων σε μεμονωμένα φωτόνια, ενώ η αλληλουχία του ενός μεταδίδεται στον Bob ένα προς ένα.
5. Μέτρηση και αποκρυπτογράφηση. Ο Bob μετρά καθένα από τα λαμβανόμενα φωτόνια σε κατάλληλη βάση σύμφωνα με το εκ των προτέρων κοινόχρηστο μυστικό κλειδί τους, ακολουθώντας τους κανόνες του βήματος 3.
6. Ανίχνευση υποκλοπής. Η Alice δηλώνει δημόσια τις θέσεις και τις τιμές των δοκιμαστικών μεμονωμένων φωτονίων και ο Bob τις συγκρίνει με τα αποτελέσματα των δικών του μετρήσεων που σχετίζονται με τα φωτόνια που καθορίζονται τον ρυθμό σφάλματος bit. Μόλις η Alice ανακοινώσει δημόσια ότι οι θέσεις των μεμονωμένων φωτονίων κωδικοποιούν τυχαίους αριθμούς, τα μεταδιδόμενα μυστικά μηνύματα είναι διαθέσιμα για τον Bob.
7. Ενημέρωση του μυστικού κλειδιού. Η Alice και ο Bob απορρίπτουν τα δυαδικά ψηφία του μυστικού κλειδιού που έχουν αντιστοιχιστεί στα φωτόνια που χρησιμοποιήθηκαν για την κωδικοποίηση τυχαίων αριθμών. Τα υπόλοιπα μυστικά κλειδιά θα αφιερωθούν για τον επόμενο γύρο μετάδοσης.

2.4.4 Κβαντικό Πρωτόκολλο Χαμηλής Πιθανότητας Αναχαίτισης

Το κβαντικό πρωτόκολλο χαμηλής πιθανότητας αναχαίτισης (QLPI) υλοποιήθηκε από τον Shapiro και άλλους το 2019. Κύριο χαρακτηριστικό του είναι η μετάδοση απευθείας του κρυπτογραφημένου κειμένου πάνω από ένα κβαντικό κανάλι για την αποτροπή του κακόβουλου χρήστη από τη λήψη πολύτιμων πληροφοριών. Παρακάτω φαίνεται η μεθοδολογία:

1. Κατάσταση προετοιμασίας και μετάδοσης. Ένα φως χαμηλής φωτεινότητας, ευρυζωνικής και ενισχυμένης αυτόματης εκπομπής (Amplified Spontaneous Emission) μεταδίδεται από τον δέκτη πληροφοριών στον πομπό, και το υπόλοιπο φως υψηλής φωτεινότητας αποθηκεύεται στη γραμμή καθυστέρησης του δέκτη πληροφοριών.
2. Κωδικοποίηση πληροφοριών. Ο πομπός πληροφοριών κρυπτογραφεί το απλό κείμενο για να λάβει κρυπτογραφημένο κείμενο, το οποίο μετατρέπεται σε κωδική λέξη από έναν κωδικοποιητή διόρθωσης σφαλμάτων προώθησης (Forward Error Correction). Η κωδική λέξη θα αντιστοιχιστεί στο φως με δυαδική διαμόρφωση πλήκτρων μετατόπισης φάσης.
3. Μετάδοση κατάστασης. Το διαμορφωμένο φως περνά μέσω ενός οπτικού ενισχυτή υψηλής απολαβής και στη συνέχεια επιστρέφει στον δέκτη πληροφοριών.
4. Αποκωδικοποίηση και αποκρυπτογράφηση πληροφοριών. Ο δέκτης συνδυάζει το επιστρεφόμενο φως και το αποθηκευμένο φως (ASE) υψηλής φωτεινότητας, το οποίο είναι στην πραγματικότητα ένας τοπικός ταλαντωτής για ευρυζωνική ανίχνευση. Τα αποτελέσματα της μέτρησης επαναφέρονται σε απλό κείμενο μετά την αποκωδικοποίηση και την αποκρυπτογράφηση (FEC).

2.4.5 Κβαντικό πρωτόκολλο ιδιωτικής επικοινωνίας χωρίς κλειδί

Το συγκεκριμένο κβαντικό πρωτόκολλο επικοινωνίας χωρίς κλειδί QKPC αναπτύχθηκε με σκοπό να επιτευχθεί άμεση ιδιωτική επικοινωνία μέσω του κβαντικού καναλιού χωρίς να είναι απαραίτητη η χρήση κλειδιού. Παρακάτω φαίνονται τα βήματα:

1. Κωδικοποίηση. Το μήνυμα κωδικοποιείται από την Alice σε μια κωδική λέξη μέσω ενός κωδικοποιητή στοχαστικής υποκλοπής.
2. Προετοιμασία και μετάδοση. Προετοιμασία μιας κατάστασης κενού $|0\rangle$ ή μιας συνεκτικής κατάστασης $|a\rangle$ με βάση την κωδική λέξη από την Alice και στη συνέχεια μετάδοση στον Bob. Ειδικότερα, κατάσταση κενού μεταδίδεται από την Alice όταν η κωδική λέξη είναι 0 και συνεκτική κατάσταση εκπέμπεται όταν η κωδική λέξη είναι 1.
3. Μέτρηση. Ο Bob λαμβάνει την κωδική λέξη, μετρώντας το σήμα άφιξης.
4. Αποκωδικοποίηση. Ο Bob εισάγει τη ληφθείσα κωδική λέξη σε έναν αποκωδικοποιητή για τη λήψη των μεταδιδόμενων πληροφοριών.

