ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΠΑΠΑΘΑΝΑΣΑΚΗ ΜΑΡΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

ΒΑΡΖΑΚΑΣ ΠΑΝΑΓΙΩΤΗΣ

ΜΕΛΟΣ Δ.Ε.Π. ΚΑΘΗΓΗΤΗΣ Α ΒΑΘΜΙΔΑΣ ΓΕΝΙΚΟΥ ΤΜΗΜΑΤΟΣ

ΣΥΝΕΠΙΒΛΕΠΩΝ

ΒΑΒΟΥΓΥΙΟΣ ΔΙΟΝΥΣΙΟΣ

ΚΑΘΗΓΗΤΗΣ

Λαμία 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΠΑΠΑΘΑΝΑΣΑΚΗ ΜΑΡΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

ΒΑΡΖΑΚΑΣ ΠΑΝΑΓΙΩΤΗΣ

ΜΕΛΟΣ Δ.Ε.Π. ΚΑΘΗΓΗΤΗΣ Α ΒΑΘΜΙΔΑΣ ΓΕΝΙΚΟΥ ΤΜΗΜΑΤΟΣ

ΣΥΝΕΠΙΒΛΕΠΩΝ

ΒΑΒΟΥΓΥΙΟΣ ΔΙΟΝΥΣΙΟΣ

ΚΑΘΗΓΗΤΗΣ

Λαμία 2020

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE &
TELECOMMUNICATIONS

QUANTUM CRYPTOGRAPHY

PAPATHANASAKI MARIA

FINAL THESIS

ADVISOR

VARZAKAS PANAGIOTIS

PROFESSOR

CO ADVISOR

VAVOUGYIOS DIONYSIOS

PROFESSOR

Lamia 2020

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [1], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: ……/…../20……

Ο – Η Δηλ….

ΠΕΡΙΛΗΨΗ

Στην παρούσα εργασία γίνεται λόγος για την κβαντική κρυπτογραφία, έναν κλάδο της κρυπτογραφίας που συνδυάζεται με την κβαντική φυσική. Ξεκινώντας με μια γενική περιγραφή τόσο της κρυπτογραφίας όσο και της κβαντομηχανικής, περνάμε στην κβαντική κρυπτογραφία. Εκεί αναλύονται μέθοδοι κβαντικής κρυπτογράφησης και αλγόριθμοι που υλοποιούν αυτές τις μεθόδους. Σκοπός της εργασίας είναι να παρακινήσει τον αναγνώστη να γνωρίσει το «πάντρεμα» των επιστημών της φυσικής και της πληροφορικής, αλλά και την πανίσχυρη δύναμη του δεσμού αυτού.

Λέξεις Κλειδιά: κρυπτογραφία, κβαντομηχανική, φωτοηλεκτρικό φαινόμενο, αρχή συμπληρωματικότητας, παράδοξο EPR, κβαντική διεμπλοκή, φαινόμενο Compton, κβαντικά συστήματα, πολωμένα φωτόνια, διαπλεγμένα σωμάτια, αλγόριθμος OTP, σύστημα RSA, αλγόριθμος Shor,κβαντική υπέρθεση, qubit

ABSTRACT

This project is about quantum cryptography, a branch of cryptography than is combined with quantum physics. The first part refers to cryptography in general, as well as quantum mechanics and then we transition to quantum cryptography. In that part we enlarge upon quantum cryptography's methods and algorithms that apply these methods. The purpose of this project is to motivate the reader to come in touch with the pairing of physics and informatics and the almighty power of that bond.

Keywords: Cryptography, quantum mechanics, photoelectric effect, correspondence principle, EPR paradox, quantum entanglement, Compton phenomenon, quantum systems, photon polarization, RSA system, Shor's algorithm, quantum superposition, qubit.

«Αφιερωμένο στον καθηγητή μου κύριο Βαρζάκα Παναγιώτη, που στάθηκε αρωγός και πολύτιμος σύμβουλος κατά την εκπόνηση της παρούσας εργασίας»

«Στην οικογένειά μου που πάντοτε ήταν στο πλευρό μου»

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ……...…….....11
   1.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ…….……12
      1.1.1. ΠΡΩΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (15ος αι. π.Χ. – 20ος αι π.Χ.)…….……...……12
      1.1.2. ΔΕΥΤΕΡΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1900 μ.Χ. – 1950 μ.Χ.)……..……13
      1.1.3. ΤΡΙΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1950 μ.Χ. – ΣΗΜΕΡΑ)…….……14
   1.2. ΜΕΤΑΒΑΣΗ ΑΠΟ ΤΗΝ ΠΡΟΚΒΑΝΤΙΚΗ ΣΤΗΝ ΚΒΑΝΤΙΚΗ ΠΕΡΙΟΔΟ……...……15
2. ΚΡΥΠΤΟΓΡΑΦΙΑ……...……17
   2.1. ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ……...…17
      2.1.1. ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ……17
      2.1.2. ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ)…….....…17
      2.1.3. ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΠΑΚΕΤΟΥ (BLOCK CIPHERS)…….……18
   2.2. ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ……...…….……19
   2.3. ΠΕΡΙΟΡΙΣΜΟΙ ΚΛΑΣΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ…….…….…23
3. ΚΒΑΝΤΙΚΗ ΜΗΧΑΝΙΚΗ……24
   3.1. ΕΙΣΑΓΩΓΗ……24
   3.2. ΤΟ Qubit……25
   3.3. ΤΟ ΦΩΤΟΗΛΕΚΤΡΙΚΟ ΦΑΙΝΟΜΕΝΟ……...……..…26
   3.4. Η ΑΡΧΗ ΤΗΣ ΣΥΜΠΛΗΡΩΜΑΤΙΚΟΤΗΤΑΣ - ΤΟ ΠΑΡΑΔΟΞΟ EPR……....27
   3.5. ΚΒΑΝΤΙΚΗ ΔΙΕΜΠΛΟΚΗ …….……...30
   3.6. ΤΟ ΦΑΙΝΟΜΕΝΟ COMPTON……..……..……...35
4. ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ……36
   4.1. ΕΙΣΑΓΩΓΗ……36
   4.2. ΚΒΑΝΤΙΚΗ ΠΛΗΡΟΦΟΡΙΑ - ΚΒΑΝΤΙΚΑ ΣΥΣΤΗΜΑΤΑ…….....…37
   4.3. ΜΕΘΟΔΟΙ ΚΒΑΝΤΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ……..…....38
      4.3.1. ΠΟΛΩΜΕΝΑ ΦΩΤΟΝΙΑ (ΜΕΘΟΔΟΣ BB84)……..38
      4.3.2. ΔΙΑΠΛΕΓΜΕΝΑ ΣΩΜΑΤΙΑ……..39
   4.4. ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ - ΑΛΓΟΡΙΘΜΟΙ……...….40
      4.4.1. ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ…….…40
      4.4.2. ΤΟ ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΣΥΣΤΗΜΑ RSA - Ο ΑΛΓΟΡΙΘΜΟΣ Shor……43
   4.5. ΕΦΑΡΜΟΓΕΣ……...…48
   4.6. ΣΥΓΚΡΙΣΗ ΚΒΑΝΤΙΚΟΥ ΜΕ ΚΛΑΣΙΚΟ ΥΠΟΛΟΓΙΣΤΗ……..52
5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ……...54
6. ΒΙΒΛΙΟΓΡΑΦΙΑ…….……...56

1. ΕΙΣΑΓΩΓΗ

Στην εργασία αυτή γίνεται λόγος για την κβαντική κρυπτογραφία και τις εφαρμογές της, καθώς και τις μελλοντικές προοπτικές που έχει στο χώρο της κρυπτογραφίας. Η εργασία χωρίζεται σε έξι κεφάλαια.

Στο πρώτο κεφάλαιο μελετάται η πορεία της κρυπτογραφίας μέσα στους αιώνες και τη μετάβαση στη σύγχρονη κρυπτογραφία.

Στο δεύτερο κεφάλαιο αναλύονται τα είδη και οι στόχοι της κρυπτογραφίας και αναλύονται κάποια από αυτά. Στη συνέχεια αναφέρονται οι εφαρμογές της, αλλά και οι περιορισμοί που έχει στους σύγχρονους υπολογιστές.

Πηγαίνοντας προς το τρίτο κεφάλαιο, θα συναντήσουμε την κβαντική μηχανική. Αφού γίνεται μια εισαγωγή στην έννοια, γνωρίζουμε το qubit, αλλά και ένα πλήθος φαινομένων που απαντώνται στην κβαντική κρυπτογραφία. Τέτοια φαινόμενα είναι το φωτοηλεκτρικό, το Compton, αλλά και κάποιες αρχές όπως αυτή της συμπληρωματικότητας. Θα μιλήσουμε για το παράδοξο EPR, και για το μοναδικό φαινόμενο της κβαντικής διεμπλοκής, καθώς και το πλήθος αρνητικών σχολίων που αναπτύχθηκαν γύρω του.

Στο τέταρτο κεφάλαιο, που είναι και το βασικό της εργασίας, θα μιλήσουμε για την κβαντική πληροφορία και τα κβαντικά συστήματα. Θα γίνει αναφορά σε μεθόδους κβαντικής κρυπτογράφησης, ενώ παράλληλα θα αναλυθούν διεξοδικά οι κβαντικές πύλες, το κρυπτογραφικό σύστημα RSA, καθώς και ο αλγόριθμος Shor.

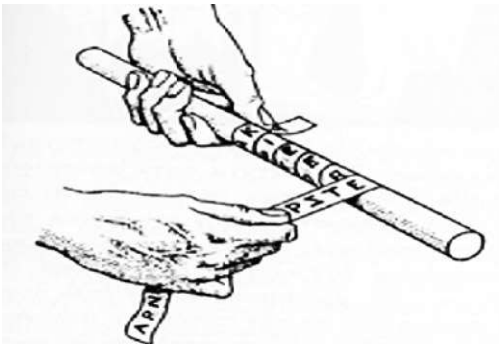
Στα δύο τελευταία κεφάλαια θα έρθουμε σε επαφή με τις προοπτικές της κβαντικής κρυπτογραφίας στο μέλλον και με τη βιβλιογραφία που χρησιμοποιήθηκε για την δημιουργία της εργασίας αυτής, αντίστοιχα.

1.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

1.1.1. ΠΡΩΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ($20^{ος}$ αι. π.Χ. – $15^{ος}$ αι π.Χ.)

Οι ρίζες της κρυπτογραφίας συναντώνται το 1500 π.Χ. στην Μεσοποταμία και συγκεκριμένα στον ποταμό Τίγρη, με την ανακάλυψη μιας σφηνοειδούς επιγραφής που περιγράφει μεθόδους αγγειοπλαστικής. Παρόμοιο εύρημα υπήρξε και στα Σούσα της Περσίας τον ίδιο αιώνα.

Μερικούς αιώνες αργότερα και συγκεκριμένα τον $5^{ο}$ αι. π.Χ. εφευρέθηκε στην Σπάρτη η «Σκυτάλη». Υπήρξε η πρώτη κρυπτογραφική μηχανή και χρησιμοποιήθηκε ευρέως για θέματα στρατιωτικής φύσεως. Η σκυτάλη χρησιμοποιούσε τη μέθοδο της μετάθεσης και πρακτικά αποτελούνταν από μια ράβδο στην οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κλειδί του μηνύματος ήταν η διάμετρος της ράβδου, και το μήνυμα ήταν γραμμένο στην περγαμηνή. Ο αποστολέας του μηνύματος τύλιγε την περγαμηνή στη ράβδο, έγραφε το επιθυμητό μήνυμα και στη συνέχεια το ξετύλιγε και το έστελνε στον παραλήπτη. Εκείνος με τη σειρά του τύλιγε το χαρτί σε ράβδο ίδιας διαμέτρου και διάβαζε το μήνυμα όπως φαίνεται στην **Εικόνα 1.1**.



Εικόνα 1.1. Σπαρτιατική Σκυτάλη

Δύο αιώνες αργότερα στη Μινωική Κρήτη, δημιουργείται ο δίσκος της Φαιστού, γραμμένος σε ιερογλυφική γραφή, μη αποκρυπτογραφημένος ακόμα και σήμερα. Τον επόμενο αιώνα, δηλαδή στις αρχές του $2^{ου}$ αι. π.Χ., εμφανίζονται οι Γραμμική Α' και Β' εκ των οποίων η πρώτη παραμένει στις μη αποκρυπτογραφημένες γραφές.

Ερχόμαστε χρονολογικά στον Μεσαίωνα, κατά τον οποίο η κρυπτογραφία γνωρίζει παρακμή και διώκεται ως τελετή μαύρης μαγείας. Θα χρειαστεί να περάσουν σχεδόν δέκα αιώνες για την ανακάλυψη του επόμενου επιτεύγματος της κρυπτογραφίας το οποίο έλαβε χώρα στην Αίγυπτο. Τον 17^{ο} αι. μ.Χ. ο Γερμανός Jean-François Champollion αποκρυπτογράφησε την Στήλη της Ροζέτας η οποία πρόκειται για μια έκφραση υποτέλειας στον ηγεμόνα της Αιγύπτου, Πτολεμαίο.

Εικόνα 1.2. Στήλη της Ροζέτας

1.1.2. ΔΕΥΤΕΡΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ(1900 μ.Χ. – 1950 μ.Χ.)

Πρόκειται για μια περίοδο κατά την οποία η Κρυπτολογία άκμασε ραγδαία λόγω των δύο παγκοσμίων πολέμων που συνέβησαν εκείνη την περίοδο. Η ανάγκη για μετάδοση μηνυμάτων κρίσιμης σημασίας ανάμεσα στα στρατεύματα και η προστασία στρατηγικών αποφάσεων, ώθησε τους επιστήμονες της εποχής να αναπτύξουν κρυπτοσυστήματα ανάλογης εμπιστοσύνης με τη σοβαρότητα του σκοπού που θα επιτελούσαν. Παράλληλα με την ανάπτυξη των εξελιγμένων αυτών μηχανών, αναπτύσσεται και η ανάλογη τεχνολογία που απαιτείται για την κάλυψη της υπολογιστικής ισχύος των κρυπτομηχανών. Αν και τα συστήματα αυτά ήταν αρκετά ικανά στην κρυπτογράφηση μηνυμάτων, υστερούσαν στον τομέα της ασφάλειας, καθώς κρυπταναλύονταν με ελάχιστη προσπάθεια. Ο Γερμανικός στρατός είχε ανάγκη να επινοήσει μια κρυπτομηχανή που θα ήταν εξαιρετικά δύσκολα παραβιάσιμη. Από την ανάγκη αυτή γεννήθηκε η συσκευή Enigma. Η Enigma I, βελτιωμένη εκδοχή της Enigma, κρυπταναλύθηκε από τον Marian Rejewski, ενώ η

μετέπειτα αναβαθμισμένη μηχανή από τον Alan Turing. Άλλες κρυπτομηχανές, αυτή τη φορά Βρετανικές και Αμερικάνικες, ήταν οι TypeX και SIGABA. Λιγότερο ασφαλείς κρυπτομηχανές που χρησιμοποιήθηκαν την ίδια περίοδο υπήρξαν τα M-209, M-94 και LCD Lacida.

1.1.3. ΤΡΙΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ(1950 μ.Χ. – ΣΗΜΕΡΑ)

Διανύουμε την Τρίτη περίοδο κρυπτογραφίας. Αναμφισβήτητα είναι η εποχή στην οποία η κρυπτογραφία βρίσκεται στο απόγειό της με συνεχή επιτεύγματα. Η περίοδος αυτή ξεκινάει με την δημοσίευση του άρθρου Communication Theory of Secrecy Systems» στο τεχνικό περιοδικό Bell System και λίγο αργότερα το βιβλίο, «Mathematical Theory of Communication», του Claude Shannon. Η λεπτομερής και αφοσιωμένη του δουλειά πάνω στη θεωρία της πληροφορίας και της κρυπτογραφίας έθεσε γερές βάσεις για την ανάπτυξη της κρυπτολογίας.

Το 1975 δημοσιεύτηκε από την IBM το πρότυπο κρυπτογράφησης DES, ως προσπάθεια ανάπτυξης ασφαλών ηλεκτρονικών εγκαταστάσεων επικοινωνίας επιχειρήσεων. Αφού τροποποιήθηκε κατάλληλα, το DES υιοθετήθηκε ευρέως στρέφοντας το ενδιαφέρον της ακαδημαϊκής κοινότητας στην περεταίρω ανάπτυξη της κρυπτολογίας.

