Σχολή Θετικών Σπουδών

Προχωρημένες Σπουδές στη Φυσική

Διπλωματική Εργασία

«Η Κρυπτογραφία στον Κόσμο της Κβαντικής Θεωρίας»

Ιωάννα-Μαρία Αναργύρου

Επιβλέπων καθηγητής: Ανδρέας Ζούπας

Πάτρα, Μάιος 2024

«Η Κρυπτογραφία στον Κόσμο της Κβαντικής Θεωρίας»

Ιωάννα-Μαρία Αναργύρου

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής:

Ανδρέας Ζούπας

Συμβασιούχος Διδάσκων, Τμήμα Φυσικής, Τμήμα Μηχανολόγων Μηχανικών, Πανεπιστήμιο Θεσσαλίας

Σ.Ε.Π. Ελληνικό Ανοικτό Πανεπιστήμιο

Συν-Επιβλέπων Καθηγητής:

Παπαδόπουλος Κωνσταντίνος

Διευθυντής Ερευνών στο Ινστιτούτο Πυρηνικής και Σωματιδιακής Φυσικής του ΕΚΦΕ "ΔΗΜΟΚΡΙΤΟΣ"

Πάτρα, Μάιος 2024

Στην οικογένειά μου για τη στήριξη

και

στον καθηγητή μου για την καθοδήγηση

Περίληψη

Η διπλωματική εργασία, με τίτλο «Η Κρυπτογραφία στον Κόσμο της Κβαντικής Θεωρίας», έχει ως θέμα να αναλύσει τις αρχές της κβαντικής φυσικής που διασφαλίζουν την διανομή του κβαντικού κλειδιού, το οποίο είναι βασικό στοιχείο για την μετάδοση της πληροφορίας. Είναι χωρισμένη σε πέντε κεφάλαια, με το 1ο κεφάλαιο να τονίζει τους λόγους για τους οποίους η κβαντική κρυπτογραφία είναι αναγκαία σε σχέση με την κλασική.

Στο 2ο κεφάλαιο αναφέρονται έννοιες που σχετίζονται με το θέμα, η κβαντική πληροφορία, η οποία αναφέρεται στην μελέτη του τρόπου με τον οποίο οι πληροφορίες μπορούν να κωδικοποιηθούν και να επεξεργαστούν χρησιμοποιώντας τις αρχές της κβαντικής μηχανικής. Ακόμα, παρατίθεται η έννοια του qubit, ως του αντίστοιχου bit για τους κλασικούς υπολογιστές, όπως επίσης οι κβαντικές λογικές πύλες και ο αλγόριθμος του Shor, που βοηθούν στην κωδικοποίηση/αποκωδικοποίηση της πληροφορίας.

Στο κεφάλαιο 3ο αναλύονται οι αρχές της κβαντικής φυσικής πάνω στις οποίες στηρίζεται η κρυπτογραφία, με ιδιαίτερη έμφαση στην κβαντική διεμπλοκή, φαινόμενο κατά το οποίο δύο σωματίδια (συγκεκριμένα φωτόνια σε αυτήν τη διπλωματική) είναι διεπλεγμένα και επηρεάζουν το ένα στο άλλο ακόμα και αν βρίσκονται σε μεγάλες αποστάσεις. Ακόμα, αναφέρεται το EPR παράδοξο, το θεώρημα του Bell και η παραβίαση των ανισοτήτων του, η οποία επιβεβαιώνει την κβαντική διεμπλοκή ως κύριο θεμέλιο της κβαντικής θεωρίας.

Το 4ο κεφάλαιο ξεκινάει με μία ιστορική αναδρομή της κβαντικής κρυπτογραφίας και συνεχίζει στην περιγραφή της διανομής του κβαντικού κλειδιού ανάμεσα στον αποστολέα, που συνήθως ονομάζεται Αλίκη και στον παραλήπτη, που συνήθως ονομάζεται Μπομπ. Αναφέρονται δύο πρωτόκολλα της διανομής του κβαντικού κλειδιού, του Ekert και το BB84, που εξηγούν πώς γίνεται η επιλογή του κλειδιού καταλήγοντας με τους λόγους που οποιαδήποτε υποκλοπή από την Εύα θα γίνει αντιληπτή.

Τέλος, στο 5ο κεφάλαια αναφέρονται τεχνολογίες που έχουν σχέση με την κβαντική κρυπτογραφία, όπως οι κβαντικοί υπολογιστές, οι οπτικές ίνες για την καλύτερη επικοινωνία μέσω του κβαντικού καναλιού και η σχέση με την τεχνητή νοημοσύνη.

Λέξεις – Κλειδιά: Κβαντική κρυπτογραφία, κβαντική διεμπλοκή, διανομή κβαντικού κλειδιού, κβαντικοί υπολογιστές, EPR παράδοξο, ανισότητες Bell

«Cryptography in the field of Quantum Information»

Ioanna-Maria Anargyrou

Abstract

The dissertation, titled "Cryptography in the field of Quantum Information," aims to analyze the principles of quantum physics that ensure the distribution of the quantum key, which is a fundamental element for information transmission. It is divided into five chapters, with the 1st chapter emphasizing the reasons why quantum cryptography is necessary compared to classical cryptography.

In the 2nd chapter, concepts related to the topic are mentioned, such as quantum information, which refers to the study of how information can be encoded and processed using the principles of quantum mechanics. The concept of the qubit is also presented as the equivalent of the bit for classical computers, as well as quantum logical gates and Shor's algorithm, which assist in the encoding/decoding of information.

The third chapter analyzes the principles of quantum physics on which cryptography is based, with particular emphasis on quantum entanglement, a phenomenon where two particles (specifically photons in this thesis) are entangled and influence each other even when separated by large distances. Additionally, the EPR paradox, Bell's theorem, and the violation of Bell's inequalities are mentioned, which confirm quantum entanglement as a key foundation of quantum theory.

The fourth chapter begins with a historical overview of quantum cryptography and continues with the description of quantum key distribution between the sender, usually named Alice, and the receiver, usually named Bob. Two protocols for quantum key distribution, Ekert and BB84, are mentioned, explaining how key selection is done and concluding with the reasons why any eavesdropping by Eve will be detected.

Finally, the fifth chapter discusses technologies related to quantum cryptography, such as quantum computers, optical fibers for better communication through the quantum channel, and the relationship with artificial intelligence.

Keywords: Quantum cryptography, entanglement, quantum key distribution, quantum computers, EPR paradox, Bell’s inequalities

1. Περιεχόμενα

2. Κατάλογος Εικόνων / Σχημάτων

3. Συντομογραφίες & Ακρωνύμια

EPR	Einstein, Podolsky, Rosen
QKD	Quantum Key Distribution
IBM	International Business Machines Corporation
NMR	Πυρηνικός Μαγνητικός Συντονισμός

1. Κρυπτογραφία

1.1 Κρυπτογραφία

Η κρυπτογραφία παίζει εδώ και πολλά χρόνια σημαντικό ρόλο στην προστασία κυρίως των εμπορικών και στρατιωτικών μυστικών πληροφοριών, με κορύφωση το τελευταίο χρονικό διάστημα την ανάπτυξη των ηλεκτρονικών συστημάτων με χρήση πιστωτικών καρτών μέχρι και αγορών μέσω Διαδικτύου. Ο κύριος στόχος της είναι να εφαρμόζει διάφορες τεχνικές κρυπτογράφησης και αποκρυπτογράφησης, ώστε να διαφυλάσσονται τα δεδομένα και να μην μπορούν να παραβιαστούν.

Ετυμολογικά η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω", που μαζί με την κρυπτανάλυση αποτελούν την επιστήμη της κρυπτολογίας, και οι λειτουργίες της βασίζονται σε τέσσερις πυλώνες.

Το πρώτο βασικό μέρος είναι η εμπιστευτικότητα, δηλαδή η μετάδοση της πληροφορίας ανάμεσα σε συγκεκριμένα μέλη να μην είναι προσβάσιμη σε κάποιον εξωτερικό παρατηρητή. Δεύτερο είναι η ακεραιότητα, δηλαδή ότι δεν μπορεί η πληροφορία να αλλοιωθεί. Επιπροσθέτως, ο αποστολέας και ο παραλήπτης δεν μπορούν να αρνηθούν την αυθεντικότητά της, ως προς την μετάδοση ή την δημιουργίας της. Τέλος, η μετάδοση της πληροφορίας βασίζεται στο γεγονός ότι μπορεί να γίνει εξακρίβωση της πηγής και του παραλήπτη, ώστε να διαβεβαιώσουμε ότι οι ταυτότητές τους είναι ορθές.

1.1.1 Ιστορική Αναδρομή

Η πρώτη περίοδος της κρυπτογραφίας ορίζεται ανάμεσα στο 1900 π.Χ. και 1900 μ.Χ. όπου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, χρησιμοποιώντας απλές αντικαταστάσεις γραμμάτων.

Η κρυπτογραφία χρησιμοποιήθηκε και σε στρατιωτικές επιχειρήσεις, όπως για παράδειγμα κατά τον 5ο π.Χ. αιώνα, από τους Σπαρτιάτες, με την «σκυτάλη», η οποία θεωρείται ότι ήταν η πρώτη κρυπτογραφική συσκευή.

Εικόνα 1-1: Η Σκυτάλη τον 5ο π.Χ. αιώνα

(Τσιαλίκη Α. (χ.χ.))

Στη συνέχεια, κατά την περίοδο του Μεσαίωνα, η κρυπτολογία ήταν απαγορευτική και θεωρούταν ως μία μορφή μαύρης μαγείας, όμως εξελίχθηκε αργότερα κυρίως στον Αραβικό κόσμο.

Ο πρώτος που κατασκεύασε μία μηχανική κρυπτοσυσκευή είναι ο C.Wheatstone, η οποία και απετέλεσε τη βάση για την ανάπτυξη των μελλοντικών κρυπτομηχανών.

Ένα μεγάλο μυστήριο για πολλούς αιώνες αποτελούσαν τα αιγυπτιακά ιερογλυφικά, τα οποία ήταν απλή αντικατάσταση των γραμμάτων με δύσκολα σύμβολα. Η αποκρυπτογράφησή τους θεωρείται μεγάλο επίτευγμα στον τομέα της κρυπτογραφίας.

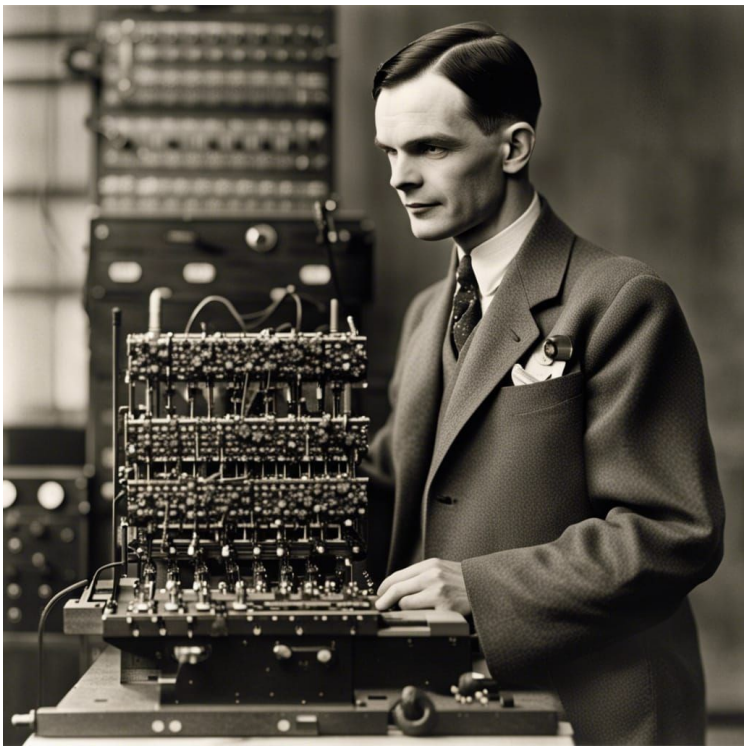
Εικόνα 1-2: Αιγυπτικά Ιερογλυφικά

(https://www.upsite.gr/istoria/i-minoiki-grafi-emfanistike-500-chronia-prin-egrafan-me-ieroglyfika-kai-grammiki-a-apo-tin-3i-chilietia-pch-foto/)

Η δεύτερη περίοδος της κρυπτογραφίας βρίσκεται ανάμεσα στο 1900 μ.Χ. και 1950 μ.Χ., κατά την οποία σημειώνονται οι δύο παγκόσμιοι πόλεμοι. Η κρυπτογραφία έπαιξε σημαντικό ρόλο καθώς ήταν επιτακτική η ανάγκη μετάδοσης πληροφοριών με απόλυτη ασφάλεια για στρατιωτικές επιχειρήσεις.

Τα κρυπτοσυστήματα αυτής της περιόδου έγιναν πιο πολύπλοκα και σύνθετα, και αποτελούνταν από μηχανικές και ηλεκτρομηχανικές κατασκευές, τις «κρυπτομηχανές».

Οι Γερμανοί στον Β' Παγκόσμιο Πόλεμο χρησιμοποίησαν ένα σύστημα, γνωστό ως *Enigma*, για την προστασία της διπλωματικής και στρατιωτικής επικοινωνίας, και θεωρήθηκε τόσο ασφαλές ώστε να κρυπτογραφεί τα πιο άκρως απόρρητα μηνύματα. Διέθετε έναν ηλεκτρομηχανικό μηχανισμό που ανακάτευε τα 26 γράμματα του αλφαβήτου. Τα γερμανικά κρυπτογραφημένα μηνύματα έσπασε ο Άλαν Μάθισον Τούρινγκ και η Ομάδα 8, στην Βρετανική Υπηρεσία Αντικατασκοπείας.



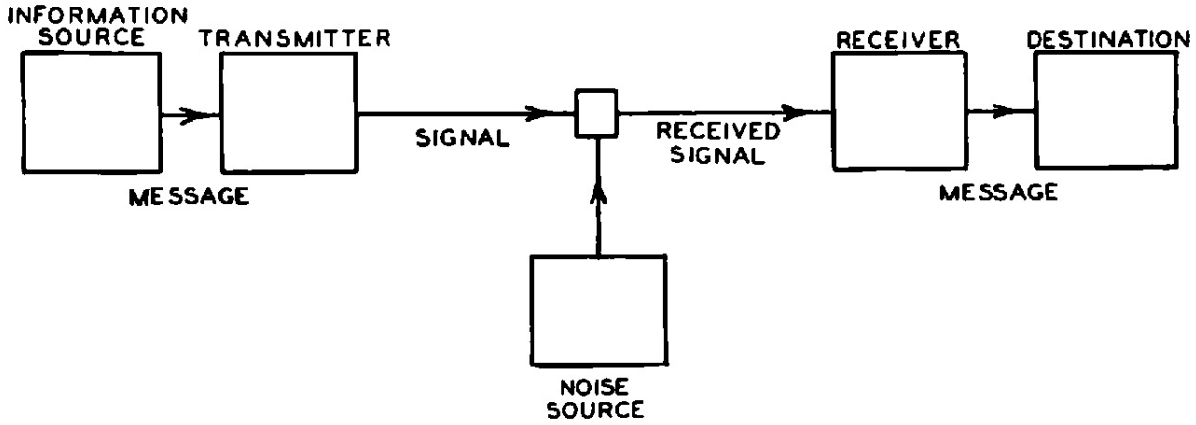
Εικόνα 1-3: Alan Mathison Turing
(https://www.bulbapp.io/p/f8179d07-c98e-41dc-9ed2-2eee0e7a8566/alan-turing-the-genius-and-tragedy-of-a-visionary-mind)

Εικόνα 1-4: Η Μηχανή Enigma
(https://www.bbvaopenmind.com/en/technology/innovation/the-human-errors-that-defeated-enigma/)

1.2 Κλασική Κρυπτογραφία

Η κλασική κρυπτογραφία χρησιμοποιεί συστήματα κωδικοποίησης που δεν μπορούν να παραβιαστούν σε ένα λογικό χρονικό διάστημα με τα υπάρχοντα μέσα υπολογισμού. Γι'αυτό τον λόγο το τωρινό επίπεδο ασφάλειας θεωρείται αποδεκτό. Παρόλο αυτά δεν είναι απόλυτο, καθώς εξαρτάται από την υπολογιστική ισχύ που διαθέτει κάποιος.

Το μεγαλύτερο μέρος της κρυπτογραφίας βασίζεται στην ιδέα της Αλίκης (αποστολέα) και του Μπομπ (παραλήπτη), αφού προηγουμένως έχουν ανταλλάξει ένα μυστικό κλειδί, δηλαδή μια μεγάλη ακολουθία τυχαίων χαρακτήρων που γνωρίζουν μόνο οι ίδιοι. Η ασφάλεια του μηνύματος διερευνάται από το αν αυτό το μυστικό κλειδί είναι ασφαλές ή θα μπορούσε να υποκλαπεί, και έχει τις βάσεις του σε ένα μαθηματικό θεώρημα που αποδείχθηκε από τον Claude Shannon και αναλύεται στις δημοσιευμένες εργασίες του «A Mathematical Theory of Cryptography» του 1945 και «Communication Theory of Secrecy Systems» το 1949. Ο Shannon έθεσε θεωρητικά θεμέλια για την κατανόηση και την ανάπτυξη ασφαλών συστημάτων επικοινωνίας και μαθηματικά θεμέλια για την μελέτη της κρυπτογραφίας, εισάγοντας τον όρο του μυστικού κλειδιού. Υποστήριξε ότι αν δεν γνωρίζουμε το μυστικό κλειδί είναι αδύνατο να αποκαλυφθεί οποιαδήποτε κρυπτογραφημένη πληροφορία.



Εικόνα 1-5: Διάγραμμα της επικοινωνίας του Shannon
(https://www.quantamagazine.org/print)

Στην σημερινή εποχή, όμως, με την εξέλιξη της επιστήμης και τεχνολογίας, ειδικά των υπολογιστών, βρίσκονται ολοένα και περισσότερες τεχνικές που μπορούν να αποκωδικοποιήσουν το μυστικό κλειδί, με αποτέλεσμα η μετάδοση της πληροφορίας να μπορεί να παραβιαστεί.

Πολλοί από τους αλγόριθμους αποκρυπτογράφησης που χρησιμοποιούνται καταφέρνουν να σπάσουν, να αποκωδικοποιήσουν τα μυστικά κλειδιά, με αποτέλεσμα να μην είναι ασφαλείς για την μετάδοση της πληροφορίας. Ένα ακόμη μεγάλο ζήτημα είναι η ραγδαία ανάπτυξη των υπολογιστών, με μεγάλη υπολογιστική ισχύ ώστε να μπορούν να τρέξουν δυνατούς αλγόριθμους παραβίασης των δεδομένων.

Το τελευταία έρχεται να ενισχύσει και η εξέλιξη των κβαντικών υπολογιστών, οι οποίοι, αν και σε πρώιμο στάδιο, διαθέτουν μεγάλη ισχύ και μπορούν να σπάσουν πολλούς ήδη υπάρχοντες αλγόριθμους σε μικρότερο χρονικό διάστημα από ότι οι κλασικοί υπολογιστές.

Έτσι, οι νέες απειλές στην ασφάλεια της μετάδοσης της πληροφορίας, φέρνουν την κλασική κρυπτογραφία σε κρίσιμο σημείο, θέτοντας επιτακτική ανάγκη εύρεσης εναλλακτικών τρόπων δημιουργίας κλειδιών, κωδικοποίησης και αποκωδικοποίησης, ώστε η ασφάλεια να είναι σχεδόν απόλυτη.

1.3 Κβαντική Κρυπτογραφία

Η κβαντική κρυπτογραφία έρχεται να λύσει το πρόβλημα παραβίασης του μυστικού κλειδιού χρησιμοποιώντας τις αρχές της κβαντικής φυσικής. Η διαμοίραση του κβαντικού κλειδιού πάλι γίνεται ανάμεσα στην Αλίκη και τον Μπομπ, που στην ουσία στέλνουν μία σειρά από πολωμένα φωτόνια.

Η κβαντική διεμπλοκή των σωματιδίων, και κυρίως των φωτονίων, η αρχή αβεβαιότητας του Heisenberg και το θεώρημα no cloning είναι από τις κυρίαρχες ιδιότητες για την δημιουργία του μυστικού κλειδιού και την ασφάλειά του. Έτσι διασφαλίζεται ότι οποιαδήποτε απόπειρα υποκλοπής του κλειδιού θα αλλάξει το σύστημα, συνεπώς θα γίνει και αντιληπτή.

Εικόνα 1-6: Μυστικό Κλειδί μέσω Κβαντικής Κρυπτογραφίας
(https://www.ma8imatikos.gr/cryptography-rsa/)

Η κβαντική κρυπτογραφία είναι κομμάτι της κβαντικής πληροφορίας και επικοινωνίας, με τη χρήση των σωματιδίων και των κβαντικών τους ιδιοτήτων. Η κβαντική κατάσταση ενός σωματιδίου χρησιμοποιείται για την κωδικοποίηση των qubits, αντιπροσωπεύοντας τις κωδικοποιημένες πληροφορίες που μπορούν να υποβληθούν σε επεξεργασία και να γίνουν αντιληπτές μόνο από τον παραλήπτη. Στην περίπτωση που ένας τρίτος προσπαθήσει να υποκλέψει τις πληροφορίες που στέλνονται, η μετάδοση της πληροφορίας καταστρέφεται.

2. Κβαντική Πληροφορία

2.1 Κβαντική Πληροφορία

Η κβαντική πληροφορία είναι ένα επιστημονικό πεδίο που επικεντρώνεται στην μετάδοση της πληροφορίας μέσω κβαντικών φαινομένων όπως η υπέρθεση καταστάσεων και η διεμπλοκή των σωματιδίων. Αναφέρεται στην μελέτη του τρόπου με τον οποίο η πληροφορία μπορεί να κωδικοποιηθεί και να επεξεργαστεί χρησιμοποιώντας τις αρχές της κβαντικής μηχανικής. Τα περισσότερα άρθρα για την επιστήμη της κβαντικής πληροφορίας εστιάζουν σε τεχνολογικές εφαρμογές, όπως η τηλεμεταφορά κβαντικών καταστάσεων από μια θέση σε μια άλλη, η δημιουργία κρυπτογραφικών κλειδιών, αλλά και την δημιουργία αλγορίθμων για τους κβαντικούς υπολογιστές του μέλλοντος.

Η θεωρία της κβαντικής πληροφορίας είναι διεπιστημονική και βασίζεται σε έννοιες από την κβαντική φυσική, τα μαθηματικά, την επιστήμη των υπολογιστών και την μηχανική. Έχει τη δυνατότητα να φέρει επανάσταση σε τομείς όπως η κρυπτογραφία, η βελτιστοποίηση, η ανακάλυψη φαρμάκων και η επιστήμη των υλικών. Ωστόσο, οι πρακτικοί κβαντικοί υπολογιστές που είναι ικανοί να ξεπερνούν τους κλασικούς υπολογιστές σε ένα ευρύ φάσμα εργασιών βρίσκονται ακόμη στα αρχικά στάδια ανάπτυξης.

Βασικές κβαντικές έννοιες που συνδέονται με την κβαντική πληροφορία είναι η υπέρθεση και η διεμπλοκή. Η υπέρθεση δύο ή περισσότερων καταστάσεων είναι θεμελιώδης αρχή της κβαντικής φυσικής και στηρίζεται στο γεγονός ότι ένα κβαντικό σύστημα μπορεί να υπάρξει σε πολλές καταστάσεις ταυτόχρονα μέχρι να μετρηθεί. Η διεμπλοκή είναι το κβαντικό φαινόμενο κατά το οποίο δύο ή περισσότερα σωματίδια συσχετίζονται, έτσι ώστε η κατάσταση του ενός να μην μπορεί να περιγραφεί ανεξάρτητα από την κατάσταση του άλλου, όπως θα συζητηθεί πιο αναλυτικά στα επόμενα κεφάλαια.

Η κβαντική πληροφορία μεταφέρεται μέσω κβαντικών συστημάτων, έχοντας ως πομπό μία συσκευή που προετοιμάζει τα κβαντικά σωματίδια, και μία άλλη συσκευή μέτρησης, ως δέκτη.

Η πληροφορία δεν είναι καθαρά μαθηματική υπόθεση αλλά έχει και φυσικό περιεχόμενο. Στην κλασική θεωρία πληροφοριών, η πληροφορία μπορεί να αναπαρασταθεί σε bit, τα οποία μπορεί να είναι είτε 0 είτε 1. Η επιστήμη της κβαντικής πληροφορίας βάζει την πληροφορία σε κβαντική αντιμετώπιση, χρησιμοποιώντας τα κβαντικά bit ή qubits, τα οποία

αντιπροσωπεύουν και το 0 και το 1 και μπορούν να προκύψουν από μια υπέρθεση καταστάσεων, και μπορούν να διεμπλέκονται. Η πληροφορία από ένα qubit πρέπει να εξαχθεί με κάποια μέτρηση, και το αποτέλεσμα θα είναι πάντα ένα 0 ή 1, παρά το γεγονός ότι το qubit περιέχει άπειρη πληροφορία.

Άλλος χρήσιμος όρος που αφορά στην κβαντική πληροφορία είναι κβαντική τηλεμεταφορά που αποτελεί την διαδικασία με την οποία η κατάσταση ενός κβαντικού συστήματος, δηλαδή το qubit, μπορεί να μεταφερθεί από τη μία θέση στην άλλη, με τη βοήθεια της διεμπλοκής, χωρίς όμως να μετακινηθεί το ίδιο το σύστημα.

Ο τομέας που ασχολείται με την ανάπτυξη υπολογιστών με βάση τις αρχές της κβαντικής μηχανικής ονομάζεται «Quantum Computing» και στηρίζεται στο γεγονός ότι οι κβαντικοί υπολογιστές έχουν τη δυνατότητα να λύσουν ορισμένα προβλήματα πολύ πιο γρήγορα από τους κλασικούς υπολογιστές λόγω της ικανότητάς τους να λειτουργούν σε πολλές καταστάσεις ταυτόχρονα.