2.4.6 QSDC σε Πραγματικό Κβαντικό Κανάλι

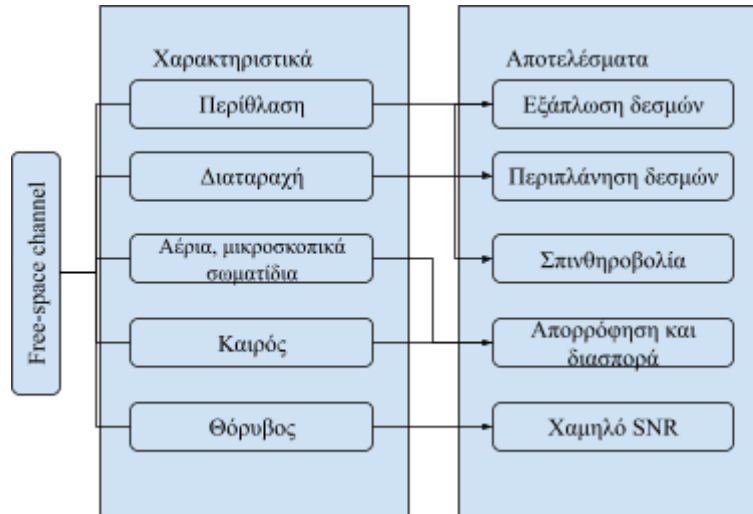
Η πλειοψηφία των πρωτοκόλλων όπως είδαμε και προηγουμένως, περιγράφεται με βάση ένα κανάλι στο οποίο επικρατούν οι ιδανικές συνθήκες, χωρίς να λαμβάνεται υπόψη ο θόρυβος και οι απώλειες που πιθανότατα προκύπτουν. Ωστόσο, με την εισαγωγή του QSDC σε ένα ρεαλιστικό κανάλι, θα είναι εφικτή η εμφάνιση των χαρακτηριστικών του καναλιού και των αποτελεσμάτων που προκύπτουν. Ειδικότερα, οι μυστικές πληροφορίες στο QSDC, οι οποίες θα μπορούσαν να έχουν πολλαπλές μορφές όπως κείμενο, φωνή, εικόνα, βίντεο, μυστικό κλειδί, κωδικοποιούνται στις κβαντικές καταστάσεις και μεταδίδονται απευθείας μέσω του κβαντικού καναλιού από την Alice στον Bob. Η αθόρυβη μετάδοση στο αρχικό πρωτόκολλο θεωρείται δεδομένη, παρόλα αυτά οι χρήστες δεν μπορούν να ερωμιστούν το κόστος της απώλειας σημαντικών μηνυμάτων που μεταδίδονται μέσω του πραγματικού κβαντικού καναλιού. Καθώς το πραγματικό κβαντικό κανάλι έρχεται αντιμέτωπο με διάφορους τρόπους υποκλοπών, θορύβου και απώλειας, η κωδικοποίηση είναι απαραίτητος παράγοντας για την καταπολέμηση αυτών των επιζήμιων παραγόντων. Αυτό το επίπεδο κωδικοποίησης περιλαμβάνει τρεις μονάδες:

1. Κωδικοποιητής FEC (Forward Error Correction) για προσθήκη επιπλέον bits στο μήνυμα.
2. Κωδικοποιητής κατά των απωλειών.
3. Κωδικοποιητής Secure-Coding.

Στη συνέχεια, η Alice λαμβάνει την κωδικοποιημένη λέξη που μεταδίδεται αφού περάσει το απλό κείμενο μέσω του επιπέδου κωδικοποίησης και ένας πομπός ενός συγκεκριμένου πρωτοκόλλου QSDC στέλνει την κωδική λέξη στον δέκτη.

2.5 Ελεύθερος Χώρος QSDC και Χαρακτηριστικά

Στο παρακάτω σχήμα απεικονίζονται τα χαρακτηριστικά του καναλιού ελεύθερου χώρου καθώς και οι επιπτώσεις τους στη μετάδοση οπτικού σήματος. Ειδικότερα, η εξάπλωση της δέσμης προκύπτει από την περίθλαση, όταν δηλαδή μία δέσμη φωτός διαδίδεται στην ατμόσφαιρα. Ακόμη, οι αναταράξεις στο ατμοσφαιρικό κανάλι θα προκαλούσαν εξάπλωση, περιπλάνηση καθώς και σπινθηρισμό της δέσμης, ενώ παράλληλα, τα αέρια, τα μικροσκοπικά σωματίδια και οι διάφορες καιρικές συνθήκες αποτελούν πηγή απορρόφησης και διασποράς του φωτός, που θα εξασθενίσουν τα οπτικά σήματα. Τέλος, το φως του ήλιου είναι ο θόρυβος περιβάλλοντος για την κβαντική επικοινωνία, μειώνει την αναλογία σήματος προς θόρυβο (SNR).



Εικόνα 9. Χαρακτηριστικά καναλιού ελεύθερου χώρου.

2.5.1 Ζητήματα που προκύπτουν στο QSDC Ελεύθερου Χώρου

Ως γνωστόν, το ατμοσφαιρικό κανάλι αποτελείται από διάφορα αέρια και άλλα αιωρούμενα σωματίδια ή αλλαγές όπως η βροχόπτωση, η ομίχλη και το χιόνι. Τόσο η απορρόφηση φωτός από μόρια αερίου όσο και η διασκόρπιση Rayleigh μπορούν να εξασθενίσουν το οπτικό σήμα που μεταδίδεται μέσω του ατμοσφαιρικού καναλιού. Η επιλογή λοιπόν, των σωστών μηκών κύματος επικοινωνίας μπορεί να μειώσει τον αντίκτυπο της ατμοσφαιρικής απορρόφησης και της διασποράς στην οπτική επικοινωνία. Συγκεκριμένα, το οπτικό σήμα με μήκος κύματος 1.550 nm έχει υψηλότερη μετάδοση στο ατμοσφαιρικό κανάλι, ενώ ορισμένα αποτελέσματα δείχνουν ότι η μετάδοση φωτονίων 1.550 nm πάνω από το ατμοσφαιρικό κανάλι με ομιχλώδη και βροχερό καιρό έχει λιγότερες απώλειες από τη μετάδοση φωτονίων 785 nm.

Από την άλλη πλευρά, η ατμοσφαιρική διασκόρπιση όχι μόνο προκαλεί εξασθένηση των οπτικών σημάτων, αλλά είναι επίσης μια κύρια αιτία της ακτινοβολίας του ουρανού, η οποία είναι η σκέδαση των ηλιακών φωτονίων καθώς ταξιδεύουν στην ατμόσφαιρα, ενώ το φως του ήλιου είναι το υπόβαθρο για το σύστημα QSDC ελεύθερου χώρου. Επομένως, θα γίνει η πηγή θορύβου του συστήματος επικοινωνίας όταν το ηλιακό φως συλλέγεται μαζί με το σήμα στον δέκτη για ανίχνευση, γεγονός που θα μειώσει το SNR του QSDC.

Οι πομποδέκτες του ελεύθερου χώρου QSDC είναι κατασκευασμένοι από συσκευές οπτικών ινών, οι οποίες είναι εύκολο να ενσωματωθούν, να συσκευαστούν και

να διατηρήσουν τη σταθερότητα. Ορισμένες συσκευές οπτικών ινών έχουν ρυθμιστεί στα 1.550 nm, γεγονός που αποτελεί σημαντικό παράγοντα για την πρακτική εφαρμογή και την εμπορευματοποίηση της κβαντικής επικοινωνίας. Έτσι, τα 1.550 nm ως μήκος κύματος επικοινωνίας έχουν ένα πλεονέκτημα αναφορικά με τη συμβατότητα με συσκευές οπτικών ινών. Παρόλα αυτά, τα μεμονωμένα φωτόνια με μήκος κύματος 800 nm ανιχνεύονται από φωτοδιόδους χιονοστιβάδας Si, οι οποίες έχουν υψηλότερη απόδοση ανίχνευσης σε σχέση με την ανίχνευση ενός φωτονίου στα 1.550 nm χρησιμοποιώντας μια φωτοδίοδο InGaAs/InP. Με αυτόν τον τρόπο η αποτελεσματικότητα ανίχνευσης των 800 nm φτάνει συνήθως το 50%, ενώ είναι μόνο περίπου 15% στα 1.550 nm. Συμπερασματικά, οι γωνίες απόκλισης που προκύπτουν από το τηλεσκόπιο εκπομπής και τις αναταράξεις είναι ανάλογες με το μήκος κύματος λ στην κβαντική επικοινωνία ελεύθερου χώρου, οπότε το άκρο λήψης χρειάζεται ένα τηλεσκόπιο συλλογής μεγαλύτερης διαμέτρου για να μειώσει τις απώλειες για την κβαντική επικοινωνία μέσω 1.550 nm.

