ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**:**

¨Η Κβαντική Τεχνολογία Στην Αμυντική Έρευνα¨

Καρανίκα Γεωργία Μαρία 2114178

Επιβλέπων: Βαρζάκας Παναγιώτης

Μέλος ΔΕΠ, Δρ. Καθηγητής Α βαθμίδας

Λαμία, 16/07/19

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις, 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.

(Υπογραφή)

Καρανίκα Γεωργία Μαρία

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία αναφέρεται στις κυριότερες εφαρμογές της Κβαντικής Τεχνολογίας στον τομέα της άμυνας, οι οποίες, γενικότερα, θα μπορούσαν να κατανεμηθούν σε δύο μεγάλες κατηγορίες, Κβαντική Πληροφορική και Κβαντικοί Αισθητήρες. Για το λόγο αυτό, στην εισαγωγή γίνεται αναφορά των σημαντικότερων ιστορικών στοιχείων της Κβαντικής Μηχανικής (απευθύνεται και στις δύο κατηγορίες) καθώς και της Κβαντικής Κρυπτογραφίας (απευθύνεται κυρίως στην πρώτη κατηγορία). Στην πρώτη κατηγορία εντάσσονται τα τρία πρώτα κεφάλαια, στα οποία περιγράφονται λεπτομερώς οι βασικές αρχές ενός κβαντικού υπολογιστή, οι κατηγορίες στις οποίες διακρίνονται τα κβαντικά κρυπτοσυστήματα-αλγόριθμοι αλλά και οι μέθοδοι διαμοίρασης των κβαντικών κλειδιών τους. Ακολουθεί αναφορά στα Ατομικά Ρολόγια, τα οποία αποτελούν ακρογωνιαίο λίθο για το συντονισμό της πλειοψηφίας των τεχνολογικών επιτευγμάτων, κβαντικών και μη, ενώ στα δύο τελευταία κεφάλαια, τα οποία αποτελούν μέρος της δεύτερης κατηγορίας, παρουσιάζονται τρία από τα σημαντικότερα είδη κβαντικών αισθητήρων και πραγματοποιείται περιγραφή του κβαντικού ραντάρ.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Ιστορικό Κβαντικής Μηχανικής

Στη φυσική, ο όρος κβάντο ή κβάντουμ αναφέρεται σε μια μονάδα ποσότητας, ένα αδιάστατο "ποσό από κάτι". Η έννοια του κβάντου είναι συνυφασμένη με το γεγονός ότι ποσότητες που χαρακτηρίζουν ιδιότητες ενός φυσικού συστήματος (δηλ. φυσικά μεγέθη π.χ. ενέργεια, στροφορμή) μπορούν να παίρνουν διακριτές και όχι συνεχείς τιμές. Δηλαδή, αντίθετα από όσα προβλέπονται από την κλασσική θεωρία, θεωρείται ότι ένα φυσικό μέγεθος αντί για συνεχές έχει διακριτό φάσμα ιδιοτιμών. Αξίζει να σημειωθεί, ότι δεν είναι όλα τα φυσικά μεγέθη ενός συστήματος που έχουν διακριτό φάσμα ιδιοτιμών, δηλ. είναι κβαντωμένα, υπάρχουν και μεγέθη που όπως και στην κλασσική μηχανική έχουν συνεχές φάσμα. Συνεπώς, παρόλο που ο όρος κβάντο επινοήθηκε αρχικά για να περιγράψει τα πακέτα ενέργειας που λέγονται φωτόνια και από τα οποία αποτελείται το φως, εν τέλει ολόκληρη η θεωρία πήρε αυτό το όνομα, κβαντομηχανική.

Προς τα τέλη του 19ου αιώνα, η κλασική φυσική-κλασική μηχανική-ηλεκτρομαγνητική θεωρία-στατιστική μηχανική είχε φτάσει πια στην ιστορική της ολοκλήρωση. Ύστερα από μια μακραίωνη διαδικασία ενοποίησης και σύνθεσης, μια τεράστια ποικιλία εμπειρικών νόμων είχε πια συμπυκνωθεί σε ένα εκπληκτικά μικρό αριθμό θεμελιωδών εξισώσεων με βάση τις οποίες φαινόταν κατ΄ αρχήν δυνατόν να ερμηνευτούν όλα τα φυσικά φαινόμενα. Στους φυσικούς εκείνης της εποχής επικρατούσε η άποψη ότι ο στόχος της φυσικής να φτάσει σε μια τελική ερμηνεία του υλικού κόσμου είχε πραγματοποιηθεί. Λίγο καιρό μετά την αναγγελία από τον Michelson του ¨τέλους της φυσικής¨, ο Planck, στις 14 Δεκεμβρίου 1900, θα ανακοινώσει στην Ακαδημία του Βερολίνου την εργασία του για το μέλαν σώμα, η οποία θα θέσει σε κίνηση μια χιονοστιβάδα εξελίξεων που θα οδηγήσουν, το 1927, στην πλήρη ανατροπή της κλασικής φυσικής και την εγκαθίδρυση ενός νέου επιστημονικού καθεστώτος, της κβαντικής μηχανικής.

Η κβαντομηχανική ή κβαντική μηχανική ή κβαντική φυσική (επίσης κυματομηχανικό μοντέλο, μηχανική μητρών και μηχανική πινάκων) αποτελεί τη βάση σχεδόν κάθε θεωρίας των συστημάτων του μικρόκοσμου. Αρχικά ήταν άμεσα συνδεδεμένη με την κλασσική Φυσική και κυρίως με τους κλάδους της κλασσικής μηχανικής, της στατιστικής μηχανικής και της ηλεκτρομαγνητικής θεωρίας του Maxwell. Η κλασσική

Φυσική, όπως είναι γνωστό άλλωστε, ασχολείται με μακροσκοπικά φαινόμενα που είναι παρατηρήσιμα είτε απ' ευθείας είτε με σχετικά απλά όργανα.

Από τις αρχές του 20ού αιώνα, η προσοχή και το ενδιαφέρον των φυσικών στράφηκε στην παρατήρηση των μοριακών, ατομικών, υποατομικών και πυρηνικών συστημάτων, όπου συμβαίνουν μικροσκοπικά φαινόμενα, φαινόμενα δηλαδή που δεν είναι εφικτό να μελετηθούν απ' ευθείας και τις ενεργειακές αλληλεπιδράσεις. Υπάρχουν λόγοι για τους οποίους η ίδια η παρατήρηση διαταράσσει αυθαίρετα το υπό παρατήρηση σύστημα και έτσι το σφάλμα της μετρήσεως φυσικών μεγεθών ενός συστήματος δεν μπορεί να ελαττωθεί απεριόριστα όπως στην κλασσική φυσική. Σύντομα έγινε αντιληπτό ότι οι νόμοι, οι μέθοδοι και τα πρότυπα της κλασσικής φυσικής δεν ήταν αρκετά για να εξηγήσουν τα φαινόμενα της μοριακής, ατομικής και πυρηνικής φυσικής. Οι πρώτες προσπάθειες στην ατομική φυσική στόχευαν στην υπερνίκηση των δυσκολιών της κλασσικής θεωρίας με τροποποίηση νόμων ή με αλλαγή των προτύπων, οι οποίες οδήγησαν στη συχνά ονομαζόμενη παλαιά κβαντική θεωρία που διαμορφώθηκε από τις εργασίες των Planck, Bohr, De Broglie, Einstein και άλλων. Η πρώτη αυτή μορφή της κβαντικής θεωρίας έφερε την επανάσταση στην επιστημονική κοινότητα, καθώς ανοίχθηκε μια νέα προοπτική αντιμετώπισης των πραγμάτων, εξηγήθηκαν πολλά από τα τότε γνωστά φαινόμενα, παρέμειναν όμως πολλά κενά στην κατανόηση άλλων.

Μέχρι εκείνη την εποχή, η κβαντική θεωρία δεν είχε κάποια γενική δομή και μαθηματικό υπόβαθρο. Ήταν ένα σύνολο από υποθέσεις, εμπειρικούς κανόνες, μεθόδους υπολογισμού και θεωρήματα και όχι μια συνεκτική θεωρία. Δεν υπήρχε σαφής αιτιολόγηση όλων αυτών, με αποτέλεσμα πολλοί να θεωρούσαν αυτούς τους πρώτους νόμους φαινομενολογικούς. Σε αντίθεση με την Κλασική Φυσική, η Κβαντική βρέθηκε και βρίσκεται διαρκώς υπό αμφισβήτηση εξαιτίας πολλών παράδοξων φαινομένων που υποστηρίζει και προβλέπει, έξω από την καθημερινή εμπειρία και την ανθρώπινη διαίσθηση. Όπως πολύ εύστοχα παρατηρήθηκε κάποτε από το σπουδαίο νομπελίστα φυσικό Richard P. Feynman, ένας εκ των θεμελιωτών της Κβαντικής θεωρίας, «παραδοξότητα είναι το μέρος της πραγματικότητας που έρχεται σε σύγκρουση με την αίσθηση που έχουμε για το πώς πρέπει να είναι η πραγματικότητα». Η τεχνολογία της εποχής δεν ευνοούσε ουδεμία πειραματική προσδοκία περί επαλήθευσης ή μη των παραδοξοτήτων αυτών και αμφότεροι θεωρητικοί και

πειραματικοί φυσικοί αρκούνταν στα περίφημα πειράματα σκέψης (gedankenexperiments).

Οι προσπάθειες, όμως, συνεχίστηκαν ώσπου οδηγήθηκαν σε επιτυχία τη χρονική περίοδο 1925-1930, οπότε και διαμορφώθηκε μια νέα μορφή κβαντικής θεωρίας από τις εργασίες των Schrödinger, Heisenberg, Dirac και άλλων. Συγκεκριμένα, ο όρος ¨Κβαντική Μηχανική¨ εμφανίστηκε πρώτη φορά σε μελέτη του Μπορν με τίτλο "Περί της κβαντομηχανικής" (Zur Quantenmechanik), το 1924. Έγινε αποδεκτή από τους περισσότερους φυσικούς κάτω από την πίεση των πειραματικών δεδομένων, μιας και ερχόταν σε σύγκρουση με τις καθιερωμένες τους αντιλήψεις, ενώ μερικοί, όπως ο Αϊνστάιν, εξακολούθησαν να έχουν αμφιβολίες γι'αυτή μέχρι και το τέλος της ζωής τους.

Ωστόσο, πολλές εφαρμογές της αναπτύχθηκαν πρόσφατα και οι πλήρεις δυνατότητές τους πρόκειται να μελετηθούν από τους φυσικούς και τους μηχανικούς τον 21ο αιώνα (Gisin et al. 2002). Κάποιες από τις εφαρμογές είναι και αυτές στον Κβαντικό Υπολογισμό, την Κβαντική Πληροφορία, τα Κβαντικά Συστήματα Μετάδοσης, με συνέπεια την Κβαντική Κρυπτογραφία.

Ιστορικό Κβαντικής Κρυπτογραφίας

Για πολλά χρόνια, οι μαθηματικοί αναζητούσαν ένα σύστημα, το οποίο θα επέτρεπε σε δύο ανθρώπους να ανταλλάσσουν πληροφορίες με απόλυτη ασφάλεια. Στη δεκαετία του '40, ο Claude Shannon απέδειξε ότι αυτός ο στόχος είναι ανέφικτος, εκτός κι αν τα δύο μέρη που επικοινωνούν μοιράζονται ένα τυχαίο μυστικό κλειδί σε μήκος όσο και το μήνυμα που επιθυμούν να ανταλλάξουν. Επιπλέον, το μυστικό αυτό κλειδί είναι εφικτό να χρησιμοποιηθεί μόνο μια φορά.

Αυτό το θεώρημα ήρθε να ανατρέψει η κβαντική κρυπτογραφία εκμεταλλευόμενη τόσο την αδυναμία να μετρηθεί με ακρίβεια η κβαντική πληροφορία όσο και τη διαταραχή που προκαλείται αναπόφευκτα από τέτοιες μετρήσεις. Όταν η πληροφορία κωδικοποιείται κατάλληλα σε κβαντικές καταστάσεις, οποιαδήποτε προσπάθεια κάποιου ωτακουστή για πρόσβαση σ' αυτήν ενέχει αναγκαστικά τον κίνδυνο η πληροφορία να καταστραφεί ανεπανόρθωτα. Η διαταραχή αυτή μπορεί ν' ανιχνευτεί από τους νόμιμους χρήστες της με τη βοήθεια κάποιων αλγοριθμικών διαδικασιών, επιτρέποντας έτσι την εγκατάσταση μιας ασφαλούς σύνδεσης. Σε αντίθεση με την

κλασσική κρυπτογραφία, η οποία βασίζεται σε ιδιότητες υπολογιστικής πολυπλοκότητας συγκεκριμένων μαθηματικών συναρτήσεων που δεν προσφέρουν καμία εγγύηση, καθώς εξαρτώνται μεταξύ άλλων και από τη διαθέσιμη τεχνολογία, η κβαντική κρυπτογραφία βασίζεται στις αρχές της κβαντικής μηχανικής.

Αναλυτικότερα, η κβαντική κρυπτογραφία αποτελεί ένα σχετικά καινούργιο πεδίο έρευνας που πρωτοεμφανίστηκε στη δεκαετία του '70 ως μια προσπάθεια δημιουργίας ενός νέου τρόπου κρυπτογράφησης που θα έδινε λύση σε ορισμένα προβλήματα της μοντέρνας κρυπτογραφίας και προφανώς ακόμη βρίσκεται στα πρώτα στάδια εξέλιξης. Αποτελεί την τομή της κβαντικής μηχανικής και της θεωρίας της πληροφορίας, ενώ η κβαντική μηχανική σε συνδυασμό με τη σχετικότητα, το EPR παράδοξο (Einstein et al. 1935) που εξηγείται παρακάτω, έχουν σχέση με την ασφάλεια της κβαντικής κρυπτογραφίας (Gisin et al. 2002). Αν και ως ιδέα συλλήφθηκε νωρίς, η πραγματοποίηση διάφορων προτάσεων ήτανε και παραμένει δύσκολη υπόθεση, εξαιτίας της δυσκολίας υλοποίησης. Η κατασκευή αρχιτεκτονικών υπολογιστών κβαντικής τεχνολογίας είναι ένα άλλο δύσκολο ζήτημα που επιβραδύνει σημαντικά την εξέλιξη.

Όλα ξεκινάνε το 1948 με τη δημοσίευση μιας εργασίας του Claude Shannon, βάσει της οποίας τέθηκαν τα μαθηματικά θεμέλια της θεωρίας της πληροφορίας, επάνω στα οποία βασίστηκαν μεταγενέστεροι. Η θεωρία της πληροφορίας είναι ένας κλάδος των εφαρμοσμένων μαθηματικών που μελετά τρόπους που ποσοτικοποιούν την πληροφορία, καθώς και τα όρια συμπίεσης μιας πληροφορίας για μια αξιόπιστη μετάδοση δεδομένων, γεγονός που σχετίζεται άμεσα με την κρυπτογραφία.

Παρόλα αυτά, ως ακρογωνιαίος λίθος έναρξης της κβαντικής κρυπτογραφίας θεωρείται το κβαντικό σύστημα, επάνω στο οποίο στηρίχθηκαν όλες οι προτάσεις υλοποίησης, καθώς μέσα σε αυτό κωδικοποιείται η πληροφορία. Συχνά στη βιβλιογραφία αντιμετωπίζεται ως μια αποθηκευτική φυσική μονάδα, ως ένα άτομο ή ποσότητα ηλεκτρομαγνητικής ακτινοβολίας. Το κβαντικό σύστημα κρυπτογραφίας, ουσιαστικά, είναι μια επέκταση της κβαντικής επικοινωνίας. Τα σωματίδια κωδικοποιούνται σε κβαντικές καταστάσεις και αποστέλονται στο δέκτη. Οι καταστάσεις αντιπροσωπεύουν τις κωδικοποιημένες πληροφορίες που μπορούν να υποβληθούν σε επεξεργασία και να γίνουν κατανοητές μόνο από αυτόν που τις λαμβάνει στο τέλος. Να σημειωθεί ότι οι υπάρχουσες μέθοδοι κβαντικής κρυπτογραφίας κάνουν χρήση των φυσικών ιδιοτήτων

του συστήματος μόνο για την παραγωγή του κλειδιού. Η ίδια η μεταφορά της πληροφορίας γίνεται με τον κλασσικό τρόπο και για την κρυπτογράφηση μπορεί να χρησιμοποιηθεί οποιοσδήποτε από τους γνωστούς αλγορίθμους. Ο πλήρης έλεγχος σε μεμονωμένα κβαντικά συστήματα, όπως, για παράδειγμα, ο εγκλωβισμός ενός ατόμου και η επεξεργασία των χαρακτηριστικών του, έγιναν προσπάθειες να επιτευχθεί στη δεκαετία του '70. Το γεγονός ήταν ιδιαίτερης αξίας, διότι είχε να προσφέρει σημαντική πρόοδο στην υλοποίηση εφαρμογών που επεδίωκαν τα ερευνητικά πεδία της κβαντικής πληροφορίας και της υλοποίησης των κβαντικών υπολογιστών.

Η κβαντική κρυπτογραφία ως ιδέα πρωτοεμφανίστηκε από τον Stephen Wiesner στις αρχές του 1970, όταν εργαζόταν στο πανεπιστήμιο Columbia της Ν. Υόρκης, δημοσιεύοντας μια εργασία σχετική με την κωδικοποίηση πληροφορίας σε συζευγμένα κβαντικά συστήματα (quantum conjugate coding). Αν και, αρχικά, η εργασία του απορρίφθηκε, το 1983 δημοσιεύτηκε. Το θέμα της εργασίας αναφερόταν στο πώς να αποθηκεύσει και να μεταφέρει κανείς δύο μηνύματα σε δύο συζυγείς φυσικές ιδιότητες ενός κβαντικού συστήματος και στη συνέχεια να αποκωδικοποιήσει τη μια από αυτές.

Για πολλά χρόνια, ο σχεδιασμός ενός πρωτοκόλλου που θα απέκρυπτε και θα δέσμευε τα bits, με χρήση κβαντικών μέσων, εθεωρείτο ως κλειδί για να ξεκλειδωθεί κάθε τι που είναι επιθυμητό να συμβεί με την κρυπτογραφία. Το 1984, από τους Charles Bennett και Gilles Brassard, προτάθηκε μια μέθοδος υλοποίησης ασφαλούς επικοινωνίας βασισμένη στη δημοσίευση του Wiesner. Η εργασία τους αποτέλεσε το βασικό πρωτόκολλο BB84. Ο ιδιαίτερος τρόπος λειτουργίας του συγκεκριμένου πρωτοκόλλου ξεχώρισε και αυτό γιατί η ασφάλεια που παρέχει έχει αποδειχθεί και δε βασίζεται στη δυσκολία επίλυσης υπολογιστικών προβλημάτων, κάτι που συμβαίνει με τα περισσότερα μοντέρνα πρωτόκολλα διαμοίρασης μυστικού κλειδιού.

Το 1985, ο Deutsch ασχολήθηκε με το θέμα εάν υπάρχει κάποιο υπολογιστικό μοντέλο, όπως η Μηχανή του Turing, το οποίο υπόσχεται ότι μπορεί να προσομοιώνει αποτελεσματικά κάθε άλλο υπολογιστικό μοντέλο. Το μοντέλο ¨Καθολικός Κβαντικός Υπολογιστής¨ που προτάθηκε υποστήριζε ότι ξεπερνάει τη δύναμη των κλασικών υπολογιστών, ακόμη και των πιθανοτικών υπολογιστικών μοντέλων.

Το 1990, από τον Artur Ekert, ένα διδακτορικό φοιτητή του πανεπιστημίου της Οξφόρδης, αναπτύχθηκε μια διαφορετική προσέγγιση της κβαντικής κρυπτογραφίας,

βασιζόμενη στην ιδιόμορφη φύση των κβαντικών συσχετισμών, η οποία είναι γνωστή ως διεμπλοκή.

Παράλληλα, η προσπάθεια του Deutsch βελτιώθηκε μέσα στην επόμενη δεκαετία και το 1994 κορυφώθηκε με την απόδειξη του Peter Shor πως ένας κβαντικός υπολογιστής μπορεί να λύσει αποτελεσματικά το μαθηματικό πρόβλημα της παραγοντοποίησης ενός ακέραιου σε πρώτους παράγοντες και το πρόβλημα του διακριτού λογάριθμου. Το γεγονός αυτό, ενίσχυσε το ενδιαφέρον, καθώς μέχρι πρόσφατα τα δύο αυτά προβλήματα δεν έχει αποδειχθεί ότι μπορούν να λυθούν αποτελεσματικά από τους κλασικούς υπολογιστές.

Η ανακάλυψη του αλγόριθμου του Grover, το 1995, αν και συγκριτικά δεν ήταν τόσο θεαματική με αυτή του Shor, από την άποψη της ταχύτητας, ωστόσο, βρήκε ιδιαίτερη απήχηση εξαιτίας της ευρείας εφαρμογής του. Το πρόβλημα σχετίζεται με την αναζήτηση σε μη δομημένο πεδίο. Συγκεκριμένα, ανακαλύπτει έναν κβαντικό αλγόριθμο που επιταχύνει την αναζήτηση βάσεων δεδομένων σε πολυωνυμικό χρόνο.

Το 1998, για πρώτη φορά, παρουσιάζεται η λειτουργία κβαντικού NMR υπολογιστή 2-qubit και έπειτα 3-qubit. Ακολουθεί, για πρώτη φορά, η εκτέλεση του αλγόριθμου του Grover. Έπειτα από δύο χρόνια, παρουσιάζεται η λειτουργία κβαντικού NMR υπολογιστή των 5-qubit και στη συνέχεια των 7-qubit. Επιπλέον, εκτελείται τμήμα του κβαντικού αλγόριθμου του Shor, ενώ το 2001, για πρώτη φορά, εκτελείται ολόκληρος ο αλγόριθμος Shor και παραγοντοποιείται ο αριθμός 15.

Το 2004, γίνεται διαθέσιμο το πρώτο εμπορικό κβαντικό σύστημα κρυπτογραφίας από την εταιρεία id Quantique.

ΚΒΑΝΤΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ

Γενικά

Η ιδέα για τη δημιουργία ενός υπολογιστή βασιζόμενο στις αρχές της κβαντικής μηχανικής διατυπώθηκε στις αρχές της δεκαετίας του ’90, όταν από τους φυσικούς Richard Feynman, David Deutsch και Paul Benioff διαπιστώθηκε ότι οι κλασικοί υπολογιστές παρουσιάζουν βασικούς περιορισμούς στο χρόνο και στη μνήμη για την εκτέλεση βασικών λειτουργιών. Σύμφωνα με τον εμπειρικό νόμο του Moore, κάθε δύο χρόνια η χωρητικότητα της μνήμης των υπολογιστών διπλασιάζεται. Συνεπώς, έγινε κατανοητό ότι το μέγεθος της βασικής μονάδας μνήμης του υπολογιστή ολοένα και θα μικραίνει μέχρι το έσχατο όριο των ατομικών διαστάσεων, επομένως και οι υπολογιστές θα μπορούσαν να κατασκευαστούν από το ίδιο το άτομο παρουσία κβαντικών κανόνων. Ο Feynman ήταν ο πρώτος που προσπάθησε να δώσει λύση στο παραπάνω ζήτημα με την παραγωγή ενός προτύπου που έδειχνε πώς ένα κβαντικό σύστημα θα ήταν δυνατό να χρησιμοποιηθεί από ένα φυσικό για να πραγματοποιήσει πειράματα στην κβαντική φυσική και να κάνει υπολογισμούς. Στο πέρας του χρόνου, ωστόσο, εμφανίστηκαν διάφορες τεχνολογίες που σύντομα βρέθηκαν αντιμέτωπες με δύο ριζικά τεχνολογικά προβλήματα που υφίστανται εν μέρει ακόμη, το φαινόμενο του θορύβου που παρουσιάζεται στα κβαντικά συστήματα και η αβεβαιότητα που διέπει τους νόμους της κβαντομηχανικής.

Τι είναι στην ουσία όμως ο Κβαντικός Υπολογισμός (Quantum Computing); Πρόκειται για ένα μοντέλο υπολογισμού που εκμεταλλεύεται τις ιδιότητες των κβαντικών αντικειμένων, όπως είναι η υπέρθεση καταστάσεων ή η διεμπλοκή, έννοιες οι οποίες θα εξεταστούν στην συνέχεια. Βασίζεται στη δημιουργία κβαντικών λογικών πυλών, οι οποίες επεξεργάζονται τις πληροφορίες σε έναν κβαντικό υπολογιστή. Η βασική μονάδα εγγραφής και επεξεργασίας της πληροφορίας στον κβαντικό υπολογισμό, το κβαντικό ανάλογο του κλασικού bit δηλαδή, είναι το qubit (quantum bit). Δεν αποτελεί ένα κλασικό αντικείμενο όπως είναι μία μαγνητική ψηφίδα μνήμης, αλλά ένα κβαντικό σύστημα. Η στιγμιαία κατάσταση ενός κβαντικού συστήματος αποδίδεται μέσω μετρήσεων των πιθανοτήτων των παρατηρήσιμων ιδιοτήτων του, όπως είναι η ενέργεια ή η θέση του. Η ειδοποιός διαφορά με το κλασικό ομόλογό του είναι ότι κάθε κβαντοδυφίο (qubit) γίνεται να βρεθεί πριν τη μέτρηση σε οποιαδήποτε επαλληλία των βασικών καταστάσεων $|0\rangle$ και $|1\rangle$ της μορφής $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, όπου ισχύει $|\alpha|^2 +$

$|\beta|^2$ =1. Έτσι ο καταχωρητής, για παράδειγμα, ενός κβαντικού υπολογιστή δύο κβαντοδυφίων μετράται στις ακόλουθες τέσσερις βασικές καταστάσεις: $|00\rangle \equiv |0\rangle\ |0\rangle$, $|01\rangle \equiv |0\rangle\ |1\rangle$, $|10\rangle \equiv |1\rangle\ |0\rangle$, $|11\rangle \equiv |1\rangle\ |1\rangle$, ενώ πριν τη μέτρηση μπορεί να βρεθεί σε οποιαδήποτε επαλληλία της μορφής:

$|\Psi\rangle \equiv c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$, με $\sum_{\alpha,\beta} |c_{\alpha\beta}|^2 = 1$, όπου α,β ∈ {0, 1}.

Η διαπίστωση αυτή δε συνιστά παραδοξότητα. Ο καταχωρητής κατά τη διάρκεια ενός κβαντικού υπολογισμού δεν επιδέχεται καμία μέτρηση, αλλά διαχειρίζεται ταυτόχρονα το σύνολο των καταστάσεων επαλληλίας, αυξάνοντας εκθετικά τις δυνατότητές του. Το φαινόμενο αυτό είναι γνωστό ως Μαζικός Κβαντικός Παραλληλισμός και συνιστά το θεμελιώδη μηχανισμό κάθε τέτοιου υπολογιστή. Αυτό επιτρέπει ορισμένα προβλήματα, των οποίων η δυσκολία αυξάνεται εκθετικά με το μέγεθος του προβλήματος στο κλασικό μοντέλο υπολογιστή, να κλιμακώνονται πολυωνυμικά ή ακόμα και γραμμικά στο κβαντικό μοντέλο, καθιστώντας έτσι δυνατή μια λύση ακόμα και για μεγάλα συστήματα που παίρνει εκατομμύρια ή και δισεκατομμύρια μέρες στους σημερινούς υπολογιστές.

Στην πράξη, η μνήμη ενός κβαντικού υπολογιστή αποτελείται από ένα πλήθος κβαντοδυφίων κοντά το ένα στο άλλο αλλά και τόσο μακρυά, ώστε να είναι δυνατός ο ανεξάρτητος έλεγχός τους από κατάλληλα εξωτερικά πεδία. Ένας κβαντικός υπολογιστής χειρίζεται τα qubits μέσω των κβαντικών λογικών πυλών, οι οποίες υλοποιούν μετασχηματισμούς σε ένα ή σε ζευγάρι qubits. Τοποθετώντας τις κβαντικές πύλες σε μία συγκεκριμένη σειρά, ένας κβαντικός υπολογιστής έχει τη δυνατότητα να πραγματοποιήσει περίπλοκους μετασχηματισμούς σε μία σειρά από qubits από μία αρχική κατάσταση στην τελική. Στη συνέχεια, τα qubits μπορούν να μετρηθούν στην τελική τους κατάσταση και από τις μετρήσεις αυτές να προκύψει ένα τελικό υπολογιστικό αποτέλεσμα.

Τα περισσότερα μοντέρνα chips, στα οποία ενσωματώνονται αυτές οι πύλες, έχουν transistors στο μέγεθος των 180 nanometers, περισσότερο από 400 φορές στενότερα από ό,τι η ανθρώπινη τρίχα. Αλλά οι κατασκευαστές των chip δεν μπορούν να φτιάξουν chips μεγέθους μικρότερου των 124 nanometers, σύμφωνα με μια βασική αρχή της οπτικής, γνωστή ως κριτήριο του Rayleigh. Επομένως, τα όρια των σημερινών τεχνικών συναντώνται σε αυτή την περιοχή μεγέθους.

Οι επιστήμονες εικάζουν πως αν χρησιμοποιηθούν τα πεπλεγμένα φωτόνια αντί για τα συμβατικά φωτόνια των laser, θα μπορούν να ξεπεραστούν τα όρια των 124 nm και να φτιαχτούν έτσι transistors μικρότερα των 64 nanometers. Τα πεπλεγμένα αυτά φωτόνια θα μπορούν να ταξιδεύουν μαζί και να συμπεριφέρονται σαν ένα μοναδικό φωτόνιο αντί για δύο ξεχωριστά και αυτό γιατί έχουν ως σύστημα το μισό μήκος κύματος από ό,τι έχουν ως ατομικά σωματίδια. Ακόμη, ευελπιστούν ότι οι κβαντικοί υπολογιστές που θα μεταφέρουν τις πληροφορίες κατ' αυτό τον τρόπο και όχι με τα καλώδια και τα τσιπ του πυριτίου, θα είναι απείρως γρηγορότεροι και ισχυρότεροι από τους παρόντες υπολογιστές.

Αν και έχουν υλοποιηθεί πολλές λειτουργίες όσον φορά τους κβαντικούς υπολογιστές και η έρευνα συνεχίζεται και σε θεωρητικό και σε πρακτικό επίπεδο, σήμερα, τα περισσότερα γνωστά κβαντικά υπολογιστικά συστήματα που έχουν υλοποιηθεί λειτουργούν επάνω σε έναν μικρό μόνο αριθμό Qubits και χρειάζονται ψυγεία στο μέγεθος δωματίου για να κρατηθούν σε θερμοκρασίες κοντά στο απόλυτο μηδέν. Το θέμα της επεξεργαστικής ισχύος τους είναι μείζονος σημασίας, καθώς σχετίζεται άμεσα με το χώρο της κρυπτανάλυσης, αφού μπορεί να προκαλέσει την κατάρρευση γνωστών κρυπτογραφικών συστημάτων, αντιμετωπίζοντας, για παράδειγμα, υπολογιστικά τα μεγάλα κλειδιά που χρησιμοποιούνται, ένα γεγονός που θα αποτελούσε σίγουρα ¨επανάσταση¨ στη μοντέρνα κρυπτογραφία.

Κβαντικά Συστήματα ή Qubits

Οποιοδήποτε σύστημα διαθέτει μια ποσότητα, η οποία μπορεί να παρατηρηθεί, διατηρείται με την εξέλιξη του χρόνου και έχει τουλάχιστον δύο διακριτές και επαρκώς κατανεμημένες διαδοχικές ιδιοτιμές, είναι κατάλληλο για να υλοποιήσει ένα qubit.

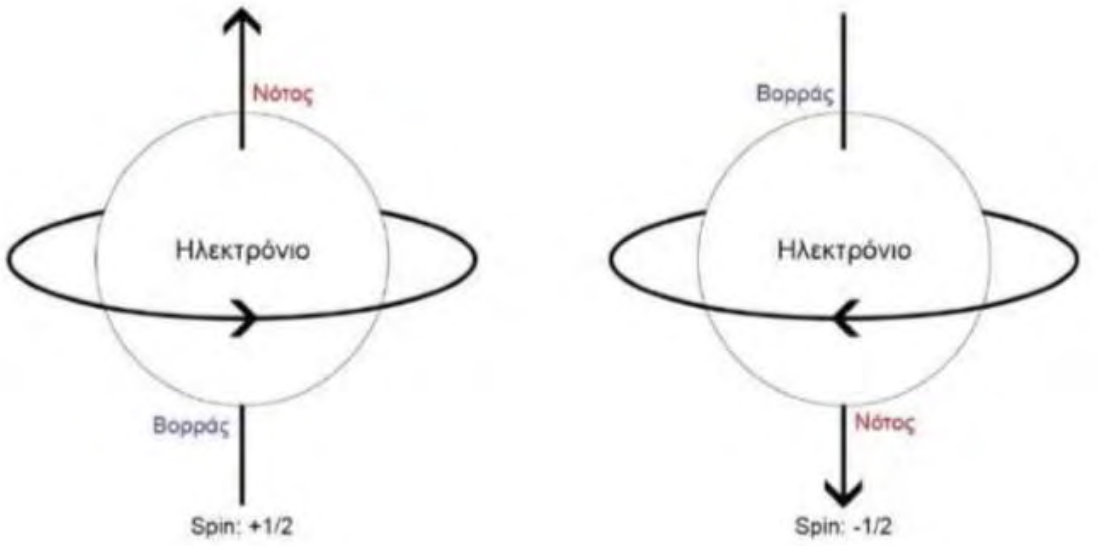
Ένα qubit μπορεί να έχει και φυσική και μαθηματική υπόσταση. Από μαθηματικής πλευράς, όπως ήδη έχει αναφερθεί, το qubit αποτελεί ένα διάνυσμα ενός κβαντικού συστήματος δύο καταστάσεων, έστω $|0\rangle$ και $|1\rangle$, και κάθε δυνατή κατάσταση εκφράζεται από μία κυματοσυνάρτηση, έστω ψ, ως γραμμικός συνδυασμός αυτών : $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, όπου $\alpha,\beta \subset \mathbb{C}$. Λέγεται τότε ότι το σύστημα βρίσκεται σε μια κατάσταση κβαντικής υπέρθεσης. Οι τιμές $|\alpha|^2$ και $|\beta|^2$ είναι η πιθανότητα εμφάνισης των δύο καταστάσεων αντίστοιχα κατά την ανάγνωση (μέτρηση) ενός qubit (εξού και το όνομα των α,β ¨πλάτος πιθανότητας¨) και θα πρέπει να ικανοποιούν την ήδη γνωστή

σχέση κανονικοποίησης $|\alpha|^2 + |\beta|^2=1$. Επομένως, μπορεί να θεωρηθεί ότι ένα qubit, πριν τη μέτρηση, καταλαμβάνει μια κατάσταση που είναι ένας συνδυασμός τόσο της κατάστασης "0" όσο και της κατάστασης "1". Δύο qubits, συνεπώς, έχουν τη δυνατότητα να αναπαραστήσουν οποιαδήποτε υπέρθεση τεσσάρων δυνατών καταστάσεων, ενώ 3 qubits οποιαδήποτε υπέρθεση 8 δυνατών καταστάσεων. Ένας κβαντικός υπολογιστής, γενικότερα, με n qubits είναι δυνατό να βρίσκεται ταυτοχρόνως σε υπέρθεση των έως 2^n καταστάσεων. Το σύμβολο $|\rangle$ ονομάζεται ket και συμβολίζει ένα πίνακα στήλη (ένα qubit μπορεί να αναπαρασταθεί και με τη μορφή πίνακα) π.χ $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$ ή διάνυσμα. Η λέξη ket προέρχεται από τα τρία τελευταία γράμματα της λέξης bracket που σημαίνει αγκύλη.

Μετά τη μέτρηση, συνεχίζοντας, μπορεί να πάρει μόνο μία εκ των δύο τιμών “0” και “1” που αντιστοιχούν στα ανάλογα ket, η οποία καθορίζεται πιθανοκρατικά κατά την ανάγνωσή του, βάσει της κυματοσυνάρτησης που εκφράζει το σύστημα που χρησιμοποιείται για να κωδικοποιηθεί η πληροφορία στο φυσικό κόσμο. Δεν παίζει ρόλο το πόσο έξυπνα έχει κωδικοποιηθεί το qubit ή πόσο έξυπνα γίνεται η μέτρηση. Το εξαιρετικό αυτό αποτέλεσμα αποδείχτηκε το 1973 από τον Alexander S. Holevo του Μαθηματικού Ινστιτούτου του Steklov στη Μόσχα, ύστερα από μια εικασία που διατύπωσε το 1964 ο J. P. Gordon των εργαστηρίων AT&T Bell. Αυτή η ιδιότητα του κβαντοδυφίου είναι που κάνει την κβαντική πληροφορία τόσο δύσκολη στην χειραγώγησή της, καθώς για να εκμεταλλευτεί κανείς την πλεονάζουσα πληροφορία για να κάνει παράλληλους υπολογισμούς, θα πρέπει να βρει μια πρακτική και ρεαλιστική μέθοδο, ώστε να μην την καταστρέφει. Είναι σαν το qubit να περιέχει κρυμμένη πληροφορία, την οποία μπορεί μεν κανείς να χειριστεί, αλλά δεν μπορεί να έχει κατευθείαν πρόσβαση σ' αυτή. Συνεπώς, είναι αντιληπτό πως το θέμα της μέτρησης σε υποατομικό επίπεδο είναι αρκετά περίπλοκο και δύσκολο. Το φαινόμενο αυτό, γνωστό ως αρχή της απροσδιοριστίας, περιγράφηκε το 1927 από το γερμανό W. Heisenberg. Η κατάσταση ενός συστήματος, λοιπόν, είναι ανέφικτο να προσδιοριστεί με ακρίβεια.

Παράδειγμα φυσικού κβαντικού συστήματος δύο καταστάσεων που μπορεί να χρησιμοποιηθεί για την κωδικοποίηση ενός qubit αποτελεί ένα φωτόνιο βάσει της πόλωσής του, ένα ηλεκτρόνιο βάσει του spin του ή ακόμα και ένας κατάλληλος πυρήνας βάσει πάλι του spin του. Η κατάσταση του spin ενός σωματιδίου, δηλαδή, με

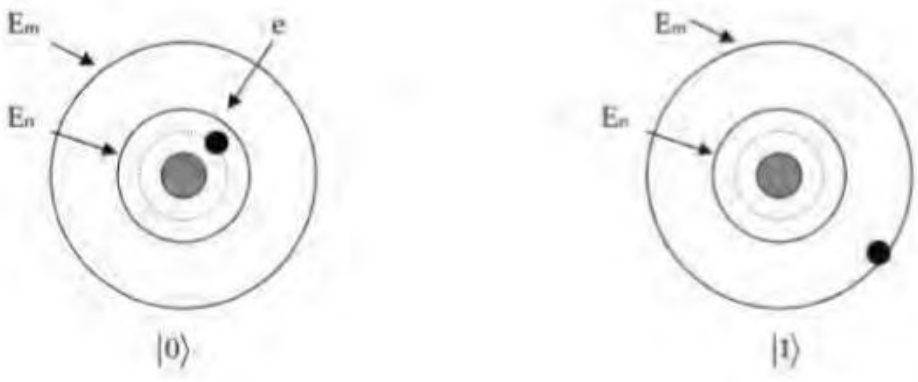
spin ½ μπορεί να θεωρηθεί ως qubit, όπου η κατάσταση spin +1/2 αντιστοιχεί στη βασική κατάσταση 0 και η κατάσταση spin -1/2 στη βασική κατάσταση 1.



Εικόνα 1: Κωδικοποίηση ενός qubit με βάση το spin ενός ηλεκτρονίου

Πηγή:
http://ikee.lib.auth.gr/record/135098/files/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE.pdf

Η διεύθυνση πόλωσης ενός φωτονίου, από την άλλη, μπορεί να αναπαραστήσει ένα qubit, όπου η οριζόντια πόλωση αντιπροσωπεύει την κατάσταση 0 και η κάθετη την 1. Ένα qubit είναι δυνατό να αναπαρασταθεί και από δύο διακριτά ενεργειακά επίπεδα, έστω Em και En, σε ένα άτομο. Η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με Em αντιστοιχεί στην κατάσταση 1 και η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με En αντιστοιχεί στην κατάσταση 0.



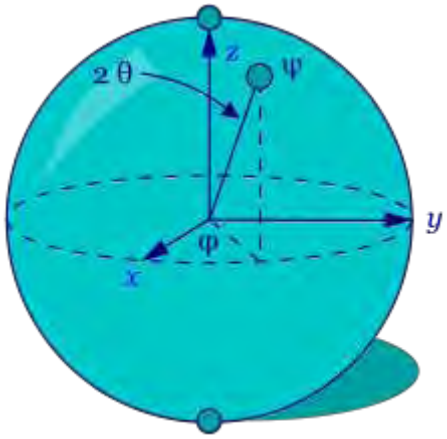
Εικόνα 2: Αναπαράσταση ενός qubit από δύο διακριτά ενεργειακά επίπεδα ενός ατόμου

Πηγή: https://ir.lib.uth.gr/bitstream/handle/11615/46115/14020.pdf?sequence=1

Κατά τη μετάβαση του ηλεκτρονίου από το ένα ενεργιακό επίπεδο στο άλλο απαιτείται μια ποσότητα ενέργειας για συγκεκριμένο χρονικό διάστημα. Αν αυτό το διάστημα είναι λίγο λιγότερο, τότε μπορεί να επιτευχθεί κατάσταση υπέρθεσης. Γενικά, ένα qubit έχει τη δυνατότητα να βρίσκεται οπουδήποτε, ακόμη και σε παραπάνω από ένα σημεία στο χώρο ταυτόχρονα. Αυτό εξηγεί και το γεγονός ότι το qubit μπορεί να είναι συγχρόνως 0 και 1 σε αντίθεση με το κλασικό bit.

Τέλος, είναι σημαντικό να αναφερθεί ότι τα qubits είναι εξαιρετικά ευαίσθητα. Τυχαίες αλληλεπιδράσεις με το περιβάλλον τους οδηγούν στην υποβάθμιση των υπερθέσεων πολύ γρήγορα, μετατρέποντάς τις σε τυχαία διατεταγμένα κλασικά bits.

Όσον αφορά τη φυσική πλευρά, το διάνυσμα κατάστασης ενός συστήματος Qubit αναπαρίσταται καλύτερα στη σφαίρα Bloch, όπου αναδεικνύονται όλα τα χαρακτηριστικά του. Η σφαίρα Bloch παριστάνει ένα μεμονωμένο διάνυσμα κατάστασης, έστω $|\Psi\rangle$, με μήκος ίσο με τη μονάδα, όπου η αρχή του ξεκινάει από το κέντρο της σφαίρας και το βέλος εφάπτεται στην εσωτερική επιφάνειά της. Όταν βρισκόμαστε στην $|0\rangle$ βασική κατάσταση το διάνυσμα δείχνει στον κατακόρυφο άξονα με φορά προς τα επάνω, ενώ στην $|1\rangle$ δείχνει με φορά προς τα κάτω. Μία πιο επίσημη και γενικευμένη μορφή αναπαράστασης της σχέσης είναι η ακόλουθη: $|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$. Οι αριθμοί φ και θ είναι πραγματικοί αριθμοί και αναφέρονται σε γωνίες. Η γωνία θ ορίζει με ακρίβεια τις τιμές των πλατών πιθανότητας και η φ δείχνει τη γωνία φάσης.



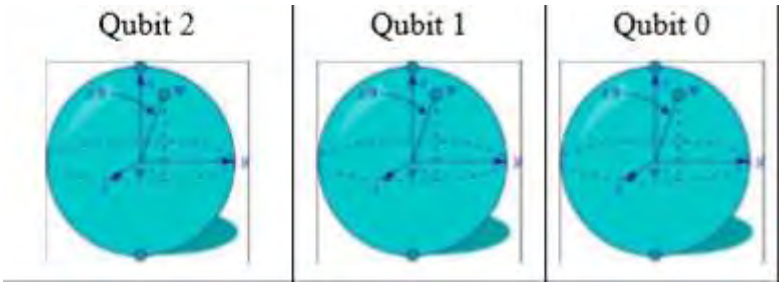
Εικόνα 3: Διάνυσμα κατάστασης ενός συστήματος Qubit στη σφαίρα Bloch

Πηγή: https://el.wikipedia.org/wiki/Qubit

Κατά τον υπολογισμό πλατών ισχύει $|e^{i\varphi}|^2 = 1$. Η γωνία φάσης μπορεί να διαφοροποιεί δύο διανύσματα, τα οποία έχουν τα ίδια πλάτη πιθανότητας, όμως αυτό πρακτικά δεν μπορεί κανείς να το διακρίνει.

Κβαντικός Καταχωρητής

Στους συμβατικούς υπολογιστές ένα σύνολο από bits αποτελεί έναν καταχωρητή. Αντίστοιχα, στους κβαντικούς υπολογιστές ένα σύνολο από qubits, συνήθως διατεταγμένα σε σειρά, αποτελεί έναν κβαντικό καταχωρητή.



Εικόνα 4: Κβαντικός καταχωρητής τριών qubits

Πηγή: https://hellanicus.lib.aegean.gr/bitstream/handle/11610/12627/file0.pdf

Η αρίθμηση των qubits, όπως παρατηρεί κανείς, γίνεται ανάποδα σε σχέση με τα bits, δηλαδή από τα δεξιά προς τα αριστερά, ενώ η σφαίρα του Bloch που υπάρχει σε κάθε θέση του κβαντικού καταχωρητή αντιπροσωπεύει το κβαντικό σύστημα.

Ακόμη, σε έναν κβαντικό καταχωρητή είναι εφικτό να αποθηκευτεί πολύ περισσότερη πληροφορία απ' ότι στον κλασικό. Παίρνοντας, για παράδειγμα, έναν κλασικό καταχωρητή των δύο bits, οι δυνατές καταστάσεις είναι 11,10,01,00. Αντιθέτως, στον δύο qubit καταχωρητή ενός κβαντικού υπολογιστή μπορούν να αποθηκευτούν και οι τέσσερις καταστάσεις ταυτοχρόνως, καθώς κάθε qubit αναπαριστά δύο τιμές. Έστω, για παράδειγμα, δύο qubit q_0 και q_1. Ο συνδυασμός των δύο, δηλαδή η κατάσταση στην οποία βρίσκεται ένας καταχωρητής των δύο qubit, είναι ένα σύστημα τεσσάρων βασικών καταστάσεων λόγω υπέρθεσης και έχει την εξής μορφή:

$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = |q_1\rangle|q_0\rangle = |q_1 q_0\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = (ac)|0\rangle\otimes|0\rangle + (ad)|0\rangle\otimes|1\rangle + (bc)|1\rangle\otimes|0\rangle + (bd)|1\rangle\otimes|1\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$ (1),

όπου $\otimes$ συμβολίζει το τανυστικό γινόμενο και $|q_R\rangle$ συμβολίζει την κατάσταση του καταχωρητή συνολικά. Τα $|q_1\rangle \otimes |q_0\rangle$, $|q_1\rangle|q_0\rangle$ και $|q_1 q_0\rangle$ συμβολίζουν το ίδιο πράγμα. Το αποτέλεσμα έχει ως πλάτη πιθανότητας τους αντίστοιχους τέσσερις μιγαδικούς

συντελεστές c_x. Η πιθανότητα να μετρηθεί η κάθε μία από τις τέσσερις βασικές καταστάσεις, στις οποίες βρίσκεται ο καταχωρητής λόγω υπέρθεσης, είναι ίση με το τετράγωνο του μέτρου των c_0, c_1, c_2 και c_3 αντίστοιχα. Συνεπώς, θα πρέπει να ισχύει $|c_0|^2+|c_1|^2+|c_2|^2+|c_3|^2=1$. Το πλεονέκτημα αυτό του κβαντικού καταχωρητή να διατηρεί τις τέσσερις βασικές καταστάσεις ταυτοχρόνως αποτελεί τη βάση της κβαντικής παραλληλίας.

Ένας άλλος συμβολισμός που χρησιμοποιείται ευρύτατα είναι η αντικατάσταση της κατάστασης του καταχωρητή από δυαδική μορφή σε δεκαδική. Συνεπώς, για την περίπτωση του καταχωρητή των δύο qubits, προκύπτει η εξής αναλογία:

Δυαδική μορφή		Δεκαδική μορφή
$\|00\rangle$	→	$\|0\rangle$
$\|01\rangle$	→	$\|1\rangle$
$\|10\rangle$	→	$\|2\rangle$
$\|11\rangle$	→	$\|3\rangle$

Εικόνα 5: Αναπαράσταση κατάστασης ενός καταχωρητή από δυαδική μορφή σε δεκαδική

Πηγή: http://ir.lib.uth.gr/bitstream/handle/11615/46115/14020.pdf?sequence=1

Γενικότερα, η κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από n Qubits δίνεται από τη σχέση: $|q_R\rangle = |q_{n-1}\rangle \otimes |q_{n-2}\rangle \otimes \ldots \otimes |q_1\rangle \otimes q_0|\rangle = |q_{n-1}\ldots q_1 q_0\rangle$. Το διάνυσμα αυτό υπάρχει σε ένα χώρο Hilbert με 2^n διαστάσεις και έχει 2^n βασικές καταστάσεις που είναι όλες ορθογώνιες μεταξύ τους. Σε κατάσταση υπέρθεσης, επομένως, ο καταχωρητής διατηρεί 2^n αριθμούς, τους αριθμούς δηλαδή από 0 έως 2^n-1:

$|q_R\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + \ldots + c_{2^n-1}|2^n-1\rangle = \sum_{i=0}^{2^n-1} c_i = |i\rangle$ ή $= c_0|0\ldots000\rangle + c_1|0\ldots010\rangle + c_2|0\ldots010\rangle + \ldots + c_{2^n-1}|111\ldots1\rangle$.

Ας εξεταστεί τώρα το τανυστικό γινόμενο με μορφή πινάκων. Έστω δύο πίνακες με μία στήλη, τον A και τον B:

$$A = \begin{bmatrix} a \\ b \end{bmatrix},\ B = \begin{bmatrix} c \\ d \end{bmatrix}$$

Το τανυστικό γινόμενο των δύο αυτών πινάκων είναι ένας πίνακας, έστω C, με μία στήλη και αριθμό στοιχείων ίσο με το άθροισμα του αριθμού των στοιχείων του A και του B:

$$C = A \otimes B = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a*c \\ a*d \\ b*c \\ b*d \end{bmatrix}.$$

Το τανυστικό γινόμενο με μορφή πίνακα, συνεπώς, των τεσσάρων βασικών καταστάσεων ενός καταχωρητή διαμορφώνεται ως εξής:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Επομένως, η (1) με μορφή πινάκων μπορεί να εκτελεστεί ως εξής:

$$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a*c \\ a*d \\ b*c \\ b*d \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} =$$

$$= c_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle.$$

Αξίζει να σημειωθεί, τέλος, πως το διάνυσμα κατάστασης του κβαντικού καταχωρητή δεν μπορεί να αναπαρασταθεί με τη χρήση της σφαίρας Bloch αλλά και με κανέναν άλλο τρόπο ο οποίος να είναι αντιληπτός και κατανοητός από τον ανθρώπινο εγκέφαλο.

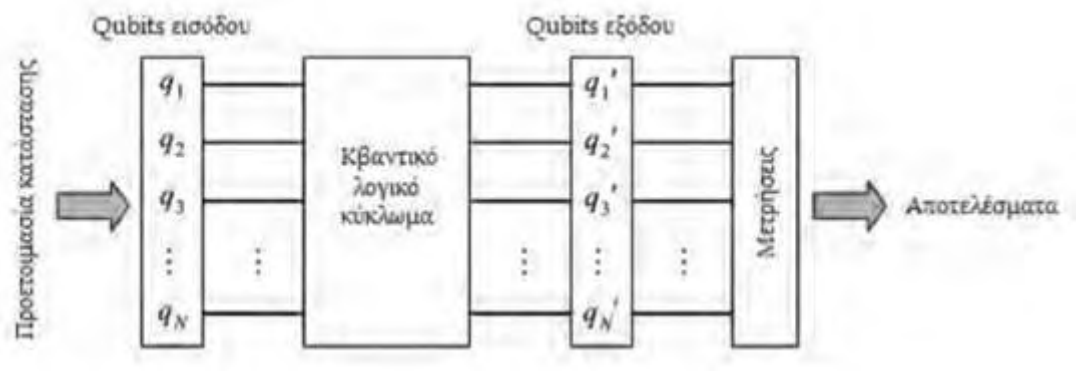
Κβαντικές Πύλες

Οι κλασικοί υπολογιστές αποτελούνται κυρίως από αγωγούς και λογικές πύλες, οι οποίες δημιουργούν κυκλώματα. Οι αγωγοί μεταφέρουν την πληροφορία μεταξύ των πυλών με τη μορφή τάσης ή ρεύματος. Οι λογικές πύλες επεξεργάζονται και

μετατρέπουν την πληροφορία που φτάνει στην είσοδό τους βασιζόμενες στον πίνακα αληθείας τους. Οι λογικές πύλες των κλασικών υπολογιστών είναι φυσικά συστήματα κατασκευασμένα από πυρίτιο, αποτελούμενα από τρανζίστορς που ονομάζονται MOSFETs.

Στους κβαντικούς υπολογιστές, οι κβαντικές πύλες αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές με μαγνητικά πεδία ή παλμούς laser. Οι δράσεις στα κβαντικά συστήματα αντιπροσωπεύονται από τελεστές, οι οποίοι περιγράφονται από πίνακες (Kaye, Lafflamme & Mosca, 2007). Συμβολίζονται με τη βοήθεια του συμβόλου ^, δηλαδή ο πίνακας R ως τελεστής θα είναι $\hat{R}$. Οι πίνακες, επομένως, επιδρούν σε ένα διάνυσμα κατάστασης που ανήκει στη σφαίρα του Bloch και το περιστρέφουν, μεταβάλλουν δηλαδή τις θ και φ γωνίες του. Εξαίρεση αποτελεί ο μοναδιαίος πίνακας, ο οποίος ασκεί μηδενική δράση επάνω σε μία κατάσταση. Η επίδραση συμβολίζεται ως ακολούθως: $\hat{R}$΄Κ1΄=΄Κ2΄, όπου ο τελεστής σε αυτή την περίπτωση έχει μεταφέρει το διάνυσμα κατάστασης από τη μία βασική του κατάσταση στην άλλη, ενώ στην περίπτωση του μοναδιαίου, ο πολλαπλασιασμός δίνει το εξής αποτέλεσμα: $\hat{I}$΄Κ΄=΄Κ΄. Ο εκάστοτε πίνακας σχετίζεται άμεσα και με τις δύο καταστάσεις. Θα ήταν δυνατό, επομένως, να ασκηθούν σε μία κατάσταση διάφορες επιδράσεις, προκαλώντας μια νέα υπέρθεση των βασικών καταστάσεων. Η διαδικασία της μετάβασης από μια αρχική κατάσταση |ψ⟩ της χρονικής στιγμής t_1 σε μια άλλη κατάσταση |ψ΄⟩ της χρονικής στιγμής t_2 ονομάζεται unitary transformation.

Μία άλλη σημαντική διαφορά ανάμεσα στις κβαντικές και τις λογικές πύλες είναι ότι η πληροφορία δε διέρχεται μέσα από τις κβαντικές πύλες. Η πληροφορία αποθηκεύεται σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί, γεγονός που συναντάται σε όλες τις υλοποιήσεις στερεάς κατάστασης κβαντικών κυκλωμάτων, όπως με παγίδες ιόντων ή με NMR. Η κβαντική πύλη αποτελεί ένα είδος κυκλώματος που πραγματοποιεί πράξεις σε qubits για κάποιο χρονικό διάστημα, ενώ σε αντίθεση με τις κλασικές πύλες είναι πάντα αντιστρεπτές. Συνεπώς, αποτελούνται από τον ίδιο αριθμό εισόδων και εξόδων.



Εικόνα 6: Λειτουργία κβαντικής πύλης (κβαντικού κυκλώματος)

Πηγή: http://ir.lib.uth.gr/bitstream/handle/11615/46115/14020.pdf?sequence=1

Ωστόσο, όλοι οι τελεστές του χώρου Hilbert δεν γίνεται να είναι κβαντικές πύλες, μιας και υπάρχουν οι ακόλουθοι περιορισμοί:

Α) Οποιαδήποτε επίδραση προκαλέσει την αλλαγή του μήκους του διανύσματος, το οποίο θα πρέπει να ισούται πάντα με τη μονάδα, απορρίπτεται.

Β) Για κάθε αλλαγή μιας κατάστασης θα πρέπει να είναι εφικτή η αντιστροφή της. Θα πρέπει, συνεπώς, να υπάρχει χρονική συμμετρία των κβαντικών συστημάτων. Αν, δηλαδή, γίνει μετάβαση από μια κατάσταση σε μία άλλη με τη βοήθεια ενός τελεστή, με τον ίδιο ακριβώς τελεστή θα πρέπει να μπορεί να γίνει επαναφορά στην προηγούμενη κατάσταση. Οι τελεστές αυτοί ονομάζονται ορθομοναδιαίοι.

Κάθε κβαντική πύλη που δρα σε n qubits περιγράφεται από έναν ορθομοναδιαίο πίνακα U διαστάσεων $2^n * 2^n$. Συνεπώς, μια κατάταξη των κβαντικών πυλών θα μπορούσε να γίνει με βάση τον αριθμό των κβαντικών συστημάτων στον οποίο δρουν.

Πύλες που δρουν σε ένα Qubit (μονοκβαντοδυφιακές)

Όπως προαναφέρθηκε, οι πύλες περιστρέφουν το διάνυσμα κατάστασης ενός συστήματος στη σφαίρα Bloch. Οι περιστροφές που θα μπορούσαν να συμβούν είναι άπειρες, συνεπώς και οι πύλες της κατηγορίας αυτής θα μπορούσαν να είναι άπειρες.

Εικόνα 7: Μονοκβαντοδυφιακή πύλη

Πηγή: http://ir.lib.uth.gr/bitstream/handle/11615/46115/14020.pdf?sequence=1

Οι σημαντικότερες πύλες αυτής της κατηγορίας είναι η πύλη αδράνειας, η πύλη μετατόπισης φάσης και η πύλη Hadamard.

Η πύλη αδράνειας δε μεταβάλλει την κατάσταση ενός κβαντικού συστήματος, ενώ συμβολίζεται με I.

$$I\,|q\rangle = |q\rangle$$

Ο πίνακας του τελεστή της πύλης αυτής είναι:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|q_{\pi\rho\iota\nu}\rangle$	$\|q_{\mu\varepsilon\tau\acute{\alpha}}\rangle$
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$
$\|q\rangle$	$\|q\rangle$

Η πύλη μετατόπισης φάσης, συμβολίζεται με Φ, αλλάζει μόνο τη γωνία φάσης του Qubit, γεγονός που δεν μπορεί να γίνει αντιληπτό με μια μέτρηση.

Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι (Barenco, 1995):

$$\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

ενώ η δράση της πύλης αυτής σε ένα qubit:

$$\Phi|q_1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ e^{i\varphi} b \end{bmatrix} = \alpha|0\rangle + e^{i\varphi} b\ \mathrm{b}|1\rangle = |q_0\rangle$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|q_1\rangle$	$\|q_0\rangle$
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{i\varphi}\|1\rangle$
$\alpha\|0\rangle + b\|1\rangle$	$\alpha\|0\rangle + e^{i\varphi} b\|1\rangle$

Κάπου εδώ αξίζει να αναφερθεί και η πύλη NOT. Λειτουργεί όπως και η κλασική NOT, δηλαδή μετατρέπει την κατάσταση από 0 σε 1 και αντίστροφα.