Το 2001 ο DES αντικαταστάθηκε από μια εξαιρετικά βελτιωμένη εκδοχή του, τον AES. Ο DES παραμένει σε χρήση στις μετέπειτα ασφαλέστερες μορφές του 2DES και 3DES ακόμα και σήμερα, [1]

1.2. ΜΕΤΑΒΑΣΗ ΑΠΟ ΤΗΝ ΠΡΟΚΒΑΝΤΙΚΗ ΣΤΗΝ ΚΒΑΝΤΙΚΗ ΠΕΡΙΟΔΟ

Η κβαντική κρυπτογραφία είναι σχετικά νέος κλάδος της κρυπτογραφίας, αφού αριθμεί λιγότερα από 50 έτη πρακτικής ύπαρξης. Αποτελεί καινοτόμα προσέγγιση στον τομέα της ασφάλειας και είναι τάχιστα ανερχόμενος κλάδος με πολλές προοπτικές.

Η ιδέα της κβαντικής κρυπτογραφίας γεννήθηκε πολύ πρώιμα αλλά η απουσία της κατάλληλης τεχνολογίας υπήρξε τροχοπέδη στην υλοποίησή της. Το βήμα που αποτέλεσε θεμέλιο της ανάπτυξης της κβαντικής κρυπτογραφίας, ήταν η δημοσίευση μιας εργασίας του Claude Shannon το 1948 που κάλυπτε το μαθηματικό υπόβαθρο που χρειαζόταν. Παράλληλα οι μελέτες του Shannon πάνω στη θεωρία της πληροφορίας, γέννησαν τρόπους κβαντοποίησης της πληροφορίας αλλά και τα όρια συμπίεσής της, επιτυγχάνοντας την ασφαλή μετάδοση δεδομένων.

Το πρώτο άτομο που ασχολήθηκε σοβαρά με την υλοποίηση της ιδέας αυτής, ήταν ο Stephen Wiesner από το πανεπιστήμιο της Columbia στη Νέα Υόρκη. Ο ίδιος δημοσίευσε μια εργασία το 1983, η οποία είχε αρχικά απορριφθεί, που αναφερόταν στην κωδικοποίηση της πληροφορίας σε συζευγμένα κβαντικά συστήματα(quantum conjugate coding). Στην προαναφερθείσα εργασία εξηγούνταν διεξοδικά ο τρόπος αποθήκευσης και μεταφοράς δύο μηνυμάτων σε δύο συζυγείς φυσικές ιδιότητες ενός κβαντικού συστήματος και έπειτα να αποκωδικοποιήσει τη μία εξ' αυτών.

Η εργασία αυτή του Wisner οδηγεί τους Charles Bennett και Gilles Brassard το επόμενο έτος στην δημιουργία ενός βασικού πρωτόκολλου ασφαλούς επικοινωνίας, το BB84.

Το 1990 στο πανεπιστήμιο της Οξφόρδης, ο διδακτορικός φοιτητής Artur Ekert προσεγγίζει την κβαντική κρυπτογραφία με διαφορετικό τρόπο, προτείνοντας το φαινόμενο της κβαντικής διεμπλοκής που βασίζεται στην ιδιαίτερη φύση των κβαντικών συσχετισμών.

Τέσσερα χρόνια μετά ο Deutsch βελτιστοποίησε την προσπάθειά του να βρει ένα υπολογιστικό μοντέλο όπως αυτό της μηχανής Turing, και αποδείχτηκε από τον Peter

Shor ότι ο κβαντικός υπολογιστής είναι σε θέση να ξεπεράσει τους κλασικούς υπολογιστές σε δύναμη. Πιο συγκεκριμένα έδειξε ότι ο κβαντικός υπολογιστής έχει την ικανότητα να φέρει εις πέρας το πρόβλημα της παραγοντοποίησης ακεραίου σε πρώτους παράγοντες, αλλά και εκείνο του διακριτού λογαρίθμου. Η απόδειξη αυτή μονοπώλησε το ενδιαφέρον την επιστημονικής κοινότητας, καθώς τα δύο αυτά προβλήματα παρέμεναν μη ικανοποιητικά επιλύσιμα από τους κλασικούς υπολογιστές. Το 1995 επινοήθηκε ο αλγόριθμος του Grover, ο οποίος αν και υστερούσε σε ταχύτητα συγκριτικά με αυτόν του Shor, ύπηρξε ιδιαίτερα αποτελεσματικός στην ανακάλυψη κβαντικού αλγορίθμου που επιταχύνει την αναζήτηση σε βάσεις δεδομένων σε πολυωνυμικό χρόνο.

Σημαντικό επίτευγμα της δεκαετίας του ’90, είναι αυτό της παρουσίασης του κβαντικού υπολογιστή NMR 2-qubit και αργότερα των 3-qubit, το 1998. Μόλις το 2000 παρουσιάστηκε ο NMR 5-qubit και αργότερα ο NMR 7-qubit. Το πρώτο κβαντικό σύστημα κρυπτογραφίας έγινε διαθέσιμο από την εταιρεία id Quantique το 2004.

Αξίζει να σημειωθεί ότι η κβαντομηχανική θέτει τις βάσεις για την ανάπτυξη της κβαντικής κρυπτογραφίας, καθώς είναι άμεσα συνδεδεμένη με τις δυνατότητες που η κβαντομηχανική προσφέρει, [2]

Η κβαντική θεωρία επεξηγεί, [3]

1. Τη διακριτότητα (κβάντωση) της ενέργειας
2. Τη δυαδικότητα του φωτός και της ύλης
3. Τον κβαντικό εναγκαλισμό
4. Τη κβαντική τηλεμεταφορά
5. Την κβαντική σήραγγα και
6. Τον κβαντικό υπολογιστή

2. ΚΡΥΠΤΟΓΡΑΦΙΑ

2.1. ΕΙΔΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ

2.1.1. ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Αναφέρεται και ως κρυπτογραφία ιδιωτικού κλειδιού(private-key cryptography), ή κρυπτογραφία ενός κλειδιού(one-key cryptography), ή κρυπτογραφία διπλής κατεύθυνσης. Ο συγκεκριμένος τρόπος κρυπτογράφησης χαρακτηρίζεται από τη χρήση ενός κλειδιού και για την κατεύθυνση της κρυπτογράφησης αλλά και αυτή της αποκρυπτογράφησης. Παλαιότερος διαχωρισμός των κρυπτοσυστημάτων διπλής κατεύθυνσης υπήρξε αυτός των συστημάτων αντικατάστασης(substitution) και μετάθεσης(permutation). Σε αυτές τις κατηγορίες συγκαταλέγονται γνωστοί αλγόριθμοι όπως αυτός του Καίσαρα, ο αλγόριθμος PLAYFAIR και Vernam καθώς και οι παραλλαγές τους. Επίσης οφείλουμε να αναφέρουμε και τα κρυπτοσυστήματα Vigenere και AUTOCLAVE, [4]

2.1.2. ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ)

Αναφέρεται και ως κρυπτογραφία δημόσιου κλειδιού(public-key cryptography). Αναφέρθηκαν για πρώτη φορά σε αυτήν το 1976 σε εργασία τους οι Diffie και Hellman, λίγο καθυστερημένα συγκριτικά με την απλότητα της σύλληψης αυτής της ιδέας. Στην κρυπτογραφία δημοσίου κλειδιού υπάρχουν δύο κλειδιά: το κλειδί κρυπτογράφησης, το οποίο είναι δημόσιο και το κλειδί αποκρυπτογράφησης που είναι το ιδιωτικό. Τα κλειδιά κρυπτογράφησης μπορούν να δημοσιοποιηθούν σε έναν server που περιέχει όλους τους χρήστες και τα αντίστοιχα κλειδιά κωδικοποίησής τους. Αν ο χρήστης Α θέλει να επικοινωνήσει ιδιαιτέρως με τον χρήστη Β, θα πρέπει να βρει το δημόσιο κλειδί του Β, και να κρυπτογραφήσει το μήνυμά του με αυτό το κλειδί. Τότε το κρυπτογραφημένο μήνυμα δεν μπορεί να διαβαστεί από οποιονδήποτε

άλλον (ούτε από τον ίδιο τον Α), εκτός από τον χρήστη Β που κατέχει το αντίστοιχο κλειδί αποκρυπτογράφησης, [4]

2.1.3. ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΠΑΚΕΤΟΥ (BLOCK CIPHERS)

Στόχος του αμερικάνικου NBS και νυν NIST(National Institute of Standards and Technology) το 1972, ήταν η δημιουργία ενός προτύπου κρυπτογράφησης προερχόμενο από κατάλληλο αλγόριθμο. Δύο έτη αργότερα η IBM προτείνει το γνωστό σήμερα πρότυπο DES(Data Encryption Standard) το οποίο ξεκίνησε να λειτουργεί το 1977 ως πρότυπο προστασίας ευαίσθητων δεδομένων. Το DES δεν είναι πληροφοριοθεωρητικά ασφαλές, αλλά η κρυπτανάλυσή του είναι υπολογιστικά απρόσιτη. Παράλληλα σε κατάλληλο hardware ο αλγόριθμος του DES είναι ταχύτατος.

Οι αυξημένες ανάγκες για προστασία των δεδομένων οδήγησαν στη δημιουργία του Double-DES και το 1993 του Triple-DES, οι οποίοι αν και ασφαλέστεροι του απλού DES ήταν και αναλόγως αργότεροι.

Μερικά χρόνια αργότερα, μόλις το 2002, τίθεται σε ισχύ το πρότυπο AES από το αμερικανικό Υπουργείο Εμπορίου ως μια ακόμα πιο βελτιωμένη εκδοχή του DES, ιδιαίτερα ασφαλές και ταχύτατο, [4]

Στόχοι Κρυπτογραφίας

- Εμπιστευτικότητα: Η προς μετάδοση πληροφορία πρέπει να είναι κρυφή προς όλους, εκτός από τα εξουσιοδοτημένα μέλη της επικοινωνίας (αποστολέας, παραλήπτης).
- Ακεραιότητα: Διασφάλιση ότι μόνο ο εξουσιοδοτημένος αποστολέας και ο αντίστοιχος παραλήπτης μπορούν να αλλοιώσουν την προς μετάδοση πληροφορία.
- Πιστοποίηση ταυτότητας: Επιβεβαίωση της ταυτότητας ενός χρήστη.
- Πιστοποίηση μηνύματος: Διασφάλιση της πηγής και του προορισμού της πληροφορίας.

- Μη απάρνηση: Τα εξουσιοδοτημένη μέλη της επικοινωνίας πρέπει να αναλαμβάνουν την ευθύνη κάθε ενέργειας που έχει πραγματοποιηθεί και να μην αρνηθούν καμία αργότερα.

2.2. ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η επιστήμη της Κρυπτογραφίας βρίσκει ποικίλες εφαρμογές και ολοένα επεκτείνεται σε περισσότερους τομείς.

Κρυπτογραφία στη Βιολογία

Μια πρωτοπόρα πρόταση τέθηκε από τον Mazhar Karimi μέσα από εργασία του τον Ιούνιο του 2017, για τη δημιουργία μοντέλου συμμετρικής δημιουργίας κλειδιών με πρότυπο τη λειτουργία του DNA. Η ανάγκη για αύξηση της ασφάλειας και της εμπιστευτικότητας των δεδομένων, οδήγησε στην αναζήτηση νέων σύγχρονων μέσων για την επίτευξη του στόχου αυτού.

Κρυπτογραφία στην Κινητή Τηλεφωνία

Οι Al-Saidi, M.A. Magamiss, S.F. Ibraheem, A. Kh. Faraj, στο άρθρο τους με τίτλο «*A new algorithm for signed binary representation and application in mobile phones*», πρότειναν αλγόριθμο ο οποίος έρχεται να αντικαταστήσει το τρέχον πρωτόκολλο ελλειπτικής καμπύλης της κρυπτογραφίας. Συγκεκριμένα ο νέος αλγόριθμος βελτιώνει τον προϋπάρχον, στο κομμάτι της βελτιστοποίησης του βαθμιαίου πολλαπλασιασμού πάνω στο οποίο εκείνος στηριζόταν.

Παράλληλα στην ίδια δημοσίευση προτείνονται και άλλοι αλγόριθμοι όπως ο «δεξιά προς τα αριστερά» της αμοιβαίας αντίθετης μορφής (Mutual Opposite Form - MOF) σε ECSM και η Συμπληρωματική Αναγνωριστική Μέθοδο (Complementary Recognition Method – CRM). Ακόμα ορίζεται ο αλγόριθμος «Μη Γειτονική Μορφή (Non Adjacent Form - NAF)» του κλιμακωτού k, τη μη προσημασμένη δυαδική

αναπαράσταση του κλιμακωτού k για την άμεση μέθοδο αναγνώρισης (Direct Recognition Method - DRM). Όλοι οι αλγόριθμοι αυτοί συνοδεύονται από παραδείγματα και αποτελέσματα εκτελέσεων.

Το άρθρο αυτό είναι πρωτοπόρο πέρα από τις κινητές τηλεφωνίες και στην κρυπτογραφία, καθώς παρουσιάζει ιδιαίτερο ενδιαφέρον η εφαρμογή που αναπτύχθηκε από την ομάδα, η οποία είναι σε θέση να υπολογίζει τις ελλειπτικές καμπύλες έχοντας ελάχιστα δεδομένα με αξιοσημείωτα τεράστια ταχύτητα. Αντίστοιχα οι χρόνοι κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων είναι πολύ μικροί, ενώ αξίζει να αναφερθεί ότι η παραπάνω θεωρία μπορεί να εφαρμοστεί σε όλες τις συσκευές με λειτουργικό σύστημα Android.

Κβαντικοί Υπολογισμοί και Κρυπτογραφία

Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι εφαρμογές της κβαντικής μηχανικής στην κρυπτογραφία. Στην παρούσα πτυχιακή εργασία θα ασχοληθούμε με αυτή ακριβώς την πρωτοπόρα ιδέα.

Είναι ήδη γνωστό ότι στο κλασικό υπολογιστικό μοντέλο η βασική μονάδα πληροφορίας είναι το bit το οποίο μπορεί να λάβει δύο μοναδικές τιμές, «0» ή «1». Σε υλικό αυτή η λειτουργία υλοποιείται σε μία πύλη εισόδου πολλών bits και εξόδου ενός bit. Ο συνδυασμός πολλών εκδοχών της πύλης αυτής μας δίνει πολύπλοκα κυκλώματα όπως εκείνο μιας Μονάδας Επεξεργασίας Δεδομένων.

Αντίθετα με το κλασικό, στο κβαντικό μοντέλο υπολογισμού η βασική μονάδα πληροφορίας είναι το qubit(quantum bit). Τα qubits μπορούν να λάβουν τιμές που είναι συνδυασμός της κατάστασης «0» και της κατάστασης «1», τιμές δηλαδή που είναι υπερθέσεις των «0» και «1». Το qubit μπορεί να υπάρξει σε οποιοδήποτε ιδανικό quantum σύστημα δύο καταστάσεων. Τέτοιες καταστάσεις περιγράφονται από:

1. φωτόνια με κάθετη και οριζόντια πόλωση που αντιπροσωπεύουν τις δύο ορθογώνιες καταστάσεις,
2. ηλεκτρόνια και άλλα συστήματα spin-1/2 με περιστροφή επάνω και αριστερά που αντιπροσωπεύουν τις δύο ορθογώνιες καταστάσεις

3. συστήματα που ορίζονται από δύο ενεργειακά επίπεδα ατόμων ή ιόντα

Με εφαλτήριο τις γνώσεις από τη κβαντομηχανική, είμαστε σε θέση να δημιουργήσουμε έναν κβαντικό υπολογιστή ο οποίος αναμένεται να λύνει προβλήματα πολύ ταχύτερα από τους κλασικούς υπολογιστές. Συγκεκριμένα, θα χρησιμοποιεί τους καλύτερους μέχρι τώρα γνωστούς αλγόριθμους, όπως η παραγοντοποίηση μεγάλων αριθμών χρησιμοποιώντας τον αλγόριθμο του Shor, ή η προσομοίωση μεγάλων συστημάτων.

Δυστυχώς σε μίας τέτοιας έκτασης προσπάθεια, είναι αναμενόμενη η ύπαρξη αρνητικών επεκτάσεων ιδιαίτερα στο κομμάτι της ασφάλειας. Οι κβαντικοί υπολογιστές αναμένεται να επηρεάσουν τους προϋπάρχοντες αλγορίθμους, όσον αφορά την ασφάλεια που αυτοί παρέχουν. Η τεράστια δύναμη που διαθέτουν οι κβαντικοί υπολογιστές τους κάνει ικανούς να σπάσουν οποιοδήποτε σύστημα δημόσιου κλειδιού ή να ανακτήσουν κλειδιά RSA τάχιστα.

Εδώ ακριβώς βρίσκει εφαρμογή η κβαντική κρυπτογραφία. Πρόκειται για μία καινοτομία που θα μένει απρόσβλητη από επιθέσεις, καθώς πρόκειται για την ασφαλέστερη μέθοδο που θα εφαρμοστεί, όσον αφορά πάντα τα περιβάλλοντα στα οποία αυτή εφαρμόζεται.