2.5.2 Στρατηγική Κωδικοποίησης Φωτονίων

Σύμφωνα, με τα προηγούμενα κεφάλαια γνωρίζουμε ότι το κανάλι της ατμόσφαιρας δεν έχει αποτέλεσμα διπλής διάθλασης για οπτικά μήκη κύματος και έτσι η πόλωση του φωτονίου μπορεί να διατηρηθεί καλά στην κβαντική επικοινωνία ελεύθερου χώρου. Ωστόσο, αξίζει επίσης να σημειωθεί η σκοπιμότητα της κβαντικής επικοινωνίας ελεύθερου χώρου με βάση την κωδικοποίηση φάσης. Ταυτόχρονα, η στρατηγική κωδικοποίησης πόλωσης δεν είναι συνήθως η πρώτη επιλογή για κβαντική επικοινωνία πάνω από οπτικές ίνες, καθώς τόσο το φαινόμενο διπλής διάθλασης όσο και το φαινόμενο διασποράς της ίνας επηρεάζουν την μετάδοση των κβαντικών καταστάσεων πόλωσης. Επομένως η κωδικοποίηση φάσης είναι ένα σχήμα που υιοθετείται ευρέως από την κβαντική επικοινωνία που βασίζεται σε οπτικές ίνες και η πρόοδος της κβαντικής επικοινωνίας ελεύθερου χώρου που βασίζεται σε αυτή, δημιουργεί νέες ευκαιρίες για την κατασκευή ενός απλοποιημένου ολοκληρωμένου δικτύου χώρου-αέρα-εδάφους.

Σε ένα τέτοιο δίκτυο, προφανώς, δεν είναι αναγκαία η τοποθέτηση συστημάτων επικοινωνίας κωδικοποίησης πόλωσης και φάσης. Ειδικότερα, η κβαντική κατάσταση που μεταδίδεται μέσω ενός καναλιού ελεύθερου χώρου μπορεί να συνεχίσει να μεταδίδεται κατά μήκος της ίνας μετά τη σύζευξή της σε αυτήν. Με αυτόν τον τρόπο επιτρέπεται η άμεση πρόσβαση στο δίκτυο για εγκαταστάσεις κινητής επικοινωνίας και απλοποιείται η αλληλεπίδραση ελεύθερου χώρου και οπτικής ίνας. Αντιθέτως, εάν γινόταν χρήση ενός μίγματος κωδικοποίησης φάσης στο δίκτυο, το σήμα που μεταδίδεται μέσω ενός καναλιού ελεύθερου χώρου θα έπρεπε να αποκωδικοποιηθεί και να αναμεταδοθεί στο κανάλι οπτικής ίνας λόγω της αλλαγής του φορέα και εξοπλισμού επικοινωνίας. Σε αυτή την περίπτωση θα ήταν αναγκαίο να κατασκευαστούν δύο σετ

εξοπλισμού επικοινωνίας στον ίδιο κόμβο, και έτσι η κωδικοποίηση φάσης ελεύθερου χώρου QSDC έχει τα πλεονεκτήματα της ευελιξίας του δικτύου και της ευκολίας ανάπτυξης, μόλις αναπτυχθεί πλήρως.

Παράλληλα, τα κλασικά bit κωδικοποιούνται στη σχετική διαφορά φάσης των δύο παλμών στην κωδικοποίηση φάσης και παρεμβαίνουν στην πλευρά λήψης. Έτσι, η αποτελεσματική παρεμβολή εξαρτάται από τη διαφορά φάσης των δύο παλμών ανεξάρτητα από τις δραστικές αλλαγές των μετώπων κύματος κατά μήκος του καναλιού. Ακόμη, το ασύμμετρο συμβολόμετρο Mach-Zehnder είναι μια συχνά χρησιμοποιούμενη υποδομή για την υλοποίηση της στρατηγικής κωδικοποίησης φάσης, η οποία εξαρτάται από τη σχετική διαφορά φάσης μεταξύ των πρώιμων και των όψιμων παλμών, οι οποίοι θα μεταδοθούν από την Alice στον Bob μέσω ενός ατμοσφαιρικού καναλιού.

Αξίζει να σημειωθεί ότι οι χρονικές κλίμακες για την αλλαγή φάσης που προκαλείται από αναταράξεις είναι της τάξης των 10 έως 100 ms, ενώ το πλάτος του κάδου μεταξύ των πρώιμων και των όψιμων παλμών είναι τυπικά της τάξης των νανο-δευτερολέπτων. Επομένως, η φάση κάθε παλμού θα έχει την ίδια μετατόπιση φάσης αφού περάσει από ένα κανάλι τυρβώδους ατμόσφαιρας, θα ακυρώσουν το ένα το άλλο στη σχετική διαφορά φάσης και, ως εκ τούτου, δεν επηρεάζουν την κωδικοποίηση bit. Τα bit θα μπορούσαν επίσης να κωδικοποιηθούν απευθείας στους πρώιμους και όψιμους παλμούς και να αποκωδικοποιηθούν μετρώντας την ώρα άφιξής τους. Αυτή η στρατηγική κωδικοποίησης φωτονίων γνωστή και ως κωδικοποίηση time-bin είναι πιο ανθεκτική έναντι των σφαλμάτων που προκαλούνται από την ταραχώδη ατμόσφαιρα. Τέλος, ορισμένες εργασίες έδειξαν ότι τα qubits χρονικού κάδου ή κωδικοποίησης φάσης είναι κατάλληλα για μετάδοση σε ελεύθερο χώρο.