Ο πίνακας του τελεστή της πύλης αυτής είναι:

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

ενώ το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit έστω $|q\rangle$:

$$\text{NOT}|q\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|q_{\pi\rho\iota\nu}\rangle$	$\|q_{\mu\epsilon\tau\acute{\alpha}}\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

Τέλος, η πύλη Hadamard, η οποία συμβολίζεται με H, προκαλεί υπέρθεση σε ένα σύστημα που βρίσκεται σε μια από τις δύο βασικές καταστάσεις. Αναλυτικότερα, για την περιστροφή ενός κβαντοφυδίου, προκαλεί μια περιστροφή κατά π/4 γύρω από τον άξονα y, η οποία συνοδεύεται από μία περιστροφή κατά π γύρω από τον άξονα z. Μάλιστα, στην κατάσταση της υπέρθεσης, οι δύο βασικές καταστάσεις γίνονται ισοπίθανες και κατά τη μέτρηση του Qubit μπορεί να προκύψει είτε η μια είτε η άλλη κατάσταση με πιθανότητα 50%. Επίσης, αν εφαρμοστεί η πύλη H σε ένα σύστημα που βρίσκεται σε υπέρθεση, τότε αυτό θα επιστρέψει σε μια από τις δύο βασικές καταστάσεις ανάλογα με το από ποια προήρθε η υπέρθεση.

Ο πίνακας του τελεστή της πύλης αυτής είναι:

$$\text{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|0\rangle$:

$$\text{H}|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|1\rangle$:

$$\mathrm{H}|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Για την αντίστροφη διαδικασία αντίστοιχα:

$$\mathrm{H}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$\mathrm{H}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Να σημειωθεί ότι η δράση της πύλης Hadamard σε ένα σύστημα n qubit ονομάζεται μετασχηματισμός Walsh ή μετασχηματισμός Walsh-Hadamard και συμβολίζεται με W_n, ενώ ισχύει:

$$W_1 = \mathrm{H} \text{ και } W_{n+1} = \mathrm{H} \otimes W_n$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|q_i\rangle$	$\|q_0\rangle$
$\|0\rangle$	$1/\sqrt{2}(\|0\rangle + \|1\rangle)$
$\|1\rangle$	$1/\sqrt{2}(\|0\rangle - \|1\rangle)$
$1/\sqrt{2}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$1/\sqrt{2}(\|0\rangle - \|1\rangle)$	$\|1\rangle$

Η πύλη Hadamard αποτελεί βασικό και κρίσιμο εργαλείο για τη σχεδίαση κβαντικών κυκλωμάτων, καθώς οι κβαντικοί υπολογιστές βασίζονται στην υπέρθεση των qubits για τις περισσότερες πράξεις που θα εκτελέσουν. Επιπλέον, αναμένεται οι πύλες Hadamard να αποτελέσουν το κύριο στοιχείο για τη διασύνδεση κλασικών και κβαντικών υπολογιστών.

Πύλες που δρουν σε δύο Qubits (δικβαντοδυφιακές)

Οι σημαντικότερες πύλες της κατηγορίας αυτής είναι οι πύλες ελεγχόμενου όχι και ελεγχόμενης μετατόπισης φάσης. Για να γίνει η αναπαράσταση των αποτελεσμάτων, θεωρείται ένας καταχωρητής των δύο Qubits που ξεκινά από την κατάσταση $|c_i t_i\rangle$ και καταλήγει στην κατάσταση $|c_0 t_0\rangle$.

Η πύλη ελεγχόμενου όχι ή αλλιώς πύλη ελεγχόμενης άρνησης, γνωστή και ως CNOT (Controlled-NOT), αλλάζει την κατάσταση του Qubit στόχου μόνο όταν η κατάσταση του Qubit ελέγχου είναι |1⟩. Η κατάσταση του Qubit ελέγχου δεν μεταβάλλεται.

Η πύλη CNOT περιγράφεται από τον παρακάτω πίνακα:

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

Η δράση της πύλης αυτής σε ένα κβαντικό καταχωρητή, έστω |10⟩, είναι:

$$\text{CNOT}|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

Όπως φαίνεται, η κατάσταση του qubit στόχου άλλαξε, διότι η κατάσταση του qubit ελέγχου είναι |1⟩.

Έστω τώρα ο καταχωρητής |01⟩:

$$\text{CNOT}|01\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

Στην περίπτωση αυτή, η κατάσταση του qubit στόχου δε μεταβλήθηκε, καθώς η κατάσταση του qubit ελέγχου είναι |0⟩.

Ο πίνακας αληθείας της είναι ο εξής:

$\|c_i t_i\rangle$	$\|c_0 t_0\rangle$
|00⟩	|00⟩
|01⟩	|01⟩
|10⟩	|11⟩

$\|11\rangle$	$e^{i\varphi}\|11\rangle$

Η πύλη ελεγχόμενης μετατόπισης φάσης συμβολίζεται με διάφορους τρόπους όπως S, CP, CΦ. Πολλαπλασιάζει την κατάσταση του qubit στόχου με τον παράγοντα $e^{i\varphi}$ μόνο όταν η κατάσταση του qubit ελέγχου και η κατάσταση του qubit στόχου είναι $|1\rangle$. Σε όλες τις άλλες περιπτώσεις δε μεταβάλλει τις καταστάσεις των qubits.

Η πύλη CΦ περιγράφεται από τον παρακάτω πίνακα:

$$\text{CΦ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix}$$

Η δράση της πύλης αυτής σε ένα κβαντικό καταχωρητή, έστω $|10\rangle$, είναι:

$$\text{CΦ}|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

ενώ στην περίπτωση του $|11\rangle$:

$$\text{CΦ}|11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ e^{i\varphi} \end{bmatrix} = e^{i\varphi} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = e^{i\varphi}|11\rangle$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|c_i t_i\rangle$	$\|c_0 t_0\rangle$
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$e^{i\varphi}\|11\rangle$

Αξίζει να προστεθεί και η πύλη εναλλαγής qubit ή αλλιώς SWAP, η οποία εναλλάσσει τις καταστάσεις στις οποίες βρίσκονται τα qubits.

Ο πίνακας του τελεστή της πύλης αυτής είναι:

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Η εφαρμογή της σε δύο qubits έστω q_1 και q_0 είναι:

$$q_1 = a|0\rangle + b|1\rangle$$

$$q_0 = c|0\rangle + d|1\rangle$$

$$|q_1 q_0\rangle = |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a*c \\ a*d \\ b*c \\ b*d \end{bmatrix}$$

$$\text{SWAP}(|q_1 q_0\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a*c \\ a*d \\ b*c \\ b*d \end{bmatrix} = \begin{bmatrix} a*c \\ b*c \\ a*d \\ b*d \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix} = |q_0 q_1\rangle$$

Ο πίνακας αληθείας της είναι ενδεικτικά ο εξής:

$\|q_{πριν}\rangle$	$\|q_{μετά}\rangle$
$\|q_1 q_0\rangle$	$\|q_0 q_1\rangle$
$\|q_0 q_1\rangle$	$\|q_1 q_0\rangle$

Η πύλη SWAP μπορεί να υλοποιηθεί με τρεις NOT πύλες.

Αξίζει να ειπωθεί πως οι πύλες CNOT, H και Φ αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών με το οποίο μπορεί να εκτελεστεί οποιοσδήποτε κβαντικός υπολογισμός. Ακόμη, όλες οι κβαντικές πύλες ανάγονται ως συνδυασμός δύο Hadamard και δύο πυλών φάσης (Καθολικό Θεώρημα).

Πύλες που δρουν σε τρία Qubits

Σε αυτή την κατηγορία ανήκουν η πύλη διπλά ελεγχόμενου όχι, CCNOT, και η πύλη Fredkin, F.

Η πύλη CCNOT, επινοήθηκε από τον ιταλό καθηγητή Tommaso Toffoli, γι' αυτό πολλές φορές αναφέρεται και ως πύλη Toffoli. Θεωρείται καθολική πύλη, δηλαδή μπορεί να εκτελεστεί οποιοσδήποτε κβαντικός υπολογισμός χρησιμοποιώντας μόνο αυτή. Ξεκινάει από την κατάσταση $|c_{1i}, c_{2i}, a_i\rangle$ και καταλήγει στην κατάσταση $|c_{1_0}, c_{2_0}, a_0\rangle$, όπου τα Qubits c_1 και c_2 είναι σταθερά. Το qubit a αλλάζει όταν τα δύο

ελεγχόμενα Qubits βρίσκονται στην κατάσταση |1⟩, ενώ δεν αλλάζει σε οποιαδήποτε άλλη περίπτωση.

Η πύλη CCNOT περιγράφεται από τον παρακάτω πίνακα:

$$\text{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Η δράση της πύλης αυτής σε ένα κβαντικό καταχωρητή, έστω |101⟩, είναι:

$$\text{CCNOT}|101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |101\rangle$$

ενώ στην περίπτωση που η κατάσταση του κβαντικού καταχωρητή είναι |111⟩:

$$\text{CCNOT}|111\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle$$

Ο πίνακας αληθείας της είναι ο εξής:

$\lvert c_{1i}, c_{2i}, a_i \rangle$	$\lvert c_{1_0}, c_{2_0}, a_0 \rangle$
|000⟩	|000⟩
|001⟩	|001⟩
|010⟩	|010⟩
|011⟩	|011⟩
|100⟩	|100⟩
|101⟩	|101⟩

|110⟩	|111⟩
|111⟩	|110⟩

Η πύλη F, από την άλλη, η οποία πήρε το όνομά της από τον καθηγητή Edward Fredkin, ξεκινάει από την κατάσταση $|c_i,a_i,b_i\rangle$ και καταλήγει στην κατάσταση $|c_0,a_0,b_0\rangle$. Το Qubit c είναι ελέγχου και αν είναι στην κατάσταση |1⟩, εναλλάσσει τις καταστάσεις μεταξύ των |a⟩ και |b⟩, διαφορετικά δε συμβαίνει εναλλαγή. Ουσιαστικά, κάνει χρήση του μετασχηματισμού της πύλης SWAP, γι' αυτό ονομάζεται και πύλη CSWAP.

Η πύλη F περιγράφεται από τον παρακάτω πίνακα:

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Η δράση της πύλης αυτής σε ένα κβαντικό καταχωρητή, έστω |001⟩, είναι:

$$F|001\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |001\rangle$$

ενώ στην περίπτωση που η κατάσταση του κβαντικού καταχωρητή είναι |101⟩:

$$F|101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle$$

Ο πίνακας αληθείας της είναι ο εξής:

$\|c_i,a_i,b_i\rangle$	$\|c_0,a_0,b_0\rangle$

|000⟩	|000⟩
|001⟩	|001⟩
|010⟩	|010⟩
|011⟩	|011⟩
|100⟩	|100⟩
|101⟩	|110⟩
|110⟩	|101⟩
|111⟩	|111⟩

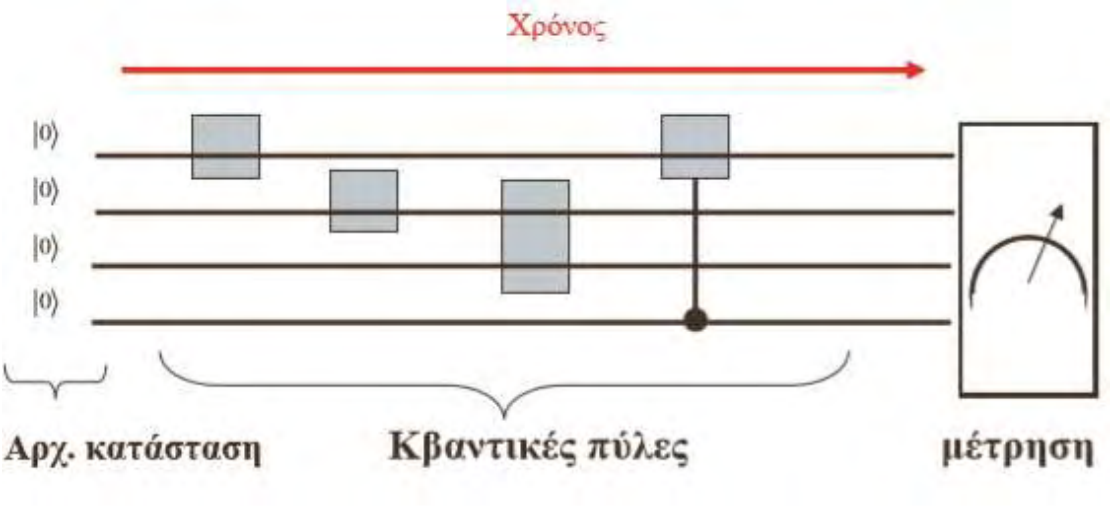
Η πύλη Fredkin είναι δυνατό να χρησιμοποιηθεί στην προσομοίωση των κλασικών πυλών NOT και AND.

Σε μια προσπάθεια να πραγματοποιηθεί αντιστοίχιση μεταξύ λογικών και κβαντικών πυλών, τα πράγματα περιπλέκονται, καθώς οι κβαντικές καταστάσεις παρουσιάζουν διαφορετική φύση. Στην περίπτωση, για παράδειγμα, της XOR, η διατήρηση της αντιστρεψιμότητας είναι αδύνατο να συμβεί, καθότι από τη φύση της πύλης είναι δύσκολο να προβλεφθεί μόνο από την έξοδο ποια ήταν τα bits εισόδου. Στην πραγματικότητα, όμως, το πρόβλημα λύνεται με τη λογική πύλη Toffoli που έχει τη δυνατότητα να μετατρέπει οποιοδήποτε κλασικό κύκλωμα σε ισοδύναμο με αντιστρεπτά στοιχεία. Ανάλογα, υπάρχει και η κβαντική πύλη Toffoli, η οποία έχει δυνατότητα προσομοίωσης κλασικών λογικών κυκλωμάτων που δε διαθέτουν την ιδιότητα της αντιστροφής και εκτέλεσης όλων των πράξεων που θα εκτελούσε ένας υπολογιστής με κλασικές πύλες. Η πύλη αυτή μπορεί να χρησιμοποιηθεί για προσομοίωση της κλασικής NAND. Επιτυγχάνοντας την υλοποίηση της κβαντικής NAND, μπορούν να προσομοιωθούν και οι υπόλοιπες κλασικές πύλες, καθώς η NAND μπορεί να χρησιμοποιηθεί για την αναπαραγωγή οποιασδήποτε λειτουργίας των άλλων λογικών πυλών. Τέλος, υπενθυμίζεται η αδυναμία ύπαρξης μιας πύλης που να αντιγράφει ένα συγκεκριμένο Qubit.

Κβαντικό Κύκλωμα

Τα κβαντικά κυκλώματα αποτελούνται από qubits, κβαντικούς καταχωρητές και κβαντικές πύλες. Στα κβαντικά κυκλώματα δεν υπάρχει ροή πληροφορίας μεταξύ των πυλών, αλλά διαδοχικές δράσεις κβαντικών πυλών σε κβαντικούς καταχωρητές στους

οποίους βρίσκεται αποθηκευμένη η πληροφορία. Τα κβαντικά κυκλώματα, δηλαδή, αντιπροσωπεύουν τη χρονική σειρά και τον τρόπο με τον οποίο δρουν οι κβαντικές πύλες στους κβαντικούς καταχωρητές.



Εικόνα 8: Κβαντικό κύκλωμα

Πηγή: http://mpla.math.uoa.gr/media/theses/msc/Rafios_X.pdf

Το θεμέλιο για την ανάπτυξη των τελικών κβαντικών κυκλωμάτων αποτέλεσε το πρώτο κβαντικό κύκλωμα, ο κβαντικός αθροιστής, η πρόταση του οποίου έγινε από τον Barenco. Είχε τη δυνατότητα να εκτελεί προσθέσεις, χρησιμοποιώντας τη μνήμη των καταχωρητών, καθώς και να αποθηκεύει δεδομένα. Επίσης, ένα ακόμη κβαντικό κύκλωμα που συνέβαλε στην ανάπτυξη των κβαντικών κυκλωμάτων ήταν ο κβαντικός πολλαπλασιαστής.

Έγιναν πολλές ερευνητικές απόπειρες για τη δημιουργία κβαντικών κυκλωμάτων και κυρίως για τη δημιουργία βέλτιστων κυκλωμάτων που θα ελλατώνουν τον υπολογιστικό χρόνο και τα σφάλματα. Από τις πρώτες έρευνες που έγιναν, κατέληξαν στο συμπέρασμα ότι οι κβαντικές πύλες του ενός και των δύο qubit είχαν τη δυνατότητα να αποτελέσουν τη βάση για την κατασκευή οποιουδήποτε κυκλώματος. Αρχικά, έγιναν έρευνες για την ανάλυση πιο σύνθετων κβαντικών πυλών από απλούστερες. Οι Chau και Wilczek ανακάλυψαν ότι η πύλη Fredkin μπορεί να προσεγγιστεί από 6 πύλες 2-qubit. Αυτό το αποτέλεσμα βελτιώθηκε από τους Smolin και DiVincenzo με την απόδειξη ότι είναι αναγκαίες μόνο 5 πύλες.

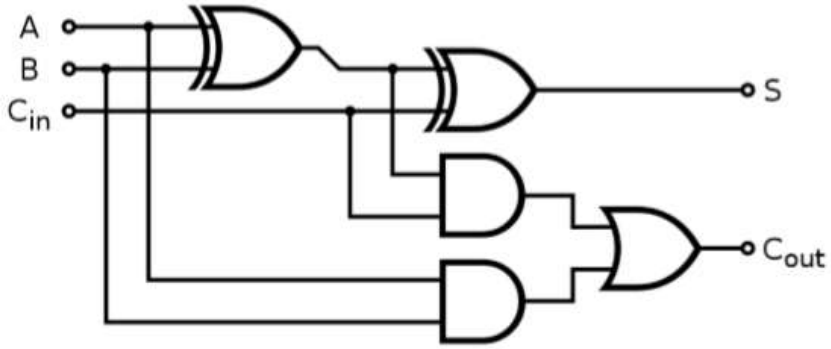
Πολλές από τις μεθόδους που προτάθηκαν ανά καιρούς στηρίζονται στις καθολικές πύλες. Κάποιες από αυτές τις μεθόδους είναι η Μέθοδος Shende, Bullock και Markov,

η Μέθοδος CSD(Cosine-sine), η Μέθοδος KGD(Khaneja-Glaser),η Μέθοδος Zhang, Vala, Sastry και Whaley, η Μέθοδος Maslov και Dueck κ.α.

Ένα βασικό θεώρημα που αφορά τα κβαντικά κυκλώματα είναι το θεώρημα αδυναμίας διακλάδωσης (no-cloning theorem). Το θεώρημα αυτό έγινε γνωστό από τους Wootters, Zurek και Dieks και αποτελεί θεμελιώδες και πολύ σημαντικό θεώρημα της επιστήμης του κβαντικού υπολογισμού. Σύμφωνα με αυτό, είναι αδύνατο να αντιγραφεί η κατάσταση ενός qubit σε ένα άλλο.

Όπως συμβαίνει στα κλασσικά λογικά κυκλώματα έτσι και στα κβαντικά, τα δεδομένα κινούνται από αριστερά προς τα δεξιά, το ίδιο και ο χρόνος.

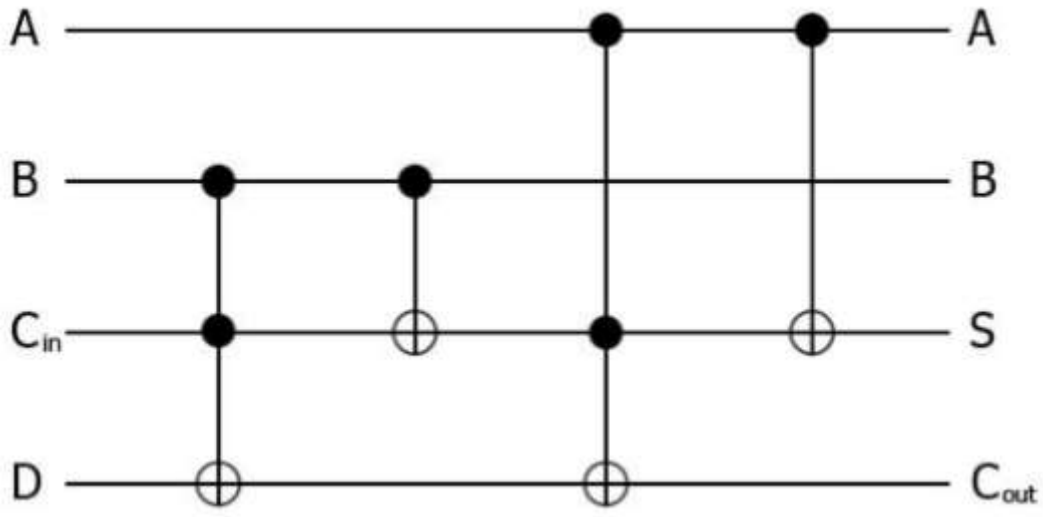
Το ακόλουθο λογικό κύκλωμα αντιπροσωπεύει έναν πλήρη αθροιστή:



Εικόνα 9: Λογικό κύκλωμα πλήρους αθροιστή

Πηγή: http://ikee.lib.auth.gr/record/135098/files/Διπλωματική.pdf

Το κβαντικό ανάλογό του είναι το εξής:



Εικόνα 10: Κβαντικό κύκλωμα πλήρους αθροιστή

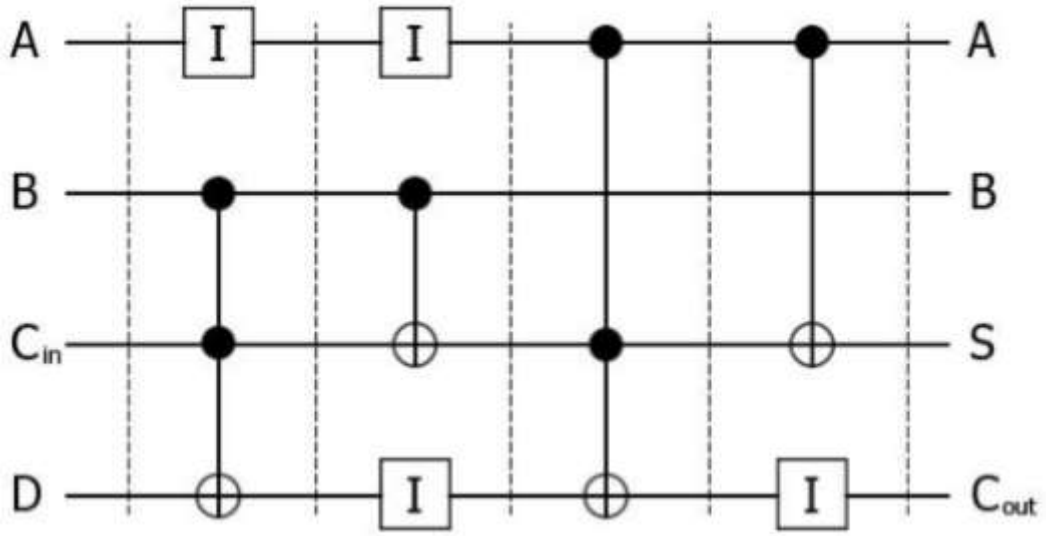
Πηγή: http://ikee.lib.auth.gr/record/135098/files/Διπλωματική.pdf

Η πρώτη διαφορά που διακρίνεται είναι η ύπαρξη τεσσάρων qubits στην είσοδο αλλά και στην έξοδο. Αντίθετα με το κλασικό κύκλωμα, στο κβαντικό οφείλεται να τηρηθεί η αντιστρεψιμότητα και για να πραγματοποιηθεί αυτό θα πρέπει το πλήθος των qubits της εξόδου να είναι ίσο με αυτό της εισόδου. Γι' αυτό το λόγο, στην είσοδο συμπεριλαμβάνεται ένα βοηθητικό qubit D (συνήθως με κατάσταση $|0\rangle$, ώστε να μην επηρεάζεται η έξοδος). Εν τέλει, τα qubits που έχουν σημασία είναι τα S και Cout, το άθροισμα και το κρατούμενο αντίστοιχα.

Μια ακόμη μεγάλη διαφορά εντοπίζεται στον τρόπο εφαρμογής και λειτουργίας του εκάστοτε κυκλώματος. Στο κλασικό κύκλωμα τα bits εισόδου εισέρχονται στο κύκλωμα ως ηλεκτρικοί παλμοί και μέσω κάποιων αγωγών μεταδίδονται από πύλη σε πύλη, ενώ, αντίθετα, στο κβαντικό κύκλωμα οι κβαντικές πύλες εφαρμόζονται με τη σειρά πάνω σε έναν κβαντικό καταχωρητή με αποθηκευμένα qubits. Επομένως, στο τέλος της εφαρμογής του κυκλώματος, παραμένει ο ίδιος καταχωρητής με διαφορετικές απλά καταστάσεις των qubits. Επίσης, ενώ η σειρά των bits στο κλασικό κύκλωμα είναι από πάνω προς τα κάτω, στο κβαντικό συμβαίνει το αντίθετο.

Μια επιπλέον διαπίστωση που μπορεί να γίνει είναι όσον αφορά τον τρόπο με τον οποίο απεικονίζεται ο χρόνος. Στην περίπτωση του κλασικού κυκλώματος, δεν μπορεί να προκύψει κάποιο σαφές συμπέρασμα για το χρόνο που απαιτείται ώστε να επεξεργαστούν τα δεδομένα εισόδου και να προκύψουν τα δεδομένα εξόδου. Αντίθετα, στο κβαντικό κύκλωμα υπάρχει διαμερισμός χρονικών διαστημάτων (βήματα), μέσα στα οποία δρά κάποια κβαντική πύλη σε κάθε qubit του κβαντικού καταχωρητή.

Τέλος, στην περίπτωση που δε συμβαίνει κάποια αλλαγή σε ένα qubit σε κάποιο χρονικό διάστημα είναι σαν να εφαρμόζεται η κβαντική πύλη αδράνειας.



Εικόνα 11: Η κβαντική πύλη αδράνειας ισοδυναμεί με μη αλλαγή της κατάστασης για συγκεκριμένο χρονικό διάστημα

Πηγή: http://ikee.lib.auth.gr/record/135098/files/Διπλωματική.pdf

Βέβαια, υπάρχουν διαφορές και στον τρόπο απεικόνισης των πινάκων αληθείας των δύο κυκλωμάτων.

Αναλυτικότερα, η διαφορά εντοπίζεται στη σειρά με την οποία εμφανίζονται τα qubits στις στήλες του πίνακα.

Πίνακας αληθείας λογικού κυκλώματος:

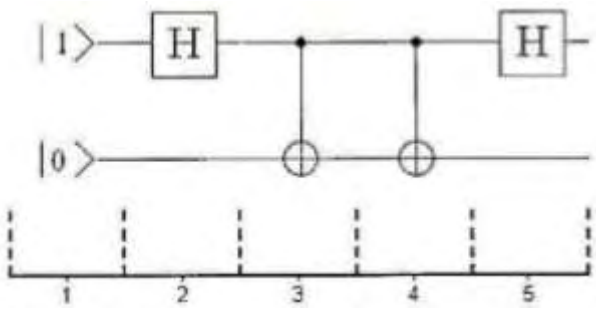
A	B	C_{in}	S	C_{out}
0	0	0	0	0
0	1	0	1	0
1	0	0	1	0
1	1	0	0	1
0	0	1	1	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	1

Πίνακας αληθείας κβαντικού κυκλώματος:

D	C_{in}	B	A	C_{out}	S	B	A
0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	1

0	0	1	0	0	1	1	0
0	0	1	1	1	0	1	1
0	1	0	0	0	1	0	0
0	1	0	1	1	0	0	1
0	1	1	0	1	0	1	0
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	0
1	0	0	1	1	1	0	1
1	0	1	0	1	1	1	0
1	0	1	1	0	0	1	1
1	1	0	0	1	1	0	0
1	1	0	1	0	0	0	1
1	1	1	0	0	0	1	0
1	1	1	1	0	1	1	1

Ένα ολοκληρωμένο παράδειγμα κβαντικού υπολογισμού είναι το ακόλουθο:



Εικόνα 12: Παράδειγμα κβαντικού υπολογισμού

Πηγή: https://dspace.lib.uom.gr/bitstream/2159/13404/2/KourtelisMsc2008.pdf

Πριν αναλυθούν τα βήματα είναι χρήσιμο να αναφερθούν τα εξής:

- Η λειτουργία n κβαντικών πυλών σε σειρά ισοδυναμεί με το αποτέλεσμα του πολλαπλασιαμού των αντίστοιχων πινάκων τους.
- Όταν συναντάται παράλληλη σύνδεση κβαντικών πυλών, το αποτέλεσμα αυτής υπολογίζεται από το γινόμενο Kronecker των πινάνων που αντιστοιχούν στις πύλες αυτές.

Γινόμενο Kronecker : $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} x & y \\ z & v \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} x & y \\ z & v \end{bmatrix} & b\begin{bmatrix} x & y \\ z & v \end{bmatrix} \\ c\begin{bmatrix} x & y \\ z & v \end{bmatrix} & d\begin{bmatrix} x & y \\ z & v \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ax & ay & bx & by \\ az & av & bz & bv \\ cx & cy & dx & dy \\ cz & cv & dz & dv \end{bmatrix}$

Βήμα 1: Ο κβαντικός καταχωρητής του κυκλώματος αποτελείται από δύο qubits και η κατάσταση του είναι η |10⟩. Ο πίνακας που αντιστοιχεί σε αυτή την κατάσταση είναι το τανυστικό γινόμενο των πινάκων των καταστάσεις των δύο qubits:

$$|10\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = 0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle$$

Βήμα 2: Στο δεύτερο βήμα του κβαντικού υπολογισμού δρουν οι πύλες I και H. Η συνολική τους δράση ισοδυναμεί με το τανυστικό τους γινόμενο. Για να υπολογιστεί το γινόμενο αυτό, γράφεται στην πιο δεξιά θέση η πύλη που δρα στο πρώτο qubit και στην πιο αριστερή θέση η πύλη που δρα στο τελευταίο qubit:

$$\mathrm{H} \otimes \mathrm{I} = \begin{bmatrix}+\frac{1}{\sqrt{2}} & +\frac{1}{\sqrt{2}}\\ +\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}+\frac{1}{\sqrt{2}} & 0 & +\frac{1}{\sqrt{2}} & 0\\ 0 & +\frac{1}{\sqrt{2}} & 0 & +\frac{1}{\sqrt{2}}\\ +\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0\\ 0 & +\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}}\end{bmatrix}$$

Μετά τη δράση των πυλών, η κατάσταση του κβαντικού καταχωρητή θα είναι η εξής:

$$(\mathrm{H} \otimes \mathrm{I})|10\rangle = \begin{bmatrix}+\frac{1}{\sqrt{2}} & 0 & +\frac{1}{\sqrt{2}} & 0\\ 0 & +\frac{1}{\sqrt{2}} & 0 & +\frac{1}{\sqrt{2}}\\ +\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0\\ 0 & +\frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\-\frac{1}{\sqrt{2}}\\0\end{bmatrix} = +\frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle - \frac{1}{\sqrt{2}}|10\rangle +$$

$$0|11\rangle = +\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Βήμα 3: Στο βήμα αυτό, δρα στον κβαντικό καταχωρητή αποκλειστικά η κβαντική πύλη Ελεγχόμενου Όχι (CNOT). Η κατάσταση του κβαντικού καταχωρητή στο τέλος αυτού του βήματος είναι η εξής:

$$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\-\frac{1}{\sqrt{2}}\\0\end{bmatrix} = \begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\0\\-\frac{1}{\sqrt{2}}\end{bmatrix} = +\frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}}|11\rangle = +\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Βήμα 4: Όπως και στο τρίτο βήμα έτσι και σε αυτό, δρα στον κβαντικό καταχωρητή μόνο η κβαντική πύλη Ελεγχόμενου Όχι. Η κατάσταση του κβαντικού καταχωρητή στο τέλος αυτού του βήματος θα είναι:

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\0\\-\frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\-\frac{1}{\sqrt{2}}\\0\end{bmatrix}=+\frac{1}{\sqrt{2}}|00\rangle+0|01\rangle-\frac{1}{\sqrt{2}}|10\rangle+0|11\rangle=+\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{\sqrt{2}}|10\rangle$$

Βήμα 5: Στο τελευταίο αυτό βήμα, δρα στο δεύτερο qubit η κβαντική πύλη Hadamard, ενώ στο πρώτο qubit δε δρα καμία πύλη, δηλαδή δρα η πύλη αδράνειας. Η συνολική τους δράση υπολογίζεται από το τανυστικό γινόμενο των πινάκων που τις περιγράφουν:

$$\begin{bmatrix}+\frac{1}{\sqrt{2}}&0&+\frac{1}{\sqrt{2}}&0\\0&+\frac{1}{\sqrt{2}}&0&+\frac{1}{\sqrt{2}}\\+\frac{1}{\sqrt{2}}&0&-\frac{1}{\sqrt{2}}&0\\0&+\frac{1}{\sqrt{2}}&0&-\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}+\frac{1}{\sqrt{2}}\\0\\-\frac{1}{\sqrt{2}}\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=|10\rangle$$

Πρότυπο Κυκλωματικό Μοντέλο

Το Πρότυπο Κυκλωματικό Μοντέλο είναι ένα μοντέλο που χρησιμοποιείται για την κατασκευή κβαντικών κυκλωμάτων. Σ' αυτό το μοντέλο είναι βασική η έννοια των καθολικών πυλών. Όπως είναι ήδη γνωστό, μία οποιαδήποτε κβαντική πύλη μπορεί να αναλυθεί χρησιμοποιώντας ένα σύνολο από βασικές πύλες, γνωστές ως καθολικές πύλες, η επιλογή των οποίων δεν είναι μοναδική. Πύλες του ενός qubit μπορούν να αναπαρασταθούν χρησιμοποιώντας μόνο πύλες Hadamard και πύλες μετατόπισης φάσης. Πύλες των δύο qubit μπορούν να αντικατασταθούν από πύλες Hadamard, CNOT και μετατόπισης φάσης και αυτό μπορεί να γενικευτεί στην περίπτωση των πυλών N-qubits, καθώς μπορεί να θεωρηθεί ότι οι πύλες των N-qubits μπορούν να αναλυθούν από $O(4^N)$ πύλες μετατόπισης φάσης, CNOT και Hadamard.

Ένα από τα μειονεκτήματα του μοντέλου είναι ότι δεν είναι βέλτιστο τόσο σε ό,τι αφορά τον αριθμό των υπολογιστικών βημάτων όσο και σε ό,τι αφορά το συνολικό χρόνο της υπολογιστικής διαδικασίας.

Επιπλέον, δείχνει προτίμηση σε φυσικά συστήματα στα οποία μπορούν να πραγματοποιηθούν οι καθολικές πύλες εύκολα. Σαν αποτέλεσμα αυτού, αποφεύγονται φυσικά συστήματα τα οποία διαθέτουν ικανοποιητικά χαρακτηριστικά για να λειτουργήσουν σαν υποψήφια για την υλοποίηση ενός κβαντικού υπολογιστή, επειδή δεν είναι εφικτό να υλοποιηθούν με ευκολία οι καθολικές πύλες. Επίσης, η ανάλυση σε καθολικές πύλες επηρεάζεται από το σύνολο των καθολικών πυλών που μπορεί να χρησιμοποιηθεί σε κάθε σύστημα. Διαφορετικό σύνολο οδηγεί σε διαφορετική ανάλυση.

Κβαντική Σύμπλεξη

Η κβαντική σύμπλεξη ή αλλιώς διεμπλοκή προέρχεται από ένα άρθρο των Albert Einstein, Boris Podolsky και Nathan Rosen που δημοσιεύτηκε το 1935, στόχος του οποίου ήταν να δειχθεί ότι η κβαντική μηχανική δεν αποτελεί μία ολοκληρωμένη φυσική θεωρία, αλλά από την κβαντική περιγραφή της φύσης λείπουν ορισμένες παράμετροι, οι αργότερα επονομαζόμενες ¨κρυμμένες μεταβλητές¨ (Bohm, 1952).

Σαν μοντέλο για την απόδειξή τους χρησιμοποιήθηκε ένα πείραμα στο οποίο δύο κβαντικά συστήματα αλληλεπιδρούσαν μεταξύ τους και μετά απομακρύνονταν το ένα από το άλλο. Όμως παρά την απομάκρυνση των κβαντικών συστημάτων, παρατηρήθηκε ότι τα συστήματα παρέμεναν διασυνδεδεμένα το ένα με το άλλο με άγνωστο τρόπο. Αυτό το φαινόμενο είχε ως συνεπακόλουθο με τη μέτρηση του ενός κβαντικού συστήματος πάνω σε μία φυσική ποσότητα, ακαριαία να καθορίζεται το αποτέλεσμα του άλλου κβαντικού συστήματος πάνω στην ίδια ποσότητα. Το πείραμα αυτό είναι ευρέως γνωστό ως EPR ή ¨παράδοξο¨ EPR και πήρε το όνομα του από τα αρχικά των επιθέτων των τριών ερευνητών που συνέταξαν το άρθρο.

Το 1935, σε άρθρο του ο Erwin Schrodinger, προκειμένου να περιγράψει την άγνωστη αυτή διασύνδεση μεταξύ δύο κβαντικών συστημάτων, χρησιμοποίησε το γερμανικό όρο ¨verschrankung¨ που σημαίνει ¨σταυρώνω τα χέρια¨. Ο όρος αποδόθηκε στα Αγγλικά ως entanglement και στα Ελληνικά μπορεί να αποδοθεί και ως εναγκαλισμός, περιπλοκή, σύζευξη ή διαπλοκή.

Το παράδοξο EPR προκάλεσε συζητήσεις και πολλές φορές διαμάχες μεταξύ των ερευνητών, λόγω μη κατανόησής του από την επιστημονική κοινότητα. Οι διαμάχες συνεχίστηκαν ώσπου ο John Bell, με ένα άρθρο που δημοσιεύτηκε το 1964, απέδειξε με τη χρήση ανισοτήτων, γνωστές ως ανισότητες Bell, ότι η κβαντική μηχανική είναι μία ολοκληρωμένη φυσική θεωρία. Αυτό το άρθρο αποδείχτηκε αργότερα και πειραματικά (πείραμα του Aspect).

Η κβαντική σύμπλεξη παρατηρείται σε πειράματα τόσο του μικρόκοσμου όσο και σε μεγαλύτερη κλίμακα. Για τους κβαντικούς υπολογιστές, συγκεκριμένα, αποτελεί φυσικό πόρο όπως είναι η ενέργεια. Δημιουργείται σε περισσότερα του ενός qubit και μάλιστα χρησιμοποιώντας μόνο δύο πύλες, την H και την CNOT. Χρησιμοποιείται για να εκτελεστούν κβαντικοί υπολογισμοί και να αναπτυχθούν κβαντικοί αλγόριθμοι (Niesen & Chuang, 2004) όπως είναι ο αλγόριθμος του Shor, ο οποίος αναφέρεται στη συνέχεια.

Ένα χρήσιμο παράδειγμα εφαρμογής του φαινομένου σχετίζεται με τις μετρήσεις κβαντικών συστημάτων. Όταν δύο qubit δεν είναι συμπλεγμένα λέγονται ανεξάρτητα. Στην περίπτωση αυτή, η κατάσταση ενός καταχωρητή που τα περιέχει μπορεί να δοθεί αν πολλαπλασιαστούν οι αντίστοιχοι συντελεστές των δύο qubit. Δύο κβαντικά φαινόμενα, όμως, που βρίσκονται σε κβαντική σύμπλεξη δεν μπορούν να δώσουν τανυστικό γινόμενο των δύο καταστάσεών τους, αλλά είναι ένας γραμμικός συνδυασμός τέτοιων γινομένων. Για παράδειγμα, έστω δύο qubits, το $|q_{e_0}\rangle$ και το $|q_{e_1}\rangle$, τα οποία βρίσκονται στην κατάσταση $|q_e\rangle$:

$$|q_e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Η $|q_e\rangle$ δεν μπορεί, όπως φαίνεται εύκολα, να γραφεί σαν τανυστικό γινόμενο των καταστάσεων των δύο qubits, οπότε τα $|q_{e_0}\rangle$ και $|q_{e_1}\rangle$ βρίσκονται σε κβαντική σύμπλεξη. Αυτό σημαίνει πως αν μετρηθεί η κατάσταση του qubit $|q_{e_1}\rangle$ της κατάστασης $|q_e\rangle$, θα βρεθεί με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση $|0\rangle$ και με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση $|1\rangle$. Αν βρεθεί στην κατάσταση $|0\rangle$, τότε, αν γίνει μέτρηση της κατάστασης του qubit $|q_{e_0}\rangle$, θα διαπιστωθεί σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|0\rangle$. Αν βρεθεί στην κατάσταση $|1\rangle$, τότε, αν μετρηθεί η κατάσταση του qubit $|q_{e_0}\rangle$, θα εντοπιστεί σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|1\rangle$. Δηλαδή, η μέτρηση της κατάστασης του ενός qubit καθορίζει την

κατάσταση του άλλου, γεγονός που είναι και η βασική διαφορά της σύμπλεξης με την υπέρθεση. Η απόλυτη αυτή συσχέτιση ισχύει πάντα, ανεξάρτητα από τον τρόπο με τον οποίο γίνεται η μέτρηση αλλά και από τη χωρική απόσταση των δύο qubits.

Ένας τρόπος κατανόησης αυτής της ¨στοιχειωμένης δράσης από απόσταση¨, κατά ακριβή μετάφραση της διατύπωσης του Einstein (spooky action at a distance), είναι η συνειδητοποίηση του γεγονότος ότι η σύμπλεκτη κατάσταση έχει προετοιμαστεί αρχικά τοπικά, αφήνοντας τα δύο υποσυστήματα να αλληλεπιδράσουν σε κάποιο σημείο του χώρου για ένα πεπερασμένο χρονικό διάστημα. Όταν στη συνέχεια τα δύο υποσυστήματα απομακρύνονται το ένα από το άλλο, η ολική κβαντική κατάσταση απλώνεται στο χώρο (καθιστάμενη μη εντοπισμένη). Έτσι, δεν υπάρχει κάποιο είδος πληροφορίας που θα μπορούσε ή θα έπρεπε να μεταδοθεί μεταξύ των δύο υποσυστημάτων. Η σύμπλεκτη κατάσταση ήδη συνιστά την πιο πλήρη περιγραφή των μεμονωμένων υποσυστημάτων και εμπεριέχει κάθε πιθανή πληροφορία αυτών.

Κβαντικοί Αλγόριθμοι

Οι αλγόριθμοι, συνήθως, αναπτύσσονται πριν την κατασκευή του μηχανήματος που θα τους διαχειριστεί και τρέξει. Χαρακτηριστικό παράδειγμα αποτελούν οι κλασικοί αλγόριθμοι των κλασικών υπολογιστών, οι οποίοι προηγήθηκαν του μηχανήματος κατά μία χιλιετία. Το ίδιο ακριβώς συμβαίνει και με τους κβαντικούς αλγορίθμους, οι οποίοι υπάρχουν εδώ και αρκετά χρόνια χωρίς την ύπαρξη των κβαντικών υπολογιστών. Η διαφορά και παράλληλα η δύναμη ενός κβαντικού αλγορίθμου βρίσκεται στο ενδιάμεσο αθέατο κομμάτι, τότε που δε γίνονται μετρήσεις και διαδραματίζονται τα κβαντικά φαινόμενα (υπέρθεση). Ένας κβαντικός αλγόριθμος χειρίζεται και κατευθύνει τα κβαντοδυφία με σκοπό την επίλυση προβλημάτων, το οποίο γενικά επιτυγχάνει με μεγαλύτερη απόδοση σε σύγκριση με τους κλασικούς υπολογιστές. Όλοι οι κβαντικοί αλγόριθμοι ακολουθούν χρονικά τα εξής τέσσερα βήματα:

i) Το σύστημα εκκινείται από μία συγκεκριμένη κλασική κατάσταση των κβαντοδυφίων (π.χ. συγκεκριμένη κατεύθυνση πόλωσης των φωτονίων).
ii) Δημιουργεί μια υπέρθεση των πιθανών καταστάσεών τους.

iii) Στις καταστάσεις αυτές δρουν σειριακά πολλοί μοναδιαίοι μετασχηματισμοί (τελεστές) με σκοπό να επιτευχθεί το τελικό αποτέλεσμα και

iv) στο τέλος, μετρώνται όλα τα κβαντοδυφία ενδιαφέροντος για να προκύψει, με βάση την κατανομή πιθανότητας, η έξοδος.

Κάποιοι αντιπροσωπευτικοί και γνωστοί κβαντικοί αλγόριθμοι που έχουν εμφανιστεί μέχρι και σήμερα είναι οι εξής:

Αλγόριθμος του Deutsch (1985)

Ο πρώτος κβαντικός αλγόριθμος, δηλαδή ένας αλγόριθμος που να μπορεί να τρέξει αποκλειστικά σε κβαντικό υπολογιστή. Χρησιμοποιεί το φαινόμενο της κβαντικής παραλληλίας, της υπέρθεσης, δηλαδή, των βασικών καταστάσεων των qubits. Αποτελεί έναν ντετερμινιστικό αλγόριθμο, το οποίο σημαίνει ότι για κάποια συγκεκριμένα δεδομένα εισόδου παράγονται πάντα οι ίδιες έξοδοι και μάλιστα οι σωστές. Για πρώτη φορά ένας κβαντικός υπολογιστής είναι δυνατό να πραγματοποιήσει υπολογισμούς που είναι ανέφικτο να εκτελεστούν από έναν κλασικό. Ο αλγόριθμος αυτός, δοσμένης μίας συνάρτησης $f:\{0,1\}\rightarrow 0,1\}$ με δυαδικό πεδίο ορισμού και συνόλου τιμών, υπό τη μορφή μαύρου κουτιού, καθορίζει για το αν είναι ισορροπημένη ή σταθερή, με λιγότερες πράξεις, τις μισές σχεδόν, σε σχέση με έναν κλασικό υπολογιστή.

Αναλυτικότερα, έστω η παραπάνω συνάρτηση f, όπου, όπως φαίνεται, η μεταβλητή x και η συνάρτηση f(x) μπορούν να πάρουν μόνο τις τιμές 0 ή 1. Συνεπώς, υπάρχουν δύο περιπτώσεις:

1) $f(0) = f(1)$, οπότε η συνάρτηση ονομάζεται σταθερή (constant),

2) $f(0) \neq f(1)$, οπότε η συνάρτηση ονομάζεται ισορροπημένη (balanced).

Ένας κλασικός υπολογιστής θα πρέπει να υπολογίσει την τιμή f(0), στη συνέχεια να υπολογίσει την f(1) και να συγκρίνει τα αποτελέσματα. Αν είναι ίδια, τότε η συνάρτηση είναι σταθερή, ενώ στην περίπτωση που είναι διαφορετικά, η συνάρτηση είναι ισορροπημένη. Δεν γίνεται, δηλαδή, να βρεθεί τι είναι η συνάρτηση με έναν μόνο υπολογισμό, κάτι που όμως γίνεται με τη χρήση κβαντικού υπολογιστή.

Αλγόριθμος των Deutsch και Josza (1992)

Αποτελεί μία γενίκευση του προηγούμενου αλγορίθμου, θέτοντας ακριβώς τον ίδιο στόχο, αλλά για μία συνάρτηση της μορφής f:$\{0,1\}^n \rightarrow \{0,1\}$, όπου, δηλαδή, το πεδίο ορισμού αποτελείται από όλες τις δυνατές n-άδες των 0 και 1.

Αλγόριθμος περιοδικότητας του Simon (1994)

Ο αλγόριθμος του Simon έχει σκοπό να βρίσκει πρότυπα μέσα σε συναρτήσεις. Αυτός ο αλγόριθμος είναι ένας συνδυασμός κβαντικών και κλασικών διεργασιών.

Έστω ότι δίνεται η συνάρτηση f:$\{0,1\}^n \rightarrow \{0,1\}^n$ που είναι black box. Είναι βέβαιο ότι υπάρχει ένα μυστικό-κρυφό δυαδικό κλειδί, μία δυαδική αλυσίδα μήκους n, c = $c_0 c_1 c_2 c_3 \ldots c_{n-1}$, τέτοιο ώστε για όλες τις συμβολοσειρές x,y $\in \{0,1\}^n$ ισχύει: f(x) = f(y) αν και μόνο αν x = y$\otimes$c, όπου $\otimes$ είναι αποκλειστική λειτουργία. Με άλλα λόγια, οι τιμές της f επαναλαμβάνονται με ένα πρότυπο και αυτό το πρότυπο το δίνει η c, η περίοδος της f. Ο στόχος του αλγορίθμου του Simon είναι να προσδιορίσει αυτό το c.

Για μία δοσμένη περιοδική f, είναι δυνατό να βρεθεί η περίοδος c με n υπολογισμούς, σε αντίθεση με τον κλασικό αλγόριθμο που χρειάζεται $2^{n-1} + 1$.

Αλγόριθμος αναζήτησης του Grover (1997)

Ο συγκεκριμένος αλγόριθμος έγινε γνωστός μέσα από ένα άρθρο του Lov Grover με τίτλο ¨Η κβαντική μηχανική μπορεί να μας βοηθήσει να βρούμε μια βελόνα στ' άχυρα¨. Ερευνά μία μη δομημένη βάση δεδομένων με N στοιχεία, τα οποία έχουν αριθμηθεί από 0 έως N-1. Το συγκεκριμένο σύστημα μπορεί να αναγνωρίσει αν κάποιο στοιχείο είναι αυτό που ζητείται ή όχι. Είναι, ουσιαστικά, ισοδύναμο με το να αναζητείται σε έναν πίνακα μεγέθους 2^n ένα στοιχείο το οποίο υπάρχει ακριβώς μία φορά. Σε έναν κλασικό υπολογιστή αυτό επιτυγχάνεται με έναν καταχωρητή, όπου έχει αποθηκευτεί ο αριθμός που αναζητείται και ένα κύκλωμα λογικών πυλών που συγκρίνει κάθε αριθμό στην είσοδό του με τον αποθηκευμένο αριθμό. Το σύστημα αυτό ονομάζεται oracle που στα ελληνικά σημαίνει ¨μάντης¨ ή ¨κάποιος που ξέρει πολλά¨.

Πρόκειται για ένα κβαντικό κύκλωμα που θεωρείται ¨μαύρο κουτί¨ όσον αφορά τη σύνθεσή του. Δεν είναι δυνατό κάποιος να έχει απευθείας πρόσβαση σε όλα τα ζευγάρια $(x, f(x))$, αλλά γίνεται να υπολογίσει την f για συγκεκριμένο x με κάποιο υπολογιστικό κόστος.

Η υλοποίησή του σε έναν κλασικό υπολογιστή είναι:

$$f(x) = \begin{cases} 1, \text{αν x} = \text{xi} \\ 0, \text{αν x} \neq \text{xi} \end{cases}$$

Κανονικά μία βάση δεδομένων με N στοιχεία θα έπαιρνε χρόνο της τάξης $O(N)$ ή της τάξης $O(N/2)$ στη μέση περίπτωση των $N/2$ αναζητήσεων. Ο χρόνος αυτός δεν μπορεί να βελτιωθεί σε κλασικούς υπολογιστές οποιασδήποτε τεχνολογίας και αρχιτεκτονικής, αλλά σε έναν κβαντικό υπολογιστή ο χρόνος αναζητήσεων είναι της τάξεως $O(\sqrt{N})$, ενώ ο αποθηκευτικός χώρος που χρειάζεται $O(\log N)$. Επιπλέον, έχει αποδειχθεί ότι ο αλγόριθμος του Grover είναι βέλτιστος, πραγματοποιεί δηλαδή τον ελάχιστο αριθμό επαναλήψεων και δεν είναι εφικτό να υπάρξει αντίστοιχος με μικρότερη πολυπλοκότητα, ενώ είναι ανθεκτικός και στον κβαντικό θόρυβο.

Ακόμα, ο αλγόριθμος Grover μπορεί να χρησιμοποιηθεί και για την εύρεση k αντικειμένων από τα N και αυτό επιτυγχάνεται με $\frac{\pi}{4}\left(\sqrt{\frac{N}{k}}\right)$ δοκιμές.

Αξίζει να αναφερθεί ότι το πρόβλημα της αναζήτησης στοιχείου σε μία μη δομημένη βάση δεδομένων έχει ως ισοδύναμη μαθηματική διατύπωση τον προσδιορισμό των τιμών της αντίστροφης κάποιας συνάρτησης. Αν, για παράδειγμα, είναι δυνατόν να βρεθούν, μέσω ενός κβαντικού υπολογιστή, οι τιμές μιας συνάρτησης f με πεδίο ορισμού κάποιο σύνολο με N το πλήθος στοιχεία, τότε το να βρεθεί η αντίστροφη εικόνα κάποιου στοιχείου είναι στην ουσία ένα πρόβλημα αναζήτησης μέσα στη βάση δεδομένων που ορίζεται από το πεδίο ορισμού της f. Αν η f είναι 1-1, τότε γίνεται αναζήτηση για ένα μόνο στοιχείο, διαφορετικά για περισσότερα.

Μία άλλη εφαρμογή του αλγορίθμου είναι στον τομέα της κρυπτογραφίας. Έστω μία εικονική βάση δεδομένων που είναι τόσο μεγάλη που δε θα ταίριαζε στις μνήμες των κλασικών υπολογιστών. Αυτό επιτρέπει στους κβαντικούς υπολογιστές να χρησιμοποιήσουν ένα ευρέως γνωστό σύστημα για την προστασία των δεδομένων. Αυτό είναι το σύστημα DES (Data Encryption Standard). Το σύστημα αυτό βασίζεται σε έναν αριθμό 56 bits. Μία εξαντλητική αναζήτηση με τα παραδοσιακά μέσα θα απαιτούσε 2^{55} αναζητήσεις πριν βρεθεί το σωστό κλειδί, σε αντίθεση με τον αλγόριθμο του Grover, ο οποίος θα μπορούσε να βρει το κλειδί μόνο μετά από 185 αναζητήσεις.

Τέλος, δεδομένου του ότι πολλά προβλήματα μπορούν να γραφούν και ως προβλήματα αναζήτησης, ο αλγόριθμος του Grover μπορεί να έχει πολύ περισσότερες εφαρμογές από όσες έχουν ανακαλυφθεί μέχρι σήμερα. Ο Nielsen και Chuang, για παράδειγμα,

υποστηρίζουν ότι ο συγκεκριμένος αλγόριθμος μπορεί να βοηθήσει στο να λυθούν πιο γρήγορα ορισμένα NP-complete προβλήματα.

Η βασική ιδέα πίσω από τη λειτουργία αυτού του αλγόριθμου είναι το γεγονός ότι αν και υπάρχει μεγάλη δυσκολία όσον αφορά την εύρεση της σωστής λύσης σε ένα πρόβλημα αναζήτησης, παρόλα αυτά η αναγνώριση της σωστής λύσης καθίσταται σχετικά εύκολη.

Αντίθετα με τον αλγόριθμο του Deutsch, ο αλγόριθμος του Grover είναι ένας πιθανοτικός αλγόριθμος. Αυτό σημαίνει ότι δε δίνει σίγουρα τη σωστή απάντηση, αλλά με μεγάλη πιθανότητα να είναι αυτή. Για να αυξήσει κάποιος την πιθανότητα η λύση του αλγορίθμου που θα δοθεί να είναι η σωστή, θα πρέπει να επαναλάβει πολλές φορές τον αλγόριθμο και να συγκρίνει τα αποτελέσματα.

Παρόλα αυτά, όπως προαναφέρθηκε, αποτελεί τον ασυμπτωτικά γρηγορότερο κβαντικό αλγόριθμο αναζήτησης σε μη ταξινομημένη λίστα σε σχέση με άλλους αλγορίθμους που εφαρμόζονται σε γραμμικά κβαντικά μοντέλα. Ενώ άλλοι παρόμοιοι κβαντικοί αλγόριθμοι για το σκοπό αυτό παρουσιάζουν εκθετική επιτάχυνση σε σχέση με τους αντίστοιχους κλασικούς, ο συγκεκριμένος παρουσιάζει τετραγωνική επιτάχυνση της διαδικασίας. Αν και η προηγούμενη βελτίωση της ταχύτητας μπορεί να φαίνεται μικρή, για μεγάλο αριθμό στοιχείων γίνεται τεράστια.

Αλγόριθμος παραγοντοποίησης του Shor (1994)

Αποτελεί έναν κβαντικό αλγόριθμο παραγοντοποίησης ενός ακέραιου αριθμού N που πραγματοποιείται σε χρόνο O((log N)3) και διάστημα O(log N).

Το πρόβλημα της παραγοντοποιήσης ακέραιων αριθμών είναι πάρα πολύ σημαντικό. Οι περισσότεροι αλγόριθμοι για την ασφάλεια του παγκόσμιου διαδικτύου και την κρυπτογράφηση, όπως ο κατά πολύ διαδεδομένος RSA, βασίζονται στη δυσκολία που παρουσιάζει η παραγοντοποίηση μεγάλων πρώτων αριθμών σε κλασικούς υπολογιστές. Η συνεχής έρευνα, όμως, στους κβαντικούς υπολογιστές έχει αποδείξει ότι καθίσταται εφικτό να παραγοντοποιήσει κανείς μεγάλους πρώτους αριθμούς σε πολυωνυμικό χρόνο με τη χρήση κβαντικών πιθανοτικών αλγορίθμων. Ένας τέτοιος αλγόριθμος είναι και αυτός του Shor.

Αναλυτικότερα, ο Peter Shor έδειξε πως κάνοντας χρήση κβαντικών υπολογιστών, μπορεί κανείς εύκολα και γρήγορα να αναλύσει σε γινόμενο δύο πρώτων αριθμών

μεγάλους ακέραιους αριθμούς και μάλιστα με πολυωνυμική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους n, δηλαδή του αριθμού των ψηφίων του αριθμού προς παραγοντοποίηση. Αντίθετα, στους κλασικούς υπολογιστές παρατηρείται εκθετική αύξηση του χρόνου υπολογισμού της παραγοντοποίησης για γραμμική αύξηση του μεγέθους n. Οι γρηγορότεροι, μάλιστα, κλασικοί αλγόριθμοι για το ίδιο πρόβλημα είναι υπερ-πολυωνυμικοί σε συνάρτηση με τον αριθμό ψηφίων n.

Συγκεκριμένα, ο αλγόριθμος του Shor έχει πολυπλοκότητα O(n^2lognloglogn) σε αντιδιαστολή με τον καλύτερο κλασικό αλγόριθμο που έχει πολυπλοκότητα O($e^{cn^{\frac{1}{3}}log^{\frac{2}{3}}n}$). Χρειάζεται O(exp[(lgN)$^{\frac{1}{3}}$ (lglgN)$^{\frac{2}{3}}$]) βήματα για έναν ακέραιο N, ενώ ο πιο γρήγορος κλασικός αλγόριθμος παραγοντοποίησης χρειάζεται 10^{10} χρόνια για έναν αριθμό με 400 ψηφία.

Αποτελείται από δύο μέρη. Το πρώτο μέρος μπορεί να εκτελεστεί και από έναν απλό κλασικό υπολογιστή, ενώ το δεύτερο μόνο από κβαντικό υπολογιστή με τη βοήθεια του κβαντικού μετασχηματισμού Fourier.