Οι κβαντικές μηχανές προσφέρουν δύο σημαντικά πλεονεκτήματα στον κλάδο της κρυπτογραφίας. Αυτά είναι η διανομή κλειδιών και η παραγωγή τυχαίων αριθμών.

- **Διανομή Κλειδιών**

  Στην κρυπτογραφία συμμετρικού κλειδιού οι δύο πλευρές πρέπει να διαθέτουν ένα προσυμφωνημένο μυστικό κλειδί. Δυστυχώς η διανομή των μυστικών κλειδιών υπήρξε αρκετά ριψοκίνδυνη όσον αφορά την ασφάλεια. Τα δύο μέρη θα έπρεπε να έχουν επαφή πρόσωπο με πρόσωπο για την ανταλλαγή του κλειδιού ή τουλάχιστον έναν έμπιστο μεταφορέα.

  Παράλληλα στην ασύμμετρη κρυπτογραφία, η διανομή του δημόσιου κλειδιού γίνεται μέσα από server δημοσίων κλειδιών. Όταν ένα άτομο δημιουργεί ένα ζεύγος κλειδιών, κρατάει για αυτόν το ιδιωτικό και

δημοσιοποιεί σε έναν server το δημόσιο, το οποίο είναι προσβάσιμο από οποιονδήποτε επιθυμεί να του αποστείλει κάποιο ιδιωτικό κρυπτογραφημένο μήνυμα. Η κρυπτογραφία δημόσιου κλειδιού θεωρείται ακόμα ασφαλής για την διαφύλαξη των πληροφοριών. Με τη βοήθεια της κβαντικής κρυπτογραφίας, όταν ολοκληρωθεί η επικοινωνία των δύο χρηστών, το κλειδί βρίσκει εφαρμογές σε κωδικό ελέγχου ταυτότητας ή ακόμα και σε συμβατικό συμμετρικό κρυπτογράφο.

Η κβαντική κρυπτογραφία δεν είναι ένας νέος τρόπος κρυπτογράφησης, ωστόσο μπορεί να παρέχει απόλυτη ασφάλεια αφού δεν έχει τόσο μαθηματικές όσο φυσικές βάσεις. Ο πυρήνας της βασίζεται στην αρχή της απροσδιοριστίας του Heisenberg, σύμφωνα με την οποία όση περισσότερη βεβαιότητα υπάρχει για τη θέση ενός σωματιδίου, τόση αντίστοιχα αβεβαιότητα υπάρχει για την ορμή του και αντίστροφα.

Η κβαντική κρυπτογραφία υστερεί για την ώρα στον τομέα των ψηφιακών υπογραφών. Επιπροσθέτως οι πρακτικές εφαρμογές της περιορίζονται μόνο στην ανταλλαγή μεγάλου όγκου δεδομένων, αλλά και συνομιλίες με ανάγκη για ύψιστη ασφάλεια και εμπιστευτικότητα, [5]

- **Παραγωγή Τυχαίων Αριθμών**

Στους κβαντικούς υπολογισμούς υπάρχει απόλυτη τυχαιότητα. Είναι αδύνατον να προβλέψουμε μελλοντικές τιμές κβαντικών διεργασιών ακόμα και με πολύ μεγάλη υπολογιστική ισχύ. Μιας και υπάρχει η ανάγκη για ύπαρξη κλειδιών μη προβλέψιμα από κάποιον κρυπταναλυτή, οι κβαντικές μηχανές μας προσφέρουν τη δυνατότητα αυτή παράγοντας κλειδιά με τυχαία σειρά, αλλά με αδύνατο από την πλευρά μας τον υπολογισμό της εντροπίας, που υπάρχει από μια γεννήτρια τυχαίων αριθμών, [1]

2.3. ΠΕΡΙΟΡΙΣΜΟΙ ΚΛΑΣΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Στη σύγχρονη κρυπτογραφία είναι απαραίτητο να κρατηθεί μυστικό το μήνυμα που μοιράζεται μεταξύ των νόμιμων χρηστών του πρωτοκόλλου και να μην είναι προσβάσιμο από κάποιο τρίτο πρόσωπο. Δεν υπάρχει καμία αποδεδειγμένα ασφαλής κρυπτογραφική μέθοδος, ώστε κάποιος αντίπαλος να είναι σε θέση να σπάσει το κλασσικό πρωτόκολλο, [6]

Οι κρυπτογραφικές μέθοδοι δημοσίου κλειδιού, αποτελούν μέχρι σήμερα την περισσότερο χρησιμοποιούμενη κλασσική λύση στο πρόβλημα διανομής κλειδιού. Ωστόσο, αυτές οι μέθοδοι έχει αποδειχθεί ότι είναι μόνο υπολογιστικά ασφαλείς. Η ασφάλειά τους βασίζεται στην παρούσα αδυναμία να λυθούν συγκεκριμένα δύσκολα μαθηματικά προβλήματα. Όμως, αυτά τα προβλήματα δεν έχει αποδειχθεί ότι είναι άλυτα. Επομένως, κάποιος αλγόριθμος που θα έβρισκε τη λύση, θα ακύρωνε την ασφάλεια των επί του παρόντος συστημάτων, [6]

3. ΚΒΑΝΤΙΚΗ ΜΗΧΑΝΙΚΗ

3.1. ΕΙΣΑΓΩΓΗ

Η κβαντική μηχανική αναπτύχθηκε στα μέσα του 20ού αι. μ.Χ., αλλά άρχισε να βρίσκει εφαρμογές έναν μόλις αιώνα αργότερα. Πρόκειται για έναν αχανή κλάδο της φυσικής με ιδιαίτερα αξιοσημείωτες δυνατότητες, που διαρκώς μελετάται και επεκτείνεται. Η ανάγκη ύπαρξής της έγινε σαφής, όταν η νευτώνεια φυσική αδυνατούσε να περιγράψει κάποια φαινόμενα.

Πιο συγκεκριμένα η κβαντομηχανική μελετάει τη συμπεριφορά της ύλης σε μοριακό, ατομικό και υποατομικό επίπεδο. Η κβαντομηχανική είναι πιο θεμελιώδης από την κλασική μηχανική, καθώς είναι σε θέση να δώσει εξήγηση σε φαινόμενα που η δεύτερη δεν μπορεί.

Τέτοια φαινόμενα είναι:

- Ο κυματοσωματιδιακό δυισμός, η εμφάνιση δηλαδή κυματικής συμπεριφοράς των σωματιδίων, κυρίως ηλεκτρόνιων.
- Η κβαντοσηράγγωση(φαινόμενο σήραγγας), το φαινόμενο κατά το οποίο ένα κβαντικό σωματίδιο ξεπερνάει το φράγμα δυναμικού κάποιας περιοχής, το οποίο φαινομενικά είναι αδύνατο να ξεπεραστεί, με περισσότερη ενέργεια από αυτή που έχει το σωματίδιο. Το φαινόμενο αυτό εξηγείται μέσα από την εξίσωση του Σρέντιγκερ(Schrödinger).
- Η κβάντωση, ή αλλιώς η διακριτοποίηση φυσικών μεγεθών, όπως η περιγραφή της κίνησης σωματιδίων σε ορισμένες ενεργειακές τροχιές.
- Ο κβαντική διεμπλοκή (κβαντικός εναγκαλισμός), φαινόμενο που περιγράφει την κατάσταση ενός συστήματος δύο ή περισσότερων σωματιδίων, που αλληλεπιδρούν αθροίζοντας τις κυματοσυναρτήσεις τους και μένοντας σε κατάσταση διεμπλοκής μεταξύ τους, ανεξαρτήτως του χώρου που μεσολαβεί μεταξύ τους. Το φαινόμενο αυτό θα εξηγηθεί εκτενέστερα σε επόμενη παράγραφο.

Η κβαντομηχανική αν και αμφισβητήθηκε από τον Άλμπερτ Αϊνστάιν με τα λόγια «ο Θεός δεν παίζει ζάρια», εδώ και έναν αιώνα δεν έχει διαψευστεί σε καμία της θεωρία. Βρίσκεται πίσω από πολλά προβλήματα που έως τώρα παρέμεναν άλυτα, και

είναι σε θέση να εξηγήσει χημικά φαινόμενα, αλλά και τη φυσική στερεάς κατάστασης.

3.2. Το Qubit

Στην επιστήμη των υπολογιστών, ως στοιχειώδης μονάδα πληροφορίας είναι το bit. Είναι μία μεταβλητή που αναπαριστά την ποσότητα της πληροφορίας που μπορεί να αποθηκευτεί σε ένα φυσικό σύστημα και μπορεί να λάβει δύο διακριτές τιμές, το 1 και το 0, ανάλογα με την ύπαρξη ρεύματος ή μη σε ένα τρανζίστορ, αντίστοιχα.

Στους κβαντικούς υπολογιστές ωστόσο, η στοιχειώδης μονάδα της κβαντικής πληροφορίας είναι το Qubit (Quantum Bit). Ειδοποιός διαφορά του από το bit, είναι ότι εκείνο μπορεί να λάβει τιμές που είναι άθροισμα των 0 και 1 (Κβαντική Υπέρθεση). Η Κβαντική Υπέρθεση ορίζει την ικανότητα του qubit να λάβει ταυτόχρονα ένα συνδυασμό καταστάσεων που συνυπάρχουν μεταξύ του. Η τελική τιμή που θα έχει λάβει το qubit είναι ένας συνδυασμός των πιθανοτήτων ύπαρξης του 0 και του 1, που αθροιστικά θα δίνουν τη μονάδα. Οι καταστάσεις αυτές συμβολίζονται με $|0\rangle$ και $|1\rangle$ και περιγράφουν το spin ενός σωματιδίου (π.χ. ηλεκτρόνιο), αν αυτό είναι «πάνω» ή «κάτω» αντίστοιχα.

Μιας και το Qubit δεν λαμβάνει διακριτές τιμές, αλλά είναι ένας συνδυασμός δύο καταστάσεων, αξίζει να αναφέρουμε τη σχέση που συνδέει τις δύο τιμές:
Δεδομένου ότι $|\alpha|^2 + |b|^2 = 1$,

$$1\ qubit = a \cdot |1\rangle + b \cdot |0\rangle \qquad (3.1)$$

Με α, b να αποτελούν τις πιθανότητες να συμβεί το 1 και το 0 αντίστοιχα, [14]

Αξίζει να αναφέρουμε ότι οι συμβολισμοί « ⟨| » και « |⟩ » δεν είναι τυχαίοι. Το πρώτο σύμβολο ονομάζεται bra, ενώ το δεύτερο ket. Το bra υποδηλώνει έναν πίνακα-γραμμή και το ket ένα πίνακα-στήλη, των οποίων το εσωτερικό γινόμενο (braket) $\langle\alpha|\alpha\rangle = |\alpha|^2$ είναι πραγματικός αριθμός.

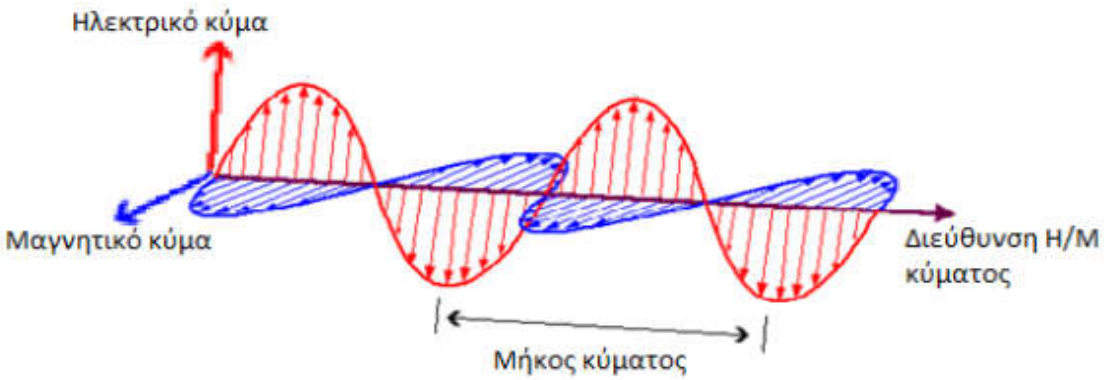
3.3. ΤΟ ΦΩΤΟΗΛΕΚΤΡΙΚΟ ΦΑΙΝΟΜΕΝΟ

Η φύση του φωτός απασχολούσε για αιώνες τους φυσικούς μέσα από έντονες διαμάχες. Τέλος στις διαμάχες αυτές έδωσε ο James Clerk Maxwell μέσα από τις εξισώσεις που περιέγραφαν τα κύματα που απαρτίζουν το φως στην Θεωρία Πεδίων των μαθηματικών.

Ο Maxwell αναφέρει ότι το φως αποτελείται από δύο πεδία, ένα ηλεκτρικό και ένα μαγνητικό, κάθετα μεταξύ τους όσον αφορά τα διανύσματα της έντασής τους, με το ένα να αποσβαίνει το άλλο.

Τα ηλεκτρικά κύματα του φωτός αποτελούνται από φωτόνια, η ένταση των οποίων ταλαντώνεται σε συγκεκριμένο επίπεδο στο οποίο ανήκει η ευθύγραμμη πορεία του φωτός. Η πόλωση του φωτός είναι το φαινόμενο κατά το οποίο τα φωτόνια ταλαντώνονται στο ίδιο επίπεδο και το φως αυτό ονομάζεται πολωμένο, [7]

Όπως έχει ήδη αναφερθεί, το φως παρουσιάζει κυματικές αλλά και σωματιδιακές ιδιότητες. Ωστόσο σε αντίθεση με την κλασική φυσική, στην κβαντομηχανική η εκδήλωση της κυματικής φύσης του φωτός είναι πιθανοκρατική και δεν αναιρεί την άλλη φύση του, [11]



Εικόνα 3.3.1. Το Ηλεκτρομαγνητικό Κύμα και η διπλή του φύση

Οι μελέτες του Maxwell έδωσαν απάντηση σε πολλά ερωτηματικά που είχαν γεννηθεί για το φως ως τότε, ωστόσο ερχόταν σε αντίθεση με πειραματικές ενδείξεις που υπήρχαν σε ορισμένες περιπτώσεις, όπως αυτή του φωτοηλεκτρικού φαινομένου.

Το φωτοηλεκτρικό φαινόμενο περιγράφει την εξαναγκασμένη εκπομπή ηλεκτρονίων από μεταλλική επιφάνεια, μετά από πτώση ηλεκτρομαγνητικής ακτινοβολίας σε αυτήν. Για παράδειγμα αν ακτινοβολήσουμε ένα κλειστό κύκλωμα με ακτίνες Χ, τα εξωτερικά ηλεκτρόνια των ατόμων του κυκλώματος απορροφούν την ενέργεια των ακτινών, αυξάνουν την ενέργειά τους, με αποτέλεσμα να διαφεύγουν από τα άτομα και να τα μετατρέπουν σε ιόντα, πράγμα το οποίο μεταφράζεται σε ρεύμα στο κύκλωμα.

Σύμφωνα με την κλασική φυσική, το παραγόμενο ρεύμα θα αυξάνεται ανάλογα με την ένταση του φωτός που προσπίπτει στην μεταλλική επιφάνεια. Πειραματικά ωστόσο, το ρεύμα εξαρτάται μόνο από τη συχνότητα του φωτός και όχι την έντασή του. Το φαινόμενο που προαναφέρθηκε, έρχεται να εξηγήσει η αρχή του δυισμού, σύμφωνα με την οποία οι δύο φύσεις του φωτός εκδηλώνονται διαφορετικά ανάλογα με τις συνθήκες.

Ο Max Planck είχε αναφέρει ότι η ενέργεια του φωτός εκπέμπεται και απορροφάται μόνο σε κβάντα ενέργειας $\hbar$*ν ($\hbar$ = σταθερά του Planck). Στηριζόμενος σε αυτή την άποψη ο Einstein, μπόρεσε να εξηγήσει το φωτοηλεκτρικό φαινόμενο ισχυριζόμενος ότι το φως μεταδίδεται σε κβάντα με σωματιδιακή υπόσταση. Στη σύγχρονη Φυσική, τα κβάντα φωτός ονομάζονται φωτόνια, με μηδενική μάζα και spin 1, [8]

3.4. Η ΑΡΧΗ ΤΗΣ ΣΥΜΠΛΗΡΩΜΑΤΙΚΟΤΗΤΑΣ - ΤΟ ΠΑΡΑΔΟΞΟ EPR

Η κβαντομηχανική εξ' αρχής δεχόταν κριτικές από την επιστημονική κοινότητα. Η τυχαιότητα πάνω στην οποία θέτει τις βάσεις της επικρίθηκε από πολλούς, αλλά κυρίως μέσα από μια εργασία που δημοσίευσαν οι Einstein, Podolsky και Rosen(EPR).