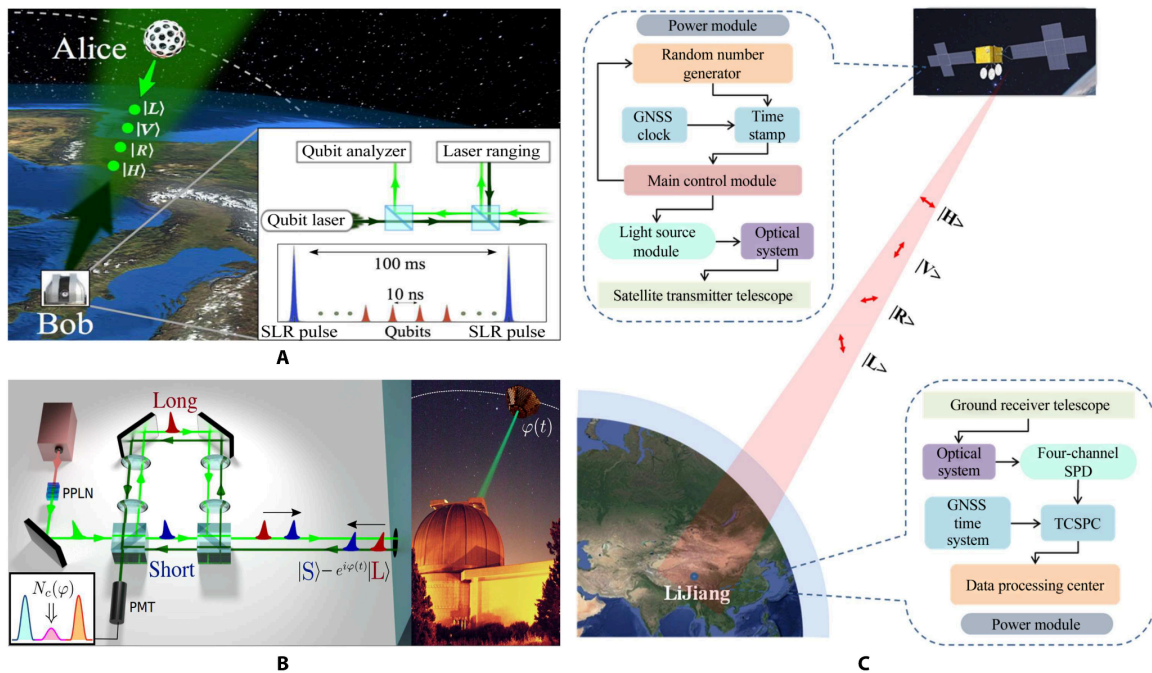
Συμπερασματικά, υπάρχει η ευελιξία επιλογής όλων των κωδικοποιήσεων φάσης ή κωδικοποίησης φάσης και χρόνου σε διαμορφώσεις κβαντικού δικτύου σύμφωνα με τις συγκεκριμένες απαιτήσεις υπηρεσιών δικτύου, ενώ συνδυάζοντας οπτικούς διακόπτες, το ασφαλές δίκτυο επαναλήπτη είναι σε θέση να πραγματοποιήσει την ανταλλαγή πληροφοριών ευρείας περιοχής του πολλαπλού χρήστη χρησιμοποιώντας την υπάρχουσα τεχνολογία.

2.5.3 Σκοπιμότητα δορυφορικού QSDC

Είναι γεγονός ότι το δορυφορικό QSDC βρίσκεται σε πρώιμο στάδιο ακόμη, καθώς δεν έχει εφαρμοστεί πλήρως μέχρι στιγμής. Παρακάτω, αναλύονται μερικά από τα τυπικά πειράματα μετάδοσης κβαντικών καταστάσεων κωδικοποιημένων με πόλωση και με timebin μεταξύ δορυφόρου και εδάφους. Συγκεκριμένα, το 2015 μια ιταλική ομάδα, υλοποίησε τη μετάδοση φωτονίων που κωδικοποιούν πόλωση από σύνθεση δορυφόρου σε έδαφος με ένα QBER και στη συνέχεια, αποδείχθηκε η μετάδοση qubits κωδικοποιημένη με time-bin μέσω μιας σύνδεσης εδάφους-δορυφόρου-εδάφους ενώ

παρατηρήθηκαν παρεμβολές φωτονίων σε έναν επίγειο σταθμό με ορατότητα έως και 67%. Αξίζει να σημειωθεί ότι, οι αποστάσεις της αμφίδρομης μετάδοσης κυμαίνονταν από 2.200 έως 5.000 χιλιόμετρα σε αυτήν την πειραματική επίδειξη.

Ταυτόχρονα, μια κινεζική ομάδα έκανε έρευνες σχετικά με τη μετάδοση φωτονίων που κωδικοποιούνται με πόλωση από γεωσύγχρονο δορυφόρο σε επίγειο σταθμό το 2021. Σε απόσταση μεγαλύτερη από 36.000 χιλιόμετρα, η απώλεια σύνδεσης είναι μεταξύ 100 και 110 dB, ενώ η μετάδοση QBER κυμαίνεται μεταξύ 2% και 8%. Εν κατακλείδι, τα συγκεκριμένα αποτελέσματα ικανοποιούν τα κριτήρια ασφαλείας των QKD και QSDC ενώ σε γενικές γραμμές όλα τα πειράματα που υλοποιήθηκαν συνεπάγονται τη σκοπιμότητα του QSDC που βασίζεται σε δορυφόρους.



Εικόνα 10. Επισκόπηση πειραματικών επιδείξεων μετάδοσης qubits μεταξύ δορυφόρου και εδάφους (<https://spj.science.org/doi/10.34133/adi.0004>).

2.5.4 CAID QSDC

Σε αυτή την ενότητα προτείνεται ένα σχήμα που έχει ως στόχο τη διευκόλυνση της ταχύτερης ανάπτυξης εφαρμογών του QSDC. Όπως είδαμε και σε προηγούμενα πρωτόκολλα, η κβαντική κρυπτογραφία και οι κβαντικές επικοινωνίες μπορούν θεωρητικά να επιτύχουν άνευ όρων ασφαλείς επικοινωνίες. Ωστόσο, η άνευ όρων ασφάλεια είναι δύσκολο να επιτευχθεί λόγω των ατελειών των πρακτικών συσκευών. Συνεπώς, είναι αρκετά χρονοβόρο να χαρακτηριστούν όλα τα κενά ασφαλείας που

προκύπτουν έτσι ώστε να αφαιρεθούν. Ορισμένα πρωτόκολλα που προσπαθούν να εξισορροπήσουν την ασφάλεια και την πρακτικότητα, όπως το MDI και το πρωτόκολλο διπλού πεδίου, έχουν προταθεί, χωρίς όμως αυτό να σημαίνει ότι δεν προκύπτουν και σε αυτά προβλήματα ασφάλειας.

Ταυτόχρονα, η ικανότητα της Eve που κρυφακούει, υποτίθεται ότι περιορίζεται μόνο από την κβαντική μηχανή, αλλά στην πραγματικότητα, οι ισχυρές επιθέσεις της Eve είναι δύσκολο να επιτευχθούν με την υπάρχουσα τεχνολογία. Για παράδειγμα, το πρωτόκολλο QSDC, που βασίζεται στο κλείδωμα κβαντικών δεδομένων καθιερώθηκε λαμβάνοντας υπόψη ότι δεν υπάρχει κβαντική μνήμη για την Eve έτσι ώστε να αποθηκεύσει κβαντικές πληροφορίες για αυθαίρετα μεγάλο χρονικό διάστημα. Τέτοιου είδους πρωτόκολλα έχουν τη ρεαλιστική τους ασφάλεια για ασφαλή επικοινωνία με ρεαλιστικούς περιορισμούς στην ικανότητα επίθεσης της Eve.