Ένα σημαντικό εργαλείο για τους κβαντικούς υπολογιστές είναι η κβαντική διόρθωση σφαλμάτων, η οποία χρησιμοποιείται για την προστασία των κβαντικών πληροφοριών από σφάλματα που εισάγονται από το θόρυβο και άλλους παράγοντες που μπορούν να επηρεάζουν την μεταδοση της κβαντικής πληροφορίας.

Η κβαντική διόρθωση σφαλμάτων στηρίζεται στο no-cloning theorem, κατά το οποίο ένα qubit δεν μπορεί να αντιγραφεί με αξιοπιστία.

Στα μέσα της δεκαετίας του 1990, ήταν ο Rolf Landauer, όπως και άλλοι φυσικοί, οι οποίοι έδειξαν ότι είναι πολύ κρίσιμη η κβαντική διόρθωση σφαλμάτων όσο αφορά στην λειτουργία των κβαντικών υπολογιστών.

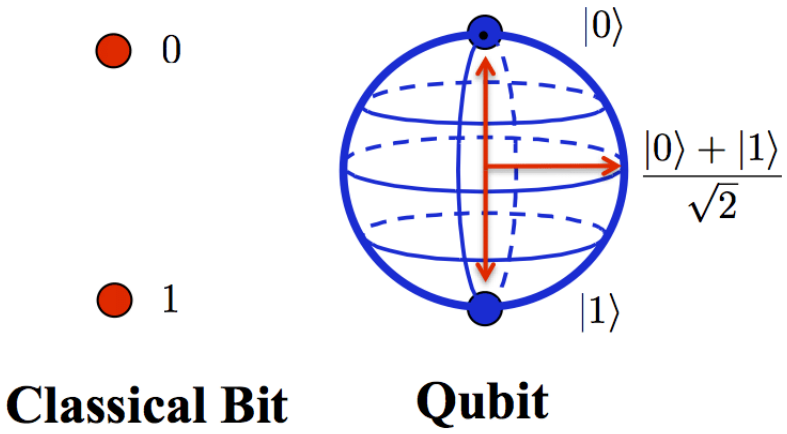
Στη συνέχεια, ο Shor και ο Andrew M. Steane του πανεπιστημίου της Οξφόρδης, το 1995, απέδειξαν την κβαντική διόρθωση σφαλμάτων, χωρίς να χρειαστεί ποτέ να γνωρίζουμε τις καταστάσεις των qubits ή να χρειαστεί να τις αντιγράψουμε.

2.2 Qubits

Η κβαντική πληροφορία συνδέει την έννοια της «πληροφορίας» με τους νόμους της κβαντικής φυσικής. Ενώ λοιπόν, η μετάδοση της κλασικής πληροφορίας γίνεται με τα bits, στο πεδίο της κβαντικής πληροφορίας εισάγεται ο όρος qubit.

Ένα bit μπορεί να πάρει τις τιμές 0, 1 και μπορεί να δίνει την κατάσταση ενός τρανζίστορ σε on ή off λειτουργία, και μπορεί να αντί του 0 και 1 να υπάρχει ένας βέλος προς τα κάτω ή αντίστοιχα ένα βέλος προς τα πάνω.

Το qubit είναι η θεμελιώδη μονάδα κβαντικής πληροφορίας, ανάλογη με τα bit στον κλασική πληροφορία. Ενώ τα κλασικά bits, όπως αναφέραμε, μπορούν να αντιπροσωπεύουν είτε ένα 0 είτε ένα 1, σε αντίθεση το qubit μπορεί να αντιπροσωπεύει ένα 0, ένα 1 ή μια υπέρθεση και των δύο καταστάσεων ταυτόχρονα βασιζόμενο στις αρχές της κβαντικής μηχανικής. Ένα qubit μπορεί να υπάρξει σε μία υπέρθεση καταστάσεων και δεν μπορεί να αναπαρασταθεί με 0, ή 1 μέχρι να μετρηθεί.



Εικόνα 2-1: Αντιστοίχηση των bits με τα qubits

(Lekas, 2023)

Στην παραπάνω εικόνα παρατηρούμε ότι ένα qubit μπορεί να πάρει την τιμή 0 στο βόρειο τμήμα της σφαίρας και την τιμή 1 στο νότιο τίμη της. Οποιοδήποτε άλλο σημείο της σφαίρας είναι κβαντικές υπερθέσεις των καταστάσεων που βρίσκεται το σωματίδιο. Συγκεκριμένα, αν το σωματίδιο είναι το ηλεκτρόνιο, οι καταστάσεις είναι οι αντίστοιχες του spin του, με τιμή

qubit 1 για spin ½ και την τιμή 0 για spin - ½. Επομένως, οι επιτρεπόμενες καταστάσεις ενός qubit είναι όλες εκείνες οι καταστάσεις που προκύπτουν αν στρίψουμε το βέλος σε όλο το χώρο και όχι απλώς κατακόρυφα.

Αν τα σωματίδια είναι τα φωτόνια, στα οποία στηρίζεται η κβαντική κρυπτογραφία που μελετάμε σε αυτήν τη διπλωματική, τότε οι τιμές του qubit δηλώνουν την κατάσταση της πόλωσης των φωτονίων σε κάθετη, ορίζοντια, δεξιόστροφη ή αριστερόστροφη.

Αξιοσημείωτο είναι το γεγονός ότι τα qubits μπορούν να διεμπλακούν, έτσι ώστε το σύστημά τους να έχει μία καλά καθορισμένη κατάσταση αλλά μέχρι να μετρηθεί να μην μπορούμε να γνωρίζουμε με σαφήνεια την κατάσταση του καθενός. Με αυτό τον τρόπο η κατάσταση του ενός εξαρτάται από την κατάσταση του άλλου, διαδραματίζοντας καθοριστικό ρόλο στα κβαντικά συστήματα για την μετάδοση της πληροφορίας και στην κβαντική πληροφορική.

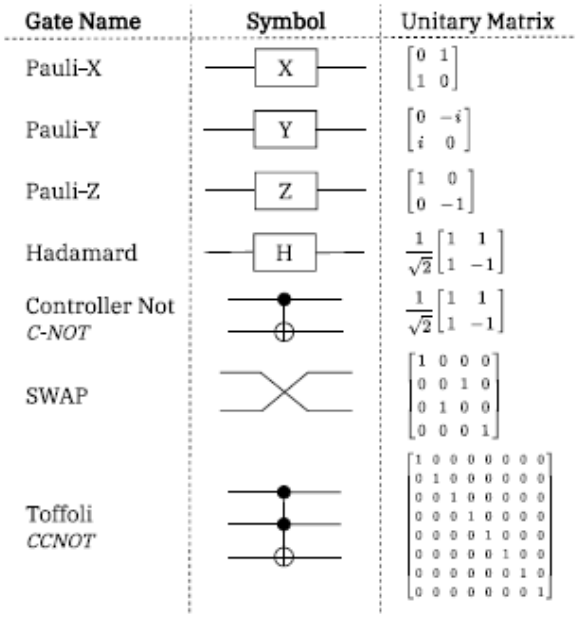
Στην κβαντική διεμπλοκή, τα φωτόνια φαίνονται να συσχετίζονται και παραμένουν συσχετισμένα ακόμα και σε μεγάλες αποστάσεις. Έτσι, φαίνεται να υπάρχει έντονη μη τοπικότητα χωρίς να υπάρχει μετάδοση της πληροφορίας με μεγαλύτερη ταχύτητα από την ταχύτητα του φωτός. Με αυτήν τη συσχέτιση, τα qubits μεταφέρουν την πληροφορία σε μεγάλες αποστάσεις αναλλοίωτη.

Η ποσότητα της πληροφορίας που μπορεί να αποθηκευτεί σε ένα qubit θεωρείται ότι είναι άπειρη λόγω της υπέρθεσης. Παρόλο αυτά, κάποιος δεν θα μπορούσε να ανακτήσει όλη αυτή την πληροφορία, καθώς θεωρείται ότι είναι «κρυμμένη», χωρίς να υπάρχει πρόσβαση σε αυτήν. Μπορούμε όμως να την χειριστούμε και με διάφορες μεθόδους να την αποκωδικοποιήσουμε.

2.2.1 Κβαντικές Πύλες

Όπως θα δούμε και στα επόμενα κεφάλαια, τα qubits είναι οι καταστάσεις υπέρθεσης των καταστάσεων των σωματιδίων και θέλουν ειδικό χειρισμό για την λειτουργία των κβαντικών υπολογιστών. Κυρίως χρησιμοποιούνται φωτόνια, και η επεξεργασία τους βασίζεται στις αρχές της κβαντικής φυσικής, με την δράση ηλεκτρομαγνητικών παλμών και τη διαδικασία της κβαντικής μέτρησης. Σε αντιστοιχία με τα κλασικά bits, η επεξεργασία των μετρήσεων πραγματοποιείται από τις λογικές κβαντικές πύλες, οι οποίες αναπαριστώνται μέσω τελεστών που δρουν πάνω στα qubits.

Κάθε πύλη δρα πάνω σε μία τυχαία κατάσταση και μπορεί να αναπαρασταθεί με ένα ορθομοναδιαίο πίνακα δηλαδή τελεστή στο χώρο Hilbert. Κάθε τελεστής δρά πάνω σε μία κατάσταση, αλλάζοντάς την. Επομένως, οι κβαντικές πύλες είναι ένα είδος κυκλώματος, και μετασχηματίζουν τα qubits ανάλογα με την σειρά που δρουν πάνω στις καταστάσεις. Οι κβαντικές πύλες μπορούν να δράσουν πάνω σε περισσότερα από ένα qubit. Κάποιες από τις κυριότερες πύλες είναι η πύλη Hadamard, οι πύλες Pauli και η πύλη CNOT.



Εικόνα 2-2: Βασικές Κβαντικές Πύλες

(Chamola, Jolfaei, Chanana, Parashari, & Hassija, 2021)

Για παράδειγμα, η πύλη Hadamard δρά σε ένα qubit και περιστρέφει το διάνυσμα μίας κατάστασης μεταβάλλοντας τις γωνίες, και δημιουργούντας ισοβαρείς επαλληλίες των βασικών καταστάσεων $|0>$ και $|1>$.

$$\hat{H}\begin{pmatrix}|0>\\|1>\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}|0>+|1>\\|0>-|1>\end{pmatrix} = \begin{pmatrix}|+>\\|->\end{pmatrix} \qquad (1)$$

Η πύλη Pauli-X δρά πάνω σε ένα qubit και αναστρέφει την κατάστασή του, αλλάζοντας τα 0 και 1, όπως αντίστοιχα κάνει η κλασική πύλη NOT. Μία πύλη που ανήκει σε αυτή την κατηγορία είναι CNOT, η οποία δρα σε δύο qubits και αν το πρώτο βρίσκεται στην κατάσταση $|0>$, το δεύτερο δεν μεταβάλλεται, ενώ αν το πρώτο είναι στην $|1>$ τότε αναστρέφεται το δεύτερο.

Άλλες κβαντικές πύλες, οι οποίες δρουν πάνω σε τρία qubits είναι η πύλη διπλού ελέγχου όχι CCNOT (αλλιώς Toffoli) και η πύλη Fredkin.

Συνοψίζοντας, οι κβαντικές πύλες αναπαριστώνται από τελεστές οι οποίοι δρουν πάνω στα qubits, που με την σειρά τους μεταφέρουν την πληροφορία. Παρά το γεγονός ότι υπάρχουν διάφορες πύλες με δράση πάνω σε ένα, δύο ή τρία qubits, δεν υπάρχει κβαντική πύλη που να μπορεί να αντιγράψει ένα συγκεκριμένο. Με άλλα λόγια, δεν υπάρχει κβαντική πύλη που να μπορεί να κλωνοποιήσει το qubit, και αυτό εδραιώνεται από το θεώρημα no-cloning, που θα παρουσιάσουμε στη συνέχεια. Σε αυτό στηρίζεται η κβαντική κρυπτογραφία, καθώς εξαιτίας αυτού του θεωρήματος μπορεί να ανιχνευθεί η υποκλοπή από κάποιον τρίτο, αν προσπαθήσει να διαβάσει το κωδικοποιημένο μήνυμα και να το στείλει πίσω χωρίς να έχει αλλάξει το μήνυμα.

2.2.2 Αλγόριθμος Shor

Ένα ακόμη πεδίο της κβαντικής πληροφορίας είναι οι κβαντικοί αλγόριθμοι και ο λόγος που χρειάζονται είναι γιατί εκμεταλλεύονται τις κβαντικές ιδιότητες των qubits για να εκτελούν εργασίες πιο αποδοτικά από τους κλασικούς αλγόριθμους, και τρέχουν σε κβαντικούς υπολογιστές. Το κύριο πλεονέκτημα συγκριτικά με τους κλασικούς αλγόριθμους είανι ότι επιλύουν ένα πρόβλημα σε πολυωνιμικό χρόνο και όχι σε εκθετικό, ιδιότητα που τους κάνει πολύ γρήγορους. Μία εφαρμογή τους βρίσκεται στην κρυπτανάλυση, που χρησιμοποιείται για να αποκωδικοποίηση των κρυπτογραφικών μηνυμάτων.

Ένα παράδειγμα αποτελεί ο αλγόριθμος του Shor, ο οποίος αναπτύχθηκε από τον Peter Shor το 1994, και στηρίζεται στην παραγοντοποίηση μεγάλων αριθμών. Είναι αρκετά χρήσιμος στην κβαντική κρυπτογραφία γιατί έχει τη δυνατότητα να παραγοντοποιεί μεγάλους ακέραιους αριθμούς και βασίζεται στην κβαντική μορφή του μετασχηματισμού Fourier. Χρησιμοποιεί την περιοδικότητα που έχουν κάποιες συναρτήσεις και υπολογίζει αποτελεσματικά τους παράγοντες ενός μεγάλου αριθμού, βρίσκοντας την περίοδο μιας εκθετικής συνάρτησης, η οποία σχετίζεται στενά με το πρόβλημα της παραγοντοποίησης ακέραιων αριθμών.

Όσο αφορά στους κλασικούς υπολογιστές, ο πιο χρήσιμος αλγόριθμος που χρησιμοποιείται για την επίλυση της παραγοντοποίησης μεγάλου αριθμού ακέραιων αριθμών είναι ο General Number Filed Sieve. Όμως, στους κβαντικούς υπολογιστές, ο αλγόριθμος του Shor είναι πιο

αποδοτικός καθώς ελαχιστοποιεί το πρόβλημα της παραγοντοποίησης, ανάγοντάς το σε πρόβλημα εύρεσης της περιόδου μιας περιοδικής συνάρτησης.

Με την χρήση της υπέρθεσης, ο αλγόριθμος του Shor μπορεί να επεξεργαστεί ταυτόχρονα πολλές τιμές και να εξάγει τα αποτελέσματα πολύ πιο γρήγορα σε σύγκριση με τους κλασικούς υπολογισμούς.

Παρά την θεωρητικά γρήγορη και αποτελεσματική επεξεργασία του αλγορίθμου του Shor, δεν έχει ακόμη δοκιμαστεί σε κβαντικούς υπολογιστές, τους οποίους σκοπεύουμε να χρησιμοποιήσουμε στο μέλλον, ώστε αυτός ο αλγόριθμος να αποτελέσει απειλή για τα υπάρχοντα κρυπτογραφικά συστήματα.

Συνοψίζοντας, τα qubits είναι ένα θεμελιώδες δομικό στοιχείο της κβαντικής πληροφορίας και των κβαντικών υπολογιστών. Η αξιοποίηση των ιδιοτήτων τους δίνει τη δυνατότητα για την επίλυση πολύπλοκων προβλημάτων σε τομείς όπως η κρυπτογραφία που είναι το κύριο θέμα αυτής της διπλωματικής, η βελτιστοποίηση μεθόδων μετάδοσης της πληροφορίας.

2.3 Κβαντική Κρυπτογραφία

Ένα πολύ ενδιαφέρον κομμάτι της κβαντικής πληροφορίας είναι η κβαντική κρυπτογραφία, η οποία χρησιμοποιεί τις αρχές της κβαντικής μηχανικής (υπέρθεση, διεμπλοκή, αβεβαιότητα Heisenberg), για την δημιουργία καναλίων επικοινωνίας με ασφάλεια. Μέσω αυτών των αρχών γίνεται η κωδικοποίση και αποκωδικοποπίηση της πληροφορίας, με την διανομή κβαντικών κλειδιών (QKD), καθιστώντας αδύνατον την παραβίαση της πηροφορίας.

Ο κύριος στόχος της κβαντικής κρυπτογραφίας είναι η μετάδοση ενός ασφαλούς κελιδιού ανάμεσα σε δύο μέρη, για παράδειγμα την Αλίκη και τον Μπομπ, αποφεύγοντας όσο γίνεται την υποκλοπή από πιθανούς εισβολείς, όπως η Εύα, που θα αναλύσουμε στα επόμενα κεφάλαια.

Η κρυπτογραφία είναι πολύ σημαντική για θέματα που αφορούν κυρίως το στρατό, τις τράπεζες και διάφορες οικονομικές επιχειρήσεις. Έχει τις ρίζες της στην αρχαιότητα, όταν οι Σπαρτιάτες εφεύραν την «σκυτάλη», και με μεγάλο ενδιαφέρον το γνωστό «Enigma» που χρησιμοποιούσαν οι Γερμανοί στον Β΄ Παγκόσμιο Πόλεμο.

Στην κλασική κρυπτογραφία, το επίπεδο ασφάλειας είναι αποδεκτό, όμως υπόκεινται σε υποκλοπές ανάλογα με την υπολογιστική ισχύ που έχει κάποιος. Βασιζέται στην διανομή ενός μυστικού κλειδιού ανάμεσα στην Αλίκη και τον Μπομπ, το οποίο δέχεται υποκλοπές αν κάποιος έχει τα κατάλληλα μέσα, με αποτέλεσμα η κλασική κρυπτογραφία να μην μπορεί να ανταπορκιθεί.

Το ζήτημα αυτό έρχεται να λύσει η κβαντική κρυπτογραφία, η οποία καθιστά πολύ δύσκολη την υποκλοπή του μυστικού κλειδιού που ανταλλάσσουν τα δύο μέρη, βασισμένη στις αρχές της κβαντικής φυσικής.

Στη συνέχεια αυτής της διπλωματικής θα εξηγήσουμε αυτές τις αρχές που διέπουν την κβαντική κρυπτογραφία, τα πρωτόκολλα που ακολουθούνται για τη δημιουργία των κλειδιών και την διαδικασία που ακολουθείται μεταξύ των δύο qubits, της Αλίκης και το Μπομπ.

3. Κβαντική Φυσική Ι

3.1 Εισαγωγή - Ιστορική Αναδρομή

Η κβαντική μηχανική μπορεί να θεωρηθεί ως η μελέτη της φυσικής σε πολύ μικρές κλίμακες μήκους, αν και υπάρχουν επίσης ορισμένα μακροσκοπικά συστήματα στα οποία εφαρμόζεται άμεσα. Η περιγραφή "κβαντική" προκύπτει επειδή, σε αντίθεση με την κλασική μηχανική, ορισμένα μεγέθη παίρνουν μόνο διακριτές τιμές.

Το πρώτο βήμα που οδήγησε στην ανάγκη για δημιουργία μίας νέας θεωρίας, πέρα από τα κλασικά όρια ήταν η ακτινοβολία του μελανού σώματος, ως ένα πρόβλημα που η κλασική φυσική δεν μπορούσε να απαντήσει.

Μέλαν σώμα στην αρχή θεωρείτο αυτό που απορροφά όλο το φως που πέφτει πάνω του ανεξάρτητα από τη γωνία πρόπτωσης και από τη συχνότητα, χωρίς όμως να αντανακλά τίποτε. Στη συνέχεια όμως, η υπόθεση αυτή καταρρίφθηκε καθώς ανακαλύφθηκε ότι τελικά εκπέμπει ηλεκτρομαγνητικό (ΗΜ) κύμα, κυρίως στο υπέρυθρο κομμάτι του ηλεκτρομαγνητικού φάσματος. Αυτή η ακτινοβολία εξαρτάται από τη θερμοκρασία του και μόνο, η οποία ονομάζεται ακτινοβολία μελανού σώματος.

Η μελέτη του μελανού σώματος ήταν το έναυσμα για την ανάπτυξη της κβαντικής φυσικής, καθώς η κλασική φυσική έδινε διαφορετικές προβλέψεις στις φυσικές ποσότητες, σε σύγκριση με τα αποτελέσματα του πειράματος. Τον πρώτο λίθο προς αυτή την κατεύθυνση έβαλε ο Max Planck.

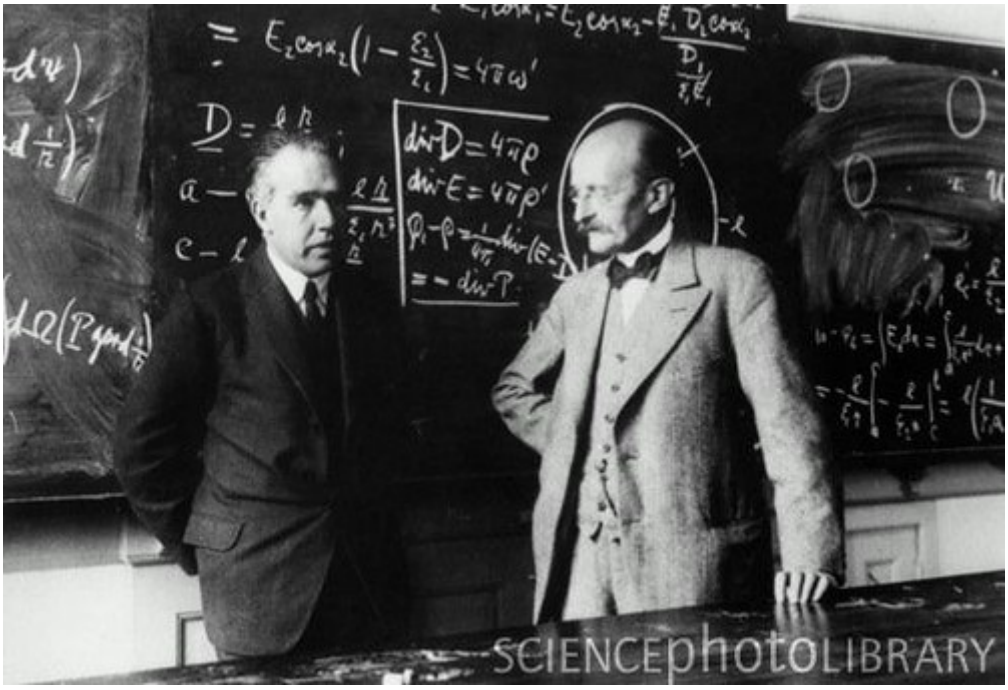
Το 1900, ο Γερμανός φυσικός Max Planck πρότεινε ότι η ενέργεια δεν εκπέμπεται ούτε απορροφάται συνεχώς, αλλά έχει διακριτές τιμές, τις οποίες ονόμασε κβάντα, με την ελάχιστη ενέργεια να είναι $\hbar\omega$ ($\hbar$ σταθερά του Planck). Ο ίδιος τιμήθηκε με το βραβείο Nobel το 1918, για την ανακάλυψη της κβαντικής θεωρίας.

Το 1905, ο Albert Einstein, με την μελέτη του στο φωτοηλεκτρικό φαινόμενο, διατύπωσε ότι τα κβάντα που είχε ορίσει ο Planck, μπορούν να ερμηνευτούν ως σωματίδια, τα οποία ονόμασε φωτόνια. Αυτό στηρίχθηκε στο γεγονός ότι ο Einstein αντιλαμβανόταν ότι δεν υπάρχει σύνδεση ανάμεσα στην κυματική θεωρία του φωτός και την ατομική θεωρία.

Στη συνέχεια, ήταν τα πειράματα του Arthur Compton το 1923, που «σφράγισαν» την έννοια των κβάντων φωτός. Ο Compton μελέτησε την ελαστική σκέδαση των ακτίνων Χ πάνω σε

ηλεκτρόνια και συμπέρανε ότι το μήκος κύματος των σκεδαζόμενων φωτονίων εξαρτάται από τη γωνία σκέδασης, κάτι που δεν μπορούσε να εξηγηθεί με την κλασική θεωρία, παρά μόνο με τα φωτόνια, έχοντας ενέργεια και ορμή.

Ο Niels Bohr, Δανός φυσικός, μελέτησε το άτομο του Υδρογόνου και εξήγησε για ποιο λόγο τα ηλεκτρόνιά του, όπως και των περισσότερων στοιχείων, εξέπεμπαν ακτινοβολία σε συγκεκριμένες διακριτές συχνότητες. Σύμφωνα με αυτό, τα ηλεκτρόνια μπορούν να μεταπηδήσουν από μια τροχιά σε μια άλλη, μόνο αν απορροφήσουν ή εκπέμψουν ένα κβάντο ενέργειας, που αντιστοιχεί στη διαφορά ενέργειας μεταξύ των δύο τροχιών τους.



Εικόνα 3-1: Neils Bohr and Max Planck
(https://www.flickr.com/photos/68906535@N06/6266280399)

Η περαιτέρω σύνδεση της κυματικής και σωματιδιακής φύσης θα έρθει το 1924, με τον Louis de Broglie, ο οποίος θα διατυπώσει ότι τα ηλεκτρόνια, όπως και όλα τα σωματίδια, έχουν κυματικές ιδιότητες. Αυτό επιβεβαιώθηκε πειραματικά το 1927 από τους Davisson και Germer, και ο de Broglie τιμήθηκε με το βραβείο Nobel το 1929.