Στη συγκεκριμένη εργασία τίθεται ως δεδομένο, η ύπαρξη πηγής που εκπέμπει ζεύγη φωτονίων. Τα ζεύγη αυτά είναι συνδυασμός ενός σωματίου-αντισωματίου. Μέσα από την αρχή διατήρησης της στροφορμής, ισχύει ότι η συνολική στροφορμή που θα έχει το σύστημα των δύο φωτονίων θα πρέπει να είναι ίση με την αρχική, δηλαδή ίση με μηδέν.

Πριν συνεχίσουμε θα αναφερθούμε στην Αρχή της Συμπληρωματικότητας (Ερμηνεία της Κοπεγχάγης), απαραίτητη προϋπόθεση για να κατανοήσουμε την ύπαρξη του παραδόξου EPR. Μόλις το 1927, πολύ πριν την διατύπωση της αρχής της απροσδιοριστίας του Heisenberg, ο Niels Bohr σε συνέδριο στο Κόμο της Ιταλίας, εκφράζει για πρώτη φορά τις ιδέες του για τη συμπληρωματικότητα στον κβαντικό μικρόκοσμο. Ο Bohr παρατηρεί ότι η παρατήρηση ενός συστήματος δε μπορεί να γίνει χωρίς τη διατάραξή του, πράγμα το οποίο ερχόταν σε αντίθεση με ότι ίσχυε έως τότε. Τέσσερα χρόνια νωρίτερα, ο Bohr είχε εισάγει την αρχή της συμπληρωματικότητας, σύμφωνα με την οποία οποιοδήποτε συστατικό στο περιβάλλον, παρουσιάζει σωματιδιακό και κυματικό χαρακτήρα και εξαρτάται από τον παρατηρητή το ποια από τις δύο αυτές φύσεις βλέπει και πότε. Το δόγμα αυτό του Bohr έχει φιλοσοφική φύση και δεν είναι καλώς καθορισμένο, γεγονός που αιτιολογεί ως ένα βαθμό τις αμφισβητήσεις που δέχτηκε στην πορεία. Θα ήταν εσφαλμένο το γεγονός να καταλήξουμε στο συμπέρασμα, ότι ο Bohr στήριξε τις απόψεις του με φιλοσοφικά επιχειρήματα, αφού όλες του οι παρατηρήσεις απορρέουν από την κβαντομηχανική και συνοδεύονται από πειραματική απόδειξη, [8]

Από τους στοχασμούς του Bohr τελικά, απορρέει το εξής ερώτημα: «Πώς θα μπορούσαμε να γνωρίζουμε ανά πάσα ώρα την κατάσταση του συστήματος;», το οποίο οδηγεί και στην εισαγωγή της αρχής της συμπληρωματικότητας. Ο ίδιος της έδωσε τον εξής ορισμό το Φθινόπωρο του 1927: «*κάθε δεδομένη εφαρμογή των κλασικών εννοιών, καθιστά αδύνατη την ταυτόχρονη χρήση άλλων κλασικών εννοιών, οι οποίες σε διαφορετική συνάφεια είναι εξίσου αναγκαίες για την ακριβή γνώση των φαινομένων*», [9]

Η αρχή της συμπληρωματικότητας αποτέλεσε βάση για την μετέπειτα εξέλιξη της κβαντικής μηχανικής, για αυτό το λόγο καθιερώθηκε αργότερα από τη σχολή της Κοπεγχάγης και ως ερμηνεία της κβαντικής μηχανικής. Πολλοί διάσημοι φυσικοί της εποχής, ανάμεσά τους και οι Heisenberg και Pauli, υποστήριξαν την αρχή της συμπληρωματικότητας, περισσότεροι ωστόσο την κατέκριναν και συγκεκριμένα αυτοί που βρίσκονταν εκτός της σχολής της Κοπεγχάγης. Συγκεκριμένα στην Αμερική οι απόψεις του Bohr, θεωρήθηκαν καθαρά φιλοσοφικές και μη χρήσιμες για την επίλυση μαθηματικών εξισώσεων και υπολογισμών, που τους ταλάνιζαν επί δεκαετίες. Ακόμα όμως και στην Γερμανία αλλά και τη Δανία, ενώ υπήρχαν αρκετοί υποστηρικτές της θεωρίας του Bohr, υπήρχε δισταγμός από τη μεριά τους να

συμπεριλάβουν την συμπληρωματικότητα στα εγχειρίδιά τους. Δεν θα έπρεπε να μας προκαλεί εντύπωση η συμπεριφορά αυτή της επιστημονικής κοινότητας, η οποία είχε μόλις εκτεθεί σε μια νέα διάσταση, αντίθετη και ασυμβίβαστη με την τρέχουσα πραγματικότητα. Η αποδοχή θα έρθει πολλά χρόνια μετέπειτα, με πρώτο επίτευγμα αυτό της καθιέρωσης της ερμηνείας της Κοπεγχάγης, ως βασική αρχή της κβαντικής μηχανικής μία δεκαετία αργότερα, το 1930, [8]

Όπως προαναφέρθηκε στην αρχή της παραγράφου, μεγάλοι διώκτες της αρχής της συμπληρωματικότητας υπήρξαν οι Einstein, Podolsky και Rosen, αν και στην ιστορία έμεινε γνωστός για τη διαμάχη του με τον Bohr ο Einstein. Αν και η συμπληρωματικότητα είχε μεγάλη επιρροή από τις θεωρίες του Einstein που αναπτύχθηκαν στην 20ετία 1905 έως 1925, εκείνος αδυνατούσε να αποδεχτεί ότι ο μικρόκοσμος περιγράφεται μόνο στατιστικά, περισσότερο για φιλοσοφικούς παρά για επιστημονικούς λόγους. Σε επιστολή του το 1927 προς τον Bohr αναφέρει πως μια φωνή μέσα του, τού έλεγε ότι η κβαντική μηχανική μας απομακρύνει από τον Ύψιστο, μιας και Εκείνος δεν παίζει ζάρια.

Ακολούθησε πλήθος αντιπαραθέσεων ανάμεσα στους δύο επιστήμονες αλλά και άλλων μη υποστηρικτών της Αρχής της Κοπεγχάγης στα επόμενα χρόνια σε συνέδρια. Ωστόσο μέσα από τις προσπάθειες του Einstein να καταρρίψει τις θεωρίες του Bohr επικαλούμενος δικές του εξισώσεις (τις ίδιες που χρησιμοποίησε και ο Bohr), ο δεύτερος κατάφερνε να βγαίνει πάντοτε νικητής, ενισχύοντας ολοένα και περισσότερο τη μποριανή αντίληψη της κβαντομηχανικής.

Ο Einstein παρά τις απανωτές του ήττες συνέχισε να ψάχνει για κενά στη θεωρία του Bohr. Η συντριπτική του πανωλεθρία ωστόσο ήρθε το 1935, με την δημοσίευση της διάσημης εργασία με τίτλο «Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? (Μπορεί να θεωρείται πλήρης η κβαντομηχανική περιγραφή της φυσικής πραγματικότητας;)» που έγραψε ο Einstein μαζί με τους Boris Podolsky και Nathan Rosen(EPR). Στην εργασία τους αναφέρουν ότι η περιγραφή της πραγματικότητας με την κβαντομηχανική δεν είναι πλήρης, με επιχειρήματα που θα αναλυθούν στην παράγραφο 3.5. Μόλις πέντε μήνες αργότερα, ο Bohr παρουσιάζει αντεπιχείρημα στην εργασία των τριών επιστημόνων καταρρίπτοντάς την.

Παρά τη διασημότητα που έλαβε η εργασία των EPR δεν ήταν αρκετή για να στρέψει την επιστημονική κοινότητα ενάντια στον Bohr, αντίθετα ολοένα και

περισσότεροι φυσικοί άρχισαν να ασχολούνται περισσότερο με αρχή της συμπληρωματικότητας.

Αξίζει να αναφέρουμε ότι ο Bohr τόνισε ότι η κβαντική θεωρία δεν περιγράφει τον μικρόκοσμο, αλλά τον τρόπο που αυτός εμφανίζεται κατά την παρατήρησή του, όσο εκείνος αλληλεπιδρά με τον παρατηρητή. Η κλασική Φυσική αδυνατεί να περιγράψει τα υποατομικά αντικείμενα και για αυτό το λόγο έρχεται η Κβαντομηχανική να τα εξηγήσει επαρκώς. Ωστόσο σε αυτή την εξήγηση δημιουργούνται ερωτήματα για το λεπτό σημείο ανάμεσα στην επιστήμη και την πραγματικότητα. Για παράδειγμα σε υποατομικό επίπεδο τα σωματίδια όπως έχουμε προαναφέρει συμπεριφέρονται άλλοτε ως κύματα και άλλοτε ως σωμάτια. Μέσα όμως από τις κατάλληλες μαθηματικές εξηγήσεις και τις θεωρίες που πρότεινε ο Bohr, αλλά και άλλοι επιστήμονες στη συνέχεια, αναιρείται το παράδοξο που προκύπτει από το δυισμό κυμάτων και σωματιδίων, [8]

3.5. ΚΒΑΝΤΙΚΗ ΔΙΕΜΠΛΟΚΗ

Δύο ή περισσότερα σωματίδια των οποίων οι κυματοσυναρτήσεις είναι σε κατάσταση διεμπλοκής, ανεξαρτήτως του διαστήματος που υπάρχει άναμεσά τους, λέμε ότι βρίσκονται σε κβαντική διεμπλοκή. Παρατηρείται μάλιστα, ότι αν απομακρύνουμε το ένα σε άπειρη απόσταση από το άλλο, το εναπομείναν θα αντιδράσει, μαρτυρώντας έτσι πως η πληροφορία ταξιδεύει με άπειρη ταχύτητα. Μάλιστα στο σύστημα των σωματιδίων, υπάρχουν τόσο έντονες αλληλεπιδράσεις, που αν επιχειρήσουμε να εξετάσουμε τις ιδιότητες του ενός, επηρεάζονται άμεσα οι ιδιότητες του άλλου, ακόμα και αν απέχουν μεγάλες αποστάσεις.. Η κβαντική διεμπλοκή έχει αποδειχτεί πειραματικά και παρατηρείται όχι μόνο στο μικρόκοσμο αλλά και σε ευρύτερες κλίμακες. Σημαντικό επίτευγμα αποτελεί η πρώτη απεικόνιση του κβαντικού εναγκαλισμού δύο φωτονίων τον Ιούλιο του 2019 από ερευνητές του Πανεπιστημίου της Γλασκώβης, [12]

Εικόνα 3.5.1. Η πρώτη απεικόνιση της κβαντικής διεμπλοκής. Ιούλιος 2019

Όπως προαναφέρθηκε σε προηγούμενη παράγραφο, ο Einstein, ο Podolsky και ο Rosen στην εργασία τους, χαρακτήρισαν την αρχή της παραλληλίας ως ημιτελή. Οι ίδιοι εξέφρασαν αυτή την άποψη στηριζόμενοι στο γεγονός ότι σύμφωνα με την κβαντομηχανική, παραδεχόμαστε ότι τα διαπλεγμένα σωματίδια λειτουργούν ως ενιαίο σύνολο στο οποίο εκείνα αλληλεπιδρούν παρά τις αποστάσεις που έχουν μεταξύ τους. Πιο συγκεκριμένα, τόνισαν ότι χρειάζονται κι άλλες αποδείξεις για να καταλήξουμε σε αυτό το συμπέρασμα για τα διαπλεγμένα σωματίδια, γεγονός που συνέβη λίγα μόλις χρόνια αργότερα με τις προόδους που έγιναν στη φυσική και τα μαθηματικά, σε θεωρητικό αλλά και πειραματικό επίπεδο.

Ο Einstein αδυνατούσε να πιστέψει ότι υπάρχει κάτι γρηγορότερο στη φύση από την ταχύτητα του φωτός. Αναρωτιόταν μάλιστα αν οι ιδιότητες των κβαντικών σωματιδίων είναι πραγματικές ή απλά είναι δημιούργημα της ανθρώπινης αντίληψης. Απάντηση στην εύλογη παρατήρησή του έδωσαν το 2008 επιστήμονες του Πανεπιστημίου της Γενεύης σε πείραμά τους, στο οποίο πραγματοποιούσαν αλλαγές σε ένα φωτόνιο 18 χιλιόμετρα μακριά από το διαπλεγμένο σε αυτό φωτόνιο. Αποτέλεσμα του πειράματος ήταν να αποδειχτεί ότι σε αυτή την απόσταση, το δεύτερο φωτόνιο άλλαξε την κατάστασή του και ταυτίστηκε με το αρχικό, με ταχύτητα 10.000 φορές γρηγορότερα από την ταχύτητα του φωτός, [13]

Η κβαντική διεμπλοκή βρίσκει ιδιαίτερη χρησιμότητα στους κβαντικούς υπολογιστές, καθώς με τη βοήθειά της εκτελούνται πολύπλοκοι κβαντικοί υπολογισμοί. Για να καταλάβουμε ένα μέρος της χρησιμότητάς της, θα θεωρήσουμε δύο ζεύγη κβαντικών συστημάτων, στην περίπτωσή μας δύο Qubits. Από τα δύο αυτά ζεύγη μόνο το δεύτερο θα βρίσκεται σε κατάσταση διεμπλοκής. Αν μετρήσουμε την

κατάσταση του πρώτου συστήματος και πάρουμε |1⟩, τότε το δεύτερο σύστημα θα δώσει κατά 50% την κατάσταση |0⟩ ή ισοπίθανα |1⟩. Αν μετρήσουμε όμως την κατάσταση του δεύτερου συστήματος, θα διαπιστώσουμε ότι παίρνουμε στην πρώτη μέτρηση. Συνεπώς αποδεικνύεται ότι οι μετρήσεις αλληλοεπηρεάζονται. Το παράδειγμα που προηγήθηκε αποτελεί πραγματική εφαρμογή του φαινομένου στους κβαντικούς καταχωρητές, [2]

Αν θέλουμε να περιγράψουμε την κβαντική διεμπλοκή με μαθηματικό τρόπο, μπορούμε να πούμε ότι δυο κβαντικά συστήματα βρίσκονται σε διεμπλοκή όταν η κατάστασή τους δεν μπορεί να γραφτεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων. Πιο συγκεκριμένα για καταστάσεις $q_{\text{όχιΔιεμπλοκή}}$, q_2 , q_3 συστημάτων που δεν βρίσκονται σε διεμπλοκή, ισχύει:

$$\left| q_{\text{όχιΔιεμπλοκή}} \right\rangle = \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle) =$$

$$= |1\rangle \otimes \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\right]$$

$$= |q2\rangle \otimes |q3\rangle, \qquad (3.2)$$

όπου $q_2 = |1\rangle$, και $q_3 = \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\right]$.

Μελετώντας την παραπάνω σχέση διαπιστώνουμε ότι η κατάσταση q_2 έχει 50% πιθανότητες για να βρεθεί και πάλι σε |1⟩, ή εναλλακτικά σε |0⟩. Συνεπώς η μέτρηση δεν επηρεάζεται. Στην περίπτωση όμως που τα συστήματα βρίσκονται σε διεμπλοκή, θα ισχύει:

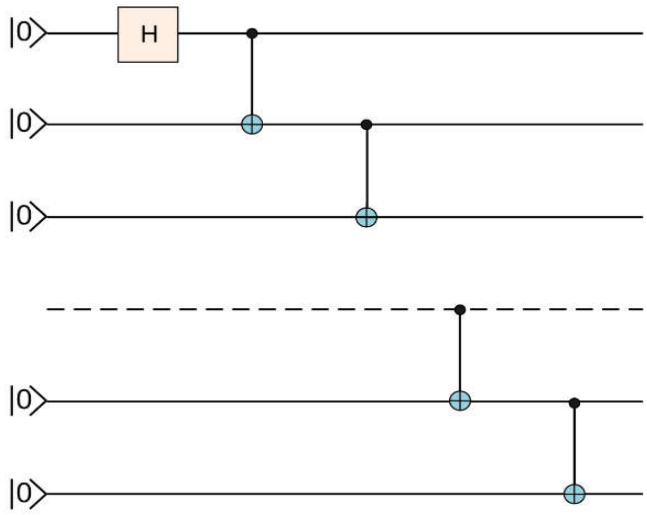
$$| q_{\text{διεμπλοκή}} \rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), \qquad (3.3)$$

όπου $q_2 = \left[\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)\right]$, και $q_3 = |11\rangle$

Διαπιστώνουμε από τη σχέση (3.3) ότι όταν το $|q_3\rangle$ είναι |1⟩, το $|q_2\rangle$ μετατρέπεται αυτόματα σε |0⟩, [18]

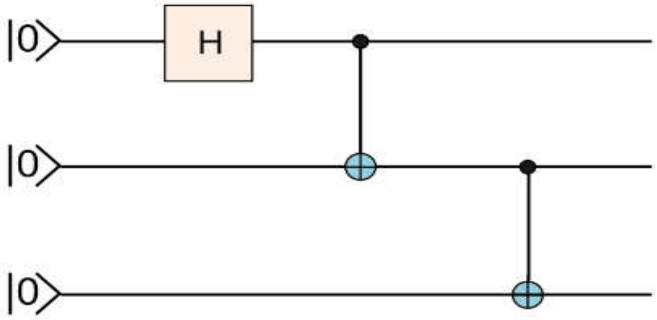
Υπάρχουν πολλοί τρόποι για να φέρει κάποιος δύο συστήματα σε κατάσταση διεμπλοκής μεταξύ τους. Δύο από αυτούς είναι με τη βοήθεια κβαντικών κυκλωμάτων, και μέσα από κβαντικούς μετασχηματισμούς Fourier.