Το 2001, η IBM έκανε μια επίδειξη όπου παραγοντοποίησε τον αριθμό 15 στο γινόμενο 3 επί 5 με την χρήση 7 qubits. Επιπλέον, με κάποιες τροποποιήσεις του αλγορίθμου Shor, έχει δειχθεί ότι το κβαντικό μέρος του μπορεί να τερματίσει σε τέσσερις με οκτώ επαναλήψεις μόνο. Οπωσδήποτε, τέτοια αποτελέσματα είναι ενδείξεις του ότι θα πρέπει σύντομα να επινοηθούν νέες μέθοδοι κρυπτογράφησης, οι οποίες να είναι απρόσβλητες σε τέτοιους υπολογιστές.

Αλγόριθμος OTP (1917)

Η μέθοδος αυτή συνίσταται στην modulus πρόσθεση ενός τυχαίου, ισομήκους με το μήνυμα προς αποστολή, κλειδιού και του ίδιου του μηνύματος. Στην περίπτωση μιας γλώσσας με μοναδικά ψηφία το 0 και το 1, αυτό ισοδυναμεί με την πράξη XOR. Αν και πολύ απλή σαν μέθοδος, χρειάστηκαν 25 χρόνια από την εφεύρεσή της για να αναγνωριστεί η ιδιαίτερη αξία της λόγω των αυστηρών περιορισμών στην υλοποίησή της.

Ο Claude Shannon είχε αποδείξει ότι αν η μέθοδος αυτή εφαρμοσθεί με ένα πραγματικά τυχαίο και όχι ψευδοτυχαίο κλειδί που θα κρατηθεί απόλυτα μυστικό και δε θα χρησιμοποιηθεί παραπάνω από μία φορά, τότε επιτυγχάνεται η πλήρης εχεμύθεια. Ακόμα, απέδειξε ότι αν οποιαδήποτε άλλη μέθοδος στοχεύει την πλήρη

εχεμύθεια, τότε θα πρέπει να πληροί τις παραπάνω προϋποθέσεις, δηλαδή ότι ο αλγόριθμος OTP είναι ¨πλήρης¨ όσον αφορά την εχεμύθεια. Το να μην γίνει χρήση του ίδιου κλειδιού πάνω από μία φορά είναι σημαντικό για την επιτυχία της μεθόδου. Ακόμα και αν χρησιμοποιηθεί μόνο δύο φορές το ίδιο κλειδί, τότε είναι εύκολο να ανακτηθεί με τη χρήση κρυπταναλυτικών μεθόδων.

Αυτή η απαίτηση χρήσης ενός πραγματικά τυχαίου κλειδιού ταιριάζει όμορφα με τις ίδιες της αρχές της κβαντομηχανικής. Η τυχαιότητα κάποιων δεδομένων, ως γνωστόν, μετριέται με βάση την εντροπία και μπορεί να αξιοποιηθεί για την επίτευξη της ασφάλειας Shannon. Η μέθοδος που έχει προταθεί από τον Von Neumann, η επονομαζόμενη ¨λεύκανση Von Neumann¨, έχει ως εξής:

Είσοδος	Έξοδος
00	Τίποτα
01	1
10	0
11	Τίποτα

Η διαδικασία αυτή παράγει μια τυχαία ακολουθία από bit, το καθένα με εντροπία ίση με τη μονάδα, εφόσον η ακολουθία εισόδου είναι πραγματικά τυχαία. Είναι προφανές, λοιπόν, ότι αν και οι κβαντικοί υπολογιστές απειλούν με κατάρρευση τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης, αυτοί οι ίδιοι είναι που προσφέρουν τη λύση για μια πιο ασφαλή κρυπτογραφία.

Σφάλματα και Προτεινόμενες Λύσεις

Παρόλο που έχει πραγματοποιηθεί εξαιρετική πρόοδος από τη στιγμή της σύλληψης της ιδέας του κβαντικού υπολογιστή έως σήμερα, παρουσιάζονται αρκετά προβλήματα όσον αφορά την υλοποίησή του. Το κυριότερο εξ αυτών είναι η ύπαρξη σφαλμάτων και η αντιμετώπισή τους. Το πρόβλημα που προκύπτει στη διόρθωση σφάλματος αναφέρεται στο ποια λάθη χρειάζονται διόρθωση. Η απάντηση σε αυτό το ερώτημα είναι πρώτα τα λάθη εκείνα που προκύπτουν ως άμεσο αποτέλεσμα αποσυσχετισμού ή από την τάση ενός κβαντικού υπολογιστή να αποσυντεθεί από μία δεδομένη κβαντική κατάσταση σε μία ασυνάρτητη κατά την αλληλεπίδρασή του με το περιβάλλον. Οι

αλληλεπιδράσεις αυτές που πραγματοποιούνται μεταξύ του περιβάλλοντος και των qubits είναι αδύνατο να αποφευχθούν, προκαλώντας έτσι τη διακοπή των πληροφοριών που αποθηκεύονται στον κβαντικό υπολογιστή και συνεπώς λάθη στον υπολογισμό.

Επομένως, η ύπαρξη μηχανισμών για τη διόρθωση των λαθών είναι απαραίτητη. Υπάρχουν δύο είδη λαθών που μπορεί να εισάγει το περιβάλλον στο σύστημα και αυτά είναι η Δυαδική αντιστροφή και ο Αποσυσχετισμός.

Όσον αφορά τη Δυαδική Αντιστροφή, ας υποτεθεί, αρχικά, ότι το σύστημά αποτελείται από ένα qubit. Το σφάλμα της δυαδικής αντιστροφής μετατρέπει την αρχική κατάσταση από π.χ. $\alpha |0\rangle + b |1\rangle$ σε $\alpha |1\rangle + b |0\rangle$. Αυτό το λάθος χρησιμοποιώντας κλασικούς κώδικες διόρθωσης μπορεί να αποφευχθεί. Η δυαδική αντιστροφή, ουσιαστικά, είναι μία αντιστρεπτή πράξη πάνω στα qubits και για αυτό το λόγο μπορεί εύκολα να διορθωθεί.

Στην περίπτωση του αποσυσχετισμού, ανεπιθύμητες αλληλεπιδράσεις μεταξύ κβαντικών καταχωρητών και περιβάλλοντος προκαλούν την κατάρρευση της κατάστασης του συστήματος. Αυτό ισοδυναμεί με ¨μέτρηση¨ του καταχωρητή, η οποία αποτελεί μία μη αντιστρεπτή διεργασία. Η επίλυση αυτού του προβλήματος καθίσταται εξαιρετικά δύσκολη και η επαναφορά του συστήματος μετά από τέτοια λάθη είναι σχεδόν αδύνατη.

Στους κλασικούς υπολογιστές για τον περιορισμό των σφαλμάτων, κωδικοποιείται κάθε bit ως μια τριπλέτα από όμοια bits. Αν κάποιος θόρυβος αντιστρέψει ένα bit, είναι εφικτό να αποκατασταθεί το σφάλμα διορθώνοντας το μεμονωμένο bit της τριπλέτας. Όσον αφορά τους κβαντικούς υπολογιστές, η κβαντομηχανική απαγορεύει να γίνει γνωστή με βεβαιότητα η άγνωστη κατάσταση ενός κβαντικού αντικειμένου. Ο κώδικας της κλασικής τριπλέτας, συνεπώς, αποτυγχάνει, διότι δεν είναι εφικτό να εξεταστεί κάθε αντίγραφο ενός qubit χωρίς να καταστραφούν όλα τα αντίγραφα. Ακόμη, το να φτιαχτούν αντίγραφα στην αρχική κατάσταση δεν είναι κάτι απλό. Η κβαντομηχανική δεν επιτρέπει από ένα άγνωστο qubit να δημιουργηθεί με αξιοπιστία ένα αντίγραφό του. Το αποτέλεσμα αυτό είναι κοινώς γνωστό ως θεώρημα αδυναμίας κλωνοποίησης.

Όμως, στις αρχές 1990, ερευνητές της IBM απέδειξαν πως είναι δυνατό να γίνει κβαντική διόρθωση σφαλμάτων χωρίς να γίνουν ποτέ γνωστές οι καταστάσεις των qubits. Όπως και με τον κώδικα της τριπλέτας, κάθε τιμή αναπαρίσταται με ένα σύνολο από qubits. Τα qubits αυτά περνάνε μέσα από ένα κύκλωμα, το οποίο εντοπίζει με

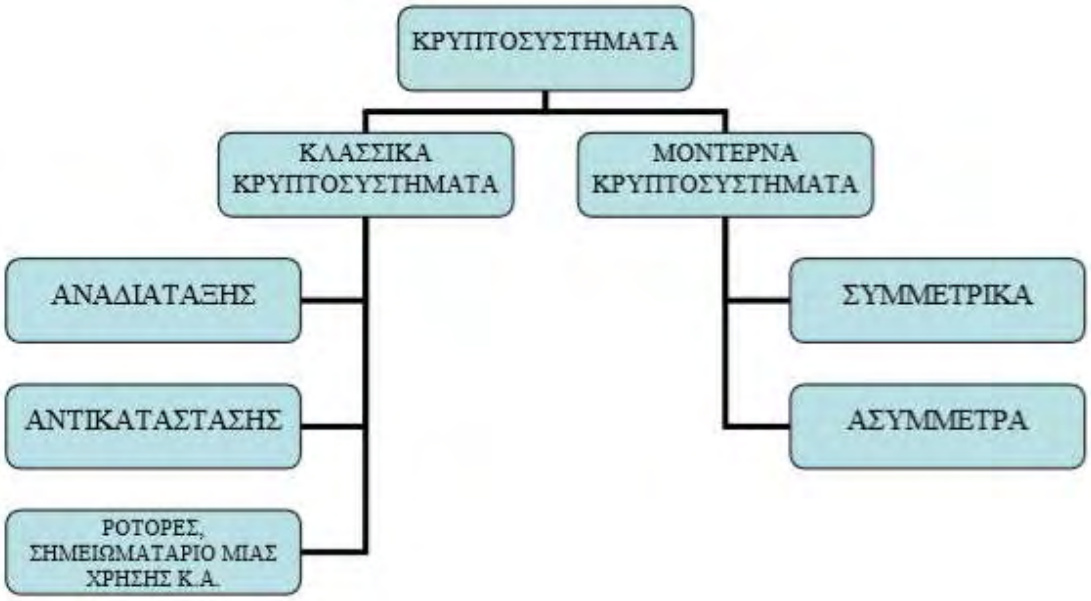
επιτυχία ένα σφάλμα σε αυτά χωρίς να διαβάσει πραγματικά ποιες είναι οι ξεχωριστές τους καταστάσεις. Η προστασία των κβαντικών καταστάσεων από το θόρυβο, συνεπώς, επιτεύχθηκε χρησιμοποιώντας ένα συνδυασμό ιδεών από την επιστήμη της πληροφορίας και από τη βασική κβαντομηχανική. Η κβαντική διόρθωση σφαλμάτων έχει προκαλέσει, επίσης, τη δημιουργία πολλων νέων ιδεών. Για παράδειγμα, μερικά φυσικά συστήματα μπορεί να έχουν ένα τύπο φυσικής ανοχής στο θόρυβο. Αυτά τα συστήματα θα χρησιμοποιούν κβαντική διόρθωση σφαλμάτων χωρίς την επέμβαση του ανθρώπινου παράγοντα και θα έχουν τη δυνατότητα να επιδείξουν εξαιρετική αντίσταση στην καταστροφή της υπέρθεσης των καταστάσεων.

ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ

Γενικά

Κρυπτοσύστημα, αρχικά, ονομάζεται το σύνολο των διαδικασιών και των πρωτοκόλλων που αναλαμβάνουν την εγκατάσταση ενός συστήματος ασφαλούς επικοινωνίας μεταξύ δύο ή περισσότερων χρηστών. Τα κρυπτοσυστήματα χωρίζονται σε δύο μεγάλες κατηγορίες, τα Κλασικά (Αναδιάταξης, Αντικατάστασης) και τα Μοντέρνα (Συμμετρικά, Ασύμμετρα).

Μια άλλη κατηγοριοποίηση των κρυπτογραφικών αλγορίθμων (κρυπτοσυστημάτων) με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων είναι αυτή κατά Δέσμη (Block Ciphers) και σε Ροή (Stream Ciphers).



Εικόνα 13: Κατηγοριοποίηση κρυπτοσυστημάτων

Πηγή: https://hellanicus.lib.aegean.gr/bitstream/handle/11610/12627/file0.pdf

Κλασικά Κρυπτοσυστήματα

Στα κλασικά κρυπτοσυστήματα διακρίνονται δύο βασικές τεχνικές κρυπτογράφησης, αυτή με αντικατάσταση και αυτή με αντιμετάθεση χαρακτήρων. Και στις δύο περιπτώσεις διακρίνονται δύο κατηγορίες που σχετίζονται με τον τρόπο αντικατάστασης (substitution) ή αντιμετάθεσης (permutation). Στην πρώτη κατηγορία, στο μονοαλφαβητικό τρόπο, συμβαίνει αντικατάσταση ή αντιμετάθεση από ένα μόνο χαρακτήρα (κάθε μονάδα του αρχικού κειμένου αναπαρίσταται πάντοτε από το ίδιο

σύμβολο-αντικαταστάτη), ενώ στον πολυαλφαβητικό τρόπο, που αποτελεί τη δεύτερη κατηγορία, από περισσότερους και κάθε φορά χρησιμοποιείται διαφορετικός (π.χ μηχανή Αίνιγμα). Συχνά, όμως, συναντώνται και συνδυασμοί των δύο παραπάνω αλλά και περαιτέρω κατηγορίες. Βασική προϋπόθεση αποτελεί το να μην προκύψει απώλεια οποιασδήποτε πληροφορίας, έτσι ώστε όλες οι διαδικασίες να μπορούν να αντιστραφούν. Τα περισσότερα συστήματα αποτελούνται από μεγάλο πλήθος σταδίων αντικαταστάσεων και μεταθέσεων.

Κρυπτοσυστήματα Αντικατάστασης

Ένας αλγόριθμος αντικατάστασης είναι μια τεχνική κρυπτογράφησης στην οποία μονάδες απλού κειμένου αντικαθίστανται από μονάδες κρυπτογραφημένου κειμένου βάση κάποιων κανόνων συστήματος. Οι μονάδες μπορεί να είναι σκέτοι χαρακτήρες ή σύμβολα ή δυαδικά ψηφία ή ομάδες αυτών ή κάποια μίξη τους ή και άλλες περιπτώσεις. Μία από τις προτεινόμενες τεχνικές είναι να ζευγαρώνονται τυχαία τα γράμματα της αλφαβήτου και στη συνέχεια να αντικαθίσταται κάθε γράμμα του αρχικού μηνύματος με το ταίρι του (Βασίλειος Ζορκάδης, 2002).

Μια διαφορετική κατηγοριοποίηση αυτών των κρυπτοσυστημάτων θα ήταν σε συστήματα αντικατάστασης χωρίς συμφραζόμενα (context-free) και σε συστήματα αντικατάστασης με συμφραζόμενα (context-sensitive). Στην πρώτη κατηγορία κάθε γράμμα κωδικοποιείται ξεχωριστά, ενώ στη δεύτερη η κωδικοποίηση πραγματοποιείται ανά ομάδες (blocks).

Υπάρχει μια πληθώρα τύπων αλγορίθμων αντικατάστασης, καθώς είναι από τους πλέον διαδεδομένους και ευρέως χρησιμοποιημένους επί σειρά αιώνων. Αν ο αλγόριθμος ασχολείται με απλούς χαρακτήρες, τότε ονομάζεται απλός αλγόριθμος αντικατάστασης. Αν διαχειρίζεται μεγαλύτερες ομάδες χαρακτήρων, ονομάζεται πολυγραφικός. Ο πιο γνωστός όμως είναι η απλή κρυπτογραφική αντικατάσταση. Ο παραλήπτης σε αυτά τα συστήματα αποκωδικοποιεί με την αντίστροφη διαδικασία.

Ο χώρος κλειδιών ενός κρυπτοσυστήματος αντικατάστασης περιέχει n! στοιχεία. Επομένως, η μέθοδος δοκιμής όλων των πιθανών κλειδιών για την αποκρυπτογράφηση ενός κρυπτογραφημένου κειμένου είναι πρακτικώς ανέφικτη. Παρ'όλα αυτά, τα κρυπτοσυστήματα αντικατάστασης μπορεί να παραβιαστούν χρησιμοποιώντας τις στατιστικές ιδιότητες της γλώσσας και κυρίως την πιθανότητα εμφάνισης των γραμμάτων της αλφαβήτου της.

Σ’αυτή την κατηγορία αλγορίθμων ανήκουν και αλγόριθμοι-συναρτήσεις κατακερματισμού. Τέτοιοι αλγόριθμοι έρχονται για να λύσουν το πρόβλημα της ακεραιότητας ενός μηνύματος, καθώς τόσο η αλλοίωση εξαιτίας της μεταφοράς μέσα από κανάλια επικοινωνίας, όσο και κακόβουλοι χρήστες, συχνά επηρεάζουν σε μικρό ή μεγάλο βαθμό ένα μήνυμα. Αυτό που κάνουν είναι να αντιστοιχίζουν το μήνυμα σε μια συμβολοσειρά προεπιλεγμένου μεγέθους (message digests). Ο τελικός χρήστης που παραλαμβάνει ένα μήνυμα μπορεί να το δώσει σαν όρισμα στην ίδια συνάρτηση και αν οι συμβολοσειρές ταυτίζονται, τότε γνωρίζει ότι δεν υπήρξε αλλοίωση.

Προκειμένου μια συνάρτηση κατακερματισμού να χρησιμοποιηθεί στην κρυπτογραφία θα πρέπει να πληροί ορισμένες προϋποθέσεις :

•Το κείμενο εισόδου να μπορεί να έχει οποιοδήποτε μήκος.

•Η συνάρτηση να μπορεί να υπολογιστεί γρήγορα (σε πολυωνυμικό χρόνο) συναρτήσει του μήκους της εισόδου.

•Η συμβολοσειρά εξόδου πρέπει να έχει σταθερό μήκος (ελάχιστο 128 bits και συνηθισμένο 160 bits).

•Να μην μπορεί να βρεθεί $x \neq y$ με $H(x) = H(y)$ σε πολυωνυμικό χρόνο.

•Να είναι αδύνατο δεδομένης της τιμής H(x) να μπορεί να ανακτηθεί το x.

Μερικοί χαρακτηριστικοί αλγόριθμοι αυτής της κατηγορίας είναι η οικογένεια των MD(Message Direct), όπως οι MD2, MD4, MD5, η οικογένεια των SHA, όπως οι SHA-1, SHA-2 και SHA-3, Snefru, και RIPEMD.

Κρυπτοσυστήματα Αναδιάταξης

Στα Κρυπτοσυστήματα Μετάθεσης/Αναδιάταξης τα σύμβολα του αρχικού κειμένου μεταθέτονται/αναδιατάσσονται συνήθως κατά ομάδες.

Αρχικά, τοποθετείται το καθαρό κείμενο σε έναν πίνακα. Από κάθε γραμμή λαμβάνονται τα γράμματα που αποτελούν το κρυπτογραφημένο κείμενο με διαφορετική σειρά από αυτή που γράφονται στο καθαρό κείμενο. Με τον τρόπο αυτό, αναδιατάσσονται τα γράμματα του καθαρού κειμένου για την παραγωγή του κρυπτογραφήματος. Το κλειδί, σε αυτήν την περίπτωση, είναι η σειρά με την οποία λήφθηκαν τα κρυπτογραφημένα σύμβολα και ο αριθμός των στηλών του πίνακα. Ένας τρόπος με τον οποίο μπορεί να καθοριστεί το κλειδί είναι χρησιμοποιώντας κώδικες

λέξεις ή φράσεις των οποίων τα γράμματα καθορίζουν τη σειρά ανάλογα με τη θέση τους στην αλφάβητο.

Τα κρυπτοσυστήματα μετατόπισης δεν είναι ασφαλή κρυπτοσυστήματα. Υπάρχουν μόλις n δυνατότητες για το κλειδί και σε πολλές περιπτώσεις το n δεν είναι μεγάλος αριθμός, με αποτέλεσμα το κλειδί και κατά συνέπεια το καθαρό κείμενο να μπορούν να βρεθούν εύκολα δοκιμάζοντας όλες τις περιπτώσεις. Συνεπώς, αυτή η μέθοδος κρυπτογράφησης καθίσταται υπερβολικά απλή και θα πρέπει να συνδιάζεται με κάποια άλλη ιδέα.

Αν συγκρίνει κανείς, επομένως, τις δύο μεθόδους, οδηγείται στο συμπέρασμα ότι σε έναν κώδικα αναδιάταξης ή αλληλομετάθεσης οι μονάδες απλού κειμένου αναδιατάσσονται κατά ένα διαφορετικό και συνήθως αρκετά περίπλοκο τρόπο, χωρίς να αλλοιώνονται. Αντιθέτως, στους αλγορίθμους αντικατάστασης οι μονάδες απλού κειμένου παραμένουν στην ίδια θέση στο κρυπτογράφημα, μεταβάλλονται, όμως, μεταξύ τους.

Μοντέρνα Κρυπτοσυστήματα

Στη σύγχρονη κρυπτογραφία, η λογική στα υπολογιστικά συστήματα είναι να συνδυαστεί το αρχικό κείμενο (plaintext) με κάποια επιπλέον πληροφορία που ονομάζεται ¨κλειδί¨, ώστε να προκύψει ένα κρυπτογράφημα (ciphertext). Αυτό υλοποιείται με έναν αλγόριθμο, ο οποίος θα πρέπει να είναι τόσο περίπλοκος και δυσνόητος, έτσι ώστε και στη περίπτωση που ο κρυπταναλυτής αντλήσει κομμάτι ενός κρυπτογραφημένου κειμένου, να μην είναι δυνατή η αποκωδικοποίησή του χωρίς να γνωρίζει το κλειδί. Ο αλγόριθμος, επομένως, μπορεί να είναι φανερός προς όλους σε αντίθεση με το κλειδί όπου φυλάσσεται μυστικό και οι μοναδικές οντότητες που θα πρέπει να το γνωρίζουν και να το χρησιμοποιούν είναι ο αποστολέας και ο παραλήπτης. Συνεπώς, αδύναμος κρίκος όσον αφορά την ασφάλεια των συγκεκριμένων κρυπτοσυστημάτων είναι μόνο η μυστικότητα του κλειδιού και όχι η μυστικότητα του αλγορίθμου που χρησιμοποιείται.

Η πιο πάνω διαδικασία ακολουθείται και στα δύο κρυπτοσυστήματα στα οποία διακρίνεται η συγκεκριμένη κατηγορία, με ορισμένες, όμως, παραλλαγές ως προς τον τρόπο παραγωγής και χρήσης των κλειδιών.

Συμμετρικά (ή διπλής κατεύθυνσης) Κρυπτοσυστήματα

Γενικά, ένα κρυπτοσύστημα καλείται συμμετρικό, αν γίνεται χρήση ενός μοναδικού μυστικού κλειδιού, το οποίο χρησιμοποιείται για την κρυπτογράφηση αλλά και για την αποκρυπτογράφηση ή γενικότερα αν το κλειδί αποκρυπτογράφησης μπορεί πολύ εύκολα να υπολογιστεί από το κλειδί κρυπτογράφησης. Για το λόγο αυτό, ονομάζονται και κρυπτοσυστήματα ιδιωτικού κλειδιού (private key cryptography) ή ενός κλειδιού (one-key cryptography) ή αλλιώς συμβατικά (conventional) κρυπτοσυστήματα. Τα συστήματα αυτά βασίζονται, όπως έχει ήδη αναφερθεί, στη μυστικότητα του κλειδιού και μπορούν να θεωρηθούν ικανοποιητικά ως προς την ασφάλεια.

Για n χρήστες χρειάζονται $n(n-1)/2$ κλειδιά (π.χ. για 2 μέλη χρειάζεται 1, αλλά για 11 μέλη χρειάζονται 55 κλειδιά). Αυτό σημαίνει ότι το πλήθος των αναγκαίων κλειδιών που πρέπει να κατέχει κάθε οντότητα αυξάνεται γεωμετρικά όσο αυξάνεται το πλήθος των υπόλοιπων οντοτήτων.

Το πρόβλημα με τα συγκεκριμένα κρυπτοσυστήματα είναι ότι, για κάθε μήνυμα που κρυπτογραφείται, το κλειδί θα πρέπει να συμβαδίζει με το μέγεθος του μηνύματος. Επιπλέον, θα πρέπει να έχει αποφασιστεί μεταξύ του πομπού και του δέκτη πριν αρχίσει η επικοινωνία τους διαμέσου του μη ασφαλούς καναλιού. Φυσικά, για αυτήν την προκαταρκτική επικοινωνία δεν μπορούν να χρησιμοποιήσουν το μη ασφαλές κανάλι που πρόκειται να χρησιμοποιήσουν για τη διακινούμενη πληροφορία στην κυρίως επικοινωνία. Το κλειδί, επίσης, θα πρέπει να αλλάζει κάθε φορά, καθώς υπάρχει περίπτωση ένας ωτακουστής να βρει δύο ή περισσότερα κρυπτογραφήματα του ίδιου κλειδιού, να τα συγκρίνει και να σχηματίσει άποψη για το αρχικό κείμενο, άρα και για το κλειδί. Συνεπώς, το κλειδί θα πρέπει να διανέμεται μέσα από ένα ασφαλές κανάλι επικοινωνίας (πιθανόν και εκτός δικτύου) ή μέσω της φυσικής παρουσίας των προσώπων, χωρίς κάποιος άλλος να λάβει γνώση αυτού. Το γεγονός αυτό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Έστω δυο χρήστες. Τα στάδια της επικοινωνίας τους μέσω της συμμετρικής μεθόδου είναι τα ακόλουθα:

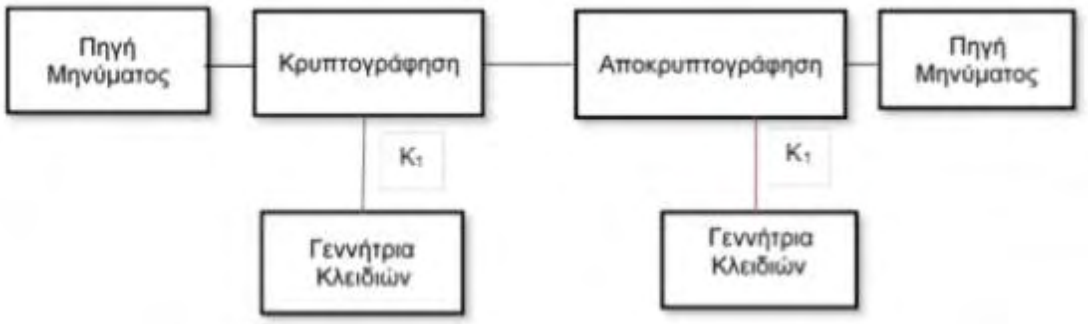
1. Οι χρήστες του συστήματος αποφασίζουν για ένα κλειδί, το οποίο λαμβάνει μια τυχαία τιμή μέσα από ένα ευρύ φάσμα πιθανών τιμών, το οποίο ονομάζεται κλειδοχώρος (keyspace).

2. Ο πρώτος χρήστης στέλνει το κλειδί αυτό στο δεύτερο χρησιμοποιώντας ένα ασφαλές κανάλι.

3. Ο δεύτερος δημιουργεί ένα μήνυμα.

4. Το κρυπτογραφεί με το κλειδί που παρέλαβε και αποστέλει την προκύπτουσα κρυπτοσυμβολοσειρά.

5. Ο πρώτος λαμβάνει την κρυπτοσυμβολοσειρά και έπειτα χρησιμοποιώντας το ίδιο κλειδί την αποκρυπτογραφεί. Η έξοδος που προκύπτει είναι το αρχικό μη κρυπτογραφημένο μήνυμα.



Εικόνα 14: Στάδια επικοινωνίας συμμετρικής μεθόδου

Πηγή:http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/2633/cse_39095.pdf?sequence=5&isAllowed=y

Ο Shannon απέδειξε ότι απαραίτητη συνθήκη, για να είναι μια κρυπτογράφηση συμμετρικού κλειδιού απόλυτα ασφαλής, είναι η αβεβαιότητα του μυστικού κλειδιού να είναι τουλάχιστον τόσο μεγάλη όσο η αβεβαιότητα του απλού κειμένου. Το πρόβλημα της διανομής τόσο μεγάλων κλειδιών, όμως, περιορίζει τις εφαρμογές του συμμετρικού σχήματος σε περισσότερο κρίσιμες εφαρμογές. Στις καθημερινές εφαρμογές, συνήθως, γίνεται χρήση μικρού κλειδιού.

Χαρακτηριστικοί αλγόριθμοι αυτής της κατηγορίας είναι ο Data Encryption Standard (DES), ο Triple DES (3DES), ο Advanced Encryption Standard (AES), ο RC4, ο IDEA, ο Camellia και ο Blowfish, ενώ το περισσότερο διαδεδομένο σύστημα που επιτρέπει την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα είναι το Kerberos που έχει αναπτυχθεί στο MIT.

Ασύμμετρα (ή μονής κατεύθυνσης) Κρυπτοσυστήματα

Η ιδέα του δημοσίου κλειδιού καθυστέρησε αρκετά να πραγματοποιηθεί και μια σημαντική αιτία γι'αυτό ήταν ότι έως τις αρχές της δεκαετίας του '70 η κρυπτογραφία

χρησίμευε κυρίως για στρατιωτική ή διπλωματική χρήση, για την οποία τα συμμετρικά κρυπτοσυστήματα ήταν αρκετά αποδοτικά, καθώς διέθεταν ισχυρό και αξιόπιστο ταχυδρομείο. Με την ανάπτυξη, όμως, της μηχανογράφησης στον οικονομικό, κυρίως, τομέα προέκυψε η ανάγκη για μια νέα μέθοδο κρυπτογραφίας με περισσότερη ασφάλεια.

Το 1968, λοιπόν, ο M. V. Wilkes άφησε πρώτος υπόνοιες για την πιθανότητα εφεύρεσης ενός νέου τύπου κρυπτοσυστήματος από τα μέχρι τότε γνωστά. Στο βιβλίο του, Time-Sharing Computer Systems, περιγράφεται ένα νέο μονόδρομο κρυπτοσύστημα, το οποίο χρησιμοποιήθηκε από τον R.M. Needham με σκοπό να επιτρέψει σε κάποιον υπολογιστή να επιβεβαιώσει κωδικούς χωρίς να χρειαστεί να αποθηκεύσει πληροφορίες, τις οποίες θα μπορούσε να εκμεταλλευτεί ένας εισβολέας, ώστε να μιμηθεί κάποιο νόμιμο χρήστη.

Στο κρυπτοσύστημα του Needham, όταν ο χρήστης θέσει τον κωδικό του, αλλά και κάθε φορά που τον αλλάζει, αυτός κρυπτογραφείται και αποθηκεύεται στον υπολογιστή. Κάθε φορά που πληκτρολογείται ο κωδικός του, ξανακρυπτογραφείται και η κρυπτογραφημένη του μορφή συγκρίνεται με την ήδη αποθηκευμένη στον υπολογιστή. Με τον τρόπο αυτό, δε θα είχε νόημα κάποιος κρυπταναλυτής να αποκτήσει τη λίστα των κωδικών που είναι αποθηκευμένοι στον υπολογιστή, αφού για να τους χρησιμοποιήσει θα έπρεπε πρώτα να τους αποκρυπτογραφήσει. Ακόμα και αν είχε στα χέρια του τον πλήρη αλγόριθμο κρυπτογράφησης, η διαδικασία αυτή θα ήταν αρκετά χρονοβόρα. Η πρώτη λεπτομερής περιγραφή μίας τέτοιας μονόδρομης συνάρτησης κοινοποιήθηκε το 1974.

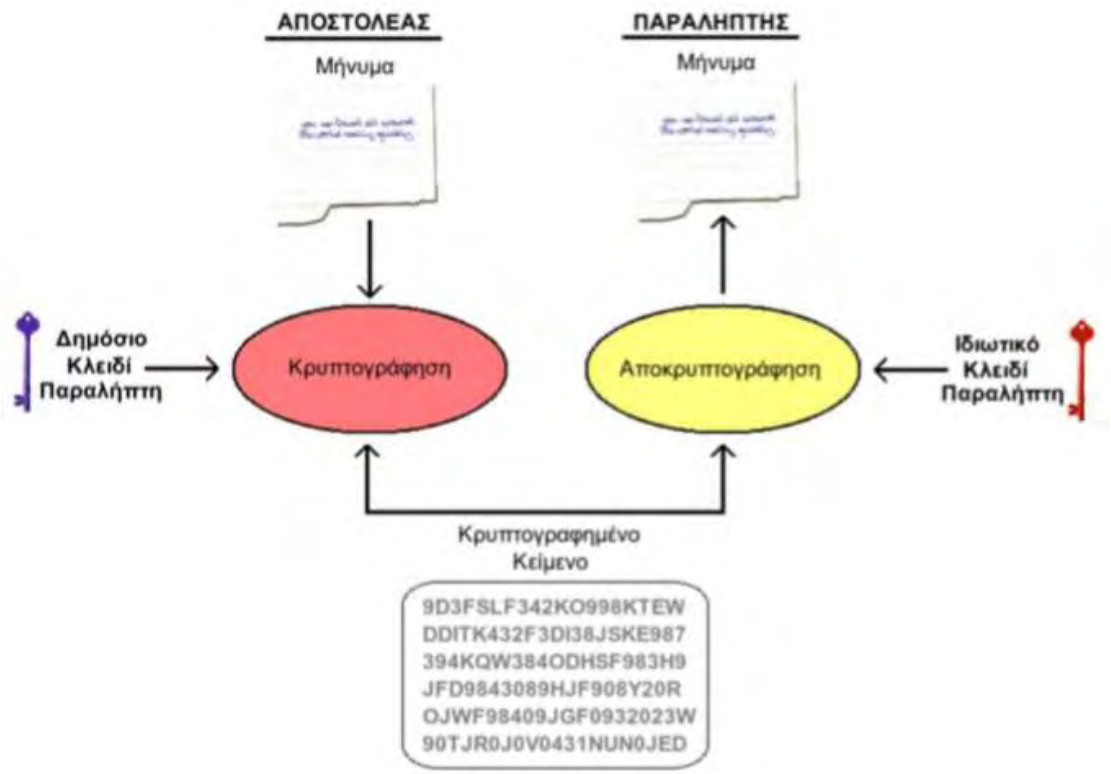
Το 1976, οι ερευνητές Whitfield Diffie και Martin Hellman δημοσίευσαν την εργασία τους με τίτλο ¨New Directions in Cryptography¨, όπου, επιχειρώντας να λύσουν το μειονέκτημα των συμμετρικών κρυπτογραφικών αλγορίθμων, πρότειναν μια εντελώς καινούρια μέθοδο διανομής κλειδιών που έγινε γνωστή ως ανταλλαγή κλειδιών των Diffie και Hellman (Diffie–Hellman key exchange) και αποτέλεσε τη βάση της ασύμμετρης κρυπτογραφίας.

Η ασύμμετρη κρυπτογραφία είναι ίσως η πιο ουσιαστική πρόοδος στη θεωρία κωδικοποίησης στα 3000 χρόνια της ιστορίας της. Σε αυτήν την κατηγορία συστημάτων, κάθε χρήστης κατέχει ένα ζεύγος (διαφορετικών) κλειδιών (key pair), επομένως, για n οντότητες απαιτούνται 2n κλειδιά. Το ένα χρησιμοποιείται για την

κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Γνωστά και ως δημόσιου κλειδιού κρυπτοσυστήματα, συγκροτούν τη νεότερη μορφή κρυπτογραφίας, καθώς έχουν γίνει αρκετά δημοφιλή τα τελευταία 20 χρόνια.

Σύμφωνα με αυτά, εάν ένας χρήστης (π.χ μια τράπεζα) θέλει να λάβει ένα κρυπτογραφημένο μήνυμα, θα πρέπει να δημιουργήσει ένα μυστικό κλειδί (private key) και από αυτό να παράγει ένα δημόσιο (public key), το οποίο θα κοινοποιήσει. Με το δημόσιο κλειδί ο χρήστης, με τον οποίο θέλει να επικοινωνήσει (π.χ. ο πελάτης της τράπεζας που θέλει να κάνει μια συναλλαγή μέσω του διαδικτύου), θα μπορεί να κρυπτογραφήσει οποιοδήποτε μήνυμα επιθυμεί (π.χ τα στοιχεία της συναλλαγής) και να το στείλει πίσω. Προκειμένου να αποκωδικοποιηθεί το μήνυμα, αναγκαίο είναι και το δημόσιο και το ιδιωτικό κλειδί, το οποίο δε φεύγει ποτέ από τον παραλήπτη, οπότε δεν υπάρχει κίνδυνος υποκλοπής. Το ιδιωτικό κλειδί, δηλαδή, δε μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες στηρίζονται στο δημόσιο. Η βασική σχέση μεταξύ τους είναι: ό,τι κρυπτογραφεί ο ένας, μπορεί να το αποκρυπτογραφήσει μόνο ο άλλος, ενώ παρά το γεγονός ότι τα κλειδιά σχετίζονται μαθηματικά, δεν είναι δυνατό να υπολογιστεί το ιδιωτικό με βάση το δημόσιο. Θεωρητικά, βέβαια, μπορεί να γίνει, αλλά το κόστος, ο χρόνος επίτευξης, η μνήμη και η υπολογιστική ισχύς είναι παράγοντες οι οποίοι το καθιστούν σχεδόν αδύνατο.

Στα κρυπτοσυστήματα δημοσίου κλειδιού, σύμφωνα με τις απαιτήσεις ασφάλειας, το είδος της εφαρμογής και της υπηρεσίας που βρίσκεται υπό σχεδιασμό και υλοποίηση, ο αποστολέας χρησιμοποιεί είτε το δικό του ιδιωτικό κλειδί είτε το δημόσιο κλειδί του παραλήπτη είτε και τα δύο με σκοπό να πραγματοποιήσει τη διαδικασία της κρυπτογράφησης. Οποιοδήποτε, δηλαδή, από τα δύο κλειδιά μπορεί να χρησιμοποιηθεί για κωδικοποίηση, αλλά για την αποκωδικοποίηση θα χρησιμοποιηθεί όποιο δε χρησιμοποιήθηκε στο πρώτο βήμα.

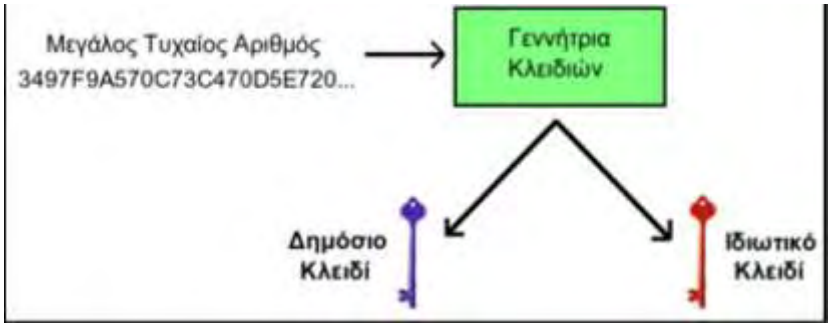


Εικόνα 15: Διαδικασία κωδικοποίησης κρυπτοσυστήματος δημοσίου κλειδιού
Πηγή:http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/2633/cse_39095.pdf?sequence=5&isAllowed=y

Η ασφάλεια της όλης διαδικασίας στηρίζεται στη μυστικότητα των ιδιωτικών κλειδιών, συνεπώς, θα πρέπει να υπάρχει διαδικασία ανάκτησης (key escrow) για την περίπτωση απώλειάς τους. Έχουν ανακαλυφθεί διάφοροι τρόποι προκειμένου να υπάρχει αυξημένο επίπεδο προστασίας τους. Οι έξυπνες κάρτες είναι ένας από τους πιο αποτελεσματικούς τρόπους. Οι τεχνολογίες για έξυπνες κάρτες αλλά και αναγνώστες έξυπνων καρτών για προσωπικούς υπολογιστές είναι ήδη διαθέσιμες και το κόστος τους κυμαίνεται σε πολύ λογικά πλαίσια.

Αν, παρ'όλα αυτά, παραβιαστεί το σύστημα, υπάρχει η δυνατότητα να αλλάξουν μόνο τα κλειδιά που έχουν χρησιμοποιηθεί και όχι ολόκληρος ο αλγόριθμος κρυπτογράφησης, όπως θα γινόταν στην περίπτωση της συμμετρικής κρυπτογράφησης.

Η δημιουργία των δύο αντιστρόφως συσχετιζόμενων κλειδιών (του δημόσιου και του ιδιωτικού) γίνεται ταυτόχρονα από ειδικές συναρτήσεις κάποιου ειδικού λογισμικού προγράμματος, οι οποίες δέχονται ως είσοδο έναν μεγάλο, τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαία είναι η είσοδος στη γεννήτρια, τόσο πιο ασφαλές είναι και το ζεύγος κλειδιών που παράγεται.



Εικόνα 16: Διαδικασία δημιουργίας ζεύγους κλειδιών

Πηγή: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1554/1/Κείμενο%20διπλωματικής.pdf

Ένας χρήστης έχει τη δυνατότητα να αλλάξει το ιδιωτικό του κλειδί όποια στιγμή επιθυμεί και ταυτόχρονα να κοινοποιήσει το αντίστοιχο καινούριο δημόσιο κλειδί, ώστε να αναπληρωθεί το προηγούμενο, μη πλέον ισχύον δημόσιο κλειδί.

Η ασφάλεια των κρυπτοσυστημάτων δημοσίου κλειδιού, συνήθως, βασίζεται, επίσης, στην υπολογιστική πολυπλοκότητα ορισμένων μαθηματικών προβλημάτων, γι' αυτό και συνιστώνται για την κρυπτογράφηση/αποκρυπτογράφηση αριθμητικών δεδομένων μικρού, κυρίως, μεγέθους. Ένα από τα μαθηματικά προβλήματα που χρησιμοποιούνται είναι η παραγοντοποίηση ακεραίου σε πρώτους αριθμούς.

Ένα άλλο μαθηματικό εργαλείο, που χρησιμοποιούν τα συστήματα αυτά, είναι οι μονόδρομες συναρτήσεις, στις οποίες είναι εύκολο να υπολογιστεί η τιμή της f(x) για δεδομένο x, όμως είναι δύσκολο να συμβεί το αντίστροφο. Στην επιστήμη των υπολογιστών, η θεωρία της υπολογιστικής πολυπλοκότητας ορίζει ως δύσκολο ένα πρόβλημα όταν ο χρόνος εκτέλεσης του αλγορίθμου επίλυσης αυξάνεται εκθετικά με τη γραμμική αύξηση της εισόδου σε bits και εύκολο όταν αυξάνεται πολυωνυμικά ή, προτιμότερα, γραμμικά. Για τα δύσκολα προβλήματα, δηλαδή, δεν υπάρχει κάποιος γρήγορος και αποτελεσματικός αλγόριθμος πολυωνυμικού χρόνου που να είναι κατάλληλος για κλασικούς υπολογιστές.

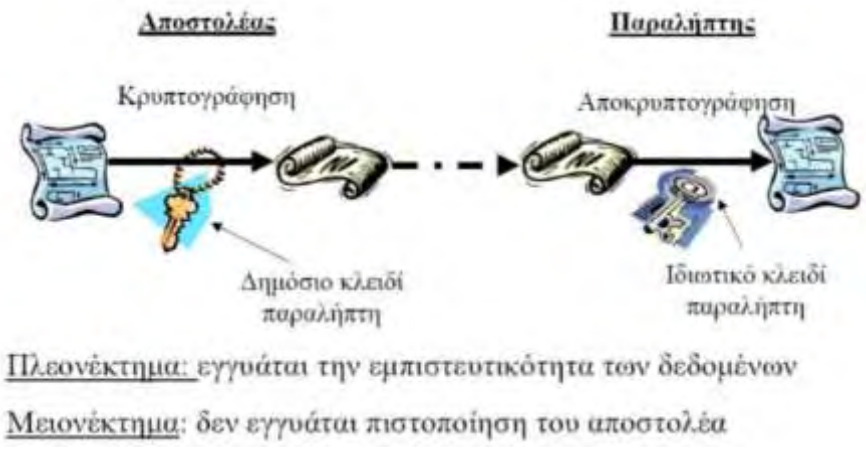
Επιπλέον, αξίζει να αναφερθεί, πως οι δυνατότητες της ασύμμετρης κρυπτογραφίας είναι αυτές που οδήγησαν στη δημιουργία των ψηφιακών υπογραφών, οι οποίες αποβλέπουν στο να αντικαταστήσουν πλήρως τις σημερινές και στη συνέχεια στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Το αρνητικό χαρακτηριστικό της κρυπτογραφίας δημοσίου κλειδιού είναι το μεγάλο υπολογιστικό κόστος της, λόγω των πολύπλοκων υπολογισμών που διαθέτει. Ακόμη

και με τη χρήση σύγχρονων υπολογιστών, η κρυπτογράφηση δημόσιου κλειδιού είναι εξαιρετικά πιο αργή έναντι της συμμετρικής κρυπτογράφησης, ακόμη και για μικρού μεγέθους μηνύματα, με αποτέλεσμα οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού να χρησιμοποιούνται κατά κύριο λόγο για την κρυπτογράφηση των κλειδιών των συμμετρικών συστημάτων και όχι για τον κύριο όγκο δεδομένων. Επομένως, είναι κατανοητό ότι δεν ήρθαν για να αντικαταστήσουν τη συμμετρική κρυπτογραφία, αλλά να τη συμπληρώσουν. Εξ'άλλου, σε μερικά κλειστά συστήματα η συμμετρική κρυπτογραφία είναι υπεραρκετή, αφού δε χρειάζεται μεταφορά του κλειδιού.

Μερικοί χαρακτηριστικοί ασύμμετροι κρυπταλγόριθμοι είναι οι RSA, DSA, Paillier, DSS, το Πρωτόκολλο Diffie-Hellman, το Πρότυπο ElGamal ή αλλιώς η Υπογραφή ElGamal και η Κρυπτογραφία ελλειπτικών καμπυλών (ECC).

Οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι εγγυώνται εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα σταλεί από τον αποστολέα μέσω του διαδικτύου στον παραλήπτη θα διαβαστεί από αυτόν και μόνο, καθώς μπορεί να αποκρυπτογραφηθεί μόνο από το ιδιωτικό του κλειδί, αλλά όχι και πιστοποίηση του αποστολέα. Αυτό, συνοπτικά, σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα, ώστε να μην υπάρξει η σκόπιμη ή μη πλαστοπροσωπία. Πράγματι, ο αποστολέας μπορεί να δώσει ψευδή στοιχεία και ο παραλήπτης να θεωρήσει ότι το μήνυμα προήλθε από άλλο πρόσωπο.



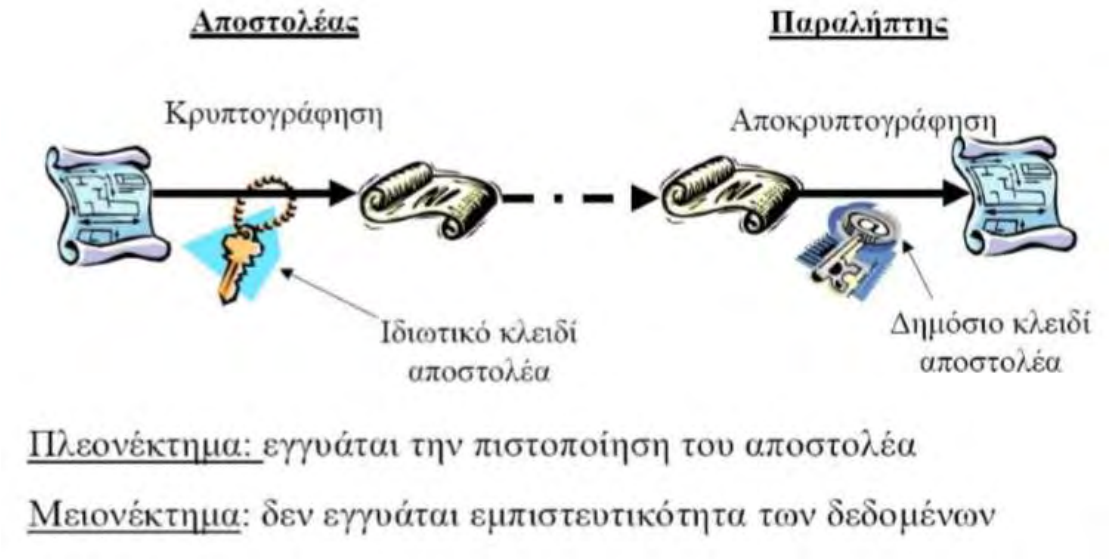
Εικόνα 17: Εγγύηση εμπιστευτικότητας αλλά όχι πιστοποίησης

Πηγή: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1554/1/Κείμενο%20διπλωματικής.pdf

Κάνοντας κατάλληλη χρήση των κρυπτογραφικών αλγορίθμων δημοσίου κλειδιού, μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με σιγουριά την ταυτότητα του αποστολέα. Για να συμβεί αυτό, θα πρέπει ο

αποστολέας να κάνει χρήση του ιδιωτικού του κλειδιού στην κρυπτογράφηση του μηνύματος. Στην συνέχεια, να το στείλει στον παραλήπτη και εκείνος να χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί είναι γνωστό μόνο στον ίδιο τον αποστολέα, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητά του.

Η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν εγγυάται, όμως, και την εμπιστευτικότητα του μηνύματος. Το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε έχει στη διάθεσή του το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη αναφερθεί, το δημόσιο κλειδί είναι γνωστό σε όλη τη διαδικτυακή κοινότητα, με αποτέλεσμα, οποιοσδήποτε να μπορεί να διαβάσει το περιεχόμενο του μηνύματος.



Εικόνα 18: Εγγύηση πιστοποίησης αλλά όχι εμπιστευτικότητας

Πηγή: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1554/1/Κείμενο%20διπλωματικής.pdf

Συνδυάζοντας τις δύο παραπάνω τεχνικές, είναι δυνατό να επιτευχθεί και εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή, και το μήνυμα να παραμένει γνωστό μόνο στον αποστολέα και τον παραλήπτη και ο παραλήπτης να γνωρίζει με σιγουριά την ταυτότητα του αποστολέα. Για να γίνει κάτι τέτοιο, ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα αρχικά με το δικό του ιδιωτικό κλειδί και μετά με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης δεχθεί το μήνυμα, θα πρέπει να κάνει χρήση του ιδιωτικού του κλειδιού για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει

αυτό που θα προκύψει κάνοντας χρήση του δημόσιου κλειδιού του αποστολέα (πιστοποίηση).

Είναι εύκολα αντιληπτό, λοιπόν, ότι είναι αρκετά πολύπλοκο το να εξασφαλίσει κανείς την ασφάλεια ενός κρυπτοσυστήματος δημοσίου κλειδιού. Δεν αρκεί, δηλαδή, να γνωρίζει κανείς ότι ο κρυπταναλυτής είναι αδύνατον να υπολογίσει την αντίστροφη συνάρτηση. Οι πιο πετυχημένες επιθέσεις στα δημοφιλή κρυπτοσυστήματα είναι πιο ¨πλάγιες¨.

Ο κρυπταναλυτής θεωρείται πάντα ότι διαθέτει όλα τα δημόσια κλειδιά, καθώς επίσης και ότι έχει στην κατοχή του μια πλήρη περιγραφή του αλγορίθμου αποκρυπτογράφησης του εκάστοτε κρυπτογραφημένου κειμένου. Για να γίνει κάποια δήλωση σχετικά με την ασφάλεια ενός κρυπτοσυστήματος, πρέπει να μπορεί να υπολογιστεί, με κάποιο τρόπο, και η δύναμη του κρυπταναλυτή, για παράδειγμα, η υπολογιστική του ισχύς. Ένα κρυπτοσύστημα θεωρείται απρόσιτο αν μπορεί να καταρρίπτει επιθέσεις από "δυνατούς" κρυπταναλυτές. Η έννοια του "απρόσιτου" είναι στενά συνδεδεμένη με την τρέχουσα διαθέσιμη υπολογιστική δύναμη, εξαρτάται, ουσιαστικά, από την εξέλιξη της τεχνολογίας των υπολογιστών. Επομένως, μια συνάρτηση που θεωρείται σήμερα ως ασφαλής, μπορεί να χάσει αυτή της την ιδιότητα στο μέλλον.

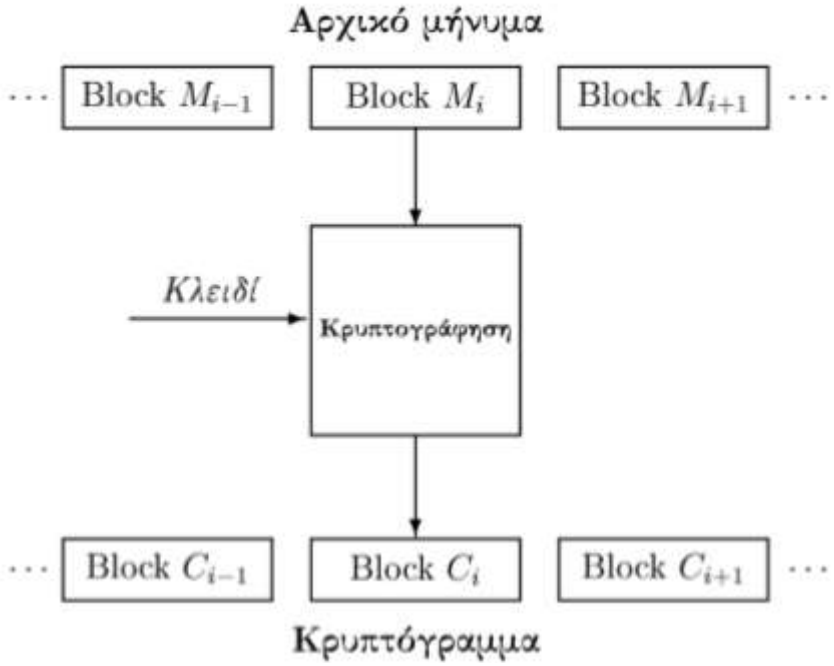
Τα τελευταία χρόνια εντοπίζονται όλο και περισσότερες επιθέσεις που εκμεταλλεύονται συγκεκριμένες ιδιότητες των εφαρμογών και του λειτουργικού συστήματος. Τέτοιου είδους επιθέσεις χρησιμοποιούν πληροφορίες που διαρρέουν από τον υπολογιστή κατά την διάρκεια διεργασιών πάνω στο δημόσιο κλειδί, όπως η αποκρυπτογράφηση και η παραγωγή υπογραφών. Οι πληροφορίες αυτές μπορεί να περιέχουν χρόνους εκτέλεσης, κατανάλωση ενέργειας, ηλεκτρομαγνητική ακτινοβολία, λάθη κατά την εκτέλεση ή και μηνύματα σφάλματος.

Υπάρχουν επαγγελματικοί οργανισμοί που εγγυώνται την ασφάλεια ενός κρυπτοσυστήματος, όπως οι ANSI, IEEE και ISO. Οι οργανισμοί αυτοί κάνουν συχνά και προτάσεις για τον ορθό τρόπο χρήσης των εγκεκριμένων κρυπτοσυστημάτων. Μιας και κανένας από αυτούς τους οργανισμούς δε ρισκάρει να εγκρίνει κάποιο κρυπτοσύστημα, το οποίο θα ¨σπάσει¨ μετά από λίγο καιρό, οι διαδικασίες έγκρισης είναι εξαιρετικά αργές. Στην περίπτωση των πιο δημοφιλών κρυπτοσυστημάτων

δημοσίου κλειδιού, για παράδειγμα, ο χρόνος από την ακαδημαϊκή τους πρόταση μέχρι την τελική έγκριση και την πρακτική τους χρήση ήταν περίπου 15 χρόνια.

Κρυπτοσυστήματα Δέσμης

Σε αυτήν την κατηγορία αλγορίθμων, το μήνυμα χωρίζεται σε κομμάτια, δηλαδή ομάδες από δυαδικά ψηφία (ψηφιακές λέξεις) και κρυπτογραφείται κάθε ένα από τα κομμάτια αυτά χωριστά. Ουσιαστικά, μια ομάδα απλού κειμένου (plaintext) καθορισμένου μήκους μετατρέπεται σε ομάδα κρυπτογραφημένου κειμένου (ciphertext) του ίδιου μήκους.



Εικόνα 19: Διαδικασία κωδικοποίησης κρυπτοσυστημάτων δέσμης

Πηγή: https://repository.kallipos.gr/bitstream/11419/5439/1/main-KOY.pdf

Μία τυπική τιμή για το μέγεθος του τμήματος (block size) σε αλγορίθμους αυτής της κατηγορίας είναι 128 bits. Σε περίπτωση που το μήκος ενός μηνύματος δεν αποτελεί πολλαπλάσιο του μεγέθους του τμήματος, κατάλληλο πλήθος ψηφίων προστίθεται σ'αυτό σύμφωνα με κάποια προεπιλεγμένη συνθήκη.

Η λειτουργία αυτών των αλγορίθμων, οι οποίοι αποτελούν ουσιαστικά κλάσεις συναρτήσεων, είναι επαναληπτική, υπό την έννοια ότι η πληροφορία ρέει μέσα από διάφορα διαδοχικά στάδιά (rounds), όπου σε κάθε στάδιο πραγματοποιείται ακριβώς ο ίδιος κρυπτογραφικός μετασχηματισμός μέσω τεχνικών που ονομάζονται καταστάσεις

λειτουργίας (modes), με σκοπό να σχηματιστεί το τελικό τμήμα κρυπτογράμματος. Ο μετασχηματισμός αυτός επιτυγχάνεται με τη χρήση ενός μυστικού κλειδιού που δίνεται από το χρήστη με ειδική συνάρτηση, ενώ με το ίδιο μυστικό κλειδί γίνεται και η αποκρυπτογράφηση (συμμετρική μορφή). Κάθε στάδιο, που ονομάζεται γύρος του κρυπταλγορίθμου, τροφοδοτείται με το αποτέλεσμα του προηγούμενου και χρησιμοποιεί διαφορετικό τμήμα του κλειδιού (subkey) που ονομάζεται κλειδί γύρου. Αυτό έχει σαν αποτέλεσμα, κάθε κείμενο, στο οποίο εφαρμόζεται το κρυπτογράφημα τμήματος, να αποδίδει διαφορετικό αποτέλεσμα.

Τα κλειδιά γύρου δημιουργούνται από ένα πρόγραμμα κλειδιού, το οποίο, συνήθως, είναι εκτός του κυρίως αλγορίθμου. Το σύνολο των υποκλειδιών καλείται σχεδιασμός κλειδιών (key schedule) και η διαδικασία υπολογισμού τους γίνεται στην αρχή για λόγους ταχύτητας.

Ο αριθμός των επαναλήψεων εξαρτάται από την επιθυμητή ασφάλεια και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει το επίπεδο ασφάλειας, αλλά για μερικά κρυπτοσυστήματα, ο αριθμός των επαναλήψεων, για να επιτευχθεί ικανοποιητική ασφάλεια, θα πρέπει να είναι πολύ μεγάλος.

Σε όλους τους αλγορίθμους τμήματος προστίθεται και μία μονάδα αντικατάστασης (Substitution Box ή S-Box) που πραγματοποιεί αντικαταστάσεις bits με μη γραμμικό τρόπο. Αποτέλεσμα αυτής είναι το να υπάρχει τελικά μία σύνθετη σχέση μεταξύ των bits του κλειδιού και των bits του κρυπτογράμματος. Η ιδιότητα αυτή ονομάζεται σύγχυση (confusion) και ορίστηκε από τον Shannon ως αναγκαία συνθήκη για να χαρακτηριστεί ένα σύστημα ασφαλές.