Όλα τα παραπάνω έστρωσαν το έδαφος για τον Erwin Schrödinger, το 1926, να επινοήσει την περίφημη εξίσωση Schrödinger. Η εξίσωση αυτή δείχνει πώς εξελίσσονται τα κύματα στο

χώρο και στο χρόνο, με τη δράση του διαφορικού τελεστή $i\hbar\frac{\partial}{\partial t}$ και του $-i\hbar\frac{\partial}{\partial x}$ στο κύμα $\psi(t,x) = e^{ikx-i\omega t}$.

Έτσι προκύπτει η εξίσωση:

$$\hbar\frac{\partial\psi(t,x)}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\psi(t,x)}{\partial x^2} \qquad (2)$$

και με δεδομένη τη συνάρτηση της Χαμιλτονιανής δίνει τη χρονοανεξάρτητη εξίσωση Schrödinger σε μία διάσταση για ελεύθερο σωματίδιο με $\psi(t,x) = \varphi_E(x)e^{\frac{-iEt}{\hbar}}$:

$$\left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\varphi_E(x) = E\varphi_E(x) \qquad (3)$$

3.2 Στατιστική ερμηνεία

Ο κυματοσωματιδιακός δυϊσμός της ύλης, που εξηγήσαμε παραπάνω, περιέχει μία θεμελιώδη αντίφαση. Ενώ ένα σωματίδιο είναι ένας εντοπισμένος και αδιαίρετος κόκκος ύλης που κινείται πάνω σε μία καλά καθορισμένη τροχιά, το κύμα από την άλλη, είναι μία εκτεταμένη φυσική διαταραχή που μπορεί να δαιρεθεί μέσω της ανάκλασής του σε κάποιο εμπόδιο.

Η απάντηση έρχεται από τις λύσεις της εξίσωσης Schrödinger, οι οποίες είναι μιγαδικές υποχρεωτικά και επομένως δεν μπορούν να αντιπροσωπεύουν καθαρά μετρήσιμες ποσότητες. Αυτό συνεπάγεται ότι «η κυματοσυνάρτηση δεν αντιπροσωπεύει ένα φυσικά παρατηρήσιμο κλασικό κύμα αλλά ένα κύμα πιθανότητας». (Τραχανάς, 2008)

Έτσι λοιπόν, ορίζεται ο όρος πυκνότητα πιθανότητας, που είναι το τετράγωνο της απόλυτης τιμής της κυματοσυνάρτησης και την πιθανότητα ανά μονάδα μήκους/όγκου να βρούμε το σωματίδιο σε μία περιοχή του χώρου:

$$P(x) = |\psi(x)|^2 \qquad (4)$$

Έτσι, η πυκνότητα σε ένα χώρο μεταξύ του x και x+dx:

$$\int_{-\infty}^{\infty} P(x)dx = \int_{-\infty}^{\infty}|\psi(x)|^2 dx \qquad (5)$$

Με ολική πιθανότητα:

$$\int_{-\infty}^{\infty}|\psi(x)|^2 dx = 1 \quad (6)$$

η οποία αποτελεί τη συνθήκη κανονικοποίησης, με $\int_{-\infty}^{\infty}|\psi(x)|^2 dx < \infty$, δηλαδή το ολοκλήρωμα πρέπει να συγκλίνει.

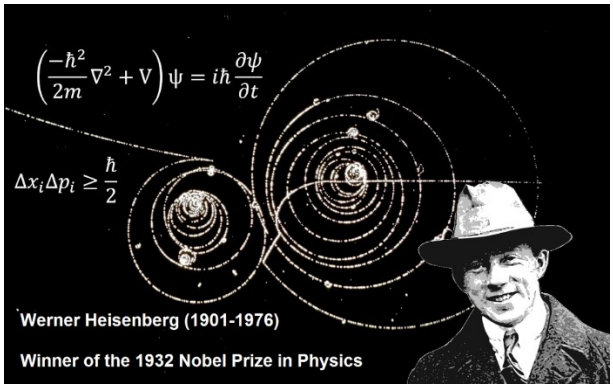
Αυτή η ιδιότητα δίνει τον όρο «τετραγωνικά ολοκληρώσιμη» συνάρτηση και είναι η προϋπόθεση ώστε μία κυματοσυνάρτηση να περιγράφει μία πραγματοποιήσιμη φυσική κατάσταση του σωματιδίου.

Με τη στατιστική ερμηνεία που εξηγήσαμε η αντίφαση που αναφέραμε στην αρχή εξαφανίζεται και το σωματίδιο μπορεί να «διαχυθεί» στον χώρο, κρατώντας τη σωματιδιακή του φύση.

3.3 Αρχή Αβεβαιότητα Heisenberg

Με τη στατιστική ερμηνεία εξηγήσαμε ότι η αντίφαση, που αναφέραμε στην αρχή, εξαφανίζεται και το σωματίδιο μπορεί να «διαχυθεί» στον χώρο, κρατώντας τη σωματιδιακή του φύση.

Η αρχή της αβεβαιότητας του Heisenberg θεωρείται ότι είναι η καρδιά του κβαντομηχανικού φορμαλισμού. Αποτελεί μία μαθηματική συνέπεια του κυματοσωματιδιακού δυϊσμού και είναι μία από τις μεγαλύτερες ανακαλύψεις του 20ου αιώνα. Ένα από τα βασικά της αποτελέσματα είναι ότι δεν μπορούμε να μιλάμε για την "κλασική" τροχιά ενός σωματιδίου, αλλά αντίθετα, μπορούμε να περιγράφουμε μόνο την πιθανότητα να βρεθεί το σωματίδιο σε μια συγκεκριμένη θέση ή να έχει μια συγκεκριμένη ορμή.



Εικόνα 3-2: Werner Heisenberg

(https://medium.com/thedialogues/what-is-heisenbergs-uncertainty-principle-7d8b44e39b07)

Είναι μία μαθηματική ανισότητα, η οποία εφαρμόζεται για δύο καλά καθορισμένες ποσότητες (προσδιορίζονται μονοσήμαντα από την κυματοσυνάρτηση) και δείχνει ότι οποιαδήποτε κυματοσυνάρτηση περιγράφει την κατάσταση ενός συστήματος θα έχει το γινόμενο των αβεβαιοτήτων θέσης-ορμής μεγαλύτερο ή ίσο με το ήμισυ της σταθεράς του Planck.

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \quad (7)$$

Η αρχή αβεβαιότητας δηλώνει ότι υπάρχει ένα θεμελιώδες όριο στην ακρίβεια με την οποία μπορούν να μετρηθούν ταυτόχρονα ορισμένα ζεύγη φυσικών μεγεθών, όπως η θέση και η ορμή ενός σωματιδίου. Όμως η αρχή αυτή ισχύει και για άλλα ζεύγη μετρήσεων που σχετίζονται με κβαντικά συστήματα, όπως η ενέργεια και ο χρόνος.

$$\Delta E \cdot \Delta t \cong \hbar \quad (8)$$

Αυτό που πρέπει να αναφερθεί σε αυτή την μορφή της αβεβαιότητας είναι ότι ο χρόνος δεν είναι ένα δυναμικό μέγεθος, αλλά μία εξωτερική παράμετρος ως προς το σύστημα και δεν υπάρχει αντίστοιχος τελεστής για αυτό το μέγεθος, όπως για παράδειγμα ο τελεστής για τη θέση.

Σε αντίθεση με τη θέση και την ορμή, ο χρόνος δεν είναι ένας παρατηρήσιμος στη κβαντική μηχανική, αλλά μια παράμετρος που περιγράφει την εξέλιξη του συστήματος. Η αβεβαιότητα χρόνου σχετίζεται με τη διάρκεια της διαδικασίας παρατήρησης/αλληλεπίδρασης και όχι με μια μέτρηση του χρόνου.

Η αβεβαιότητα ανάμεσα στο χρόνο και την ενέργεια δηλώνει ότι όσο πιο αργά μεταβάλλεται ένα φυσικό σύστημα, τόσο πιο καλά καθορισμένη είναι η ενέργειά του, και αντιστρόφως.

3.4 Ο ρόλος της μέτρησης

Ο ρόλος της μέτρησης σε ένα κβαντικό σύστημα είναι θεμελιώδης και σημαντικός για την κατανόηση της κβαντικής φυσικής. Η διαδικασία της μέτρησης σε ένα κβαντικό σύστημα είναι διαφορετική από την κλασική φυσική και αποτελεί το κρίσιμο σημείο διαφόρων παραδόξων και ερμηνειών της κβαντικής θεωρίας.

Όπως εξηγήσαμε, η κατάσταση ενός συστήματος περιγράφεται από μια κυματοσυνάρτηση ψ, η οποία περιέχει όλες τις πιθανές καταστάσεις για το σύστημα. Η κυματοσυνάρτηση εξελίσσεται σύμφωνα την εξίσωση Schrödinger και περιγράφει στην ουσία μια υπέρθεση καταστάσεων, όπου το σύστημα μπορεί να βρίσκεται σε πολλαπλές καταστάσεις ταυτόχρονα.

$$\psi = \sum_n c_n \psi_n \qquad (9)$$

Με πιθανότητα εμφάνισης καθεμίας:

$$P_n = |c_n|^2 \qquad (10)$$

Κατά τη μέτρηση, η κυματοσυνάρτηση «καταρρέει» σε μια από τις δυνατές ιδιοκαταστάσεις που μετράμε. Αυτό σημαίνει ότι η μέτρηση προκαλεί μια διακοπή της εξέλιξης της κυματοσυνάρτησης και το σύστημα βρίσκεται σε μια συγκεκριμένη κατάσταση μετά τη μέτρηση.

Η αρχή της αβεβαιότητας του Heisenberg, όπως εξηγήσαμε προηγουμένως, εξηγεί ότι δεν μπορούμε να μετρήσουμε ταυτόχρονα ζεύγη φυσικών μεγεθών με ακρίβεια. Η μέτρηση ενός μεγέθους επηρεάζει την ακρίβεια με την οποία μπορούμε να μετρήσουμε το άλλο μέγεθος.

Η μέτρηση έχει επιπτώσεις και σε μία άλλη κβαντική ιδιότητα, που θα αναλύσουμε στα επόμενα κεφάλαια, την κβαντική διεμπλοκή. Σε ένα διεπλεγμένο σύστημα, η μέτρηση σε ένα από τα σωματίδια, που βρίσκονται σε αυτό φαίνεται να επηρεάζει την κατάσταση του άλλου, ακόμα και όταν βρίσκονται σε μεγάλες αποστάσεις. Αυτό το φαινόμενο, στην αρχή είχε εγείρει πολλές αντιδράσεις για το πόσο η κβαντική φυσική μπορεί να υπάρξει ως ενιαία θεωρία, αλλά

έχει επιβεβαιωθεί πειραματικά και προκαλεί παράδοξες καταστάσεις που έρχονται σε αντίθεση με την κλασική έννοια της τοπικότητας.

Η μέτρηση σε ένα κλασικό σύστημα δεν επηρεάζει το ίδιο το σύστημα, και αν το κάνει η επίδραση μπορεί να μετρηθεί και να διορθωθεί το αποτέλεσμα της. Αντίθετα, στην κβαντική φυσική παίζει κρίσιμο ρόλο και επηρεάζει άμεσα την κατάσταση του συστήματος. Η κατάρρευση της κυματοσυνάρτησης, η αβεβαιότητα, και οι κβαντικές συσχετίσεις είναι θεμελιώδη χαρακτηριστικά που προκύπτουν από τη διαδικασία της μέτρησης.

Η επίδραση της μέτρησης πάνω στο κβαντικό σύστημα θα είναι πάντα της μορφής:

$$\psi = (\sum_n c_n \psi_n) \longrightarrow \psi_n \qquad (11)$$

χωρίς να μπορούμε να προβλέψουμε ποια από τις ιδιοσυναρτήσεις ψ_n θα επιλεγεί και ποιο αποτέλεσμα θα πάρουμε.

4. Κβαντική Φυσική ΙΙ

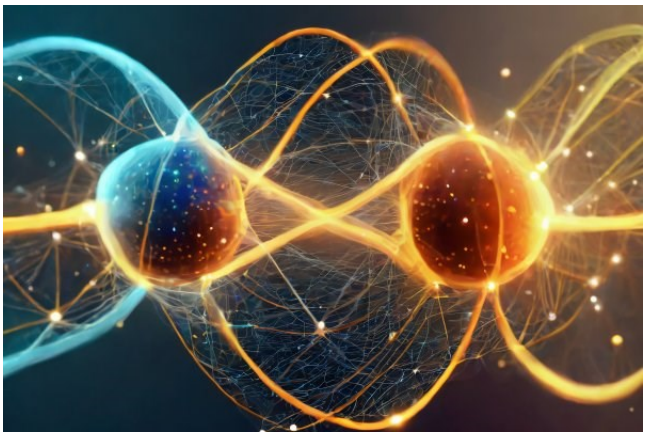
Οι αρχές που διέπουν τη κβαντική πληροφορία, στηρίζονται στις διαδικασίες που περιλαμβάνουν τη διαχείριση διεμπλοκών μεταξύ αντικειμένων σε μεγάλες μεταξύ τους αποστάσεις. Για να εξάγουμε και να μελετήσουμε το αποτέλεσμα από μια διαδικασία μετάδοσης της κβαντικής πληροφορίας, πρέπει να παρατηρήσουμε ή να μετρήσουμε το σύστημα, το οποίο αναπόφευκτα αλλάζει, καταστρέφοντας την υπέρθεση, στην οποία βασίζεται όλη η διαδικασία.

Το βασικό χαρακτηριστικό για την επιστήμη της κβαντικής πληροφορίας είναι η κατανόηση ότι δύο ή περισσότερα κβαντικά συστήματα μπορούν να έχουν καταστάσεις που να είναι διαπλεγμένες. Οι ιδιότητες αυτών των καταστάσεων θέτουν τα θεμέλια για τις διάφορες πτυχές της κβαντικής πληροφορίας, όπως η κβαντική κρυπτογραφία, η οποία μελετάται σε αυτήν την ενότητα.

4.1 Κβαντική Διεμπλοκή – Entanglement

4.1.1 Ιστορική Αναδρομή

Η κβαντική διεμπλοκή είναι ένα φαινόμενο στην κβαντική φυσική, στο οποίο στηρίζεται η μετάδοση της κβαντικής πληροφορίας και η κβαντική κρυπτογραφία. Συνδέεται με την αρχή της υπέρθεσης, όταν αυτή εφαρμόζεται σε συστήματα με περισσότερα από ένα σωματίδια.



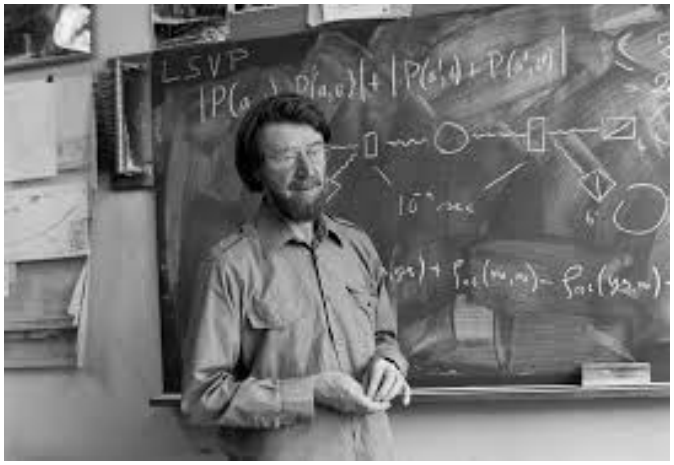
Εικόνα 4-1: Κβαντική Διεμπλοκή δύο φωτονίων
(https://icc.ub.edu/news/entanglement-key-a-better-understanding-quantum-field-theories)

Η κβαντική διεμπλοκή έχει τις ρίζες της στο EPR παράδοξο στο οποίο δυο κβαντικά συστήματα έρχονται σε αλληλεπίδραση και μετά απομακρύνονται, και παρά τις μεγάλες αποστάσεις που μπορεί να έχουν μεταξύ τους, φαίνεται ότι το ένα σύστημα δεν είναι ανεξάρτητο του άλλου. Το EPR φαινόμενο είναι γνωστό από τα αρχικά των Einstein, Podolsky, Rosen, οι οποίοι ήταν οι πρώτοι που εισάγαγαν αυτό τον όρο. Άλλοι σπουδαίοι φυσικοί που άνοιξαν τη συζήτηση για την διεμπλοκή ήταν ο Schrodinger, ο Bohr και ο von Neumann, ο οποίος περιέγραψε τη διαδικασία της μέτρησης κβαντικών συστημάτων. Ο Schrödinger είχε εντυπωσιαστεί πολύ από την διεμπλοκή, χαρακτηρίζοντάς την ως το κύριο χαρακτηριστικό της κβαντομηχανικής, σε μια εργασία του του 1935.

Εικόνα 4-2: Erwin Schrödinger
(https://physicsworld.com/a/quantum-theory-and-the-nobel-prize/)

Ακόμα, διερευνήθηκε θεωρητικά από τον John Bell το 1964, ο οποίος έδωσε έμφαση στην ουσιώδη διαφορά ανάμεσα στις κβαντικές και τις κλασικές πιθανότητες των καταστάσεων. Τέλος, επιβεβαιώθηκε, μέσα από πειραματικούς υπολογισμούς, ότι τα διεπλεγμένα κβαντικά συστήματα παρουσιάζουν τέτοια συμπεριφορά, η οποία είναι αδύνατη στον κλασικό κόσμο, απονέμοντας το Nobel σε σημαντικούς επιστήμονες, όπως θα δούμε παρακάτω.

Στις αρχές της δεκαετίας του 1990, η ιδέα της διεμπλοκής έγειρε ερωτήματα όσο αφορά στο αν θα μπορούσε να φανεί χρήσιμη ως νέα πηγή επίλυσης προβλημάτων επεξεργασίας πληροφορίας. Η απάντηση ήρθε το 1991 από τον Artur K. Ekert του πανεπιστημίου του Cambridge, ο οποίος έδειξε πώς να χρησιμοποιήσουμε τη διεμπλοκή για να διαμοιράσουμε κρυπτογραφικά κλειδιά που δεν μπορούν να υποκλαπούν. (Ekert, 1991)



Εικόνα 4-3: Stephen Wiesner
(https://cds.cern.ch/record/969985)

Λίγο αργότερα, το 1992, ο Charles H. Bennett στην IBM και ο Stephen Wiesner του πανεπιστημίου του Tel Aviv, έδειξαν πώς η διεμπλοκή θα μπορούσε να βοηθήσει στην αποστολή κλασικής πληροφορίας από ένα τόπο σ' έναν άλλο. (Bennett, Wiesner, 1992)

4.1.2 Θεωρία Κβαντικής Διεμπλοκής

Το φαινόμενο της διεμπλοκής είναι πολύ σημαντικό στο πεδίο της κβαντικής πληροφορίας διότι μπορεί να επιτρέψει να γίνουν πολύπλοκοι υπολογισμοί με τη χρήση μεγάλου πλήθους κβαντικών συστημάτων και σε συνδυασμό με τους αλγόριθμους παραγοντοποίησης του Shor και του Grover θα μπορούσαν να ενισχύσουν την υπολογιστική ισχύ των κβαντικών υπολογιστών.

Η κβαντική πληροφορία χρησιμοποιεί το φαινόμενο διεμπλοκής μόνο μεταξύ δύο ή τριών σωματιδίων, και συγκεκριμένα για την μέγιστη διεμπλοκή τους, διότι τέτοια μικρά συστήματα διεμπλοκής φτάνουν για να πάρουμε ισχυρές μεθόδους επικοινωνίας (κβαντική κρυπτογραφία, κβαντική κωδικοποίηση και κβαντική μεταφορά πληροφορίας). Ένας ακόμη λόγος είναι ότι ο μεγάλος αριθμός των κβαντικών καταστάσεων αυξάνει την πολυπλοκότητα για τον έλεγχο των qubits με την υπολογιστική ισχύ που διαθέτουμε μέχρι τώρα. Πέρα όμως από το πεδίο της

κβαντικής επικοινωνίας, το φαινόμενο της διεμπλοκής παρατηρείται και σε περισσότερα από δύο σωματίδια, ακόμα και για καταστάσεις που δεν προβλέπεται η μέγιστη συσχέτισή τους.

Εικόνα 4-4: Κβαντική κωδικοποίηση
(https://www.nist.gov/blogs/manufacturing-innovation-blog/supporting-digital-transformation-legacy-components)

Η βασική ιδιότητα της κβαντικής διεμπλοκής στηρίζεται στην υπέρθεση. Σε ένα κβαντικό σύστημα, έστω ότι υπάρχουν δύο βασικές καταστάσεις, ορθογώνιες μεταξύ τους, |0> και |1> με αποτέλεσμα το σύστημα να μπορεί να βρεθεί σε οποιαδήποτε κατάσταση που προκύπτει από την υπέρθεση αυτών των δύο (Alber, Beth, Horodeckis, Rotteler, Weinfurter, Werner & Zeilinger, 2001):

$$|\psi >= \frac{1}{\sqrt{2}}(|0> + |1>) \qquad (12)$$

Για παράδειγμα θα πάρουμε την κατάσταση διεμπλοκής για κβαντικά συστήματα δύο ίσων καταστάσεων:

$$|\Psi >= \frac{1}{\sqrt{2}}(|0>_1 |0>_2 + |1>_1 |1>_2) \qquad (13)$$

Συγκεκριμένα, λοιπόν, στην κβαντική επικοινωνία μας ενδιαφέρουν οι ιδιότητες και οι καταστάσεις που προκύπτουν από την μέγιστη διεμπλοκή δύο σωματιδίων, δηλαδή όταν η κατάσταση ένος συστήματος εξαρτάται πλήρως από την κατάσταση του άλλου. Η μέγιστη διεμπλοκή περιγράφεται από τέσσερις ορθογώνιες καταστάσεις, οι οποίες ονομάζονται καταστάσεις Bell ή EPR ζεύγη, και παραβιάζουν τις ανισότητες του Bell με μέγιστο τρόπο (θα αναλύσουμε στα επόμενα κεφάλαια αυτής της διπλωματικής):

$$|\Psi^+>_{12}=\frac{1}{\sqrt{2}}(|0>_1|1>_2+|1>_1|0>_2) \quad (14)$$

$$|\Psi^->_{12}=\frac{1}{\sqrt{2}}(|0>_1|1>_2-|1>_1|0>_2) \quad (15)$$

$$|\Phi^+>_{12}=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \quad (16)$$

$$|\Phi^->_{12}=\frac{1}{\sqrt{2}}(|0>_1|0>_2-|1>_1|1>_2) \quad (17)$$

Οι ανισότητες του Bell προέρχονται από το πεδίο των τοπικών ρεαλιστικών θεωριών, και στα πλαίσια της κβαντικής φυσικής, δίνουν πρόβλεψη για τις καταστάσεις των σωματιδίων, τα οποία δεν είναι διεπλεγμένα, αφού μπορούν να εκφραστούν από το τανυστικό γινόμενων των χώρων Hilbert του καθενός. Όσο αφορά όμως στη διεμπλοκή, τα αποτελέσματα είναι διαφορετικά, λόγω του γεγονότος ότι η κατάσταση διεμπλοκής δεν προέρχεται από το τανυστικό γινόμενο, και τα σωματίδια δεν μπορούν να θεωρηθούν ανεξάρτητα, παραβιάζοντας τις ανισότητες του Bell. Αυτό σημαίνει ότι αν προσπαθήσουμε να μετρήσουμε το ένα, τότε θα αλλάξουν οι προβλέψεις για τις μετρήσεις του άλλου.

Ειδικότερα, αν κάποιος εστιάσει μόνο στο ένα από τα δύο σωματίδια, το μόνο που μπορεί να γνωρίζει είναι η ίση πιθανότητα να το βρεί στην κατάσταση |0> ή |1>, χωρίς να έχει περισσότερη πληροφορία για το αποτέλεσμα της μέτρησης. Από την άλλη η μέτρηση σε ένα από τα δύο σωματίδια καθορίζει την μέτρηση για το άλλο. Παρατηρώντας όμως το ένα σωματίδιο, καθορίζεται η μέτρηση για το άλλο, όπως αναφέραμε παραπάνω.

Στην περίπτωση διεμπλοκής δύο φωτονίων (τα οποία ενδιαφέρουν την συγκεκριμένη διπλωματική εργασία), που είναι πολωμένα σε κάθετες καταστάσεις μεταξύ τους, και βρίσκονται στην κατάστηση $|\Psi^->_{12}$, αν μετρήσουμε το ένα κατακόρυφα τότε το άλλο θα ξέρουμε ότι θα είναι σε οριζόντια πόλωση. Αντίστοιχα θα συμβεί για την κυκλική πόλωση του πρώτου αριστερά και του δεύτερου φωτονίου δεξιά.

Συνοψίζοντας, υπάρχουν τρεις βασικές ιδιότητες οι οποίες οφείλονται στην κβαντική διεμπλοκή και διαχωρίζουν την κβαντική επικοινωνία από την κλασική. Πρώτον, προκύπτουν διαφορετικά στατιστικά αποτελέσματα στις μετρήσεις διεπλεγμένων σωματιδίων και μη. Δεύτερον, παρά το γεγονός ότι τα αποτελέσματα των μετρήσεων για κάθε φωτόνιο είναι τυχαία, υπάρχουν πολύ καλοί συσχετισμοί στις παρατηρήσεις του ζεύγους αυτών. Και τρίτον, «πειράζοντας» την κατάσταση Bell ενός μόνο από τα δύο σωματίδια μεταβαίνουμε πάλι σε κατάσταση Bell, αλλά και πάλι θα παραβιάζονται οι ανισότητες .

4.2 No-cloning Θεώρημα

Στην κλασική φυσική ένα σύστημα μπορεί να αντιγραφεί με μεγάλη ακρίβεια χωρίς να καταστραφεί το πρωτότυπο. Αυτό όμως δεν ισχύει όταν αναφερόμαστε σε κβαντικά συστήματα.