Στην πρώτη περίπτωση γίνεται χρήση κβαντικών κυκλωμάτων και στην εικόνα που έπεται είναι το συγκεντρωτικό κβαντικό κύκλωμα για την κβαντική διεμπλοκή οποιουδήποτε αριθμού qubits.



Εικόνα 3.5.2. Κβαντικό κύκλωμα για την κβαντική διεμπλοκή οποιουδήποτε αριθμού qubits

Ουσιαστικά δηλαδή μπορούμε να φέρουμε σε κατάσταση κβαντικής διεμπλοκής περισσότερες καταστάσεις των qubits, με τη χρήση κβαντικών πυλών H και CNOT. Στο ακόλουθο σχήμα φαίνεται ένα κβαντικό κύκλωμα, που φέρνει σε κατάσταση κβαντικής διεμπλοκής τρία qubits.

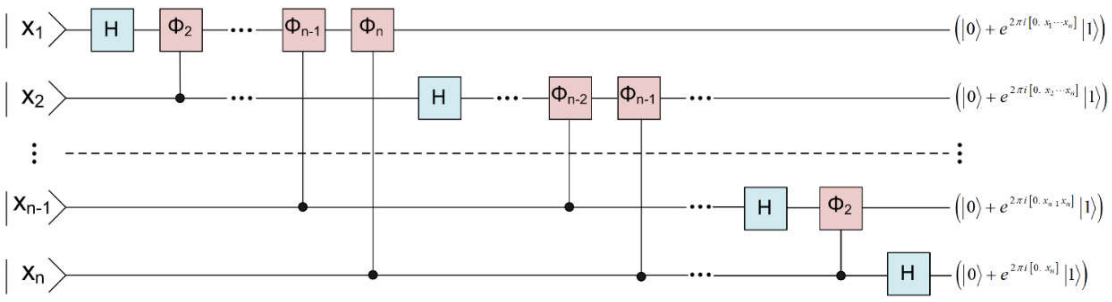


Εικόνα 3.5.3. Κύκλωμα που φέρνει σε κβαντική διεμπλοκή 3 qubits

Ο κβαντικός υπολογισμός που περιγράφεται από αυτό το κύκλωμα είναι:

$$(I \otimes CNOT)(CNOT \otimes I)(H \otimes I \otimes I)|000\rangle = 1/\sqrt{(2(|000\rangle + |111\rangle)} \quad (3.4)$$

Όπως προαναφέρθηκε, ένας άλλος δημοφιλής τρόπος να φέρουμε συστήματα σε κβαντική διεμπλοκή, είναι με τη χρήση κβαντικών μετασχηματισμών Fourier. Ο κβαντικός μετασχηματισμός Fourier δρα σε ένα qubit με τον ίδιο τρόπου που δρα η πύλη H. Αυτός είναι και ο λόγος που η πύλη Hadamard (Πύλη H), λέγεται και «μετασχηματισμός Hadamard». Στην εικόνα 3.5.2 δόθηκε ένα συγκεντρωτικό κβαντικό κύκλωμα για τη διεμπλοκή δυο συστημάτων. Αντίστοιχο κύκλωμα για τον κβαντικό μετασχηματισμό Fourier απεικονίζεται στην εικόνα 3.5.4, [18]



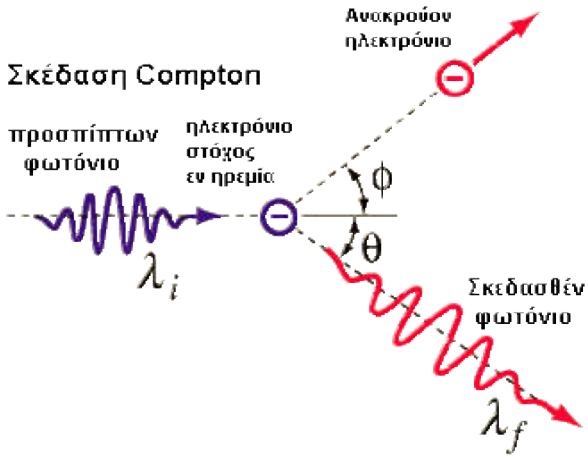
Εικόνα 3.5.4. Το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier

3.6. ΤΟ ΦΑΙΝΟΜΕΝΟ COMPTON

Το 1985 ο Wilchelm Rontgen, ανακάλυψε τις ακτίνες Χ. Ο μηχανισμός παραγωγής τους είναι ο αντίστροφος του φωτοηλεκτρικού φαινομένου, στο οποίο μια μεταλλική επιφάνεια βομβαρδίζεται με ηλεκτρομαγνητικό κύμα και εκπέμπει ηλεκτρόνια, ενώ στις ακτίνες Χ η επιφάνεια βομβαρδίζεται με ηλεκτρόνια και εκπέμπει ηλεκτρομαγνητικό κύμα, [15]

Μόλις το 1922 ο Arthur Compton, απέδειξε ότι η Κλασική Φυσική δεν επαρκούσε να ερμηνεύσει τη σκέδαση των ακτινών Χ. Σύμφωνα με τις ισχύουσες απόψεις τότε, όταν η ηλεκτρομαγνητική ακτινοβολία προσπίπτει με μια συχνότητα f_o σε ένα ελεύθερο ηλεκτρόνιο που ταλαντώνεται αρμονικά, η δευτερογενής ακτινοβολία που προκύπτει από τη σκέδαση, θα έχει ίδια συχνότητα με την αρχική. Ωστόσο η άποψη αυτή, όπως παρατήρησε ο Compton, δεν ισχύει πειραματικά. Ο ίδιος διαπίστωσε ότι η δευτερογενής ακτινοβολία, είχε μικρότερη συχνότητα από την αρχική f_o, ενώ παράλληλα έδειξε ότι το μήκος κύματος των σκεδαζόμενων ακτινών, εξαρτιόταν μόνο από η γωνία πρόσπτωσης τους και όχι από το χρόνο έκθεσης του υλικού στην ακτινοβολία και την έντασή της, [10]

Εξήγηση στο φαινόμενο αυτό έδωσε η Κβαντική Θεωρία και η Ειδική Θεωρία της Σχετικότητας. Στο σχήμα που ακολουθεί βλέπουμε το πείραμα που εκτέλεσε ο Compton, το οποίο απέδειξε για ακόμα μια φορά τη σωματιδιακή φύση της ακτινοβολίας, ορατής και μη, καθώς και την ύπαρξη των φωτονίων:



Εικόνα 3.6.1. Σκέδαση Compton

4. ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

4.1. ΕΙΣΑΓΩΓΗ

Σε προηγούμενο κεφάλαιο έχουν τονιστεί οι περιορισμοί που τίθενται από το κλασικό σύστημα κρυπτογραφίας, όσον αφορά την ασφάλεια που παρέχει. Με την ολοένα αυξανόμενη πρόοδο της τεχνολογίας, η ασφάλεια δέχεται πλήγματα από κακόβουλες επιθέσεις, με αποτέλεσμα να βρίσκονται εκτεθειμένες σε κινδύνους τραπεζικές συναλλαγές, διπλωματικά δίκτυα, ασύρματα δίκτυα και άλλες μεταφορές της πληροφορίας.

Με την ανάπτυξη της Κβαντικής Μηχανικής ωστόσο, βρέθηκαν τομείς της Επιστήμης των Υπολογιστών στους οποίους θα μπορούσε να συνεισφέρει. Ένας τέτοιος κλάδος είναι αυτός της Κρυπτογραφίας, στον οποίο η κβαντομηχανική έχει αρχίσει να βρίσκει πρόσφορο έδαφος για να εξαπλωθεί.

Η κβαντική κρυπτογραφία εκμεταλλεύεται τις ιδιότητες ενός φυσικού συστήματος, για να δημιουργήσει ένα κλειδί κρυπτογράφησης, με τη βοήθεια του οποίου θα εξασφαλίζεται η μέγιστη ασφάλεια του καναλιού επικοινωνίας των δύο πλευρών. Τι είναι αυτό που διαχωρίζει την επικοινωνία αυτή από μία που προστατεύεται από κλασικές μεθόδους κρυπτογράφησης; Είναι ότι στην πρώτη περίπτωση, οι μετέχοντες στην επικοινωνία είναι σε θέση να αναγνωρίσουν αν κάποιος υποκλέπτει το κανάλι τους και μάλιστα να τον βγάλουν ξανά εκτός του καναλιού, πετυχαίνοντας ξανά μια ασφαλή επικοινωνία.

Συνεπώς, η μοναδική διαφορά των δύο μεθόδων κρυπτογράφησης, κλασικής και κβαντικής, έγκειται μόνο στον τρόπο παραγωγής του κλειδιού και στην ικανότητα των μετεχόντων να αναγνωρίσουν τις υποκλοπές. Η μεταφορά της πληροφορίας γίνεται και στις δύο περιπτώσεις με τον ίδιο τρόπο και οι αλγόριθμοι που χρησιμοποιούνται μπορεί προαιρετικά να είναι οι ίδιοι, [8]

4.2. ΚΒΑΝΤΙΚΗ ΠΛΗΡΟΦΟΡΙΑ - ΚΒΑΝΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

Σήμερα στον κλάδο της Θεωρίας Πληροφορίας και συγκεκριμένα στην Κβαντική Πληροφορία, οι επιστήμονες αναζητούν τη σχέση που υπάρχει ανάμεσα στην κλασική και στη κβαντική πληροφορία, ψάχνουν δηλαδή το σύνδεσμο που ενώνει αυτές τις τόσο διαφορετικές φύσεις.

Με γνώμονα τις γνώσεις γύρω από την κβαντική διεμπλοκή, οι επιστήμονες ανακάλυψαν ότι η διαχείριση της κβαντικής πληροφορίας είναι ανάλογη της διαθέσιμης διεμπλοκής που έχει ένα σύστημα. Πιο συγκεκριμένα παρατήρησαν ότι διάφορα συστήματα έχουν μικρή διεμπλοκή και άλλα μεγάλη, πράγμα το οποίο επηρεάζει το πόσο κατάλληλα είναι για τη διαχείριση της πληροφορίας.

Αυτές οι ανακαλύψεις έχουν οδηγήσει τους επιστήμονες στη δημιουργία νόμων που αφορούν τη διεμπλοκή και αποδείξεων που θα τη θεμελιώνουν. Ανθίζει έτσι αργά αλλά σταθερά, η επιστήμη της κβαντικής πληροφορίας που αναμένεται να φέρει ισχυρές αλλαγές στην επιστήμη της Θεωρίας Πληροφορίας και στην Πληροφορική.

Έχει προαναφερθεί σε προηγούμενο κεφάλαιο ότι οι κβαντικές καταστάσεις περιγράφονται με τη βοήθεια της κβαντική υπέρθεσης. Χαρακτηριστικό της όμως είναι ότι ισχύει μόνο σε μικροσκοπικό επίπεδο, και όσο απομακρυνόμαστε από αυτό και εισερχόμαστε στον μακρόκοσμο, η κβαντική υπέρθεση εξασθενεί. Πιο συγκεκριμένα, η μετάβαση από τον μικρόκοσμο στον μακρόκοσμο, αντιστοιχεί στην αντίστοιχη μετάβαση από το κβαντικό στο κλασικό επίπεδο. Η μετάβαση αυτή συμβαίνει επειδή τα μεγάλα συστήματα αλληλεπιδρούν με το περιβάλλον τους, προκαλώντας την καταστροφή της υπέρθεσης ή αποσυμφωνία (Decoherence), [17]

Η κβαντική αποσυμφωνία είναι η μεγαλύτερη πρόκληση της κβαντικής τεχνολογίας. Οι επιστήμονες καλούνται να παλέψουν με μια φυσική διαδικασία αποτρέποντάς την, γεγονός που είναι πρόκληση και για τη δημιουργία κβαντικών συσκευών με εμπορική αξία, [16]

4.3. ΜΕΘΟΔΟΙ ΚΒΑΝΤΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

4.3.1. ΠΟΛΩΜΕΝΑ ΦΩΤΟΝΙΑ (ΜΕΘΟΔΟΣ BB84)

Υποθέτουμε ένα κβαντικό κανάλι επικοινωνίας με συμμετέχοντες την Alice και τον Bob, των οποίων η σύνδεση κινδυνεύει να υποκλαπεί από την Eve, η οποία αναζητεί το κλειδί.

Στην επικοινωνία αυτή η Alice αποστέλλει στον Bob μέσα από το κανάλι μια ακολουθία qubit, κωδικοποιημένα τυχαία. Η Alice πρακτικά στέλνει ένα σύνολο φωτονίων με συγκεκριμένη πόλωση στον αποδέκτη Bob.

Ο Bob στη συνέχεια λαμβάνει τις πολώσεις των φωτονίων, τις καταγράφει και τις κρατάει κρυφές έως ότου ολοκληρωθεί η αποστολή. Ο Bob στέλνει στην Alice με τη σειρά του τις καταγραφές του από το κλασικό κανάλι, κι εκείνη τις συγκρίνει με τις πρωτότυπες που έστειλε. Από το κλασικό κανάλι και πάλι, η Alice θα ενημερώσει τον Bob ποια qubits ήταν σωστά, και επιλέγονται αυτά για τη δημιουργία του κλειδιού. Αναμένεται περίπου τα μισά qubits να είναι ίσα βάσει πιθανοτήτων, άρα ο Bob αντίστοιχα θα έχει καταγράψει μόνο τις μισές πολώσεις σωστά.

Αν θεωρήσουμε ότι η Eve επιχειρεί να υποκλέψει πληροφορίες στο κβαντικό κανάλι, καταγράφει κι εκείνη όπως και ο Bob, τις πολώσεις των φωτονίων, με το ενδεχόμενο πάντα να κάνει κι αυτή μόνο τις μισές καταγραφές σωστά. Ωστόσο, όπως προβλέπει ο πολλαπλασιαστικός νόμος των πιθανοτήτων, αν στο κανάλι εμπλέκεται και η Eve, ο Bob θα έχει μόνο 25% πιθανότητα για σωστές καταγραφές και όχι 50% όπως προηγουμένως. Έτσι η Alice κατά την σύγκριση των τιμών που έλαβε από τον Bob με τις δικές τις, θα διαπιστώσει την τεράστια απόκλιση που έχουν από τις δικές της και θα αντιληφθεί την παρουσία της Eve.

Θα πρέπει να αναφέρουμε βέβαια ότι οι λάθος τιμές στις μετρήσεις των πολώσεων δεν οφείλονται αποκλειστικά στην Eve, αλλά και στην αλληλεπίδραση του καναλιού επικοινωνίας με το περιβάλλον. Για παράδειγμα, αν η μεταφορά των φωτονίων γίνει μέσα από οπτικές ίνες, πιθανές φθορές που αυτές φέρουν, οδηγούν σε εσφαλμένες τιμές. Βέβαια, η Alice και ο Bob δεν μπορούν να γνωρίζουν εξ' αρχής τέτοιες ανωμαλίες στο κβαντικό κανάλι, και για αυτό υποθέτουν ότι όλα τα σφάλματα οφείλονται στην Eve.

Φυσικά υπάρχει μέθοδος που μπορούν να εφαρμόσουν οι Alice και Bob ώστε να μπορέσουν να δημιουργήσουν κλειδί με ασφάλεια. Η μέθοδος αυτή οδηγεί στην παραγωγή μικρών πανομοιότυπων κλειδιών, είναι αποδοτική στην ενίσχυση της ιδιωτικότητας, αν και δουλεύει εξαιρετικά στην περίπτωση των διαπλεγμένων σωματίων που θα αναλύσουμε αργότερα.