Σε αυτό το κομμάτι εισέρχεται το CAID QSDC, καθώς η αναπτυσσόμενη διαδρομή δεν είναι απαραίτητο να περιμένει το QSDC να είναι άνευ όρων ασφαλές προτού το προωθήσει σε πρακτικές εφαρμογές. Σε ένα σχήμα ασφαλούς επαναλήπτη λοιπόν, η κλασική μετα-κβαντική κρυπτογραφία βοηθά στην επίτευξη τελικής ασφάλειας του κβαντικού δικτύου και η μετάδοση πληροφοριών προστατεύεται διπλά από κβαντικές και κλασικές προσεγγίσεις. Όταν το QSDC χρησιμοποιείται για ασφαλή επικοινωνία, μπορεί να συνδυαστεί με ατελείς συσκευές με κλασική ή μετα-κβαντική κρυπτογραφία, όπου η χρήση QSDC μεταδίδει το κρυπτογραφημένο κείμενο. Όσον αφορά την κλασική κρυπτογραφία, το CAID QSDC στερεί την ικανότητα της Eve να έχει πρόσβαση στο κρυπτογραφημένο κείμενο, συνεπώς δεν υπάρχει η ανησυχία της άμεσης αποθήκευσης και αποκρυπτογράφησης αργότερα. Τέλος, στο QSDC με ατελείς συσκευές, η κλασική κρυπτογραφία παρέχει μια διασφάλιση της ασφάλειας των πληροφοριών εάν υπάρξει αποτυχία, συνεπώς το CAID QSDC θα παρέχει την υψηλότερη ασφάλεια με την υπάρχουσα τεχνολογία.

Αυτή η αναπτυσσόμενη διαδρομή είναι εξαιρετικά εύκολη στην εφαρμογή χάρη στη συμβατότητα του QSDC με τα υπάρχοντα κλασικά δίκτυα. Ειδικότερα, το κρυπτογραφικό στρώμα ενός εμπιστευτικού συστήματος επικοινωνίας μπορεί να συνεχίσει να ενισχύεται, όπως η αναβάθμιση σε μετα-κβαντική κρυπτογραφία. Ακόμη, με την αντικατάσταση των μονάδων επικοινωνίας στο κλασικό δίκτυο με μονάδες QSDC ή με την προσθήκη αναπτύξεων, μπορούν να επιτευχθούν εμπιστευτικές επικοινωνίες βελτιωμένες με κβαντικό τρόπο μη επαγωγικά για τους χρήστες επικοινωνίας. Ως εκ τούτου, το CAID QSDC μπορεί να εφαρμοστεί γρήγορα στην πραγματική ζωή αυτή τη στιγμή.

Συμπερασματικά, λαμβάνοντας υπόψη τις συναρπαστικές προοπτικές εφαρμογής των επικοινωνιών ελεύθερου χώρου, παραπάνω εξετάστηκε τόσο η θεωρητική όσο και η πειραματική πρόοδος του QSDC ελεύθερου χώρου. Παράλληλα, οι πειραματικές επιδείξεις μετάδοσης κωδικοποιημένων qubits μεταξύ δορυφόρων και εδάφους έχουν

προτείνει τη σκοπιμότητα ενός QSDC που βασίζεται σε δορυφόρους. Εν ολίγης, το QSDC έχει αποδειχθεί αρκετά χρήσιμο σε πρακτικές εφαρμογές και μπορεί να επιτύχει υψηλότερο επίπεδο ασφάλειας επικοινωνίας σε συνδυασμό με την κλασική ή την μετα-κβαντική κρυπτογραφία. Δεδομένης λοιπόν της κβαντικής φύσης της επικοινωνίας του QSDC, θα παρέχει έναν τρόπο κβαντικής διασύνδεσης στο μελλοντικό κβαντικό διαδίκτυο [11].

3. Εξέλιξη της Κβαντικής Ασφαλούς Άμεσης Επικοινωνίας

Η ασφάλεια των επικοινωνιών πρέπει να εξελιχθεί σε υψηλότερο επίπεδο ενόψει της απειλής από την τεράστια υπολογιστική ισχύ των αναδυόμενων κβαντικών υπολογιστών. Ειδικότερα, η κβαντική άμεση επικοινωνία (QSDC) αποτελεί ένα πολλά υποσχόμενο κλάδο της κβαντικής επικοινωνίας, ο οποίος είναι αποδεδειγμένα ασφαλής και ξεπερνά την απειλή του κβαντικού υπολογισμού, ενώ παράλληλα μεταφέρει μυστικά μηνύματα απευθείας μέσω του κβαντικού καναλιού. Ακόμη, είδαμε παραπάνω ότι η κρυπτογραφία χρησιμοποιείται για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών για τους εξουσιοδοτημένους χρήστες έναντι των κακόβουλων δραστηριοτήτων τρίτων. Τα λειτουργικά κρυπτογραφικά συστήματα τείνουν να βασίζονται στην εκτέλεση μαθηματικών πράξεων, που είναι δύσκολο να “αποκρυπτογραφηθούν” με τη βοήθεια υπερσύγχρονων υπολογιστών. Με άλλα λόγια, η πρακτική επιστήμη των υπολογιστών προσφέρει αυτό που ονομάζεται υπολογιστική ασφάλεια, η οποία είναι πρακτικά άθραυστη σε σχετικά σύντομο χρονικό διάστημα χρησιμοποιώντας πρακτικούς υπολογιστικούς πόρους.

Το QSDC αρχικά προτάθηκε από τους Long και Liu το 2000 και σε αυτές τις θεμελιώδεις συνεισφορές, επισημάνθηκε ότι ένα κλειδί παρήχθη από την Alice πριν πραγματοποιηθεί η μετάδοση και μέχρι σήμερα έχει εξελιχθεί σε ένα πλήρες πρωτόκολλο επικοινωνιών. Ταυτόχρονα, η ελλειψη πρακτικής κβαντικής μνήμης αποτελούσε ένα σοβαρό εμπόδιο για την εξέλιξη της κβαντικής επικοινωνίας, επειδή η χρήση αναμετάδοσης απαιτεί μνήμη. Ως εκ τούτου, το πρακτικό QKD έχει παραμείνει περιορισμένο σε μικρές αποστάσεις. Παρόλα αυτά, πολύ πρόσφατα, σχεδιάστηκε ένα πρωτόκολλο QSDC χωρίς κβαντική μνήμη, όπου το απλό κείμενο κρυπτογραφήθηκε χρησιμοποιώντας ένα τυχαίο κλειδί και στη συνέχεια το κρυπτογραφημένο κείμενο χρησιμοποιήθηκε για την απόσπαση μυστικών κλειδιών για την κρυπτογράφηση μεταγενέστερων μπλοκ μηνυμάτων. Επιπλέον, ο συνδυασμός QSDC και μετα-κβαντικής κρυπτογραφίας επιτρέπει την κατασκευή ενός ασφαλούς επαναλήπτη, ο οποίος μπορεί να δημιουργήσει ένα μεγάλης κλίμακας κβαντικό δίκτυο επικοινωνίας χρησιμοποιώντας την υπάρχουσα τεχνολογία. Εάν κοιτάξει κανείς πίσω στην ιστορία του QSDC, θα παρατηρήσει ότι αρκετά στάδια ανάπτυξης εμφανίζονται και υλοποιούνται ήδη.