Έστω ότι έχουμε ένα κβαντικό σύστημα στην κατάσταση $|\psi>$ σε ένα χώρο Hilbert H, και θέλουμε να το αντιγράψουμε. Θεωρούμε ότι υπάρχει ένα ίδιο κβαντικό σύστημα που βρίσκεται σε κατάσταση $|\varphi>$, σε έναν ίδιο χώρο Hilbert και υπάρχει ένας τελεστής $\hat{U}$ που δρα πάνω στο χώρο $\mathcal{H}\otimes\mathcal{H}$. (Αναστόπουλος, 2023)

Το τανυστικό γινόμενο θα δώσει:

$$\hat{U}(|\psi>\otimes|\varphi>) = |\psi>\otimes|\psi> \quad (18)$$

Αν για οποιαδήποτε κατάσταση $|\psi>$, πάρουμε δύο καταστάσεις $|\rho_1>$, $|\rho_2>$ τότε η παραπάνω σχέση θα γίνει:

$$\hat{U}(|\rho_{1,2}>\otimes|\varphi>) = |\rho_{1,2}>\otimes|\rho_{1,2}> \quad (19)$$

Χρησιμοποιώντας το εσωτερικό γινόμενο και στα δύο μέλη προκύπτει:

$$<\rho_1|\rho_2> = (<\rho_1|\rho_2>)^2 \quad (20)$$

το οποίο δίνει:

$$\begin{cases} <\rho_1|\rho_2> = 0 \\ <\rho_1|\rho_2> = 1 \end{cases} \quad (21)$$

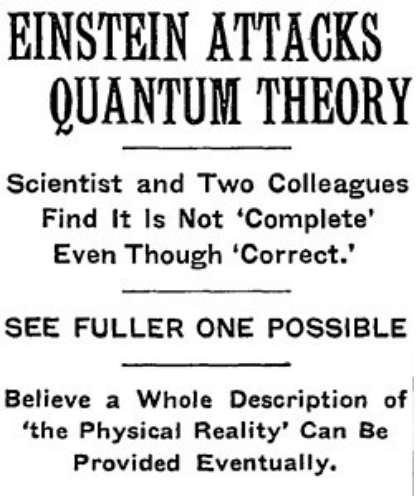
Οι τελευταίες σχέσεις δείχνουν ότι οι καταστάσεις είναι ορθοκανονικές, το οποίο δεν μπορεί να ισχύει για τυχαίες καταστάσεις, καταλήγοντας ότι δεν μπορεί να γίνει η αντιγραφή.

4.3 Ανισότητες Bell

4.3.1 Παράδοξο EPR

Το 1935 οι Einstein-Podolsky-Rosen διατύπωσαν το περίφημο παράδοξο EPR και «κατασκεύασαν» ένα νοητό πείραμα για να καταρρίψουν την κβαντομηχανική ερμηνεία του κόσμου. Αυτό στηρίχθηκε στις αντιρρήσεις, κυρίως του Einstein, ο οποίος θεωρούσε πως

οποιοδήποτε σύστημα έχει ιδιότητες πριν ακόμη το μετρήσουμε (η βασική αρχή του ρεαλισμού). Στο πείραμα αυτό, εξέτασαν ένα ζευγάρι διεπλεγμένων σωματιδίων και υποστήριξαν ότι με τη μέτρηση της θέσης ή της ορμής του ενός, οι ιδιότητες του άλλου θα μπορούσαν να γίνουν άμεσα γνωστές, χωρίς να μετρηθεί. Αυτό φαινόταν να οδηγεί στο συμπέρασμα ότι η πληροφορία μεταδιδόταν ταχύτερα από το φως, κάτι που ερχόταν σε σύγκρουση με τη θεωρία της σχετικότητας.



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Εικόνα 4-5: Επικεφαλίδα σε άρθρο για την εργασία πάνω στο EPR τον Μάιο του 1935 στην The New York Times

(https://medium.com/@bent_99096/toe-theory-of-everything-9376b27eddc6)

Εικόνα 4-6: Albert Einstein, Boris Podolsky, Nathan Rosen (EPR Paradox)

(https://medium.com/@jasvir/conways-proof-of-free-will-2aa2ac168dda)

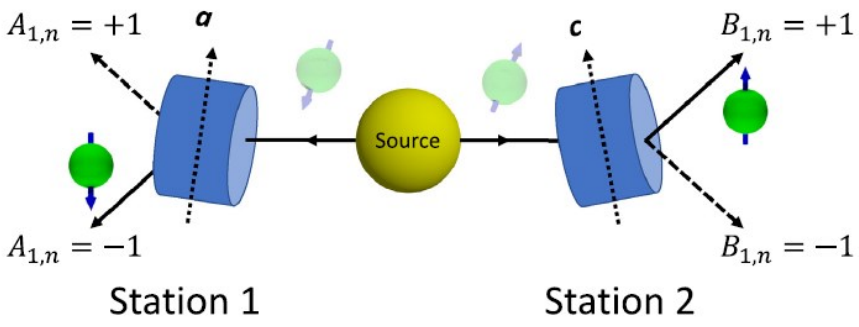
Στη συνέχεια ο Bohm, στηρίχτηκε στην υπόθεση ότι ένα σωματίδιο με spin μηδέν, αν διασπαστεί σε δυο σωματίδια, υποχρεωτικά θα έχουν συνολικό spin μηδέν, λόγω των νόμων διατήρησης. Αυτό συνεπάγεται ότι αν το ένα σωματίδιο έχει spin «πάνω» ως προς μια τυχούσα

κατεύθυνση, τότε υποχρεωτικά το spin του δεύτερου σωματιδίου θα είναι «κάτω». Έδωσε τη δική του περιγραφή με ένα πείραμα, έχοντας μία πηγή που εκπέμπει ηλεκτρόνια σε ζεύγη και τα σωματίδια που προκύπτουν έχουν αντίθετα spin ½, το ένα με πορεία προς τα αριστερά και το άλλο προς τα δεξιά, αλλά πάντα διατηρώντας το συνολικό spin μηδέν. Η κυματοσυνάρτηση του συστήματος θα μπορούσε να γραφτεί ως:

$$|\Psi^- >_{AB} = \frac{1}{\sqrt{2}}(|\downarrow>_A |\uparrow>_B - |\uparrow>_A |\downarrow>_B \quad (22)$$

όπου $|\downarrow>$ και $|\uparrow>$ είναι οι ιδιοκαταστάσεις της προβολής του spin στον άξονα z και αυτή η διεπλεγμένη κατάσταση ονομάζεται κατάσταση Bell.

Με την παραπάνω διαδικασία τα δύο ηλεκτρόνια απομακρύνονται χωρικά και σε κάποια απόσταση μετρούμε την κατεύθυνση του spin του σωματιδίου με μία διάταξη Stern-Gerlach. Αν μετρήσουμε το spin του ενός τότε, αυτομάτως γνωρίζουμε και το spin του άλλου χωρίς να πρέπει να την μετρήσουμε. Αυτό έγειρε αντιρρήσεις από τον Einstein, ο οποίος δεν μπορούσε να δεχθεί την ακαριαία μετάδοση της πληροφορίας μεταξύ των δύο ηλεκτρονίων, η οποία θα παραβίαζε τη σχετικότητα, αφού τίποτε δεν μπορεί να διαδοθεί με ταχύτητα μεγαλύτερη του φωτός.



Εικόνα 4-7 Αναπαράσταση του πειράματος σκέψης Einstein-Podolsky-Rosen στην τροποποιημένη μορφή που προτείνεται από τον Bohm

(De Raedt, Katsnelson, Jattana, Mehta, Willsch, Willsch, Michielsen, & Jin 2023)

Το παράδοξο EPR ανάγεται στο κεντρικό παράδοξο της κβαντομηχανικής που είναι το αξίωμα της μέτρησης, δηλαδή η στιγμιαία κατάρρευση της κυματοσυνάρτησης.

Σύμφωνα με την κβαντομηχανική, κάθε φυσικό σύστημα εκφράζεται μέσω μίας κυματοσυνάρτησης και πριν να το μετρήσουμε βρίσκεται σε μία κατάσταση υπέρθεσης ιδιοκαταστάεων, χωρίς να γνωρίζουμε και χωρίς να έχει νοήμα να ρωτήσουμε σε ποια

ιδιοκατάσταση υπέρθεσης βρίσκεται πριν την μέτρηση. Τη στιγμή της μέτρησης, η κυματοσυνάρτηση «καταρρέει», και αποκαλύπτεται η φύση και η ταυτότητά του, με το σύστημα να έρχεται σε μία φάση «αποσύνδεσης», με αποτέλεσμα την φανέρωσή του στο φυσικό, πραγματικό κόσμο.

Έτσι, τα δύο ηλεκτρόνια βρίσκονται σε μία κατάσταση υπέρθεσης πριν την μέτρησή τους, και η κυματοσυνάρτηση δίνεται από τη σχέση:

$$\psi = \frac{1}{\sqrt{2}}(\psi_+(1)\psi_-(2) + \psi_-(1)\psi_+(2)) \qquad (23)$$

Τη στιγμή της μέτρησης η κυματοσυνάρτηση «καταρρέει», οδηγώντας στο γεγονός ότι με την μέτρηση του spin του ηλεκτρονίου, ταυτόχρονα γίνεται και η "επιλογή" της τιμής του spin του δεύτερου. Αυτό συμβαίνει διότι τα σωματίδια 1 και 2 δεν είναι ξεχωριστές οντότητες αλλά συμμετέχουν στην ολική κυματοσυνάρτηση. Συνεπώς, αν μετρήσουμε πρώτα την τιμή του 1 τότε η κυματοσυνάρτηση παίρνει την μορφή : $\psi_+(1)\psi_-(2)$.

4.3.2 Θεώρημα Bell – Ανισότητες

Το θεώρημα Bell διατυπώθηκε το 1964 και αναφέρεται σε μία οικογένεια αποτελεσμάτων, τα οποία προέρχονται από κατανομές πιθανοτήτων μέσα από εκτιμήσεις τοπικής αιτιότητας, μαζί με τις προβλέψεις υποθέσεων για τα αποτελέσματα χωρικά διαχωρισμένων πειραμάτων που συγκρούονται με τις κβαντομηχανικές προβλέψεις. Αυτές οι πιθανολογικές προβλέψεις αναπαριστώνται με την μορφή ανισοτήτων, οι ανισότητες του Bell, που πρέπει να ικανοποιούνται από την κλασική θεωρία, αλλά παραβιάζονται, υπό ορισμένες συνθήκες, από συσχετίσεις που υπολογίζονται μέσω της κβαντομηχανικής.

Αυτό το θεώρημα δείχνει ότι καμία θεωρία που να ικανοποιεί τις τοπικές ρεαλιστικές θεωρίες που επιβάλλονται στο πρίσμα της κλασικής φυσικής, δεν μπορεί να αναπαράγει τις πιθανολογικές προβλέψεις της κβαντικής μηχανικής υπό οποιεσδήποτε συνθήκες.

Οι κύριες συνθήκες που χρησιμοποιούνται για την εξαγωγή των ανισοτήτων Bell είναι η συνθήκη της τοπικότητας, που αποτελεί τον συσχετισμό μεταξύ απομακρυσμένων γεγονότων, και του ρεαλισμού. Η τοπικότητα διατυπώνει ότι ένα σύστημα μπορεί να επηρεαστεί μόνο από το άμεσο περιβάλλον του και οποιαδήποτε αντίδραση δεν μπορεί να ταξιδέψει με ταχύτητα μεγαλύτερη από του φωτός. Ο ρεαλισμός στηρίζεται στο γεγονός ότι τα αντικείμενα έχουν συγκεκριμένες ιδιότητες, ακόμα και πριν να μετρηθούν/παρατηρηθούν.

Ξεκινώντας από τη δεκαετία του 1970, υπήρξε μία σειρά πειραμάτων για να ελεγχθεί εάν οι ανισότητες Bell ικανοποιούνται. Με ελάχιστες εξαιρέσεις, τα αποτελέσματα αυτών των πειραμάτων έχουν επιβεβαιώσει τις κβαντομηχανικές προβλέψεις, παραβιάζοντας τις σχετικές ανισότητες Bell. Πριν από το 2015, ωστόσο, αυτά τα πειράματα ήταν ευάλωτα σε τουλάχιστον ένα από του δύο πυλώνες, που αναφέρονται ως κενό επικοινωνίας ή τοπικότητας.

Το 2015, πραγματοποιήθηκαν πειράματα που έδειξαν παραβίαση των ανισοτήτων Bell. Στη συνέχεια, η στάση της κοινότητας της φυσικής ως προς τη σημασία του θεωρήματος του Bell άλλαξε δραματικά με την απονομή του Βραβείου Νόμπελ Φυσικής για το 2022 στους Alain Aspect, John Clauser και Anton Zeilinger για «πειράματα με διεπλεγμένα φωτόνια, που αποδεικνύουν την παραβίαση των ανισοτήτων Bell και την πρωτοποριακή επιστήμη της κβαντικής πληροφορίας».

4.3.3 Απόδειξη Ανισοτήτων του Bell

Ξεκινώντας από τις υποθέσεις για το παράδοξο EPR, θέλουμε να βρούμε και να εξηγήσουμε τον συσχετισμό των πολώσεων για δύο φωτόνια, και να εξηγήσουμε τις συσχετίσεις πόλωσης μεταξύ δύο ζεύγων, χρησιμοποιώντας δύο μετρικές μηχανές A και B σε κάποια απόσταση μεταξύ τους.

Εισάγεται η παράμετρος λ που είναι τυχαία μεταβλητή, κοινή και στα δύο φωτόνια του ζεύγους, και αλλάζει τυχαία από το ένα ζευγάρι στο άλλο. Η πυκνότητα πιθανότητας της παραμέτρου είναι (Grynberg, Aspect & Fabre, 2010) :

$$\rho(\lambda) \geq 0 \text{ και } \int d\lambda\, \rho(\lambda) = 1 \quad (24)$$

Έστω οι μετρήσεις πόλωσης 1 και 2 στα φωτόνια με την παράμετρο λ, που ορίζονται από τις συναρτήσεις A(λ, a) και B(λ, b), οι οποίες μπορούν να πάρουν μόνο τις τιμές +1 ή −1, έτσι:

$$|A(\lambda, a)| = |B(\lambda, b)| = 1 \quad (25)$$

Για κάθε πολωμένη μέτρηση ισχύει:

$$\int d\lambda\, \rho(\lambda) A(\lambda, a) = \int d\lambda\, \rho(\lambda) B(\lambda, b) = 0 \quad (26)$$

Συνεπώς ο συσχετισμός των πολώσεων:

$$ELHVT(a, b) = \overline{A(\lambda, a) \cdot B(\lambda, b)} = \int d\lambda\, \rho(\lambda) A(\lambda, a) B(\lambda, b) \quad (27)$$

Στη συνέχεια, ορίζουμε την ποσότητα:

$$s(\lambda, a, a', b, b') = A(\lambda, a)B(\lambda, b) - A(\lambda, a)B(\lambda, b') + A(\lambda, a')B(\lambda, b) + A(\lambda, a')B(\lambda, b') \Rightarrow$$
$$s(\lambda, a, a', b, b') = A(\lambda, a)(B(\lambda, b) - B(\lambda, b')) + A(\lambda, a')(B(\lambda, b) + B(\lambda, b')) \quad (28)$$

Από την **(25)** και **(28)**:

$$s(\lambda, a, a', b, b') = \pm 2 \quad (29)$$

Ολοκληρώνοντας την τελευταία σχέση:

$$-2 \leq \int d\lambda\, \rho(\lambda)\, s(\lambda, a, a', b, b') \leq +2 \quad (30)$$

Τότε από την **(27)**:

$$-2 \leq S(\lambda, a, a', b, b') \leq +2 \quad (31)$$

με S:

$$S = E(a, b) - E(a, b') + E(a', b) + E(a', b') \quad (32)$$

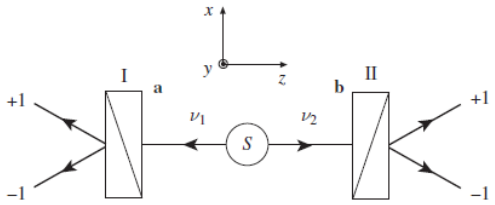
Η **(31)** είναι μία μορφή των ανισοτήτων του Bell, που είναι γνωστή ως ανισότητες των Bell–Clauser–Horn–Shimony–Holt.

4.4 Διεμπλοκή και EPR

Σε αυτό το υποκεφάλαιο θα εξετάσουμε πώς από το παράδοξο EPR καταλήγουμε να έχουμε μέγιστη διεμπλοκή ανάμεσα σε δύο σωματίδια που αλληλεπιδρούν. (Grynberg G., et al., *2010)*

Ας υποθέσουμε ότι έχουμε ένα ζεύγος φωτονίων ν_1 και ν_2, με συχνότητες ω_1 και ω_2 αντίστοιχα, τα οποία εκπέμπονται ταυτόχρονα από δύο πολωτές στη διεύθυνση –Oz και Oz. Η κατάσταση της πόλωσης του ζεύγους των φωτονίων δίνεται από το τανυστικό γινόμενο των πολώσεων για το καθένα ξεχωριστά:

$$E = E_1 \oplus E_2 = \{|x1, x2\_\,;\ |x1, y2\_\,;\ |y1, x2\_\,;\ |y1, y2\_\}\ \ (33)$$



Εικόνα 4-8: Υποθετικό πείραμα EPR με ζεύγη φωτονίων, συσχετιζόμενων πολώσεων.
(De Raedt, Katsnelson, Jattana, Mehta, Willsch, Willsch, Michielsen, & Jin 2023)

Χρησιμοποιώντας τους πολωτές στις κατευθύνσεις a και b, σχηματίζοντας γωνίες θ_{a} και θ_b με τον άξονα Ox, και κάνοντας μετρήσεις για το ζεύγος παίρνουμε τα αποτελέσματα (+1, +1), (+1, -1), (-1, +1), (-1, -1) με τις αντίστοιχες πιθανότητες:

$$P_{++}(\mathrm{a},\mathrm{b}) = |\langle +_{\mathrm{a}}, +_{\mathrm{b}}|\psi\rangle|^2 \quad (34)$$

$$P_{+-}(\mathrm{a},\mathrm{b}) = |\langle +_{\mathrm{a}}, -_{\mathrm{b}}|\psi\rangle|^2 \quad (35)$$

$$P_{-+}(\mathrm{a},\mathrm{b}) = |\langle -_{\mathrm{a}}, +_{\mathrm{b}}|\psi\rangle|^2 \quad (36)$$

$$P_{--}(\mathrm{a},\mathrm{b}) = |\langle -_{\mathrm{a}}, -_{\mathrm{b}}|\psi\rangle|^2 \quad (37)$$

Έτσι λοιπόν, η πιθανότητα για το κάθε φωτόνιο μπορεί να υπολογιστεί, όπως για παράδειγμα το φωτόνιο 1, η πιθανότητα να πάρουμε +1 είναι:

$$P_{+}(\mathrm{a}) = P_{++}(\mathrm{a},\mathrm{b}) + P_{+-}(\mathrm{a},\mathrm{b}) \quad (38)$$

Η ιδιοκατάσταση EPR του ζεύγους (που στην ουσία είναι η εξίσωση (16) που έχουμε γράψει παραπάνω):

$$|\psi_{EPR}>=\frac{1}{\sqrt{2}}(|x,x>+|y,y>) \quad (39)$$

Αυτή η κατάσταση δηλώνει ότι δεν μπορεί να παραγοντοποιηθεί, ώστε να πάρουμε τις καταστάσεις για κάθε φωτόνιο χωριστά, το οποίο οδηγεί στην διεμπλοκή των φωτονίων.

Χρησιμοποιώντας τα ιδιοδιανύσματα για τον προσανατολισμό και την (34):

$$|+\theta>=\cos\theta\ |x>+\sin\theta\ |y> \quad (40)$$

$$|-\theta>=-\sin\theta\ |x>+\cos\theta\ |y> \quad (41)$$

τότε οι πιθανότητες, με $(\mathrm{a},\mathrm{b}) = \theta_b - \theta_{\mathrm{a}}$, δίνονται από τις σχέσεις:

$$P_{++}(\mathrm{a},\mathrm{b}) = |\langle +_{\mathrm{a}}, +_{\mathrm{b}}|\psi_{EPR}\rangle|^2 = \frac{1}{2}\cos^2(\theta_{\mathrm{a}} - \theta_b) = \frac{1}{2}\cos^2(\mathrm{a},\mathrm{b}) \quad (42)$$

$$P_{--}(\mathrm{a},\mathrm{b}) = \frac{1}{2}\cos^2(\mathrm{a},\mathrm{b}) \qquad (43)$$

$$P_{+-}(\mathrm{a},\mathrm{b}) = P_{-+}(\mathrm{a},\mathrm{b}) = \frac{1}{2}\sin^2(\mathrm{a},\mathrm{b}) \quad (44)$$

Καταλήγουμε στο συμπέρασμα ότι οι πιθανότητες εξαρτώνται μόνο από το (a,b) και όχι από τον προσανατολισμό των πολωτών.

Επομένως, η (34) δίνει:

$$P_{+}(\mathrm{a}) = P_{++}(\mathrm{a},\mathrm{b}) + P_{+-}(\mathrm{a},\mathrm{b}) = \frac{1}{2} \quad (45)$$

Με τον ίδιο τρόπο έχουμε:

$$P_{-}(\mathrm{a}) = P_{+}(b) = P_{-}(b) = \frac{1}{2} \quad (46)$$

το οποίο με τη σειρά του δηλώνει ότι αν προσπαθούσαμε να μετρήσουμε την πόλωση για το καθένα χωριστά, τα αποτελέσματα θα ήταν εντελώς τυχαία, δηλαδή τα φωτόνια θα φαίνονταν μη πολωμένα στην EPR κατάσταση.

Αν υποθέσουμε ότι χρησιμοποιούμε μία τυχαία μεταβλητή $A(\mathrm{a})$ που αντιπροσωπεύει την μέτρηση από τον πολωτή 1, παίρνοντας τις τιμές +1 και -1, και αντίστοιχα για τον πολωτή 2 την τυχαία μεταβλητή $B(b)$, ο συντελεστής συσχέτισης δίνεται από τη σχέση:

$$E_{QM}(\mathrm{a},\mathrm{b}) = \overline{A(\mathrm{a}) \cdot B(b)} = \cos 2(\mathrm{a},\mathrm{b}) \qquad (47)$$

Από τη σχέση (43) μπορούμε να συμπεράνουμε ότι τέλεια συσχέτιση θα υπάρξει όταν οι πολωτές βρίσκονται στην ίδια διεύθυνση και $(\mathrm{a},\mathrm{b}) = 0$.

Υπό αυτή τη συνθήκη έχουμε ότι:

$$P_{+}(\mathrm{a}) = P_{++}(\mathrm{a},\mathrm{a}) = \frac{1}{2} \qquad (48)$$

Επομένως, η πιθανότητα να βρούμε +1 για το φωτόνιο 2, όταν $\mathrm{a} = b$, αφού έχουμε βρεί +1 για το φωτόνιο 1 στην κατεύθυνση a:

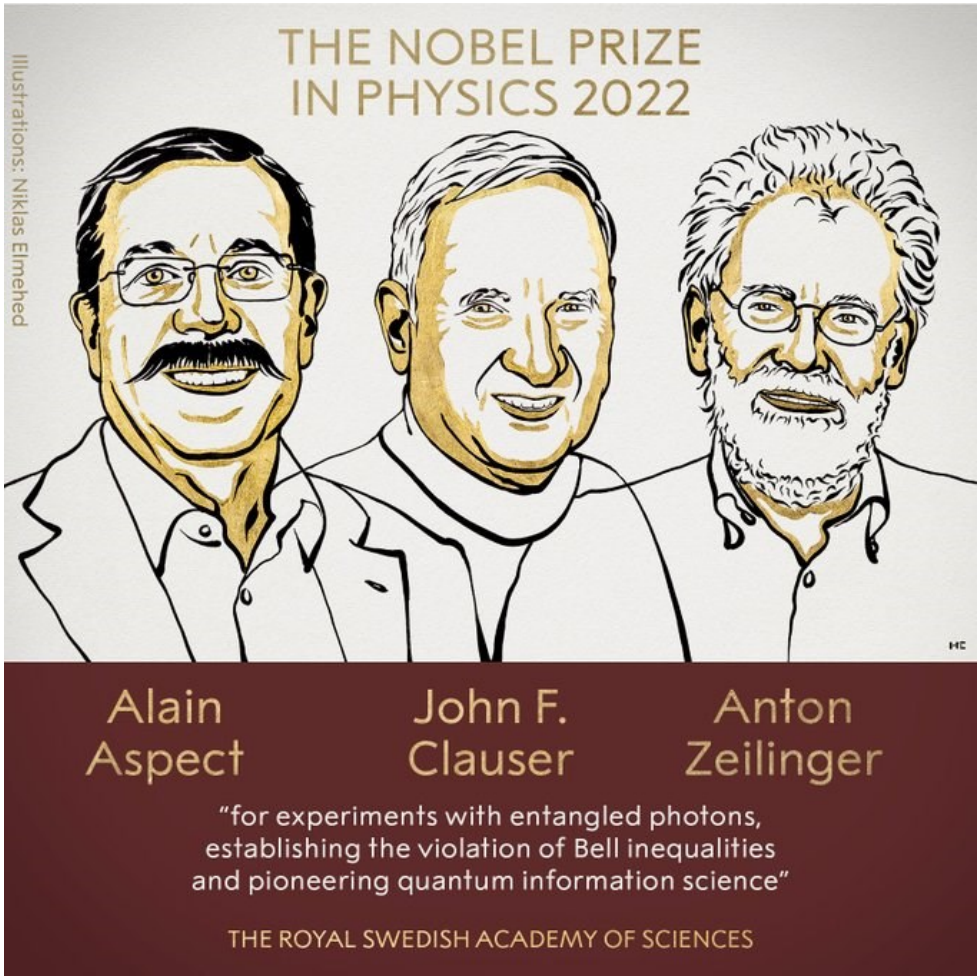
$$P\{B(\mathrm{a}) = +1 | A(\mathrm{a}) = +1\} = \frac{P_{++}(\mathrm{a},\mathrm{a})}{P_{+}(\mathrm{a})} = 1 \quad (49)$$

Το ίδιο θα ισχύει αν βρούμε -1 για το φωτόνιο 2 ενώ έχουμε βρει -1 για το φωτόνιο 1, ενώ για την τιμή +1 στο φωτόνιο 2, με -1 για το φωτόνιο 1 είναι μηδέν.

$$P_{+-}(a, a) = P_{-+}(a, a) = 0 \qquad (50)$$

4.5 Nobel 2022

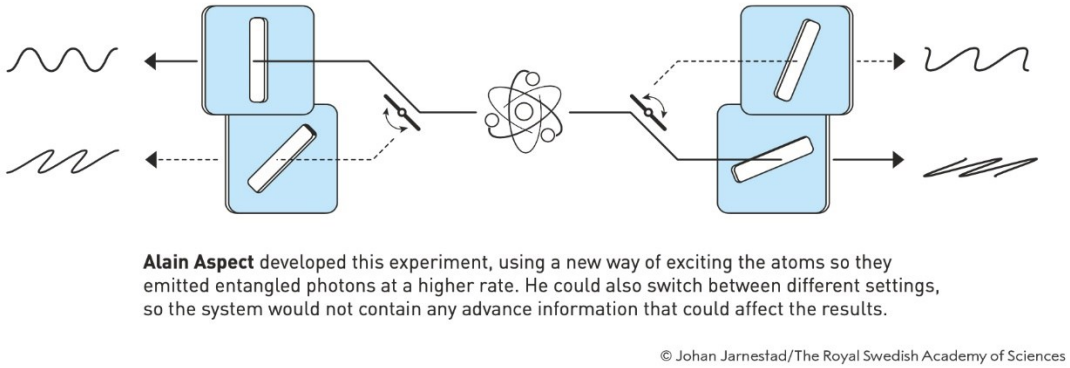
Το 2022, η Βασιλική Σουηδική Ακαδημία Επιστημών έδωσε το Nobel Φυσικής στους Alain Aspect, John F. Clauser και Anton Zeilinger, «για πειράματα με διεμπλεγμένα φωτόνια, που αποδεικνύουν την παραβίαση των ανισοτήτων Bell και αποτελούν πρωτοπορία για την επιστήμη της κβαντικής πληροφορίας».