Όλη η διαδικασία που προαναφέρθηκε παραπάνω, είναι μια μέθοδος που προτάθηκε το 1884 από τους Charles H. Bennett και Gilles Brassard και είναι ευρέως γνωστή ως BB84, [8]

4.3.2. ΔΙΑΠΛΕΓΜΕΝΑ ΣΩΜΑΤΙΑ

Επτά χρόνια μετά την παρουσίαση του BB84, ο Artur Ekert προτείνει ένα νέο πρωτόκολλο , αυτό των διαπλεγμένων σωματίων.

Η μέθοδος του Ekert μοιάζει πολύ με το BB84, ωστόσο σε αυτήν την περίπτωση η Alice και ο Bob λαμβάνουν το ένα από τα δύο φωτόνια ενός διαπλεγμένου ζεύγους. Μόλις ολοκληρωθεί το μήνυμα, οι δυο τους θα έχουν από μια ακολουθία bits αντίθετες μεταξύ τους, αν για παράδειγμα η Alice έχει 0101, ο Bob θα έχει NOT(0101) δηλαδή ισοδύναμα 1010.

Στη συνέχεια για κλειδί επιλέγεται μία από τις δύο ακολουθίες μέσω του κλασικού καναλιού. Και στην περίπτωση των διαπλεγμένων σωματίων υπάρχουν κίνδυνοι υποκλοπής αλλά και σφάλματα από το περιβάλλον, σε αντίθεση όμως με το BB84 η μέθοδος αυτή εξασφαλίζει μεγαλύτερα ποσοστά επιτυχούς λήψης της πόλωσης των φωτονίων που έστειλε η Alice, [8]

Το πρωτόκολλο που πρότεινε ο Ekert έγινε γνωστό ως «EPR πρωτόκολλο», καθώς βασίστηκε στο φαινόμενο «παράδοξο EPR» το οποίο εξηγήθηκε σε προηγούμενο κεφάλαιο. Μάλιστα, ο Ekert είναι ο πρώτος που έδωσε πρακτική εφαρμογή σε ένα παράδοξο που έως τότε παρέμενε στη θεωρία, [2]

4.4. ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ - ΑΛΓΟΡΙΘΜΟΙ

4.4.1. ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

Ένας σύγχρονος υπολογιστής δομείται από ένα ηλεκτρικό κύκλωμα, το οποίο με τη σειρά του απαρτίζεται από λογικές πύλες και τις μεταξύ τους συνδέσεις. Οι κβαντικοί υπολογιστές ωστόσο διαθέτουν κβαντικές πύλες.

Οι πύλες που δύναται να υπάρχουν σε έναν απλό υπολογιστή είναι οι AND, OR, NOT, NAND, XOR, XNOR και NOR, ενώ σκοπός τους είναι να διαχειρίζονται την πληροφορία που λαμβάνουν και να τη μετατρέπουν σε μια νέα μορφή.

Οι κατηγορίες στις οποίες διαχωρίζονται οι πύλες, διακρίνονται με βάση τον αριθμό των bits στα οποία δρουν. Με αυτή τη λογική, απλές πύλες είναι αυτές που διαχειρίζονται ένα μόνο bit και στην περίπτωσή μας αυτή είναι μόνο η πύλη NOT. Η λογική πύλη NOT έχει ως ρόλο να αντιστρέφει την κατάσταση ενός bit, δηλαδή από 0 να το μετατρέπει σε 1 και το αντίστροφο. Ωστόσο έχει αναφερθεί προηγουμένως ότι στην κβαντική μηχανική, δεν υπάρχουν οι δύο απόλυτες τιμές 0 και 1 για να αναθέσουμε σε bits, αλλά υπάρχουν και όλες οι ενδιάμεσες κβαντικές καταστάσεις (καταστάσεις επαλληλίας) των bit. Έτσι η μετατροπή ενός qubit το οποίο εισέρχεται μέσα από μία κβαντική πύλη NOT, δεν μπορεί να αντιστοιχιστεί πλήρως με την κλασική περίπτωση.

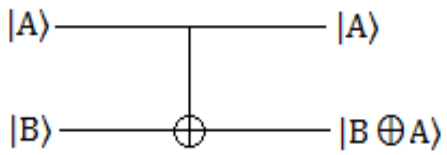
Συνεπώς η κβαντική πύλη NOT εναλλάσσει τους ρόλους των $|0\rangle$ και $|1\rangle$ ώστε να ισχύει:

$$a|0\rangle + b|1\rangle \longrightarrow a|0\rangle + b|1\rangle \qquad (4.1)$$

Χάριν ευκολίας συμβολίζουμε κάθε κβαντική κατάσταση υπό τη μορφή ενός τετραγωνικού πίνακα. Για παράδειγμα η $|y\rangle = a|0\rangle + b|1\rangle$ συμβολίζεται και ως $\binom{a}{b}$. Η μετατροπή του $\binom{a}{b}$ μέσα από μια κβαντική πύλη NOT θα είναι$\binom{b}{a}$. Η σχέση αυτή ικανοποιείται εμφανώς από τον πίνακα $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Αυτό μας οδηγεί στο συμπέρασμα ότι με πίνακα 2x2 μπορούμε να αναπαραστήσουμε κβαντικές πύλες που δρουν σε ένα μόνο qubit.

Οι υπόλοιπες έξι πύλες από αυτές που αναφέρθηκαν στην αρχή της παραγράφου 4.4.1 δρουν σε περισσότερα από ένα bits. Μία κβαντική πύλη που δεν υπάρχει στις

απλές, είναι η CNOT(control-NOT). Η πύλη αυτή διαθέτει δύο εισόδους, το qubit ελέγχου $|A\rangle$ και το qubit στόχος $|B\rangle$. Κυκλωματικά η πύλη CNOT έχει την παρακάτω δομή:



Η λειτουργία της πύλης αυτής είναι να αφήνει ανεπηρέαστη την κατάσταση του qubit στόχου αν η κατάσταση του qubit ελέγχου είναι $|0\rangle$. Αν ωστόσο αυτή είναι $|1\rangle$, τότε η κατάσταση του qubit στόχου αντιστρέφεται, δηλαδή:

$$|00\rangle \longrightarrow |00\rangle \tag{4.2}$$

$$|01\rangle \longrightarrow |01\rangle \tag{4.3}$$

$$|10\rangle \longrightarrow |11\rangle \tag{4.4}$$

$$|11\rangle \longrightarrow |10\rangle \tag{4.5}$$

Η αντιστοίχηση των καταστάσεων της CNOT σε πίνακες είναι η ακόλουθη:

$$|00\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{4.6}$$

$$|01\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{4.7}$$

$$|10\rangle \rightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{4.8}$$

$$|11\rangle \rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{4.9}$$

Η αναπαράσταση της CNOT συνολικά σε πίνακα είναι:

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

Πίνακας 4.4.1

Όπως τονίστηκε προηγουμένως, υπάρχουν πολλές ακόμα κβαντικές πύλες που δρουν σε δύο ή περισσότερα qubits, αλλά αν και δεν υπάρχει λόγος αναφοράς σε αυτές, καθώς η CNOT αλλά και οι απλές λογικές πύλες αποτελούν τη βάση για τη σύνθεση και τη λειτουργία όλων των άλλων πυλών, θα τις μελετήσουμε αμέσως τώρα, [23]

Κβαντικές πύλες που δρουν επάνω σε ένα κβαντοδυφίο είναι η μοναδιαία I, η πύλη Hadamard (H) και οι PauliX, PauliY, PauliZ.

Η μοναδιαία πύλη I χαρακτηρίζεται από τον εξής πίνακα:

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (4.10)$$

και ισχύει $I|0\rangle=|0\rangle$, $I|1\rangle=|1\rangle$.
Διαπιστώνουμε λοιπόν ότι η μοναδιαία πύλη αφήνει ανεπηρέαστο το qubit.

Η πύλη Hadamard χαρακτηρίζεται από τον πίνακα:

$$H \equiv 1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (4.11)$$

και ισχύει $H|0\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)\equiv|+\rangle$, $H|1\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)\equiv|-\rangle$.

Η πύλη Hadamard δημιουργεί ισοβαρείς επαλληλίες των βασικών καταστάσεων.

Οι πύλες PauliX, PauliY, PauliZ διαθέτουν αντίστοιχα τους εξής πίνακες:

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (4.12)$$

$$Y \equiv \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad (4.13)$$

$$Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (4.14)$$

και ισχύει $X|x\rangle=|\overline{x}\rangle$, $Y|0\rangle=i|1\rangle=e^{i\pi/2}|1\rangle$, $Y|1\rangle=-i|0\rangle=e^{i\pi/2}|0\rangle$, $Z|0\rangle=|0\rangle$, $Z|1\rangle=-|1\rangle$.

Η πύλη PauliX αντιστρέφει τις βασικές καταστάσεις, η PauliY λειτουργεί όπως η PauliX αλλά αποδίδει και σχετική φάση, ενώ τέλος η PauliZ παρέχει τις ιδιοτιμές των βασικών καταστάσεων.

4.4.2. ΤΟ ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΣΥΣΤΗΜΑ RSA - Ο ΑΛΓΟΡΙΘΜΟΣ Shor

Το κρυπτογραφικό σύστημα RSA

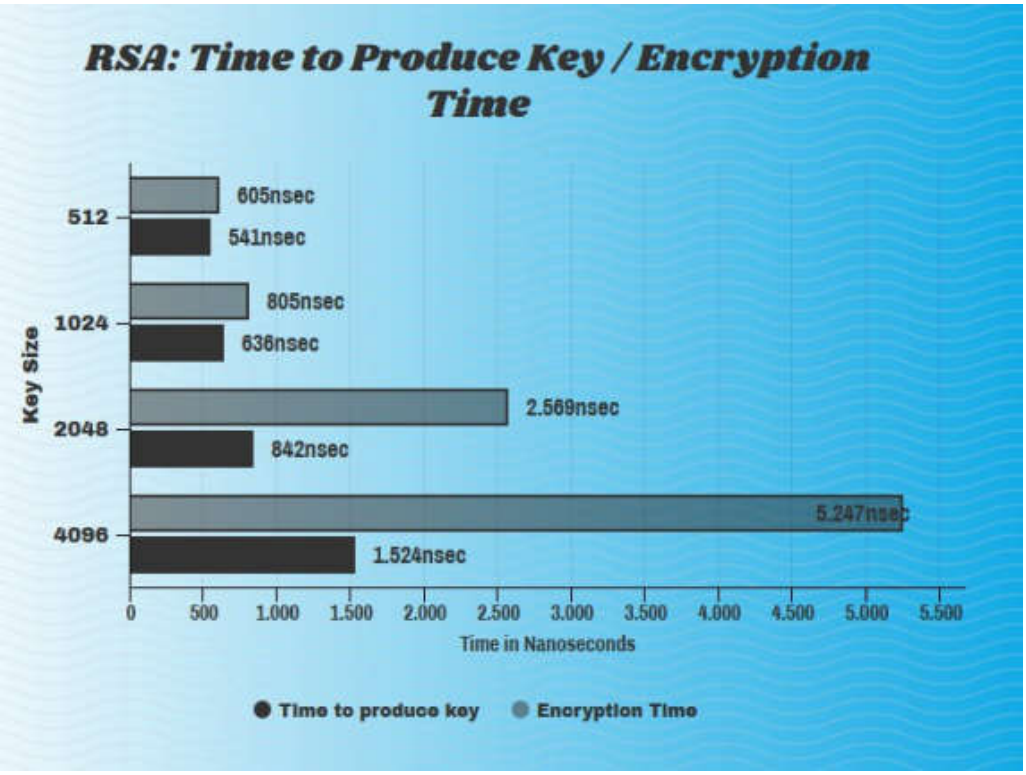
Το RSA είναι ένα δημοφιλές και αρκετά επιτυχημένο κρυπτογραφικό σύστημα δημοσίου κλειδιού, που δημιουργήθηκε το 1978 από τους Rivest, Shamir και Adelman, τα αρχικά των οποίων φέρει. Πρόκειται για ένα εξαιρετικά ασφαλές σύστημα απαραβίαστο από τους σύγχρονους κλασικούς υπολογιστές και πάνω στο οποίο στηρίζονται τραπεζικές συναλλαγές και ευαίσθητα δεδομένα. Η ασφάλειά του βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακέραιων αριθμών. Στον αλγόριθμο RSA γίνεται χρήση ενός δημόσιου κλειδιού για την κρυπτογράφηση και ενός ιδιωτικού για την αποκρυπτογράφηση.

- Κατά την εκτέλεση του RSA επιλέγουμε τυχαία δύο αριθμούς p και q , οι οποίοι είναι πρώτοι και ακέραιοι.
- Στην συνέχεια υπολογίζουμε το γινόμενο $n=p\times q$

- Επιλέγουμε έπειτα έναν τυχαίο d αριθμό ο οποίος είναι πρώτος ως προς τις διαφορές (p-1) και (q-1).
- Υπολογίζουμε το $e = \frac{1 mod(\varphi(n))}{d}$, όπου φ(n)=(p-1)×(q-1).
- Αφού εκτελεστούν τα παραπάνω βήματα, προκύπτει ότι το ζεύγος (e,n) αποτελεί το δημόσιο κλειδί, ενώ το (d,n) είναι το ιδιωτικό.

Έτσι σε μια τραπεζική συναλλαγή ο πελάτης λαμβάνει ένα δημόσιο κλειδί, ενώ η τράπεζα κρατάει το ιδιωτικό και το κρατάει αυτή και μόνο αποφεύγοντας κάθε κίνδυνο υποκλοπής. Ο πελάτης πραγματοποιεί τη συναλλαγή που θέλει με τη χρήση του δημόσιου κλειδιού (αποστέλλει δηλαδή ένα κρυπτογραφημένο μήνυμα), και η τράπεζα με τη σειρά της επεξεργάζεται το αίτημα αυτό με τη βοήθεια και των δύο κλειδιών (αποκρυπτογραφεί το μήνυμα).

Στη θεωρία το να σπάσει κάποιος ένα σύστημα RSA είναι απλό. Από τη στιγμή που κάποιος αποκτήσει πρόσβαση στο δημόσιο κλειδί (e,n) και γνωρίζοντας την μεθοδολογία στην οποία στηρίζεται ο RSA, μπορεί να αναλύσει τον n σε γινόμενο πρώτων αριθμών. Βρίσκει έτσι άμεσα τους αριθμούς p, q και αποκτά πρόσβαση στο ιδιωτικό κλειδί υπολογίζοντας το d. Ωστόσο όπως προαναφέρθηκε ο RSA είναι το πλέον ασφαλές σύστημα κρυπτογράφησης, αδιαπέραστο από τους σύγχρονους κλασικούς υπολογιστές.



Εικόνα 4.1. Συνοπτικός πίνακας χρόνου δημιουργίας κλειδιού και κρυπτογράφησης με τη χρήση του RSA

Αυτό συμβαίνει γιατί το πρόβλημα ανάλυσης ενός αριθμού n σε γινόμενο πρώτων παραγόντων, απαιτεί εκθετική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του n. Αβίαστα οδηγούμαστε στο συμπέρασμα ότι όσο περισσότερο πλήθος ψηφίων έχει ο αριθμός n, τόσο πιο ασφαλής είναι η επικοινωνίας μας. Ο κλασικός υπολογιστής αδυνατεί να εκτελέσει τόσο πολύπλοκες πράξεις σε εύλογο χρονικό διάστημα, ένας κβαντικός υπολογιστής θα μπορούσε όμως;

Στο ερώτημα αυτό έρχεται να δώσει απάντηση η δημιουργία ενός κβαντικού αλγορίθμου με ανυπολόγιστες δυνατότητες, ανάμεσα στις οποίες και η κρυπτανάλυση του συστήματος RSA.

Ο αλγόριθμος Shor

Το παράδοξο με το σύστημα RSA είναι ότι το στοιχείο που το κάνει άτρωτο σήμερα, είναι ταυτόχρονα και η αχίλλειος πτέρνα του στο μέλλον. Η βάση του ασφάλειας του RSA όπως προαναφέρθηκε, είναι η εκθετική αύξηση του χρόνου υπολογισμού του μεγέθους n.

Μέχρι σήμερα πλήθος αλγορίθμων έχουν προταθεί για την παραβίαση του συστήματος RSA, ένας όμως είναι αυτός που ξεχωρίζει. Το 1994 ο Peter Shor, διάσημος μαθηματικός, δημιουργεί έναν κβαντικό αλγόριθμο που φέρει το όνομά του (Shor) και ο οποίος είναι σε θέση να εκμηδενίσει την ασφάλεια του RSA αλλά και των περισσότερων κρυπτογραφικών συστημάτων που υπάρχουν σήμερα, σε ασύλληπτο χρόνο. Ο Shor μπορεί να εφαρμοστεί μόνο σε κβαντικούς υπολογιστές, αν και αξίζει να σημειωθεί πως ακόμα δεν υπάρχει κάποιος αρκετά ισχυρός, πάνω στον οποίο θα μπορούσε να τρέξει ο αλγόριθμος αυτός.