Χαρακτηριστικά παραδείγματα αλγορίθμων αυτής της υποκατηγορίας αποτελούν οι αλγόριθμοι 3Way ,Blowfish, CAST ,CMEA , TripleDES, DEAL FEAL, GOST, IDEA,LOKI, Lucifer, MacGuffin, TwofishMARS, MISTY, MMB, NewDES, RC2, RC5, RC6 REDOC, Rijndael, Safer, Serpent, SQUARE, Skipjack, Tiny Encryption Algorithm κ.α..

Οι αλγόριθμοι αυτοί έχουν διάφορους τρόπους λειτουργίας. Καθένας από αυτούς μπορεί να έχει τις ιδιότητές του, εκτός από αυτές που κληρονομεί από τον βασικό αλγόριθμο. Οι βασικοί τρόποι λειτουργίας είναι: ο Electronic Code Book (ECB), ο

Cipher Block Chaining (CBC), ο Cipher Feedback (CFB) και ο Output Feedback (OFB).

Κρυπτοσυστήματα Ροής

Στη δεύτερη κατηγορία, οι αλγόριθμοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα. Οι κρυπταλγόριθμοι αυτοί συναντώνται τόσο σε συμμετρική όσο και σε ασύμμετρη μορφή. Λειτουργούν κρυπτογραφώντας μεμονωμένα τη μικρότερη μονάδα ενός ψηφιακού συστήματος, τα δυαδικά ψηφία, (bits) χρησιμοποιώντας ένα μετασχηματισμό κρυπτογράφησης, ο οποίος μεταβάλλεται με τον χρόνο. Για το λόγο αυτό, μερικές φορές λέγονται και κρυπταλγόριθμοι κατάστασης επειδή η κρυπτογράφηση εξαρτάται όχι μόνο από το κλειδί και το απλό κείμενο αλλά και από την τρέχουσα κατάσταση.

Δυστυχώς, όμως, η απαίτηση, το μέγεθος του κλειδιού να ισούται με αυτό του μηνύματος, καθιστά ένα τέτοιο σύστημα δύσκολο να εφαρμοστεί στην πράξη λόγω δυσκολιών στη δημιουργία, διαχείριση και διανομή των κρυπτογραφικών κλειδιών. Τα κρυπτοσυστήματα ροής προσπαθούν να παρακάμψουν αυτό το εμπόδιο. Έτσι, χρησιμοποιούν ένα κλειδί, το οποίο παράγεται με τυχαίο τρόπο και έχει πολύ μικρό μέγεθος, ανεξάρτητο από το μήνυμα προς κρυπτογράφηση, προσπαθώντας, όμως, να το επεκτείνουν, ώστε να έχει το μέγεθος του μηνύματος. Φυσικά, η επέκταση αυτή παράγει μια ακολουθία bits (κλειδοροή), η οποία δεν είναι πραγματικά τυχαία και συνδυάζεται με το αρχικό κείμενο, συνήθως, με τη συνάρτηση XOR, προκειμένου να παραχθεί το κρυπτογραφημένο μήνυμα.

Η παραγωγή της κλειδοροής μπορεί να είναι ανεξάρτητη του αρχικού κειμένου και του κρυπτογραφήματος (συγχρονισμένοι κώδικες ροής (synchronous stream cipher)) ή μπορεί να εξαρτάται από αυτά (ασύγχρονοι κώδικες ροής (self-synchronizing stream cipher)). Τις περισσότερες φορές, βέβαια, είναι ανεξάρτητη. Στόχος είναι να φαίνεται τυχαία σε έναν ωτακουστή με περιορισμένους υπολογιστικούς πόρους. Συνεπώς, τα κρυπτοσυστήματα αυτά δεν προσφέρουν απόλυτη ασφάλεια.

Παρόλα αυτά, είναι αρκετά γρήγορα στην εκτέλεση, κατά πολύ ταχύτερα από τους κώδικες τμήματος και μπορούν να υλοποιηθούν με σχετικά λιγότερο πολύπλοκη διάταξη κυκλωμάτων. Έχουν μνήμη, με την έννοια ότι το αποτέλεσμα της κρυπτογράφησης ενός δυαδικού ψηφίου μπορεί να εξαρτάται από την κρυπτογράφηση

των προηγούμενων δυαδικών ψηφίων, σε αντίθεση με τους κρυπταλγορίθμους τμήματος, οι οποίοι χρησιμοποιούν την ίδια συνάρτηση για την κρυπτογράφηση διαδοχικών τμημάτων, επομένως είναι άνευ μνήμης (memoryless). Αυτή η διάκριση μπορεί να πάψει να υφίσταται αν προσθεθεί μια μικρής ποσότητας μνήμη σε έναν κρυπταλγόριθμο τμήματος, ώστε να δώσει ως αποτέλεσμα έναν κρυπταλγόριθμο ροής με μεγάλα τμήματα.

Οι κρυπταλγόριθμοι ροής επιβάλλονται όταν η προσωρινή μνήμη είναι περιορισμένη ή όταν πρέπει οι χαρακτήρες να υποστούν επεξεργασία μεμονωμένα καθώς παραλαμβάνονται. Επειδή έχουν περιορισμένο ή και μηδενικό αριθμό σφαλμάτων μεταβίβασης, πλεονεκτούν σε καταστάσεις όπου είναι πολύ πιθανό να συμβούν τέτοιου είδους σφάλματα (π.χ. τηλεπικοινωνιακές εφαρμογές). Εξαιτίας, λοιπόν, αυτών των σημαντικών πλεονεκτημάτων τους, οι κρυπταλγόριθμοι ροής χρησιμοποιούνται σήμερα ευρέως, αν και οι περισσότεροι έχουν την τάση να είναι ιδιωτικοί και εμπιστευτικοί.

Ισχύς Κρυπτογραφικών Αλγορίθμων

Η ασφάλεια των κρυπτογραφικών συστημάτων, η αντοχή τους, δηλαδή, στις προσπάθειες παραβίασης, είναι ένα από τα πρώτα ερωτήματα που θέτονται πριν αποφασιστεί η εκμετάλλευσή τους σε πρακτικές εφαρμογές. Παρουσιάζουν διάφορα επίπεδα ασφαλείας ανάλογα με το πόσο δύσκολα παραβιάζονται.

Θεωρητικά, κανένα κρυπτοσύστημα δεν είναι απρόσβλητο, καθώς οποιοσδήποτε αλγόριθμος, ο οποίος χρησιμοποιεί κλειδί κρυπτογράφησης, είναι δυνατόν να σπάσει κάνοντας δοκιμή όλων των πιθανών κλειδιών (brute force attack). Αυτό που κάνει ένα κρυπτογραφικό σύστημα να είναι ασφαλές είναι ο χρόνος που χρειάζεται, κάνοντας χρήση της υπάρχουσας τεχνολογίας, ώστε να γίνει έλεγχος όλων των πιθανών κλειδιών, να είναι υπέρογκος. Επομένως, λοιπόν, γίνεται σαφές ότι το μέγεθος του κλειδιού παίζει πρωταρχικό ρόλο στην ασφάλεια ενός συστήματος, καθώς η υπολογιστική δύναμη που απαιτείται για το ¨σπάσιμο¨ ενός συστήματος αυξάνεται εκθετικά με το μέγεθος του κλειδιού.

Από την άλλη πλευρά, η συνεχής βελτίωση της υπολογιστικής δύναμης των υπολογιστών και η ανάπτυξη ολοένα και ευφυέστερων λογισμικών αποκρυπτογράφησης αποτελούν ισχυρό σύμμαχο της κρυπτανάλυσης. Λαμβάνοντας

υπόψιν, επομένως, την ταχύτατη εξέλιξη της τεχνολογίας, το πιο απαιτητικό στάδιο κατά τη διαδικασία υλοποίησης ενός κρυπτοσυστήματος είναι ο καθορισμός του μεγέθους του κλειδιού.

Η μέθοδος επίθεσης που συνηθίζεται στα συμμετρικά συστήματα είναι η brute force attack. Για να αποφεύγονται, σε όσο δυνατόν μεγαλύτερο βαθμό, αυτού του είδους οι απειλές, πρέπει το πλήθος των πιθανών κλειδιών για έναν κρυπτογραφικό αλγόριθμο να είναι μεγαλύτερο από αυτό που θεωρείται αναγκαίο. Αυτό συμβαίνει γιατί, σε περίπτωση που ο κρυπταναλυτής αποκτήσει ένα ζεύγος αρχικού και κρυπτογραφημένου κειμένου, μπορεί προσπαθώντας με όλα τα πιθανά κλειδιά να βρει ποιο ταιριάζει και στη συνέχεια να το χρησιμοποιήσει ώστε να αποκρυπτογραφεί κι άλλα κείμενα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Διαφορετικά, στην περίπτωση που απλά κατάφερε να υποκλέψει ένα κρυπτογραφημένο κείμενο, μπορεί να το αποκρυπτογραφήσει μέσω συνεχών δοκιμών κλειδιών έως ότου βρει ένα αρχικό κείμενο που να έχει λογική σημασία, οπότε τότε αποκτά, ουσιαστικά, και το σωστό κλειδί που, στη συνέχεια, μπορεί να το χρησιμοποιήσει για την αποκρυπτογράφηση και άλλων κειμένων.

Όπως είναι ήδη γνωστό, τα κλειδιά αντιστοιχούν σε σειρές από bits, επομένως, η ανάγκη για μεγάλο πλήθος κλειδιών έχει την έννοια της χρήσης ολοένα και περισσότερων bits. Το πλήθος των πράξεων που χρειάζονται για την αποκάλυψη του κλειδιού λέγεται παράγοντας εργασίας (work factor). Η χρήση 64 bits αποτελεί ένα σύνηθες μήκος κλειδιού, το οποίο έχει παράγοντα εργασίας 2^{64}, δηλαδή απαιτούνται 1019 πράξεις για την παραβίασή του. Για παράδειγμα, για ένα σύστημα με κλειδί 56-bit απαιτείται μεγάλη προσπάθεια προκειμένου να σπάσει, καθώς τα πιθανά κλειδιά είναι 256, παρ'όλα αυτά, όμως, με τη χρήση ειδικού hardware (το οποίο είναι εφικτό να αγοραστεί μόνο από εταιρείες, κυβερνήσεις, κτλ.) το σπάσιμό του γίνεται πιο εύκολο.

Από την άλλη, στα ασύμμετρα συστήματα χρησιμοποιούνται κλειδιά που από τη φύση τους είναι πολύ μεγαλύτερα από εκείνα των συμμετρικών συστημάτων. Σ αυτά τα συστήματα η δυσκολία, πλέον, βρίσκεται στο να υπολογιστεί το ιδιωτικό κλειδί κατέχοντας το δημόσιο κι όχι να βρεθεί το σωστό κλειδί.

Συνεπώς, ένας αλγόριθμος είναι απόλυτα ασφαλής (unconditionally secure) αν, ανεξαρτήτως του μεγέθους του κρυπτογραφημένου μηνύματος ή του κλειδιού των

υπολογιστικών πόρων και του χρόνου που μπορεί να έχει στη διάθεσή του ο κρυπταναλυτής, δεν υπάρχει δυνατότητα να παραβιαστεί, δηλαδή να αποκαλυφθεί το αρχικό ακρυπτογράφητο μήνυμα, ούτε τώρα αλλά ούτε και στο μέλλον.

Κάποιος θα μπορούσε να υποστηρίξει ότι αφού όσο μεγαλύτερο το μέγεθος του κλειδιού τόσο πιο ασφαλές το σύστημα, ας γίνει χρήση ακόμα μεγαλύτερων κλειδιών. Σίγουρα το μέγεθος του κλειδιού εξασφαλίζει ασφαλή συστήματα, όμως, όσο πιο ισχυρή η κρυπτογραφία, τόσο υψηλότερο και το κόστος που απαιτείται σε υπολογιστική ισχύ και χρόνο.

Στην πραγματικότητα, πολλά συστήματα έχουν σπάσει και χωρίς να υπολογιστεί το κλειδί. Ο λόγος για τον οποίο έχουν παραβιαστεί είναι εξαιτίας του ασθενούς σχήματος διαχείρισης κλειδιών (key management). Ένα σχήμα διαχείρισης κλειδιών περιλαμβάνει:

- Δημιουργία κλειδιών (key generation): Πόσο προβλέψιμοι και τυχαίοι είναι οι αριθμοί που θα χρησιμοποιηθούν για τη δημιουργία του κλειδιού.
- Αποθήκευση κλειδιών (key storage): Τα κλειδιά αποθηκεύονται και φυλάσσονται π.χ. σε smart cards ή κρυπτογραφούνται με κάποιο άλλο κλειδί και αποθηκεύονται σε μια βάση δεδομένων.
- Αλλαγή κλειδιών (key change): Ανά τί χρονικά διαστήματα αλλάζονται τα κλειδιά, ποιό σχήμα αντικατάστασης κλειδιών είναι διαθέσιμο σε περίπτωση που κάποιο από τα κλειδιά διαρρεύσει.
- Καταστροφή κλειδιών (key destruction): Ο τρόπος με τον οποίο καταστρέφονται μη χρησιμοποιούμενα κλειδιά και αν υπάρχει κίνδυνος ανάκτησής τους.
- Χρήση και Διαχωρισμός κλειδιών (key usage and separation): Τα κλειδιά διαχωρίζονται ανάλογα με τη χρήση τους (κλειδί αποθήκευσης δεδομένων, κλειδί διανομής άλλων κλειδιών κτλ.)

(Πηγή:http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/2633/cse_39095.pdf?sequence=5&isAllowed=y)

Συνεπώς, ο σχεδιαστής του κρυπτογραφικού αλγορίθμου ή ο χρήστης που πρόκειται να μεταχειριστεί ένα προϊόν κρυπτογράφησης πρέπει να αποπειραθεί να σπάσει τον αλγόριθμο. Μόνο με αυτόν τον τρόπο μπορεί κανείς να επιβεβαιώσει την ανθεκτικότητα ενός κρυπτογραφικού συστήματος. Κατά τ' άλλα, δεν υπάρχουν

μέθοδοι που να αποδεικνύουν την ασφάλεια που παρέχουν οι περισσότεροι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στην πράξη (Wenbo Mao, 2003).

ΚΒΑΝΤΙΚΗ ΔΙΑΜΟΙΡΑΣΗ ΚΛΕΙΔΙΟΥ

Γενικά

Όπως έχει ήδη αναφερθεί, κανένα κλασικό κρυπτοσύστημα δεν είναι απόλυτα ασφαλές. Το κεντρικό ζήτημα των κρυπτοσυστημάτων ανέκαθεν είναι το πώς θα πραγματοποιηθεί η διαμοίραση του μυστικού κλειδιού μεταξύ δυο χρηστών με ασφαλή τρόπο. Με τη διαμοίραση, ωστόσο, συμπεριλαμβάνεται και η παραγωγή ενός πραγματικά τυχαίου μυστικού κλειδιού.

Το πρόβλημα αυτό ήρθαν να λύσουν τα κβαντικά κρυπτογραφικά συστήματα επικοινωνίας. Στα συστήματα αυτά, αφού πραγματοποιηθεί η διαδικασία της δημιουργίας και της διαμοίρασης του μυστικού κλειδιού, το κβαντικό μέρος τους, ουσιαστικά, έχει λάβει τέλος. Συνεπώς, έπεται η κλασική διαδικασία κρυπτογράφησης, αποστολής και αποκρυπτογράφησης των δεδομένων, όπως περιγράφθηκε στο προηγούμενο κεφάλαιο.

Η αρχική δημιουργία και διαμοίραση του μυστικού κλειδιού πραγματοποιείται με τη βοήθεια ενός ¨κβαντικού καναλιού¨ και ενός καθιερωμένου, ενώ, στη συνέχεια, η διαδικασία ολοκληρώνεται μόνο με τη βοήθεια του καθιερωμένου μέσου μετάδοσης.

Το ¨κβαντικό κανάλι¨ είναι το κανάλι που παρέχει τη μετάδοση των qubits (του κλειδιού) προσφέροντας τις συνθήκες που χρειάζεται για τη συντήρησή του το κάθε σύστημα. Το κανάλι αυτό μπορεί να διαφοροποιείται ανάλογα με το είδος του κβαντικού συστήματος που έχει επιλεχθεί για την κωδικοποίηση των qubits.

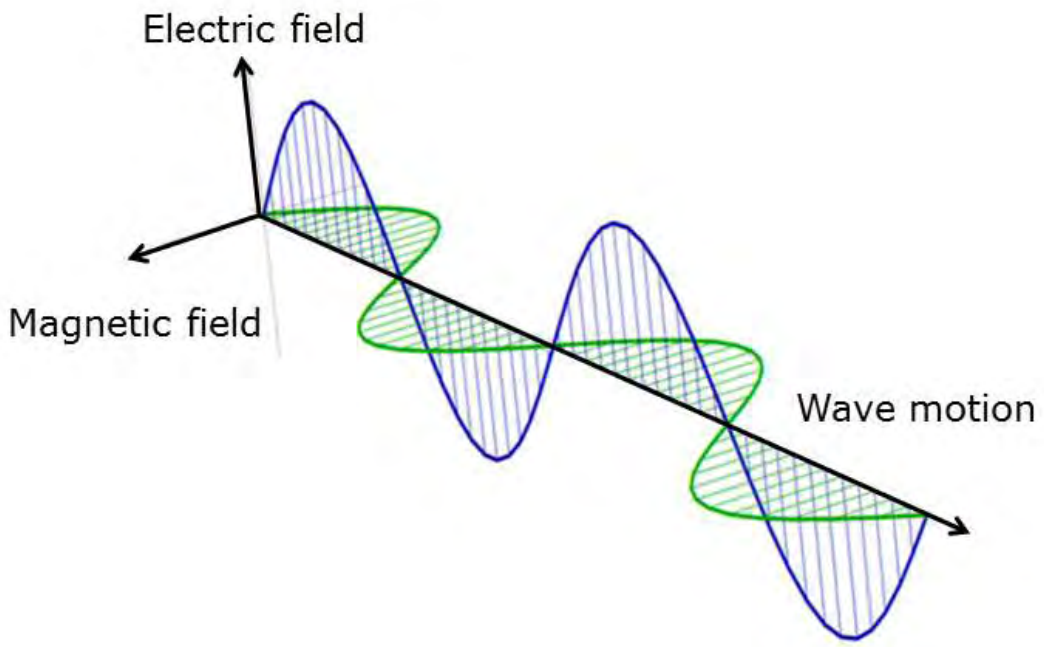
Το κλειδί της επιτυχίας του ασυνήθιστου αυτού τρόπου επικοινωνίας εστιάζεται στο περίφημο κβαντικό φαινόμενο της ¨Αρχής της απροσδιοριστίας¨ του W. Heisenberg και στο φαινόμενο της ¨Διεμπλοκής¨. Χάρις αυτών, είναι αδύνατο να μην εντοπιστεί η παραμικρή απόπειρα παρεμβολής.

Στη δημιουργία και διαμοίραση του μυστικού κλειδιού έχουν προταθεί λίγα πρωτόκολλα, από τα οποία τα περισσότερα βρίσκονται σε πειραματικό στάδιο. Το BB84 όμως είναι το σημαντικότερο εξ’ αυτών.

Πρωτόκολλο BB84

Το BB84 αποτέλεσε ιστορικά το πρώτο κβαντικό πρωτόκολλο για τη μυστική διανομή κλειδιού (QKD), το οποίο έγινε γνωστό το 1984 από τους Charles Bennet και Gilles Brassard, στους οποίους οφείλεται και το όνομά του. Χρησιμοποιήθηκε πειραματικά για διάδοση έως 30 km μέσω καλωδίου οπτικής ίνας και στον κενό χώρο για απόσταση πάνω από 100 μέτρα, ενώ αναμένεται να είναι εκτελέσιμο για αποστάσεις τουλάχιστον 100 km.

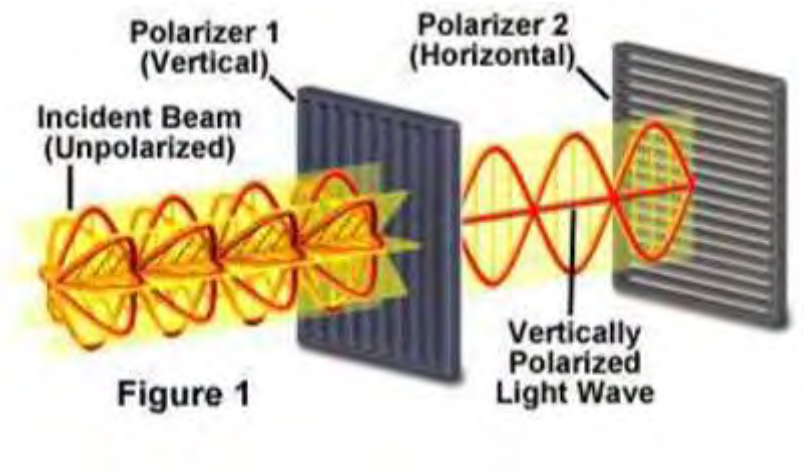
Στο πρωτόκολλο αυτό, το κβαντικό σύστημα που κωδικοποιεί τα bits είναι το πολωμένο φωτόνιο. Πιο συγκεκριμένα, τα φωτόνια όταν εκπέμπονται από μία πηγή φωτός πάλλονται τυχαία προς όλες τις κατευθύνσεις (unpolarized light). Αν και σωματίδια, όταν βρίσκονται σε κίνηση θεωρούνται ηλεκτρομαγνητικά κύματα με ηλεκτρικό και μαγνητικό πεδίο κάθετα μεταξύ τους αλλά και ως προς τη διεύθυνση διάδοσης.



Εικόνα 20: Ηλεκτρομαγνητικό κύμα φωτονίου

Πηγή: http://quantumgazette.blogspot.com/2016/09/the-bb84-protocol-for-quantum-key.html

Όταν, λοιπόν, περάσουν από έναν πολωτή (φίλτρο πόλωσης), η έξοδος είναι πολωμένη ανάλογα με το είδος πόλωσης που καθορίζει ο πολωτής π.χ. φωτόνια κάθετα ως προς το φίλτρο πόλωσης δε βγαίνουν στην έξοδό του.

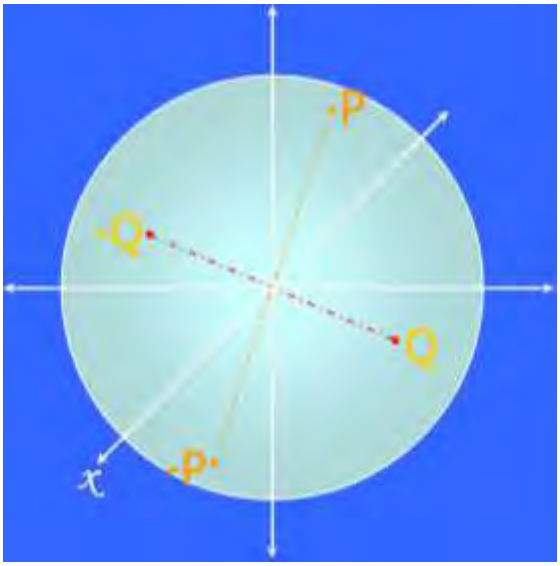


Εικόνα 21: Πόλωση φωτονίων

Πηγή: http://ikee.lib.auth.gr/record/291310/files/diplomatiki.pdf

Η πόλωση καθορίζεται, ουσιαστικά, από τη συμπεριφορά του διανύσματος του ηλεκτρικού πεδίου και μπορεί να χρησιμοποιηθεί για την κωδικοποίηση των bits. Συνήθως, είναι γραμμική ή κυκλική. Όταν το ηλεκτρικό πεδίο περιστρέφεται με κάποια συχνότητα, τότε ισχύει η κυκλική πόλωση, ενώ όταν το ηλεκτρικό πεδίο παραμένει στο ίδιο επίπεδο ισχύει η γραμμική.

Μία γραμμική πόλωση είναι πάντα παράλληλη σε μία σταθερή γραμμή, π.χ. ευθύγραμμες ή διαγώνιες πολώσεις, ενώ μία κυκλική πόλωση σχηματίζει έναν κύκλο γύρο από τον άξονα κίνησης. Οι άξονες x, y και z στο ακόλουθο σχήμα αντιπροσωπεύουν την ευθύγραμμη, διαγώνια και κυκλική πόλωση αντίστοιχα και κάθε σημείο της επιφάνειας της μοναδιαίας αυτής σφαίρας αντιπροσωπεύει μία κατάσταση πόλωσης ενός φωτονίου.

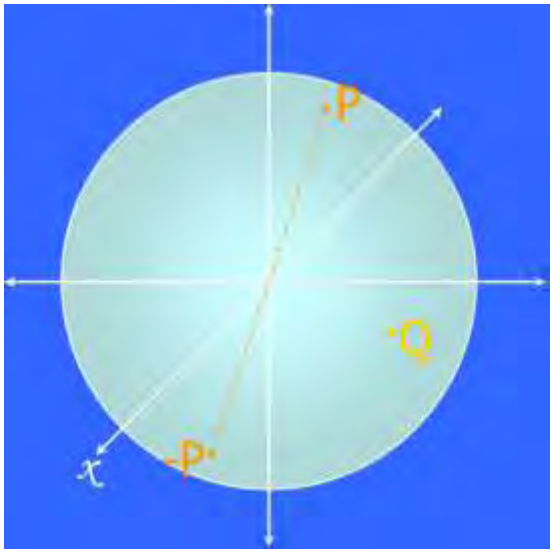


Εικόνα 22: Q, -Q, P, -P: Καταστάσεις πόλωσης φωτονίου

x,y,z: Ευθύγραμμη, διαγώνια και κυκλική πόλωση

Πηγή: http://ikee.lib.auth.gr/record/291310/files/diplomatiki.pdf

Σημεία τα οποία είναι συμμετρικά ως προς τη διάμετρο αποτελούν μία βάση, π.χ. {P,-P} και {Q,-Q}. Οποιεσδήποτε βάσεις απέχουν 90° ονομάζονται συζυγείς βάσεις. Για 2 συζυγείς βάσεις, λοιπόν, εάν ένα φωτόνιο είναι πολωμένο ως προς τη μία, η μέτρησή του ως προς την άλλη δε δίνει καμία πληροφορία.



Εικόνα 23: Q: Κατάσταση πόλωσης φωτονίου

P, -P: Βάση πόλωσης

Πηγή: http://ikee.lib.auth.gr/record/291310/files/diplomatiki.pdf

Έστω, για παράδειγμα, ένα φωτόνιο στην κατάσταση Q, ως προς τη βάση {P,-P}, όπου α η γωνία μεταξύ P και Q.

Συμπεριφέρεται σαν P με πιθανότητα: $cos^2\left(\frac{a}{2}\right) = \frac{1+\cos a}{2}$ και σαν –P με πιθανότητα: $sin^2\left(\frac{a}{2}\right) = \frac{1-\cos a}{2}$

Ακόμη: Prob(P) + Prob(-P) = 1

Εάν α είναι 90° ή 270°, Prob(P) = Prob(-P) = 0.5

Εάν α είναι 0° ή 180°, Prob(P) = 1

Γίνεται χρήση, επομένως, δύο διαφορετικών ορθογώνιων βάσεων. Η μία είναι π.χ. η κυκλική βάση πόλωσης, στην οποία περιλαμβάνονται τα διανύσματα για τη δεξιά και για την αριστερή κυκλική κατάσταση πόλωσης, ενώ η άλλη η γραμμική κατάσταση πόλωσης, στην οποία περιλαμβάνονται τα διανύσματα για την κάθετη και για την οριζόντια γραμμική κατάσταση πόλωσης αντίστοιχα.

Το πρωτόκολλο κάνει χρήση, συνεπώς, δύο οποιωνδήποτε μη συμβατών ορθογώνιων κβαντικών αλφάβητων του χώρου Hillbert. Στη συγκεκριμένη περίπτωση, το κβαντικό αλφάβητο κυκλικής πόλωσης:

Symbol	Bit
$\|\curvearrowright\rangle$	$\|1\rangle$
$\|\curvearrowleft\rangle$	$\|0\rangle$

και το κβαντικό αλφάβητο γραμμικής πόλωσης:

Symbol	Bit
$\|\updownarrow\rangle$	$\|1\rangle$
$\|\leftrightarrow\rangle$	$\|0\rangle$

Οι Bennett και Brassard διαπίστωσαν ότι, εάν ο αποστολέας χρησιμοποιούσε ένα συγκεκριμένο ορθογώνιο κβαντικό αλφάβητο, η παρεμβολή ενός ωτακουστή δε θα γινόταν αντιληπτή. Θα μπορούσε να υποκλέπτει, δηλαδή, τις εκπομπές του αποστολέα με ακρίβεια 100% και στη συνέχεια να τον μιμείται, ξαναεκπέμποντας τις μετρήσεις του στον παραλήπτη. Αν, για παράδειγμα, ο αποστολέας χρησιμοποιούσε μόνο το πρώτο ορθογώνιο κβαντικό αλφάβητο, τότε ο ωτακουστής θα μπορούσε να μετρήσει κάθε bit μετάδοσης του αποστολέα με μια συσκευή βασιζόμενη σε κάποιο χειρισμό μέτρησης κυκλικής πόλωσης. Αντίστοιχα, εάν γινόταν χρήση μόνο του δεύτερου ορθογώνιου γραμμικού αλφάβητου, τότε ο ωτακουστής θα μπορούσε να μετρήσει κάθε bit μετάδοσης με μια συσκευή βασιζόμενη σε κάποιο χειρισμό μέτρησης γραμμικής πόλωσης. Η συγκεκριμένη στρατηγική υποκλοπής ονομάζεται αδιαφανής παρεμβολή.

Για να σιγουρευτούν ότι η παρεμβολή αυτή θα είναι ανιχνεύσιμη, οι Bennett και Brassard πραγματοποιούν την επικοινωνία σε δύο στάδια. Το πρώτο μέσω ενός κβαντικού καναλιού μιας διαδρομής, με σκοπό να δημιουργηθεί και να μοιραστεί το μυστικό κλειδί και το δεύτερο μέσω ενός δημοσίου συμβατικού καναλιού αμφίδρομης κατεύθυνσης, μέσω του οποίου θα μεταδοθούν οι κρυπτογραφημένες πληροφορίες που επιθυμούν τα μέλη της επικοινωνίας να ανταλλάξουν στη συνέχεια.

Στο πρώτο στάδιο, ο αποστολέας, κάθε φορά που αποστέλλει ένα τυχαίο bit, χρησιμοποιεί τυχαία και με ίση πιθανότητα ένα από τα δύο αλφάβητα. Το γεγονός ότι είναι τυχαίο το μήνυμα εξασφαλίζει και τη μοναδικότητα του μυστικού κλειδιού.

Ο παραλήπτης, από την άλλη, για κάθε μία κατάσταση επιλέγει, και πάλι, τυχαία και με ίση πιθανότητα μεταξύ των δύο αλφάβητων για να υπολογίσει την πολικότητα του κάθε φωτονίου. Για κάθε φωτόνιο σημειώνει τη μέτρηση καθώς και το αλφάβητο που χρησιμοποίησε. Από τη στιγμή που δεν υπάρχει χειρισμός μέτρησης και των δύο αλφάβητων ταυτοχρόνως, προκύπτει, σύμφωνα με την αρχή της απροσδιοριστίας του Χάιζενμπεργκ, ότι κανείς δεν μπορεί να λάβει την εκπομπή του αποστολέα με ακρίβεια μεγαλύτερη του 75%.

Αναλυτικότερα, για κάθε bit που μεταδίδεται από τον αποστολέα, κάποιος μπορεί να επιλέξει ένα χειρισμό μέτρησης συμβατό με το πρώτο αλφάβητο ή με το δεύτερο, όχι όμως και με τα δύο συγχρόνως. Επομένως, κάποιος μπορεί να γνωρίζει την επιλογή του κβαντικού αλφάβητου μόνο με πιθανότητα 50% τη φορά. Αν κάποιος επιλέξει στην τύχη κβαντικό αλφάβητο συμβατό με αυτό του αποστολέα, τότε το bit μετάδοσης θα λαμβάνεται σωστά με πιθανότητα 1. Στην αντίθετη περίπτωση, το bit μετάδοσης θα λαμβάνεται σωστά με πιθανότητα ½. Επομένως, η πιθανότητα κάποιος να λάβει σωστά το bit μετάδοσης είναι:

$$P = \frac{1}{2}1 + \frac{1}{2}\frac{1}{2} = \frac{3}{4}$$

Συνολικά, λοιπόν, ο παραλήπτης θα έχει ένα μέσο όρο ρυθμού λάθους (error rate) 25% στα bits που λαμβάνει (Antoniades et al. 2005). Αυτός ο ρυθμός λάθους είναι μεγάλος αλλά διορθώνεται στη συνέχεια.

Έστω ότι για κάθε bit που εκπέμπεται, ο ωτακουστής είτε κάνει αδιαφανής παρεμβολή με πιθανότητα λ, όπου $0 \leq \lambda \leq 1$, είτε δεν κάνει παρεμβολή με πιθανότητα 1 - λ. Άρα, όταν $\lambda = 1$ κάνει παρεμβολή σε κάθε bit μετάδοσης, ενώ όταν $\lambda = 0$ δεν κάνει καθόλου παρεμβολή.

Στην περίπτωση της αδιαφανούς παρεμβολής, θα έχει μια πιθανότητα 50% να στείλει την ίδια κατάσταση με την αρχική, χωρίς να αποκαλυφθεί η παρέμβασή του. Παρ'όλα αυτά, στο υπόλοιπο 50% των περιπτώσεων θα επιλέξει μια αντίθετη βάση και κατά συνέπεια θα προσθεθεί ένα λάθος 25% στην τελική ακολουθία που λαμβάνεται από τον παραλήπτη ακόμα και αφού συγκρίνουν τα δύο μέλη τις βάσεις. Ο αποστολέας και

ο παραλήπτης, επομένως, μπορούν να καταλάβουν αν κάποιος τους παρακολουθούσε αλλά και το ποσοστό της πληροφορίας που παραβιάστηκε.

Στο δεύτερο στάδιο, αρχικά, ο στόχος είναι να διαγραφούν τα bits, στα οποία θα μπορούσε να έχει συμβεί λάθος χωρίς την παρεμβολή κάποιου ωτακουστή. Κάποια λάθη, για παράδειγμα, οφείλονται στην αλληλεπίδραση του συστήματος κωδικοποίησης με το περιβάλλον. Επειδή δεν είναι δυνατόν να διαχωριστεί αυτός ο θόρυβος από την πραγματική υποκλοπή, η μόνη ασφαλής λύση είναι να θεωρηθεί ότι όλα τα λάθη οφείλονται στον ωτακουστή.

Έτσι, ο παραλήπτης μεταδίδει δημόσια τους χειρισμούς μέτρησης που χρησιμοποίησε για κάθε ένα από τα bit που έλαβε χωρίς να κάνει γνωστή την ίδια τη μέτρηση και στη συνέχεια, ο αποστολέας μεταδίδει δημόσια, και πάλι, στον παραλήπτη ποιες επιλογές χειρισμών μέτρησης που αυτός έκανε ήταν σωστές. Μετά από αυτήν τη συνδιαλλαγή (reconciliation), διαγράφουν και οι δύο τα bits που αντιστοιχούν στις μη συμβατές επιλογές μέτρησης και με αυτόν τον τρόπο προκύπτει μια κατά 50% μειωμένη ακολουθία τυχαίων bits, το ακατέργαστο κλειδί. Εάν δεν υπήρξαν σφάλματα ή παρεμβολή, τότε τα ακατέργαστα κλειδιά θα ταυτίζονται απόλυτα. Στην αντίθετη περίπτωση, που είναι και η πιο ρεαλιστική, η αντιστοιχία των bits των ακατέργαστων κλειδιών δε θα συμφωνεί με πιθανότητα:

$$0\ (1\text{-}\lambda) + \frac{1}{4}\lambda = \frac{\lambda}{4}$$

Στη συνέχεια, τα μέλη χρησιμοποιούν το κοινόχρηστο κανάλι για να υπολογίσουν ένα ρυθμό λάθους R στο ακατέργαστο κλειδί. Συμφωνούν δημόσια σε ένα τυχαίο δείγμα του ακατέργαστου κλειδιού και συγκρίνουν δημόσια τα bits αυτά, τα οποία, στη συνέχεια, επειδή έχουν αποκαλυφθεί αφαιρούνται από το ακατέργαστο κλειδί. Εάν το R περάσει ένα συγκεκριμένο ανώτατο όριο R_{max}, που έχει προσυμφωνηθεί, τότε θα είναι αδύνατο τα δύο μέλη να έρθουν σε συμφωνία για το κρυφό κλειδί. Έτσι, επανέρχονται στο πρώτο στάδιο και ξεκινούν από την αρχή. Αν η εκτίμηση λάθους R δεν υπερβεί το R_{max}, τότε συνεχίζουν στη διαδικασία διόρθωσης σφαλμάτων (error correction) από το υπόλειμμα του ακατέργαστου κλειδιού, έτσι ώστε να προκύψει ένα κοινό κλειδί χωρίς λάθη, το κλειδί συνδιαλλαγής.

Αρχικά, αποφασίζουν δημόσια μια τυχαία μετάθεση που θα πραγματοποιήσουν στα εναπομείναντα ακατέργαστα κλειδιά τους. Έπειτα, διαιρούν το ακατέργαστο αυτό

κλειδί σε μπλοκ συγκεκριμένου μήκους. Το μήκος αυτό επιλέγεται έτσι ώστε να μην είναι δυνατό σε μπλοκ τέτοιου μήκους να βρεθούν παραπάνω από ένα λάθη. Για κάθε ένα από αυτά τα μπλοκ, ο αποστολέας και ο παραλήπτης συγκρίνουν δημόσια την ολική ισοτιμία ελέγχου και διαγράφουν κάθε φορά το τελευταίο του bit. Κάθε φορά που η ολική ισοτιμία ελέγχου δε συμφωνεί, τα δύο μέλη ξεκινούν ένα δυαδικό έλεγχο για να προσδιορίσουν το λάθος, π.χ. διαιρώντας το μπλοκ σε δύο υπομπλοκ, έπειτα συγκρίνουν δημόσια τις ισοτιμίες αυτών των υπομπλοκ διαγράφωντας το δεξί bit σε κάθε υπομπλοκ. Αυτού του είδους ο έλεγχος με διαίρεση στα δύο συνεχίζεται σε κάθε υπομπλοκ όπου οι ισοτιμίες δε βρίσκονται σε συμφωνία. Όταν όλα τα εσφαλμένα bit εντοπισθούν και διαγραφούν, τότε συνεχίζουν στο επόμενο μπλοκ. Η συγκεκριμένη διαδικασία επαναλαμβάνεται έως ότου δεν είναι πλέον αποτελεσματική.

Στη συνέχεια, τα δύο μέλη κάνουν χρήση μιας πιο ακριβούς διαδικασίας συνδιαλλαγής. Επιλέγουν δημόσια τυχαία δείγματα από το υπόλειμμα του ακατέργαστου κλειδιού, συγκρίνουν δημόσια τις ισοτιμίες διαγράφοντας κάθε φορά το ίδιο και οι δύο bit. Αν μια ισοτιμία δε συμφωνεί, τότε χρησιμοποιείται ο δυαδικός έλεγχος, και πάλι, ώστε να προσδιορίσουν και να διαγράψουν το λάθος.

Τελικά, όταν μετά από έναν προκαθορισμένο αριθμό από συνεχείς επαναλήψεις αυτού του βήματος δεν εντοπισθεί κανένα λάθος, τότε τα μέλη υποθέτουν με πολύ μεγάλη πιθανότητα ότι το εναπομείναν ακατέργαστο κλειδί, κλειδί συνδιαλλαγής πλέον, είναι χωρίς λάθη και συνεχίζουν στην επόμενη και τελευταία φάση της επικοινωνίας τους.

Σε αυτήν τη φάση υπάρχουν πολλές διαδικασίες, ωστόσο επιλέχθηκε να περιγραφεί μια απλή αν και πλέον υπάρχουν πολύ πιο αποδοτικές διαδικασίες.

Στην τελική, λοιπόν, φάση του δεύτερου σταδίου, τα μέλη γνωρίζουν ότι το κοινό κλειδί συνδιαλλαγής τους είναι μόνο μερικώς κρυφό. Απομένει να κάνουν ενίσχυση της μυστικότητας (privacy amplification) που είναι η εξαγωγή του κρυφού κλειδιού από το μερικώς κρυφό κλειδί. Εκμεταλλευόμενοι την εκτίμηση του ρυθμού λάθους, ο αποστολέας και ο παραλήπτης θέτουν ένα άνω όριο k του αριθμού των bits που είναι δυνατό να γνωρίζει ο ωτακουστής, φυσικά μικρότερο του αριθμού των bits του κλειδιού συνδιαλλαγής. Ακόμη, καθορίζουν αυθαίρετα μια παράμετρο ασφάλειας έστω s και επιλέγουν δημόσια τυχαία n-k-s δείγματα του κλειδιού συνδιαλλαγής, χωρίς να κάνουν γνωστό ούτε το περιεχόμενό τους ούτε τις ισοτιμίες τους. Οι ισοτιμίες που

δεν έχουν αποκαλυφθεί συγκροτούν το τελικό κρυφό κλειδί, ενώ η μέση πληροφορία που γνωρίζει ο ωτακουστής για το κλειδί αυτό είναι λιγότερη από $2^{-s}/\ln 2$ bits.

Πρωτόκολλο EPR (Ekert's Protocol)

Το 1991, ο Artur Ekert, επηρεασμένος από το EPR παράδοξο, επινόησε το EPR πρωτόκολλο βασισμένο σε ιδιότητες κβαντικά συσχετισμένων σωματιδίων. Όπως και το πρωτόκολλο BB84, χωρίζεται σε δύο στάδια επικοινωνίας. Το πρώτο στάδιο πραγματοποιείται μέσω ενός κβαντικού καναλιού και το δεύτερο μέσω ενός κοινόχρηστου καναλιού.

Στο πρώτο στάδιο, για κάθε χρονικό διάστημα, η κατάσταση, έστω $|\Omega_j\rangle$, διαλέγεται τυχαία, με ίση πιθανότητα από μια ομάδα τριών καταστάσεων, έστω $\{|\Omega_0\rangle, |\Omega_1\rangle, |\Omega_2\rangle\}$, και ένα EPR ζευγάρι, συνήθως φωτονίων, δημιουργείται στην επιλεγμένη αυτή κατάσταση. Το ένα φωτόνιο από το προκύπτον αυτό ζεύγος αποστέλλεται στο ένα μέλος της επικοινωνίας και το άλλο φωτόνιο στο άλλο μέλος.

Ως πιθανές καταστάσεις πόλωσης επιλέγονται, για παράδειγμα, οι ακόλουθες:

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\frac{3\pi}{6}\right\rangle_2 - \left|\frac{3\pi}{6}\right\rangle_1 |0\rangle_2\right)$$

$$|\Omega_1\rangle = \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}\rangle_1 \left|\frac{4\pi}{6}\right\rangle_2 - \left|\frac{4\pi}{6}\right\rangle_1 |\frac{\pi}{6}\rangle_2\right) \text{ και}$$

$$|\Omega_2\rangle = \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}\rangle_1 \left|\frac{5\pi}{6}\right\rangle_2 - \left|\frac{5\pi}{6}\right\rangle_1 |\frac{2\pi}{6}\rangle_2\right)$$

Για κάθε μία από αυτές τις καταστάσεις διαλέγονται, επομένως, τα ακόλουθα αντίστοιχα μη ορθογώνια αλφάβητα:

Symbol	Bit
$\|0\rangle$	0
$\left\|\frac{3\pi}{6}\right\rangle$	1

Symbol	Bit
$\|\frac{\pi}{6}\rangle$	0

$\lvert\frac{4\pi}{6}\rangle$	1

Symbol	Bit
$\lvert\frac{2\pi}{6}\rangle$	0
$\lvert\frac{5\pi}{6}\rangle$	1

Τα δύο μέλη της επικοινωνίας, τυχαία, ισοπίθανα, ξεχωριστά και ανεξάρτητα, επιλέγουν έναν από τρεις χειρισμούς μέτρησης, έστω M0, M1 και M2, και σύμφωνα με αυτούς μετρούν τα αντίστοιχα φωτόνιά τους. Ο αποστολέας καταγράφει το bit που μέτρησε. Από την άλλη, ο παραλήπτης καταγράφει την κατάσταση που σχετίζεται με το bit που μέτρησε. Η διαδικασία επαναλαμβάνεται για όσα χρονικά διαστήματα χρειαστεί.

Ένα παράδειγμα μιας τέτοιας κατάστασης διεμπλοκής είναι το εξής:

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\frac{\pi}{2}\right\rangle_2 - \left|\frac{\pi}{2}\right\rangle_1 |0\rangle_2\right)$$

Εύκολα γίνεται αντιληπτό, λοιπόν, ότι αν ένα φωτόνιο μετρηθεί και διαπιστωθεί ότι βρίσκεται σε κατάσταση κάθετης γραμμικής πόλωσης |0⟩, το άλλο όταν μετρηθεί θα εντοπισθεί σε κατάσταση οριζόντιας γραμμικής πόλωσης |π/2⟩ και αντιστρόφως.

Στο δεύτερο στάδιο, μετά την ολοκλήρωση των εκπομπών, τα δύο μέλη εξακολουθούν να επικοινωνούν μέσω κοινόχρηστου καναλιού για να προσδιορίσουν τα bit για τα οποία χρησιμοποίησαν τους ίδιους χειρισμούς μέτρησης.

Στη συνέχεια, ο καθένας τους χωρίζει τη δικιά του ακολουθία των bit σε δύο υποακολουθίες. Η μία υποακολουθία, η οποία λέγεται ακατέργαστο κλειδί, σχηματίζεται από τα bit για τα οποία χρησιμοποίησαν τους ίδιους χειρισμούς μέτρησης και αποτελεί το κοινό μυστικό τους κλειδί. Θα πρέπει να αναμένουν αντίθετα αποτελέσματα, όπως προαναφέρθηκε, καθώς η μία είναι συμπληρωματική της άλλης. Αν ο αποστολέας έχει, για παράδειγμα, την ακολουθία 00101, τότε ο παραλήπτης θα έχει την NOT 00101 = 11010. Μπορούν να καταλήξουν μέσω του κοινόχρηστου

καναλιού στην επιλογή μιας από τις δύο και ένας από τους δύο να αντιστρέψει το κλειδί του, ώστε να έχουν και οι δύο στη διάθεσή τους το μυστικό κλειδί.

Η άλλη υποακολουθία, που λέγεται απορριφθέν κλειδί, αποτελείται από όλα τα υπόλοιπα bit. Αντίθετα με το πρωτόκολλο BB84, το πρωτόκολλο EPR αντί να ¨πετάει¨ το απορριφθέν κλειδί, το χρησιμοποιεί για να ελέγξει για τυχόν παρουσία ενός τρίτου στην επικοινωνία. Ο αποστολέας και ο παραλήπτης μπορούν να μετρήσουν αυτά τα φωτόνια με μια τρίτη βάση και να συζητήσουν μέσω κοινόχρηστου καναλιού τα αποτελέσματά τους. Με τη βοήθεια αυτών εξετάζουν αν ικανοποιείται ή όχι η Ανεξαρτησία του Bell, η οποία δεν υφίσταται σε πεπλεγμένα σωματίδια. Εάν η ανισότητα ικανοποιείται, συνεπάγεται ότι τα φωτόνια δεν ήταν πραγματικά εμπλεγμένα και επομένως είναι δυνατόν να υπάρχει κάποιος τρίτος που επιχειρεί να υποκλέψει την επικοινωνία. Αν όχι, τότε δεν υπάρχει.

Για το πρωτόκολλο EPR, η ανισότητα του Bell μπορεί να περιγραφεί ως εξής:

Έστω $P(\neq \mid i,j)$ συμβολίζει την πιθανότητα δύο αντίστοιχα bits του αποστολέα και του παραλήπτη από τα απορριφθέντα κλειδιά να μην ταιριάζουν, δεδομένου ότι οι χειρισμοί μέτρησης που επιλέχθηκαν ήταν αντίστοιχα είτε Mi και Mj είτε Mj και Mi.

Έστω $P(= \mid i,j) = 1- P(\neq \mid i,j)$ και $\Delta(i,j) = P(\neq \mid i,j) - P(= \mid i,j)$.

Τέλος, έστω $\beta= 1 + \Delta(1,2) - |\Delta(0,1) – \Delta(0,2)|$.

Η ανισότητα του Bell ισοδυναμεί με τον τύπο $\beta\geq 0$. Επιπλέον, για την κβαντομηχανική ισχύει $\beta= - ½$, κάτι που συντελεί παραβίαση της ανισότητας.

Ο θόρυβος και οι υποκλοπές, όπως είναι ήδη γνωστό, αλλοιώνουν τις μετρήσεις και η σχέση μεταξύ των δύο ακολουθιών δε θα είναι μια ακριβής σχέση NOT. Όμως χάρη στην κβαντική διαπλοκή, ο αποστολέας έχει πιθανότητα μεγαλύτερη του 50% να εξάγει σωστά την ακολουθία του παραλήπτη και αντιστρόφως, πιθανότητα που είναι εξαιρετικά μεγαλύτερη από οποιαδήποτε άλλη κλασσική μέθοδος μπορεί να προσφέρει. Ακόμη, τεχνικές διαφόρων ειδών μπορούν να χρησιμοποιηθούν για την επαλήθευση των ακολουθιών, χωρίς να χρειαστεί να γνωστοποιηθούν αυτές καθ' εαυτές από το κοινόχρηστο κανάλι.

Η τελευταία φάση του πρωτοκόλλου EPR είναι η συνδιαλλαγή και είναι ίδια με αυτήν που περιγράφηκε στο πρωτόκολλο BB84.

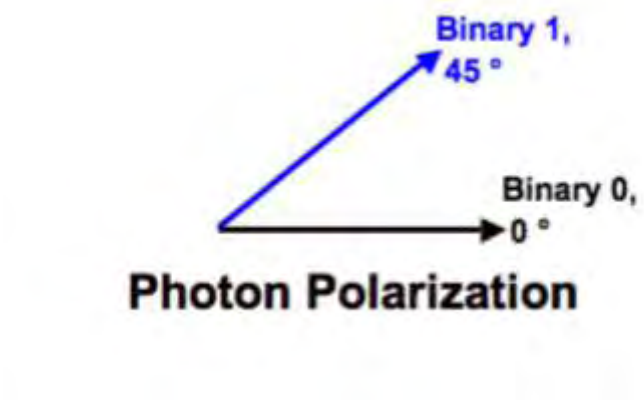
Αν, λοιπόν, η πηγή λειτουργεί αξιόπιστα, υποστηρίζεται πως το πρωτόκολλο αυτό είναι ισάξιο του BB84.

Πρωτόκολλο B92

Το 1992, ο Charles Bennett πρότεινε μια απλοποιημένη εκδοχή του BB84 στην εργασία του ¨Κβαντική κρυπτογραφία¨, το πρωτόκολλο B92. Η κύρια διαφορά στο B92 είναι ότι μόνο δύο καταστάσεις είναι αναγκαίες αντί για τις 4 πιθανές καταστάσεις πόλωσης στο BB84. Όπως το κβαντικό πρωτόκολλο BB84, έτσι και το B92 μπορεί να περιγραφεί με βάση ένα κβαντικό σύστημα που αντιπροσωπεύεται από ένα δισδιάστατο χώρο Hillbert, χρησιμοποιώντας, όμως, μη ορθογώνιες βάσεις.

Επιλέγονται, λοιπόν, ως μη ορθογώνιες βάσεις τα σύμβολα $|A\rangle$ και $|\bar{A}\rangle$, όπου αντιπροσωπεύουν αντίστοιχα την κατάσταση πόλωσης ενός φωτονίου γραμμικά πολωμένο σε μια γωνία α και σε μια γωνία –α ως προς την κατακόρυφο και ισχύει $0 < \alpha < \pi/4$.

Σύμφωνα με την εικόνα, το 0 μπορεί να κωδικοποιηθεί ως 0 μοίρες στην ορθογώνια βάση και το 1 μπορεί να κωδικοποιηθεί στις 45 μοίρες στη διαγώνια βάση.



Εικόνα 24: Πόλωση φωτονίων

Πηγή: https://apothesis.eap.gr/bitstream/repo/43544/1/Διπλωματική-Δριτσοπούλου%20Μαρία%20Χριστίνα%20-%20123548.pdf

Σε αντίθεση με το BB84 που προϋποθέτει δύο ορθογώνια κβαντικά αλφάβητα, το B92 χρειάζεται μόνο ένα μη ορθογώνιο κβαντικό αλφάβητο. Επιλέγεται, για παράδειγμα, το εξής μη ορθογώνιο κβαντικό αλφάβητο :

Symbol	Bit
$\|A\rangle$	1
$\|\bar{A}\rangle$	0

Όπως συμβαίνει και στα πρωτόκολλα BB84 και EPR, ο αποστολέας και ο παραλήπτης επικοινωνούν σε δύο στάδια, το πρώτο μέσω ενός κβαντικού καναλιού μιας διαδρομής και το δεύτερο μέσω ενός κοινόχρηστου καναλιού αμφίδρομης κατεύθυνσης.

Αρχικά, ο αποστολέας χρησιμοποιεί το κβαντικό αλφάβητο για να αποστείλει τη δυαδική ακολουθία στον παραλήπτη, χρησιμοποιώντας τυχαία και με ίση πιθανότητα “0” και “1”. Επειδή τα $|A\rangle$ και $|\bar{A}\rangle$ δεν είναι ορθογώνια, δεν υπάρχει κανένα πείραμα που να μπορεί να διακρίνει μεταξύ των δύο καταστάσεων πόλωσης, συνεπώς ο παραλήπτης μπορεί να διαλέξει μία, μεταξύ πολλών, στρατηγική μέτρησης. Με αυτόν τον τρόπο, είτε εξάγει ορθά το bit μετάδοσης του αποστολέα είτε προκύπτει ένα ασαφές αποτέλεσμα, π.χ. μια εξάλειψη που δηλώνεται ως “?”. Επίσης, θεωρείται ότι και ο παραλήπτης για κάθε bit που λαμβάνει επιλέγει τυχαία και με ίση πιθανότητα ανάμεσα σε δύο χειρισμούς.

Η δεύτερη φάση της επικοινωνίας του πρωτοκόλλου B92 είναι ακριβώς ίδια με αυτή του BB84, με τη μόνη διαφορά ότι ο παραλήπτης ενημερώνει δημόσια τον αποστολέα σε ποια χρονικά διαστήματα δεν προέκυψε εξάλειψη. Έτσι, τα bits που εντοπίζονται μέσα σε αυτά τα διαστήματα αποτελούν τα ακατέργαστα κλειδιά τους.

Η παρουσία ενός ωτακουστή διαπιστώνεται από έναν ασυνήθιστο ρυθμό λαθών στο ακατέργαστο κλειδί του παραλήπτη. Είναι, επίσης, πιθανό να ανιχνευτεί ο ωτακουστής από έναν ασυνήθιστο ρυθμό εξαλείψεων. Ωστόσο, ο Ekert τονίζει ότι ο ωτακουστής μπορεί να επιλέξει κάποιες στρατηγικές παρεμβολής που να μην έχουν καμία επιρροή στο ρυθμό εξαλείψεων, συνεπώς είναι δυνατό να ανιχνευθεί μόνο αν ο παραλήπτης δεχθεί ασυνήθιστο ρυθμό λαθών στο ακατέργαστο κλειδί του.

Κβαντική Γεννήτρια Τυχαίων Αριθμών

Τα τελευταία χρόνια, ο κόσμος έχει ¨απευθυνθεί¨ στους υπολογιστές για να ζητήσει υποστήριξη για όλες σχεδόν τις εργασίες. Οι υπολογιστές είναι ντετερμινιστικά μηχανήματα, συνεπώς κάθε φορά που τους γίνεται η ίδια ερώτηση, θα δίνουν την ίδια απάντηση. Έχουν κατασκευαστεί, επομένως, έχοντας ως στόχο την εξάλειψη της τυχαιότητας στα αποτελέσματά τους. Ταυτόχρονα, όμως, το γεγονός αυτό δημιουργεί σημαντικό πρόβλημα, καθώς σε πολλές διαδικασίες καθίσταται αναγκαία. Στον τομέα της κυβερνοασφάλειας, για παράδειγμα, κάθε είδους προσπάθεια θα ήταν ανώφελη και ανεπαρκής χωρίς τυχαίες τιμές. Πρόσφατα, ο κβαντικός υπολογιστής της Google κατόρθωσε να επιλύσει σε 3 λεπτά και 20 δευτερόλεπτα ένα πρόβλημα που ο ταχύτερος υπερυπολογιστής του κόσμου θα χρειαζόταν 10.000 χρόνια, 1,5 δισ. φορές ταχύτερα δηλαδή. Αν και είναι ακόμα πάρα πολύ νωρίς, οι ειδικοί της κυβερνοασφάλειας ήδη ανησυχούν για την ασφάλεια των συστημάτων μπροστά στα κβαντικά υπολογιστικά συστήματα και τους άπειρους υπολογισμούς που έχουν τη δυνατότητα να πραγματοποιούν σε ελάχιστα μόλις δευτερόλεπτα.

Με τον όρο τυχαιότητα χαρακτηρίζεται η έλλειψη τάξης και οργάνωσης και αυτή αυξάνεται όσο πιο μεγάλη είναι η εντροπία ενός συστήματος. Η τυχαιότητα στην οποία συναντάται οργάνωση και τάξη, ακόμα και αν αυτή είναι αμελητέα, ονομάζεται ψευδοτυχαιότητα. Οι υπολογιστές συνήθως παράγουν ψευδοτυχαίους αριθμούς μέσω μιας γεννήτριας τυχαίων αριθμών.

Στόχος μιας γεννήτριας τυχαίων αριθμών είναι το να παράγει γρήγορα και φθηνά πολλά ανεξάρτητα bits με ομοιόμορφη κατανομή πιθανότητας και χωρίς την παραμικρή σύνδεση μεταξύ τους. Με τον τρόπο αυτό, η γνώση μερικών δυαδικών ψηφίων δεν παρέχει καμία πληροφορία για τα υπόλοιπα. Οι ακολουθίες των ¨τυχαίων¨ αυτών αριθμών είναι αναγκαίες σε πλήθος εφαρμογών, π.χ. για να κατοχυρώνεται η ασφάλεια των κρυπτονομισμάτων κ.α.

Παρά την ονομασία τους, όμως, οι σημερινές γεννήτριες τυχαίων αριθμών εξαρτώνται κυρίως από αλγορίθμους υπολογιστών, γεγονός που τις καθιστά ντετερμινιστικές. Αυτό, συνεπώς, σημαίνει ότι η έξοδος που παράγουν καθορίζεται από την αρχική τους κατάσταση αλλά και τις εισόδους τους. Επομένως, με την ίδια είσοδο θα παράγεται πάντα η ίδια έξοδος. Αν και οι αριθμοί που προκύπτουν φαίνονται πραγματικά τυχαίοι,

η γνώση ορισμένων πληροφοριών για την είσοδο μπορεί να δώσει σε κάποιον το δικαίωμα πρόσβασης σε προστατευμένα δεδομένα που θεωρούνταν ασφαλή. Επίσης, υπάρχει το ενδεχόμενο όσοι έχουν συμβάλει στη δημιουργία του λογισμικού για μια τέτοια γεννήτρια, να έχουν κρατήσει αντίγραφό της, γεγονός που θα αποτελούσε απειλή. Στην πραγματικότητα, λοιπόν, στόχος είναι η δημιουργία μιας ακολουθίας δυαδικών, όχι απόλυτα τυχαίων ψηφίων, και στη συνέχεια, η επίδραση σε αυτή μιας συνάρτησης (hash function), με σκοπό να προκύψει ένα είδος ανακατέματος, ώστε να παραχθεί μια ¨τυχαία¨ σειρά από bits.