Εικόνα 4-9: Οι φυσικοί νομπελίστες του 2022, Alain Aspect, John F. Clauser, Anton Zeilinger
(https://www.eef.gr/articles/brabeio-nompel-fysikis-2022)

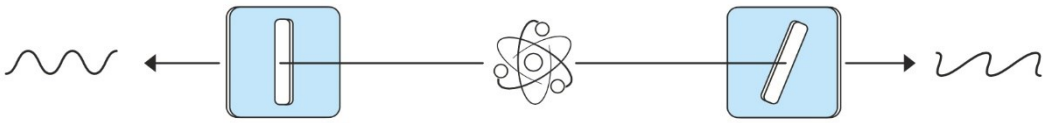
Και οι τρεις επιστήμονες διεξήγαγαν πειράματα χρησιμοποιώντας κβαντικά συστήματα διεπλεγμένων σωματιδίων, αποδεικύοντας ότι αυτά θα επηρεάζουν το ένα το άλλο, ακόμα και όταν θα είναι χωρικά χωρισμένα.

Αναλυτικότερα, ο Alain Aspect, που είναι σήμερα καθηγητής στο Université Paris-Saclay και στο École Polytechnique, Palaiseau, στη Γαλλία, κατάφερε να αλλάξει τις ρυθμίσεις μέτρησης στο κβαντικό σύστημα, αφότου ένα διεμπλεγμένο ζεύγος φωτονίων είχε φύγει από την πηγή του. Αυτό είχε ως αποτέλεσμα η ρύθμιση που υπήρχε όταν εκπέμπονταν να μην μπορεί να επηρεάσει το αποτέλεσμα. Η δήλωσή του μετά την απονομή του Nobel ήταν: «Το συμπέρασμα είναι, ναι, πράγματι η κβαντομηχανική αντιστέκεται σε όλες τις δυνατές επιθέσεις».



Εικόνα 4-10: Το πείραμα του Aspect για εκπομπή διεπλεγμένων φωτονίων
(https://www.ertnews.gr/eidiseis/mono-sto-ertgr/nompel-fysikis-2022-aponemetai-se-treis-epistimones-gia-ta-protoporiaka-toys-peiramata-kvantikis-fysikis/)

Ο John F. Clauser, που είναι Ερευνητής Φυσικός στο J.F. Clauser & Assoc., στο Walnut Creek στις Η.Π.Α., κατασκεύασε μια συσκευή που εξέπεμπε δύο διεμπλεγμένα φωτόνια κάθε φορά, το καθένα προς ένα φίλτρο που δοκίμαζε την πόλωσή τους. Αυτό που παρατήρησε μέσα από το πείραμά του είναι μια σαφής παραβίαση μιας ανισότητας του Bell, το οποίο είναι σε πλήρη συμφωνία με τις προβλέψεις της κβαντικής μηχανικής. Ο Clauser μετά το Nobel, δήλωσε απέδειξε με αυτό το βραβείο ότι είναι αξιοπρεπής πειραματιστής, καθώς δεν έγινε ποτέ καθηγητής, ρισκάροντας την καριέρα του προσπαθώντας να καταρρίψει την κβαντομηχανική.

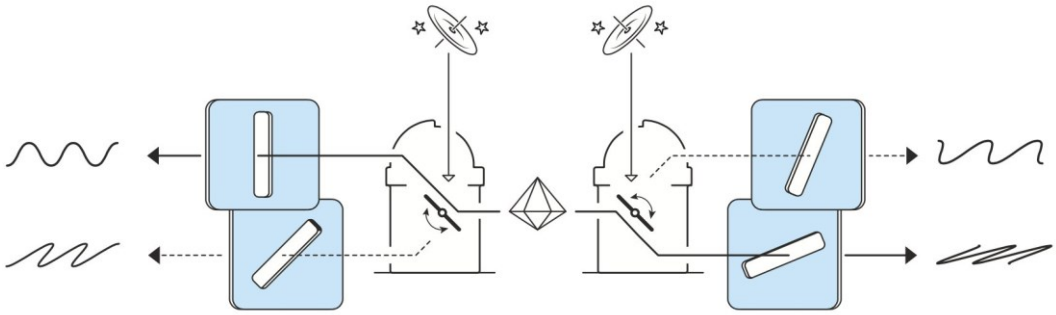


John Clauser used calcium atoms that could emit entangled photons after he had illuminated them with a special light. He set up a filter on either side to measure the photons' polarisation. After a series of measurements, he was able to show they violated a Bell inequality.

© Johan Jarnestad/The Royal Swedish Academy of Sciences

Εικόνα 4-11: Το πείραμα του Clauser για την παραβίαση των ανισοτήτων του Bell
(https://www.ertnews.gr/eidiseis/mono-sto-ertgr/nompel-fysikis-2022-aponemetai-se-treis-epistimones-gia-ta-protoporiaka-toys-peiramata-kvantikis-fysikis/)

Τέλος, ο Anton Zeilinger, είναι καθηγητής στο Πανεπιστήμιο της Βιέννης, όπου και έλαβε το διδακτορικό δίπλωμα του το 1971. Ο ίδιος με την ομάδα του ερεύνησε διεμπλεγμένες κβαντικές καταστάσεις και απέδειξαν το φαινόμενο της κβαντικής τηλεμεταφοράς, το οποίο καθιστά δυνατή τη μετακίνηση μιας κβαντικής κατάστασης από ένα σωματίδιο σε ένα άλλο σε απόσταση.



Anton Zeilinger later conducted more tests of Bell inequalities. He created entangled pairs of photons by shining a laser on a special crystal, and used random numbers to shift between measurement settings. One experiment used signals from distant galaxies to control the filters and ensure the signals could not affect each other.

©Johan Jamestad/The Royal Swedish Academy of Sciences

Εικόνα 4-12: Το πείραμα του Zeilinger για την παραβίαση των ανισοτήτων του Bell χρησιμοποιώντας ένα laser πάνω σε ένα κρύσταλλο
(https://www.ertnews.gr/eidiseis/mono-sto-ertgr/nompel-fysikis-2022-aponemetai-se-treis-epistimones-gia-ta-protoporiaka-toys-peiramata-kvantikis-fysikis/)

Εικόνα 4-13: ο Zeilinger στην απονομή του Nobel 2022
(https://www.nobelprize.org/prizes/physics/2022/zeilinger/podcast/)

Τα πειράματά τους βασίστηκαν στο κβαντικό φαινόμενο της κβαντικής διεμπλοκής, κατά το οποίο, όπως έχουμε ήδη αναφέρει, επιτρέπει σε δύο ή περισσότερα σωματίδια να επηρεάζουν μεταξύ τους τις καταστάσεις τους, ακόμα και αν βρίσκονται σε πολύ μεγάλη απόσταση μεταξύ τους.

Επιπροσθέτως, στηρίχθηκαν στις ανισότητες και το θεώρημα του Bell, ο οποίος όπως εξηγήσαμε παραπάνω, ανέπτυξε μία θεωρία το 1960, την οποία απέδωσε μαθηματικά με μία ανισότητα, η οποία δείχνει πως αν υπάρχουν κρυφές μεταβλητές στα διεπλεγμένα σωματίδια, τότε η συσχέτιση μεταξύ των αποτελεσμάτων ενός μεγάλου αριθμού μετρήσεων δεν θα μπορούσε να υπερβεί ποτέ μια ορισμένη τιμή.

Από την ματιά της κβαντικής φυσικής λοιπόν, προβλέπεται ότι όταν υπάρχει συσχετισμός ανάμεσα στις κβαντικές καταστάσεις (διεμπλοκή), τότε η ανισότητα αυτή παραβιάζεται, δείχνοντας την μεγάλη εξάρτηση μεταξύ των διεπλεγμένων σωματιδίων.

Τα αποτελέσματα των πειραμάτων των τριών Φυσικών Επιστημών, που έλαβαν το Nobel Φυσικής 2022, έθεσαν τα θεμέλια για την εποχή της κβαντικής τεχνολογίας, ανοίγοντας νέους τεχνολογικούς δρόμους για την κβαντική πληροφορική, βρίσκοντας εφαρμογή σε κβαντικούς υπολογιστές και δίκτυα, και στην κβαντική κρυπτογραφία.

4.6 Συνοψίζοντας

Συνοψίζοντας η κβαντική διεμπλοκή είναι ένα πολύ σημαντικό κομμάτι της κβαντικής φυσικής που έχει θέσει τους επιστήμονες επί τάπητος για να εξερευνήσουν τις δυνατότητες που δημιουργούνται με τα αποτελέσματά της, και έχει απασχολήσει στο παρελθόν μεγάλους φυσικούς με τα ερωτήματα που διεγείρονταν.

Η κβαντική διεμπλοκή, το θεώρημα no-cloning και η παραβίαση των ανισοτήτων του Bell παίζουν καθοριστικό ρόλο στην μετάδοση της πληροφορίας, χρησιμοποιώντας πολωμένα φωτόνια.

Αυτό που πρέπει να αποδεχτούμε είναι η ιδέα ότι ένα διαπλεγμένο σύστημα δεν μπορεί να θεωρηθεί ότι αποτελείται από ξεχωριστά υποσυστήματα με τοπικά καθορισμένες φυσικές ιδιότητες που δεν είναι ικανά να επηρεάσουν το ένα το άλλο. Ένα ζεύγος διαπλεγμένων φωτονίων πρέπει να θεωρηθεί ως ένα ενιαίο, αδιαχώριστο σύστημα, το οποίο περιγράφεται από μία παγκόσμια κβαντική κατάσταση, η οποία δεν μπορεί να διασπαστεί σε δύο καταστάσεις, μία για κάθε φωτόνιο. Οι καθιερωμένες ιδιότητες της κβαντικής διεμπλοκής οδηγούν στο να εγκαταλείψουμε την τοπική ρεαλιστική άποψη.

Οι ανισότητες του Bell, καταλήγουν στο συμπερασμα αν εμείς θελουμε να έχουμε μια ρεαλιστική κβαντική θεωρία, η αναγκαία απόρριψη της τοπικότητας είναι ένα τίμημα που φαίνεται να επηρεάζει τη μη τοπικότητα , δηλαδή ότι οι μετρήσεις είναι ανεξάρτητες μεταξύ τους και δεν επηρεάζει η μέτρηση της μίας την άλλη, κάτι που θα οδηγούσε σε μεγαλύτερες ταχύτητες από την ταχύτητα του φωτός.

Αυτές οι αρχές της κβαντικής φυσικής παίζουν σημαντικό ρόλο στον τομέα της κβαντικής πληροφορίας, επομένως και στην κβαντική κρυπτογραφία, η οποία αναλύεται σε αυτήν τη διπλωματική.

5 Κβαντική Κρυπτογραφία

5.1 Ιστορική Αναδρομή

Η κβαντική κρυπτογραφία μπήκε στο χώρο των πειραμάτων το 1989, όπου και έγινε η πρώτη πειραματική κβαντική ανταλλαγή, όμως οι βάσεις είχαν τεθεί πολύ νωρίτερα.

Το 1960, ο Stephen Wiesner έγραψε το "Conjugate Coding", στο οποίο προσπάθησε να εξηγήσει για το πώς η κβαντική φυσική θα μπορούσε να μεταδώσει σημειώσεις που θα ήταν αδύνατον να αποκρυπτογραφηθούν. Διατύπωσε μία επαναστατική ιδέα για εκείνη την εποχή, ονόματι «multiplexing channel», που βασιζόταν στη χρήση κβαντικών καταστάσεων για την ασφαλή κωδικοποίηση και μετάδοση πληροφοριών. Η συγκεκριμένη εργασία δεν δημοσιεύτηκε τότε, καθώς περάσε απαρατήρητη, και είχε αρχικό στόχο την χρήση της κβαντικής φυσικής στην παραγωγή χαρτονομισμάτων που δεν θα μπορούσαν να παραχαραχθούν. (Wiesner, 1983)

Εικόνα 5-1: Κρυπτογραφία και κβαντικό κλειδί

(https://www.linkedin.com/pulse/quantum-cryptography-future-secure-communication-guilherme-junior)

Στη συνέχεια, τον Οκτώβριο του 1979, οι Charles H. Bennett και Gilles Brassard, στο 20ο IEEE Συμπόσιο για τα Θεμέλια της Επιστήμης των Υπολογιστών (*20th IEEE Symposium on the Foundations of Computer Science*), ανακάλυψαν τη διαδικασία ενσωμάτωσης της έννοιας του δημόσιου κλειδιού στην κβαντική κρυπτογραφία, μέσω της εργασίας Crypto '82. Όμως και

αυτό έμεινε στη σφαίρα της φαντασίας, καθώς πρακτικά φάνταζε ακατόρθωτο με τις γνώσεις που είχαν μέχρι τότε.

Η επιβεβαίωση των παραπάνω ήρθε με την ανακάλυψη των ίδιων επιστημόνων, ότι τα φωτόνια «κουβαλούν» και μεταδίδουν την πληροφορία, όπως είχε αναφέρει πρώτος ο Wiesner. Αυτό το γεγονός αποτέλεσε και τον λόγο που δημοσιεύτηκε και η εργασία του Wiesner στο Sigact News, παρά τα χρόνια που είχαν περάσει. (Bennett, et al, 1992)

Με αφετηρία το αποτέλεσμα αυτό, ο Bennett σκέφτηκε την ιδέα της διανομής ενός κβαντικού κλειδιού μέσω ενός κβαντικού καναλιού και ο Brassard σχεδίασε το πρωτόκολλο «cointossing», που στην ουσία είναι ένα κρυπτογραφικό πρωτόκολλο ανάμεσα σε δύο μέρη (Αλίκη και Μπομπ), τα οποία συμφωνούν για μία τυχαία ακολουθία bits, παρά το γεγονός ότι βρίσκονται σε μεγάλη απόσταση μεταξύ τους. (Bennett, Brassard, 1984)

Είναι σημαντικό να αναφέρουμε ότι η κβαντική κρυπτογραφία αντιμετωπίστηκε στην αρχή με καχυποψία και θεωρήθηκε μη ρεαλιστική. Πολλοί ήταν αυτοί που την θεώρησαν καταδικασμένη καθώς έθετε ζητήματα που δεν μπορούσαν να αποδειχθούν ή να μελετηθούν, αφού δεν υπήρχε η αντίστοιχη τεχνολογία για να υλοποιηθεί.

Αργότερα, οι Kilian και Crépeau έδειξαν σε θεωρητικό επίπεδο, πώς να χρησιμοποιηθεί ένα κβαντικό κανάλι, χωρίς όμως να υπάρξει κάποια πρακτική εφαρμογή. (Crépeau and Kilian, 1988)

Πολλά πρακτικά πρωτόκολλα αναπτύχθηκαν, στη συνέχεια από τους Bennet, Brassard και Crépeau, ώστε να πετύχουν την μεταφορά της πληροφορίας μέσω ενός κβαντικού καναλιού.

Τέλος, ο Ekert, πρότεινε το πρωτόκολλου το 1984, το οποίο στηριζόταν σε έναν άλλο τρόπο διανομής του κβαντικού κλειδιού με την χρήση του θεωρήματος EPR και της παραβίασης των ανισοτήτων του Bell. Βασίζεται στη δημιουργία διεπλεγμένων σωματιδίων από μία πηγή EPR, η οποία στέλνει ένα σωματίδιο στην Αλίκη και το άλλο στον Μπομπ. Η παραβίαση της ανισότητας του Bell οδηγεί στο συμπέρασμα ότι τα σωματίδια είναι ισχυρά διεπλεγμένα και άρα δεν υπάρχει πιθανότητα υποκλοπής. Αντίθετα, αν υπάρχει η πιθανότητα υποκλοπής τότε οι συσχετίσεις που «βλέπουν» η Αλίκη και ο Μπομπ θα μειωθούν με αποτέλεσμα να καταλάβουν την μη ασφάλη μετάδοση του κβαντικού κλειδιού. (Ekert, 1991)

5.2 Εισαγωγή στην Κβαντική Κρυπτογραφία

Η κβαντική κρυπτογραφία παίζει σημαντικό ρόλο στην μετάδοση πληροφοριών, διότι προσφέρει την μεγαλύτερη ασφάλεια, βασισμένη στις αρχές της κβαντικής μηχανικής. Ο

κύριος στόχος της είναι η δημιουργία και η διανομή του κλειδιού για την ασφαλή κωδικοποίηση της πληροφορίας, το οποίο επιτυγχάνεται με την μετάδοση φωτονίων κυρίως μέσα σε οπτικές ίνες.

Η ασφάλεια στην μετάδοση των φωτονίων, άρα και της ασφαλούς επικοινωνίας ανάμεσα σε δύο μέρη είναι πολύ σημαντική, και η κβαντική φυσική μπορεί να το επιτύχει σε πολύ μεγάλο ποσοστό. Αυτό στηρίζεται στο γεγονός ότι οποιαδήποτε παρεμβολή στο κβαντικό κανάλι θα διαταράξει το σύστημα με τυχαίο τρόπο και μη ελεγχόμενο τρόπο, κάνοντας γνωστή αυτή την ενέργεια.

Η αρχή της αβεβαιότητας του Heisenberg έρχεται να επιβεβαιώσει τα παραπάνω, με την διατύπωση ότι για ζεύγη ιδιοτήτων (θέση-ορμή, ενέργεια-χρόνος, γραμμική-κυκλική πόλωση), η μέτρηση της μίας αναγκαστικά τυχαιοποιεί την τιμή για την άλλη. Ορίζεται λοιπόν ως βάση ένα οποιοδήποτε μετρήσιμο ζεύγος καταστάσεων πόλωσης για ένα φωτόνιο, και θεωρούμε δύο βάσεις συζυγείς όταν η μέτρηση της μίας, καθορίζει τυχαία την τιμή της άλλης.

Στη συνέχεια, για την υλοποίηση του κβαντικού κλειδιού χρησιμοποιούνται δύο συζυγείς βάσεις, η ορθογώνια, οριζόντια και κατακόρυφη, και η κυκλική, δεξιόστροφη και αριστερόστροφη. Αν κάποιος προσπαθήσει να μετρήσει την ορθογώνια πόλωση τυχαιοποιεί την κυκλική, με αποτέλεσμα να φανερωθεί αυτή η παρεμβολή στη διανομή του κβαντικού κλειδιού.

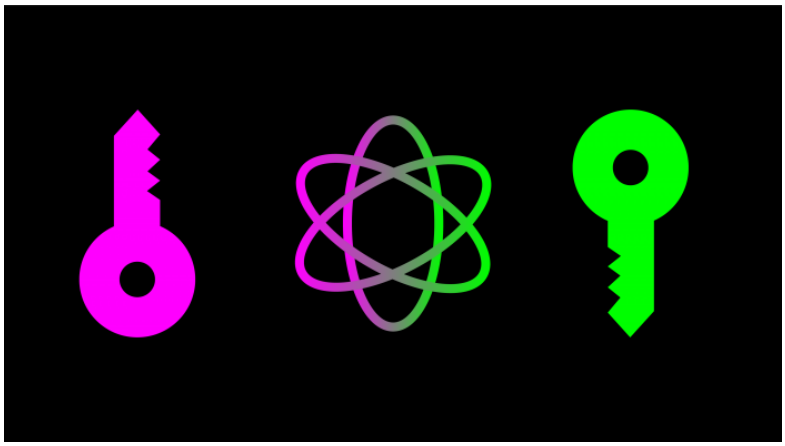
Ένα ακόμη κβαντικό φαινόμενο που παρουσιάζουν ζεύγη ή πλήθη φωτονίων, ως τυπικά κβαντικά συστήματα είναι η κβαντική διεμπλοκή που αναλύσαμε στο 3ο Κεφάλαιο, η οποία αναφέρεται σε μία κατάσταση δύο ή περισσότερων φωτονίων που είναι διεπλεγμένα και φαίνεται να επηρεάζει το ένα το άλλο, ακόμα και όταν βρίσκονται σε μεγάλη απόσταση μεταξύ τους. Η μέτρηση του ενός θα «επηρεάζει» την μέτρηση του άλλου, με αποτέλεσμα πάλι να γίνεται αντιληπτή οποιαδήποτε παρεμβολή στο κβαντικό σύστημα.

Η κβαντική πληροφορία μεταδίδεται με την μορφή των qubits, που όταν μετρηθούν, η πιθανά αποτελέσματα των καταστάσεων παίρνουν τιμές 0 ή 1, έχοντας πρωταρχικό στόχο την διαδικασία διανομής του κβαντικού κλειδιού μέσω ενός κβαντικού καναλιού. Στη συνέχεια, χρησιμοποιούνται οι κλασικές κρυπτογραφικές μέθοδοι, με μυστικό κλειδί για την μετάδοση πληροφοριών.

5.3 Διανομή Κβαντικού Κλειδιού

Η διανομή του κβαντικού κλειδιού (QKD – quantum key distribution) είναι μια ασφαλής μέθοδος επικοινωνίας, η οποία χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για να επιτρέψει την ανταλλαγή κρυπτογραφικών κλειδιών.

Η θεμελιώδης αρχή που στηρίζεται η QKD είναι η Αρχή της Αβεβαιότητας του Heisenberg, η οποία εξηγεί ότι, στην κβαντομηχανική, φυσικές ιδιότητες, όπως η θέση και η ορμή, δεν μπορούν να μετρηθούν ταυτόχρονα με ακρίβεια, με αποτέλεσμα μετρώντας την μία να μην γνωρίζουμε την άλλη.



Εικόνα 5-2: QKD
(https://www.linkedin.com/pulse/how-quantum-communication-works-hector-cardenas-wyjvc?trk=public_post_main-feed-card_feed-article-content)

Ο σκοπός του QKD είναι οι δύο χρήστες, ο αποστολέας (Αλίκη) και τον δέκτη (Μπομπ), οι οποίοι αρχικά δεν μοιράζονται καμία πληροφορία μεταξύ τους, να καταφερουν να συμφωνήσουν σε ένα τυχαίο κλειδί, το οποίο να παραμένει μυστικό από την "Εύα", η οποία κρυφακούει τις επικοινωνίες τους.

Η διανομή του κβαντικού κλειδιού γίνεται με την ανταλλαγή κβαντικών καταστάσεων, συνήθως με την χρήση πολωμένων φωτονίων, οι οποίες κωδικοποιούνται για τη δημιουργία ενός κοινόχρηστου κρυπτογραφικού κλειδιού. Οποιαδήποτε προσπάθεια υποκλοπής (Εύα) των κβαντικών καταστάσεων θα παρεμποδίσει την επικοινωνία ανάμεσα στην Αλίκη και τον Μπομπ, διαταράσσοντας το κβαντικό σύστημα και ειδοποιώντας τους για αυτήν την ενέργεια. Επίσης είναι αξιοσημείωτο να τονίσουμε ότι ακόμα και αν η Εύα μπορέσει να «κρυφακούσει», η ποσότητα της πληροφορίας θα είναι πολύ μικρή. Η πιθανότητα παρεμβολής της Εύας στην

μετάδοση της πληροφορίας αποτελεί έναν παράγοντα «θορύβου», ορολογία που είχε αναφέρει και ο Shannon τη δεκαετία του ’50 (κεφάλαιο 1.2 αυτής της διπλωματικής), που επηρεάζει το κβαντικό σύστημα και θέτει σε κίνδυνο την ασφάλεια της μετάδοσης της πληροφορίας. Άλλοι παράγοντες «θορύβου», που μπορούν να έχουν παρόμοια αποτελέσματα, είναι οι παρεμβολές από το περιβάλλον, όπως οι διακυμάνσεις της θερμοκρασίας του μέσου διάδοσης και η απόσβεση του σήματος μέσα στις οπτικές ίνες λόγω σκεδάσεων. Για αυτό το λόγο, θα πρέπει να ελέγχεται το ποσοστό του σφάλματος που προκύπτει ώστε να εκτιμάται η πιθανότητα υποκλοπής ή όχι.