Για την επίλυση του προβλήματος της παραγοντοποίησης μεγάλων ακεραίων σε πολυωνυμικό χρόνο αντί εκθετικό, υπάρχει σήμερα ο αλγόριθμος GNFS (General Number Field Sieve) ο οποίος εφαρμόζεται σε κλασικούς υπολογιστές. Ο χρόνος που απαιτείται για τον αλγόριθμο αυτόν ώστε να εκτελέσει γρήγορους πολλαπλασιασμούς, είναι $O(e^{1.9(logN)1/3(logN)2/3})$. Ο αντίστοιχος κβαντικός αλγόριθμος του Shor με κβαντικές πύλες, απαιτεί σημαντικά λιγότερο χρόνο και συγκεκριμένα:

$$O((logN)^2(\log(logN))(\log(\log(logN))) \qquad (4.15)$$

Πώς όμως γίνεται να είναι τόσο ταχύς ο αλγόριθμος του Shor συγκριτικά με τον GNFS; Ο Shor εκμεταλλεύεται τις ιδιότητες των κβαντικών συστημάτων.

Πιο συγκεκριμένα επωφελείται από την ιδιότητά τους, να βρίσκονται σε υπέρθεση ενός πολύ μεγάλου αριθμού καταστάσεων που υποβάλλονται στον ίδιο κβαντικό μετασχηματισμό. Έτσι είναι εφικτοί πολλαπλοί υπολογισμοί ταυτόχρονα σε όλες τις καταστάσεις και όχι σε κάθε μία ξεχωριστά. Ο παράλληλος αυτός υπολογισμός μειώνει δραματικά τον απαιτούμενο χρόνο για τον υπολογισμό του n και κατ'επέκταση του κλειδιού.

Αξίζει να σημειωθεί ότι ένα δημόσιο κλειδί μήκους 300 ψηφίων (1024 bits) θα χρειαστεί 10^{11} έτη για να σπάσει από τον GNFS, ενώ από τον αλγόριθμο Shor, λιγότερο από 1 δευτερόλεπτο, [20]

Ας δούμε τώρα την εκτέλεση του αλγορίθμου του Shor σταδιακά.

Μας ζητείται να βρούμε την περίοδο « r » της συνάρτησης $f_{n,a}$(x) = a^x(mod n), με n ακέραιος και α τυχαίος ακέραιος και πρώτος ως προς το n.

- Ξεκινάμε με δύο κβαντικούς καταχωρητές Register1 και Register2 οι οποίοι συνθέτουν ένα σύστημα κβαντικού καταχωρητή Register.
- Παρακάτω θα αναφερόμαστε στους Register1, Register2, Register, ως Reg1, Reg2, Reg αντίστοιχα.
- Οι καταστάσεις των Reg1, Reg2, Reg, δίνονται παρακάτω:
  Reg1=$|\psi_1\rangle$
  Reg2=$|\psi_2\rangle$
  Reg=$|\psi\rangle$=$|\psi_1\rangle|\psi_2\rangle$=$|\psi_1\psi_2\rangle$
- Η αρχική κατάσταση του Reg είναι $|00\rangle$.
- Επιλέγουμε έναν ακέραιο q ώστε $2n^2 \leq q \leq 3n^2$
- Φέρνουμε τον Reg1 σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως (q-1). Πιο συγκεκριμένα δημιουργούμε την υπέρθεση των x=1,2,3,4,...,q-1.
- Με τη βοήθεια της κβαντικής παραλληλίας υπολογίζουμε την $f_{n,a}$ για κάθε ένα από τα παραπάνω x, και καταχωρούμε τα αποτελέσματα στον Reg2.
- Ο καταχωρητής Reg παύει να είναι το γινόμενο $|\psi_1\rangle|\psi_2\rangle$, αφού οι καταχωρητές Reg1 και Reg2 είναι πλέον σε κατάσταση κβαντικής διεμπλοκής και το αποτέλεσμα του ενός επηρεάζει άμεσα του άλλου.
- Ορίζουμε τώρα ένα k το οποίο είναι μία τιμή της $f_{n,a}$, και την έχουμε λάβει από μέτρηση της κατάστασης του Reg2 που βρίσκεται σε υπέρθεση. Συνεπώς η κατάσταση του Reg2 είναι $|k\rangle$.
- Στον καταχωρητή Reg1 αντίστοιχα, θα βρίσκονται τα x για τα οποία ισχύει

$$f_{n,a}(x) = a^x (mod\ n) = k \qquad (4.16)$$

και τα οποία επηρεάζονται άμεσα από την μέτρηση του Reg2, αφού όπως προαναφέρθηκε, οι δύο καταχωρητές είναι σε διεμπλοκή.

- Ζητούμενο της διαδικασίας που περιγράφηκε παραπάνω, ήταν η εύρεση της περιόδου « r » της $f_{n,a}(x)$. Η περίοδος αυτή εντοπίζεται στις καταστάσεις του Reg1 {x, x+r, x+2r,…,}.

Θα μπορούσαμε εύκολα να καταλήξουμε στο συμπέρασμα ότι η μέτρηση δύο διαδοχικών καταστάσεων του Reg2 θα μας έδινε την περίοδο ακόμα πιο γρήγορα. Ωστόσο κάτι τέτοιο δεν είναι δυνατό, καθώς κάθε μέτρηση θα έδινε τον ίδιο αριθμό σαν αποτέλεσμα μιας και θα είχαμε καταστροφή της υπέρθεσης. Με τη βοήθεια του κβαντικού μετασχηματισμού Fourier στον Reg1, προλαμβάνουμε το πρόβλημα αυτό, [20]

Ο κβαντικός μετασχηματισμός Fourier είναι η βάση πολλών κβαντικών αλγορίθμων και είναι σε θέση να προκαλεί αλληλεπιδράσεις μεταξύ qubits και κβαντικών καταχωρητών, πράγμα που θα παίξει ρόλο στη λύση του προβλήματος που προαναφέρθηκε, [21]

Αν εφαρμόσουμε τον κβαντικό μετασχηματισμό Fourier στις καταστάσεις του Reg1 {x, x+r, x+2r,…,}, θα έχουμε ως αποτέλεσμα τη δημιουργία νέας υπέρθεσης καταστάσεων, στην οποία τα πλάτη πιθανότητας των καταστάσεων δεν είναι ίσα όπως προηγουμένως. Πλέον τα πλάτη πιθανότητας θα αντιστοιχούν σε ακέραια πολλαπλάσια του 1/r και θα είναι επίσης πολύ μεγαλύτερα. Τα βήματα του αλγόριθμου Shor επαναλαμβάνονται log(q) φορές ώστε να έχουμε όσο το δυνατόν πιο ακριβή υπολογισμό της αντίστροφης περιόδου 1/r, [20]

Συνοψίζοντας, ο κβαντικός αλγόριθμος του Shor έδωσε λύση σε ένα περίφημο πρόβλημα, αυτό της παραγοντοποίησης ενός μεγάλου ακέραιου αριθμού, στηριζόμενος στον κβαντικό μετασχηματισμό Fourier, [22]

4.5. ΕΦΑΡΜΟΓΕΣ

Η κβαντική μηχανική και κρυπτογραφία βρίσκει πλήθος εφαρμογών σήμερα, εκατό και πλέον έτη μετά την ανακάλυψή της.

- **Κβαντικά Ραντάρ**

Μία εξαιρετικά χρήσιμη εφαρμογή της είναι στην αμυντική έρευνα μέσα από τη δημιουργία κβαντικών αισθητήρων και ραντάρ. Η ανάγκη για ανίχνευση αεροσκαφών μη ανιχνεύσιμων από τα ραντάρ (stealth), οδήγησε τους επιστήμονες στην προσπάθεια δημιουργίας κβαντικών ραντάρ, τα οποία θα ανιχνεύουν με υψηλή ακρίβεια τα stealth. Επίσης θα είναι ικανά να αντιλαμβάνονται κακόβουλα σήματα παρεμβολής και ενδεχομένως να τα αντιμετωπίζουν. Τα κβαντικά ραντάρ θα είναι όμοια με τα ήδη υπάρχοντα με διαφορά ότι τα πρώτα, θα κάνουν χρήση ενός πλήθους φωτονίων. Η δημιουργία τους πρόκειται να βελτιώσει τις σημερινές συνθήκες όσον αφορά την ανίχνευση, την ανάλυση και την ταυτοποίηση στόχων με τη βοήθεια κβαντικών φαινομένων, όπως αυτών της κβαντικής διεμπλοκής, [24]

Διακρίνουμε δύο είδη κβαντικών ραντάρ. Εκείνα που εκπέμπουν μεμονωμένα φωτόνια και εκείνα που εκπέμπουν φωτόνια που βρίσκονται σε κατάσταση διεμπλοκής. Και στις δύο περιπτώσεις γίνεται εκμετάλλευση της κβαντικής διεμπλοκής και η διαδικασία έχει ως εξής:

1. Δημιουργείται ένα ζεύγος φωτονίων σε διεμπλοκή
2. Το ένα φωτόνιο κρατείται στο σύστημα ανίχνευσης
3. Το δεύτερο φωτόνιο εκπέμπεται προς τον στόχο σε μορφή μικροκύματος
4. Το δεύτερο φωτόνιο ανακλάται από τον στόχο και επιστρέφει στο σύστημα ανίχνευσης
5. Οι καταστάσεις των δύο φωτονίων μετρώνται και συγκρίνονται μεταξύ τους και ανάλογα τη συσχέτιση που υπάρχει μεταξύ τους, εξάγεται το συμπέρασμα που αφορά το στόχο.

- **Κβαντικός Υπολογιστής**

Η σημαντικότερη χρήση της κβαντικής κρυπτογραφίας, είναι αναμφισβήτητα στους κβαντικούς υπολογιστές και στην ασφάλειά τους.

Ένας κβαντικός υπολογιστής είναι όμοιος με τον συμβατικό, με μόνη διαφορά ότι στον πρώτο η βασική μονάδα εγγραφής και επεξεργασίας της πληροφορίας στο δυαδικό σύστημα, είναι ένα κβαντικό σύστημα και όχι ψηφίδες ολοκληρωμένων κυκλωμάτων μνημών τύπου ROM και RAM.

Οι κβαντικοί υπολογιστές πρόκειται αναπόφευκτα να κατακλύσουν την αγορά, καθώς το μέγεθος της βασικής μονάδας μνήμης του υπολογιστή συνεχώς μικραίνει, λόγω της αύξησης της χωρητικότητας της μνήμης και σύντομα θα είναι ανεπαρκές. Αυτό σε έναν κβαντικό υπολογιστή δεν αποτελεί πρόβλημα μιας και η μνήμη του αποτελείται από κβαντοδυφία, [24]

Με τη βοήθεια της κβαντικής μηχανικής, μπορούμε να δημιουργήσουμε νέες σταθερότερες βάσεις στον τομέα της ασφάλειας. Ο τρόπος, που έχει περιγραφεί και σε προηγούμενο κεφάλαιο, που λειτουργεί η κβαντική κρυπτογράφηση είναι ο καλύτερος που έχει υπάρξει έως τώρα. Ακόμα και σε περίπτωση υποκλοπής, όσο ελάχιστες κι αν είναι οι πιθανότητες αυτή να συμβεί, υπάρχει τρόπος να ανιχνευτεί αλλά και να γίνει διακοπή της υποκλοπής.

Θα πρέπει να λάβουμε υπόψη μας ότι οι κβαντικοί υπολογιστές δεν είναι καθολικά καλύτεροι των συμβατικών, απλώς υπερέχουν σε κάποιες συγκεκριμένες περιπτώσεις. Κατά τ’ άλλα οι κβαντικοί υπολογιστές δεν παρουσιάζουν ιδιαίτερες διαφορές κατά τη χρήση τους από τους υπάρχοντες υπολογιστές. Η κβαντική κρυπτογραφία καλύπτει ουσιαστικά τα κενά της κλασικής, της οποίας η ασφάλεια εξαρτάται από την επίλυση μαθηματικών εξισώσεων που δεν έχει αποδειχτεί ακόμα ότι είναι άλυτα.

- **Ασφάλεια ευαίσθητων προσωπικών δεδομένων**

Η ραγδαία ανάπτυξη της κβαντικής κρυπτογραφίας αναμένεται να εξασφαλίσει πολύ σύντομα τη μέγιστη ασφάλεια στις επικοινωνίες. Ευαίσθητα δεδομένα, τραπεζικές συναλλαγές, κυβερνητικά θέματα αλλά και άλλα δεδομένα που σήμερα

κινδυνεύουν ανά πάσα στιγμή να βρεθούν εκτεθειμένα, πρόκειται να προστατευθούν απόλυτα με την έλευση της κβαντικής κρυπτογραφίας. Οι επιθέσεις από εισβολείς θα περιοριστούν δραματικά και ένα κλίμα ασφάλειας πρόκειται να επικρατήσει. Σαφώς η κβαντική κρυπτογραφία δεν αντιπροσωπεύει μια ουτοπία, καθώς για να καταστούν δυνατά στο μέγιστο όλα όσα περιγράφηκαν, απαιτείται ύπαρξη τέλειων πηγών φωτονίων, άψογων καναλιών επικοινωνίας (π.χ. οπτικές ίνες) και αλάνθαστων ανιχνευτών φωτονίων.

- **Ασφαλείς Ψηφοφορίες**

Η κβαντική κρυπτογραφία μπορεί να εγγυηθεί την αδιαβλητότητα των ηλεκτρονικών ψηφοφοριών. Πιο συγκεκριμένα η πρώτη δημόσια ψηφοφορία έλαβε χώρα στην Γενεύη της Ελβετίας το 2007, με τη χρήση κβαντικής κρυπτογραφίας σε περιβάλλον δικτύου. Πιο συγκεκριμένα υπήρξε η εγγύηση του να μην υπάρξει καμία απώλεια στις ψήφους, κατά τη μετάδοσή τους από τα εκλογικά κέντρα, [25]

4.6. ΣΥΓΚΡΙΣΗ ΚΒΑΝΤΙΚΟΥ ΜΕ ΚΛΑΣΙΚΟ ΥΠΟΛΟΓΙΣΤΗ

Οι κλασικοί υπολογιστές παρά την γενικότερη ομοιότητά τους με τους κβαντικούς, έχουν και ένα σημαντικά μεγάλο πλήθος διαφορών τόσο στη δομή, όσο και στη λειτουργία τους.

Έχει ήδη αναφερθεί σε προηγούμενες παραγράφους, ότι στους κλασικούς υπολογιστές η στοιχειώδης μονάδα πληροφορίας είναι το bit. Αντίθετα στους κβαντικούς υπολογιστές είναι το qubit. Το bit λαμβάνει τις διακριτές τιμές 0 και 1 και συμβολίζονται με τον ίδιο τρόπο, ενώ το qubit λαμβάνει ως τιμή, έναν συνδυασμό των πιθανοτήτων να υπάρχει το 0 και το 1 και συμβολίζονται ως $|0\rangle$ και $|1\rangle$.

Παράλληλα να σημειωθεί ότι το 0 και το 1 του bit υποδηλώνουν την παρουσία ρεύματος ή όχι σε ένα τρανζίστορ. Από την άλλη πλευρά τα $|0\rangle$ και $|1\rangle$ του qubit περιγράφουν το spin ενός σωματιδίου.

Εξίσου σημαντική διαφορά υπάρχει και στις πύλες που απαρτίζουν τα κυκλώματα των υπολογιστών αυτών. Όπως έχει ήδη γίνει γνωστό, ο κλασικός υπολογιστής διαθέτει τις λογικές πύλες AND, OR, NOT, NAND, XOR, XNOR και NOR. Αντίθετα, ο κβαντικός υπολογιστής χρησιμοποιεί κβαντικές πύλες, οι σημαντικότερες εκ των οποίων είναι οι CNOT, I, Hadamard (H), PauliX, PauliY και PauliZ.

Η κατάσταση του bit στον κλασικό υπολογιστή συμβολίζεται μονάχα ως 0 ή 1. Ωστόσο οι κβαντικές καταστάσεις μπορούν να εκφραστούν και ως τετραγωνικοί πίνακες, όπως έχουμε δει στην παράγραφο 4.4.1.

Η πιο μεγάλη διαφορά ωστόσο, είναι αυτή της ταχύτητας επεξεργασίας δεδομένων και της επίλυσης πολύπλοκων προβλημάτων. Ο κβαντικός υπολογιστής είναι σε θέση να επιλύει προβλήματα σε ελάχιστα δευτερόλεπτα, έναντι εκατοντάδων χιλιάδων ετών που απαιτεί ο κλασικός. Παράλληλα μπορεί να επιλύσει ταυτόχρονα μαθηματικά προβλήματα εκθετικού χρόνου τάχιστα, μετατρέποντάς τα σε πολυωνυμικού.