Ξεκινώντας από το 2000, όταν δημιουργήθηκε για πρώτη φορά η παραπάνω φιλοσοφία, οι ερευνητές προσπάθησαν να κατασκευάσουν πρωτόκολλα επικοινωνίας από σημείο προς σημείο. Στη συνέχεια, τα πρώιμα πρωτόκολλα QSDC αναπτύχθηκαν περαιτέρω για την επίλυση ποικίλων κβαντικών κρυπτογραφικών εργασιών, συμπεριλαμβανομένων κβαντικών διαλόγων και υπογραφών που άνοιξαν το δρόμο για την εκτεταμένη εφαρμογή του QSDC. Η ασφάλειά του μπορεί να αποδειχθεί θεωρητικά, δηλαδή ότι τα πρωτόκολλα είναι ασφαλή σε θεωρητικό επίπεδο. Ωστόσο, οι πρόσφατες προσπάθειες μηχανικής ολοκλήρωσαν το πείραμα απόδειξης της αρχής αυτής και έκαναν ένα βήμα πιο κοντά προς την πρακτική λειτουργία του πεδίου.

3.1 Σχεδίαση Πρωτοκόλλων QSDC

Ως γνωστόν τα πρωτόκολλα QSDC έχουν μελετηθεί κυρίως στον τομέα της διακριτής μεταβλητής. Βέβαια, τα σχήματα συνεχούς μεταβλητής είναι δυνητικά πιο συμβατά με τον τρέχοντα εξοπλισμό τηλεπικοινωνιών και έχουν το πλεονέκτημα των οικονομικά αποδοτικών ανιχνευτών, καθώς και υψηλότερους ρυθμούς από τα πρωτόκολλα διακριτών μεταβλητών και για αυτόν τον λόγο υπάρχει μια πληθώρα από αρχικές μελέτες πάνω σε αυτό το κομμάτι. Ωστόσο, όλα ανήκουν στην οικογένεια των QSDC, καθώς η πρόσθετη επικοινωνία είναι απαραίτητη προϋπόθεση για την τελική αποκωδικοποίηση πληροφοριών, γεγονός που μειώνει την αποτελεσματικότητα της επικοινωνίας. Έτσι, ένα από τα ανοιχτά προβλήματα είναι αυτό του σχεδιασμού των συνεχών-μεταβλητών πρωτοκόλλων QSDC, των οποίων ο δέκτης μπορεί να ανιχνεύσει πληροφορίες χωρίς τη βοήθεια πρόσθετης επικοινωνίας.

Τα παραδοσιακά πρωτόκολλα QSDC απαιτούν μετάδοση κβαντικών καταστάσεων μετ' επιστροφής. Ακόμη, ο σχεδιασμός μονόδρομων πρωτοκόλλων QSDC θα ήταν επωφελής τόσο από την άποψη της μείωσης των απωλειών καναλιού όσο και της πολυπλοκότητας του συστήματος. Η απόδοση του ρυθμού σε σχέση με την απόσταση πρέπει να βελτιωθεί με την αξιοποίηση νέων φυσικών πόρων, για την υπέρβαση των θεωρητικών ορίων. Παράλληλα, κατά τη μετάδοση εμπιστευτικών πληροφοριών μέσω κβαντικών καναλιών με θόρυβο, απώλεια και υποκλοπή, απαιτούνται εξαιρετικοί κωδικοί διόρθωσης σφαλμάτων, όπως πολικοί κωδικοί και κωδικοί ελέγχου ισοτιμίας χαμηλής πυκνότητας. Συνεπώς μια ιδιαίτερα πολλά υποσχόμενη τεχνική αποτελεί ο σχεδιασμός κωδικών διόρθωσης σφαλμάτων για σχήματα QSDC.

3.2 Ασφάλεια Πρωτοκόλλου QSDC

Όπως είδαμε και στα προηγούμενα κεφάλαια, η απόδειξη ασφαλείας του αλγορίθμου BB84 QKD έχει πραγματοποιηθεί από μια σειρά διαφορετικών προοπτικών. Βέβαια, η απόδειξη ασφαλείας του QSDC απαιτεί ακόμη περαιτέρω έρευνα. Μια από τις προκλήσεις είναι ότι η αμφίδρομη μετάδοση είναι ευάλωτη σε επιθέσεις από κβαντικούς χάκερ. Απαιτείται επίσης, η ανάλυση ασφαλείας ατελών συσκευών. Πρέπει με λίγα λόγια, να καθοριστεί η ικανότητα μυστικότητας λαμβάνοντας υπόψη τα αποτελέσματα πεπερασμένου μήκους και τις πρακτικές παραμέτρους του συστήματος.

3.3 Πειραματικές Υλοποιήσεις QSDC

Η βελτιστοποίηση των παραμέτρων των συσκευών και η βελτίωση της απόδοσης των πρακτικών συστημάτων QSDC αντιπροσωπεύει συνεχείς προκλήσεις στην πειραματική πλευρά. Διαισθητικά, η απόσταση επικοινωνίας ενός μοναδικού φωτονίου QSDC μπορεί να προσεγγίσει το μισό της απόστασης του QKD με τον ίδιο ρυθμό πληροφοριών, λαμβάνοντας υπόψη ότι το QSDC απαιτεί αμφίδρομη μετάδοση με βάση το μπλοκ. Ο συνδυασμός κβαντικής μνήμης με QSDC συμβάλλει στην περαιτέρω βελτίωση της απόστασης επικοινωνίας και στην υποστήριξη του QSDC με μετάδοση βάσει μπλοκ. Επιπλέον, η διερεύνηση του οπτικού QSDC ελεύθερου χώρου θα συμβάλει στη μελλοντική εφαρμογή δικτύων QSDC που βασίζονται σε δορυφόρους. Εν ολίγοις, το QSDC που βασίζεται σε τσιπ θα οδηγήσει σε ένα πιο σταθερό, συμπαγές και φορητό πρακτικό σύστημα.

3.4 Υβριδικό QSDC Δίκτυο

Συμπερασματικά, οι περισσότερες από τις κρυπτογραφικές εργασίες που εξετάζονται, λειτουργούν στον κβαντικό τομέα. Ωστόσο, είναι επίσης εφικτό να ενσωματωθεί το QSDC σε κλασικό δίκτυο επικοινωνίας υψηλής ασφάλειας. Ειδικότερα, το ασφαλές δίκτυο επαναλήπτη είναι συμβατό με το υπάρχον διαδίκτυο αλλά απαιτούνται πρόσθετες προσπάθειες για να σχεδιαστεί η αρχιτεκτονική του και να δημιουργηθεί η διεπαφή με το κλασικό δίκτυο. Εν ολίγοις, η κλασική κρυπτογραφία που εγγύεται την ατελή συσκευή QSDC, συνδυάζει κλασικές κρυπτογραφικές τεχνικές με QSDC χρησιμοποιώντας υπάρχουσα τεχνολογία, επιτρέποντας εμπιστευτική επικοινωνία σε βελτιωμένο επίπεδο ασφάλειας [12].