Ένα από τα πιο σημαντικά πρωτόκολλα για το QKD είναι το πρωτόκολλο BB84, που αναπτύχθηκε από τους Charles Bennett και Gilles Brassard το 1984. (Bennett and Brassard, 1984). Σε αυτό, η Αλίκη κωδικοποιεί τυχαία κάθε bit του κλειδιού ως μία από τις τέσσερις πιθανές καταστάσεις πόλωσης των φωτονίων, χρησιμοποιώντας συνήθως δύο βάσεις . Ο Bob επιλέγει τυχαία μία από τις δύο πιθανές βάσεις για να μετρήσει κάθε φωτόνιο που λαμβάνει. Στη συνέχεια, η Αλίκη και ο Μπομπ συγκρίνουν δημόσια ένα μέρος από τις διαδικασίες τους ώστε να ελέγξουν για αποκλίσεις που θα μπορούσαν να υποδείξουν ότι υπάρχει πιθανή υποκλοπή, καταλήγοντας αν η επικοινωνία είναι ασφαλής.

Παρά το γεγονός ότι η διανομή του κβαντικού κλειδιού είναι αποτελεσματική, υπάρχουν προβλήματα που παρεμποδίζουνν την διαδικασία, όπως η απώλεια φωτονίων, ο θόρυβος και η ανάγκη για εξειδικευμένο εξοπλισμό και χρειάζονται συγκεκριμένους χειρισμούς.

5.4 Επικοινωνία Αλίκη – Μπόμπ

Πριν ξεκινήσουμε την περιγραφή της διαδικασίας, είναι σημαντικό να αναφέρουμε ότι θεωρούμε μία βάση ως οποιοδήποτε ζεύγος πολωμένων καταστάσεων, που θα ανταποκρίνονται σε μετρήσεις ενός φωτονίου, ενώ δύο βάσεις θα είναι συζυγείς αν η μία μέτρηση της μίας τυχαιοποιεί την άλλη.

5.4.1 BB84 Πρωτόκολλο

Στο βασικό πρωτόκολλο που περιγράφουν οι Bennet, Bessette, Brassard, Salvail και Smolin, στην εργασία «Experimental Quantum Cryptography», θεωρούνται δύο συζυγείς βάσεις, η

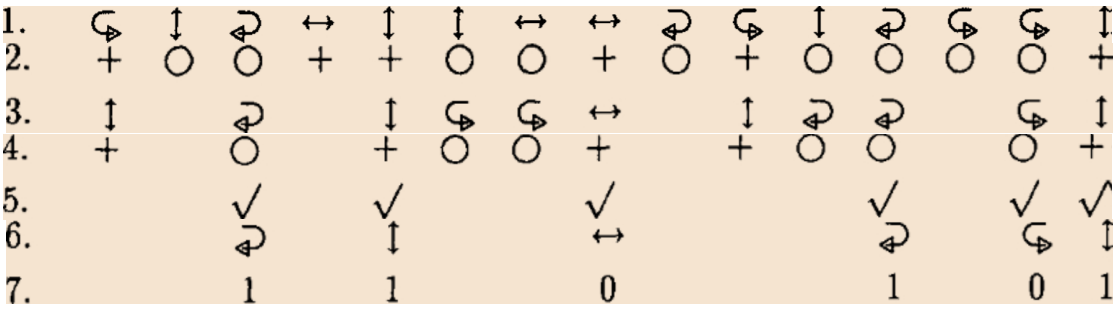
ευθύγραμμη και η κυκλική. Η ευθύγραμμη ορθογώνια βάση αποτελείται από οριζόντια και κατακόρυφη πόλωση, ενώ η κυκλική από κυκλική δεξιά και αριστερά πόλωση. Σε άλλες βιβλιογραφίες θεωρείται επίσης, η βάση που αποτελείται από 45° και 135° πόλωση, η οποία ενσωματώνεται στις δύο παραπάνω. (Bennett, Brassard, Smolin, 1992)

Η περιγραφή της διαδικασίας διανομής του κβαντικού κλειδιού, ονομάζεται και κβαντική μετάδοση, ξεκινάει με την Αλίκη, τον αποστολέα, η οποία στέλνει μία τυχαία ακολουθία από τα κανονικά πολωμένα φωτόνια στον Μπομπ, μέσω ενός κβαντικού καναλιού.

Στη συνέχεια, ο Μπομπ επιλέγει τυχαία, και ανεξάρτητα από τις επιλογές της Αλίκης, αν θα μετρήσει για κάθε φωτόνιο που λαμβάνει την ευθύγραμμη ή κυκλική πόλωση, και ανακοινώνει δημόσια αυτές τις επιλογές του. Η Αλίκη με την σειρά της, ενημερώνει δημόσια αν ο Μπομπ έκανε τη σωστή μέτρηση και συμφωνούν να απορρίψουν εκείνα τα bit για το οποία ο Μπομπ έκανε λάθος μέτρηση, καθώς και αυτά για τα οποία δε έλαβε κανένα φωτόνιο (κάποια φωτόνια δεν θα μετρήθηκαν από τους ανιχνευτές του Μπομπ).

Οι πολώσεις των φωτονίων που μετρήθηκαν σωστά ερμηνεύονται ως bit 0 για την οριζόντια ή την αριστερόστροφη πόλωση και bit 1 για την κατακόρυφη ή δεξιόστροφη αντίστοιχα. Αυτή η συμβολοσειρά αποτελεί την μυστική πληροφορία, που είναι κοινή για την Αλίκη και τον Μπομπ, υπό την προϋπόθεση ότι δεν έχει παρεμβάλλει η Εύα στο κβαντικό κανάλι (υποκλοπή).

Στον παρακάτω πίνακα φαίνεται μία τυχαία ακολουθία από φωτόνια και τα βήματα που περιγράψαμε παραπάνω, ώστε να προκύψει το κβαντικό κλειδί μέσω των bits.



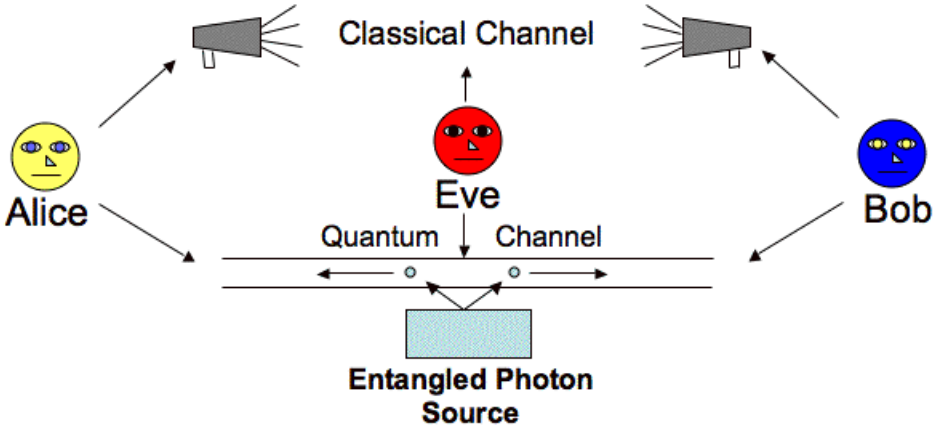
Εικόνα 5-3: Βήματα δημιουργίας κβαντικού κλειδιού με το BB84 πρωτόκολλο
(Bennett, Bessette, Brassard, Salvail & Smolin, 1992).

Αναλύοντας τον πίνακα, ξεκινάμε με την Αλίκη που στέλνει μία τυχαία σειρά από φωτόνια πολωμένα οριζόντια (↔), κατακόρυφη (↕), δεξιόστροφα (↻) και αριστερόστροφα (↺). Στη συνέχεια ο Μπομπ μετράει την πόλωση των φωτονίων σε τυχαίες βάσεις με (+) για τις

ευθύγραμμες και (0) για τις κυκλικές, και στο βήμα 3, είναι τα αποτελέσματα των μετρήσεων με κάποια από τα φωτόνια να μην έχουν μετρηθεί καθόλου. Στο βήμα 4, ο Μπομπ λέει στην Αλίκη ποια βάση χρησιμοποίησε για κάθε φωτόνιο και η Αλίκη, στο βήμα 5, τον ενημερώνει για τις σωστές μετρήσεις. Τέλος και οι δύο κρατούν τις σωστές μετρήσεις των φωτονίων και κωδικοποιούνται ως ↔=↺= 0 και ↕=↻= 1.

5.4.2 Το Πρωτόκολλο του Ekert

Το πρωτόκολλο του Ekert αποτελεί μία άλλη μέθοδο για την διανομή του κβαντικού κλειδιού, χρησιμοποιώντας διεπλεγμένα ζεύγη φωτονίων. (Grynberg, Aspect, Fabre, 2010).



Εικόνα 5-4: Το πρωτόκολλο του Ekert
(www.cse.wustl.edu)

Όπως φαίνεται στην εικόνα **5-4,** μία πηγή εκπέμπει ζεύγη διεπλεγμένων φωτονίων, τα οποία διαχωρίζονται και το ένα πηγαίνει στην Αλίκη και το άλλο στον Μπομπ. Με τη σειρά τους αυτοί επιλέγουν να κάνουν τις μετρήσεις για τα φωτόνια που λαμβάνουν, σε μία τυχαία βάση.

Η Αλίκη και ο Μπομπ πραγματοποιούν τις μετρήσεις τους για τέσσερις καταστάσεις γραμμικής πόλωσης. Οι δύο είναι στον οριζόντιο άξονα |h⟩ και στον κατακόρυφο άξονα |v⟩ και είναι ορθογώνιες μεταξύ τους, δίνοντας αποτέλεσμα + και -, και η βάση τους είναι η hv. Αντίστοιχα, οι άλλες δύο καταστάσεις είναι στον άξονα στις 45° δεξιά |d⟩ και στον άξονα στις 45° αριστερά |g⟩, δίνοντας και αυτές + και – αποτελέσματα μετρήσεων, με βάση dg.

Οι βάσεις που προκύπτουν είναι μεταξύ τους ασυμβίβαστες (συζυγείς), δηλαδη, αν η πόλωση είναι γνωστή σε μία από τις βάσεις, τότε θα είναι εντελώς τυχαία στην άλλη:

$$|h\rangle = \frac{1}{\sqrt{2}}(|d\rangle + |g\rangle) \qquad (51)$$

$$|v\rangle = \frac{1}{\sqrt{2}}(|d\rangle - |g\rangle) \qquad (52)$$

$$|d\rangle = \frac{1}{\sqrt{2}}(|h\rangle + |v\rangle) \qquad (53)$$

$$|g\rangle = \frac{1}{\sqrt{2}}(|h\rangle - |v\rangle) \qquad (54)$$

Όταν η Αλίκη και ο Βασίλης κάνουν τις μετρήσεις τους στις πόλωσεις των διεπλεγμένων φωτονίων στις βάσεις hv και dg, η κβαντική φύση των φωτονίων διασφαλίζει ότι τυχόν προσπάθεια της Εύας να υποκλέψει τα φωτόνια θα προκαλέσει σφάλματα που θα ανιχνευθούν από την Αλίκη και τον Βασίλη.

Οι μετρήσεις που κάνουν η Αλίκη και ο Μπομπ καταγράφονται και μοιράζονται οι πληροφορίες για τις βάσεις που χρησιμοποιήθηκαν, αλλά όχι τα αποτελέσματα των μετρήσεων.

Στη συνέχεια συγκρίνουν τις βάσεις που χρησιμοποίησαν μέσω ενός δημόσιου καναλιού επικοινωνίας. Όταν οι βάσεις τους ταιριάζουν, τα αποτελέσματα των μετρήσεων τους θα είναι συσχετισμένα και μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός μυστικού κλειδιού. Όταν οι βάσεις δεν ταιριάζουν, τα δεδομένα απορρίπτονται.

Με την παραπάνω διαδικασία, εξασφαλίζεται ότι οποιαδήποτε προσπάθεια της Εύας να παρακολουθήσει και να υποκλέψει το κλειδί θα προκαλέσει σφάλματα που θα γίνουν αντιληπτά, επιτρέποντας στην Αλίκη και τον Μπομπ να γνωρίζουν αν η επικοινωνία τους είναι ασφαλής. Αυτό στηρίζεται στο ότι η Εύα δεν μπορεί να γνωρίζει αυτές τις μετρήσεις από πριν, ούτε μπορεί να κλωνοποιήσει το φωτόνιο που φτάνει σε αυτήν, δηλαδή δεν μπορεί να δημιουργήσει ένα ακριβές αντίγραφο. Έτσι, οποιαδήποτε προσπάθεια της Εύας να υποκλέψει το φωτόνιο θα διαταράξει την κατάστασή του και θα δημιουργήσει σφάλματα μετάδοσης.

Για παράδειγμα αν η Εύα διαλέξει να ευθυγραμμίσει τον πολωτή της αυθαίρετα με hv ή dg τότε θα επανεκπέμπει προς την Αλίκη ή τον Μπομπ ένα φωτόνιο στην ακριβώς ίδια κατάσταση πόλωσης με αυτή που μόλις μέτρησε.

Χρησιμοποιώντας τις εξισώσεις *51-54*, έστω ότι η Αλίκη έχει ανιχνεύσει ένα φωτόνιο στην κατάσταση |d⟩ και ο Μπομπ έχει ευθυγραμμίσει τον πολωτή του με τη βάση dg. Στη συνέχεια η Εύα ευθυγραμμίζει τον δικό της πολωτή με τη βάση hv.

Από τα παραπάνω προκύπτει ότι η Εύα θα μετρήσει + ή - με πιθανότητα 1/2 σε κάθε περίπτωση. Ανάλογα με το αποτέλεσμά της, στέλνει στον Μπομπ ένα φωτόνιο στην κατάσταση h ή v. Σε κάθε περίπτωση, αν ο πολωτής του Μπομπ είναι ευθυγραμμισμένος με τη βάση dg, ο Μπομπ μπορεί να μετρήσει +(d) με πιθανότητα 1/2 και −(g) με πιθανότητα 1/2.

Αυτό έρχεται σε αντίθεση με τις μετρήσεις που θα έπρεπε να είχαν η Αλίκη και ο Μπομπ, αν δεν είχε παρέμβει η Εύα, διότι τα φωτόνια θα παρέμεναν διεπλεγμένα και οι μετρήσεις τους συσχετισμένες, με πιθανότητα 1.

Καταλήγωντας λοιπόν, το πρωτόκολλο του Ekert που στηρίζεται στα διεπλεγμένα φωτόνια επιτρέπει στον Μπομπ και την Αλίκη να διαπιστώσουν την πιθανή υποκλοπή από κάποιον τρίτο (Εύα). Έτσι, με την κβαντική κρυπτογραφία εξασφαλίζεται η ασφάλεια του κλειδιού και κατ'επέκταση η ασφάλεια των επικοινωνιών.

5.5 Η Εύα

Όπως εξηγήσαμε παραπάνω, σημαντικό βήμα για την ασφάλεια της διανομής του κβαντικού κλειδιού είναι ο έλεγχος της ύπαρξης υποκλοπής από την «Εύα». Η Αλίκη και ο Μπομπ συγκρίνουν δημοσίως τις πολώσεις των φωτονίων ώστε να συμφωνήσουν για το κβαντικό κλειδί. Αν διαπιστώσουν ότι δεν υπάρχει καμία ασυμφωνία, και ότι η Εύα δεν μπόρεσε να αλλοιώσει το περιεχόμενο των δημόσιων μηνυμάτων που ανταλλάσσονται μεταξύ τους, τότε μπορούν να συμπεράνουν με ασφάλεια ότι υπάρχουν λίγα ή καθόλου σφάλματα και στα υπόλοιπα μη συγκρίσιμα δεδομένα που θα ανταλλάξουν. Ακολούθως μπορούν να υποθέσουν ότι λίγα ή καθόλου από αυτά είναι γνωστά σε οποιονδήποτε υποκλοπέα. (Bennett, Brassard, Smolin, 1992)

Σύμφωνα με το πρωτόκολλο του Ekert, αν η Εύα είχε υποκλέψει τα δεδομένα, τότε θα κατέληγε με μία συμβολοσειρά που θα μοιραζόταν με την Αλίκη και με μία άλλη που θα μοιραζόταν με τον Μπομπ, με αποτέλεσμα το περιεχόμενο της δημόσιας πληροφορίας να είχε αλλοιωθεί.

Για να υπάρχει η ασφάλεια του δημοσίου κλειδιού και η μη αλλοίωσή του, και με δεδομένο ότι κάποια bits χάνονται κατά την μετάδοση στον Μπομπ, ή και λόγω της Εύας, η Αλίκη και ο Μπομπ θα πρέπει να έχουν διαθέσιμη μία επαρκή ποσότητα κοινής μυστικής πληροφορίας

ώστε να μπορούν να αντικαταστήσουν την πληροφορία που έχει χαθεί και να επεκτείνουν το κβαντικό κλειδί. Έτσι εκτός από τη διανομή του κλειδιού, αναγκαία είναι και η επέκταση αυτού.

Στην διαδικασία που περιγράψαμε σε αυτό το κεφάλαιο, η πρακτική εφαρμογή της διανομής τους κβαντικού κλειδιού παρουσιάζει προβλήματα λόγω δύο σημαντικών παραγόντων. Ο πρώτος παράγοντας είναι ο θόρυβος που προκαλείται από τους ρεαλιστικούς ανιχνευτές, ο οποίος μπορεί να οδηγήσει σε σφάλματα των δεδομένων ανάμεσα στη Αλίκη και τον Μπομπ, χωρίς να υπάρχει καν υποκλοπή.

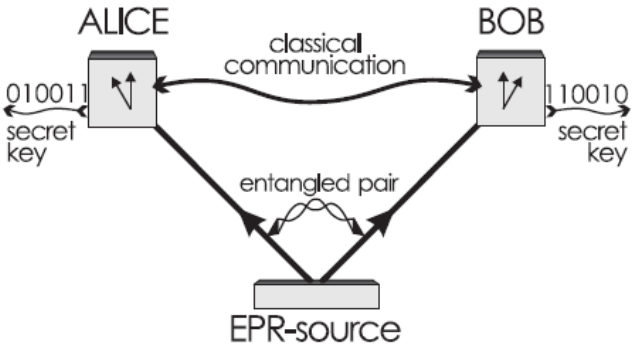
Ο δεύτερος παράγοντας είναι η δυσκολία να παραχθεί ένας φωτεινός παλμός (οι φάσεις των Η/Μ κυμάτων είναι συσχετισμένες ώστε να αποτελεί ένα καλά καθορισμένο κύμα), που να περιέχει ακριβώς ένα φωτόνιο. Ένας συνεκτικός παλμός φωτός είναι πολύ χρήσιμος στο πεδίο της κβαντικής πληροφορίας επειδή, εξαιτίας των σταθερών φάσεων μεταξύ των φωτονίων, δίνει χαμηλό επίπεδο θορύβου, μειώνοντας την πιθανότητα σφαλμάτων, και διατηρεί την κβαντική συνοχή.

Είναι πολύ πιο εύκολο να παραχθεί ένας συνεκτικός παλμός, ο οποίος μπορεί να θεωρηθεί ως μια υπέρθεση κβαντικών καταστάσεων με p φωτόνια ανά παλμό. Αν το p είναι μικρότερο του 1, τότε υπάρχει πιθανότητα περίπου $\frac{p^2}{2}$ να υπάρχει η Εύα και να μπορέσει να χωρίσει έναν παλμό σε δύο ή περισσότερα φωτόνια, διαβάζοντας το ένα και αφήνοντας το άλλο ή τα άλλα να πάνε στον Μπομπ. Αυτό θα έχει ως αποτέλεσμα η Εύα να μάθει ένα σταθερό αριθμό των bits που μοιράζονται η Αλίκη και ο Μπομπ, χωρίς να προκαλέσει σφάλματα και να μπορεί να ανιχνευτεί. Ένα ικανοποιητικό πρωτόκολλο διανομής κβαντικού κλειδίου θα πρέπει να αναγνωρίζει αυτά τα προβλήματα και να είναι σε θέση να τα ξεπερνάει.

5.6 Ασφάλεια Κβαντικού Κλειδιού και Ανισότητα Wigner

Η κβαντική κρυπτογραφία μπορεί να εκμεταλλευτεί τις σημαντικές ιδιότητες της διεμπλοκής των φωτονίων για να παρέχει ασφάλεια στη διανομή του κβαντικού κλειδιού. Υποθέτουμε ότι η Αλίκη και ο Μπομπ λαμβάνουν φωτόνια που είναι σε διεπλεγμένες καταστάσεις, από μία EPR πηγή που παράγει διεπλεγμένα φωτόνια (εικόνα **5-5**), και συμφωνούν σε μία βάση , $|0>$ και $|1>$ για τις οποίες ξεκινούν τις μετρήσεις. Τα πιθανά αποτελέσματα είναι +1 και -1, για

τις αντίστοιχες παρατηρήσεις αυτών των καταστάσεων, και λόγω της διεμπλοκής, αν η Αλίκη μετρήσει το αποτέλεσμα +1, τότε θα ξέρει ότι ο Μπομπ θα μετρήσει -1 και έτσι μπορούν να φτιάξουν ένα τυχαίο κλειδί για να κωδικοποιούν τα μηνύματα. (Alber, Beth, Horodeckis, Rotteler, Weinfurter, Werner & Zeilinger, 2001)



Εικόνα 5-5: Αναπαράσταση της πηγής και της μεταφοράς των διεπεγμένων φωτονίων ανάμεσα στην Αλική και τον Μπομπ

(Alber, Beth, Horodeckis, Rotteler, Weinfurter, Werner & Zeilinger, 2001)

Όπως είδαμε στην προηγούμενη παράγραφο, δεν θα μπορούσε κάποιος (Εύα) να υποκλέψει τα μηνύματα που ανταλλάσουν η Αλίκη και ο Μπομπ και αυτό θα μπορούσε να διερευνηθεί με την παραβίαση της ανισότητας του Wigner, που αποτελεί μία πιο απλή μορφή των ανισοτήτων του Bell.

Ένας σημαντικός παράγοντας είναι η ευθραυστότητα της διεμπλοκής κατά την μέτρηση, καθώς οποιαδήποτε κίνηση από την Εύα να κρυφακούσει, μειώνει την διεμπλοκή, συνεπώς η Αλίκη και ο Μπομπ μπορούν να ελέγχουν την ασφάλεια της επικοινωνίας τους.

Αυτό οφείλεται στους κανόνες της διεμπλοκής, βασιζόμενοι στο ότι οποιαδήποτε μέτρηση υπακούει στη στατιστική συσχέτιση και παραβιάζει τις ανισότητες του Bell. Η παραβίαση των ανισοτήτων του Bell επιβεβαιώνει την διεμπλοκή των σωματιδίων και οποιαδήποτε παρεμβολή θα ακυρώνει τη συσχέτιση αυτών. Αυτό έχει ως αποτέλεσμα να μην υπάρχει πια το φαινόμενο της διεμπλοκής, συνεπώς δεν θα υπάρχει και η παραβίαση των ανισοτήτων του Bell, γεγονός που θα μπορούσε να οδηγήσει στο συμπέρασμα ότι η Εύα προσπαθεί να κρυφακούσει.

Έστω ότι η Αλίκη διαλέγει μεταξύ δύο μετρήσεων της πόλωσης ενός φωτονίου A, στους άξονες a ή b, και ο Μπομπ αντίστοιχα για ένα φωτόνιο B στους άξονες b και c. Η διεύθυνση b είναι κοινή και για τους δύο και με καταστάσεις της βάσης $|0>$ και $|1>$.

Μια ανιχνεύσιμη πόλωση, που είναι παράλληλη στον άξονα του αναλυτή, αντιστοιχεί σε αποτέλεσμα +1 και πόλωση κάθετη αντίστοιχα, σε -1. Έτσι λοιπόν, αν κάποιος υποθέσει ότι κάθε φωτόνιο φέρει προκαθορισμένες τιμές, οι οποίες καθορίζουν τα αποτελέσματα των μετρήσεων σε καθένα από τα ζεύγη φωτονίων, προκύπτει ότι οι πιθανότητες που έλαβαν την τιμή +1 (p_{++}) και στις δύο πλευρές, θα πρέπει να υπακούν στην ανισότητα του Wigner:

$$p_{++}(a_A, b_B) + p_{++}(b_A, c_B) - p_{++}(a_A, c_B) \geq 0 \qquad (55)$$

Αν θέσουμε Θ_A και Θ_B, για την Αλίκη και τον Μπομπ αντίστοιχα, για μία κατάσταση Ψ^-, τότε η κβαντική πιθανότητα:

$$p_{++}(\Theta_A, \Theta_B) = {}^1\!/_2 \, sin^2(\Theta_A - \Theta_B) \quad (56)$$

Για μέγιστη παραβίαση της ανισότητας του Wigner, θεωρούμε a=-30°, b=0°, c=30°:

$$p_{++}(-30^o, 0^o) + p_{++}(0^o, 30^o) - p_{++}(-30^o, 30^o) = -\frac{1}{8} \qquad (57)$$

Καταλήγοντας, για να παραγματοποιηθεί η κβαντική διανομή κλειδιού, η Αλίκη πρέπει να ρυθμίσει του αναλυτές της ανάμεσα στο $-30^o, 0^o$, και ο Μπομπ αντίστοιχα $0^o, 30^o$. Με αυτόν το τρόπο θα προκύψουν τέσσερις πιθανοί συνδυασμοί των αναλυτών, εκ των οποίων οι τρεις πλάγιες ρυθμίσεις επιτρέπουν μία δοκιμή της ανισότητας Wigner, και ο συνδυασμός με την παράλληλη ρύθμιση θα δημιουργήσει τα κλειδιά, όπου η Αλίκη και ο Μπομπ πρέπει να αντιστρέψουν όλα τα bit του κλειδιού για να αποκτήσουν τα ίδια κλειδιά.