Οι μόνοι παράγοντες στους οποίους ο κλασικός υπολογιστής «κερδίζει», είναι στην δυνατότητα του να προσφέρει λειτουργίες στο χρήστη, όπως μια απλή επεξεργασία κειμένου, web surfing, κ.ά., καθώς ο κβαντικός υπολογιστής είναι

φτιαγμένος αποκλειστικά για την επίλυση προβλημάτων και την επεξεργασία δεδομένων. Την ίδια στιγμή, οι κβαντικοί υπολογιστές υστερούν όσον αφορά την αντοχή των υλικών τους στις υψηλές θερμοκρασίες. Οι τεράστιες ταχύτητες μεταφοράς δεδομένων αναπτύσσουν σημαντικά υψηλές θερμοκρασίες στα κυκλώματα, με αποτέλεσμα να απαιτείται η χρήση κάποιου υλικού που θα έχει περισσότερες αντοχές στις ακραίες μεταβολές της θερμοκρασίας, [25]

Όλα τα παραπάνω παρουσιάζονται συγκεντρωτικά στον παρακάτω πίνακα:

ΚΛΑΣΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ	**ΚΒΑΝΤΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ**
1. Στοιχειώδης μονάδα πληροφορίας είναι το bit.	1. Στοιχειώδης μονάδα πληροφορίας είναι το qubit.
2. Το bit υποδηλώνει παρουσία ρεύματος σε τρανζίστορ.	2. Το qubit υποδηλώνει το spin κάποιου σωματιδίου.
3. Λογικές πύλες	3. Κβαντικές πύλες
4. Πύλες AND, OR, NOT, NAND, XOR, XNOR και NOR.	4. Πύλες CNOT, I, Hadamard (H), PauliX, PauliY και PauliZ.
5. Μικρή ταχύτητα επεξεργασίας δεδομένων.	5. Τεράστια ταχύτητα επεξεργασίας δεδομένων.
6. Αδυναμία επίλυσης δύσκολων μαθηματικών προβλημάτων.	6. Δυνατότητα επίλυσης δύσκολων μαθηματικών προβλημάτων.
7. Προσφέρει λειτουργίες ψυχαγωγίας και άλλα, πέρα από την εκτέλεση πράξεων και επεξεργασία δεδομένων.	7. Εκτελεί μονάχα περίπλοκες μαθηματικές εξισώσεις, και επεξεργάζεται δεδομένα.
8. Οι θερμοκρασίες που αναπτύσσονται στα κυκλώματά του είναι ανεκτές από τα υλικά που τα αποτελούν.	8. Οι θερμοκρασίες που αναπτύσσονται στα κυκλώματά του είναι υπερβολικά υψηλές για τις αντοχές των υλικών.

Πίνακας 4.6.1

5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

Κλείνοντας αυτή την εργασία, κρίνεται σκόπιμο να αναφερθούμε στο πόσο πρόκειται η κβαντική τεχνολογία να αλλάξει τις μελλοντικές ικανότητες των υπολογιστών. Είναι αναπόφευκτο το γεγονός της εμπορικής χρήσης των κβαντικών υπολογιστών στο άμεσο μέλλον, αλλά και η περεταίρω ανάπτυξη και τελειοποίησή τους.

Η κβαντική κρυπτογραφία γεννήθηκε μέσα από την ένωση της κβαντικής μηχανικής και της κρυπτογραφίας, αμέσως μετά τα μεγάλα άλματα προόδου της κβαντικής οπτικής. Η αρχή πάνω στην οποία θέτει τις βάσεις της η κβαντική κρυπτογραφία είναι αυτή της αβεβαιότητας του Heisenberg, που αναλύθηκε διεξοδικά σε προηγούμενο κεφάλαιο.

Η κβαντική κρυπτογραφία είναι ένας σχετικά νέος κλάδος της πληροφορικής και παρά τις πολλές υποσχέσεις της όσον αφορά το μέλλον της ασφάλειας και της ιδιωτικότητας, έχει ακόμα πολλά πεδία ανεξερεύνητα που αποτελούν πρόκληση για τους επιστήμονες.

Για την ώρα προέχει η βελτιστοποίηση των ήδη υπαρχόντων μέσων, όπως οι ανιχνευτές σωματιδίων απόλυτα συμβατοί με τις οπτικές ίνες. Ακόμη είναι αναγκαία η αξιοποίηση του αέρα ως μέσο μεταφοράς πληροφορίας για την μείωση των σφαλμάτων αλλά και του θορύβου σε κβαντικό επίπεδο.

Είναι πολύ σημαντικό να μην αφήνουμε τον ενθουσιασμό της νέας αυτής τεχνολογικής προόδου να μας παρασύρει. Η επιστημονική κοινότητα οφείλει να αναγνωρίσει τους πολλαπλούς κινδύνους που κρύβει αυτή η τεχνολογική έκρηξη και να βρει άμεσα λύσεις για την πρόληψη αυτών των κινδύνων. Ευτυχώς ή δυστυχώς οι κβαντικοί αλγόριθμοι απέχουν ακόμα αρκετά χρόνια έρευνας ως την τελειοποίησή τους, αφήνοντας χρόνο να τεθούν ισχυρά θεμέλια στην ανάπτυξη της κβαντικής κρυπτογραφίας.

Πολλά κρυπτογραφικά πρωτόκολλα έχουν προταθεί ως τώρα με το BB84 να ξεχωρίζει ανάμεσα στα άλλα, λόγω της ασφάλειας που προσφέρει. Η μεγαλύτερη απειλή ως τώρα είναι να υπάρξει μία καλά οργανωμένη ομαδική επίθεση σύντομα,

όταν ακόμα η εμπιστευτικότητα αλλά και όλοι οι άλλοι στόχοι της κρυπτογραφίας, δεν έχουν ακόμα εδραιωθεί.

Η έρευνα που αφορά την κβαντική διεμπλοκή συνεχίζεται ως σήμερα και θα συνεχίσει να υφίσταται έως ότου γνωρίσουμε πλήρως, όλα όσα έχει το φαινόμενο αυτό να μας προσφέρει. Τα πειράματα που λαμβάνουν χώρα, δείχνουν πως υπάρχουν ακόμα τεράστια περιθώρια βελτίωσης σε ότι έχουμε δημιουργήσει ως τώρα.

Το όραμα της τέλειας μυστικότητας πλησιάζει ολοένα και περισσότερο την πραγματικότητα, όμως είναι εξαιρετικά εύκολο με τα σημερινά δεδομένα να παραβιαστεί η ασφάλεια αυτή. Ο μελλοντικός τεχνολογικός εξοπλισμός υπόσχεται να είναι αντάξιος της ασφάλειας που η κβαντική κρυπτογραφία, από πλευράς φυσικής, προσφέρει.

Ένα πράγμα είναι το μόνο σίγουρο. Ότι η κβαντική κρυπτογραφία ήρθε για να αλλάξει το μέλλον της επιστήμης των υπολογιστών και να ανοίξει μια καινούρια σελίδα στον κλάδο της κρυπτογραφίας.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Α. Τσότσου, «*ΚΡΥΠΤΟΓΡΑΦΙΑ*», Πανεπιστήμιο Πατρών, Πολυτεχνική Σχολή, Πάτρα, 2018.(Πρόσβαση 8/4/2019)

[2] Κ. Προύσαλης, «*Κβαντική Κρυπτογραφία & Κβαντική Κρυπτανάλυση*», Πανεπιστήμιο Αιγαίου, Σχολή Θετικών Επιστημών, Σάμος, 2008. (Πρόσβαση 29/4/2019)

[3] Μ.Β. Τσετσίλα, «*ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ*», Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Αθήνα. (Πρόσβαση 24/3/2019)

[4] Ζάχος, Ε., Παγουρτζής, Α., Σούλιου, Θ. 2015. «Κρυπτογραφία και Ασφάλεια». [Κεφάλαιο Συγγράμματος]. Στο Ζάχος, Ε., Παγουρτζής, Α., Σούλιου, Θ. 2015. *Θεμελίωση επιστήμης υπολογιστών*. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ 16. Διαθέσιμο στο: http://hdl.handle.net/11419/5467(Πρόσβαση 20/7/2019)

[5] Du, Wenliang Kevin; Deng, Jing; Han, Yunghsiang S.; and Varshney, Pramod K., "*A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks*" (2000). Electrical Engineering and Computer Science. Paper 36. (Πρόσβαση 20/7/2019)

[6] Antoniades I. P., Miliou A. N., Hatalis M. K., "*Quantum Cryptography : The Ultimate Solution to Secure Data Transmission ?*" in Proceedings of the 2nd Balkan Conference in Informatics, Ohrid, 2005. (Πρόσβαση 21/07/2019)

[7] *Φυσική Γενικής Παιδείας - Γ Τάξης γενικού λυκείου. (pdf)*. Οργανισμός Εκδόσεων Διδακτικών Βιβλίων - Παιδαγωγικό Ινστιτούτο - ΥΠΕΠΘ. 2008, σελ. 28. (Πρόσβαση 20/07/2019)

[8] Β. Καραγεώργος, «*Κβαντική Κρυπτογραφία*», Πανεπιστήμιο Αθηνών, Σχολή Θετικών Επιστημών, Αθήνα, 2006 (Πρόσβαση 12/4/2019)

[9] physics4u (2009), https://physics4u.wordpress.com/2009/10/10/%CE%AF-%CF%8C-%CE%AD-%CE%AE-iot/ (Πρόσβαση 9/8/2019)

[10] physics4u (2002), http://www.physics4u.gr/articles/2002/comptonscatter.html (Πρόσβαση 18/8/2019)

[11] Τσετσιλα Μ.Β., «*Κρυπτογραφία και Κβαντικοί Υπολογιστές*», Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Αθήνα. (Πρόσβαση 21/8/2019)

[12] Chris Elpidis, «*Αυτή είναι η πρώτη φωτογραφία που απεικονίζει την κβαντική σύζευξη δυο φωτονίων!»,* 13/7/2019, https://www.techgear.gr/quantum-entaglement-first-photo-162233/ , (Πρόσβαση 22/8/2019)

[13] «*Μια παραξενιά της κβαντομηχανικής: στοιχειωμένη δράση από απόσταση*», 20/6/2018, https://physics4u.wordpress.com/2018/06/20/%ce%bc%ce%b9%ce%b1-%cf%80%ce%b1%cf%81%ce%b1%ce%be%ce%b5%ce%bd%ce%b9%ce%ac-%cf%84%ce%b7%cf%82-%ce%ba%ce%b2%ce%b1%ce%bd%cf%84%ce%bf%ce%bc%ce%b7%cf%87%ce%b1%ce%bd%ce%b9%ce%ba%ce%ae%cf%82-%cf%83%cf%84/,(Πρόσβαση 23/8/2019)

[14] Βενέρης Ιωάννης, Μίμησις Πληροφορική, εκδ. Τζιόλα, Αθήνα, 2007. ISBN 978-960-418-134-6 (Πρόσβαση 20/08/2019)

[15] Φυσική Θετικής & Τεχνολογικής Κατεύθυνσης – Γ' τάξης γενικού λυκείου, *(pdf)*. Οργανισμός Εκδόσεων Διδακτικών Βιβλίων - Παιδαγωγικό Ινστιτούτο - ΥΠΕΠΘ, σελ. 232. (Πρόσβαση 22/08/2019)

[16] Σταματίου Γ., «*Μελέτη Ιδιοτήτων της Κβαντικής Πληροφορίας σε Κβαντικά Συστήματα*», Πανεπιστήμιο Πατρών, Τμήμα Φυσικής, Πάτρα 2010, σ.3, στον ιστότοπο: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/4136/7/Stamatiou-PhD-UPatras-2010.pdf (Πρόσβαση 29/8/2019)

[17] Michael A. Nielsen, «*Κβαντική πληροφορία: Οι κανόνες για ένα πολύπλοκο κβαντικό κόσμο*», scientificamerican.com, Ιανουάριος 2004(Πρόσβαση 25/08/2019)

[18] Καραφυλλίδης, Ι., 2015. «*Κβαντική υπολογιστική*». [ηλεκτρ. βιβλ.], κεφ.6, Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/216 (Πρόσβαση 02/01/2020)

[19] Καραφυλλίδης, Ι. 2015. «*Η Κβαντική Διεμπλοκή και ο Κβαντικός Μετασχηματισμός Fourier*». [Κεφάλαιο Συγγράμματος]. Στο Καραφυλλίδης, Ι. 2015. *Κβαντική υπολογιστική*. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ 6. Διαθέσιμο στο: http://hdl.handle.net/11419/222 (Πρόσβαση 10/01/2020)

[20] Δριτσοπούλου Μαρία Χριστίνα, «*Μετακβαντική Κρυπτογραφία*», Ελληνικό Ανοιχτό Πανεπιστήμιο, Σχολή Θετικών Επιστημών και Τεχνολογίας, 2019. (Πρόσβαση 13/01/2020)

[21] Karafyllidis, I.G., "*Visualization of the quantum Fourier transform using a quantum computer simulator, Quantum Information Processing*", vol. 2, pp. 271-288, 2003. (Πρόσβαση 13/01/2020)

[22] Ανδρομίδας Πέτρος, «*Στοιχειώδης Εισαγωγή στην Κβαντική Πληροφορία και στους Κβαντικούς Υπολογιστές*», Ελληνικό Ανοιχτό Πανεπιστήμιο, Σχολή Θετικών Επιστημών και Τεχνολογίας, Αθήνα 2015. (Πρόσβαση 14/02/2020)

[23] Ζαρμπούτης Δημήτριος, «*Κβαντικοί Υπολογιστές Θεωρητική Μελέτη-Δυνατότητες Πραγματοποίησης*», Ελληνικό Ανοιχτό Πανεπιστήμιο, Σχολή Θετικών Επιστημών και Τεχνολογίας, 2018. (Πρόσβαση 16/02/2020)

[24] Δουβρόπουλος Θ.Γ, Σολωμός Ν.Χ, Δεββές Φ.Ν, «*Η Κβαντική Τεχνολογία στην Αιχμή της Αμυντικής Ερευνας: Κβαντικό ραντάρ, Κβαντική κρυπτογραφία»,* Τομέας Φυσικών Επιστημών, Εργαστήριο Γενικής & Εφαρμοσμένης Φυσικής / Ναυτικής Ηλεκτροοπτικής, Σχολή Ναυτικών Δοκίμων, Πειραιεύς, ΝΔ/ΙΥ ΣΝΔ Πολεμικού Ναυτικού, Μάιος 2018. (Πρόσβαση 23/02/2020)

[25] Κοκκινάκης Δ., «*Κβαντικός Υπολογιστής & Κβαντική Πληροφορία*», Εθνικόν και Καποδιστριακόν Παναπιστήμιον Αθηνών, Τμήμα Φυσικής, Αθήνα, 2014. (Πρόσβαση 25/02/2020)

Εικόνες

Εικόνα 1.1. https://spartorama.gr/articles/2619/ (Πρόσβαση 30/6/2019)

Εικόνα 1.2. https://el.wikipedia.org/wiki/%CE%A3%CF%84%CE%AE%CE%BB%CE%B7_%CF%84%CE%B7%CF%82_%CE%A1%CE%BF%CE%B6%CE%AD%CF%84%CF%84%CE%B1%CF%82 (Πρόσβαση 30/6/2019)

Εικόνα 3.6.1. http://www.physics4u.gr/articles/2002/comptonscatter.html(Πρόσβαση 18/8/2019)

Εικόνα 3.3.1. https://repository.kallipos.gr/bitstream/11419/1841/1/02_chapter_1.pdf (Πρόσβαση 20/8/2019)

Εικόνα 3.5.1 https://www.techgear.gr/quantum-entaglement-first-photo-162233/ (Πρόσβαση 22/8/2019)

Εικόνα 3.5.2. – Εικόνα 3.5.3 – Εικόνα 3.5.4 https://repository.kallipos.gr/pdfviewer/web/viewer.html?file=/bitstream/11419/216/7/%ce%9a%ce%92%ce%91%ce%9d%ce%a4%ce%99%ce%9a%ce%97_%ce%a5%ce%a0%ce%9f%ce%9b%ce%9f%ce%93%ce%99%ce%a3%ce%a4%ce%99%ce%9a%ce%97_144.pdf (Πρόσβαση 13/01/2020)

Εικόνα 4.1. https://apothesis.eap.gr/bitstream/repo/43544/1/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%94%CF%81%CE%B9%CF%84%CF%83%CE%BF%CF%80%CE%BF%CF%8D%CE%BB%CE%BF%CF%85%20%CE%9C%CE%B1%CF%81%CE%AF%CE%B1%20%CE%A7%CF%81%CE%B9%CF%83%CF%84%CE%AF%CE%BD%CE%B1%20-%20123548.pdf (Πρόσβαση 13/01/2020)