Όλα όμως τα ασφαλή κρυπτοσυστήματα, κλασικά και κβαντικά, έχουν την ανάγκη πραγματικά τυχαίων και απρόβλεπτων αριθμών. Από τις υπάρχουσες μεθόδους διακρίνονται αυτές που έχουν τη δυνατότητα να περάσουν στατιστικά τέστ τυχαιότητας, αχρηστεύονται όμως αν βρεθούν σε ¨λάθος¨ χέρια και άλλες που κάνουν χρήση σύμπλοκων ιόντων, αλλά έχουν την τάση να είναι πιο δαπανηρές τόσο όσον αφορά το χρόνο όσο και το κόστος.

Ακόμη και αν ακούγεται παράξενο, δεν είναι καθόλου εύκολο να παραχθεί πραγματική τυχαιότητα, μάλιστα οι επιστήμονες δε συμφωνούν ούτε στο αν υπάρχει. Ο Αϊνστάιν υποστήριζε ότι ο Θεός δεν παίζει ζάρια, καθώς ισχυριζόταν πως υπάρχει μια άγνωστη υποκείμενη τάξη σε όλα στο σύμπαν. Ο Στήβεν Χόκινγκ, από την άλλη πλευρά, δήλωνε ότι: «Ο Θεός παίζει ζάρια με το σύμπαν. Όλα τα αποδεικτικά στοιχεία δείχνουν ότι είναι ένας μανιώδης τζογαδόρος που ρίχνει τα ζάρια σε κάθε πιθανή περίσταση».

Λαμβάνοντας υπόψη, λοιπόν, ότι ούτε οι υπολογιστές αλλά ούτε και οι άνθρωποι μπορούν να παράξουν αυτή την τυχαιότητα, η αναζήτηση πρέπει να στραφεί προς τη φύση. Υπάρχουν φυσικές διαδικασίες που αγνοούν την τάξη, όπως η ραδιενεργή αποσύνθεση, η κίνηση ενός διπλού εκκρεμούς, η ακτινοβολία υποβάθρου κ.α. Οι διαδικασίες αυτές είναι υψηλής εντροπίας, κάτι που τις κάνει να θεωρούνται πραγματικά τυχαίες.

Πριν από μερικά χρόνια, Αμερικανοί και Ευρωπαίοι φυσικοί, εκμεταλλευόμενοι το φαινόμενο του κβαντικού εναγκαλισμού, κατόρθωσαν να κατασκευάσουν μια μηχανή που να παράγει αυθεντικά τυχαίους αριθμούς, φέρνοντας εις πέρας, έτσι, για πρώτη φορά, την τελευταία ¨εκκρεμότητα¨ στον τομέα της κρυπτογράφησης.

Το φαινόμενο αυτό, όπου ο Αϊνστάιν το είχε ονομάσει ¨στοιχειωμένη δράση από απόσταση¨, υποστήριζε την κρυπτογράφηση αλλά και την αποστολή μηνυμάτων σε μεγάλη απόσταση, όμως, δεν ήταν εφικτό να αξιοποιηθεί πρακτικά, καθώς η διαδικασία ήταν υπερβολικά χρονοβόρα, ενώ οι κρυπτογράφοι έχουν την ανάγκη αστραπιαίων ταχυτήτων.

Μια νέα, σχετικά, τεχνική κατόρθωσε να παράξει τυχαίους αριθμούς, κάνοντας χρήση φωτός από απομακρυσμένα άστρα και κβάζαρ που, θεωρητικά, δεν έχουν κάποιου είδους σύνδεση με τα πειράματα στη Γη.

Ένας ισχυρισμός, που επηρεάζει τα επονομαζόμενα πειράματα Bell που ελέγχουν την κβαντική φυσική, αναφέρεται σε μία πιθανή συσχέτιση μεταξύ των σωματιδίων που χρησιμοποιήθηκαν στα πειράματα και την υποθετικά τυχαία επιλογή των ρυθμίσεων του ανιχνευτή. Μια τέτοιου είδους σύνδεση θα είχε τη δυνατότητα να μεταβάλλει τα σωματίδια, έτσι ώστε η συμπεριφορά τους να παρουσιάζει κβάντωση όταν φθάνουν στον ανιχνευτή.

Προκειμένου να μην υπάρχει τέτοιο ζήτημα, οι ερευνητές, κάνοντας χρήση φωτός από άστρα του Γαλαξία μας, εξαφάνισαν κάθε τοπική συσχέτιση μεταξύ σωματιδίων και ανιχνευτών πηγαίνοντας 600 χρόνια πίσω. Τώρα, μάλιστα, έχουν προβεί σε βελτιώσεις, έτσι ώστε το σύστημα να ανταποκρίνεται ταχύτερα και με σώματα πολύ πιο απομακρυσμένα. Για πηγές τους διάλεξαν 50 άστρα και 12 κβάζαρ. Κάποια από τα κβάζαρ βρίσκονται δισεκατομμύρια έτη φωτός μακριά, γεγονός που, ενδεχομένως, σημαίνει ότι κάθε είδους συσχέτιση με κάποιο επίγειο ανιχνευτή θα έχει συμβεί κοντά στην αρχή του σύμπαντος. Το σύστημα διαλέγει bit σύμφωνα με το εάν ή όχι το μήκος κύματος ενός ανιχνευόμενου φωτονίου είναι μεγαλύτερο από 700 nm, παράγοντας τυχαία bits με ρυθμό υψηλό όσο 10^6 Hz χρησιμοποιώντας τα άστρα ή 10^3 Hz χρησιμοποιώντας τα κβάζαρ.

Επιπλέον, εφευρέθηκε σύστημα που εκμεταλλεύεται τις κβαντικές διακυμάνσεις του κενού, κατευθύνοντάς τες μέσω μιας δέσμης laser σε συσκευή που τις ανάγει σε αριθμούς.

Η δέσμη κατευθύνεται σε ένα διαχωριστή, προστατευμένο από εξωτερικές πηγές φωτός, ο οποίος τη διαχωρίζει. Οι δυο δέσμες που προκύπτουν καταλήγουν σε δύο ανιχνευτές, όπου και μετατρέπονται σε ηλεκτρονικά σήματα. Δίχως την επίδραση των κβαντικών διακυμάνσεων του κενού, οι δέσμες θα ήταν πανομοιότυπες. Με την αφαίρεση, όμως, του ενός σήματος από το άλλο καθώς και της ολικής αταξίας του συστήματος, κατορθώθηκε η απομάκρυνση του θορύβου που πηγάζει από το κενό και η αναγωγή του σε μια σειρά αυθεντικά τυχαίων αριθμών.

Η ταχύτητα της δέσμης φτάνει τα 6.5 Mbps και μπορεί να αναμετρηθεί με εκείνες των εμπορικά διαθέσιμων γεννητριών. Η αξία μιας τέτοιας συσκευής θα ήταν εφικτό να κατέβει μέχρι τα 100 ευρώ και τα τεχνικά χαρακτηριστικά της δίνουν τη δυνατότητα να αποτελέσει κομμάτι ενός προσωπικού υπολογιστή.

Μια άλλη μέθοδος, στην οποία η τυχαιότητα διασφαλίζεται από τους νόμους της κβαντικής μηχανικής, είναι η δημιουργία τσιπ, τα οποία βασίζονται στις κβαντικές ιδιοτήτων του φωτός, διαδικασία που, έτσι και αλλιώς, είναι απρόβλεπτη. Παρόλα αυτά, οφείλει κανείς να είναι ιδιαιτέρως προσεκτικός, ώστε να μην προσθέσει κάποιο μηχανισμό ή κάποιο εξάρτημα που να εμπεριέχει στοιχεία κλασσικής φυσικής.

Τα νέα αυτά τσιπ παράγουν ηλεκτρονικά σήματα και εν τέλει μια ακολουθία αυθεντικά τυχαίων αριθμών, οι οποίοι είναι εφικτό να χρησιμοποιηθούν ως ασφαλή κλειδιά κρυπτογράφησης, τα οποία δεν είναι δυνατό κανείς να προβλέψει, ανεξάρτητα από το πλήθος των δεδομένων που μπορεί να έχει στη διάθεσή του. Το ίδιο το τσιπ μπορεί να παραβιαστεί, αλλά μπορεί να ενταχθεί στο εσωτερικό ενός πιο πολύπλοκου συστήματος. Η βασική λειτουργία του, όμως, δεν μπορεί να παραβιαστεί.

Παράγουν εκατομμύρια bits ανά δευτερόλεπτο και διαθέτουν ικανοποιητική ταχύτητα για κρυπτογράφηση σε πραγματικό χρόνο δεδομένων επικοινωνιών, όπως σε τηλέφωνα ή βιντεοκλήσεις ή για την κρυπτογράφηση μεγάλων όγκων δεδομένων που κινούνται από ή προς εξυπηρετητές σαν αυτούς που συναντώνται στα μέσα κοινωνικής δικτύωσης. Έχουν αρκετά μικρό μέγεθος, ώστε να μπορούν να τοποθετηθούν στο εσωτερικό υπολογιστών, tablets, smartphones και να γίνει χρήση τους σε αρκετές εφαρμογές. Επίσης, θα μπορούσαν να χρησιμοποιηθούν σε περίπλοκες επιστημονικές εξομοιώσεις, όσον αφορά βιολογικές αλληλεπιδράσεις ή πυρηνικές αντιδράσεις. Άλλα

παραδείγματα είναι στα συνδεδεμένα αυτοκίνητα αλλά και στα δίκτυα με τις συσκευές που σχετίζονται με το ίντερνετ των πραγμάτων.

Η νέα αυτή συσκευή εξαφανίζει κάθε ανησυχία, καθώς παράγει αυθεντικά τυχαίους αριθμούς σε περιβάλλον πλήρους μυστικότητας. Στην κβαντομηχανική, οι ιδιότητες των πραγμάτων είναι από τη φύση τους ασαφείς. Η πιθανότητα μιας οποιαδήποτε ιδιότητας είναι εφικτό να εκτιμηθεί, αλλά μια σίγουρη τιμή παίρνει μόνο όταν πραγματοποιηθεί μέτρηση. Παρόλο που κατά το παρελθόν είχαν κατασκευαστεί και άλλες κβαντικές γεννήτριες τυχαίων αριθμών, είτε δεν ανταποκρίνονταν στον επιθυμητό χρόνο είτε το μέγεθος τους δεν ήταν χρηστικό. Επιπλέον, έχουν υλοποιηθεί και άλλες πειραματικές γεννήτριες που εύκολα κανείς τις βρίσκει και στο εμπόριο.

Σε λίγο καιρό τα τσιπ αυτά θα είναι διαθέσιμα στην αγορά, γεγονός που μεταφράζεται σε πολύ μεγαλύτερη αξιοπιστία όσον αφορά τα δισεκατομμύρια των συνδεδεμένων συσκευών τις οποίες χρησιμοποιούν όλοι καθημερινά. Τα δεδομένα όλων θα προφυλάσσονται. Επίσης, ο τομέας της άμυνας και της ασφάλειας θα λάβει ισχυρά οφέλη, όπως και τα δίκτυα ηλεκτρικής ενέργειας αλλά και μεταφοράς. Η επίτευξη αυτή συντελεί στην άφιξη μιας γενιάς πλήρως αδιάβλητων επικοινωνιών.

Η Ε.Ε., συγκεκριμένα, χρηματοδοτεί 20 ερευνητικές ομάδες που έχουν σκοπό να βγάλουν αυτή την τεχνολογία από το χώρο των εργαστηρίων και να τη διανείμουν στην αγορά, ενώ υλοποιούν και το επόμενο στάδιο, το κβαντικό ίντερνετ!

ΑΤΟΜΙΚΑ ΡΟΛΟΓΙΑ

Γενικά

Για αιώνες χρονόμετρο της ανθρωπότητας ήταν η Γη. Η μέρα χωριζόταν σε ώρες, λεπτά και δευτερόλεπτα με βάση την περιστροφή της. Μια πλήρης περιστροφή αντιστοιχεί σε μια μέρα, γι' αυτό και είχε ανατεθεί η ευθύνη της μέτρησης του χρόνου στα αστεροσκοπεία, όπως αυτό του Greenwich στην Αγγλία. Καθώς, όμως, τα ρολόγια γίνονταν όλο και πιο ακριβή, άρχισαν να φανερώνουν ότι ο πλανήτης μας ταλαντεύεται επάνω στον άξονά του καθώς περιστρέφεται, με αποτέλεσμα μερικές μέρες να είναι μικρότερες από άλλες.

Εξαιτίας αυτής της αστάθειας στο χρόνο περιστροφής της Γης, προστίθεται πλέον κάθε τόσο ένα δευτερόλεπτο στον Παγκόσμιο Χρόνο, για να βρίσκεται σε συμφωνία με το μέσο χρόνο του Γκρίνουιτς. Ακριβώς όπως προστίθεται κάθε 4 χρόνια μια μέρα στη διάρκεια του έτους, για να εξισορροπηθεί το γεγονός ότι η διάρκεια του έτους δεν είναι ακριβώς 365 μέρες.

Γενικά, κάθε ρολόι έχει ένα μετρητή που μετρά κάτι περιοδικό. Όσο πιο μικρή είναι η περίοδος αυτή, τόσο πιο ακριβές είναι και το ρολόι. Το μυστικό, δηλαδή, για να βελτιώσει κανείς την ακρίβεια ενός ρολογιού, είναι να αυξήσει τη συχνότητα των χτύπων του. Για το λόγο αυτό, τις δεκαετίες του 1940 και του 1950, το ρόλο του χρονόμετρου από τα ηλιακά ρολόγια με περίοδο μιας μέρας, αρχικά, πήραν τα εκκρεμή που είχαν περίοδο ενός δευτερολέπτου, στη συνέχεια, τα ρολόγια χαλαζία με 10.000 ταλαντώσεις το δευτερόλεπτο και τέλος, τα ατομικά ρολόγια, τα οποία χρησιμοποιούνται έως σήμερα.

Ατομικό ρολόι ονομάζεται το εργαλείο μέτρησης χρόνου που προσφέρει την υψηλότερη, μέχρι σήμερα, διαθέσιμη ακρίβεια μέτρησης. Τα ατομικά ρολόγια είναι οι πρώτες κβαντικές συσκευές μέτρησης που βρίσκουν ευρεία χρήση. Χρησιμοποιούνται ως πρωτογενή πρότυπα για τον καθορισμό της Συντονισμένης Παγκόσμιας Ώρας και το συγχρονισμό ρολογιών σε εθνικό και παγκόσμιο επίπεδο, τον έλεγχο συχνότητας τηλεοπτικών σταθμών, τη λειτουργία συστημάτων GPS (Global Positioning System), κ.α. Για τον καθορισμό της Συντονισμένης Παγκόσμιας Ώρας, συγκεκριμένα,

χρησιμοποιείται ένα παγκόσμιο δίκτυο από περίπου 250 ατομικά ρολόγια που βρίσκονται σε πάνω από 50 εθνικά εργαστήρια.

Τα ατομικά ρολόγια ονομάζονται έτσι διότι η αρχή λειτουργίας τους βασίζεται στη συμπεριφορά των ατόμων ενός στοιχείου. Τα άτομα, όπως και τα μόρια, εκπέμπουν και απορροφούν ηλεκτρομαγνητική ακτινοβολία σε κάποιες σταθερές συχνότητες, οι οποίες εξαρτώνται από τη δομή τους. Η συχνότητα της ακτινοβολίας αυτής μετριέται σε Hertz. Τα ατομικά ρολόγια, επομένως, αποτελούνται, κυρίως, από ένα σύστημα παραγωγής μιας σταθερής ατομικής συχνότητας και από μια ηλεκτρονική διάταξη για τη μέτρηση των αντίστοιχων ταλαντώσεων.

Στην καρδιά κάθε ατομικού ρολογιού, για την ακρίβεια, βρίσκεται ένα νέφος ατόμων, συνήθως καισίου ή ρουβιδίου, τα οποία εκτίθενται σε ακτινοβολία μικροκυμάτων, με συνέπεια να ταλαντώνονται, κερδίζοντας ή χάνοντας ενέργεια αντίστοιχα, αλλά πάντα σε διακριτές ποσότητες. Η συχνότητα αυτών των ταλαντώσεων, της μεταπήδησης δηλαδή από μια ενεργειακή κατάσταση σε άλλη, μπορεί να μετρηθεί με ακρίβεια και να χρησιμοποιηθεί για τον καθορισμό του χρόνου. Ο χρόνος ζωής ενός τέτοιου ρολογιού εξαρτάται από τα συστατικά του. Τα ατομικά ρολόγια που βασίζονται στις ταλαντώσεις ρουβιδίου, για παράδειγμα, έχουν διάρκεια ζωής 10 έτη, ενώ τα ατομικά ρολόγια καισίου 7 έτη.

Το πρώτο ατομικό ρολόι, βασισμένο σε ηλεκτρομαγνητική ακτινοβολία αμμωνίας, κατασκευάστηκε το 1949 στις Η.Π.Α. από το National Bureau of Standars (NBS), ενώ το 1955, βασιζόμενοι στο έργο του Ιζιντόρ Ράμπι του Πανεπιστημίου Κολούμπια και σε πρωτότυπα ρολόγια του αμερικανικού Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας του Μπόλντερ του Κολοράντο, ο Louis Essen και ο Jack Parry στο Εθνικό Εργαστήριο Φυσικής στο Middlesex σχεδίασαν και κατασκεύασαν το πρώτο αξιόπιστο ατομικό ρολόι. Το αποτέλεσμα ήταν ένα χρονόμετρο ακριβείας καισίου με καθυστέρηση ενός δευτερολέπτου ανά 300 χρόνια, γεγονός που καθιέρωσε νέα στάνταρτ για εκείνη την εποχή. Μετά από αυτή την ανακάλυψη, 400 ατομικά ρολόγια σε όλο τον κόσμο συντονίστηκαν σε ένα παγκόσμιο σύστημα μέτρησης εκατομμύρια φορές καλύτερο από το προηγούμενο, ενώ ένα χρόνο αργότερα (1956), το πρώτο εμπορικό ατομικό ρολόι, το Atomichron, αποκαλύφθηκε από την National Company, Inc of Malden, Massachusetts. Είχε ύψος περίπου 2 μέτρα, ζύγιζε 200 κιλά και κόστιζε 50.000 $.

Εικόνα 25: Atomichron
Πηγή:https://gr.dreamstime.com/%CE%B5%CE%BA%CE%B4%CE%BF%CF%84%CE%B9%CE%BA%CE%AE-%CF%86%CF%89%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF-%CF%8C%CE%B9-atomichron-image53075797

Το 1967, μετά από συνεχείς επιστημονικές έρευνες που είχαν αρχίσει το 1958, ο Έσσεν ανακάλυψε ότι το καίσιο ακτινοβολούσε στη χαρακτηριστική για αυτό συχνότητα των 9.192.631.770 Hertz. Η ιδιοσυχνότητα αυτή του καισίου χρησιμοποιήθηκε ως συχνότητα του νέου ατομικού ρολογιού καισίου, με βάση το οποίο ορίστηκε με ακρίβεια η βασική μονάδα μέτρησης του χρόνου, το χρονικό διάστημα του ενός δευτερολέπτου, από το Διεθνές σύστημα μονάδων. Ονομάστηκε ¨ατομικό δευτερόλεπτο¨ ή διεθνώς ¨S.I. second¨ (System International second).

Για να λειτουργήσει ένα τέτοιο ρολόι, αρχικά, θερμαίνονται τα άτομά του, ώστε να μετατραπούν απευθείας σε αέριο (εξάχνωση) και στη συνέχεια διαβιβάζονται σ' ένα σωλήνα υψηλού κενού.

Εικόνα 26: Σωλήνας υψηλού κενού
Πηγή:https://www.chemist.gr/%CF%81%CE%BF%CE%BB%CF%8C%CE%B3%CE%B9%CE%B1-%CF%83%CF%84%CF%81%CE%BF%CE%BD%CF%84%CE%AF%CE%BF%CF%85-87/

Τα άτομα αυτά, αρχικά, περνάνε από ένα μαγνητικό πεδίο, το οποίο επιλέγει εκείνα που βρίσκονται στην επιθυμητή ενεργειακή στάθμη. Στη συνέχεια, περνάνε από μια περιοχή, στην οποία επικρατεί μεγάλης έντασης πεδίο μικροκυμάτων. Η συχνότητα των μικροκυμάτων μεταβάλλεται σαρώνοντας μια περιοχή συχνοτήτων και ξανά από την αρχή, έτσι ώστε σε κάθε κύκλο της μεταβολής πετυχαίνει κάποια στιγμή ακριβώς τη συχνότητα των 9,192,631,770 Hertz. Όταν ένα άτομο καισίου απορροφά ενέργεια μορφής μικροκυμάτων που έχει ακριβώς την προαναφερόμενη συχνότητα, μεταπηδά σε συγκεκριμένη ανώτερη ενεργειακή στάθμη.

Στο άκρο του σωλήνα, ένα άλλο μαγνητικό πεδίο διαχωρίζει εκείνα τα άτομα που έχουν διεγερθεί από την απορρόφηση των μικροκυμάτων και βρίσκονται στην επιθυμητή ενεργειακή στάθμη. Ένας ανιχνευτής, επίσης στην άκρη του σωλήνα, δίνει μια ένδειξη ανάλογη με τον αριθμό των ατόμων καισίου που ανιχνεύει και συνεπώς η ένδειξή του κορυφώνεται όταν η συχνότητα των μικροκυμάτων είναι ακριβώς η σωστή. Η ένδειξη του ανιχνευτή χρησιμεύει για να γίνονται ελαφρές διορθώσεις που είναι αναγκαίες, ώστε η συχνότητα των μικροκυμάτων να έχει ακριβώς την τιμή που αναφέρθηκε.

Το καίσιο, παρόλα αυτά, δεν αποτελεί το στοιχείο με τη μεγαλύτερη ταχύτητα παλμών. Επελέγη μόνο και μόνο για λόγους ευκολίας. Άλλα άτομα είναι μέχρι και 100.000 φορές ταχύτερα και μπορούν να επιτύχουν ακόμη μεγαλύτερη ακρίβεια. Το πρόβλημα εντοπίζεται στο ότι δεν μπορούν να ανιχνευθούν με μικροκύματα αλλά μόνο με ακτίνες λέιζερ, οι οποίες πάλλονται σε πολύ ψηλές συχνότητες, σχεδόν ίδιες με αυτές του ορατού φωτός. Την εποχή της καθιέρωσης των ατομικών ρολογιών, η τεχνολογία των λέιζερ βρισκόταν ακόμη σε αρχικά στάδια. Αργότερα, προστέθηκε το πρόβλημα ότι το πλήθος των παλμών των λέιζερ είναι τόσο μεγάλο, περίπου ένα εκατομμύριο δισεκατομμύρια το δευτερόλεπτο, που δεν ήταν εφικτό να μετρηθεί επακριβώς. Το εμπόδιο αυτό ξεπεράστηκε το 1999 με την επινόηση από τον Τέοντορ Χενς του Ινστιτούτου Κβαντικής Οπτικής Μαξ Πλανκ της Γερμανίας της τεχνικής συνδυασμού συχνοτήτων, η οποία ¨κατεβάζει¨ τις οπτικές συχνότητες στις κλίμακες των μικροκυμάτων.

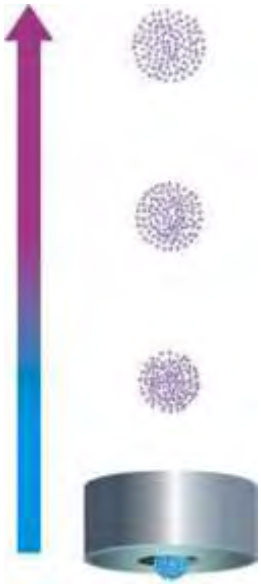
Τις επόμενες δεκαετίες, τα συστήματα ατομικού χρονισμού υπέστησαν μια σειρά επαναληπτικών βελτιώσεων και καινοτομιών, όλες με στόχο να κάνουν τα ρολόγια πιο ακριβή, σταθερά, συμπαγή και ανθεκτικά. Το δεύτερο μεγάλο άλμα πραγματοποιήθηκε το 1989, όταν ο φυσικός του Πανεπιστημίου Στάνφορντ Στίβεν Τσου και οι συνάδελφοί

του ανέπτυξαν το ¨ατομικό σιντριβάνι¨, μια τεχνική που βασίζεται σε μια σφαίρα εκατομμυρίων ατόμων καισίου, τα οποία ψύχονται σχεδόν στο απόλυτο μηδέν ανάμεσα σε ακτίνες λέιζερ.

Για να γίνει καλύτερα αντιληπτό, σε ένα ατομικό ρολόι συντριβάνι, αέριο ατόμων καισίου εισάγεται σ' ένα θάλαμο κενού. Δέσμες λέιζερ, σε ορθή γωνία η μια προς την άλλη, κατευθύνονται προς το κέντρο του θαλάμου. Τα λέιζερ σπρώχνουν ήρεμα τα άτομα του καισίου και τα παγιδεύουν ώστε να σχηματίσουν μια μικρή σφαίρα. Κατά τη διαδικασία του σχηματισμού της, τα λέιζερ επιβραδύνουν την κίνηση των ατόμων, με αποτέλεσμα να τα ψύχουν κοντά στο απόλυτο μηδέν.

Εικόνα 27: Δέσμες λέιζερ, σε ορθή γωνία η μια προς την άλλη, σπρώχνουν άτομα καισίου ώστε να σχηματίσουν μια σφαίρα
Πηγή:https://www.rizospastis.gr/story.do?id=308579&textCriteriaClause=%2B%CE%91%CE%A4%CE%9F%CE%9C%CE%99%CE%9A%CE%9F+%2B%CE%A1%CE%9F%CE%9B%CE%9F%CE%99

Δύο κατακόρυφα λέιζερ χρησιμοποιούνται για να σπρώξουν μαλακά τη σφαίρα προς τα επάνω και τότε όλα τα λέιζερ σβήνουν. Η δράση αυτή, παρόμοια με του σιντριβανιού, έδωσε και το όνομα στο είδος αυτό του ρολογιού. Η μικρή αυτή ώθηση έχει τη δυνατότητα να ανεβάσει τη σφαίρα σε ύψος περίπου ενός μέτρου, περνώντας τη μέσα από μια κοιλότητα μικροκυμάτων.



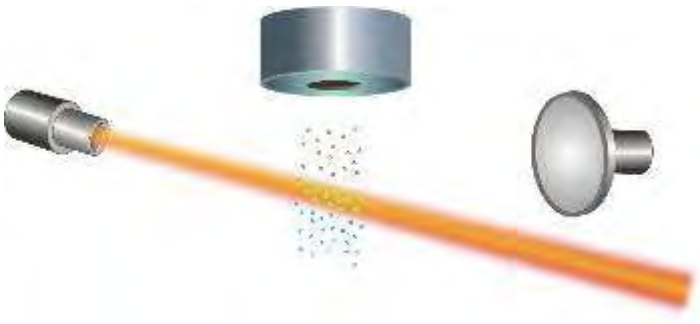
Εικόνα 28: Η σφαίρα καθώς ανεβαίνει περνά μέσα από μια κοιλότητα μικροκυμάτων

Πηγή: http://users.uoa.gr/~nektar/science/physics/atomic_clock.htm

Κάτω από την επίδραση της βαρύτητας, η σφαίρα πέφτει πάλι πίσω στην κοιλότητα των μικροκυμάτων. Το ταξίδι αυτό της σφαίρας (επάνω-κάτω) διαρκεί περίπου 1 δευτερόλεπτο. Κατά τη διάρκεια αυτή, οι καταστάσεις των ατόμων μπορεί ν' αλλάζουν ή και όχι, καθώς αλληλεπιδρούν τα άτομα με την ακτινοβολία μικροκυμάτων.

Εικόνα 29: Εξαιτίας της βαρύτητας, η σφαίρα πέφτει πάλι πίσω στην κοιλότητα των μικροκυμάτων
Πηγή: http://users.uoa.gr/~nektar/science/physics/atomic_clock.htm

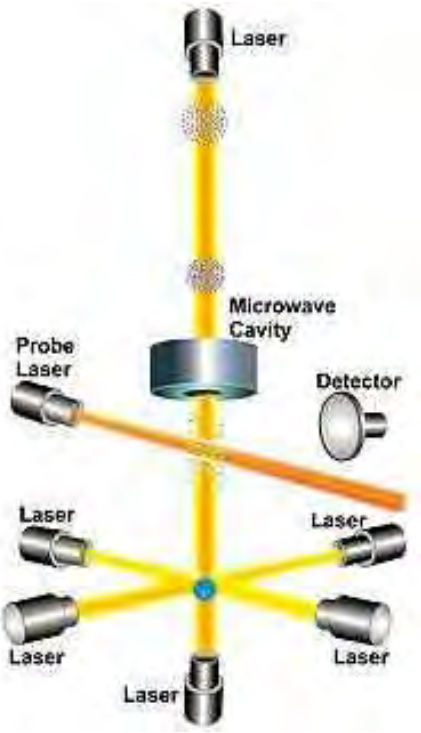
Όταν το ταξίδι τους τελειώνει, πέφτοντας προς τα κάτω, μια άλλη δέσμη λέιζερ κατευθύνεται προς τα άτομα. Τα άτομα εκείνα, των οποίων η ατομική κατάσταση άλλαξε κατά την αλληλεπίδραση με τα μικροκύματα, έχουν απορροφήσει ενέργεια δηλαδή, εκπέμπουν φως. Το φαινόμενο αυτό είναι γνωστό ως φθορισμός. Τα φωτόνια, δηλαδή τα μικροσκοπικά πακέτα φωτός που εκπέμπονται, μετρούνται από έναν ανιχνευτή.



Εικόνα 30: Τελαυταίο στάδιο της τεχνικής του ατομικού σιντριβανιού

Πηγή: http://users.uoa.gr/~nektar/science/physics/atomic_clock.htm

Η διαδικασία αυτή επαναλαμβάνεται αρκετές φορές, την ώρα που το σήμα μικροκυμάτων στην κοιλότητα σαρώνει διάφορες συχνότητες. Από όλες αυτές τις συχνότητες κάποια συντονίζεται με τα άτομα καισίου, αλλάζοντας τις καταστάσεις των περισσοτέρων εξ αυτών, μεγιστοποιώντας έτσι την ακτινοβολία που εκπέμπεται κατά το φθορισμό. Η συχνότητα αυτή είναι η φυσική συχνότητα συντονισμού του καισίου.



Εικόνα 31: Διαδικασία τεχνικής ατομικού σιντριβανιού

Πηγή: http://www.physics4u.gr/news/2004/scnews1289.html

Ο συνδυασμός της ψύξης με λέιζερ και του φαινομένου του σιντριβανιού επιτρέπει να παρατηρηθούν τα άτομα για μεγαλύτερη χρονική διάρκεια. Ο μεγαλύτερος χρόνος παρατήρησης δίνει τη δυνατότητα καλύτερου συντονισμού της δέσμης μικροκυμάτων, ώστε να απορροφηθεί από τα άτομα, γεγονός που οδηγεί σε μεγαλύτερη σταθερότητα και ακρίβεια του ρολογιού.

Τα παραδοσιακά ρολόγια καισίου χρησιμοποιούν άτομα σε θερμοκρασία δωματίου που κινούνται με αρκετές εκατοντάδες μέτρα ανά δευτερόλεπτο. Καθώς τα άτομα κινούνται με τέτοια ταχύτητα, ο χρόνος παρατήρησης περιορίζεται σε λίγα χιλιοστά του δευτερολέπτου. Τα ρολόγια με την ψύξη των λέιζερ ρίχνουν τη θερμοκρασία των ατόμων σε λίγα εκατομμυριοστά του βαθμού πάνω από το απόλυτο μηδέν κι έτσι η θερμική τους ταχύτητα αντιστοιχεί σε μερικά εκατοστά/δευτερόλεπτο. Τα ψυχρά άτομα ανεβαίνουν κατακόρυφα και περνάνε από την κοιλότητα μικροκυμάτων μια φορά κατά την άνοδο και μια κατά την κάθοδο. Το αποτέλεσμα είναι ο χρόνος παρατήρησης να επιμηκύνεται περίπου σε ένα δευτερόλεπτο, καθώς περιορίζεται μόνο από τη βαρύτητα που τραβάει τα άτομα προς το έδαφος.

Τα ατομικά ρολόγια, στο σύνολό τους, έδωσαν τη δυνατότητα να υπολογίζεται με μεγάλη ακρίβεια ο χρόνος χωρίς τη βοήθεια των αστρονομικών παρατηρήσεων. Η ακρίβεια του αστρονομικού χρόνου, μάλιστα, ο οποίος είναι ακόμα απαραίτητος για πρακτικούς σκοπούς, ελέγχεται πλέον με βάση τη συχνότητα της ατομικής ακτινοβολίας. Σε αντίθεση με τη συχνότητα ταλάντωσης του εκκρεμούς, η συχνότητα της ακτινοβολίας, που εκπέμπεται και απορροφάται όταν τα ηλεκτρόνια των ατόμων πάλλονται ανάμεσα σε δύο κοντινά ενεργειακά επίπεδα, όπως και όλες οι ατομικές ιδιότητες άλλωστε, είναι σταθερή παντού και πάντοτε.

Οπτικά Ατομικά Ρολόγια

Σήμερα, ο ακριβής συγχρονισμός στηρίζει μεγάλο μέρος της ζωής μας, καθώς υψηλής τεχνολογίας επιτεύγματα βασίζονται σε αυτόν. Καθημερινά, για να πραγματοποιήσουν τα δίκτυα μηχανών και συστημάτων που χρησιμοποιούν το διαδίκτυο αλλά και άλλες εκατομμύρια εφαρμογές που λειτουργούν αυτόματα, τις συντονισμένες ενέργειες που απαιτούνται, πρέπει να συμφωνούν με ακρίβεια στην ώρα. Τεχνολογίες που θεωρούνται δεδομένες, όπως τα κινητά τηλέφωνα και οι ψηφιακές τηλεοράσεις, εξαρτώνται από ατομικά ρολόγια. Η επικοινωνία στο πλαίσιο της οικονομίας της πληροφορίας βασίζεται σε τρεις πυλώνες: δίκτυα υπολογιστών, ραδιοτηλεοπτικές εκπομπές και τηλεπικοινωνίες. Όλα εξαρτώνται από ακριβή, συγχρονισμένο χρόνο σε ένα γεωγραφικά κατανεμημένο δίκτυο αλλά και από παγκόσμια δορυφορικά συστήματα πλοήγησης (GNSS). Μόνο οι συνηθισμένες επικοινωνίες και απευθείας ανταλλαγές εικόνων μέσα από τον παγκόσμιο ιστό απαιτούν μια ακρίβεια ενός εκατομμυριοστού του δευτερολέπτου μέσα σε ένα εικοσιτετράωρο. Για τα συστήματα προσδιορισμού θέσης (GPS), όπου κινούνται συνεχώς δορυφόροι και ανταλλάσσονται σήματα απαραίτητα για τον προσδιορισμό της θέσης, απαιτείται ακόμη πιο μεγάλη ακρίβεια, η οποία φθάνει το 1 δισεκατομμυριοστό του δευτερολέπτου για κάθε μέρα. Τα ατομικά ρολόγια είναι ο τρόπος με τον οποίο οι δορυφόροι κρατούν το χρόνο αλλά και το πιο καθιερωμένο είδος κβαντικής τεχνολογίας που χρησιμοποιείται από το 1967 για διεθνή χρονομέτρηση.

Μπορεί στην καθημερινότητα ένα δευτερόλεπτο πίσω ή μπροστά να μην έχει τόση μεγάλη σημασία, δεν ισχύει, όμως, το ίδιο στη σύγχρονη οικονομία και σε διάφορες

τεχνολογικές εφαρμογές. Χαρακτηριστικό παράδειγμα αποτελεί το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS), από το οποίο υπάρχει μια διεθνής υπερβολική εξάρτηση. Ένας δέκτης, πέρα από κατάλληλους τριγωνομετρικούς υπολογισμούς, απαιτεί την ακριβή γνώση του χρόνου που χρειάζεται για να φτάσουν σε αυτόν τα σήματα των δορυφόρων GPS**,** ώστε να είναι σε θέση να προσδιορίσει με ακρίβεια τη θέση του επί της Γης.

Ένα ατομικό ρολόι καισίου έχει τη δυνατότητα να είναι εξαιρετικά αξιόπιστο, καθώς χάνει μόνο ένα δευτερόλεπτο ανά 100 εκατομμύρια χρόνια, δεν έχει, όμως, τη δυνατότητα να διαιρέσει ένα δευτερόλεπτο παραπάνω από τη συχνότητα ταλάντωσής του, περιορίζοντας με αυτόν τον τρόπο την ακρίβεια στη μέτρηση του χρόνου. Καθώς αυτά τα ρολόγια προσκρούουν σε περιορισμούς ως προς την ακρίβειά τους, ήταν επιτακτική η ανάγκη για ένα σύστημα νέας γενιάς.

Σε μια ζήτηση της τελειότητας, επομένως, ερευνητές προσπάθησαν να κάνουν τη μέτρηση ακριβέστερη με τη βοήθεια οπτικών ατομικών ρολογιών (λειτουργούν με ορατό ή υπεριώδες φως). Η πρώτη μεγάλη ανακοίνωση έγινε το 2001 από το Αμερικανικό Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, το οποίο χρησιμοποίησε ένα λέιζερ και ένα απλό ιόν υδραργύρου για να κατασκευάσει ένα πλήρες σύστημα οπτικού ρολογιού με καθυστέρηση μικρότερη του ενός δευτερολέπτου ανά 4,5 εκατομμύρια χρόνια. Οι συσκευές αυτές έχουν θέσει πλέον νέα στάνταρτ στην ακρίβεια, αποσπώντας, μάλιστα, το ρεκόρ (περίπου 150 φορές πιο ακριβείς) από τα άτομα του καισίου που το κατείχαν εδώ και μισό αιώνα, μιας και έχουν τη δυνατότητα να παρέχουν ένα πιο σταθερό σήμα χρόνου, παρόλο που οι τεχνολογίες μικροκυμάτων εξακολουθούν να βελτιώνονται.

Αναλυτικότερα, χρησιμοποιούν δέσμες λέιζερ, οι οποίες προκαλούν ταχύτερη ταλάντωση συγκριτικά με την ακτινοβολία των μικροκυμάτων, κάτι που σημαίνει ότι ο χρόνος χωρίζεται σε πολύ μικρότερα τμήματα και συνεπώς μπορεί να μετρηθεί με μεγαλύτερη ακρίβεια. Με μια τέτοια εκπληκτική ακρίβεια, το επίτευγμα είναι κολοσσιαίο αλλά και προβληματικό.

Κατ΄ αρχάς, για να αποκομιστούν τα οφέλη μιας τέτοιας ακρίβειας, η τεχνολογία αυτή δε θα πρέπει να ενσωματωθεί μόνο στα επίγεια ρολόγια αλλά και στα ρολόγια των δορυφόρων, κάτι το οποίο δεν είναι καθόλου εύκολο να επιτευχθεί.

Παρόλα αυτά, έχει την προοπτική για ένα ευρύ φάσμα εφαρμογών. Για παράδειγμα, πολλές εφαρμογές ζωτικής σημασίας για την άμυνα και την ασφάλεια, που οδηγούν σε κύκλο εργασιών πολλών δισεκατομμυρίων ευρώ ετησίως, απαιτούν εξαιρετικά ακριβή πρότυπα χρόνου και συχνότητας που επιτρέπονται μόνο από ατομικά ρολόγια. Στις αμυντικές ρυθμίσεις, συγκεκριμένα, παρέχουν τα χρονικά πρότυπα σε οπλικά συστήματα ακριβείας και σε πολλά άλλα εξελιγμένα ηλεκτρονικά συστήματα. Η εξαιρετική σταθερότητα θα μπορούσε να επεκτείνει σημαντικά το χρόνο μεταξύ των ενημερώσεων ενός ρολογιού, αποτρέποντας έτσι τις προσπάθειες ενός αντιπάλου να παρασύρει σήματα GPS, ενώ στα συστήματα ραντάρ θα επέτρεπε μεγαλύτερη ευαισθησία, ικανή να εντοπίσει μικρότερους στόχους.

Όσον αφορά το GPS, ειδικότερα, κάθε δορυφόρος του που βρίσκεται σε τροχιά έχει τέσσερα ατομικά ρολόγια (ρουβιδίου και καισίου). Τα ρολόγια αυτά παρέχουν σήματα θέσης που επιτρέπουν ακρίβεια εντός μερικών μέτρων (συνήθως μεταξύ 1 και 10). Αυτή η ακρίβεια αρκεί για καθοδηγούμενα πυρομαχικά και πλοήγηση, αλλά η ανάγκη για ακρίβεια υπομέτρου θα αυξηθεί, καθώς τα αυτόνομα οχήματα και τα αεροσκάφη χρησιμοποιούνται ευρύτερα αλλά και καθώς βελτιώνεται η κατασκευή εξαιρετικά ακριβών συστημάτων αδρανειακής πλοήγησης. Η τεχνολογία των οπτικών ατομικών ρολογιών έχει τη δυνατότητα να προσφέρει στο GPS ακρίβεια μικρότερη του ενός μέτρου σε πραγματικό χρόνο αλλά και να βελτιώσει θεαματικά όλα τα ηλεκτρονικά συστήματα.

Από την άλλη πλευρά, όμως, ίσως έθεται σε σκληρή δοκιμασία τους γνωστούς νόμους της Φυσικής. «Υπάρχουν πολλές μελλοντικές προοπτικές που ο άνθρωπος ούτε που μπορεί να φανταστεί», λέει ο συγγραφέας και ερευνητής Κρίστιαν Γκρέμπινγκ (Christian Grebing).

Η τελευταία ανακάλυψη (2017) αφορά οπτικά ατομικά ρολόγια που αν υπήρχαν από την εποχή της εξαφάνισης των δεινοσαύρων, δε θα είχαν χάσει ούτε ένα τέταρτο του δευτερολέπτου. Συγκεκριμένα, ερευνητές στη Γαλλία, τη Βρετανία και τη Γερμανία χρησιμοποίησαν ατομικά ρολόγια που βασίζονται στη συχνότητα της ακτινοβολίας που εκπέμπουν άτομα στροντίου και δεν πάνε ¨πίσω¨ ή ¨μπροστά¨ ούτε ένα δευτερόλεπτο για περίπου 15 δισεκατομμύρια χρόνια, υπερκαλύπτοντας έτσι ακόμη και την ηλικία του σύμπαντος (14,8 δισ. χρόνια), πόσο μάλλον της Γης (4,5 δισεκατομμύρια χρόνια), αν υποτεθεί ότι θα μπορούσαν να διαρκέσουν τόσο πολύ.

Στην καρδιά της συσκευής βρίσκεται ένας θάλαμος κενού όπου διατηρούνται μετέωρα, μέσα σε ένα οπτικό πλέγμα από διασταυρούμενες δέσμες λέιζερ, άτομα του ραδιενεργού ισοτόπου στροντίου. Με αυτόν τον τρόπο, τα άτομα διατάσσονται σε διαδοχικά στρώματα και ψύχονται κοντά στο απόλυτο μηδέν. Ένα σταθερό ερυθρό φως λέιζερ, το οποίο έχει την ίδια ακριβώς οπτική συχνότητα με αυτή που τα άτομα του στροντίου μεταπηδούν μεταξύ δύο ενεργειακών επιπέδων (430 τρισεκατομμύρια φορές το δευτερόλεπτο), προκαλεί την ταλάντωσή τους.

Η παγίδευση των ατόμων στο δικτυωτό αυτό πλέγμα εμποδίζει τις συγκρούσεις μεταξύ τους, επιτρέπει τη μέτρηση της ταλάντωσης πολλών ατόμων ταυτοχρόνως, χωρίς το ηλεκτρομαγνητικό πεδίο του καθενός να επηρεάζει τα γειτονικά του, ενισχύοντας έτσι τη σταθερότητα του ρολογιού.

Η ακρίβεια και η σταθερότητα είναι τα δύο βασικά κριτήρια για την απόδοση ενός ρολογιού, ωστόσο διαφέρουν μεταξύ τους. Η σταθερότητα αφορά το πόσο πιστά το ρολόι συντονίζεται με τη φυσική συχνότητα με την οποία τα άτομά του ταλαντώνονται. Συνεπώς, όσο πιο σταθερό είναι ένα ρολόι, τόσο πιο ακριβείς είναι και οι μετρήσεις που κάνει.

Το σημαντικό στην ανακάλυψη αυτή είναι πως τα συγκεκριμένα ρολόγια κάνουν πολλά περισσότερα από την απλή μέτρηση του χρόνου. Η τεχνολογία τους καθιστά εφικτό να μελετηθούν φαινόμενα που απαιτούν εξαιρετική ακρίβεια, ανοίγοντας νέους ορίζοντες στην κοσμολογία και τη φυσική.

Ένα από αυτά είναι το γεγονός ότι ένα δευτερόλεπτο ή ένα οποιοδήποτε κλάσμα του δευτερολέπτου δεν έχει την ίδια διάρκεια παντού στη Γη. Το νέο ρολόι είναι υπερυψηλής ακρίβειας, ώστε είναι σε θέση να μετρά οριακές αλλαγές τόσο στην πάροδο του χρόνου όσο και στη δύναμη της βαρύτητας με την παραμικρή υψομετρική διαφορά π.χ. ενός ή δύο εκατοστών. Αυτές οι μεταβολές αποτελούν σημαντικό πρόβλημα στη μέτρηση του χρόνου, η οποία απαιτεί να υπάρχουν πολλά ρολόγια απόλυτα συγχρονισμένα μεταξύ τους.

Η νέα αυτή μελέτη, η οποία αναρτήθηκε στην υπηρεσία προδημοσίευσης arXiv, συγκρίνει τρία τέτοια ρολόγια, τα οποία βρίσκονται στο Παρίσι, το Λονδίνο και το Μπράουνσβαϊγκ της Γερμανίας. Χάρη στα ακριβή ατομικά ρολόγια, λοιπόν, η

ερευνητική ομάδα υπολογίζει με εντυπωσιακή ακρίβεια πώς ο χρόνος κυλά με διαφορετικό ρυθμό στο Λονδίνο και το Παρίσι, επιβεβαιώνοντας με αυτόν τον τρόπο τη σχετικότητα του χρόνου.

Ο χρόνος, όπως και ο χώρος, είναι έννοιες σχετικές, είχε πει ο Άλμπερτ Αϊνστάιν. Το φαινόμενο της ¨διαστολής του χρόνου¨ οφείλεται σε δύο διαφορετικούς παράγοντες που σχετίζονται με την έννοια της Σχετικότητας. Ο πρώτος παράγοντας είναι η ταχύτητα. Ένα ρολόι που κινείται με μεγάλη ταχύτητα σε σχέση με έναν παρατηρητή μετράει το χρόνο πιο αργά σε σχέση με το ρολόι του παρατηρητή. Ο δεύτερος παράγοντας είναι η βαρύτητα. Όταν η δύναμη της βαρυτικής έλξης αυξάνεται στο σημείο που βρίσκεται ο παρατηρητής, το ρολόι του θα λειτουργεί πιο αργά σε σχέση με το ρολόι ενός παρατηρητή που δέχεται ασθενέστερη έλξη. Με άλλα λόγια, ένα ρολόι στην κορυφή του Έβερεστ θα τρέχει πιο γρήγορα από ό,τι ένα ρολόι στην επιφάνεια της Γης.

Προκειμένου να συγκριθεί ο ρυθμός του χρόνου στις τρεις τοποθεσίες, οι ερευνητές σύνδεσαν τα ρολόγια σε δίκτυα οπτικών ινών που λειτουργούσαν στις ίδιες συχνότητες με καθένα από τα ρολόγια. Κάθε διαφορά στη συχνότητα του φωτός μεταξύ των ινών θα υποδήλωνε διαφορές και στο ρυθμό του χρόνου.

Πράγματι, οι μετρήσεις έδειξαν ότι ο ρυθμός του χρόνου στις τρεις τοποθεσίες τρέχει διαφορετικά επειδή κάθε πόλη έχει διαφορετική απόσταση από το κέντρο της Γης (και επομένως δέχεται διαφορετικές βαρυτικές δυνάμεις) και διαφορετική απόσταση από τον ισημερινό (και συνεπώς διαφορετική ταχύτητα περιστροφής γύρω από τον άξονα της Γης). Μάλιστα, η χρονική απόκλιση που εντοπίζεται ανάμεσα στο Παρίσι και το Λονδίνο κατά τη διάρκεια ενός 24ωρου φτάνει τα 5 δισεκατομμυριοστά του δευτερολέπτου.

Οι επιστήμονες πρέπει να κάνουν, συνεπώς, διορθώσεις ακόμα κι όταν τα ατομικά ρολόγια βρίσκονται σε διαφορετικό όροφο του ίδιου κτιρίου! Ανεβάζοντας ένα ρολόι ακόμη και κατά 10 εκατοστά αλλάζει ο ρυθμός του. Κι αν η διαφορά ύψους είναι εφικτό να υπολογιστεί, κανείς δεν μπορεί να συνυπολογίσει τις μεταβολές της βαρύτητας λόγω τοπικής γεωλογίας, παλιρροιών ή κίνησης του μάγματος βαθιά μέσα στη Γη.

Τα αποτελέσματα του πειράματος, σύμφωνα με το περιοδικό New Scientist, επέτρεψαν στους ερευνητές να υπολογίσουν μια παράμετρο που ονομάζεται άλφα. Αν ο Αϊνστάιν είχε απόλυτο δίκιο για τη διαστολή του χρόνου, τότε η τιμή της θα πρέπει να ισούται με μηδέν. Το να αποδειχθεί ότι το άλφα ισούται με μηδέν είναι τεχνικά αδύνατο, όμως, η τελευταία μελέτη δείχνει ότι η τιμή του είναι μικρότερη από 10^{-8}, ένα επίπεδο ακρίβειας δυο φορές μεγαλύτερο σε σχέση με προηγούμενες μετρήσεις ρολογιών στροντίου. Δεν αποκλείεται, όμως, το γεγονός να διαψευτεί τελικά από πιο ακριβή πειράματα.

Αν η τιμή του άλφα μετρηθεί στο μέλλον με μεγαλύτερη ακρίβεια και βρεθεί ότι δεν ισούται με μηδέν, οι συνέπειες θα είναι πραγματικά τεράστιες. Μεταξύ άλλων, μια τιμή πάνω από το μηδέν θα μπορούσε να λύσει το αιώνιο μυστήριο που αφορά τον τρόπο με τον οποίο αλληλεπιδρούν ο χώρος και ο χρόνος, ανοίγοντας, με αυτόν τον τρόπο, νέες συναρπαστικές προοπτικές για το μεγάλο όνειρο των φυσικών, την ενοποίηση της Σχετικότητας του Αϊνστάιν με την Κβαντομηχανική.

Πόσο γρήγορα είναι εφικτό τα οπτικά ρολόγια να ξεκινήσουν να χρησιμοποιούνται σε συστήματα, όπως π.χ. τα ευρυζωνικά δίκτυα (που διακινούν τεράστιες πληροφορίες στο διαδίκτυο); Αυτό εξαρτάται από το πόσο γρήγορα θα δρομολογηθεί η καθιέρωση ενός νέου προτύπου, το οποίο θα αντικαταστήσει το καίσιο. Προς το παρόν δεν υπάρχει συμφωνία σχετικά με το ποιο θα μπορούσε να αποτελέσει το νέο πρότυπο. Κάθε εθνικό εργαστήριο υποστηρίζει τη δική του επιλογή ιόντος ή ατόμου. Το 2006 η Διεθνής Επιτροπή Μέτρων και Σταθμών ενέκρινε τις οπτικές μεταβάσεις στον υδράργυρο, στο στρόντιο και στο υττέρβιο αλλά μόνο ως την αντικατάσταση του καισίου, ως δευτερεύουσες, δηλαδή, αντιπροσωπεύσεις του δευτερολέπτου. Επομένως, σύμφωνα και με τον τρέχοντα επίσημο διεθνή ορισμό των μονάδων του χρόνου, μόνο τα ατομικά ρολόγια καισίου θεωρούνται μέχρι στιγμής ακριβή.

Το Απόλυτο Παγκόσμιο Ρολόι

Η ταχύτατη επιστημονική και τεχνολογική πρόοδος, όσον αφορά τα πειραματικά ατομικά ρολόγια, τόσο στο NIST όσο και σε άλλα εργαστήρια ανά τον κόσμο, έχουν φτάσει τη χρονομέτρηση σε απίστευτα επίπεδα ακρίβειας και σταθερότητας, με

αποτέλεσμα την εμφάνιση όλο και πιο εξελιγμένων ατομικών ρολογιών που ανοίγουν εντελώς νέες εφαρμογές και αγορές.

Τα συστήματα, όμως, τα οποία εξαρτώνται από αυτά τα ρολόγια για να παρέχουν ακριβή σήματα χρονισμού, είναι ευάλωτα σε διαταραχές, διακοπές, αποτυχία, όπως ελαττωματικές μεταφορτώσεις δεδομένων και αντιμετωπίζουν πολλαπλές απειλές από κακόβουλες επιθέσεις, όπως παρεμβολές, σε σπάνιους αλλά πραγματικούς κινδύνους, όπως οι ηλιακές εκλάμψεις και οι διαστημικές καιρικές συνθήκες που θα μπορούσαν να διαταράξουν ολόκληρο το σύστημα.

Τα σήματα ώρας GNSS, για παράδειγμα, χρησιμοποιούνται σε ένα ευρύ φάσμα εφαρμογών, από την πλοήγηση έως τα χρηματοοικονομικά δίκτυα και τα δίκτυα διανομής ηλεκτρικής ενέργειας. Σε επικοινωνίες υψηλής ταχύτητας, ακόμη, η χρονομέτρηση χρησιμοποιεί ατομικά ρολόγια συγχρονισμένα με υπηρεσίες διάδοσης χρόνου που βασίζονται στο GNSS για την πραγματοποίηση χρονοσήμανσης και δρομολόγησης πληροφοριών. Αυτές οι δυνατότητες είναι θεμελιώδεις για την υψηλή απόδοση και τη διαθεσιμότητα του Διαδικτύου και όλων των σχετικών υπηρεσιών του. Τα περισσότερα από αυτά τα δίκτυα, όμως, δε διαθέτουν εφεδρικά συστήματα. Τα δεδομένα υποδηλώνουν ότι ο οικονομικός αντίκτυπος μιας διαταραχής του GNSS στο Ηνωμένο Βασίλειο θα μπορούσε να ανέλθει σε 5,2 δισεκατομμύρια λίρες Αγγλίας σε διάστημα πέντε ημερών, συμπεριλαμβανομένων των υπηρεσιών έκτακτης ανάγκης, της εφοδιαστικής αλυσίδας και της ναυτιλιακής βιομηχανίας.

Ακόμα κι ένας προσωρινός αποσυγχρονισμός των ρολογιών θα έκανε αισθητή την εμφάνισή του. Ο χρόνος δεν αποτελεί πλέον απλά την τέταρτη διάσταση του σύμπαντος. Παίζει καθοριστικό ρόλο στη σύγχρονη οικονομία (καπιταλιστική ή σοσιαλιστική). Για το λόγο αυτό, η ακριβής μέτρηση και διανομή του είναι αντικείμενο λεπτομερών διεθνών συμφωνιών και της Συνθήκης για το Μέτρο, η οποία ισχύει από το 1875.

Η Βασιλική Ισπανική Ακαδημία (RAE), μάλιστα, προειδοποίησε ότι μια διακοπή των σημάτων GNSS θα μπορούσε να προκαλέσει την ταυτόχρονη αποτυχία υπηρεσιών που πρέπει να συνεργαστούν σε περίπτωση έκτακτης ανάγκης. Σε περίπτωση ακραίων διαστημικών καιρικών συνθηκών, η RAE συνιστά να σχεδιαστούν συστήματα

επικοινωνίας και ασφάλειας που να λειτουργούν χωρίς GNSS για χρονικό διάστημα έως και τρεις μέρες.

Επιπλέον, εκείνο που έχει ουσιαστική σημασία στη διεθνή χρονομέτρηση δεν είναι το ένα και μοναδικό εξαιρετικά ακριβές και σταθερό ρολόι, αλλά ένα παγκόσμιο δίκτυο ρολογιών. Η Συντονισμένη Παγκόσμια Ώρα (Coordinated Universal Time – UTC) εξαρτάται όχι μόνο από την ακρίβεια της μέτρησης του χρόνου αλλά και από την ακρίβεια σύγκρισης των χρόνων που δίνουν τα κέντρα μέτρησης χρόνου σε όλο τον κόσμο.

Αν κοιτάξει κανείς ένα ρολόι δε γνωρίζει αν πηγαίνει καλά ή όχι. Αν κοιτάξει δύο ρολόγια και δε συμφωνούν μεταξύ τους και πάλι δεν ξέρει ποιο είναι σωστό. Με τρία ρολόγια, όμως, μπορεί να απορρίψει το ένα που αποκλίνει περισσότερο από τα άλλα δύο και να υπολογίσει το χρόνο βάση κάποιου αλγορίθμου που θα λαμβάνει υπόψη την ακρίβεια και τη σταθερότητα, βραχυπρόθεσμη και μακροπρόθεσμη, των δύο ¨αποδεκτών¨ ρολογιών.

Διάφορα ερευνητικά κέντρα έχουν το δικό τους ρολόι καισίου και συνεργάζονται με το Διεθνές Γραφείο Μέτρων και Σταθμών στο Παρίσι, το οποίο υπολογίζει τον μέσο όρο τους και τον δημοσιεύει κάθε μήνα σε ένα ενημερωτικό δελτίο που καθορίζει τον Παγκόσμιο Χρόνο. Αλλά αυτό σημαίνει πως δεν υπάρχει άμεση μέτρηση ενός καθολικά αποδεκτού προτύπου χρόνου.

Η πιο αποδοτική λύση είναι η υιοθέτηση ατομικών ρολογιών με κβαντική ενίσχυση. Τα ατομικά αυτά ρολόγια θα μπορούσαν να υποστηρίξουν και να παρέχουν μηχανισμό ανάκαμψης και ανθεκτικότητας σε ένα δορυφορικό δίκτυο που δεν είναι άτρωτο σε πολύ σοβαρές απειλές. Μπορούν να ενσωματωθούν, για παράδειγμα, σε επίγεια συστήματα ως αντίγραφο ασφαλείας σε περίπτωση μη διαθεσιμότητας ή απώλειας του GNSS.