Το συμπέρασμα είναι πως αν οι πιθανότητες παραβιάζουν την ανισότητα του Wigner, τότε επιβεβαιώνεται η ασφάλεια του κβαντικού καναλιού, ως ένας ακόμη έλεγχος όπως κάνουν οι ανισότητες του Bell. (Wigner, 1970)

6 Εφαρμογές Κβαντικής Κρυπτογραφίας

6.1 Κβαντικοί υπολογιστές

Εικόνα 6-1: Κβαντικοί Υπολογιστές

(https://medium.com/the-true-sparks/how-quantum-computing-will-change-the-future-8bbf46ae2f30)

Κβαντικός υπολογιστής είναι ένας υπολογιστής που η λειτουργία του βασίζεται στις αρχές της κβαντικής φυσικής. Αυτές οι αρχές, όπως η υπέρθεση και η διεμπλοκή των σωματιδίων δίνουν τη δυνατότητα επεξεργασίας και υπολογισμού πολλών δεδομένων σε μικρό χρονικό διάστημα, λόγω της μεγάλης υπολογιστικής ισχύς που παρουσιάζουν αυτοί οι υπολογιστές.

Οι φυσικοί Richard Feynman, David Deutsch και Paul Benioff ήταν οι πρώτοι που σκέφτηκαν τη δημιουργία ενός υπολογιστή που θα βασίζεται στις αρχές της κβαντομηχανικής, στις αρχές της δεκαετίας του ’80. Η αρχική τους ιδέα βασίστηκε στο γεγονός ότι οι κλασικοί υπολογιστές είχαν βασικούς περιορισμούς στον χρόνο και στην μνήμη για την εκπόνηση βασικών λειτουργιών. Επίσης, παρατήρησαν ότι τα στοιχεία που κατασκευάζονταν για να λειτουργήσουν επάνω στα τσιπ πυριτίου μίκραιναν κατά πολύ σε διαστάσεις, τόσο πολύ που θα έφταναν να είναι συγκρίσιμα με το μέγεθος κάποιων ατόμων. Αυτό οδήγησε στην σκέψη

ότι θα μπορούσαν να κατασκευαστούν υπολογιστές από τα ίδια τα άτομα, σεβόμενοι τις αρχές και τους κανόνες της κβαντομηχανικής.

Έτσι, στη σημερινή εποχή ένας κβαντικός υπολογιστής δεν φαντάζει σενάριο επιστημονικής φαντασίας. Το βασικό χαρακτηριστικό του είναι ότι μπορεί να επεξεργάζεται διαφορετικές λύσεις ενός προβλήματος ταυτόχρονα, δίνοντας ταυτόχρονα πολλές εναλλακτικές λύσεις, κάτι που έιναι ιδιαίτερα χρήσιμο για την επίλυση προβλημάτων με πολλές μεταβλητές.

Ένα άλλο χαρακτηριστικό των κβαντικών υπολογιστών είναι ότι θα μπορούσαν στο μέλλον, να μεταφέρουν πληροφορίες χωρίς να χρησιμοποιούντια καλώδια και τσιπ πυριτίου, με αποτέλεσμα να είναι πιο γρήγοροι και ισχυροί.

Η λειτουργία ενός κβαντικού υπολογιστή στηρίζεται στην μεταφορά των qubits. Ένα qubit μπορεί να είναι 1 ή 0 ταυτόχρονα, όπως εξηγήσαμε στο Κεφάλαιο 2ο, το οποίο επιτρέπει να γίνοντια άπειροι ογκώδεις υπολογισμοί, πάρα πολύ γρήγορα. Ο χειρισμός των qubits σε έναν κβαντικό υπολογιστή καθορίζεται από το σύστημα που έχει επιλεγεί για να επεξεργαστούμε την πληροφορία. Αυτό το κβαντικό σύστημα μπορεί να είναι τα πολωμένα φωτόνια ή οι ιδιότητες της δομής των ατόμων.

6.1.1 Τα Qubits στους κβαντικούς υπολογιστές

Όπως αναλύσαμε στα προηγούμενα κεφάλαια, το qubit, το οποίο αντιστοιχίζεται με το bit στους κλασσσικούς υπολογιστές, είναι γραμμικός συνδυασμός δύο ορθογώνιες καταστάσεις ενός πολωμένου φωτονίου.

Ο χειρισμός των qubits γίνεται μέσω των κβαντικών πύλων, τοποθετημένες σε μία συγκεκριμένη σειρά, και υλοποιώντας περίπλοκους μετασχηματισμούς σε ένα ή σε ζευγάρι qubits. Στη συνέχεια, μετρώντας τα qubits στην τελική τους κατάσταση μπορεί να εξαχθεί ένα τελικό υπολογιστικό αποτέλεσμα.

Ένα πολύ κρίσιμο σημείο είναι η ανάπτυξη ισχυρών qubits για την λειτουργία των κβαντικών υπολογιστών ώστε να δίνουν μεγάλη ακρίβεια. Ένας παράγοντας που επηρεάζει αυτή την αποτελεσματικότητα είναι η ευαισθησία που έχουν τα qubits στις διακυμάνσεις της θερμοκρασίας του περιβάλλοντός τους. Ένα ακόμη σημαντικό ζήτημα που σχετίζεται με αυτούς τους υπολογιστές είναι ότι η μέχρι στιγμής τεχνολογία, τους επιτρέπει να λειτουργούν μόνο για ένα πολύ μικρό χρονικό διάστημα χωρίς σφάλματα.

Μία προτεινόμενη λύση στα παραπάνω έρχεται να δώσει μία ομάδα δεκατριών επιστημών από τα πανεπιστήμια της Μελβούρνης και του Μάντσεστερ, με τη δημοσίευση της έρευνάς τους με τίτλο «Highly ^{28}Si enriched silicon by localised focused ion beam implantation», στο περιοδικό Communication Materilas (Ravi Acharya et al., 2024).

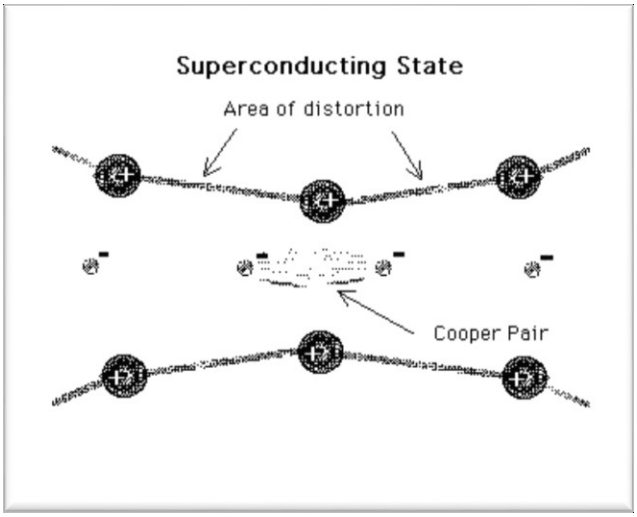
Σε αυτή την έρευνα κατάφεραν να κατασκευάσουν το πιο καθαρό πυρίτιο ώστε να χρησιμοποιηθεί στους κβαντικούς υπολογιστές. Το πυρίτιο είναι ημιαγώγιμο υλικό και λόγω των ιδιοτήτων του προτιμάται γενικά σε κυκλώματα και συσκευές στους κλασικούς υπολογιστές. Αποτελείται από τρία ισότοπα, ^{28}Si, ^{29}Si και ^{30}Si, με το πιο επιθυμητό να είναι το ^{28}Si το οποίο έχει σε μικρό ποσοστό και ^{29}Si, που με τη σειρά του δημιουργεί προβλήματα στην κβαντική συνοχή που χρειάζονται οι υπολογιστές και δημιουργεί σφάλματα. Η μέθοδος που ακολούθησαν κατάφερε να ελαχιστοποιήσει το ^{29}Si και να μειώσει έτσι τις ατέλειες στο κρυσταλλικό πλέγμα που αλληλεπιδρούσαν με τα qubits.

Τα qubits μέσα σε κρυστάλλους πυριτίου παρουσιάζουν μία πολλά υποσχόμενη πλατφόρμα για την κλιμάκωση των κβαντικών επεξεργαστών και δίνουν μεγάλο χρόνο συνοχής τους στη στερεά κατάσταση, δίνοντας τη δυνατότητα να επιλυθούν περίπλοκα προβλήματα σε λίγες ώρες ή και λεπτά.

6.1.2 Η Υπεραγωγιμότητα και Κβαντικοί υπολογιστές

Η υπεραγωγιμότητα είναι ένα κβαντικό φαινόμενο κατά το οποίο κάποια υλικά, όπως κυρίως μέταλλα και κεραμικά, παρουσιάζουν μηδενική ειδική αντίσταση. Αυτά ονομάζονται υπεραγωγοί και ελαχιστοποιούν τις συγκρούσεις μεταξύ των ατόμων και των ηλεκτρονίων, με αποτέλεσμα το ηλεκτρικό ρεύμα να περνάει χωρίς καμία δυσκολία. Η θερμοκρασία είναι βασικός παράγοντας για να γίνει ένα υλικό υπεραγωγός και ονομάζεται κρίσιμη θερμοκρασία. Τα μέταλλα έχουν κρίσιμη θερμοκρασία κοντά στο απόλυτο μηδέν.

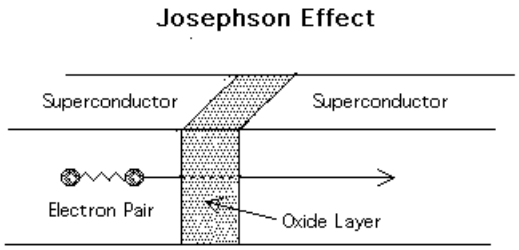
Ένας μηχανισμός που μπορεί να δώσει υπεραγώγιμες ιδιότητες στο υλικό είναι τα ζεύγη Cooper. Η ελάχιστη ταλάντωση των ατόμων του πλέγματος οδηγεί τα ηλεκτρόνια να κάνουν δεσμούς ανά δύο, με αποτέλεσμα να σχηματίζεται ένα «ιδεατό» σωματίδιο, το οποίο έχει διαφορετικές ιδιότητες από τα ηλεκτρόνια.



Εικόνα 6-2: Ζεύγη Cooper

(Λάμπρου, χ.χ.)

Το 1962, ο Brian D. Josephson, προέβλεψε το φαινόμενο που περιγράφει την συμπεριφορά ενός υπερρεύματος, δηλαδή ενός ρεύματος που ρέει απεριόριστα χωρίς να εφαρμόζεται κάποια τάση, ανάμεσα σε δύο υπεραγωγούς που χωρίζονται από ένα πολύ λεπτό μονωτικό φράγμα.



Εικόνα 6-3: Φαινόμενο Josephson

(Λάμπρου, χ.χ.)

Με βάση αυτό κατασκευάστηκαν οι επαφές Josephson, από δύο υπεραγώγιμα υλικά που χωρίζονται από ένα λεπτό μονωτικό φράγμα. Μία από τις πιο χρήσιμες ιδιότητές τους είναι η ικανότητα να εμφανίζουν μία ροή ηλεκτρικού ρεύματος χωρίς καμία εφαρμοσμένη τάση.

Οι κβαντικοί υπολογιστές που κατασκευάζονται από επαφές Josephson διασφαλίζουν τη συνοχή των κβαντικών καταστάσεων, με την ύπαρξη των qubits φορτίου και τα qubits ροής.

Τα πρώτα στηρίζονται στα ζεύγη Cooper και τα δεύτερα χωρίζονται στα qubits συνοχής φάσης ή στη σύνθεση τριών επαφών Josephson.

Καταλήγοντας να σημειώσουμε ότι τα πλεονεκτήματα τέτοιων υπολογιστών είναι αξιοσημείωτα, καθώς θα παρέχουν μεγαλύτερη ταχύτητα, τεράστια μνήμη και δυνατότητα επίλυσης ορισμένων «υπολογιστικά δύσκολων» κλασικών προβλημάτων σε πολυωνυμικό χρόνο.

6.1.3 Υλοποιήσεις Κβαντικών Υπολογιστών

Οπτική Φωτονίων

Η κβαντική οπτική μελετά την αλληλεπίδραση των φωτονίων ενός ηλεκτρομαγνητικού πεδίου με άλλα σωματίδια και είναι ιδιαίτερα σημαντικός κλάδος καθώς τα φαινόμενά της συνδέονται με την κβαντική τηλεμεταφορά. Τα qubits κωδικοποιούνται ανάλογα με την επιλογή των βαθμών ελευθερίας ενός φωτονίου, όπως η πόλωση ή η τροχιακή στροφορμή (κυρίως στις οπτικές ίνες).

Οι πιο κατανοητές τεχνικές που χρησιμοποιούνται είναι αυτές που στηρίζονται στα φωτόνια που εκπέμπονται από συσκευές χειρισμού ηλεκτρομαγνητικής ακτινοβολίας. Σε αυτές τις τεχνικές στηρίχτηκε η κβαντική κρυπτογραφία και η κβαντική τηλεμεταφορά.

Τα φωτόνια θεωρούνται σταθεροί φορείς μετάδοσης της πληροφορίας και μπορούν να λαμβάνονται είτε με τυχαίο τρόπο , είτε όχι όταν το επιθυμούμε.

Ένα μειονέκτημα όμως είναι ότι πρέπει να υπάρχει η μεσολάβηση ενός τρίτου στοιχείου, για παράδειγμα το άτομο, για να αλληλεπιδράσουν.

Η κβαντική οπτική επικοινωνία βασίζεται στη χρήση των φωτονίων μέσω ηλεκτρομαγνητικού πεδίου, ώστε να μεταφερθούν τα qubits από έναν πομπό σε έναν δέκτη, τα οποία αντιδρούν ελάχιστα με το περιβάλλον.

Παγίδες Ιόντων

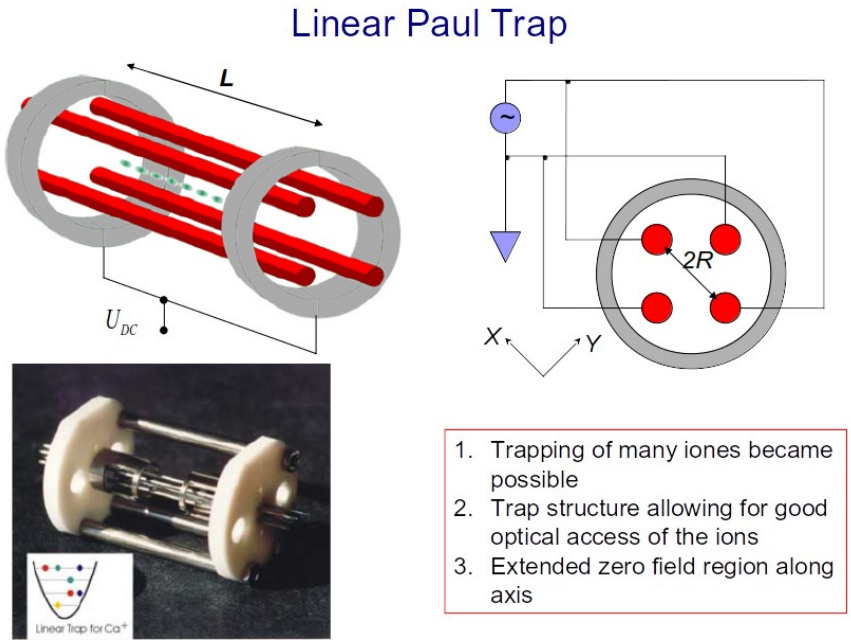
Ένας άλλος τρόπος χειρισμού των qubits είναι η παγίδευση ενός μικρού αριθμού ατόμων (φορτισμένα σωματίδια ή ουδέτερα άτομα) σε ένα συγκεκριμένο και περιορισμένο χώρο.

Η ηλεκτρομαγνητική ακτινοβολία χρησιμοποιείται για να μπορούμε να χειριστούμε την πληροφορία που αποθηκεύεται στα άτομα. Αυτό επιτυγχάνεται όταν αναπτύσσονται διπολικές

δυνάμεις μεταξύ γειτονικών ατόμων, μέσω των ηλεκτρομαγνητικών παλμών που δημιουργούνται από τις πύλες. Οι ιοντικοί κλωβοί, οι κλωβοί Paul και ο πυρηνικός μαγνητικός συντονισμός είναι μερικοί τρόποι παγίδευσης των ιόντων.

Ο ιοντικός κλωβός, που προτάθηκε από τους I. Cirac και P. Zoller, είναι ουσιαστικά ένας θάλαμος κενού ώστε να μπορέσουμε να απομονώσουμε το σύστημα των qubits από το περιβάλλον του. Τα qubits είναι ιόντα ατόμων ώστε να μπορούν να παραμένουν αιωρούμενα και με την εφαρμογή μίας ηλεκτρομαγνητικής διάταξης μένουν σε σταθερές θέσεις. Επιπροσθέτως, τοποθετούνται δύο θετικά φορτισμένες πλάκες κάθετα στον άξονα του κλωβού, ώστε να επιτευχθεί μία σταθερή διάταξη λόγω της απώθηση των πλακών και των απωστικών δυνάμεων των ιόντων.

Στον κλωβό Paul, τα ιόντα που παγιδεύνται, ελέγχονται από μά δέσμη laser και ανιχνεύονται από μία άλλη. Ο κλωβός αυτός αποτελείται από τέσσερα παράλληλα ηλεκτρόδια, με τροφοδότηση από μία πηγή ραδιοσυχνοτήτων, τα οποία αλλάζουν συνεχώς πολικότητα ανά ζεύγη και δεν αφήνουν τα ιόντα να διαφύγουν και τα παγιδεύουν στο κέντρο της διάταξης.



Εικόνα 6-4: Κλωβός Paul

(https://medium.com/@anastasiya.khromova17/paul-radio-frequency-ion-traps-e60770ef3b6c)

Ο κλωβός όμως έχει μειονεκτήματα καθώς δημιουργούνται παράσιτα ηλεκτρικά πεδία λόγω της τυχαίας θερμικής κίνησης τω ηλεκτρονίων μέσα στους αγωγούς (θόρυβος Johnson) και των ανωμαλιών στις επιφάνειες των ηλεκτροδίων, που οδηγούν σε θέρμανση των ιόντων.

Πυρηνικός Μαγνητικός Συντονισμός (NMR)

Ένας ενδιαφέρον τρόπος που στηρίζεται η λειτουργία του κβαντικού υπολογιστή είναι ο Πυρηνικός Μαγνητικός Συντονισμός (NMR), ο οποίος στηρίζεται στην χρήση μορίων και όχι ατόμων. Ο συνδυασμός αυτών των δύο μπορεί να φέρει επανάσταση σε διάφορα επιστημονικά πεδία, παρέχοντας πιο ακριβείς και αποδοτικές μεθόδους για την μοριακή ανάλυση και την επεξεργασία δεδομένων, οδηγώντας σε νέες ανακαλύψεις και καινοτομίες στη χημεία, τη βιολογία, την επιστήμη των υλικών και την ιατρική.

Ο Πυρηνικός Μαγνητικός Συντονισμός βασίζεται στις μαγνητικές ιδιότητες ορισμένων πυρήνων ατόμων, που όταν τοποθετούνται σε ισχυρό μαγνητικό πεδίο, απορροφούν και επανεκπέμπουν ηλεκτρομαγνητική ακτινοβολία σε συγκεκριμένες συχνότητες. Οι κυριότεροι πυρήνες που χρησιμοποιούνται στο NMR είναι το υδρογόνο-1 (^{1}H) και ο άνθρακας-13 (^{13}C).

Η λειτουργία ενός NMR ξεκινάει με την τοποθέτηση των πυρήνων σε ισχυρό μαγνητικό πεδίο, προκαλώντας την προσανατολισμένη τάση τους προς το πεδίο. Στη συνέχεια εφαρμόζεται ένας ηλεκτρομαγνητικός παλμός, διεγείροντας τους πυρήνες σε υψηλότερα ενεργειακά επίπεδα, ενώ αργότερα όταν οι πυρήνες επιστρέψουν στην βασική τους κατάσταση, εκπέμπουν με την σειρά τους ηλεκτρομαγνητική ακτινοβολία η οποία ανιχνεύεται και αναλύεται.

Σε αυτές τις διατάξεις η πληροφορία αποθηκεύεται στη φορά περιστροφής του πυρήνα των ατόμων μέσα στο μόριο και μπορούμε να την χρησιμοποιήσουμε ανιχνεύοντας και αναλύοντας την εκπεμπόμενη ακτινοβολία.

6.1.4 Microsoft, Quantinuum

Τον Απρίλιο του 2024, η Microsoft και η Quantinuum, μία εταιρεία που κατασκευάζει κβαντικούς υπολογιστές, ανακοίνωσαν ότι κατάφεραν να δημιουργήσουν 4 αξιόπιστα λογικά qubits (logical qubits), από 30 φυσικά qubits, το οποίο σημαίνει ότι βελτιώθηκε κατά 800 φορές το ποσοστό σφάλματος ανάμεσα στα λογικά και τα φυσικά qubits. Αυτό έχει ως αποτέλεσμα να μπορεί να υπάρξει ένας κβαντικός υπολογιστής, ανθεκτικός στα σφάλματα που θα μπορεί να εκτελέσει περίπλοκους και μεγάλους υπολογισμούς.

Όπως, αναφέραμε και στα προηγούμενα κεφάλαια το qubit είναι η βασική μονάδα της κβαντικής πληροφορίας και βασίζεται στην υπέρθεση των καταστάσεων και την διεμπλοκή των σωματιδίων. Από την άλλη τα λογικά qubits κατασκευάζονται από πολλαπλά φυσικά qubits, μέσα από την κβαντική διόρθωση σφαλμάτων. Είναι μία αφηρημένη έννοια που χρησιμοποιείται για την εκτέλεση περίπλοκων υπολογισμών από τους κβαντικούς υπολογιστές, χωρίς να επηρεάζονται από την ύπαρξη σφαλμάτων.

Έτσι λοιπόν, η Quantinuum διέθεσε στην Microsoft, 32 φυσικά qubits, χρησιμοποιώντας παγιδευμένα ιόντα. Τα ιόντα αυτά περιορίζονται σε ένα ηλεκτρομαγνητικό πεδίο στο οποίο μπορούν να αιωρηθούν ελεύθερα και αποθηκεύουν τα qubits στις σταθερές ηλεκτρονιακές τους καταστάσεις. Η κβαντική πληροφορία μεταφέρεται με την ολική κίνηση των ιόντων και με την εφαρμογή ενός laser, μπορεί να επιτευχθεί η διεμπλοκή των qubits.

Στη συνέχεια, η Microsoft, μέσα από ένα σύστημα εικονοποίησης κατάφερε να δημιουργήσει τέσσερα αξιόπιστα λογικά qubits, τα οποία όταν ήταν διεπλεγμένα παρουσίασαν πολύ χαμηλά ποσοστά σφάλματος. Αυτό ανοίγει τον δρόμο στην βελτιστοποίηση των κβαντικών υπολογιστών, οι οποίοι χρειάζονται κατά προσέγγιση 100 αξιόπιστα qubits ώστε να φτάσουν στις επιδόσεις τους, όπως υπολογίζουν οι επιστήμονες που ασχολούνται με αυτόν τον κλάδο. (da Silva, et al., 2024)

6.2 Οπτικές Ίνες και μετάδοση πληροφορίας

Οι οπτικές ίνες και η κβαντική κρυπτογραφία είναι δύο διαφορετικές έννοιες και φαντάζουν ασύνδετες, αντιθέτως όμως είναι αλληλένδετες όσο αφορά στην επικοινωνία και την ασφάλεια της πληροφορίας.

Οι οπτικές ίνες είναι λεπτές ίνες κατασκευασμένες από γυαλί ή πλαστικό, με διάμετρο μικρότερητων 10μm. Επιτρέπουν την μετάδοση φωτεινών σημάτων σε πολύ μεγάλες αποστάσεις και με μεγάλες ταχύτητες. Πιο συγκεκριμένα, μεταδίδουν πληροφορίες χρησιμοποιώντας παλμούς φωτός, το οποίο ταξιδεύει μέσα στην οπτική ίνα και αντανακλάται συνεχώς στα τοιχώματά της. Αυτό συνεπάγεται ότι η μετάδοση των δεδομένων θα γίνεται σε πολύ μεγάλες ταχύτητες, σε συνδυασμό με μικρή απώλεια σήματος. Γι’αυτό τον λόγο

χρησιμοποιούνται ευρέως στις τηλεπικοινωνίες για μετάδοση δεδομένων σε μεγάλες αποστάσεις,

Από την άλλη, η κβαντική κρυπτογραφία, όπως έχουμε αναφέρει σε αυτήν τη διπλωματική, χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για την ασφαλή μετάδοση της πληροφορίας. Αυτό που παίζει καθοριστικό ρόλο είναι η διανομή των κβαντικών κλειδιών (QKD), μεταξύ δύο μερών, χρησιμοποιώντας σημαντικούς νόμους της κβαντικής, όπως η αρχή αβεβαιότητας του Heisenberg και η διεμπλοκή των φωτονίων.

Η ανάγκη για ασφαλή δίκτυα επικοινωνίας είναι ο λόγος που οι οπτικές ίνες και η κβαντική κρυπτογραφία συνδέονται, με τις οπτικές ίνες να παρέχουν την υποδομή για την μετάδοση κβαντικών σημάτων σε μεγάλες αποστάσεις χωρίς ή με ελάχιστες παρεμβολές, και η κβαντική κρυπτογραφία να διασφαλίζει την μετάδοση των πληροφοριών, αξιοποιώντας τις θεμελιώδεις αρχές της κβαντικής μηχανικής. Το πλεονέκτημα αυτών τω δύο είναι ότι δημιουργούνται ασφαλή κανάλια επικοινωνίας, αποφεύγοντας τις υποκλοπές.