2000	Ο Long και ο Liu πρότειναν ένα αποτελεσματικό πρωτόκολλο QSDC χρησιμοποιώντας τη μετάδοση μπλοκ των ζευγών Einstein-Podolsky-Rosen (EPR).
2003	Ο Deng κατασκεύασε το πρωτόκολλο QSDC δύο σταδίων και συζητήθηκε το τυπικό κριτήριο του QSDC.
2004	Οι Deng και Long παρουσίασαν το

	πρωτόκολλο DL04 QSDC με μεμονωμένα φωτόνια.
2005	Ο Wang χρησιμοποίησε την πηγή των καταστάσεων Bell d-διάστασης για να υλοποιήσει ένα πρωτόκολλο QSDC δύο βημάτων υψηλής διάστασης. Ο Wang δημιούργησε το σχήμα QSDC πολλαπλών βημάτων χρησιμοποιώντας πυκνή κωδικοποίηση GHZ κατάστασης. Ο Zhang πρότεινε ένα σχήμα πολυμερούς κβαντικής κοινής χρήσης μυστικών με βάση το πρωτόκολλο DL04 QSDC.
2006	Ο Jin συνέλαβε το τριμερές ταυτόχρονο QSDC με βάση τις καταστάσεις GHZ. Ο Lee κατασκεύασε ένα πρωτόκολλο QSDC με έλεγχο ταυτότητας που βασίζεται σε καταστάσεις GHZ. Ο Deng πρότεινε ένα δίκτυο QSDC που δίνει τη δυνατότητα σε οποιονδήποτε από τους εξουσιοδοτημένους χρήστες να μπορεί να επικοινωνήσει με ένα άλλο στο δίκτυο.
2007	Ο Deng πρότεινε το δίκτυο QSDC με φωτόνια εμπλοκής και δόλωμα.
2008	Ο Lin σχεδίασε το πρωτόκολλο QSDC χρησιμοποιώντας την κατάσταση χ. Ο Pirandola κατασκεύασε ένα πρωτόκολλο κβαντικής άμεσης επικοινωνίας συνεχούς μεταβλητής.
2009	Ο Qin μελέτησε το QSDC σε συλλογικό κανάλι απόσβεσης πλάτους.
2010	Ο Gao ανέλυσε την ασφάλεια ενός πολυμερούς ελεγχόμενου πρωτοκόλλου QSDC που βασίζεται στην κατάσταση GHZ.

2011	Ο Lu παρείχε την άνευ όρων απόδειξη ασφαλείας της κβαντικής επικοινωνίας τεσσάρων καταστάσεων που ταιριάζει στο DL04 πρωτόκολλο.
2012	Ο Sun πρότεινε ένα QSDC πρωτόκολλο με κατάσταση συμπλέγματος.
2013	Ο Chang πρότεινε ένα πρωτόκολλο QSDC με έλεγχο ταυτότητας χρησιμοποιώντας μεμονωμένα φωτόνια.
2014	Ο Yadav πρότεινε ένα QSDC δύο βημάτων με τη βοήθεια της αναδιάταξης της τάξης. Ο Shapiro και άλλοι πρότειναν ένα πρωτόκολλο QSDC βασισμένο στον κβαντικό φωτισμό.
2015	Ο Farouk σχεδίασε ένα πρωτόκολλο QSDC <i>N</i> συμβαλλόμενου μέρους με έλεγχο ταυτότητας.
2016	Ο Hu σχεδίασε και απέδειξε πειραματικά ένα πρωτόκολλο DL04 QSDC κωδικοποιημένο με συχνότητα ενός φωτονίου. Ο Lum έδειξε ότι το κβαντικό κλείδωμα δεδομένων μπορεί να εφαρμοστεί στο QSDC.
2017	Ο Zhang χρησιμοποίησε την υπερσύγχρονη ατομική κβαντική μνήμη και έδειξε τις αρχές του αποτελεσματικού QSDC και το πρωτόκολλο QSDC δύο βημάτων για πρώτη φορά. Ο Zhang πραγματοποίησε QSDC σε μεγάλες αποστάσεις χρησιμοποιώντας το αποτελεσματικό QSDC και τα πρωτόκολλα QSDC δύο βημάτων.
2018	Ο Zhou ανέφερε ένα ανεξάρτητο από τη συσκευή μέτρησης (MDI) σχέδιο QSDC μεμονωμένων φωτονίων.

	Niu: προτεινόμενο σχέδιο MDI QSDC ζευγών EPR. Ο Sun σχεδίασε ένα πρωτόκολλο QSDC που δεν απαιτεί κβαντική μνήμη, ξεπερνώντας ένα πρακτικό εμπόδιο QSDC.
2019	Ο Qi εφάρμοσε ένα πρακτικό σύστημα QSDC με την ανάλυση ασφαλείας της θεωρίας του καναλιού υποκλοπής Wyner. Ο Shapiro πρότεινε ότι το πρωτόκολλο κβαντικής χαμηλής πιθανότητας αντίληψης μπορεί να θεωρηθεί ως παράδειγμα QSDC. Ο Zhou πρότεινε το πρωτόκολλο QSDC ανεξάρτητα από τη συσκευή (DI). Ο Massa απέδειξε πειραματικά αμφίδρομη QSDC.
2020	Ο Sun πρότεινε ένα πρωτόκολλο DL04 QSDC χωρίς κβαντική μνήμη χρησιμοποιώντας τη θεωρία κωδικοποίησης. Ο Pan ανέφερε ένα QSDC ελεύθερου χώρου. Ο Lindsey πρότεινε μια προσέγγιση φάσματος για την επίτευξη QSDC πάνω από τα θορυβώδη κβαντικά κανάλια.
2021	Ο Qi παρουσίασε ένα δίκτυο QSDC 15 χρηστών που βασίζεται στη διανομή εμπλοκής. Ο Vázquez-Castro χρησιμοποίησε μια κβαντική έκδοση της διαμόρφωσης on-off keying για την απευθείας μετάδοση εμπιστευτικών πληροφοριών πάνω από ένα κβαντικό κανάλι.