Η ακρίβεια ενός ατομικού ρολογιού εξαρτάται από παράγοντες, οι οποίοι περιλαμβάνουν τον αριθμό των ατόμων που χρησιμοποιούνται. Όσο περισσότερα άτομα τόσο καλύτερα. Σ ' ένα κλασικό ατομικό ρολόι, η ακρίβεια είναι ανάλογη της τετραγωνικής ρίζας του αριθμού των ατόμων. Επομένως, έχοντας 4 φορές περισσότερα άτομα, η ακρίβεια θα διπλασιαστεί. Σ' ένα διαπλεγμένο ατομικό ρολόι, όμως, η

βελτίωση είναι απευθείας ανάλογη προς τον αριθμό των ατόμων. 4 φορές περισσότερα άτομα, δηλαδή, προσφέρουν 4 φορές καλύτερο ρολόι. Χρησιμοποιώντας άφθονα άτομα, λοιπόν, θα ήταν δυνατόν να κατασκευαστεί ένα ρολόι με μέγιστη διεμπλοκή, σταθερό κατά 1 μέρος στα 10^{18}, όπου θα έπρεπε κανείς να το παρατηρεί 30 δισεκατομμύρια χρόνια για να κερδίσει ή να χάσει ένα δευτερόλεπτο, εξηγεί ο Alex Kuzmich, φυσικός στο Ινστιτούτο Τεχνολογίας της Georgia, ο οποίος μάλιστα υποστηρίζει ότι ένα τέτοιο γεγονός θα συνέβαλε και στη μείωση των ενδογενών αβεβαιοτήτων ενός συστήματος.

Τα ατομικά ρολόγια, όμως, μπορούν να δικτυωθούν μεταξύ τους για να σχηματίσουν ένα ακόμη πιο ακριβές δίκτυο ρολογιών. Όταν κβαντικά αντικείμενα, όπως τα άτομα, διαπλέκονται, μια μέτρηση στο ένα από αυτά θα έχει μια ακαριαία και προβλέψιμη επίδραση στο άλλο. Εάν τοποθετούνταν ατομικά ρολόγια σε σύμπλεξη σε διάφορα μέρη του πλανήτη αλλά και στους δορυφόρους, θα ήταν εφικτό να συγκρίνονταν ταυτόχρονα μεταξύ τους.

Ένα δίκτυο οπτικών ατομικών ρολογιών εξαιρετικής ακρίβειας, που συνδέονται μεταξύ τους με το εκπληκτικό φαινόμενο της κβαντικής σύμπλεξης, θα μπορούσε να λειτουργήσει κοντά στο όριο του Heisenberg, δημιουργώντας το απόλυτο παγκόσμιο ρολόι. Αν θεωρηθούν τα ρολόγια ως εκκρεμή, τότε η σύμπλεξη των διαφορετικών ρολογιών κάνει τα ρολόγια να ταλαντώνονται με τέλεια συμφωνία, πραγματοποιώντας έτσι μια υπερσύγχρονη μέτρηση που παρέχει μια ασφαλή και ανεξάρτητη χρονική βάση για παγκόσμια τήρηση χρόνου. Ένα τέτοιο επίτευγμα, δηλαδή, θα επέτρεπαι όλες οι χώρες να συμφωνήσουν σε μια ακριβή μέτρηση του χρόνου, δημιουργώντας ταυτόχρονα έναν τεράστιο κβαντικό αισθητήρα που επιπλέον θα μπορούσε να επιφέρει δραματική βελτίωση και σε περαιτέρω εφαρμογές με τη μεγιστοποίηση της ακρίβειας που είναι ικανό να επιτύχει.

Η δυνατότητα της μέτρησης του χρόνου με πολύ υψηλή ακρίβεια είναι ένα ανεκτίμητο εργαλείο στην επιστημονική έρευνα και την τεχνολογία, σύμφωνα με τον Kuzmich, ο οποίος ασχολείται με τη μελέτη της κβαντικής διεμπλοκής εδώ και πολλά χρόνια, ενώ πλέον ασχολείται με τη χρήση της στα ατομικά ρολόγια. Από το γραφείο Βιολογικών και Φυσικών ερευνών της NASA, μάλιστα, η οποία χρησιμοποιεί ατομικά ρολόγια για την πλοήγηση των διαστημοπλοίων της, προσφέρθηκε στον Kuzmich και τους συνεργάτες του μια χρηματοδότηση για να υποστηριχθεί η έρευνά τους.

Η εκτίμηση της ερευνητικής ομάδας είναι ότι ένα παγκόσμιο δίκτυο κβαντικού ρολογιού θα είναι κατά περίπου 100 φορές πιο ακριβές από οποιοδήποτε ατομικό ρολόι. Ακόμη, θα είναι προστατευμένο με φυσικό τρόπο, δεδομένου ότι κάθε εξωτερική παρέμβαση, σύμφωνα με την κβαντική μηχανική, γίνεται απευθείας αντιληπτή.

Συνεπώς, είναι εύκολα κατανοητό ότι το δευτερόλεπτο που μετράται σήμερα μπορεί να μην είναι ίδιο με εκείνο που θα μετράται στο μέλλον. Ίσως, λοιπόν, κάποια στιγμή χρειαστεί να αναθεωρηθεί ο τρόπος με τον οποίο μετράται ο χρόνος αλλά και η αντίληψη που υπάρχει γι΄ αυτόν.

Η κβαντική εμπλοκή, ωστόσο, είναι μια εξαιρετικά ευαίσθητη κατάσταση και ένα τόσο μεγάλο κβαντικό δίκτυο είναι πολύ δύσκολο να παραμείνει κβαντικά συνδεδεμένο. Επομένως, το πόσο γρήγορα θα μπορούσε να κατασκευαστεί ένα τέτοιο δίκτυο είναι δύσκολο να προβλεφθεί. Υπάρχει ακόμα πολύς δρόμος να διανυθεί, καθώς απαιτούνται σημαντικές τεχνολογικές εξελίξεις, αν και έχουν επιτευχθεί όλα τα βήματα σε μικρή κλίμακα.

Ατομικά Ρολόγια Μικροτσίπ

Τα ατομικά ρολόγια που χρησιμοποιούνται σήμερα ως τα κύρια πρότυπα για τη διεθνή χρονομέτρηση είναι σε μέγεθος ψυγείου και περιορίζονται σε έναν μικρό αριθμό εθνικών εργαστηρίων μέτρησης σε όλο τον κόσμο, όπως το Εθνικό Εργαστήριο Φυσικής (NPL) στο Ηνωμένο Βασίλειο. Μια σειρά ρολογιών που βασίζονται σε αυτά έχουν διατεθεί στο εμπόριο σύμφωνα με το αν το μειωμένο μέγεθος, το βάρος ή η κατανάλωση ισχύος είναι σημαντικός παράγοντας για μια συγκεκριμένη αγορά. Ωστόσο, οι μικρότερες εκδόσεις αυτών των ρολογιών είναι λιγότερο ακριβείς.

Εικόνα 32: Ατομικά ρολόγια

Πηγή: https://www.pemptousia.gr/2012/07/i-metrisi-tou-chronou-ke-ta-atomika-rol/

Μια έρευνα για την κβαντική τεχνολογία, που διεξήχθη από την επιστημονική συμβουλευτική επιτροπή της Πολεμικής Αεροπορίας των ΗΠΑ, κατέληξε στο συμπέρασμα ότι είναι αναγκαίο να καταβληθούν έντονες προσπάθειες για να δημιουργηθούν μικροσκοπικά ρολόγια με βελτιωμένη ακρίβεια.

Βασιζόμενοι σε αυτό, επιστήμονες στο NPL, στο Ελβετικό Κέντρο Ηλεκτρονικής και Μικροτεχνικής και σε άλλα εργαστήρια σε όλο τον κόσμο, αναπτύσσουν νέες τεχνολογίες ατομικών ρολογιών που είναι ώριμες για εμπορευματοποίηση. Στόχος τους είναι να συνεχίσουν τη βελτίωση της σταθερότητας και της ακρίβειας, μειώνοντας, παράλληλα, την πολυπλοκότητα, το μέγεθος και το βάρος. Σμίκρυνση και απλοποίηση σημαίνει μείωση του κόστους παραγωγής, μαζικές πωλήσεις του ρολογιού και μείωση της ενεργειακής κατανάλωσης, με σκοπό να ενσωματωθούν ατομικά ρολόγια σε περισσότερα όργανα και κινητές συσκευές, μέχρι και σε ρολόγια χειρός. Να παραχθούν, επομένως, μικροσκοπικές συσκευές που είναι φθηνές και απλές στη χρήση και που μπορούν να ενσωματωθούν σε τρέχοντα και μελλοντικά συστήματα, ακόμη και εκτός εργαστηρίου.

Τα ακριβέστερα φορητά ρολόγια θα ενισχύσουν την ευφυΐα των σημάτων, τον ηλεκτρονικό πόλεμο και τις δυνατότητες παρεμβολής αντι-ραντάρ, ενώ θα διευκολύνουν πιο ισχυρές επικοινωνίες. Μερικά ατομικά ρολόγια κλίμακας τσιπ, που λειτουργούν με χαμηλή ισχύ και καταλαμβάνουν μόνο μερικά κυβικά εκατοστά όγκου, είναι ήδη διαθέσιμα στο εμπόριο.

Η αρχή έγινε το 2002 όταν ο Οργανισμός Προηγμένων Έργων Έρευνας για την Άμυνα (DARPA) ξεκίνησε ένα πρόγραμμα ατομικού ρολογιού σε κλίμακα τσιπ στις ΗΠΑ, χρηματοδοτώντας το NIST για τη διεξαγωγή θεμελιωδών ερευνών και μετρολογίας. Το πρώτο εμπορικά διαθέσιμο ατομικό ρολόι κλίμακας τσιπ, ωστόσο, κυκλοφόρησε στην αγορά το 2011 από τη Symmetricom Inc.. Παρείχε ακρίβεια μεγαλύτερη από 3 μικροδευτερόλεπτα τη μέρα, είχε όγκο 16 κυβικά εκατοστά, βάρος 35 g και κατανάλωση ισχύος 155 mW. Με ακριβή χρονισμό σε αυτήν την κλίμακα και ισχύ, θα επιτραπεί μια ευρεία γκάμα πρακτικών εφαρμογών στο πεδίο των επικοινωνιών, του γεωγραφικού εντοπισμού θέσης (GPS) αλλά και σε άλλες τεχνολογίες.

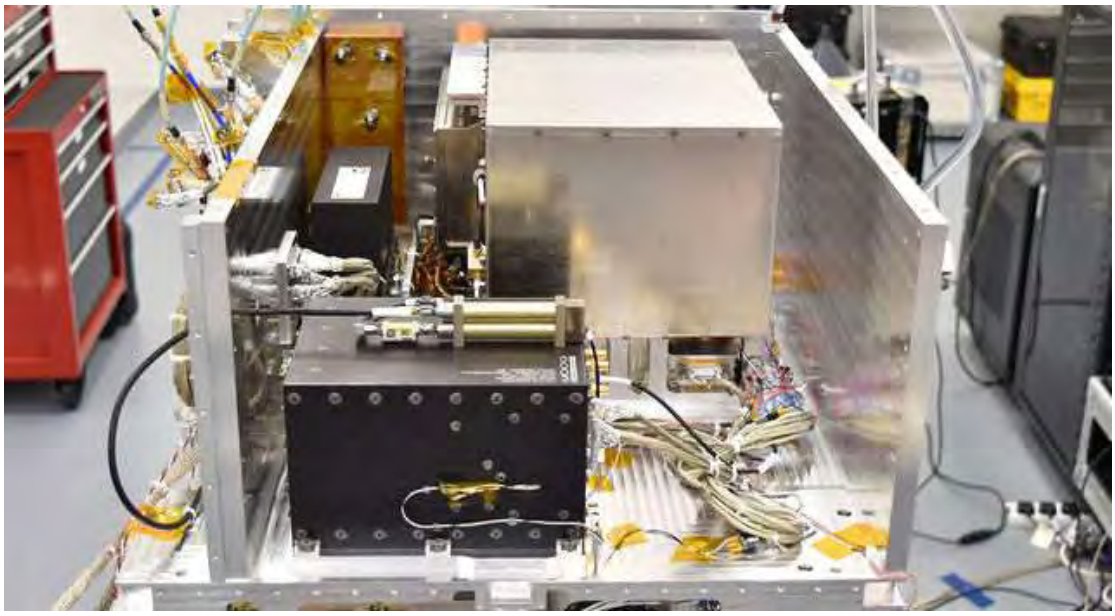
Επιπλέον, μπορούν να αξιοποιηθούν για τη δημιουργία ιδιαίτερα ευαίσθητων μετρητών υψόμετρου που θα καταγράφουν τις υψομετρικές διαφορές ανάλογα με τις ανεπαίσθητες μεταβολές της βαρύτητας, αλλά και για τον εντοπισμό σχηματισμών του υπεδάφους που προκαλούν αυτές τις μεταβολές, επομένως και αλλαγή στο ρυθμό του χρόνου. Ακόμη, καθίστανται ικανά να βοηθήσουν στην ανάπτυξη τεχνολογιών, όπως οι σουπερ αισθητήρες μαγνητικών πεδίων, θερμοκρασίας κ.α., ενώ ήδη έχουν συμβάλλει στην κατασκευή του πρώτου φορητού ρολογιού μέτρησης βαρύτητας, η οποία ολοκληρώθηκε το 2018 από ευρωπαίους επιστήμονες και ειδικούς του Physikalisch-Technische Bundesanstal της Γερμανίας.

Τα σταθερά, φορητά ατομικά ρολόγια θα επιτρέψουν μεγαλύτερη ακρίβεια στην πλοήγηση σε παγκόσμια κλίμακα τόσο για ειρηνικούς σκοπούς, όπως η ναυσιπλοΐα, η εξερεύνηση του Διαστήματος, η λειτουργία των δικτύων ηλεκτρονικών υπολογιστών, η αστρονομία και η σεισμολογική έρευνα, αλλά και για στρατιωτικούς σκοπούς, όπως η πραγματοποίηση πυρηνικών δοκιμών.

Στο διάστημα, αναλυτικότερα, υπάρχει ανάγκη για σταθερά και ακριβή, αλλά μικρά και ελαφριά ρολόγια με χαμηλή κατανάλωση ενέργειας. Τα ρολόγια υψηλότερης απόδοσης χρειάζεται να διορθώνονται λιγότερο συχνά, φέρνοντας έτσι επανάσταση στην deepspace πλοήγηση. Με σταθερά ρολόγια ένα διαστημικό σκάφος θα μπορούσε να υπολογίσει τα δικά του δεδομένα χρονισμού και πλοήγησης χωρίς αμφίδρομη σύνδεση με τη Γη, με αποτέλεσμα τη μείωση του ¨κόστους¨ αποστολής και τη βελτίωση ορισμένων δυνατοτήτων του, όπως π.χ οι προσγειώσεις.

Ο χρόνος για να υιοθετηθούν, βέβαια, θα είναι μεγαλύτερος για τα διαστημικά ρολόγια παρά για τα επίγεια, καθώς αντιμετωπίζουν πρόσθετες τεχνικές προκλήσεις. Αυτά τα ρολόγια πρέπει να επιβιώσουν από τις εξαιρετικά υψηλές δυνάμεις και τους κραδασμούς που βιώνουν κατά την εκτόξευση, τις μεγάλες αλλαγές στη θερμοκρασία και τα υψηλά επίπεδα κοσμικής ακτινοβολίας. Επιπλέον, χωρίς δυνατότητα συντήρησης, αλλά με ανάγκη λειτουργίας χωρίς αποτυχία για πολλά χρόνια, η αξιοπιστία είναι πολύ πιο σημαντική από ό, τι στις επίγειες εφαρμογές.

Το 2018, το Jet Propulsion Laboratory της NASA τελειοποίησε σχεδόν το Deep Space Atomic Clock. Το DSAC είναι ένα μικρό, ελαφρύ ατομικό ρολόι, βασισμένο σε τεχνολογία παγίδευσης ιόντος υδραργύρου και έχει το μέγεθος μιας τετραπλής τοστιέρας, ενώ υπάρχουν σχέδια για περαιτέρω σμίκρυνση.



Εικόνα 33: Deep Space Atomic Clock

Πηγή: https://www.newspepper.gr/dite-to-atomiko-roloi-gia-tin-ploigisi-sto-diastima-foto/

Τα φτηνά, φορητά ατομικά ρολόγια μεγέθους μικροτσίπ, από την άλλη, πέρα από τα συστήματα κρυπτογράφησης και εξασφάλισης του απαραβίαστου των τηλεφωνικών επικοινωνιών, πιθανό να βρουν μυριάδες χρήσεις που ακόμα κανείς δεν μπορεί να φανταστεί.

Με την ανάπτυξη μικροσκοπικών ατομικών ρολογιών χαμηλού κόστους, αν μη τι άλλο, δε θα είναι αναγκαία η ¨μετακίνηση¨ στο NPL κάθε φορά, επιτρέποντας τον εντοπισμό

προβλημάτων σε πρώιμο στάδιο και τη μείωση του κόστους σε χρόνο. Ένα τέτοιο δίκτυο θα μπορούσε, επίσης, να είναι μια δοκιμαστική βάση για πειράματα επίδειξης τεχνολογίας όχι μόνο για ρολόγια, αλλά και για κβαντικές επικοινωνίες.

Η επιδίωξη της υπεροχής στις επιδόσεις δεν αποτελεί ζήτημα κύρους. Η ακρίβεια των ατομικών ρολογιών προσφέρει την ακρίβεια που απαιτείται σήμερα σε δεκάδες εφαρμογές τόσο στην καθημερινότητα, όσο και στον τομέα των επιστημονικών ερευνών, εξασφαλίζοντας, με αυτό τον τρόπο, την εύρυθμη λειτουργία τους. Βελτιώνοντας, επομένως, την ακρίβεια μέτρησης του χρόνου, όλες οι τεχνολογίες, από τις οποίες εξαρτάται η κοινωνία, μπορούν επίσης να βελτιωθούν.

Οι ειδικοί δεν ελπίζουν μόνο ότι θα χρησιμοποιήσουν την καινοτομία για τέτοιου είδους εφαρμογές, αλλά θα την εκμεταλλευτούν και για επιστημονικές μελέτες. Ρολόγια τέτοιας ακρίβειας θα επέτρεπαν ακόμη και δοκιμές που θα έδειχναν αν οι φυσικοί νόμοι και οι σταθερές έχουν μεταβληθεί από τις απαρχές του κόσμου ως σήμερα με τον πιο λεπτομερή τρόπο.

ΚΒΑΝΤΙΚΟΙ ΑΙΣΘΗΤΗΡΕΣ

Γενικά

Πλέον η ανθρωπότητα διανύει τη δεύτερη επανάσταση της Κβαντικής Φυσικής, όπου όχι μόνο έχουν αποδεχτεί σχεδόν όλοι τις παραδοξότητές της ως κύρια γνωρίσματα της κβαντικής πραγματικότητας, αλλά και επιθυμούν, και πολλές φορές καταφέρνουν, να τις χαλιναγωγήσουν με σκοπό την επίτευξη αποτελεσμάτων που σε παλαιότερες εποχές θα φάνταζαν ως θαύματα, αν κανείς τολμούσε να τα επιδιώξει ή έστω να τα διατυπώσει. Στα πλαίσια των υπαρκτών αλλά και των αναδυόμενων αμυντικών εφαρμογών, ξεχωρίζουν δύο κύρια πεδία επικράτησης της κβαντικής τεχνολογίας, αυτό της κβαντικής πληροφορικής που έχει περιγραφεί στα προηγούμενα κεφάλαια και αυτό των κβαντικών αισθητήρων. Παρόλο που η τεχνολογία των κβαντικών αισθητήρων δεν είναι τόσο παλιά όσο της κβαντικής πληροφορικής, τα τελευταία χρόνια οι κβαντικοί αισθητήρες έχουν καταφέρει να κερδίσουν σημαντικό από το χαμένο έδαφος, συμπληρώνοντας και ενισχύοντας το κοινό πεδίο της μετάδοσης και διαχείρισης της πληροφορίας σε κβαντικό επίπεδο.

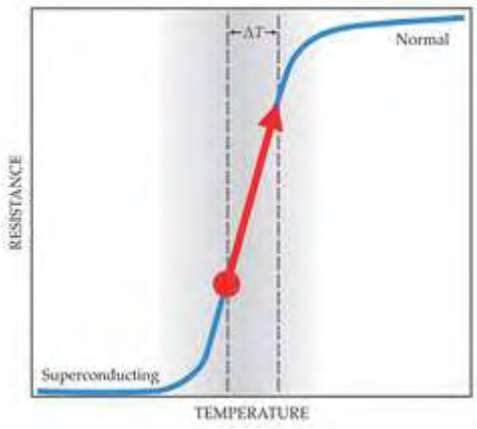
Ένας κβαντικός αισθητήρας είναι μια συσκευή κβαντικού χαρακτήρα, η οποία ανταποκρίνεται σε ένα ερέθισμα. Αναλυτικότερα, οι κβαντικοί αισθητήρες αναφέρονται σε κβαντικά φυσικά συστήματα, τα οποία έχουν τη δυνατότητα να μετρήσουν πληθώρα φυσικών μεγεθών όπως είναι τιμές μαγνητικών και ηλεκτρικών πεδίων, χρονικές διαφορές και συχνότητες, περιστροφές, τιμές θερμοκρασίας, βαρύτητας, επιτάχυνσης αλλά και πίεσης. Εκμεταλλεύονται δε τον κβαντικό τους χαρακτήρα, συνήθως, χρησιμοποιώντας την κβαντική συνοχή για τη μέτρηση της φυσικής ποσότητας ή την εμπλοκή για να βελτιώσουν σημαντικά την ευαισθησία ή την ακρίβεια των μετρήσεων πέρα από αυτό που μπορούν να καταφέρουν οι αισθητήρες της τρέχουσας τεχνολογίας.

Οι κβαντικοί αισθητήρες μπορούν, γενικότερα, να προσφέρουν βαθμιαία αλλαγή στην απόδοση. Πιο ευαίσθητοι, ακριβείς, πιο γρήγοροι στη χρήση και σταθεροί, μερικές φορές πολλές τάξεις μεγέθους από τους κλασικούς ομολόγους τους, μπορούν να ξεκλειδώσουν νέες εφαρμογές που είναι δυνατές μόνο με τέτοιες βελτιώσεις. Οι κβαντικές τεχνολογίες δεύτερης και τρίτης γενιάς, μάλιστα, αναμένεται τα επόμενα χρόνια να συρρικνωθούν, με αποτέλεσμα οι κβαντικοί αισθητήρες να αρχίσουν να κυκλοφορούν στην αγορά. Και σε έναν κόσμο που εξαρτάται όλο και περισσότερο από

τους αισθητήρες και την αίσθηση, έχουν τη δυνατότητα να προσφέρουν ένα σημαντικό ανταγωνιστικό πλεονέκτημα μιας και από τη στιγμή που θα μπουν στο πεδίο, δε θα υπάρχει κανείς και τίποτα που θα μπορεί να κρυφτεί!

Υπεραγώγιμοι Αισθητήρες Μεταβατικής Ακμής (TES)

Ένας υπεραγώγιμος αισθητήρας μεταβατικής ακμής (TES) ονομάζεται, επίσης, υπεραγώγιμο θερμόμετρο μετάβασης φάσης (SPT). Είναι ένας ισχυρός ενεργειακός ανιχνευτής, ικανός να ανιχνεύσει τον αριθμό των προσπιπτόντων φωτονίων μέσω της ικανότητας της εσωτερικής ανάλυσης ενέργειας. Είναι, ουσιαστικά, ένα εξαιρετικά ευαίσθητο θερμόμετρο, ο πυρήνας του οποίου είναι ένα λεπτό υπεραγώγιμο υμένιο που λειτουργεί σε θερμοκρασία μεταξύ της κανονικής και της υπεραγώγιμης κατάστασης. Κατά τη μετάβασή του από υπεραγωγό σε κανονικό μέταλλο, μια πολύ μικρή αλλαγή στη θερμοκρασία που προκαλείται από την απορρόφηση των φωτονίων, προκαλεί μια μεγάλη αλλαγή στην αντίσταση.



Εικόνα 34: Αλλαγή αντίστασης κατά τη μετάβαση από υπεραγωγό σε κανονικό μέταλλο

Πηγή: https://physicstoday.scitation.org/doi/full/10.1063/PT.3.3995

Όταν ένα φωτόνιο απορροφάται, η θερμοκρασία της μεμβράνης αυξάνεται, αυξάνοντας την αντίστασή της, η οποία με τη σειρά της μειώνει το ρεύμα που ρέει στον αισθητήρα. Η μείωση του ρεύματος μειώνει τη θερμότητα Joule της συσκευής και επαναφέρει την αρχική θερμοκρασία της μεμβράνης. Η ολοκλήρωση της προκύπτουσας πτώσης του ρεύματος είναι ανάλογη με την ενέργεια που απορροφά ο ανιχνευτής και το σήμα εξόδου είναι ανάλογο με τη μεταβολή της θερμοκρασίας. Τέτοιες συσκευές, επί του παρόντος, χρησιμοποιούνται για έλεγχο θερμοκρασιών μετάβασης σε συσκευές ανίχνευσης ακτινοβολίας ευρέως φάσματος π.χ. ακτίνες Χ,

υπέρυθρα φωτόνια, άτομα, μόρια, κ.λπ, ωστόσο, ενδέχεται να έχουν ευρύτερη εφαρμογή στο μέλλον.

Οι υπεραγώγιμοι αισθητήρες μετάπτωσης (TES) είναι ευρυζωνικοί με σχετικά μεγάλη έκταση, χαμηλό θόρυβο, υψηλή αποδοτικότητα και χαμηλό κατώτατο όριο ανιχνεύσιμης ενέργειας. Η βασική διαφορά, όμως, μεταξύ των ανιχνευτών TES και άλλων θερμικών ανιχνευτών είναι το υπεραγώγιμο θερμόμετρο. Η επιλογή του υπεραγώγιμου υλικού που χρησιμοποιείται για αυτό το θερμόμετρο παίζει σημαντικό ρόλο στον προσδιορισμό των χαρακτηριστικών του ανιχνευτή. Από τις ιδιότητες του υπεραγωγού, η θερμοκρασία μετάβασης, το Tc του θερμομέτρου δηλαδή, έχει τη μεγαλύτερη επίδραση στην απόδοση της συσκευής. Σημαντικές ιδιότητές που περιλαμβάνουν όχι μόνο θερμική χωρητικότητα αλλά και θερμική αγωγιμότητα και θερμικό θόρυβο εξαρτώνται έντονα από τη θερμοκρασία μετάβασης, επομένως, η επιλογή της είναι κρίσιμη για το σχεδιασμό της συσκευής και μία από τις πιο σημαντικές παραμέτρους για έναν TES. Ως αποτέλεσμα, οι περισσότεροι TES έχουν θερμοκρασίες μετάβασης κοντά στα 100-400 mK. Υπάρχουν διάφοροι στοιχειώδεις υπεραγωγοί που έχουν κρίσιμες θερμοκρασίες στο εύρος ενδιαφέροντος, αλλά για διάφορους λόγους μόνο μερικοί έχουν χρησιμοποιηθεί σε ανιχνευτές TES. Τα κύρια μέταλλα που χρησιμοποιούνται είναι το μολυβδαίνιο (Mo), το τιτάνιο (Ti), το βολφράμιο (W), το νιόβιο (Nb), το ιρίδιο (Ir) και το αλουμίνιο ή αλλιώς αργίλιο (Al).

Για να είναι χρήσιμος ο ανιχνευτής πρέπει να συνδέεται αποτελεσματικά με την εισερχόμενη ακτινοβολία. Ο βασικός σχεδιασμός του θερμομέτρου μπορεί να παραμείνει ο ίδιος για διαφορετικές ενεργειακές περιοχές, απλά πρέπει να συνδεθεί με έναν απορροφητή που είναι κατάλληλος για την προβλεπόμενη εφαρμογή. Η φύση αυτής της απορροφητικής δομής εξαρτάται από τον τύπο της ακτινοβολίας που μετριέται. Ένας ιδανικός απορροφητής πρέπει να απορροφά εντελώς την εκάστοτε εισερχόμενη ακτινοβολία και να μετατρέπει γρήγορα όλη την ενέργεια που προσπίπτει σε θερμότητα. Αυτή η θερμότητα πρέπει να συνδεθεί με τον TES, χωρίς πρόσθετες διαδρομές, ώστε να αποφευχθεί πιθανή απώλεια. Η θερμική χωρητικότητα του απορροφητή πρέπει να είναι μικρή σε σύγκριση με τον TES, καθώς η επιπλέον θερμική χωρητικότητα μειώνει την ευαισθησία και αυξάνει το θόρυβο. Για εφαρμογές όπου η απορρόφηση ενέργειας είναι πολύ εντοπισμένη (π.χ απορρόφηση ενός μόνο φωτονίου), η απορροφόμενη ενέργεια πρέπει να εξαπλωθεί σε ολόκληρο τον TES σε πολύ λιγότερο

από τη θερμική σταθερά χρόνου. Η υψηλή αντίσταση θέτει όρια είτε στον ίδιο τον ανιχνευτή είτε στην ταχύτητά του.

Όταν ένας θερμικός ανιχνευτής χρησιμοποιείται για τη μέτρηση της ενέργειας μεμονωμένων φωτονίων, ονομάζεται θερμιδόμετρο. Εάν η ροή των προσπιπτόντων φωτονίων είναι πολύ μεγάλη για να διαχωριστούν, ο ανιχνευτής χρησιμοποιείται για τη μέτρηση των αλλαγών στη ροή και ονομάζεται βολόμετρο. Οι πρώτες επιδείξεις των δύο αυτών τύπων υπεραγώγιμων ανιχνευτών μεταβατικής ακμής εμφανίστηκαν τη δεκαετία του 1950, 30 χρόνια μετά την ανακάλυψη της υπεραγωγιμότητας από τον Onnes. Το 1941, ο D. H. Andrews εφάρμοσε ρεύμα σε ένα καλώδιο ταντάλιου και μέτρησε τη μεταβολή της αντίστασης που προκλήθηκε από ένα υπέρυθρο σήμα. Αυτή ήταν η πρώτη επίδειξη ενός βολόμετρου TES. Στη συνέχεια, επέδειξε ένα θερμιδόμετρο από νιτρίδιο νιοβίου που χρησιμοποιήθηκε για τη μέτρηση των σωματιδίων άλφα.

Κατά τη διάρκεια του πρώτου μισού αιώνα μετά την εφεύρεσή τους, οι ανιχνευτές TES σπάνια χρησιμοποιήθηκαν σε πρακτικές εφαρμογές, κυρίως, λόγω της δυσκολίας ανάγνωσης σήματος από ένα τέτοιο σύστημα χαμηλής αντίστασης. Ένα δεύτερο εμπόδιο στην υιοθέτηση των ανιχνευτών TES ήταν η επίτευξη σταθερής λειτουργίας στην υπεραγώγιμη περιοχή μετάβασης. Η θερμότητα Joule μπορεί να οδηγήσει σε θερμική διαφυγή που οδηγεί τον ανιχνευτή στην κανονική (μη υπεραγώγιμη) κατάσταση, ένα φαινόμενο γνωστό ως θετική ηλεκτροθερμική ανάδραση. Αντιθέτως, η ισχυρή αρνητική ηλεκτροθερμική ανάδραση ευθυγραμμίζει την απόκριση του TES. Το πρόβλημα αυτό λύθηκε το 1995 από τον K. D. Irwin, γεγονός που οδήγησε σε ευρεία υιοθέτηση των ανιχνευτών TES. Πλέον, μεγάλες συστοιχίες ανιχνευτών TES αναπτύσσονται για διάφορες εφαρμογές.

Η ευαισθησία ενός TES καθιστά δυνατή την ανάπτυξη θερμικών ανιχνευτών με ταχύτερη απόκριση, μεγαλύτερη χωρητικότητα θερμότητας και μικρότερη ανιχνεύσιμη είσοδο ενέργειας από τους θερμικούς ανιχνευτές που κατασκευάζονται χρησιμοποιώντας συμβατικά θερμίστορ ημιαγωγών. Ωστόσο, η απότομη μετάβαση οδηγεί σε μεγαλύτερη τάση αστάθειας, με αποτέλεσμα να απαιτείται προσεκτικός σχεδιασμός.

Οι τεχνολόγοι της NASA έχουν αναπτύξει έναν νέο, υπεραγώγιμο αισθητήρα μεταβατικής ακμής. Ο νέος αυτός σχεδιασμός παρέχει άμεση βελτίωση στη διαδικασία

σχεδιασμού και κατασκευής της υπάρχουσας τεχνολογίας TES, παράγοντας συσκευές που μπορούν να ικανοποιήσουν τις βέλτιστες υπεραγώγιμες τιμές θερμοκρασίας μετάβασης και να βελτιώσουν την απόδοση. Επιπλέον, αυτή η νέα μέθοδος παρέχει τη δυνατότητα δημιουργίας αισθητήρων πολύ μικρότερου μεγέθους και με βελτιωμένη απλότητα κατασκευής, αξιοπιστία και αναπαραγωγιμότητα. Παρέχει πολύ χαμηλή λειτουργία θορύβου για ανίχνευση ακτινοβολίας μεγάλου μήκους κύματος και υψηλή ανάλυση ενέργειας για ανίχνευση ακτινοβολίας μικρού μήκους κύματος. Ο νέος σχεδιασμός επιτρέπει, επίσης, τη χρήση απλών υλικών που δεν μπορούσαν προηγουμένως να χρησιμοποιηθούν στους TES. Όλα αυτά, τον καθιστούν εύκολα εφαρμόσιμο στην επεξεργασία οπτικών κβαντικών πληροφοριών.

Μια τέτοιου είδους ενδιαφέρουσα νέα εφαρμογή είναι η κβαντική κρυπτογραφία. Τα ασφαλή συστήματα απαιτούν ανιχνευτές με ευαισθησία ενός φωτονίου σε μήκη κύματος τηλεπικοινωνιών και πολύ χαμηλές μετρήσεις σκοτεινής ενέργειας. Ακόμη, οι ανιχνευτές αυτοί υπόσχονται πολλά όσον αφορά πειραματικές δοκιμές που βασίζονται στις ανισότητες Bell γενικότερα αλλά και στην αστρονομία, όπου απαιτούνται ανιχνευτές με την ικανότητα να παρέχουν ταυτόχρονες μετρήσεις ενέργειας φωτονίων και ώρας άφιξης. Συμβάλλουν στη μελέτη της σκοτεινής ύλης και της υπερσυμμετρίας, αλλά και τη χημική σύνθεση υλικών.

Αναλυτικότερα, μια ομάδα επιστημόνων στο Los Alamos, συνεργαζόμενη με ερευνητές από το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας και το Κολέγιο Albion, κατάφερε τη διανομή κβαντικού κλειδιού σε μήκος κύματος 1.550 nm μέσω μιας οπτικής ίνας 50 χιλιομέτρων (QKD), εκμεταλλευόμενη τους υπεραγώγιμους αισθητήρες. Η εργασία αυτή θα ήταν δυνατό να επιταχύνει την ανάπτυξη QKD για ασφαλείς επικοινωνίες στις οπτικές ίνες τόσο σε απόσταση όσο και σε απόδοση πέρα από τα μέχρι πρότινος τεχνολογικά όρια, αναφέρει η ομάδα σύμφωνα με το Applied Physics Letters.

Η κβαντικός φυσικός Danna Rosenberg του Los Alamos λέει ότι οι TES δίνουν σημαντικά υψηλότερες αποδόσεις ανίχνευσης ενός φωτονίου από τις προηγούμενες φωτοδιόδους. Η υψηλή αυτή απόδοση, που σχετίζεται με το σχετικά σύντομο χρόνο αποκατάστασής τους, θα οδηγήσει σε υψηλότερους ρυθμούς μετάδοσης μυστικών κλειδιών σε ακόμα μεγαλύτερες αποστάσεις από τα σημερινά συστήματα.

Εκτός από τους TES, η ομάδα δοκίμασε φωτεινό παλμό και ηλεκτρικούς μηχανισμούς συγχρονισμού σημάτων. Μια μέθοδος του συγχρονισμού περιλάμβανε την αποστολή ενός φωτεινού παλμού 1.310 nm αμέσως πριν σταλεί ένας παλμός 1.550 nm, ενώ χρησιμοποιήθηκε ένας ακόμη φωτεινός παλμός για να μειώσει τα πιθανά λάθη. Έγινε χρήση, επίσης, ενός μηχανισμού συγχρονισμού με ένα ατομικό ρολόι ρουβιδίου για το συγχρονισμό αποστολέων και δεκτών πληροφοριών.

Όταν χρησιμοποιούνται μαζί με ηλεκτρικούς μηχανισμούς συγχρονισμού, οι TES έχουν τη δυνατότητα να μεγαλώσουν τις αποστάσεις για τις οποίες θα υπήρχε η δυνατότητα να χρησιμοποιηθούν οι οπτικές ίνες για τη διανομή κβαντικού κλειδιού. Πιο περίπλοκες μέθοδοι από ό,τι χρησιμοποίησαν οι πειραματιστές, κάποια μέρα μπορεί να επιτρέψουν στους χρήστες να στείλουν κβαντικά κλειδιά ασφαλώς σε αποστάσεις μεγαλύτερες των μέχρι στιγμής 404 χιλιομέτρων.

Μέχρι στιγμής, η κβαντική κρυπτογραφία χρησιμοποιείται σε γεωγραφικώς περιορισμένα δίκτυα. Το σημαντικότερο πλεονέκτημα της τεχνικής, ότι όποιος υποκλέπτει τη μετάδοση ενός κλειδιού το μεταβάλλει και κατά μη αναστρέψιμο τρόπο, σημαίνει πως το σήμα, με το οποίο μεταφέρονται κβαντικά κλειδιά, δεν είναι εφικτό να ενισχυθεί από τον εξοπλισμό του δικτύου που αντισταθμίζει την εξασθένηση και το βοηθά να φτάσει μέχρι τον επόμενο επαναλήπτη. Ένας οπτικός ενισχυτής θα αλλοίωνε τα qubits.

Προκειμένου να μεγαλώσουν την εμβέλεια αυτών των ζεύξεων, οι ερευνητές αναζητούν μέσα διάδοσης για τη διανομή των κβαντικών κλειδιών ικανοποιητικότερα από τις οπτικές ίνες. Οι επιστήμονες ανέβηκαν σε βουνοκορφές, όπου το υψόμετρο ελαχιστοποιεί τις ατμοσφαιρικές αναταράξεις, για να αποδείξουν ότι η αποστολή φωτονίων διαμέσου του αέρα αποτελεί εφαρμόσιμη λύση. Ένα τέτοιο πείραμα, που πραγματοποιήθηκε το 2002 στο Εθνικό Εργαστήριο του Λος Άλαμος, δημιούργησε μια ζεύξη 10 χιλιομέτρων, ενώ ένα άλλο, που πραγματοποιήθηκε τον ίδιο χρόνο από τη Βρετανική QinetiQ και το Πανεπιστήμιο Ludwig Maximilian του Μονάχου, έζευξε επιτυχώς δύο βουνοκορφές των νότιων Άλπεων που απείχαν μεταξύ τους 23 χιλιόμετρα. Πόλυ πρόσφατα, μάλιστα, ο αριθμός αυτός ανέβηκε και άλλο στα 1.120 χιλιόμετρα, μετά από ένα πείραμα ερευνητών στην Κίνα, στο οποίο έγινε χρήση του φαινομένου της κβαντικής διεμπλοκής.

Με τη βελτίωση της τεχνολογίας αυτής, πιθανόν να καταστεί δυνατή η χρήση ενός τέτοιου συστήματος, καθώς τέτοια εμβέλεια επαρκεί για να επιτευχθεί η επικοινωνία με δορυφόρους που περιφέρονται γύρω από τη Γη σε χαμηλή τροχιά. Ένα δίκτυο τέτοιων δορυφόρων θα επέτρεπε επικοινωνία παγκοσμίου επιπέδου.

Η Ευρωπαϊκή Ένωση, τον Απρίλιο του 2004, ξεκίνησε μια προσπάθεια για ανάπτυξη κβαντικής κρυπτογράφησης σε δίκτυα επικοινωνιών, προσπάθεια η οποία, εν μέρει, παρακινήθηκε από την επιθυμία να αντιμετωπιστεί η κατασκοπευτική δραστηριότητα του Echelon, ενός συστήματος που υποκλέπτει ηλεκτρονικά μηνύματα για λογαριασμό των υπηρεσιών πληροφοριών των ΗΠΑ, της Βρετανίας και άλλων κρατών. Τα τελευταία χρόνια, η Ευρωπαϊκή Επιτροπή και ο Ευρωπαϊκός Οργανισμός Διαστήματος (ESA) υπέγραψαν τεχνική συμφωνία για συνεργασία στη δημιουργία της υποδομής ενός απολύτως ασφαλούς πανευρωπαϊκού δικτύου κβαντικών επικοινωνιών (Quantum Communication Infrastructure (QCI)), ενώ τον Οκτώβρη του 2018 εγκαινιάστηκε και η πρώτη δεκαετής φάση της Εμβληματικής αυτής Πρωτοβουλίας (Quantum Flagship), η οποία χρηματοδοτήθηκε με ένα δισεκατομμύριο ευρώ από την Ευρωπαϊκή Επιτροπή.

Πριν λίγα χρόνια, μάλιστα, η ID Quantique και μια συνεργαζόμενη εταιρεία, ο παροχέας υπηρεσιών πληροφοριών Deckpoint στη Γενεύη, παρουσίασαν ένα δίκτυο, το οποίο επέτρεπε σε μια συστοιχία διακομιστών στη Γενεύη να αποθηκεύει τα αντίγραφα ασφαλείας της σε απόσταση 10 χιλιομέτρων, με τα νέα κλειδιά να διανέμονται μέσω μιας ζεύξης προστατευμένης με αλγορίθμους κβαντικής κρυπτογραφίας.

Η κβαντική κρυπτογραφία, ωστόσο, ενδέχεται να προκύψει ευάλωτη σε ορισμένες ανορθόδοξες μορφές προσβολής. Ο υποκλοπέας θα είχε τη δυνατότητα, για παράδειγμα, να σαμποτάρει τους ανιχνευτές του αποδέκτη, ώστε τα ληφθέντα qubits να διαρρεύσουν στην οπτική ίνα, από την οποία μεταδόθηκαν και να υποκλαπούν. Και φυσικά, μια υποκλοπή με εκ των έσω βοήθεια θα καθίσταται πάντα αναπότρεπτη.

Όσον αφορά το θόρυβο στους ανιχνευτές TES εμπίπτει σε τέσσερις γενικές κατηγορίες. Σε ορισμένες περιπτώσεις, οι διαφορετικοί τύποι θορύβου σχετίζονται. Ο πρώτος τύπος αναφέρεται ως εσωτερικός θόρυβος θερμικών διακυμάνσεων (ITFN) και σχετίζεται με σύνθετη θερμική αντίσταση. Ο δεύτερος τύπος θορύβου τείνει να είναι χειρότερος για χαμηλότερη αντίσταση. Γίνεται αναφορά σε αυτόν ως ηλεκτρικός θόρυβος. Ο τρίτος τύπος είναι ο θόρυβος χαμηλής συχνότητας και συσχετίζεται συχνά με ιδιαίτερα

υψηλές τιμές του ηλεκτρικού θορύβου. Τέλος, σε ορισμένες περιπτώσεις παρατηρείται θόρυβος στη χρονική απόκριση ενός TES. Αυτές οι πηγές θορύβου θέτουν θεμελιώδη όρια στην ισχύ θορύβου και στην ανάλυση ενέργειας ενός TES. Πρόσθετες πηγές θορύβου υποβαθμίζουν την απόδοσή του από αυτά τα θεμελιώδη όρια, ενώ πρόσφατες μελέτες έχουν δείξει ότι η τοποθέτηση σε αυτόν πρόσθετων κανονικών μεταλλικών δομών μπορεί να μειώσει σημαντικά τον υπερβολικό θόρυβο.

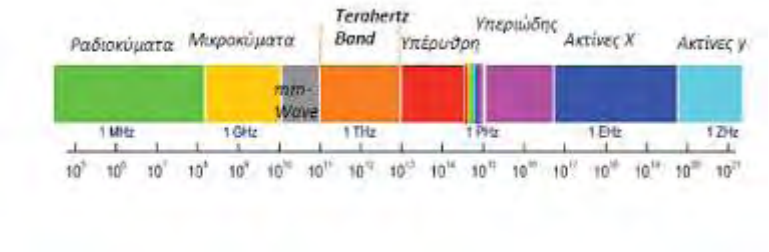
Αισθητήρες Rydberg

Οι κεραίες χρησιμοποιούνται καθημερινά σε αμέτρητες στρατιωτικές και εμπορικές συσκευές και είναι σημαντικές για ένα ευρύ φάσμα εφαρμογών για τη μετάδοση και τη λήψη δεδομένων, χρησιμοποιώντας ηλεκτρομαγνητικά κύματα που αντιστοιχούν σε ακτινοβολία συχνότητας ραδιοκυμάτων, μικροκυμάτων και terahertz. Αν μπορούσε κανείς να δει το δωμάτιο γύρω του, θα ήταν γεμάτο από αυτά τα κύματα που ταλαντεύονται, επιτρέποντας την επικοινωνία μεταξύ πολλών συσκευών μέσω δικτύων, όπως WiFi, Bluetooth και κινητών τηλεφώνων. Χρησιμοποιούνται, ακόμη, για την επικοινωνία στην αεροδιαστημική βιομηχανία και τα αυτοκίνητα αυτοδήγησης, για σαρωτές ασφαλείας στα αεροδρόμια κ.α.

Τον Οκτώβριο του 2018, επιστήμονες από το Ερευνητικό Εργαστήριο του Στρατού των Ηνωμένων Πολιτειών (Sensors and Electron Devices Directorate) συζήτησαν δημοσίως τις προσπάθειές τους για ανάπτυξη ενός ραδιοφωνικού δέκτη ευρείας ζώνης, χρησιμοποιώντας υπερευαίσθητα άτομα, διεγερμένα σε ασυνήθιστα υψηλά επίπεδα ενέργειας, γνωστά ως άτομα Rydberg. Κατά τη διάρκεια της έρευνάς τους, κατάφεραν να προσδιορίσουν ότι ο αισθητήρα τους μπορεί να ανιχνεύσει με ακρίβεια σήματα σε ολόκληρο το φάσμα ραδιοσυχνοτήτων και έχει τη δυνατότητα να συγκριθεί με άλλες καθιερωμένες αντίστοιχες τεχνολογίες αισθητήρων ηλεκτρικού πεδίου, όπως τα ηλεκτροοπτικά κρύσταλλα.

Τα άτομα, εξάλλου, όπως έχει ξαναναφερθεί, είναι ιδιαίτερα πλεονεκτικά ως συσκευές μέτρησης, πρώτα επειδή είναι τα ίδια παντού και δεύτερον επειδή οι ιδιότητές τους δεν εξελίσσονται με την πάροδο του χρόνου. Μπορεί κανείς να χρησιμοποιεί τα ίδια άτομα, οπουδήποτε και αν είναι, για πάντα, για επακόλουθες μετρήσεις, χωρίς αυτά να επηρεάζονται. Αυτό τα καθιστά ιδανικούς μετρητές, οι οποίοι κατανέμονται σε όλο το σύμπαν και δεν υποφέρουν από μετατόπιση.

Οι αρχικές πειραματικές παρατηρήσεις των ατόμων Rydberg είχαν γίνει σε καυτά αέρια, διεγερμένα με πηγές φωτός ευρείας ζώνης. Από τότε, έχουν χρησιμοποιηθεί για μια ποικιλία εφαρμογών ανίχνευσης. Για παράδειγμα, στις οθόνες φθορισμού, στις αρχές του 20ου αιώνα, χρησιμοποιήθηκαν για την ανίχνευση ηλεκτρονίων, ακτίνων Χ και ακτινοβολίας γάμμα. Ωστόσο, ενώ ήταν ευρέως γνωστό ότι είναι ευαίσθητα, δεν είχε γίνει ποτέ στο παρελθόν ποσοτική περιγραφή της ευαισθησίας τους.



Εικόνα 35: Ηλεκτρομαγνητικό φάσμα
Πηγή:http://amitos.library.uop.gr/xmlui/bitstream/handle/123456789/4661/%CE%A0%CF%84%CF%85%CF%87%CE%B9%CE%B1%CE%BA%CE%AE_%CE%93%CE%B1%CF%81%CE%B1%CE%BD%CF%84%CE%B6%CE%B9%CF%8E%CF%84%CE%B7%CF%82%20%CE%A0%CE%B5%CF%81%CE%B9%CE%BA%CE%BB%CE%AE%CF%82_%CE%A0%CE%9C%CE%A3%20%CE%A4%CE%B7%CE%BB%CE%B5%CF%80%CE%B9%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%B1%CE%BA%CE%AC%20%CE%A3%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1.pdf?sequence=1&isAllowed=y

Το Μάρτιο του 2020, οι ερευνητές του SEDD ανακοίνωσαν ότι ανέλυσαν την ευαισθησία αυτού του κβαντικού αισθητήρα στα ταλαντούμενα ηλεκτρικά πεδία, σε ένα τεράστιο εύρος συχνοτήτων από 0 έως 10^{12} Hertz. Παρόλο που δεν είναι ασυνήθιστο να υπάρχει ραδιοφωνική κάλυψη ευρείας ζώνης με μία μόνο συσκευή, η μετάβαση από 0 Hz στα 1000 GHz με μία κεραία είναι πολύ μεγάλη. Αυτή η ευρεία φασματική κάλυψη είναι αδύνατη σε ένα παραδοσιακό σύστημα δέκτη, ακόμη και με την προσθήκη πολλαπλών συστημάτων μεμονωμένων κεραιών που αποτελούνται από εξαρτήματα, όπως ενισχυτές.

Οι επιστήμονες του στρατιωτικού αυτού εργαστηρίου, επομένως, ήταν οι πρώτοι στον κόσμο που κατάφεραν να δημιουργήσουν έναν κβαντικό δέκτη, ο οποίος θα τους επέτρεπε να ανιχνεύσουν αξιόπιστα σήματα επικοινωνίας που καλύπτουν ένα τέτοιο εύρος. Αυτοί οι νέοι αισθητήρες είναι πολύ μικροί σε μέγεθος (περίπου ένα εκατοστό) και σχεδόν μη ανιχνεύσιμοι, δίνοντας στους στρατιωτικούς ένα αποτρεπτικό πλεονέκτημα.

Σύμφωνα με τα όσα δήλωσαν, η κβαντική μηχανική ήταν αυτή που βοήθησε ώστε να γίνει γνωστή σε πολύ μεγάλο βαθμό η βαθμονόμηση και η απόλυτη απόδοση του

δέκτη, μετρήσεις οι οποίες είναι ίδιες για κάθε τέτοιο αισθητήρα. Όπου και αν δημιουργούνται καταστάσεις Rydberg, σε άτομα, μόρια ή στερεά, μοιράζονται κοινά χαρακτηριστικά. Χωρίς αυτές τις πληροφορίες, ο αισθητήρας δεν θα μπορούσε να λειτουργήσει κάτω από εργαστηριακές ρυθμίσεις, πόσο μάλλον εκτός εργαστηρίου, ενώ θα ήταν αδύνατο να καθοριστεί ο τρόπος με τον οποίο θα ήταν εφικτό να χρησιμοποιηθεί στον τομέα. Το έργο τους έγινε, μάλιστα, πρόσφατα αποδεκτό δημοσίευσης στο Physical Review Letters.

Οποιοδήποτε άτομο με πολύ διεγερμένο ηλεκτρόνιο σθένους και με ένα ή περισσότερα ηλεκτρόνια που έχουν πολύ μεγάλο κύριο κβαντικό αριθμό n (όσο υψηλότερη η τιμή του n τόσο πιο μακριά είναι το ηλεκτρόνιο από τον πυρήνα) είναι γνωστό ως άτομο Rydberg. Τέτοιες καταστάσεις ατόμων παρατηρούνται, συνήθως, σε περιβάλλοντα υψηλής ενέργειας, όπως μέσα στο διάστημα, καθώς και σε πλάσματα στη Γη.

Το 1965, οι αστρονόμοι στο Εθνικό Αστεροσκοπείο Ραδιοαστρονομίας της Δυτικής Βιρτζίνια των ΗΠΑ ανακάλυψαν την ακτινοβολία μικροκυμάτων που εκπέμπεται από άτομα υδρογόνου στον Orion (αστερισμό του Ωρίωνα), ξεκινώντας από μια κατάσταση με κύριο κβαντικό αριθμό n = 110. Καθώς αναπτύχθηκε η τεχνολογία, οι φυσικοί μπόρεσαν να παρατηρήσουν άτομα Rydberg με όλο και υψηλότερους κύριους κβαντικούς αριθμούς, ενώ, πιο πρόσφατα, παρατηρήθηκαν καταστάσεις με n = 1000.

Τα άτομα Rydberg έχουν, ακόμη, μεγάλη διάρκεια ζωής, μιας και παρεμποδίζεται σημαντικά η αποδιέγερσή τους, είναι εξαιρετικά μεγάλα σε μέγεθος, μεγαλύτερα από έναν ιό και 10.000 φορές μεγαλύτερα από ένα κλασικό άτομο και τα ηλεκτρόνια σθένους τους είναι ασθενώς συνδεδεμένα (καθώς είναι τόσο μακριά από τον πυρήνα), με αποτέλεσμα να είναι εύκολα διαταραγμένα ή ιονισμένα από συγκρούσεις και να έχουν μια σημαντικά ισχυρή απόκριση σε εξωτερικά πεδία, συμπεριλαμβανομένων των πεδίων που προκαλούνται από τα κοντινά άτομα Rydberg.

Η βασική ιδέα είναι ότι μια ακτίνα λέιζερ διεγείρει ένα άτομο σε κατάσταση Rydberg και ένα άλλο λέιζερ ελέγχει την κατάστασή του. Για την ερευνητική στρατιωτική ομάδα, συγκεκριμένα, τα άτομά τους διατηρούνται σε ένα απλό γυάλινο κελί σε θερμοκρασία δωματίου και χρησιμοποιούνται δύο χρώματα φωτός λέιζερ για να διεγείρουν ταυτόχρονα τα άτομα Rydberg και να ανιχνεύουν την αντίδρασή τους στα εξωτερικά ηλεκτρικά πεδία. Μάλιστα, η ομάδα έδειξε ότι ένας δέκτης Rydberg μπορεί

να επιτύχει τη μέγιστη επιτρεπόμενη θεωρητική απόδοση και να περιορίζεται μόνο από τη θεμελιώδη κατάρρευση της λειτουργίας κυμάτων.

Η θεωρητική απόδοση ενός τέτοιου αισθητήρα RF, για παράδειγμα, είναι, τουλάχιστον, μια τάξη μεγέθους ανώτερη από εκείνη της τυπικής ανίχνευσης RF. Η ηλεκτρομετρία RF με βάση τα άτομα Rydberg, επομένως, είναι πολλά υποσχόμενη για την εκτέλεση μετρήσεων, με υψηλότερη ευαισθησία, ακρίβεια και σταθερότητα από τα συμβατικά πρότυπα. Είναι φανερό, συνεπώς, ότι το σύστημα συμπεριφέρεται με θεμελιωδώς διαφορετικό τρόπο από μια συνηθισμένη κεραία, γεγονός που οδηγεί τους επιστήμονες να εξετάσουν νέες εφαρμογές και νέες δυνατότητες.

Η υπερβολική ευαισθησία που το χαρακτηρίζει πηγάζει από τη μεγάλη χωρική έκταση του κύματος του ασθενώς δεσμευμένου ηλεκτρονίου. Εξαιτίας αυτής, ο αισθητήρας Rydberg καθίσταται ιδανικός για τη μέτρηση ασθενών πεδίων. Τα φαινόμενα, επομένως, που είναι αδύνατο να ανιχνευθούν από τα κλασικά άτομα, μπορούν να μετρηθούν και να οπτικοποιηθούν με άτομα Rydberg, μετατρέποντας την αόρατη ακτινοβολία χαμηλής ενέργειας σε διαμορφωμένο οπτικό φως λέιζερ σε πραγματικό χρόνο.

Η ευαισθησία τους φτάνει τέτοια επίπεδα, ώστε ένα μόνο φωτόνιο, που διεγείρει ένα άτομο σε μια κατάσταση Rydberg, μπορεί να αλληλεπιδράσει και να επηρεάσει σημαντικά τα επίπεδα ενέργειας Rydberg όχι μόνο ενός, αλλά δεκάδων ή εκατοντάδων κοντινών ατόμων σε αποστάσεις που μπορεί κανείς εύκολα να δει κάτω από ένα οπτικό μικροσκόπιο. Το εύρος τέτοιων ισχυρών αλληλεπιδράσεων είναι εφικτό να φτάσει ακόμη και σε κλίμακες απόστασης της τάξης ~ 10 μm.

Λόγω του μεγάλου μεγέθους τους, τα άτομα αυτά μπορούν να παρουσιάσουν πολύ υψηλές ηλεκτρικές διπολικές ροπές, οι οποίες σε συνδυασμό με τη μεγάλη διάρκεια ζωής τους, που φτάνει μέχρι και εκατοντάδες μικροδευτερόλεπτα (μs), οδηγούν, επίσης, σε ισχυρές αλληλεπιδράσεις μεταξύ δύο ατόμων Rydberg και μάλιστα πολύ μεγαλύτερης διάρκειας σε σύγκριση με τις χαμηλές διεγερμένες καταστάσεις, οι οποίες έχουν διάρκεια ζωής, μόλις, μερικές δεκάδες νανοδευτερόλεπτα. Το γεγονός αυτό, πέρα από την ανίχνευση και οπτικοποίηση σημάτων, προκαλεί κβαντικές συμπεριφορές, καθιστώντας, έτσι, τα άτομα Rydberg κατάλληλους υποψήφιους για την πραγματοποίηση της κατασκευής κβαντικού υπολογιστή και κατ'επέκταση πειραμάτων κβαντικής προσομοίωσης. Το 2010, μάλιστα, σύμφωνα με τους ερευνητές,

σημειώθηκε μεγάλη πρόοδος στην ευρύτερη επιστημονική κοινότητα, καθώς επιτεύχθηκαν πειραματικά με τη βοήθεια των ατόμων αυτών οι πύλες δύο qubit, ενώ η ομάδα του SEDD τα μελετά εντατικά και για χρήση στα κβαντικά δίκτυα.

Αναλυτικότερα, οι αλληλεπιδράσεις των ατόμων Rydberg προσφέρουν δυνατότητες εκμετάλλευσής τους ακόμη και σε υπεραγωγούς για κυκλώματα μικροκυμάτων. Μια σύζευξη ατόμων Rydberg μπορεί να παρέχει μια σημαντική διεπαφή για πληροφορίες σε τέτοιου είδους κυκλώματα, καθώς τα άτομα Rydberg μπορούν να συλλάβουν οπτικές πληροφορίες και να τα τροφοδοτήσουν με αυτές. Η τεχνική αυτή εφαρμόζεται πλέον με επιτυχία στις στοιχειώδεις λογικές πύλες κβαντικού υπολογισμού, αλλά και σε δίκτυα κινητής τηλεφωνίας, βελτιώνοντας σημαντικά την απόδοσή τους.

Τα Rydberg excitons, από την άλλη πλευρά, μοιράζονται τις εκπληκτικές ιδιότητες των καταστάσεων ατόμων και μορίων Rydberg, ενώ η φύση της στερεάς τους κατάστασης τους προσδίδει πολύ πιο εύκολη και ταχύτερη τεχνολογική εκμετάλλευση.

Οι ισχυρές αλληλεπιδράσεις μεταξύ δύο ατόμων που διεγείρονται σε καταστάσεις Rydberg προέρχονται από την ανταλλαγή εικονικών φωτονίων μεταξύ τους. Το αποτέλεσμα είναι μια μεταφορά κατάστασης και ενέργειας μεταξύ των ατόμων. Συνεπώς, αυτός ο τύπος αλληλεπίδρασης κλιμακώνεται με τον κύριο κβαντικό αριθμό.