Οι οπτικές ίνες αποτελούν το μέσο για την μετάδοση των qubits σε μεγάλες αποστάσεις, δηλαδή την κβαντική πληροφορία. Όμως, ένα πρόβλημα που παρουσιάζουν είναι ότι έχουν απώλειες και προκαλούν «θόρυβο», χωρίς απαραίτητα να υπάρχει υποκλοπή, όπως έχουμε εξηγήσει και στα προηγούμενα κεφάλαια, με αποτέλεσμα να περιορίζουν την απόσταση που διαδίδεται η πληροφορία.

Για την μείωση του «θορύβου» και την διασφάλιση της μετάδοσης για μεγάλες αποστάσεις, χρησιμοποιούνται κβαντικοί επαναληπτές στα δίκτυα των οπτικών ινών, που αναγεννούν τα κβαντικά σήματα, ώστε να επεκταθεί η εμβέλεια των συστημάτων για τη διανομή του κβαντικού κλειδιού.

Η μεγάλη πρόκληση είναι να αναπτυχθούν δίκτυα εντός πόλης, αλλά και μεταξύ πόλεων, χρησιμοποιώντας την υποδομή των οπτικών ινών που υπάρχουν μέχρι τώρα, για την αποτελεσματική και αποδοτική διανομή του κβαντικού κλειδίου. Πάνω σε αυτό βασίζονται πολλές έρευνες και μελέτες για να βρεθούν ανιχνευτές μονοφωτονίων, αποτελεσματικοί αλγόριθμοι για τη διόρθωση σφαλμάτων και αποδοτικοί κβαντικοί επαναληπτές.

Ένας από τους σημαντικούς στόχους είναι η ανάπτυξη ενός κβαντικού διαδικτύου, ικανό να μεταδίδει την κβαντική πληροφορία σε όλο τον κόσμο, με απαράμιλλη ασφάλεια. Έτσι, έχουν ξεκινήσει να αναπτύσσονται διάφορα πρωτόκολλα για να ξεπεραστούν τα προβλήματα που

περιορίζουν τις αποστάσεις της μετάδοσης της κβαντικής πληροφορίας, που προκύπτουν από τις οπτικές ίνες.

6.2.1 Προβλήματα στην μετάδοση της πληροφορίας μέσω οπτικών ινών

Όπως εξηγήσαμε αναλυτικά στα προηγούμενα κεφάλαια, η μετάδοση της κβαντικής πληροφορίας βασίζεται στις αρχές της κβαντικής φυσικής, και στηρίζεται στη διανομή του κβαντικού κλειδιού ανάμεσα σε δύο μέρη, την Αλίκη και τον Μπομπ. Η Αλίκη στέλνει ένα φωτόνιο (BB84 πρωτόκλλο) ή διεπλεγμένα φωτόνια μέσω μίας οπτικής ίνας και ο Μπομπ, λαμβάνοντας τα φωτόνια με φωτονικούς ανιχνευτές, διαλέγει μία βάση για να μετρήσει την πόλωσή τους. Με τη διαδικασία που έχουμε ήδη περιγράψει συμφωνούν για το μυστικό κλειδί. Η χρήση των οπτικών ινών για το QKD δημιουργεί κάποια προβλήματα στην μετάδοση, που μπορεί να είναι κρίσιμα για την αποτελεσματικότητα και την απόδοση της διαδικασίας.

Αρχικά, η μετάδοση μέσω οπτικής ίνας είναι πιθανό να προκαλέσει απώλεια φωτονίων λόγω της σκέδασής τους και της απορρόφησης από το μέσο. Ακόμα, υπάρχει περιορισμός της απόστασης που θα διανύσει το σήμα, καθώς φαίνεται να εξασθενεί για μεγάλες αποστάσεις. Τέλος, υπάρχει πιθανότητα οι ανιχνευτές φωτονίων να μην καταγράφουν όλα τα φωτόνια που στάλθηκαν, προκαλώντας σφάλματα.

Η χρήση υψηλής ποιότητας οπτικών ινών ελαχιστοποιεί τις απώλειες λόγω του μέσου, και μπορούν να χρησιμοποιηθούν κβαντικοί επαναληπτές για την επέκταση του QKD, αλλά και για την διανομή του σε μεγάλες αποστάσεις.

Συνοψίζοντας, η διανομή του κβαντικού κλειδιού μέσω οπτικών ινών εγείρε αρκετά προβλήματα που εμποδίζουν την απόδοση και την αποτελεσματικότητα αυτής της διαδικασίας. Πολλές μελέτες και έρευνες πραγματοποιούνται πάνω σε αυτό το πεδίο ώστε να βρεθεί και διασφαλιστεί ο βέλτιστος τρόπος για την μετάδοση της κβαντικής πληροφορίας.

6.2.2 Επίδειξη κβαντικής επικοινωνίας μέσω οπτικών ινών μήκους άνω των 600 Km.

Μία από τις πιο δύσκολες τεχνολογικές προκλήσεις, όπως αναφέραμε, για την κατασκευή του κβαντικού διαδικτύου, είναι το πρόβλημα της μετάδοσης κβαντικών bits, μέσω μεγάλου μήκους οπτικών ινών. Αυτό έγκειται στο γεγονός ότι προκαλείται διαστολή και συστολή των οπτικών ινών λόγω μικρών αλλαγών στις συνθήκες του περιβάλλοντος, όπως διακυμάνσεις

της θερμοκρασίας. Αυτό έχει ως αποτέλεσμα να διαταράσσονται τα εύθραυστα qubits, τα οποία είναι κωδικοποιημένα, και να εμφανίζεται ένας ασθενής οπτικός παλμός στην ίνα.

Το ερευνητικό εργαστήριο Cambridge της Toshiba Europe ανακοίνωσε την πρώτη επίδειξη κβαντικής επικοινωνίας μέσω οπτικών ινών μήκους άνω των 600 χιλιομέτρων, το οποίο θα επιτρέψει την ασφαλή μεταφορά πληροφοριών σε μεγάλες αποστάσεις. Χρησιμοποιώντας μία νέα τεχνική σταθεροποίησης «διπλής ζώνης», στέλνονται δύο οπτικά σήματα αναφοράς, σε διαφορετικά μήκη κύματος, ώστε να ελαχιστοποιηθούν οι διακυμάνσεις φάσης. Το πρώτο μήκος κύματος στοχεύει στην ακύρωση των ταχέως μεταβαλλόμενων διακυμάνσεων και το δεύτερο, το οποίο είναι το ίδιο μήκος κύματος με τα qubits, χρησιμοποιείται για την λεπτή ρύθμιση της φάσης. Με αυτό το τρόπο, διαπιστώθηκε ότι η οπτική φάση ενός κβαντικού σήματος μπορεί να διατηρηθεί σταθερή σε ένα κλάσμα του μήκους κύματος, με ακρίβεια 10 νανομέτρων, ακόμη και μετά από διάδοση μέσω οπτικής ίνας 100 km. Αν δεν υπάρχει αυτή η διαδικασία, η οπτική ίνα θα διαστέλλεται και θα συστέλλεται με τις μεταβολές της θερμοκρασίας, καταλήγοντας στην αλλοίωση της κβαντικής πληροφορίας.

Η Toshiba κατάφερε να εφαρμόσει το Twin Field QKD, σε συνδυασμό με τη τεχνική σταθεροποίησης διπλής ζώνης, σε μήκος 600 χιλιομέτρων. Το Twin Field QKD σχεδιάστηκε για να ξεπεράσει τους περιορισμούς που προκύπτουν στο κλασικό QKD, λόγω των μεγάλων αποστάσεων. Αυτό βασίζεται στο ότι δύο μέρη που βρίσκονται σε απόσταση μεταξύ τους (Αλίκη και Μπομπ), στέλνουν αδύναμους συνεκτικούς παλμούς σε έναν κεντρικό σταθμό μέτρησης (Charlie), ο οποίος εκτελεί μια μέτρηση παρεμβολής στους εισερχόμενους παλμούς

Αυτή η μελέτη, της Toshiba, ανοίγει το δρόμο για ένα εμπορικά βιώσιμο παγκόσμιο κβαντικό δίκτυο ασφαλείας και το QKD αναμένεται να γίνει ένα αξιόπιστο εργαλείο για την προστασία των επικοινωνιών για τόσο για τις επιχειρήσεις όσο και για τις κυβερνήσεις. (Pittaluga, et al., 2021)

6.3 Κβαντική Κρυπτογραφία και Τεχνητή Νοημοσύνη

Η σύνδεση μεταξύ της τεχνητής νοημοσύνης και της κβαντικής κρυπτογραφίας αποτελεί ένα νέο πεδίο ενδιαφέροντος στον επιστημονικό και τεχνολογικό κλάδο. Η τεχνητή νοημοσύνη εξελίσσεται ραγδαία, σημειώνοντας αξιοσημείωτα βήματα στην υγειονομική περίθαλψη και

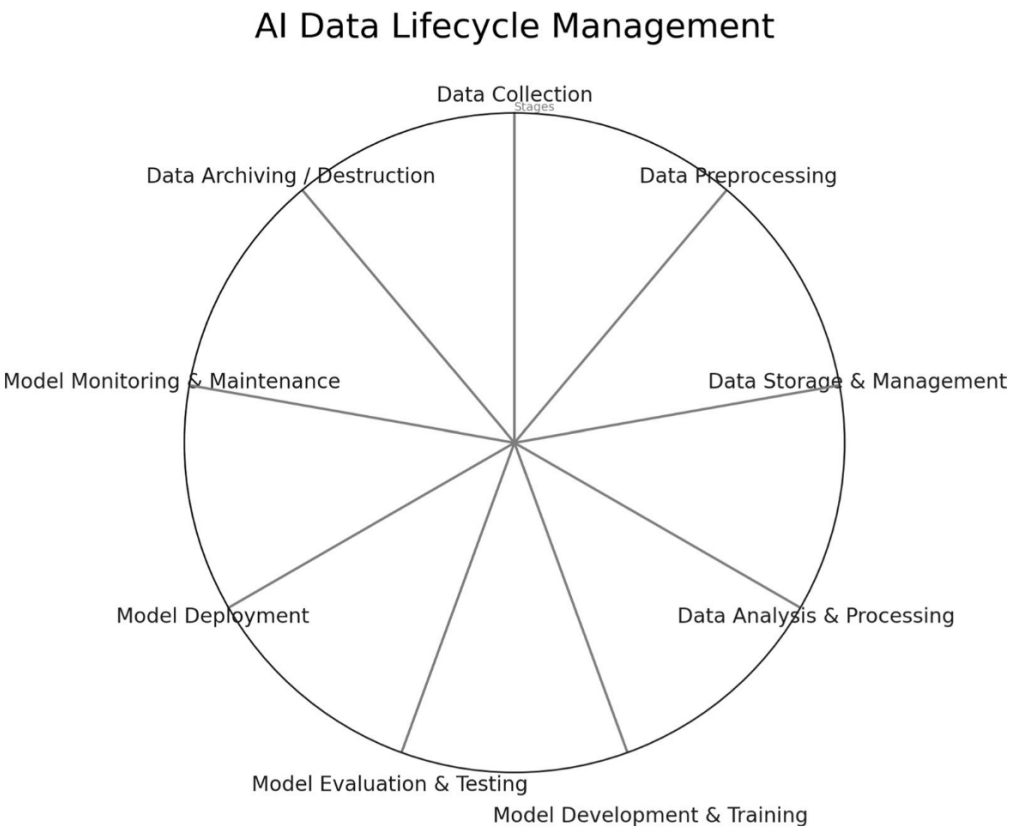
τα χρηματοοικονομικά, αφού στηρίζεται στην εξαιρετική ικανότητα να επεξεργάζεται δεδομένα, να αναγνωρίζει μοτίβα και να λαμβάνει εμπεριστατωμένες αποφάσεις.

Εικόνα 6-5: AI και Κβαντική Κρυπτογραφία
(https://medium.com/@hasannaim/the-role-of-machine-learning-in-enhancing-cybersecurity-current-applications-and-future-prospects-5baa2994cc56)

Αντίστοιχα, η κβαντική κρυπτογραφία παρέχει ασφάλεια στην μετάδοση της πληροφορίας, κυρίως μέσω της κβαντικής διανομής κλειδιών (QKD) που εξηγήσαμε στα προηγούμενα κεφάλαια και ανάλογων πρωτοκόλλων.

Η ασφάλεια που παρέχει η κβαντική κρυπτογραφία στην μετάδοση της πληροφορίας, σε συνδυασμό με την μεγάλη υπολογιστική ισχύ της τεχνητής νοημοσύνης δίνουν τη δυνατότητα για μεταφορά μεγάλων ποσοτήτων πληροφοριών, προστατευμένες από απειλές και κυβερνοεπιθέσεις. Η Τεχνητή Νοημοσύνη αναβαθμίζει τις διαδικασίες της κβαντικής κρυπτογραφίας, με αποτέλεσμα να γίνουν πιο αποδοτικές και προσδοφόρες. Από την άλλη, η κβαντική κρυπτογραφία παρέχει ένα ασφαλές πλαίσιο για Τεχνητή Νοημοσύνη και διασφαλίζει ότι τα δεδομένα και οι αλγόριθμοι που διαχειρίζονται παραμένουν ασφαλή.

Η Τεχνητή Νοημοσύνη χρησιμοποιεί τους αλγόριθμους για να αναλύει και τα ερμηνεύει μεγάλα σύνολα δεδομένων, διαδραματίζοντας καθοριστικό ρόλο στην ασφάλεια των κβαντικών κρυπτογραφικών μηνυμάτων.



Εικόνα 6-6: Δεδομένα από τον κύκλο διαχείρησης των δεδομένων από την Τεχνητή Νοημοσύνη
(Radanliev, 2024)

Η αναγκαιότητα της αλληλεπίδρασης αυτών των δύο κλάδων έγκειται στο γεγονός ότι με την εμφάνιση των κβαντικών υπολογιστών παρουσιάστηκε μια νέα πρόκληση για τα κρυπτογραφικά συστήματα, η "κβαντική απειλή". Οι κβαντικοί υπολογιστές μπορούν να παραβιάσουν τις παραδοσιακές κρυπτογραφικές μεθόδους, που χρησιμοποιούνται σήμερα.

Οι συνέπειες αυτής της απειλής βαραίνουν τις βιομηχανίες που βασίζονται στην τεχνητή νοημοσύνη και πρέπει να δίνουν προτεραιότητα στην ασφάλεια των αλγορίθμων τους και των δεδομένων που χειρίζονται. Αυτό διότι οι παραβιάσεις δεδομένων μπορεί να έχουν σοβαρές συνέπειες, συμπεριλαμβανομένης της φήμης και της οικονομικής απώλειας.

Η χρήση κβαντικών κρυπτογραφικών τεχνικών είναι ένας τρόπος για διασφαλιστούν τα συστήματα της Τεχνητής Νοημοσύνης, χρησιμοποιώντας τις αρχές της κβαντικής μηχανικής για την προστασία των δεδομένων από πιθανές απειλές, καθιστώντας υπολογιστικά αδύνατη την παραβίαση του συστήματος από οποιονδήποτε.

Με αυτόν το τρόπο οι βιομηχανίες μπορούν να επιβεβαιώσουν την ασφάλεια και την ακεραιότητα των συστημάτων της τεχνητής νοημοσύνης και των ευαίσθητων δεδομένων που επεξεργάζονται. (Radanliev, 2024)

6.4 Συνοψίζοντας

Η κβαντική κρυπτογραφία παίζει σημαντικό ρόλο στην προστασία κυρίως των εμπορικών και στρατιωτικών μυστικών πληροφοριών και βασίζεται σε κβαντικά φαινόμενα, με το πιο σημαντικό τη διεμπλοκή των σωματιδίων. Προσφέρει την μεγαλύτερη ασφάλεια έναντι υποκλοπών, με την ασφαλή μετάδοση των φωτονίων ανάμεσα σε δύο μέρη.

Ένα σημαντικό άλμα στην τεχνολογία υπολογιστών αποτελούν οι κβαντικοί υπολογιστές, χρησιμοποιώντας αρχές της κβαντικής μηχανικής για την επεξεργασία πληροφοριών με θεμελιωδώς διαφορετικούς τρόπους σε σύγκριση με τους κλασικούς υπολογιστές.

Η κβαντική διεμπλοκή ίσως είναι το πιο σημαντικό κβαντικό φαινόμενο για τους νέους αυτούς υπολογιστές, όπου τα qubits γίνονται διεπλεγμένα, έτσι ώστε η κατάσταση ενός qubit να επηρεάζει άμεσα την κατάσταση ενός άλλου, ανεξάρτητα από την απόσταση μεταξύ τους. Αυτό οδηγεί στην εκθετική αύξηση της υπολογιστικής ισχύος.

Η μελλοντική τους χρήση θα μπορούσε να σπάσει τις ευρέως χρησιμοποιούμενες μεθόδους κρυπτογράφησης, αλλά και να δημιουργήσει νέες, απαραβίαστες τεχνικές κρυπτογράφησης μέσω της διανομής των κβαντικών κλειδιών.

Τέλος, η μεγάλη υπολογισιτκή ισχύ θα μπορούσε να ενισχύσει τους αλγόριθμους μάθησης, δηλαδή τη τεχνητή νοημοσύνη, ανοίγοντας τον δρόμο για νέες προκλήσεις.

Σημαντικός παράγοντας, όμως, είναι το μέσο μετάδοσης της κβαντικής πληροφορίας, όπως είναι οι οπτικές ίνες, το οποίο μπορεί να προκαλέσει ατέλειες στην μετάδοση και στη διαδικασία της μέτρησης.

Οι εφαρμογές της κβαντικής διεμπλοκής, κυρίως μέσα από την κβαντική κρυπτογραφία αποτελούν την νέα πρόκληση για τους επιστήμονες και μελέτες και έρευνες έχουν αρχίσει ήδη να αποδίδουν σημαντικά αποτελέσματα για την υλοποίησή τους.

Βιβλιογραφικές Αναφορές

Ακολουθούν οι ξενόγλωσσες βιβλιογραφικές αναφορές (πηγές) της Εργασίας.

Acharya, R., Coke, M., Adshead, M., Li, K., Achinuq, B., Cai, R., Gholizadeh, A. B., Jacobs, J., Boland, J. L., Haigh, S. J., Moore, K. L., Jamieson, D. N., & Curry, R. J. (2024). *Highly 28Si enriched silicon by localised focused ion beam implantation. Communications Materials*, 5(1). https://doi.org/10.1038/s43246-024-00498-0

Bennett, C. H., & Brassard, G. (1984). *QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING*.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). *Experimental Quantum Cryptography. 9 1992 International Association for Cryptologic Research* (Vol. 5).

Bennett C. H., Wiesner S. J., (1992). *Communication via One-and Two-Particle Operators on Einstein-Podolsky-Rosen States.* The American Physical Society

Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021*). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography*. Computer Communications, *176*, 99–118. https://doi.org/10.1016/j.comcom.2021.05.019

Crepeau, C., J. Kilian, (1988). *Achieving oblivious transfer using weakened security assumptions*. Proceedings of 29th IEEE Symposium on the Foundations of Computer Science, White Plains, New York

Da Silva, M. P., Ryan-Anderson, C., Bello-Rivas, J. M., Chernoguzov, A., Dreiling, J. M., Foltz, C., Frachon, F., Gaebler, J. P., Gatterman, T. M., Grans-Samuelsson, L., Hayes, D., Hewitt, N., Johansen, J., Lucchetti, D., Mills, M., Moses, S. A., Neyenhuis, B., Paz, A., Pino, J., Svore, K. M. (2024). *Demonstration of logical qubits and repeated error correction with better-than-physical error rates*. http://arxiv.org/abs/2404.02280

Ekert, A. K., (1991). *Quantum Cryptography Based on Bell's Theorem*.

G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rotteler, H. Weinfurter, R. Werner, A. Zeilinger (2001). *Quantum Information. An Introduction to Basic Theoretical Concepts and Experiments*. Springer Tracts in Modern Physics Volume 173

De Raedt, H., Katsnelson, M. I., Jattana, M. S., Mehta, V., Willsch, M., Willsch, D., Michielsen, K., & Jin, F. (2023*). Einstein–Podolsky–Rosen–Bohm experiments: A discrete data driven approach*. *Annals of Physics*, *453*. https://doi.org/10.1016/j.aop.2023.169314

Fedorov, A. K., Kiktenko, E. O., Khabarova, K. Yu., & Kolachevsky, N. N. (2023). *Quantum entanglement, teleportation, and randomness*: Nobel Prize in Physics 2022. Physics-Uspekhi, 66(11), 1095–1104. https://doi.org/10.3367/ufne.2023.06.039412

Grynberg, Gilbert, Aspect, Alain, Fabre, & Claude. (2010). *Introduction to Quantum Optics from the Semi-classical Approach to Quantized Light*.

Halperina, B. I., & Bergmanb, D. J. (2010). *Heterogeneity and disorder: Contributions of Rolf Landauer*. Physica B: Condensed Matter, 405(14), 2908–2914. https://doi.org/10.1016/j.physb.2010.01.002

Hu, C., Wang, W., Chan, K. S., Yuan, Z., & Lo, H. K. (2023). *Proof-of-Principle Demonstration of Fully Passive Quantum Key Distribution.* Physical Review Letters, 131(11). https://doi.org/10.1103/PhysRevLett.131.110801

Leka, B., & Leka, D. (2023). *Programming in Quantum Computers.* Department of Mathematics and Informatics, Faculty of Economics and Agribusiness, Agricultural University of Tirana, Albania

Martinis J.M., Osborne K. (1985). *Superconducting Qubits and the Physics of Josephson Junctions.* National Institute of Standards and Technology. Broadway, USA

Myrvold, Wayne, Marco Genovese, and Abner Shimony, (Spring 2024 Edition). *"Bell's Theorem"*, The Stanford Encyclopedia of Philosophy, Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/spr2024/entries/bell-theorem/

Pittaluga Mirko, Minder M., Lucamarini M., Sanzaro M., Woodward R., Li Ming-Jun, Yuan Zhiliang, Shields A. J., (2021). *600-km repeater-like quantum communications with dual-band stabilization*. Nature Photonics. DOI: 10.1038/s41566-021-00811-0

Quantinuum: Accelerating Quantum Computing. https://www.quantinuum.com/

Radanliev, P. (2024). *Artificial intelligence and quantum cryptography*. In Journal of Analytical Science and Technology (Vol. 15, Issue 1). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s40543-024-00416-6

Rao, V. N., Banerjee, A., & Srikanth, R. (2023). Quantum counterfactuality with identical particles. *Communications in Theoretical Physics*, *75*(6). https://doi.org/10.1088/1572-9494/acb9fd

Renner Renner@Ethz.Ch, R., & Wolf, R. (2023). Quantum Advantage in Cryptography. *AIAA Journal*, *61*(5), 1895–1910. https://doi.org/10.2514/1.J062267

Rodrigues, N., & Lackey, B. (2023). Fully device-independent quantum key distribution using synchronous correlations. *Leibniz International Proceedings in Informatics, LIPIcs*, *266*. https://doi.org/10.4230/LIPIcs.TQC.2023.8

Shannon C. E., (1945). *A Mathematical Theory of Cryptography*.

Shannon C. E., (1949). *Communication Theory of Secrecy Systems*.

Tse, D. (2020). *How Claude Shannon Invented the Future*. https://www.quantamagazine.org/print

Vasani, V., Prateek, K., Amin, R., Maity, S., & Dwivedi, A. D. (2024). Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions. In *Journal of Industrial Information Integration* (Vol. 39). Elsevier B.V. https://doi.org/10.1016/j.jii.2024.100594

Walls D.F., Gerard J. Milburn (2008). *Quantum Optics (2nd Edition).* Springer-Verlag Berlin Heidelberg

Wiesner, S. (1983). *Conjugate coding*. ACM SIGACT News, 15(1), 78–88. https://doi.org/10.1145/1008908.1008920

Wigner E.P., (1970). *On Hidden Variables and Quantum Mechanical Probabilities*. American Journal Physics

Zeilinger, A. (2007). Long-distance quantum cryptography with entangled photons. *Quantum Communications Realized*, *6780*, 67800B. https://doi.org/10.1117/12.740268

Zhou, L. (2013). *The Implications of Experimental Violation of Bell's Inequalities for Local Realism*.

Ακολουθούν οι ελληνικές βιβλιογραφικές αναφορές (πηγές) της Εργασίας.

Αναστόπουλος Χ., Σαββίδου Κ., (2024). *Κβαντική Θεωρία. Μια σύγχρονη παρουσίαση.* Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις.

Δριτσοπούλου Μ.Χ. (2019). *Μετά-κβαντική κρυπτογραφία* (Μεταπτυχιακή Εργασία). Ελληνικό Ανοικτό Πανεπιστήμιο. Πάτρα

Λάμπρου Λ. (χ.χ.). *Επαφή Josephson: Φαινόμενα Και Εφαρμογές* (Διπλωματική Εργασία). Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης. Θεσσαλονίκη

Πίσσας Μ.(2005). *Επιστήμη των Υλικών και Διατάξεων, Εισαγωγή στην Υπεραγωγιμότητα.* Ελληνικό Ανοικτό Πανεπιστήμιο. Πάτρα

Προύσαλης Κ. (2008). *Κβαντική Κρυπτογραφία & Κβαντική Κρυπτανάλυση* (Μεταπτυχιακή Εργασία). Πανεπιστήμιο Αιγαίου. Σάμος

Τραχανάς Σ., (2008). *Κβαντομηχανική ΙΙ.* Πανεπιστημιακές Εκδόσεις Κρήτης.

Τσιαλίκη Α. (χ.χ.). *Κβαντική Κρυπτογραφία* (Διπλωματική Εργασία). Εθνικό Μετσόβιο Πολυτεχνείο. Αθήνα

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986, η παρούσα εργασία 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.