2022	Ο Zhang δήλωσε σημαντική ανακάλυψη σε 100 km QSDC με βάση τις ίνες. Ο Wu απέδειξε την ασφάλεια του QSDC λαμβάνοντας υπόψη το φαινόμενο πεπερασμένου μεγέθους. Ο Long πρότεινε ένα ασφαλές δίκτυο επαναλήπτη και το απέδειξε πειραματικά. Ο Liu ανέφερε ένα πείραμα απόδειξης αρχής QSDC σε ένα κανάλι ινών μήκους 5 km. Ο Sheng χαλάρωσε την απαίτηση αμφίδρομης μετάδοσης φωτονίων στο σχήμα QSDC δύο βημάτων, προτείνοντας έναν μονόδρομο μετάδοσης για την επίτευξη QSDC.
2023	Ο Panda παρουσίασε ένα πρωτόκολλο QSDC χρησιμοποιώντας κβαντικούς περιπάτους σε καταστάσεις τροχιακής γωνιακής ορμής (OAM). Ο Zhou σχεδίασε ένα σχήμα DI QSDC που βασίζεται σε πηγές ενός φωτονίου. Ο Li πρότειναν ένα πρωτόκολλο MDI QSDC με μνήμη ενός φωτονίου και συνήγαγαν την ικανότητά του για μυστικότητα. Ο Sun χαλάρωσε την απαίτηση για κρατική προετοιμασία στο MDI QSDC και προσδιόρισε την πρακτική ικανότητα μυστικότητας του πρωτόκολλο ενσωματώνοντας προσαρμοσμένες μεθόδους κατάστασης δόλωσης. Ο Xu πρότεινε ένα σχήμα κβαντικής αλυσίδας μπλοκ που βασίζεται στο QSDC.

4. Συμπεράσματα

Το κύριο πλεονέκτημα της επικοινωνίας στον κβαντικό τομέα είναι ότι μπορεί να ανιχνευθεί η υποκλοπή, κάτι που δεν συμβαίνει στον κλασικό τομέα. Έτσι, εάν μια διαδικασία QKD διαταραχθεί από έναν υποκλοπέα, οποιαδήποτε περαιτέρω διαδικασία περιορίζεται και η βασική διαπραγμάτευση ξεκινά εκ νέου. Μόλις καθοριστεί το κλειδί, μπορεί να χρησιμοποιηθεί ακριβώς με τον ίδιο τρόπο όπως στην κλασική κρυπτογράφηση. Ακόμη, σε αντίθεση με την “οικογένεια” των QKD πρωτοκόλλων που αποτελούνται από μυστικά κλειδιά διαπραγμάτευσης, το QSDC υποστηρίζει ασφαλή επικοινωνία χωρίς να απαιτείται κρυπτογραφικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.

Παράλληλα, η διανομή ενός μυστικού κλειδιού καθίσταται δυνατή, επειδή στο QSDC τα εμπιστευτικά μηνύματα ενσωματώνονται απευθείας στο κβαντικό σύστημα και μεταδίδονται μεταξύ των μερών που επικοινωνούν μέσω ενός κβαντικού καναλιού. Ακόμη, τα πρωτόκολλα QSDC είναι εξαιρετικά κατάλληλα για διάφορες κρυπτογραφικές εργασίες ενώ με το πέρασμα των χρόνων κατασκευάστηκε μεγάλος αριθμός κρυπτογραφικών πρωτοκόλλων πέρα από το QSDC. Τέλος, σύμφωνα με τα παραπάνω ο ρυθμός πληροφόρησης καθώς και η απόσταση επικοινωνίας αποτελούν δύο παράγοντες που περιορίζουν την απόδοση του QSDC, συνεπώς βρίσκεται σε πρώιμο στάδιο μέχρι στιγμής.

Συμπερασματικά, υπάρχουν σημαντικές αναξιοποίητες ευκαιρίες και πολυάριθμα ανοιχτά προβλήματα προς επίλυση μιας ισχυρά διεπιστημονικής ερευνητικής κοινότητας, συμπεριλαμβανομένων πολλών ανοιχτών προβλημάτων στην κβαντική θεωρία πληροφοριών και επικοινωνίας, στην κβαντική φυσική και σε πολλές πτυχές της κβαντικής μηχανικής. Συνεπώς, η περαιτέρω διερεύνηση των δυνατοτήτων του ασύρματου QSDC τόσο στο πλαίσιο της οπτικής δορυφορικής επικοινωνίας όσο και στα επίγεια σενάρια, στηριζόμενα σε επικοινωνίες ορατού φωτός και ασύρματες επικοινωνίες αποτελεί μια συναρπαστική κατεύθυνση που πιθανότατα να καταλήξει στην εφεύρεση ενός νέου αλγορίθμου.

5. Αναφορές

- [1] McMahon, D. (2007). Quantum Computing Explained. In *Quantum Computing Explained*. <https://doi.org/10.1002/9780470181386>
- [2] Wolf, R. (2021) *Quantum Key Distribution: An introduction with exercises*. Cham, Switzerland: Springer.
- [3] UNRUH, W. G. (1995). Varieties of Quantum Measurement. *Annals of the New York Academy of Sciences*, 755(1). <https://doi.org/10.1111/j.1749-6632.1995.tb38996.x>
- [4] DiVincenzo, D. P. (1998). Quantum gates and circuits. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 454(1969). <https://doi.org/10.1098/rspa.1998.0159>
- [5] Yanofsky, N. S., & Mannucci, M. A. (2008). Quantum computing for computer scientists. In *Quantum Computing for Computer Scientists* (Vol. 9780521879965). <https://doi.org/10.1017/CBO9780511813887>
- [6] Nurhadi, A. I., & Syambas, N. R. (2018). Quantum Key Distribution (QKD) Protocols: A Survey. *Proceeding of 2018 4th International Conference on Wireless and Telematics, ICWT 2018*. <https://doi.org/10.1109/ICWT.2018.8527822>
- [7] Reddy, S., Mandal, S., & Mohan, C. (2023). Comprehensive Study of BB84, A Quantum Key Distribution Protocol. *International Research Journal of Engineering and Technology*. Retrieved from www.irjet.net
- [8] Long, G. L., & Liu, X. S. (2002). Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A - Atomic, Molecular, and Optical Physics*, 65(3). <https://doi.org/10.1103/PhysRevA.65.032302>
- [9] Deng, F. G., Long, G. L., & Liu, X. S. (2003). Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A - Atomic, Molecular, and Optical Physics*, 68(4). <https://doi.org/10.1103/PhysRevA.68.042317>
- [10] Qin, H., Sun, W., & Tang, W. K. S. (2022). Quantum secure direct communication based on single particles. *Optical and Quantum Electronics*, 54(8). <https://doi.org/10.1007/s11082-022-03920-4>
- [11] Pan, D., Song, X.-T., & Long, G.-L. (2023). Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook. *Advanced Devices & Instrumentation*, 4. <https://doi.org/10.34133/adi.0004>

- [12] Pan, D., Long, G. L., Yin, L., Sheng, Y. B., Ruan, D., Ng, S. X., Lu, J., & Hanzo, L. (2024). The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet. *IEEE Communications Surveys and Tutorials*.
<https://doi.org/10.1109/COMST.2024.3367535>