Συνήθως, απασχολούν οι αλληλεπιδράσεις με αποστάσεις πολύ μικρότερες από το μήκος κύματος των φωτονίων που μεσολαβούν στην αλληλεπίδραση. Για παράδειγμα, ισχυρές αλληλεπιδράσεις μεταξύ ατόμων Rydberg με n = 60 συμβαίνουν, συνήθως, σε αποστάσεις έως και μm, ενώ το μήκος κύματος της ακτινοβολίας που προκαλεί αυτήν την αλληλεπίδραση είναι 1 mm.

Οι νέες τεχνολογίες ήταν ζωτικής σημασίας για την προώθηση της έρευνας όσον αφορά την ανίχνευση και τη μελέτη των καταστάσεων Rydberg, καθώς χωρίς αυτές πολλά επιτεύγματα δεν θα ήταν δυνατά ή θα ήταν σημαντικά πιο περίπλοκα. Χάρις την τεχνολογία λέιζερ, για παράδειγμα, τις τελευταίες δεκαετίες έχει καταστεί δυνατή η ελεγχόμενη διέγερση επιλεγμένων ατόμων Rydberg, ενώ για την ανίχνευση έχουν αναπτυχθεί μέθοδοι με βάση τη φασματοσκοπία με λέιζερ, όπως η τεχνική της ηλεκτρομαγνητικά επαγόμενης διαφάνειας.

Οι αισθητήρες Rydberg έχουν ήδη αποδείξει την αποτελεσματικότητά τους, παρόλα αυτά χρησιμοποιούνται, κυρίως, μέχρι στιγμής, για γενικές εφαρμογές ανίχνευσης

ηλεκτρικού πεδίου. Την ίδια στιγμή, η πειραματική πρόοδος, οι νέες θεωρητικές ιδέες και οι τεχνολογικές εξελίξεις συνεχίζονται με ταχύ ρυθμό, τροφοδοτώντας ο ένας τον άλλον σε μια προσπάθεια βελτίωσης της ευαισθησίας τους, ώστε να κατορθώσουν να αποκρυπτογραφήσουν πιο αδύναμα σήματα καθώς και περίπλοκες κυματομορφές.

Παρόμοια έρευνα έχει αρχίσει, μάλιστα, να εμφανίζεται και από ερευνητές σε όλο τον κόσμο, καθώς, όπως οι ίδιοι δηλώνουν, υπάρχει ακόμη τεράστιο ανεκμετάλλευτο δυναμικό, αλλά και νέες τεχνολογικές δυνατότητες εξερεύνησης, όσον αφορά την καλύτερη ευαισθησία από αυτούς τους αισθητήρες, γεγονός που προκαλεί στην ερευνητική κοινότητα ενθουσιασμό για το τι ακόμη θα μπορούσε να επιτρέψει αυτή η ανακάλυψη.

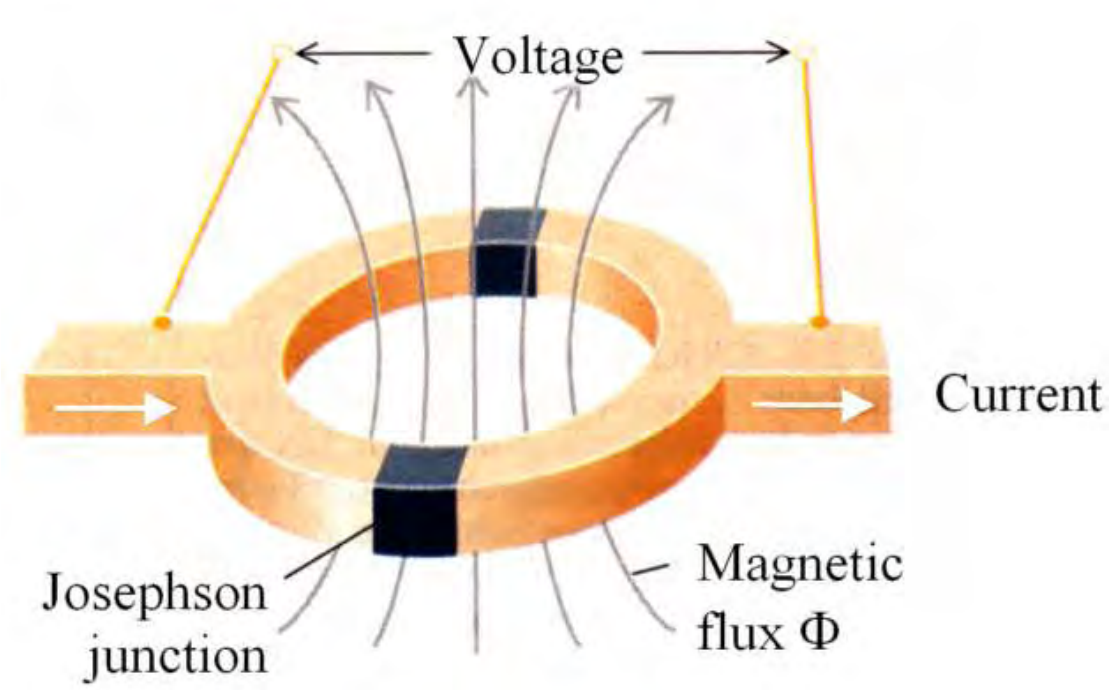
Θα μπορούσε, για παράδειγμα, να εξοπλίσει τους μελλοντικούς στρατιώτες με πιο ακριβείς αισθητήρες που λειτουργούν με λιγότερο θόρυβο και περιορίζουν τον ογκώδη εξοπλισμό τους, φέρνοντας, με αυτόν τον τρόπο, επανάσταση σε κρίσιμες δυνατότητες, όπως η χρονομέτρηση και η ανίχνευση μαγνητικού πεδίου. Γενικότερα, όπως επισημαίνει η στρατιωτική ερευνητική ομάδα, αυτή η ανακάλυψη θα υποστηρίξει τις προσπάθειες εκσυγχρονισμού του στρατού σε δίκτυα υπολογιστών επόμενης γενιάς, πλοήγηση και συγχρονισμό, καθώς θα μπορούσε, ενδεχομένως, να επηρεάσει νέες μορφές επικοινωνιών, αλλά και να υποστηρίξει νέες δυνατότητες σε παραδοσιακούς χώρους εφαρμογής, όπως οι επικοινωνίες ραδιοσυχνοτήτων.

Από το 2000, η ερευνητική προσπάθεια κατευθύνεται, κυρίως, σε εφαρμογές που απευθύνονται σε τρεις τομείς: ανίχνευση, κβαντική οπτική και κβαντική προσομοίωση, ενώ παράλληλα προσπαθούν να εντοπίσουν και άλλους τομείς στους οποίους οι αισθητήρες Rydberg θα μπορούσαν να χρησιμεύσουν, ιδιαίτερα στο στρατό. Συγκεκριμένα, για να γίνει αυτή η τεχνολογία πραγματικότητα, υπάρχουν πολλά βήματα ακόμη που πρέπει να πραγματοποιηθούν, μιας και εξακολουθούν να υπάρχουν πάρα πολλά θεμελιώδη επιστημονικά ερωτήματα σχετικά με αυτούς που πρέπει να απαντηθούν, όμως οι μηχανικοί του στρατού πιστεύουν ότι αυτή η τεχνολογία θα αποδειχθεί ισχυρό εργαλείο.

Υπεραγώγιμοι Αισθητήρες Κβαντικής Παρεμβολής (SQUID)

Η συσκευή υπεραγώγιμης κβαντικής παρεμβολής (SQUID-Superconducting Quantum Interference Device) είναι ένας εξαιρετικά ευαίσθητος μαγνητικός αισθητήρας που

αποτελείται από ένα μικροσκοπικό υπεραγώγιμο δακτύλιο και μία ή περισσότερες διασταυρώσεις Josephson.



Εικόνα 36: SQUID

Πηγή: https://www.sjsu.edu/people/raymond.kwok/courses/physics/phys120s-lab/squid/

Χρησιμοποιούνται για τη μέτρηση εξαιρετικά ασθενών μαγνητικών πεδίων και βρίσκουν εφαρμογή σε πολυάριθμους τομείς, μέχρι την κατασκευή υπερευαίσθητων τηλεσκοπίων και ανιχνευτών σκοτεινής ύλης, μιας και έχουν εντοπίσει πεδία από πράγματα τόσο μακρινά όσο οι ηλιακές εκλάμψεις. Δεδομένου ότι η απόδοση της SQUID βελτιώνεται και σταθεροποιείται, τώρα είναι έτοιμη και για περαιτέρω εφαρμογές.

Συγκεκριμένα, μια πιθανή στρατιωτική εφαρμογή της αφορά τη χρήση της στον αντι-υποβρύχιο πόλεμο ως ανιχνευτής μαγνητικών ανωμαλιών (MAD) που ενεργοποιείται από το μεταλλικό κύτος του υποβρυχίου, προσαρμοσμένη σε αεροσκάφη θαλάσσιας περιπολίας. Η απειλή που προκαλούν οι MAD έχει οδηγήσει στην προτίμηση υποθαλάσσιων σκαφών de-gauss (εξουδετέρωσης μαγνητικών πεδίων) για την ελαχιστοποίηση των μαγνητικών προφίλ. Η Γερμανία, μάλιστα, έχει αναπτύξει ειδικά υποβρύχια με μη μεταλλικά κύτη. Ωστόσο, οι MAD έχουν πολύ μικρό εύρος.

Στις 21 Ιουνίου 2017, ένα κινέζικο περιοδικό ανήγγειλε ότι ο καθηγητής XIamong Xie είχε αναπτύξει κρυογόνο SQUID με ψύξη υγρού αζώτου που μείωνε το πρόβλημα του

θορύβου και στις δοκιμές πεδίου είχε αποδειχθεί ικανό στην ανίχνευση σιδηρούχων αντικειμένων βαθιά κάτω από το έδαφος, ακόμη και όταν είναι τοποθετημένα μέσα σε ελικόπτερο.

Ο επιστημονικός δημοσιογράφος Dave Hambling σημείωσε στο New Scientist ότι ο νέος αισθητήρας του Xiamong χρησιμοποίησε μια δικτυωμένη σειρά SQUID για να επιτύχει να ακυρώσει το θόρυβο του περιβάλλοντος. Αν και υπήρξε μια αναταραχή ενδιαφέροντος, μετά από ένα άρθρο της Νότιας Κίνας στη Morning Post, όπου εξέφρασε το σκεπτικό του κατά πόσο ανήλθε "στον πιο ισχυρό ανιχνευτή υποβρυχίων στον κόσμο" αλλά και από τη συζήτηση των στρατιωτικών εφαρμογών της ανακάλυψης από δημοσιογράφους, η σχετική ανακοίνωση ανακλήθηκε και το αρχικό άρθρο καταργήθηκε. Αποτέλεσε, όμως, τουλάχιστον θεωρητικά, ένα βήμα προς την επιτυχή λειτουργία της τεχνολογίας.

Οι ερευνητές εκτιμούν ότι ένα μαγνητόμετρο SQUID αυτού του τύπου θα μπορούσε να ανιχνεύσει από 6 χιλιόμετρα μακριά, ενώ ο ερευνητής του Imperial College David Caplin λέει ότι με καλύτερη καταστολή θορύβου η ανιχνεύσιμη περιοχή θα μπορούσε να είναι πολύ μεγαλύτερη. Ένας τυπικός MAD, αντίθετα, είναι αποτελεσματικός μόνο σε μερικές εκατοντάδες μέτρα, ενώ τα ατομικά μαγνητόμετρα SERF που εφευρέθηκαν πρόσφατα είναι πιθανώς πιο ευαίσθητα και δεν απαιτούν ψύξη, αλλά είναι μεγαλύτερου μεγέθους (~ 1 cm3) και πρέπει να λειτουργούν σε σχεδόν μηδενικό μαγνητικό πεδίο.

Αναλυτικότερα, το να γνωρίζει κανείς πού είναι άλλα υποβρύχια, σκάφη και αεροσκάφη είναι κρίσιμο στον τομέα της άμυνας. Ο παραδοσιακός τρόπος για ένα βυθισμένο υποβρύχιο για τη συλλογή τέτοιων δεδομένων είναι με ακουστικά μέσα. Όμως, χάρη στον εξέχοντα ρόλο που έπαιξε το σόναρ εδώ και δεκαετίες, κλασικές συσκευές έχουν αναπτυχθεί παράλληλα με τεχνικές ησυχίας για να αφήνουν επιθετικές και αμυντικές δυνατότητες σε σκληρή ισορροπία. Συνεπώς, απαιτούνται άλλες μέθοδοι εύρεσης υποβρυχίων.

Οι ανιχνευτές μαγνητικών ανωμαλιών που παίρνουν τη μαγνητική υπογραφή ενός υποβρυχίου υπήρχαν εδώ και δεκαετίες. Δεν ήταν ποτέ συσκευές μεγάλης εμβέλειας και ως επί το πλείστον θεωρήθηκαν ως τρόπος εντοπισμού ενός υποβρυχίου η γενική θέση του οποίου είχε καθοριστεί με άλλα μέσα. Σήμερα, το πραγματικό εύρος δεν υπερβαίνει μερικές εκατοντάδες μέτρα και, επειδή η ισχύς του μαγνητικού πεδίου

μειώνεται με την απόσταση, χρειάζονται πολύ πιο ακριβείς ανιχνευτές για την επέκταση αυτού του εύρους.

Για την ακριβή μέτρηση των μαγνητικών πεδίων, μεταξύ των πρώτων κβαντικών συσκευών ήταν οι υπεραγώγιμες συσκευές κβαντικής παρεμβολής, οι οποίες αναπτύχθηκαν τη δεκαετία του 1960. Οι SQUID είναι τόσο ακριβείς στη μέτρηση μικροσκοπικών μαγνητικών πεδίών, που, για να καταλάβει κανείς καλύτερα τι σημαίνει αυτό, θα μπορούσαν να ανιχνεύσουν ένα μαγνήτη ψυγείου από 1,5 χιλιόμετρο μακριά, εάν ήταν απομονωμένος από άλλα εξωτερικά πεδία. Η ανίχνευση τέτοιων εξαιρετικά μικρών μαγνητικών πεδίων θα μπορούσε να χρησιμοποιηθεί εκτός από την παρακολούθηση υποβρυχίων, στην ανίχνευση κρυφών μεταλλικών αντικειμένων μέσω ενός τοίχου.

Στην περίπτωση της μέτρησης του μαγνητικού πεδίου, το κύκλωμα ανίχνευσης έχει σχεδιαστεί για τη μέτρηση του μαγνητικού πεδίου (μαγνητόμετρο) ή της διαβάθμισής του (βαθμιδόμετρο). Και στις δύο περιπτώσεις, πάντως, αποτελείται από ένα πηνίο παραλαβής και ένα πηνίο εισόδου που συνδέεται επαγωγικά με το δακτύλιο της SQUID.

Για να ευθυγραμμιστεί η απόκριση της SQUID, χρησιμοποιείται συχνά μια Flux-Locked-Loop (FLL), όπου η έξοδος μετατρέπεται σε ρεύμα από μια αντίσταση και τροφοδοτείται ξανά στη SQUID, μέσω ενός πηνίου που συνδέεται με τον αισθητήρα, ακυρώνοντας τη μαγνητική ροή εισόδου. Έτσι, η SQUID λειτουργεί ως ανιχνευτής μηδενικής μαγνητικής ροής.

Τα παραδοσιακά υπεραγώγιμα υλικά για SQUID είναι καθαρό νιόβιο ή κράμα μολύβδου με 10% χρυσό ή ίνδιο, καθώς ο καθαρός μόλυβδος είναι ασταθής όταν η θερμοκρασία του αλλάζει επανειλημμένα. Για να διατηρηθεί η υπεραγωγιμότητά τους, ολόκληρη η συσκευή πρέπει να ψύχεται με υγρό, συνήθως, ήλιο κοντά στο απόλυτο μηδέν.

Οι συσκευές αυτές αποτέλεσαν βασικό παράγοντα στην ανάπτυξη και εμπορευματοποίηση υπερευαίσθητων ηλεκτρικών και μαγνητικών συστημάτων μέτρησης. Σε πολλές περιπτώσεις, προσφέρουν τη δυνατότητα πραγματοποίησης μετρήσεων όπου δεν είναι δυνατή καμία άλλη μεθοδολογία. Εκτός από τη μέτρηση μαγνητικών πεδίων, οι αισθητήρες SQUID μπορούν να διαμορφωθούν για να

μετρήσουν μια μεγάλη ποικιλία ηλεκτρομαγνητικών ιδιοτήτων με ευαισθησίες, οι οποίες κυμαίνονται από τα επίπεδα microtesla έως picotesla.

Οι SQUID μπορούν να χρησιμοποιηθούν σε βολτόμετρα, σε αισθητήρες μέτρησης περιστροφών (CNT-SQUID) αλλά και ως αισθητήρες κίνησης ακριβείας σε μια ποικιλία επιστημονικών εφαρμογών, όπως η ανίχνευση βαρυτικών κυμάτων. Η SQUID, συγκεκριμένα, ήταν ο αισθητήρας σε καθένα από τα τέσσερα γυροσκόπια που χρησιμοποιήθηκαν στο πείραμα Gravity Probe B προκειμένου να δοκιμαστούν τα όρια της θεωρίας της σχετικότητας.

Οι προηγμένες SQUID αποτελούν, επίσης, τη βάση για τον κβαντικό υπολογιστή D-Wave Systems 2000Q αλλά και του πειράματος Axion Dark Matter (ADMX) στο Πανεπιστήμιο της Ουάσιγκτον, όπου τα Axions είναι οι πρώτοι υποψήφιοι για τη μελέτη της σκοτεινής ύλης.

Τέλος, λόγω των μοναδικών ιδιοτήτων τους, χρησιμοποιούνται ευρέως σε εφαρμογές όπως η νανοεπιστήμη και σε πρόσφατα ενδιαφέροντα βασικά φυσικά πειράματα όπως η ακτινοβολία Hawking, δυναμικό φαινόμενο Casimir, fermions Majorana, εφέ Sunyaev-Zeldovich κ.α..

Ωστόσο, παρόλο που οι εφαρμογές τους συζητούνται σε επιστημονικούς και εθνικούς κύκλους ασφαλείας, η τεχνολογία SQUID παραμένει προβληματική από επιχειρησιακή άποψη. Η ακρίβεια της συσκευής έρχεται αντιμέτωπη με το ¨κόστος¨ της ευκολίας. Για να ανιχνεύσει κανείς το μαγνήτη ψυγείου στην απόσταση που προαναφέρθηκε, θα πρέπει να λάβει μετρήσεις για αρκετές ημέρες. Αυτό δεν αποτελεί πρόβλημα αν το θέμα αφορά τη θεμελιώδη επιστήμη, αλλά είναι λιγότερο χρήσιμο εάν η συσκευή προορίζεται να παρέχει τακτικά δεδομένα σε πραγματικό χρόνο. Οι SQUID, ακόμη, πρέπει να ψύχονται σε εξαιρετικά χαμηλές θερμοκρασίες, κάτι που είναι δύσκολο να γίνει έξω από το εργαστήριο. Το μαγνητικό πεδίο της Γης, επιπλέον, πρέπει να φιλτραριστεί. Αυτό είναι απλό σε μαγνητικά θωρακισμένους χώρους, αλλά πιο δύσκολο εάν τα πεδία που πρέπει να εντοπιστούν βρίσκονται έξω από το ελεγχόμενο περιβάλλον. Όλα αυτά γίνονται ακόμα πιο δύσκολα όταν το σύστημα μέτρησης βρίσκεται εν κινήση.

Για τους λόγους αυτούς, οι SQUID δεν είναι από τις πιο πολλά υποσχόμενες σύγχρονες κβαντικές τεχνολογίες για την ανίχνευση μαγνητικών πεδίων. Εάν τα ομολογουμένως σημαντικά αυτά προβλήματα μπορούν να ξεπεραστούν, οι ανιχνευτές μαγνητικών

ανωμαλιών που χρησιμοποιούν SQUID έχουν τη δυνατότητα να ανιχνεύσουν αντικείμενα καλύπτοντας ακόμα και χιλιάδες φορές περισσότερα τετραγωνικά μέτρα από τα κλασικά αντίστοιχου σκοπού μαγνητόμετρα.

ΚΒΑΝΤΙΚΟ ΡΑΝΤΑΡ

Γενικά

Από τον πρώτο καιρό ανάπτυξης και χρήσης του συμβατικού ραντάρ, κατά τη διάρκεια του Β Παγκοσμίου Πολέμου, άρχισαν και οι πρώτες προσπάθειες για την κατασκευή αεροσκαφών τεχνολογίας stealth, δηλαδή μη ανιχνεύσιμων. Στις μέρες μας, όπου η τεχνολογία stealth είναι γεγονός, η πορεία της έρευνας έχει στραφεί προς την κατεύθυνση του σχεδιασμού και κατασκευής των πλέον προηγμένων τύπων ραντάρ.

Η τεχνολογία ραντάρ αποτελεί σημαντικό εργαλείο για τον πόλεμο, αφού χρησιμοποιείται για την παρακολούθηση του ηλεκτρομαγνητικού φάσματος, για την ανίχνευση και παρακολούθηση εχθρικών αεροσκαφών, πυραύλων, δορυφόρων και άλλων συστημάτων που με τη σειρά τους έχουν γίνει πιο εξελιγμένα στην αποφυγή της ανίχνευσης.

Η οικοδόμηση καλύτερων, πιο ευαίσθητων και πιο δύσκολο να εντοπιστούν συστημάτων ραντάρ αποτέλεσε προτεραιότητα για τους αμυντικούς κατασκευαστές, ειδικά, από τον Οκτώβριο του 2018 που το Πολεμικό Ναυτικό των ΗΠΑ όρισε το ηλεκτρομαγνητικό φάσμα ως πεδίο μάχης που αντιστοιχεί στη θάλασσα, τη γη, τον αέρα, το διάστημα και τον κυβερνοχώρο. Έπρεπε να αναπτυχθεί μια συσκευή, η οποία, εκτός των άλλων, θα είχε τη δυνατότητα να αναμετρηθεί με την τεχνολογία stealth.

Το κύριο πλεονέκτημα των πολεμικών αυτών αεροσκαφών πέμπτης γενιάς, που αναπτύχθηκαν στα τέλη του 20ου αιώνα, είναι το ότι εμφανίζουν ένα απειροελάχιστο ίχνος στις οθόνες των ραντάρ και αυτό όταν κινούνται πολύ αργά και γύρω στα 30 χιλιόμετρα απόσταση. Αυτό συμβαίνει εξαιτίας του ειδικού σχεδιασμού της κατασκευής τους που αποτελείται από πολλά επίπεδα, γωνίες και προσπίπτουσες επιφάνειες, ώστε να εκμεταλλεύεται την ιδιότητα των ηλεκτρομαγνητικών κυμάτων να ανακλώνται και να μην επιστρέφουν πίσω στον αποστολέα, αλλά να μεταπηδούν σε διαφορετική κατεύθυνση, καθιστώντας τα έτσι κυριολεκτικά αόρατα ή τουλάχιστον πολύ μικρότερα από ό, τι είναι πραγματικά, αφού λιγότερα φωτόνια επιστρέφουν στον ανιχνευτή.

Οι κατασκευαστές τους, όπως η αμερικανική Lockheed Martin, γνώριζαν ότι πολύ σύντομα δεν θα ήταν οι μόνοι κάτοχοι αυτής της τεχνολογίας, καθώς ανάλογα αεροσκάφη ετοίμαζαν και οι στρατηγικοί αντίπαλοι των Ρωσία και Κίνα. Έπρεπε

λοιπόν να αναπτύξουν ένα ραντάρ που θα μπορούσε να τα ανιχνεύσει έγκαιρα. Εννοείται, βέβαια, ότι το όποιο εύρημά της θα έπρεπε να παραμείνει μυστικό ως τεχνολογία για να μην αχρηστευθεί το ήδη υπάρχον επίτευγμα.

Σύμφωνα με τον Ned Allen, τον επικεφαλή επιστήμονα της Lockheed Martin, η πρώτη προσέγγιση για τη λύση του προβλήματος έγινε περίπου το 2002, με τη Lockheed να αναφέρεται στο πρόβλημα μειωμένης αξιοπιστίας των συμβατικών ραντάρ για μακρινούς στόχους, καθώς και στο γεγονός ότι αδυνατούν να εντοπίσουν στόχους που έχουν μικρή ανακλαστικότητα (πχ αεροσκάφη σχεδίασης stealth) ή στόχους που βρίσκονται μέσα σε ισχυρό περιβάλλον θορύβου.

Ακόμη, τα κλασσικά ραντάρ μπορούν να εντοπίζουν αντικείμενα με μεγάλη ευκολία, αλλά παρέχουν πολύ λίγες λεπτομέριες για αυτά. Μπορούν να προσδιορίσουν το ύψομετρο, την κατεύθυνση και την απόσταση, αλλά κατά τα άλλα ο στόχος είναι μια άμορφη μάζα. Οι υπερασπιστές του αέρα αλλά και η αεράμυνα γενικότερα πρέπει να βασιστούν και σε άλλα στοιχεία, όπως για παράδειγμα το ραντάρ αναγνώρισης και άλλα ηλεκτρομαγνητικά σήματα που μπορεί να προέρχονται από το στόχο, ώστε να διακρίνουν αν αυτή η μάζα αντιστοιχεί σε εχθρικό μαχητικό αεροσκάφος, βομβαρδιστικό ή ακόμη και πολιτικό. Τα προβλήματα αυτά, σύμφωνα με τη Lockheed, θα ήταν δυνατό να επιλυθούν με διεμπλοκή των κυμάτων των ραντάρ.

Είναι γνωστό άλλωστε, ότι ένα από τα πλεονεκτήματα της κβαντικής επανάστασης είναι η ικανότητά της να αντιλαμβάνεται τον κόσμο με νέους τρόπους, χρησιμοποιώντας τις ιδιότητες του κβαντικού χώρου για να δημιουργήσει κβαντικούς αισθητήρες και συστήματα ανίχνευσης που είναι εκατομμύρια φορές πιο ευαίσθητα από οτιδήποτε έχουμε σήμερα. Για τους περισσότερους ερευνητές η γενική ιδέα πίσω από τη χρήση της κβαντικής μηχανικής είναι να χρησιμοποιήσει τις ειδικές ιδιότητές της για να πραγματοποιήσει μετρήσεις που διαφορετικά είναι αδύνατες, με ένα παράδειγμα να είναι το κβαντικό αυτό ραντάρ, στο οποίο αναφέρεται η Lockheed, ένα νέο είδος συστήματος ραντάρ που βασίζεται στις αρχές του φαινομένου του κβαντικού φωτισμού, της διαδικασίας, δηλαδή, απομόνωσης ζευγών εμπλεκόμενων φωτονίων και έχει τη δυνατότητα να καταστήσει όλη την τεχνολογία κρυφών αντικειμένων απαρχαιωμένη.

Τι είναι το Κβαντικό Ραντάρ;

Αρχικά γιατί ¨κβαντικό¨; Πότε μια τεχνολογία γίνεται ¨κβαντική¨; Για τον OSA Fellow Miles Padgett, οπτικό φυσικό στο Πανεπιστήμιο της Γλασκόβης στο Ηνωμένο Βασίλειο, ο ορισμός θα πρέπει, αυστηρά, να συνεπάγεται εμπλοκή. Αλλά υποστηρίζει ότι η τεχνική θα πρέπει, ακόμα, να θεωρηθεί ως κβαντική δεδομένου ότι βασίζεται στην ανίχνευση μεμονωμένων φωτονίων. "Από την άποψη της γενικότερης τεχνολογίας," λέει, "μόλις αρχίσετε να μετράτε μεμονωμένα φωτόνια ή μεμονωμένα άτομα, μιλάμε για κβαντική τεχνολογία".

Το κβαντικό ραντάρ, λοιπόν, είναι ένας απομακρυσμένος ως προς το στόχο τύπος κβαντικού αισθητήρα υψηλής ευκρίνειας. Το κίνητρο πίσω από την πρόταση σχεδιασμού και υλοποίησής του δεν είναι άλλο από την αύξηση της ευαισθησίας του συστήματος και τη βελτίωση των δυνατοτήτων ανίχνευσης, ανάλυσης και ταυτοποίησης των στόχων.

Το κβαντικό ραντάρ είναι σε θέση να ανιχνεύσει αντικείμενα με πολύ μεγαλύτερο επίπεδο ακρίβειας από το συμβατικό ραντάρ. Θα μπορούσε να παρέχει στους χρήστες τόσο λεπτομερείς αναλύσεις, ώστε να μπορούν να αναγνωρίσουν το ακριβές μοντέλο των αεροσκαφών, πυραύλων αλλά και όποιου άλλου είδους εναέριου στόχου εντοπίζει, βασιζόμενο στα φυσικά τους χαρακτηριστικά. Το γεγονός μάλιστα ότι μπορεί να ανιχνεύσει και αεροσκάφη τύπου stealth, το καθιστά ελκυστικό υποψήφιο για την παρακολούθηση πάσης φύσεως αντικειμένων μυστικότητας. Σύμφωνα με τρεις ειδικούς στο θέμα, που ρωτήθηκαν από το Institution of Engineering and Technology, οι ¨αντί stealth¨ ισχυρισμοί που το χαρακτηρίζουν είναι μια χονδροειδής απλοποίηση του ζητήματος.

Όλα τα κλασικά ραντάρ εκπέμπουν ηλεκτρομαγνητική ακτινοβολία υψηλής ενέργειας για να εντοπίσουν ιπτάμενα αντικείμενα. Αυτή η ακτινοβολία, επειδή είναι εντοπίσιμη, κάνει και το ίδιο το ραντάρ ανιχνεύσιμο. Είναι σα να κρατά κάποιος φακό σε ένα σκοτεινό δωμάτιο. Ανάβοντας το φακό θα μπορεί να δει τι υπάρχει στο δωμάτιο, αλλά την ίδια στιγμή η δέσμη του φωτός οδηγεί κατευθείαν πίσω και κάνει και τον εαυτό του ορατό σε άλλους που πιθανόν να βρίσκονται μέσα στο ίδιο δωμάτιο, χαρίζοντάς τους πέρα από την παρουσία και την τοποθεσία του.

Η μη εντοπισιμότητα, λοιπόν, προσδίδει σαφές πλεονέκτημα σε συνθήκες πολέμου. Ένα κβαντικό ραντάρ θα μπορέσει να εντοπίσει μια ομάδα εχθρικών αεροσκαφών χωρίς να αποκαλύψει τη δική του παρουσία, καθώς χρησιμοποιεί σχετικά χαμηλή ισχύ εκπεμπόμενης ακτινοβολίας, επιτρέποντας έτσι στο ίδιο να κρύβεται πίσω από το θόρυβο του φόντου και οι χειριστές του να παραμένουν κρυφοί. Το γεγονός ότι δεν εκτίθεται το ίδιο θα έκανε τα εχθρικά πολεμικά αεροσκάφη να απενεργοποιήσουν τα συστήματα αυτοπροστασίας και παρεμβολής που διαθέτουν, κάτι το οποίο θα μπορούσε να γίνει άμεσα αντιληπτό από τους υπερασπιστές. Με τις άμυνες τους απενεργοποιημένες, τα εχθρικά μαχητικά θα μπορούσαν να πέσουν σε ενέδρα μαχητικών και συστημάτων αεράμυνας, αφού, πλέον, έχουν καταστεί ορατά σε αυτούς.

Η τεχνολογική αυτή ανακάλυψη, επομένως, προσδοκάται προς ικανοποίηση πληθώρας απαιτήσεων τόσο σχετικά με την έγκαιρη ανίχνευση και ταυτοποίηση των εχθρικών στόχων, προσφέροντας υψηλότερη ανάλυση και ακρίβεια επί των μετρούμενων φυσικών μεγεθών, όσο και με την ανίχνευση και ενδεχομένως εξουδετέρωση κακόβουλων σημάτων παρεμβολής (jamming), καθιστώντας το ιδανικό εργαλείο για μια ποικιλία εφαρμογών σε τομείς και συστήματα ασφαλείας. Είναι μια πολλά υποσχόμενη τεχνολογία που θα μπορούσε να έχει ισχυρό αντίκτυπο στην πολιτική και στρατιωτική σφαίρα. Στο πεδίο μάχης, συγκεκριμένα, μπορεί να γίνει μια επαναστατική τεχνολογία, όπως ακριβώς και η τεχνολογία stealth τις τρεις τελευταίες δεκαετίες του 20ού αιώνα και να αλλάξει ολοσχερώς τη φύση των συρράξεων.

Πώς λειτουργεί;

Όλα τα συστήματα ραντάρ στοχεύουν στον εντοπισμό και την παρακολούθηση στόχων χρησιμοποιώντας ηλεκτρομαγνητική ενέργεια. Τα κβαντικά ραντάρ λειτουργούν παρόμοια με τα κλασικά ραντάρ, αλλά αντί για ραδιοκύματα, εκπέμπουν ζευγάρια κβαντικά εναγκαλισμένων φωτονίων, δηλαδή η ιδέα τους αξιοποιεί το παράξενο φαινόμενο της κβαντικής διεμπλοκής.

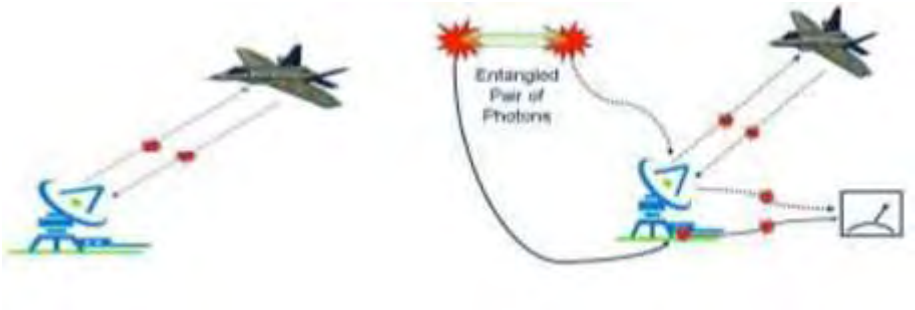
Για την ακρίβεια, υπάρχουν δύο τύποι κβαντικού ραντάρ, εκπομπής μεμονωμένων φωτονίων και εκπομπής σύμπλεκτων καταστάσεων φωτονίων. Στην παρούσα ενότητα γίνεται αναφορά στη δεύτερη μόνο κατηγορία.

Στην κατάσταση της κβαντικής διεμπλοκής, επομένως, όπως είναι γνωστό, δύο φωτόνια ή άλλα υποατομικά σωματίδια συνδέονται μεταξύ τους με άρρηκτη σχέση,

ανεξάρτητα από το πόσο μακριά βρίσκονται. Οποιαδήποτε αλλαγή, επομένως, στις κβαντικές ιδιότητες του ενός σωματιδίου μεταβάλλει ακαριαία την κατάσταση του άλλου σωματιδίου. Είναι το μόνο φαινόμενο στη φύση που καταλύει την αρχή της τοπικότητας (locality - τα μέρη που σχετίζονται μεταξύ τους πρέπει να βρίσκονται σχετικά κοντά).

Το κλασικό ραντάρ λειτουργεί στέλνοντας μια δέσμη ακτινοβολίας σε συχνότητες ραδιοφώνου ή μικροκυμάτων και μέσω ενός δέκτη που ανιχνεύει αντανακλάσεις από οποιαδήποτε αντικείμενα στη διαδρομή του σήματος, προκειμένου να υπολογίσει τη θέση και την ταχύτητά τους. Σε χαμηλά επίπεδα ισχύος, όμως, που περιλαμβάνουν μικρό αριθμό φωτονίων μικροκυμάτων, δεν είναι τόσο ευαίσθητο με αποτέλεσμα να αποτυγχάνει.

Στο κβανικό ραντάρ, το ένα από τα σωματίδια του ζεύγους των εμπλεγμένων φωτονίων εκπέμπεται υπό τη μορφή μικροκυμάτων, ενώ το άλλο παραμένει στο σύστημα για παρατήρηση. Το σωματίδιο που ακτινοβολήθηκε θα συμπεριφερθεί με συγκεκριμένο τρόπο καθώς θα έρχεται σε επαφή με αντικείμενα και επιφάνειες. Αυτή η συμπεριφορά μπορεί να παρατηρηθεί μελετώντας το κρατημένο σωματίδιο. Εξετάζοντας το δεύτερο σωματίδιο, για παράδειγμα, το ραντάρ θα μπορούσε να υπολογίσει αν το πρώτο φωτόνιο συνάντησε κάποιο αντικείμενο στην πορεία του (π.χ. ένα αεροσκάφος) και να το χρησιμοποιήσει για να παρακολουθήσει αυτό το αντικείμενο. Αξίζει να σημειωθεί ότι τα φωτόνια δεν επηρεάζονται από το σχήμα του αεροσκάφους και δεν είναι ευάλωτα σε αντίμετρα.



Εικόνα 37: Λειτουργία κβαντικού ραντάρ σύμπλεκτων φωτονίων
Πηγή:file:///C:/Users/gld/Desktop/%CE%A0%CE%A4%CE%A5%CE%A7%CE%99%CE%91%CE%9A%CE%97%20%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%99%CE%91/HNA-APNEO-QUANTUMTECS-REVIEW-2018.pdf

Αναλυτικότερα, μια δέσμη φωτός χωρίζεται σε δύο που είναι κβαντικά εναγκαλισμένες (συσχετισμένες, εμπλεγμένες, πεπλεγμένες), πράγμα που σημαίνει ότι οι καταστάσεις

των φωτονίων σε κάθε δέσμη συσχετίζονται απόλυτα όσο κι αν απέχουν μεταξύ τους. Όταν δύο έντονα συσχετισμένες δέσμες παρεμβάλλονται σε έναν ανιχνευτή, το σήμα ενισχύεται, παρέχοντας στο ραντάρ σημαντική βελτίωση επιπέδου ακρίβειας και αποτελεσματικότητας σε σύγκριση με τα αποτελέσματα από μη συσχετισμένες δέσμες συμβατικού ραντάρ. Η μία από τις δύο δέσμες, η οποία ονομάζεται αδρανές φωτόνιο, διατηρείται στο σύστημα, αλλά η άλλη, που ονομάζεται φωτόνιο σήματος, εκπέμπεται για να εντοπίσει πιθανό στόχο.

Εξετάζοντας το σωματίδιο που κρατήθηκε, το ραντάρ μπορεί να γνωρίζει αν το φωτόνιο που εξέπεμψε ήρθε σε επαφή με κρυφό στόχο στην πορεία του. Εάν συνάντησε όντως κάτι, αντανακλάται και ταξιδεύει πίσω στον ανιχνευτή. Επειδή είναι εμπλεγμένο, ο ανιχνευτής μπορεί να εντοπίσει, στο περίπου, το σημείο στο οποίο πήγε και να συνεχίσει να στέλνει περισσότερα φωτόνια έως ότου δημιουργηθεί μια εικόνα του αντικειμένου ενδιαφέροντος που βρίσκεται στην ατμόσφαιρα.

Είναι σημαντικό εδώ να διευκρινιστεί ότι η εμπλοκή δεν επιτρέπει σε ένα σωματίδιο να στέλνει σήματα στον εμπλεκόμενο σύντροφό του, όπως αναφέρουν πολλά άρθρα ειδήσεων. Η έκφραση "στοιχειωμένη δράση από απόσταση", λέει ο Lloyd, καθηγητής μηχανολογίας και φυσικής στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης, αναφερόμενος στη διάσημη απόρριψη του Einstein από τη θεωρία της κβαντικής εμπλοκής, είναι λίγο παραπλανητική. Αυτό που ο Αϊνστάιν είπε στην πραγματικότητα είναι λίγο διαφορετικό. Αυτό που έχει σημασία να γίνει κατανοητό είναι ότι αν εκπεμφθεί ένα εμπλεγμένο σωματίδιο, ό, τι και αν του συμβεί, δε θα μεταφέρει πληροφορίες στο σωματίδιο πίσω στο εργαστήριο με την έννοια που αντιλαμβάνεται κανείς.

Το ανακλώμενο φωτόνιο που επιστρέφει στο σταθμό, λοιπόν, συλλέγεται από το σύστημα, όπου και μετράται σε συνδυασμό με το κρατούμενο. Εκτελείται ένα “πείραμα συσχέτισης”, μια μέτρηση, δηλαδή, και στα δύο φωτόνια για να προσδιοριστεί αν είναι στην πραγματικότητα το φωτονίο που επιστρέφει ή απλά θόρυβος παρασκηνίου. Είναι ένα δύσκολο έργο, δεδομένου ότι το μεγαλύτερο μέρος του φωτός που συλλαμβάνεται από το δέκτη είναι θόρυβος.

Ακόμη, όμως, και αν η εμπλοκή μεταξύ των δύο δεσμών έχει διασπαστεί από τον υψηλό αυτό θόρυβο, από αντίξοες καιρικές συνθήκες, όπως ατμοσφαιρικούς στροβιλισμούς, ή από άλλου είδους παράγοντες και παρεμβολές, που είναι μια διαδικασία γνωστή ως «Decoherence», εξακολουθούν να παραμένουν κάποιες εναπομένουσες συσχετίσεις που μπορούν να διακριθούν.

Αυτό το γεγονός οξύνεται ιδιαίτερα σε μεγαλύτερα υψόμετρα, όπως οι περιοχές της Αρκτικής. Σε περιοχές όπως αυτές, τα stealth αεροσκάφη, τα οποία δεν αντανακλούν έτσι και αλλιώς πολύ φως, γίνονται μέρος αυτού του θορύβου.

Χάρις το κβαντικό φαινόμενο της εμπλοκής, όμως, ακόμη και εάν το σύστημα λειτουργεί σε τέτοιες περιοχές με ισχυρές πηγές παρασκηνιακού θορύβου, είναι δυνατό να διακρίνει κανείς την ακτινοβολία που στάλθηκε από το βασικό σταθμό και αντανακλάται πίσω. Επιπλέον, καθίσταται δυνατός ο προσδιορισμός των αντανακλάσεων από το στόχο ακόμη και όταν η επιστροφή είναι εξαιρετικά αδύναμη και προέρχεται από ένα μακρινό στόχο, επιτρέποντας έτσι την ανίχνευση της παρουσίας ενός αντικειμένου με μικρότερη πιθανότητα σφάλματος. «Βασικά, αυτό που κάνει η κβαντική εμπλοκή είναι να βελτιώσει την αναλογία σήματος προς θόρυβο για μια δεδομένη ποσότητα ισχύος», λέει ο Lloyd.

Σύμφωνα μάλιστα και με τον εμπειρογνώμονα κβαντικών υπολογιστών, καθηγητή Alan Woodward του Πανεπιστημίου του Surrey, όταν ένα εμπλεγμένο φωτόνιο εκτοξεύεται, υπάρχει πολύ υψηλότερο επίπεδο βεβαιότητας ότι το φωτονίο που επιστρέφει στο σύστημα είναι στην πραγματικότητα ένα από αυτά που εκτοξεύτηκαν, σε αντίθεση με άλλα φωτόνια που απλά συνέβη να βρίσκονταν κοντά στο αντικείμενο ενδιαφέρονος εκείνη τη στιγμή.

Η διαδικασία αυτή ταυτοποίησης εξαλείφει την ανάγκη για σύνθετες συσκευές μικρο-σάρωσης, οι οποίες καθιστούν το σύστημα πολύ ακριβό, περίπλοκο και να εξαρτάται από τις μηχανικές ανοχές. Στην πραγματικότητα, αντί να σαρώνονται λεπτές γωνίες στο χώρο για να εξάγονται λεπτομέρειες του αντικειμένου, χρησιμοποιείται κβαντική μηχανική των μεμονωμένων φωτονίων για να σαρώνονται μικροσκοπικές γωνίες του χώρου με πιθανοτικό τρόπο. Τα φωτόνια ανακλώνονται τυχαία από διαφορετικά μέρη της επιφάνειας του στόχου με διαφορετικό χρόνο πτήσης και στη συνέχεια το σύστημα, μέσω ενός προγράμματος, δείχνει το ¨βάθος¨ του στόχου.

Το πιο σημαντικό πλεονέκτημα, όμως, αυτού του σχεδιασμού, είναι η ικανότητά του να διακρίνει μεταξύ των δολωμάτων και των πραγματικών στόχων, γεγονός στο οποίο συμβάλλει ο τρόπος με τον οποίο τα μεμονωμένα φωτόνια αλληλεπιδρούν με τις επιφάνειες που έρχονται σε επαφή.

Για να βρει εφαρμογή η συγκεκριμένη τεχνική στον κόσμο των ραντάρ, όμως, έπρεπε κάποιος να κατορθώσει να «δέσει» κβάντα πάνω σε μικροκύματα. Ο πρώτος που το κατάφερε ήταν ένας Ιταλός, ο Στέφανο Πιράντολα από το βρετανικό Πανεπιστήμιο του Γιορκ, με μια πολυεθνική ομάδα ερευνητών από πανεπιστήμια της Γερμανίας, των ΗΠΑ και του Καναδά, στις 16 Φεβρουαρίου 2015.

Την ιδέα την πήραν από τον αμερικανό καθηγητή του MIT Σεθ Λόιντ, ο οποίος είχε παρουσιάσει το 2008 την έννοια του «κβαντικού φωτισμού».

Το πείραμα του Πιράντολα πέτυχε και έτσι αποδείχτηκε για πρώτη φορά ότι είναι εφικτό να σαρώνεται ο ορίζοντας με κβαντικά μικροκύματα και να ειδοποιείται κανείς από τα δίδυμά τους κβάντα για το τί συνάντησαν, έστω κι αν αυτό είναι «μικροκυματικά αόρατο». Επιπλέον, προσέφερε το τεράστιο πλεονέκτημα του να φωτίζει κανείς το στόχο του με μια ελάχιστη ποσότητα ενέργειας, πράγμα που βελτιώνει πολύ την πιθανότητά να μη τον ανιχνεύσει το ραντάρ του στόχου. Ωστόσο, το πείραμα πέτυχε μόνο στο ορατό φάσμα του φωτός. Για να είναι εφικτό μια τέτοια διάταξη να αξιοποιηθεί στο φάσμα των κυμάτων που χρησιμοποιούν τα ραντάρ, έπρεπε να γίνει πολλή ακόμη δουλειά που κανείς δεν έδειχνε να γνωρίζει τα επόμενα βήματά της.

Πέρασε ενάμισης χρόνος, μέχρι τις 16 Αυγούστου 2016, όταν η Κίνα εκτόξευσε στο Διάστημα το Μόζι, τον πρώτο δορυφόρο κβαντικής επικοινωνίας. Σύμφωνα με την επίσημη ανακοίνωση, με αυτό το δορυφόρο οι ερευνητές του Πολυτεχνείου της Χεφέι θα δοκίμαζαν τη διεμπλοκή σε απόσταση 1.200 χιλιομέτρων, προκειμένου να διαπιστώσουν τη δυνατότητα αξιοποίησής της σε κρυπτογραφημένες τηλεπικοινωνίες. Ένα μήνα μετά, η κινεζική στρατιωτική βιομηχανία ηλεκτρονικού εξοπλισμού CETC ανέφερε και ένα επιπλέον κομμάτι δοκιμών. Είχαν ελέγξει με αποτελεσματικότητα το πρώτο κβαντικό ραντάρ της ανθρώπινης ιστορίας.

Το πώς ακριβώς το κατάφεραν παραμένει μυστικό. Δήλωσαν όμως ότι είναι τεχνολογίας «μοναδιαίου φωτονίου», άρα το ραντάρ τους θα είναι «άφαντο» για τα

επιτιθέμενα αεροσκάφη και η ακτίνα εντοπισμού των αεροσκαφών stealth θα φτάνει στα 100 χλμ. Σημειώνεται ότι, παραδοσιακά, οι ανακοινώσεις στρατιωτικής τεχνολογίας εμφανίζουν μειωμένες επιδόσεις, επομένως μπορεί κανείς να υποψιαστεί ανίχνευση η οποία ανέρχεται γύρω στα 150 χιλιόμετρα που αντιστοιχούν σε μια απόσταση χονδρικά 70 χιλιομέτρων.

Η ανάπτυξη ενός κβαντικού ραντάρ, συνεπώς, περιλαμβάνει κάποιες προκλήσεις. Απαιτεί την πρόταση ενός ρεαλιστικού φυσικού συστήματος για παραγωγή εξαιρετικά αξιόπιστων ρευμάτων σύμπλεκτων φωτονίων στη μικροκυματική περιοχή, μια πηγή, δηλαδή, μικροκυματικών εμπλεγμένων φωτονίων και αντιστοίχως την πρόταση ενός εξαιρετικά ευαίσθητου ανιχνευτικού συστήματος της ίδιας περιοχής, αποδοτικό και αξιόπιστο στην ανίχνευση μεμονωμένων φωτονίων.

«Επειδή εργαζόμαστε στο επίπεδο ενός φωτονίου, έχουμε να κάνουμε με επίπεδα ισχύος που είναι πολλές τάξεις μεγέθους ασθενέστερα από τα συμβατικά συστήματα ραντάρ, γεγονός που δημιουργεί μια τεχνική πρόκληση», εξηγεί ο Jonathan Baugh, αναπληρωτής καθηγητής στο Ινστιτούτο Κβαντικής Πληροφορικής του Πανεπιστημίου του Waterloo (IQC). Αυτό σημαίνει ότι η τεχνική της αποστολής εμπλεγμένων κβάντων αντί της κλασικής ακτινοβολίας, θεωρητικά, προσφέρει σημαντικά πλεονεκτήματα. Το κύριο εξ αυτών είναι η επίτευξη υψηλότερης ανάλυσης της εικόνας από το κλασικό ραντάρ, μιας πολύ πιο ακριβής εικόνας, χωρίς αύξηση της συχνότητας, η οποία θα επέτρεπε να εντοπίσει κανείς όχι μόνο την ύπαρξη ενός εχθρικού αεροπλάνου ή πυραύλου, αλλά και να προσδιορίσει το σχήμα, την ταχύτητα και το μέγεθός του, ακόμη και αν έχουν ελαχιστοποιηθεί φυσικά με τεχνικές stealth. Η ανάλυση από οποιαδήποτε συσκευή οπτικοποίησης είναι άμεσα ανάλογη με την ενέργεια των φωτονίων που χρησιμοποιείται για την αναγνώριση της συσκευής και ένα από τα πιο ενδιαφέροντα πράγματα για το κβαντικό ραντάρ είναι η συμπεριφορά της δέσμης καθώς διαδίδεται μέσω της ατμόσφαιρας, επειδή ο χαρακτήρας της εικόνας που ακτινοβολείται πίσω είναι συνάρτηση όλων των φωτονίων που προστίθενται μαζί », εξηγεί ο Allen. «Ενώ με ένα κλασικό ραντάρ βλέπετε απλώς ένα σχήμα και δεν ξέρετε τι είναι αυτό », λέει.

Ωστόσο, τα αντίμετρα ραντάρ περιλαμβάνουν τη χρήση μπλοκαρίσματος για την απόκρυψη ενός στόχου. Είναι σημαντικό να αναφερθεί ότι το Κβαντικό Ραντάρ είναι ανθεκτικό έναντι των επιδράσεων τέτοιων συστημάτων παρεμβολής, γεγονός για το

οποίο χαρακτηρίζεται ως ¨άτρωτο¨. Από την άποψη της εμπλοκής ως πόρου, είναι εκθετικά λιγότερο πιθανό να επηρεαστεί από ένα κβαντικό ραντάρ που λειτουργεί με μη εμπλεγμένα φωτόνια, πόσο μάλλον από ένα κλασικό ραντάρ. Υπάρχουν, επίσης, ισχυρισμοί ότι κάθε προσπάθεια απόκρυψης ίχνους ραντάρ από κβαντικά ραντάρ είναι μάταιη. Το τι σημαίνουν όλα αυτά για τα στρατιωτικά δεδομένα παγκοσμίως είναι ευνόητο: τα πανάκριβα αεροσκάφη stealth πέμπτης γενιάς δεν θα είναι πια «αόρατα», καθώς δε θα μπορούσαν να ξεγελάσουν ένα κβαντικό ραντάρ.

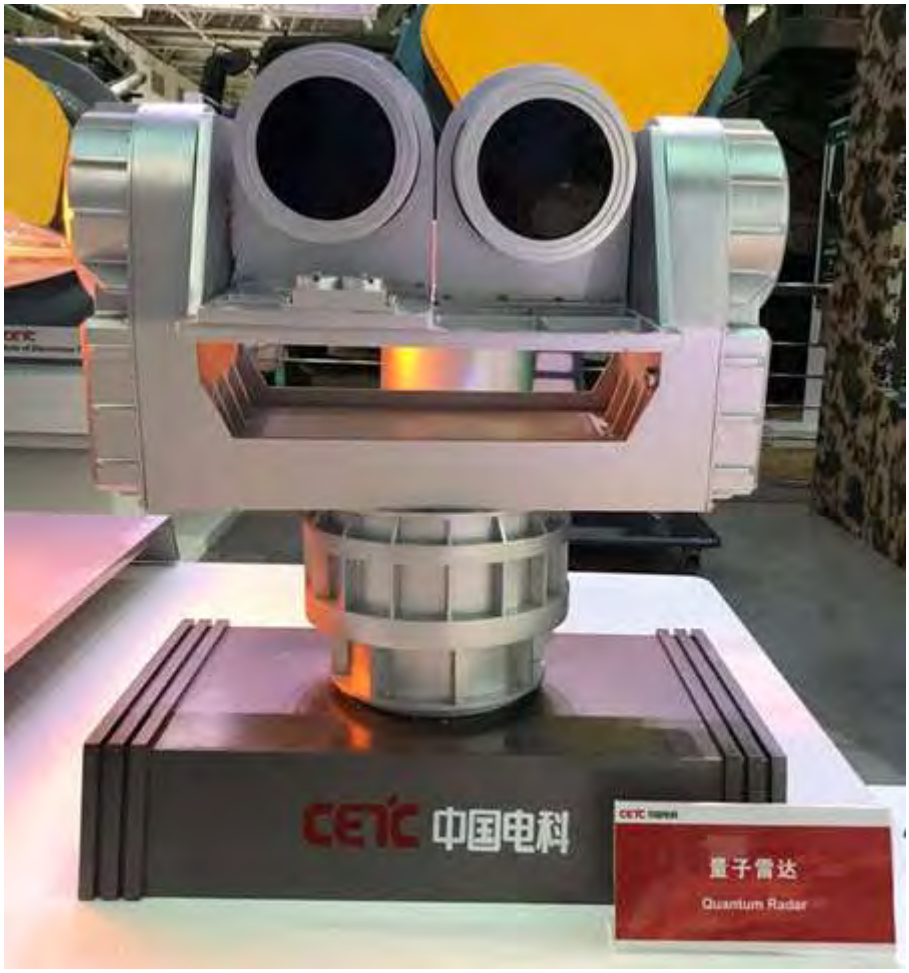
Μία από τις βασικές παραμέτρους που πρέπει να λαμβάνεται υπόψιν είναι ο λόγος σήματος προς θόρυβο (SNR). Το SNR δείχνει πόσο ισχυρό είναι το σήμα σε σύγκριση με το θόρυβο. Αν και το κατώφλι ανίχνευσης ποικίλλει, ένας τυπικός αριθμός για ένα κλασικό σύστημα είναι ότι το σήμα πρέπει να είναι περίπου 30 φορές ισχυρότερο από τη γραμμή θορύβου (ισοδύναμο με περίσσεια σήματος 15 ντεσιμπέλ). Μια μελέτη το Φεβρουάριο του 2017 πρότεινε μείωση του ορίου SNR στα περίπου 12 ντεσιμπέλ. Αυτό σημαίνει ότι θα μπορούσε είτε να δει μικρότερους στόχους σε μια δεδομένη απόσταση είτε να δει στόχους ενός δεδομένου μεγέθους σε μεγαλύτερες αποστάσεις. Ένας στόχος με υπογραφή ραντάρ για το μέγεθος μιας μπάλας γκολφ, για παράδειγμα, θα μοιάζει με πουλί. Εναλλακτικά, οποιοσδήποτε στόχος θα μπορούσε να ανιχνευθεί περίπου 20% πιο μακριά.

Τα κβαντικά ραντάρ που βασίζονται σε εμπλοκή έρχονται, όμως, αντιμέτωπα με θεμελιώδεις περιορισμούς αλλά και με σημαντικές τεχνικές προκλήσεις που πρέπει να ξεπεράσουν. Η κβαντική εμπλοκή είναι δύσκολο να διατηρηθεί για μεγάλα χρονικά διαστήματα, συνεπώς, όπως τα παραδοσιακά ραντάρ, έτσι και αυτά υποβαθμίζονται σε ανάλυση σε μεγάλες αποστάσεις. Το περιορισμένο εύρος τους, όμως, δεν είναι το μόνο πρόβλημα. Η εμπλοκή είναι εξαιρετικά εύθραυστη και ευαίσθητη ιδιότητα του κβαντικού κόσμου και απαιτεί ένα πολύ ακριβές και εξαιρετικά κρύο περιβάλλον, κάτι που είναι χαρακτηριστικό για τις περισσότερες κβαντικές τεχνολογίες στερεάς κατάστασης. Επιπλέον, αυτή η μέθοδος μπορεί να ανιχνεύσει ένα στόχο αλλά δεν μπορεί να καθορίσει με ακρίβεια τη θέση του. Εξαιτίας αυτών, οι ερευνητές υποστηρίζουν ότι η τεχνική αυτή στοχεύει περισσότερο στο να βελτιώσει το συμβατικό ραντάρ παρά να το αντικαταστήσει. Αυτό, όμως, δε σημαίνει ότι το κβαντικό ραντάρ αποτελεί απλά ένα όνειρο για την αμυντική κοινότητα.

Τα κβαντικά ραντάρ μπορεί να αποτελούν μια πολύ πρόσφατη τεχνολογική και επιστημονική εξέλιξη για την οποία ακόμα δεν είναι πλήρως κατανοητό γιατί ή πώς λειτουργεί στους επιστήμονες που τη μελετούν, δεν τους εμποδίζει, όμως, να βρουν τρόπους να τη χρησιμοποιήσουν προς όφελος όλων. Συγκεκριμένα, ερευνητές έχουν προωθήσει την ιδέα πολύ περισσότερο, αποδεικνύοντας τις δυνατότητές της με ένα λειτουργικό πρωτότυπο.

Όπως ανέφερε η κρατική κινεζική εφημερίδα Global Times, επικαλούμενη το κρατικό πρακτορείο Xinhua, η μεγαλύτερη αμυντική ηλεκτρονική εταιρεία της Κίνας, η κρατική εταιρεία οπλικών συστημάτων China Electronic Technology Group Corporation (CETC), ανακοίνωσε ότι ανέπτυξε το πρώτο «κβαντικό σύστημα ραντάρ» επόμενης γενιάς στον κόσμο, το οποίο, όπως ισχυρίζεται, μπορεί να ανιχνεύσει πυραύλους και άλλα αντικείμενα που πετούν «με μεγάλη ταχύτητα μέσω του διαστήματος». Επιπλέον, όπως ανέφερε, είναι ανθεκτικό σε παρεμβολές και μπορεί να εντοπίσει αεροσκάφη χαμηλής παρατηρησιμότητας (όπως τα stealth), γεγονός που θα καθιστούσε τις στρατιωτικές τεχνολογίες μυστικότητας τίποτα περισσότερο από ξεπερασμένες από τη μια μέρα στην άλλη.

Το 2015, μάλιστα, η ομάδα ανακοίνωσε την επιτυχή δοκιμή του, ενώ στις 6 Νοεμβρίου του 2018 παρουσίασε ένα πρόπλασμά του στο διήμερο Zhuhai Airshow σε πραγματικές ατμοσφαιρικές συνθήκες με εμβέλεια τουλάχιστον 100 χιλιομέτρων (60 μίλια).



Εικόνα 38: Πρόπλασμα κβαντικού ραντάρ στο Zhuhai Airshow, 6 Νοεμβρίου 2018

Πηγή: https://www.ptisidiastima.com/china-quantum-radar/

Η κινεζική αυτή ανακοίνωση προκάλεσε σοκ στην αμυντική κοινότητα. Ερευνητικές ομάδες από όλο τον κόσμο είχαν πειραματιστεί με κβαντικό ραντάρ για παραπάνω από μια δεκαετία, κανένας τους όμως δεν έφτασε κοντά σε αυτό. Μια μελέτη είχε θέσει το μέγιστο αποτελεσματικό εύρος κβαντικών ραντάρ κάτω από 7 μίλια, με αποτέλεσμα ο ισχυρισμός αυτός να φανεί σε πολλούς υπερβολικός.

Ενώ τα 100 χιλιόμετρα δεν είναι ένα ιδιαίτερα τεράστιο κατόρθωμα, το γεγονός ότι ένα τέτοιο σύστημα ραντάρ μπορεί να εντοπίζει με ακρίβεια και αξιοπιστία stealth μαχητικά είναι εντυπωσιακό. Τα περισσότερα ραντάρ που λειτουργούν σε συχνότητες όπως η X ή η Ku είναι σε θέση να εντοπίζουν τα stealth μαχητικά μόνο σε πολύ κοντινές αποστάσεις.

Οι Baugh, Lloyd και Allen απορρίπτουν τον ισχυρισμό αυτό και τον χαρακτηρίζουν μη αξιόπιστο. Ο Άλλεν, συγκεκριμένα, λέει ότι πιστεύει πως οι Κινέζοι έχουν

πραγματοποιήσει ένα επιτυχημένο πείραμα χρησιμοποιώντας ένα κβαντικό σύστημα ραντάρ. Κινέζοι ερευνητές, λέει, τοποθέτησαν την κβαντική γεννήτρια ραντάρ σε ένα δορυφόρο στο διάστημα, πράγμα που, ουσιαστικά, σημαίνει ότι δε διαδίδει την κβαντική δέσμη μέσω της ατμόσφαιρας, αλλά στο κενό. Επιπλέον, ο δέκτης βρισκόταν σε βουνό μεγάλου υψόμετρου στο Θιβέτ. Προσθέτει ότι ορισμένοι στα αμερικανικά Υπουργεία Άμυνας ισχυρίστηκαν ότι η κινεζική ανακοίνωση ήταν μπλόφα για να τρομάξει τους Αμερικανούς όσον αφορά τη χρήση των μαχητικών μυστικότητας. Ωστόσο, «Εάν οι Κινέζοι ήταν επιτυχείς στην επίλυση του προβλήματος αποσυνοχής, θα μπορούσαν να αναπτύξουν πολλές κβαντικές τεχνολογίες».

Οι αξιωματούχοι των δυτικών αμυντικών βιομηχανιών, συγκεκριμένα, θεωρούν πως η ανάπτυξη ενός τέτοιου ραντάρ είναι εξαιρετικά δύσκολη. Ακόμα και αν έχει κατακτηθεί πλήρως αυτή η τεχνολογία, υπάρχουν σοβαρά προβλήματα στην κατασκευή και λειτουργία τέτοιων ραντάρ, πόσο μάλλον η αξιόπιστη δοκιμή τους εκτός εργαστηρίου.

Σκεπτικός αρκετά παρουσιάστηκε και ο Μα Σαοσιόνγκ, καθηγητής Φυσικής στο Πανεπιστήμιο της Νανζίνγκ. Είπε στην εφημερίδα South China Morning Post «Η εμβέλεια που αναφέρει η διεθνής ερευνητική κοινότητα είναι πολύ μικρότερη από 100 χιλιόμετρα». Μέχρι σήμερα, πρόσθεσε, σημαντικές τεχνικές δυσκολίες περιόριζαν την τεχνολογία του κβαντικού ραντάρ σε συνθήκες εργαστηρίου.

Παρόλα αυτά, αν ο ισχυρισμός αυτός είναι αλήθεια, είναι μακράν η πιο εντυπωσιακή δημόσια δήλωση της τεχνολογίας, καθώς αποτελεί τεράστια νίκη για την άμυνα. Ωστόσο, καμία πληροφορία δεν κοινοποιήθηκε σχετικά με την ευαισθησία ή τις παραμέτρους λειτουργίας της ή ακόμη και τον τρόπο με τον οποίο "αποθηκεύτηκαν" τα σήματα για περιοχές τόσο μεγάλης απόστασης.

Συνεπώς, υπάρχουν ακόμη πολλά που πρέπει να γίνουν για να επιτευχθεί ένα πρακτικό κβαντικό ραντάρ εμπλοκής στην ισχυρότερη μορφή του. Θα χρειαστεί πολλή προσπάθεια για να βγει ένα ραντάρ από το εργαστήριο και, ακόμη και τότε, μπορεί να διαμορφωθεί περισσότερο για να είναι μια εξέλιξη της υπάρχουσας ικανότητας ή ένα χρήσιμο συμπλήρωμα σε αυτό, αντί για άμεση αντικατάσταση. Και το κόστος και οι πρακτικές δυσκολίες πρέπει να σταθμίζονται έναντι των ταυτόχρονων εξελίξεων στα κλασικά ραντάρ. Όμως διακυβεύονται αρκετά και πιθανώς μεγάλη δραστηριότητα

πίσω από κλειστές πόρτες. για να παραδεχτεί κανείς την πιθανότητα να επιλυθούν οι σημερινές τεχνικές προκλήσεις.

Επιπλέον, χωρίς τις λεπτομερείς, τεχνικές προδιαγραφές των κβαντικών ραντάρ, είναι δύσκολο να γνωρίζει κανείς με σιγουριά πόσο αναγκαία θα είναι η απαίτηση για πρόσθετα συστήματα εμβέλειας. Αλλά ακόμα και σήμερα, η τεχνολογία stealth δεν είναι πανάκεια και οι πλατφόρμες stealth τείνουν να βελτιστοποιούνται για συγκεκριμένες ζώνες συχνοτήτων. Για παράδειγμα, τα stealth αεροσκάφη είναι συνήθως X-band, συχνότητα με την οποία λειτουργούν ραντάρ αλλά και όπλα αέρα.

Η κατάσταση του κβαντικού ραντάρ αποδεικνύεται ως επί το πλείστον σε ακαδημαϊκές δημοσιεύσεις. Όσο για την απόλυτη σκοπιμότητα της τεχνολογίας, παραμένει μια βάση σκεπτικισμού στην ευρύτερη επιστημονική κοινότητα. Αυτός ο σκεπτικισμός, όμως, δεν εμποδίζει τα ενδιαφερόμενα μέρη να αντισταθμίσουν τα στοιχήματά τους. Στις ΗΠΑ, πραγματοποιήθηκε έρευνα εντός εθνικών εργαστηρίων και έχει υποστηριχθεί από τον Οργανισμό Προχωρημένων Ερευνητικών Έργων Άμυνας (DARPA). Αρκετές κρατικές επιχειρήσεις ερευνούν το κβαντικό ραντάρ στην Κίνα. Και, δεδομένης της μεγάλης κλίμακας χρηματοδότησης στην Ευρώπη για την κβαντική τεχνολογία, είναι πολύ πιθανό να πραγματοποιηθεί, επίσης, πρόσθετη διαβαθμισμένη έρευνα. Αυτό υποδηλώνει ότι υπάρχει συνεταιριστικό και ανταγωνιστικό πνεύμα, τουλάχιστον στον ακαδημαϊκό χώρο.

Σύμφωνα με τις τελευταίες εξελίξεις στον τομέα, ένας νέος τύπος κβαντικού ραντάρ εμπλοκής, κάτι ακατόρθωτο με προηγούμενες προτάσεις αντίστοιχων ραντάρ, είναι τώρα στο προσκήνιο.

Συγκεκριμένα, ο Lorenzo Maccone, από το Πανεπιστήμιο της Παβία, στην Ιταλία και ο Changliang Ren, από το Ινστιτούτο Πράσινης και Ευφυούς Τεχνολογίας της Chongqing, στην Κίνα, υποστηρίζουν ότι αυτή η μέθοδός τους θα μπορούσε να επιτρέψει περισσότερο ακριβείς μετρήσεις θέσεων.

Θεωρητικές προβλέψεις, όπως είναι γνωστό, υποδεικνύουν ότι η εκπομπή διεμπλεκόμενων φωτονίων θα βελτίωνε την ακρίβεια των μετρήσεων του ραντάρ. Παρόλα αυτά, οι μέχρι στιγμής προτεινόμενες μέθοδοι κβαντικού ραντάρ προσδιορίζουν την απόσταση ενός αντικειμένου με μεγαλύτερη ακρίβεια από ότι ένα

κλασικό ραντάρ, δεν προσφέρουν, όμως, βελτιώσεις όσον αφορά τον προσδιορισμό της κατεύθυνσής του. Η μέθοδος των Maccone και Ren τα κάνει και τα δύο.

Αναλυτικότερα, υποστηρίζουν ότι η θέση ενός αντικειμένου θα μπορούσε να εντοπιστεί εκπέμποντας και τα δύο εμπλεγμένα φωτόνια. Χάρη στην εμπλοκή, τα μεμονωμένα φωτόνια θα ενεργούσαν και τα δύο σαν να ήταν μεμονωμένα φωτόνια υψηλής ανάλυσης που περιείχαν την ενέργεια και των δύο μελών του ζεύγους. Αυτό το «συλλογικό» φωτόνιο θα επέστρεφε πιο ακριβείς πληροφορίες σχετικά με το στόχο.

Για να αναπτύξουν το σχέδιό τους, οι δυο τους επέκτειναν σε τρεις διαστάσεις (3D) μια προηγούμενη προτεινόμενη μέθοδο μιας (1D) διάστασης. Αιτιολόγησαν και ανάλυσαν κάθε στοιχείο που ανέφεραν και βρήκαν ότι για N διεμπλεκόμενα φωτόνια, η τρισδιάστατη περιοχή των πιθανών θέσεων ενός αντικειμένου στένευε κατά $N^{\frac{3}{2}}$ σε σύγκριση με ένα κλασικό ραντάρ με τον ίδιο αριθμό ανεξάρτητων φωτονίων.

Η τεχνική παρουσιάζει περιορισμούς, όπως μια υψηλή ευαισθησία στο θόρυβο. Η απώλεια, ακόμη, ενός διεμπλεκόμενου φωτονίου θα κόστιζε στο σύστημα ορισμένα από τα πλεονεκτήματά του σε σχέση με την κλασική εκδοχή. Υπάρχουν τρόποι να διορθωθούν μέχρι ένα βαθμό αυτά τα προβλήματα, αλλά οι ερευνητές υποστηρίζουν, και πάλι, ότι το σχέδιό τους θα μπορούσε να συμπληρώσει μάλλον παρά να αντικαταστήσει τα κλασικά συστήματα ραντάρ.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σήμερα, η κβαντική τεχνολογία έχει υπερβεί κατά πολύ τα άλλοτε απαγορευτικά όρια προόδου, με αποτέλεσμα την υλοποίηση διαδικασιών έξω από την κλασική πραγματικότητα και αντίληψη του κόσμου. Πλέον είναι διαθέσιμα τέτοια μέσα και εργαλεία, τα οποία δεν τολμούσε κανείς να ονειρευτεί πριν από μερικά χρόνια. Χάρη σε αυτό το τεχνολογικό άλμα, η κβαντική μηχανική έφερε επανάσταση στην επιστήμη της Φυσικής αλλά και στην κοινή λογική.

Η ενσωμάτωση των κβαντικών τεχνολογιών αντιπροσωπεύει, επί του παρόντος, μια από τις πιο αναμενόμενες εξελίξεις για τις ένοπλες δυνάμεις, ωστόσο η ευρεία χρήση τους εξακολουθεί να απέχει χρόνια. Πολλές κβαντικές τεχνολογίες μπορεί να βρίσκονται ακόμη σε θεωρητικό στάδιο είτε σε πρώιμη ανάπτυξη, δεν υπάρχει αμφιβολία, όμως, ότι θα έχουν αποδιοργανωτικό αποτέλεσμα στο μέλλον.

Ειδικότερα στο πεδίο της αμυντικής έρευνας, οι δύο κατευθύνσεις της κβαντικής ανίχνευσης και της ασφαλούς διακίνησης της κβαντικής πληροφορίας, αναμένεται να κυριαρχήσουν προσανατολίζοντας σθεναρά το παγκόσμιο ερευνητικό ενδιαφέρον.

Το γενικό συμπέρασμα είναι πως υπάρχουν ακόμη ανοιχτά ερωτήματα που αναζητούν απαντήσεις, ενώ διάφορες τεχνολογικές προκλήσεις παραμένουν. Το σίγουρο είναι, πως η κβαντική τεχνολογία αποτελεί το επόμενο βήμα προς ένα «θαυμαστό καινούργιο κόσμο».

ΛΕΞΙΚΟ ΟΡΩΝ

Αναπαραγωγιμότητα: είναι ο βαθμός της ομοιογένειας μεταξύ των συμπερασμάτων ασύνδετων αξιολογήσεων που προκύπτουν με την ίδια διαδικασία, στο ίδιο δείγμα, κάτω από διαφορετικές συγκυρίες.

Διασταύρωση Josephson: Αποτελεί ένα λεπτό, μη αγώγιμο στρώμα τοποθετημένο μεταξύ δύο υπεραγώγιμων στρωμάτων. Υπό τις σωστές συνθήκες, τα ηλεκτρόνια έχουν τη δυνατότητα να ταξιδέψουν από το ένα υπεραγώγιμο στρώμα στο άλλο δίχως αντίσταση, μέσω αυτής της διασταύρωσης. Αν το ρεύμα, όμως, φτάσει σε κρίσιμο επίπεδο, εμφανίζεται ξαφνικά μια πεπερασμένη αντίσταση και αναπτύσσεται τάση σε όλη τη συσκευή. Οι διασταυρώσεις Josephson πήραν το όνομά τους από τον Brian Josephson, από τον οποίο και ανακαλύφθηκε η χρήση τους το 1962.

Εντροπία: Αποτελεί φυσικό μέγεθος με το οποίο δηλώνεται το μέτρο της αποδιοργάνωσης ή της αταξίας/τυχαιότητας σε ένα σύστημα. Έτσι, αν ένα σύστημα έχει εντροπία μηδέν, τότε δεν έχει τυχαιότητα. Μάλιστα, μια ιστορία αναφέρει ότι στο τέλος της δεκαετίας του 1940, ο John Neumann, ένας πρωτοπόρος της εποχής των υπολογιστών, συμβούλεψε τον θεωρητικό των επικοινωνιών Claude E. Shannon ν'αρχίσει να χρησιμοποιεί τον όρο εντροπία όταν μιλάει για πληροφορία διότι ¨…κανείς δεν καταλαβαίνει τι είναι πραγματικά η εντροπία, κι έτσι σε μια συζήτηση θα έχεις πάντα το πλεονέκτημα…¨

(Πηγή: http://www.physics4u.gr/articles/2002/secondlaw2.html)

Έξυπνες κάρτες (smart cards): Κάρτες μικρού μεγέθους, οι οποίες ενσωματώνουν ένα ολοκληρωμένο κύκλωμα με ηλεκτρικές επαφές που περιλαμβάνει ένα μικροεπεξεργαστή (ή/και μνήμη), ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Για την ανάγνωσή της απαιτείται ειδική συσκευή. Οι έξυπνες κάρτες χρησιμοποιούν προηγμένες τεχνικές κρυπτογράφησης, ώστε να προσφέρουν τη δυνατότητα αποθήκευσης και επεξεργασίας τεράστιου όγκου δεδομένων με ασφαλή τρόπο, στα οποία για να έχει κανείς πρόσβαση απαιτείται συχνά η χρήση κωδικού (PIN), καθιστώντας έτσι αδύνατο το γεγονός να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία). Είναι εύκολες και αρκετά ασφαλείς στη χρήση μιας και έχουν τις απαραίτητες διεργασίες και πληροφορίες αποθηκευμένες στο σώμα τους και βρίσκουν πολλές και ποικίλες εφαρμογές.

Ηλεκτρική διπολική ροπή: Αποτελεί μέτρο πόλωσης ενός συστήματος ηλεκτρικών φορτίων. Η ηλεκτρική διπολική ροπή, έστω p, με φορτία +q και -q, ορίζεται ως p=qr, όπου r συμβολίζει το διάνυσμα από το αρνητικό στο θετικό φορτίο. Από τη στιγμή που το r είναι διάνυσμα συγκεκριμένης διεύθυνσης, θα είναι και η p. Η μονάδα SI της ηλεκτρικής διπολικής ροπής είναι coulomb-meter.

Ηλεκτρομαγνητικά επαγόμενη διαφάνεια: Η ηλεκτρομαγνητικά επαγόμενη διαφάνεια (electromagnetically induced transparency, EIT) είναι ένα φαινόμενο κβαντικής συμβολής στο οποίο ένα οπτικό μέσο μετατρέπεται σε αδιαφανές, γεγονός που τυπικά είναι εφικτό μόνο σε άτομα ειδικών ενεργειακών δομών. Πιο συγκεκριμένα, μια δέσμη λέιζερ προσεκτικά επιλεγμένης συχνότητας εκπέμπει φως προς ένα νέφος ατόμων και το μεταβάλλει από τελείως αδιαφανές σε διαφανές. Η διαφάνεια αναφέρεται σε φως μιας άλλης καθορισμένης συχνότητας.

Ηλιακές εκλάμψεις: Οι εκλάμψεις είναι εκρήξεις, από τις μεγαλύτερες του ηλιακού συστήματος, που παρατηρούνται στην ατμόσφαιρα ενός άστρου, του ήλιου στη συγκεκριμένη περίπτωση, και δημιουργούνται κατά την ξαφνική και απότομη απελευθέρωση τεράστιας ποσότητας ενέργειας που έχει συσσωρευτεί στα τοπικά μαγνητικά πεδία της ηλιακής ατμόσφαιρας. Η ενέργεια αυτή εκπέμπεται ως ισχυρή ακτινοβολία σε ολόκληρο το εύρος του ηλεκτρομαγνητικού φάσματος. Το φαινόμενο συνοδεύεται από θερμοκρασίες που υπερβαίνουν ακόμη και τους 20 εκατ. °C αλλά, συχνά, και από εκπομπή φορτισμένων σωματιδίων που ταξιδεύουν με πολύ μεγάλες ταχύτητες.

Θερμική διαφυγή: Όταν μια εξώθερμη αντίδραση, δηλαδή μια χημική αντίδραση που παράγει ενέργεια είτε με φως είτε με θερμότητα, προξενεί θέρμανση του δοχείου της αντίδρασης που δεν μπορεί να τεθεί υπό έλεγχο, ο ρυθμός της αντίδρασης είναι δυνατό να αναπτυχθεί, οδηγώντας με τη σειρά του σε μεγαλύτερη αύξηση θερμότητας. Η κατάσταση αυτή ονομάζεται θερμική διαφυγή.

Θερμική σταθερά χρόνου: Αποτελεί μέτρο αδράνειας, το οποίο αναφέρεται στην ταχύτητα με την οποία είναι εφικτό να αντιδράσει μια αντίσταση στις εναλλαγές της θερμοκρασίας.

Θερμική σύνθετη αντίσταση: Μέγεθος του ηλεκτρισμού (μιγαδικός αριθμός) που εκράζει τη δυσκολία στην κίνηση των ηλεκτρονίων σε κύκλωμα εναλλασσόμενου ρεύματος.

Όταν ένα κύκλωμα διαρρέεται από εναλλασσόμενο ρεύμα, δημιουργείται, συνήθως, μια δυσκολία στη διέλευσή του. Η ολική, λοιπόν, αυτή αντίσταση λέγεται σύνθετη αντίσταση του κυκλώματος (Impedance). Αποτελείται από δύο στοιχεία, ένα πραγματικό, την καθαρά ωμική αντίσταση R του κυκλώματος και ένα φανταστικό, την αντίδραση X που παρουσιάζει το κύκλωμα κατά τη διέλευση μέσα από αυτό του εναλλασσόμενου ρεύματος. Η σύνθετη αντίσταση ενός κυκλώματος είναι πάντα μεγαλύτερη ή ίση από την καθαρά ωμική αντίσταση που αυτό θα παρουσιάζει.

Θερμική χωρητικότητα: Η ποσότητα θερμότητας που χρειάζεται ένα σώμα για να αυξηθεί η θερμοκρασία του κατά ένα βαθμό. Η θερμική χωρητικότητα είναι ανάλογη της μάζας m του σώματος και συμβολίζεται, συνήθως, με C.

Θερμικός θόρυβος (thermal noise): Οφείλεται στην κίνηση φορέων ηλεκτρικού φορτίου που συναντάται σε κάθε ηλεκτρονικό κύκλωμα. Ο θόρυβος αυτός είναι γνωστός και ως θόρυβος Johnson, Nyquist, λευκός θόρυβος αλλά και ως θερμική διαταραχή. Υπάρχει πάντοτε στα άκρα μιας αντίστασης, ανεξάρτητα του εάν η ίδια διαρρέεται ή όχι από ηλεκτρικό ρεύμα και η φύση του είναι καθαρά τυχαία.

Θερμίστορ ημιαγωγών: Η λέξη ¨θερμίστορ¨ αποτελεί συνδυασμό των λέξεων thermal και resistor. Επομένως, αναφέρεται σε τύπους αντίστασης, η τιμή των οποίων εντοπίζεται ανάμεσα σε αυτές των μονωτών και των αγωγών. Παρουσιάζουν εκθετική ελάττωση με την άνοδο της θερμοκρασίας και γι΄ αυτό το λόγο χρησιμοποιούνται εκτεταμένα για τη μείωση της ραγδαίας αύξησης των ρευμάτων λόγω υπερτάσεων.

Κβάζαρ: Με τον όρο ¨κβάζαρ¨ αποκαλείται στην Αστρονομία κάθε εξαιρετικά λαμπρός και μακρινός ενεργός γαλαξιακός πυρήνας που παρουσιάζεται στο ορατό φως σαν αστέρας. Από εκεί προέρχεται και η ονομασία τους, καθώς *quasi-stellar* σημαίνει ¨παρόμοιος με αστέρα¨. Μάλιστα, μία αρχική απόδοση του όρου στα ελληνικά ήταν ημιαστέρας. Χάρη στη μεγάλη μετατόπιση προς το ερυθρό που παρουσιάζουν τα φάσματά τους, διακρίνονται από τους αστέρες, ενώ, ταυτόχρονα, αποτελούν και σημειακές ραδιοπηγές.

Κοσμική ακτινοβολία: Η κοσμική ακτινοβολία (ή κοσμικές ακτίνες) είναι μία κατηγορία ακτινοβολίας που αποτελείται από σωματίδια υψηλών ενεργειών που παράγονται σε κάποιο σημείο του σύμπαντος και προσκρούουν στην ατμόσφαιρα της Γης με ανιχνεύσιμα αποτελέσματα. Παράγεται από πηγές όπως ο ήλιος, άλλα αστέρια,

μακρινούς γαλαξίες κ.α.. Δεν μπορεί κανείς να τη δει ή να τη νιώσει, αλλά γεμίζει κάθε σπιθαμή από αυτό που μοιάζει κενός χώρος. Είναι επιβλαβής για διάφορα τεχνολογικά μέσα αλλά και για τον ανθρώπινο οργανισμό, ωστόσο οι άνθρωποι προφυλάσσονται από τα περισσότερα σωματίδιά της χάρη στο γήινο μαγνητικό πεδίο που τα εκτρέπει μακριά από την επιφάνεια του πλανήτη.

¨Μαύρο κουτί¨: Στην επιστήμη της πληροφορικής, ο όρος αυτός χρησιμοποιείται όταν είναι επιθυμητό να γίνει αναφορά σε ένα αυτόνομο, ανεξάρτητο σύστημα ή αντικείμενο ή συσκευή για το οποίο είναι γνωστές οι είσοδοι και οι έξοδοί του, αλλά η εσωτερική του δομή παραμένει άγνωστη ή μη κατανοητή.

Μέλαν σώμα: Ένα ιδανικό σώμα στη φυσική που απορροφά όλο το φως, και κατ' επέκταση όλη την ηλεκτρομαγνητική ακτινοβολία, που προσκρούει πάνω του. Αυτό σημαίνει ότι δεν ανακλά ούτε διαχέει το φως που προσπίπτει σε αυτό (ή άλλης μορφής ηλεκτρομαγνητική ακτινοβολία), αλλά ούτε επιτρέπει στο φως να το διαπεράσει. Γι' αυτές του τις ιδιότητες ονομάζεται μέλαν σώμα. Σε αντίθεση με την εικόνα που δημιουργείται από την ονομασία του, το ίδιο το σώμα εκπέμπει κάποια ακτινοβολία, το φάσμα της οποίας εξαρτάται μόνο από τη θερμοκρασία του.

NMR (μαγνητικός πυρηνικός συντονισμός): Τα qubits αντιστοιχούν στη φορά περιστροφής (spin) των πυρήνων των ατόμων που απαρτίζουν ένα μόριο. Χρησιμοποιείται εναλλασσόμενο μαγνητικό πεδίο για να μεταβάλλει το spin στους πυρήνες, οι οποίοι συντονίζονται με αυτό.

NP-complete προβλήματα: Η κλάση των προβλημάτων που λύνονται σε πολυωνυμικό χρόνο είναι η NP. Τα δυσκολότερα προβλήματα αυτής ονομάζονται NP-complete. Πιο συγκεκριμένα, ένα πρόβλημα, έστω Π, λέγεται NP-complete όταν ισχύουν τα εξής:

1. $\Pi \in NP$

2. $\forall \Xi \in NP \Rightarrow \Xi \leq \Pi$

Όριο του Heisenberg: Στην κβαντομηχανική υπάρχει πάντα ανακρίβεια-αβεβαιότητα μέτρησης, η οποία δεν μπορεί να περιοριστεί κάτω από ένα συγκεκριμένο όριο (Όριο του Heisenberg). Η απροσδιοριστία αυτή, γνωστή από την ¨Αρχή της απροσδιοριστίας του Heisenberg¨, δεν αναφέρεται στην ανικανότητα του ανθρώπου ή στον περιορισμό της τεχνολογικής εξέλιξης των οργάνων μέτρησης να παρατηρήσουν ορισμένα

φαινόμενα στο μικρόκοσμο, αλλά σε μία ιδιότητα της Φύσης, η οποία εντοπίζεται και πειραματικά.

Παγίδες ιόντων: Ομάδα ιόντων παγιδεύεται σε συνδυασμό ηλεκτρικών πεδίων και μία ακτίνα laser τα εξαναγκάζει να μεταβάλλουν τις ατομικές τους καταστάσεις που αντιστοιχούν στα qubits του συστήματος.

Σκοτεινή ενέργεια: αναγνωρίζεται ως υπαίτια για την παρουσία μιας απωθητικής ενέργειας που έχει ως αποτέλεσμα την όλο και με μεγαλύτερη ταχύτητα επέκταση του σύμπαντος. Με την επίδρασή της, υπολογίζεται ότι το σύμπαν διπλασιάζεται κάθε δέκα δισεκατομμύρια χρόνια, ενώ καταλαμβάνει περίπου το 70% της συνολικής μάζας-ενέργειάς του. Θεωρείται ότι έχει αρνητική πίεση, ότι δεν έχει μάζα και δρα ως ένα είδος αντιβαρύτητας. Ονομάζεται σκοτεινή πολύ απλά επειδή κανένας δε γνωρίζει ακριβώς τι είναι, μιας και καμία ερμηνεία της δεν έχει αποδειχτεί. Η πλειοψηφία των αστρονόμων, παρ΄όλα αυτά, δηλώνουν βέβαιοι για την ύπαρξή της, καθώς είναι ορατές οι συνέπειες της δράσης της στην κίνηση των γαλαξιών.

Χαρακτηρίζεται από τρεις καθοριστικές ιδιότητες. Αρχικά, δεν είναι ορατή και δεν αλληλεπιδρά, μέσω οποιασδήποτε από τις θεμελιώδεις δυνάμεις, εκτός της βαρύτητας, με την ύλη. Ενδεχομένως να συμβαίνει, αλλά δεν έχει παρατηρηθεί κάτι τέτοιο μέχρι στιγμής. Δεν είναι αισθητή ούτε ανιχνεύσιμη με καμία μέθοδο, ακόμη και με προηγμένα επιστημονικά εργαλεία. Δεύτερον, κατανέμεται ομοιόμορφα. Τρίτον, διατηρεί την πυκνότητά της, σχεδόν, αμετάβλητη, καθώς πραγματοποιείται διαστολή του σύμπαντος, σε αντίθεση με την ύλη. Στις δύο τελευταίες ιδιότητες οφείλεται το γεγονός ότι αποκαλείται ¨ενέργεια¨ και όχι ¨ύλη¨.

Σκοτεινή ύλη: είναι ένα θεωρητικό είδος ύλης που είναι αδύνατο να εντοπισθεί με τηλεσκόπια. Της δόθηκε η ονομασία αυτή όχι μόνο επειδή αποτελεί κάτι ανεξήγητο, αλλά επειδή δεν αντανακλά, δεν απορροφά ούτε εκπέμπει φως ή άλλη ηλεκτρομαγνητική ακτινοβολία σε μεγάλο βαθμό ώστε να γίνεται αντιληπτή. Συγκεκριμένα, δεν αλληλεπιδρά με καμία θεμελιώδη δύναμη εκτός της βαρύτητας. Επομένως, το γεγονός της ύπαρξής της αλλά και οι ιδιότητές της στηρίζονται στις παρατηρούμενες βαρυτικές επιπτώσεις της στην ορατή ύλη, στην ακτινοβολία και στη δομή του σύμπαντος.

Η σκοτεινή ύλη υπολογίζεται ότι αποτελεί το 84,5% του συνόλου της ύλης και το 26,8% του περιεχομένου του σύμπαντος. Θεωρείται ότι περικλείει και οριοθετεί τους

γαλαξίες, με σκοπό η περιστροφή τους να εκτελείται γρήγορα χωρίς η ύλη τους να διασκορπίζεται στο διάστημα.

Οι έμμεσες επιβεβαιώσεις της είναι μεγάλες σε αριθμό και προκύπτουν από ξεχωριστές πλευρές, με αποτέλεσμα η πλειονότητα των επιστημόνων να καθίσταται υπέρμαχός της. Ταυτόχρονα, όμως, ένα πλήθος θεωρητικών φυσικών τη χαρακτηρίζουν "ψευδαίσθηση" που οφείλεται στις ανεπαρκείς πληροφορίες μας για τη βαρύτητα και τους θεμελιώδους νόμους της φύσης.

Σόναρ: Ηχοεντοπιστικά συστήματα ή αλλιώς ηλεκτροακουστικές συσκευές που εκμεταλλεύονται τη διάδοση των κυμάτων ηχητικής ενέργειας μέσα στη θαλάσσια μάζα. Ο σκοπός των συστημάτων sonar (SOund Navigation And Ranging, ελληνικά: ηχοπλοήγηση) είναι ο εντοπισμός/ανίχνευση, αναγνώριση/ταξινόμηση και παρακολούθηση υποβρύχιων σκαφών και διαφόρων αντικειμένων, η ακουστική χαρτογράφηση του βυθού, οι υποθαλάσσιες επικοινωνίες κ.α..

Συνδεδεμένα αυτοκίνητα: Υπάρχουν πάμπολλοι τρόποι με τους οποίους έχουν τη δυνατότητα τα αυτοκίνητα να συνδεθούν. Οι οδηγοί έχουν τη δυνατότητα επικοινωνίας με πληθώρα σημείων σύνδεσης που είτε βρίσκονται γύρω τους είτε πιο μακριά. Ουσιαστικά, τα συνδεδεμένα αυτοκίνητα είναι αυτοκίνητα εξοπλισμένα με τη δυνατότητα να αλληλοεπιδρούν με τις γύρω υποδομές, με άλλα οχήματα, με δίκτυο cloud, με πεζούς μέσω smartphones και άλλων συσκευών, με συνδυασμό των παραπάνω ή με όλες αυτές τις επιλογές μαζί. Ακόμη, μοιράζονται συνεχώς σημαντικές πληροφορίες για την ασφάλεια και την κινητικότητά τους με μια σειρά από φορείς, όπως είναι ο κατασκευαστής του οχήματος, οι εταιρείες παροχής υπηρεσιών, άλλα φυσικά ή νομικά πρόσωπα, οι διαχειριστές βασικών κρατικών μεταφορικών συστημάτων μεταφοράς και υπηρεσιών κ.α.. Συνήθως, η επαφή πραγματοποιείται μέσω σύνδεσης στο Internet ή μέσω ασύρματου τοπικού δικτύου.

Συστήματα αδρανειακής πλοήγησης: Είναι αυτόνομα συστήματα πλοήγησης, τα οποία βασίζονται στις αρχές της αδράνειας και της νευτώνειας μηχανικής.

Σωματίδιο άλφα: Το σωματίδιο άλφα είναι η στενή σύνδεση δύο πρωτονίων και δύο νετρονίων. Η δομή αυτή χαρακτηρίζεται από μηδενικό spin και ταυτίζεται με αυτήν του πυρήνα ενός ατόμου ηλίου.

Transistor: Κρυσταλλοτρίοδος ή και κρυσταλλολυχνία στα ελληνικά, αναφέρεται σε διάταξη ημιαγωγών στερεάς κατάστασης. Βρίσκει πολλών ειδών εφαρμογές στην ηλεκτρονική, μερικές από τις οποίες είναι η ενίσχυση, η σταθεροποίηση τάσης, η διαμόρφωση συχνότητας, η λειτουργία ως διακόπτης αλλά και ως μεταβλητή ωμική αντίσταση. Ανάλογα με την τάση με την οποία πολώνεται, έχει τη δυνατότητα να ρυθμίζει τη ροή του ηλεκτρικού ρεύματος που απορροφά από συνδεδεμένη πηγή τάσης.

Υπερσυμμετρία: είναι μια μη επιβεβαιωμένη θεωρία του σύμπαντος, σύμφωνα με την οποία κάθε γνωστό σωματίδιο έχει ένα αντίστοιχο, άγνωστο προς το παρόν, υπερσυμμετρικό σωματίδιο που ονομάζεται υπερσύντροφος και αντίστροφα. Το ζεύγος των δύο αυτών σωματιδίων έχει τις ίδιες θεμελιώδεις ιδιότητες, αλλά τα υπερσωματίδια πιθανόν να είναι αρκετά μεγαλύτερα σε βάρος και γι΄αυτό το λόγο να μην έχει ανακαλυφθεί κανένα έως σήμερα. Σκοπός της θεωρίας αυτής είναι να αποκτήσει η φύση παραπάνω συμμετρία.

Φωτοδίοδος: αποτελεί ένα είδος διόδου ημιαγωγού, μέσω του οποίου η φωτεινή ενέργεια (φως) μετατρέπεται σε ηλεκτρική ενέργεια (ρεύμα). Είναι γνωστή και ως φωτοανιχνευτής ή αισθητήρας φωτός (φωτοαισθητήρας). Η παραγωγή ρεύματος πραγματοποιείται με την απορρόφηση των φωτονίων, ενώ ένα μικρό ποσοστό αυτής παράγεται και χωρίς την παρουσία φωτός. Ενδέχεται να περιλαμβάνει οπτικά φίλτρα, ενσωματωμένους φακούς και να διαθέτει μικρές ή μεγάλες επιφάνειες.

Χρονισμός: η επιλογή συγκεκριμένης χρονικής στιγμής κατά την οποία θα πραγματοποιηθεί κάποια ενέργεια.

Χώρος Hilbert: Είναι ένας διανυσματικός χώρος (πραγματικός ή μιγαδικός) που χρησιμοποιείται στην κβαντική μηχανική και είναι απείρων διαστάσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Κβαντικός Υπολογιστής:

1. https://www.newsbeast.gr/weekend/arthro/3306993/ti-ine-o-kvantikos-ipologistis-ke-pos-tha-allaxi-tin-kathimerinotita-mas
2. https://docplayer.gr/30306071-To-provlima-toy-diakritoy-logarithmoy.html
3. https://el.wikipedia.org/wiki/Κβαντικός_υπολογιστής
4. https://astrobay.wordpress.com/2013/08/08/%CF%87%CF%8E%CF%81%CE%BF%CF%82-%CF%87%CE%AF%CE%BB%CE%BC%CF%80%CE%B5%CF%81%CF%84/
5. http://mpla.math.uoa.gr/media/theses/msc/Rafios_X.pdf
6. http://www.physics.ntua.gr/cv/kvantikh_fysikh_amalia_konsta.pdf
7. https://quantumcomputers-infotech.blogspot.com/p/blog-page_30.html
8. https://docplayer.gr/32819152-Kvantikoi-yiologmiies.html
9. http://estia.hua.gr/file/lib/default/data/19417/theFile
10. http://www.physics4u.gr/articles/2002/spintronics.html
11. https://tvxs.gr/news/sci-tech/i-kbantiki-texnologiki-epanastasi-ksekinise
12. http://repository.teiwest.gr/xmlui/bitstream/handle/123456789/1915/EPDO_0060.pdf
13. http://users.uoa.gr/~wvkarag/files/wvk-quantum_cryptography.pdf
14. https://repository.kallipos.gr/bitstream/11419/4015/1/chapter10Final.pdf
15. https://thalis.math.upatras.gr/~streklas/public_html/meta/Krinidi.pdf
16. https://d-michail.github.io/assets/teaching/algorithms/080_Intractability.el.pdf
17. http://www.intelligence.tuc.gr/~theory/previous/Theory_2006/lectures/lecture17.pdf
18. https://docplayer.gr/31270730-Klasi-np-np-complete-provlimata.html
19. http://ikee.lib.auth.gr/record/135513/files/1775_PANAGIOTIS_PAPOULIDIS.PDF
20. https://docplayer.gr/amp/47654659-4-i-arhi-tis-kvantikis-ypologistikis-kvantikos-algorithmos-toy-deutsch.html
21. https://docplayer.gr/47654659-4-i-arhi-tis-kvantikis-ypologistikis-kvantikos-algorithmos-toy-deutsch.html

22. https://docplayer.gr/amp/16590747-Kvantikoi-ypologistes-methodoi-ylopoiisis-kvantikon-pylon.html
23. http://ikee.lib.auth.gr/record/135098/files/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE.pdf
24. https://el.wikipedia.org/wiki/%CE%A4%CF%81%CE%B1%CE%BD%CE%B6%CE%AF%CF%83%CF%84%CE%BF%CF%81
25. https://www.huffingtonpost.gr/entry/ta-mestika-tes-kvantikes-diemplokes_gr_5bd8fd31e4b0aec2cb9ae748
26. http://ikee.lib.auth.gr/record/133590/files/KERMEZHS-1396-DIPLWMATIKI.pdf
27. http://www2.aueb.gr/users/douros/algorithms/tutorials_2012/14_frontistirio_complete.pdf
28. https://courses.corelab.ntua.gr/pluginfile.php/787/course/section/268/Reductions-P-NP-Completeness.pdf
29. https://euclid.ee.duth.gr/courses/old/2005-06/ProgJava/DraftSlides/IntroAlg%20Lecture%20Complexity-Large.pdf
30. https://el.wikipedia.org/wiki/%CE%A0%CF%81%CF%8C%CE%B2%CE%BB%CE%B7%CE%BC%CE%B1_P%3DNP
31. http://tccc.iesl.forth.gr/education/local/Physics_II-XHM-017/Lecture_Ch38_GR.pdf
32. http://www.physics4u.gr/articles/2002/quantumrelativ.html
33. https://sites.google.com/site/icsdkvantikoiypologistes/home/kephalaio-e/e3-kbantikes-logikes-pyles
34. http://docplayer.gr/16590747-Kvantikoi-ypologistes-methodoi-ylopoiisis-kvantikon-pylon.html
35. http://www.enet.gr/?i=news.el.article&id=171928
36. http://www.businessdictionary.com/definition/black-box.html
37. https://el.wikipedia.org/wiki/Qubit
38. https://www.academia.edu/36273630/Οδυσσέας_Γκιλής_ΕΝΤΡΟΠΙΑ
39. https://repository.kallipos.gr/bitstream/11419/216/7/ΚΒΑΝΤΙΚΗ_ΥΠΟΛΟΓΙΣΤΙΚΗ_144.pdf
40. https://repository.kallipos.gr/bitstream/11419/222/1/6%CE%BF_%CE%9A%CE%95%CE%A6%CE%91%CE%9B%CE%91%CE%99%CE%9F_%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
41. https://manosdanezis.gr/wp-content/uploads/2019/02/Κβαντικός-Υπολογιστής-και-Κβαντική-Πληροφορία.pdf
42. http://quantumcomputers-infotech.blogspot.com/p/qubits-hilbert.html
43. https://eclass.upatras.gr/modules/document/file.php/EE742/Open%20Courses/35.QuantumHardware.pdf
44. http://quantumcomputers-infotech.blogspot.com/p/blog-page_30.html
45. http://ikee.lib.auth.gr/record/114834/files/ptuxiaki.pdf
46. http://www.physics4u.gr/articles/2002/secondlaw2.html
47. http://corelab.ntua.gr/~gkaouri/DT2005-0160.pdf
48. https://eclass.upatras.gr/modules/units/?course=EE742&id=6407
49. https://www.urbandictionary.com/define.php?term=black%20box
50. http://docplayer.gr/52372609-Meleti-arhon-kvantikon-pylon.html
51. http://docplayer.gr/33563665-3-telestes-kai-kvantikes-pyles.html
52. http://users.auth.gr/~massen/KMIII/avisotntes-Bell-1.pdf
53. http://www.physics4u.gr/articles/2002/belltheorem.html
54. http://christselentis.blogspot.com/2008/09/bells-theorem.html
55. http://pyraeizoon.blogspot.com/2015/11/bell.html
56. https://science.fandom.com/el/wiki/Θεώρημα_Bell
57. https://manosdanezis.gr/wp-content/uploads/2019/02/%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C%CF%82-%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82-%CE%BA%CE%B1%CE%B9-%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE-%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B1.pdf
58. https://www.radiospot.gr/%CF%84%CE%BF-%CF%80%CF%81%CF%8E%CF%84%CE%BF-%CE%BF%CE%BB%CE%BF%CE%BA%CE%BB%CE%B7%CF%81%CF%89%CE%BC%CE%AD%CE%BD%CE%BF-

%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C-%CE%BA%CF%8D%CE%BA%CE%BB%CF%89/

59. https://www.tovima.gr/2015/10/06/science/eftiaksan-kbantiko-oloklirwmeno-kyklwma/
60. https://repository.kallipos.gr/bitstream/11419/220/1/4%CE%BF_%CE%9A%CE%95%CE%A6%CE%91%CE%9B%CE%91%CE%99%CE%9F_%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
61. http://lyk-pallin.att.sch.gr/wordpress/wp-content/uploads/2015/04/%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C%CF%82-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82.pdf
62. http://users.auth.gr/ganoulis/quantum/THMMY-2020/16-%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE%20%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AE.pdf
63. https://science.fandom.com/el/wiki/%CE%95%CE%BD%CF%84%CF%81%CE%BF%CF%80%CE%AF%CE%B1_%5C%CE%9C%CE%AD%CE%B3%CE%B5%CE%B8%CE%BF%CF%82
64. https://repository.kallipos.gr/bitstream/11419/219/1/3%CE%BF_%CE%9A%CE%95%CE%A6%CE%91%CE%9B%CE%91%CE%99%CE%9F_%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
65. https://fysikhblog.wordpress.com/2016/09/28/%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%BF%CE%AF-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82/
66. https://repository.kallipos.gr/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

67. https://euclid.ee.duth.gr/courses/old/2005-06/ProgJava/DraftSlides/IntroAlg%20Lecture%20Complexity-Large.pdf
68. https://el.wikipedia.org/wiki/%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82
69. https://el.wikipedia.org/wiki/%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE_%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE
70. https://el.wikipedia.org/wiki/%CE%99%CF%83%CF%84%CE%BF%CF%81%CE%AF%CE%B1_%CF%84%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD

Κρυπτογραφικά Συστήματα:

1. http://ikee.lib.auth.gr/record/126605/files/GRI-2011-6746.pdf
2. https://repository.kallipos.gr/bitstream/11419/1031/1/05_Chapter_07.pdf
3. https://eclass.hmu.gr/modules/document/file.php/TP122/03.Εργαστήρια/Lab%203%20-%20Symmetric/Lab3-Symmetric.pdf
4. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1
5. http://1lyk-glyfad.att.sch.gr/new/images/Project/kryptograf2012.pdf
6. http://1epal-argyroupolis.eu/component/attachments/download/203
7. https://repository.kallipos.gr/bitstream/11419/5444/1/ch5.pdf
8. https://en.calameo.com/books/0030940223193b7dc1826
9. http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13470/STE_MHP_00225_Medium.pdf?sequence=1
10. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1307/6/Nimertis_Antonopoulos.pdf
11. https://el.wikipedia.org/wiki/%CE%88%CE%BE%CF%85%CF%80%CE%BD%CE%B7_%CE%BA%CE%AC%CF%81%CF%84%CE%B1
12. http://nefeli.lib.teicrete.gr/browse/sefe/hlk/2006/FragkiadakisKonstantinos/attached-document/2006Fragkiadakis.pdf

13. https://dspace.lib.uom.gr/bitstream/2159/21881/4/GiantsiouFoteiniMsc2017.pdf
14. https://ocw.aoc.ntua.gr/modules/document/file.php/ECE103/crypto2013_pres1_classic.pdf
15. https://www.forth.gr/index_main.php?l=g&c=28&i=1546
16. https://openclass.teiwm.gr/modules/document/file.php/INFORMATIC118/2_Symmetric_cryptography.pdf
17. http://1lyk-evosm.thess.sch.gr/wordpress/wp-content/uploads/2014/03/parousiasi_pdf.pdf
18. https://eclass.aueb.gr/modules/document/file.php/INF208/Διαλέξεις/crypto13-03-basic-cryptosystems.pdf
19. https://el.wikipedia.org/wiki/Κλασικά_κρυπτοσυστήματα
20. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%B4%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%BA%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D
21. http://cgi.di.uoa.gr/~klimn/cryptography/chapter_2-Stream_Ciphers.pdf
22. https://cryptography444.wordpress.com/κρυπτοσυστηματα/
23. https://olympias.lib.uoi.gr/jspui/bitstream/123456789/6998/1/%CE%9C.%CE%95.%20-%20%CE%A0%CE%91%CE%A3%CE%A7%CE%91%CE%9B%CE%97%CE%A3%20%CE%A0%CE%91%CE%A0%CE%91%CE%9D%CE%99%CE%9A%CE%9F%CE%9B%CE%91%CE%9F%CE%A5.pdf
24. http://www.physics4u.gr/articles/2006/quantum_crypto.html
25. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/143/tlp_000416.pdf?sequence=1
26. https://cryptography444.wordpress.com/%CE%BA%CF%81%CF%85%CF%80%CF%84%CE%BF%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%B1/
27. http://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies_foitht wn/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1%20ceid6248.pdf

28. https://docplayer.gr/1558047-Systimata-pistopoiisis-kryptografia-psifiakes-ypografes.html
29. https://eclass.hmu.gr/modules/document/file.php/TP122/03.%CE%95%CF%81%CE%B3%CE%B1%CF%83%CF%84%CE%AE%CF%81%CE%B9%CE%B1/Lab%203%20-%20Symmetric/Lab3-Symmetric.pdf
30. https://newtech-pub.com/wp-content/uploads/2013/10/kef-ergasthriakes.pdf
31. http://digilib.teiemt.gr/jspui/bitstream/123456789/358/1/022013108.pdf
32. http://users.uom.gr/~steph/material/crypto/HAC_Ch06.pdf
33. https://newtech-pub.com/wp-content/uploads/2013/10/kef-praktika.pdf
34. http://utopia.duth.gr/~vkatos/documents/the_book/ch3.pdf
35. https://repository.kallipos.gr/bitstream/11419/5467/1/Kallipos_Zachos-Ch16.pdf
36. https://docplayer.gr/31154787-Kryptografia-kai-asfaleia.html
37. https://repository.kallipos.gr/bitstream/11419/5440/1/ch1.pdf
38. https://docplayer.gr/12264671-Symmetrikoi-algorithmoi-kryptografisis-dedomenon-i-periptosi-toy-algorithmoy-aes.html
39. http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kruptografia.htm
40. http://www.ebusinessforum.gr/old/content/downloads/smart_all.pdf
41. http://docplayer.gr/32727637-Diatmimatiko-metaptyhiako-programma-ilektroniki-kai-epexergasia-tis-pliroforias.html
42. http://cosynet.auth.gr/sites/default/files/Thesis/MAKRIS%20Cryptography%20with%20Chaos%20%CE%95%CE%9B.pdf
43. http://delab.csd.auth.gr/~katsaros/web%20security.pdf
44. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/5896/1/AES.pdf
45. https://gramenos.wixsite.com/smarthood/single-post/smartcard

Κβαντική Διαμοίραση Κλειδιού:

1. https://greekphysics.wordpress.com/2010/10/04/γεννήτρια-τυχαίων-αριθμών-αξιοποιεί/
2. https://www.seat.gr/seat-cars/connected-cars.html
3. http://futuremobility.gr/connectivity/why-connected-vehicles-are-important

4. https://www.techgear.gr/connected-cars-kaspersky-lab-6089
5. https://m.naftemporiki.gr/story/1145524
6. https://infoservice.com.gr/technologia/sindede%C2%B5ena-aftokinita-i-prosvasi-sta-dedo%C2%B5ena-tou-ochi%C2%B5atos-tha-ine-klidomeni/
7. https://www.cnn.gr/tech/story/68901/eyalota-ta-syndedemena-aytokinita-stis-diatheseis-ton-xaker
8. https://tvxs.gr/news/sci-tech/i-kbantiki-texnologia-allazei-tin-psifiaki-mas-zoi
9. https://tinanantsou.blogspot.com/2018/05/blog-post_2.html
10. http://www.enet.gr/?i=news.el.article&id=153494
11. https://gr.euronews.com/2019/07/30/i-kbantiki-texnologia-ejafanizei-to-xakarisma
12. http://physics4u.gr/blog/2019/08/03/%CE%B7-%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE-%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1-%CE%B1%CE%BB%CE%BB%CE%AC%CE%B6%CE%B5%CE%B9-%CF%84%CE%B7%CE%BD-%CF%88%CE%B7%CF%86/
13. https://www.athensvoice.gr/life/technology/582533_tyhaioi-arithmoi-nteterminismos-kai-tyhaiotita-ginontai-ena
14. http://users.auth.gr/ganoulis/quantum/THMMY-2020/32-%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE%20%CE%94%CE%B9%CE%B1%CE%BD%CE%BF%CE%BC%CE%AE%20%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D.pdf
15. https://www.sigmalive.com/news/scitech/technology/362043/tsip-kryptografisis-se-forites-syskeves
16. https://el.wikipedia.org/wiki/%CE%9A%CE%B2%CE%AC%CE%B6%CE%B1%CF%81
17. http://quantumgazette.blogspot.com/2016/09/the-bb84-protocol-for-quantum-key.html
18. https://www.sjsu.edu/people/raymond.kwok/courses/physics/phys120s-lab/squid/

Ατομικά Ρολόγια:

1. http://physics4u.gr/blog/2018/02/15/%CF%86%CE%BF%CF%81%CE%B7%CF%84%CF%8C-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9-%CF%80%CE%BF%CF%85-%CE%BC%CE%B5%CF%84%CF%81%CE%AC%CE%B5%CE%B9-%CF%84%CE%B7%CE%BD-%CE%B2/
2. https://repository.kallipos.gr/bitstream/11419/1495/3/02_chapter_07.pdf
3. http://ikee.lib.auth.gr/record/130985/files/GRI-2013-9825.pdf
4. http://aliatas.blogspot.com/2017/11/blog-post_4.html
5. https://enfo.gr/ar568
6. https://ir.lib.uth.gr/xmlui/bitstream/handle/11615/41181/10847.pdf?sequence=1&isAllowed=y
7. https://www.rizospastis.gr/story.do?id=9497976
8. https://www.avgi.gr/entheta/prisma/267902_iliakes-ekrixeis-magnitika-skoinia-kai-magnitika-kloybia
9. https://www.orionas.gr/_presentations/Ngizani-KosmikiAktinovolia.pdf
10. https://www.newsbomb.gr/kosmos/story/822960/simantiki-anakalypsi-h-isxyri-kosmiki-aktinovolia-poy-vomvardizei-ti-gi-exei-exogalaxiaki-proeleysi
11. https://physicsgg.me/2016/11/29/%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AE%CE%B8%CE%B7%CE%BA%CE%B5-%CF%84%CE%BF-%CF%80%CE%B9%CE%BF-%CE%B1%CE%BA%CF%81%CE%B9%CE%B2%CE%AD%CF%82-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9-%CF%83%CF%84/
12. https://www.energia.gr/article/55742/pyrhnika-rologia-neo-rekor-ston-hrono
13. https://skai.gr/neo-pagkosmio-rekor-gia-to-pio-akrives-roloi-ston-kosmo/amp
14. https://www.energia.gr/article/34975/eftiaxan-to-pio-akrives-roloi-toy-kosmoy-
15. http://www.hellenicaworld.com/Technology/gr/AtomikoRoloi.html
16. https://docplayer.gr/46662304-Apo-ta-atomika-sta-optika-rologia.html
17. https://energypress.gr/news/rologia-me-pyriniki-akriveia
18. https://www.eklogika.gr/inews/Atomika-rologia-epibebaionoun-ti-schetikotita-tou-chronou-01-01-1970

19. https://gr.euronews.com/2013/04/02/swiss-sets-sights-on-miniscule-atomic-clock
20. https://www.rizospastis.gr/story.do?id=2776138
21. https://www.pemptousia.gr/2012/07/i-metrisi-tou-chronou-ke-ta-atomika-rol/
22. https://www.skai.gr/atomiko-roloi-akriveias-xanei-mono-ena-deyterolepto-ana-300-ekatommy
23. https://www.meteo24news.gr/2015/07/atomika-rologia-metroun-ta-ifaisteia.html?m=1
24. https://www.cnn.gr/tech/story/33577/epanaprosdiorizetai-i-ennoia-tis-oras
25. https://www.skai.gr/dimiourgithike-to-pio-akrives-roloi-ston-kosmo
26. http://physics4u.gr/blog/2017/03/28/ατομικά-ρολόγια-επιβεβαιώνουν-τη-σχε/
27. https://www.newsbeast.gr/technology/arthro/634525/kataskeuastike-to-pio-akrives-roloi-ston-kosmo
28. https://www.tovima.gr/2009/03/29/science/apo-ta-atomika-sta-optika-rologia/
29. https://www.protothema.gr/technology/article/469790/neo-rekor-akriveias-apo-atomiko-roloi-den-hanei-oute-deuterolepto-sta-15-disekatommuria-hronia/
30. https://www.energia.gr/article/78448/neo-pagkosmio-rekor-akriveias-apo-peiramatiko-atomiko-roloi-strontioy-poy-den-hanei-oyte-ena-deyterolepto-sta-5-disekatommyria-hronia
31. https://www.thetoc.gr/new-life/article/to-atomiko-roloi-pou-den-xanei-oute-ena-deuterolepto/
32. https://unboxholics.com/news/tech/29256-forito-atomiko-roloi-pou-metraei-tin-varytita
33. https://www.in.gr/2012/11/13/tech/o-ainstain-kai-ta-atomika-rologia-sti-meleti-toy-eswterikoy-tis-gis/
34. https://www.tovima.gr/2017/07/04/science/brethike-to-problima-sta-atomika-rologia-toy-galileo/
35. http://www.focusmag.gr/forito-roloi-akrivias-chrisimopiite-proti-fora-gia-na-metrai-tin-varytita/
36. http://www.enikonomia.gr/technology/127907,to-pio-stathero-roloi-ston-kosmo-einai-gegonos.html
37. https://m.naftemporiki.gr/story/1219736/neo-petuximeno-kras-test-gia-ti-sxetikotita-tou-xronou

38. https://www.newscientist.com/article/mg23331184-900-atomic-clocks-make-best-measurement-yet-of-relativity-of-time/
39. http://atlaswikigr.wikifoundry.com/page/%CE%A0%CF%8E%CF%82+%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF+%CF%84%CE%BF+%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C+%CF%81%CE%BF%CE%BB%CF%8C%CE%B9+%CF%80%CE%AF%CE%B4%CE%B1%CE%BA%CE%B1+%CE%BA%CE%B1%CE%B9%CF%83%CE%AF%CE%BF%CF%85%3B
40. http://www.45dimpatras.gr/afieromata/afto-to-kserate/106-pos-douleyoun-afta-ta-atomika-rologia-pou-deixnoun-me-toso-tromaktiki-akriveia-ton-xrono
41. https://www.in.gr/2017/03/27/tech/atomika-rologia-epibebaiwnoyn-ti-sxetikotita-toy-xronoy/
42. https://physicsgg.me/2014/01/23/%CF%84%CE%BF-%CE%B1%CE%BA%CF%81%CE%B9%CE%B2%CE%AD%CF%83%CF%84%CE%B5%CF%81%CE%BF-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9/
43. https://allflavors.net/eftiaxan-neo-optiko-atomiko-roloi-pou-epanakathorizi-to-defterolepto/
44. https://physicsgg.me/2013/07/10/%CE%BD%CE%AD%CE%BF-%CE%BF%CF%80%CF%84%CE%B9%CE%BA%CF%8C-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9-%CF%8D%CF%88%CE%B9%CF%83%CF%84%CE%B7%CF%82-%CE%B1%CE%BA%CF%81%CE%AF/
45. https://www.tovima.gr/2013/07/10/science/atomiko-roloi-yposxetai-na-dwsei-neo-orismo-ston-xrono/
46. https://www.tanea.gr/2010/02/23/world/eftiaksan-to-pio-akribes-roloi-toy-kosmoy/
47. https://physicsgg.me/2013/08/23/%CF%84%CE%BF-%CF%80%CE%B9%CE%BF-%CE%B1%CE%BE%CE%B9%CF%8C%CF%80%CE%B9%CF%83%CF%84%CE%BF-

%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9/
48. https://www.in.gr/2008/02/16/tech/peiramatiko-roloi-menei-akribes-gia-200-ekatommyria-xronia/
49. https://www.taxheaven.gr/news/3346/atomiko-roloi?output=printer
50. https://www.kathimerini.gr/96383/article/epikairothta/kosmos/to-roloi-poy-xanei-1-ka8e-30-dis-xronia
51. https://www.tovima.gr/2012/03/12/science/pyrinika-rologia-neo-rekor-ston-xrono/
52. https://www.cnn.gr/tech/story/33577/nea-ereyna-allazei-tin-ora
53. https://www.iefimerida.gr/news/140115/επιστήμονες-έφτιαξαν-το-πιο-ακριβές-ρολόι-στον-κόσμο-δεν-χάνει-δευτερόλεπτο-σε-5-δισ-χρό
54. https://m.naftemporiki.gr/story/689205/atomika-rologia-neas-genias
55. https://el.wikipedia.org/wiki/Ατομικό_ρολόι
56. https://www.skai.gr/roloi-strontiou-den-xanei-oute-deyterolepto-sta-5-dis-xronia-video
57. http://www.physics4u.gr/articles/2006/sundial_atomic.html
58. http://www.physics4u.gr/faq/atomicclock.html
59. http://users.uoa.gr/~nektar/science/physics/atomic_clock.htm
60. https://gr.dreamstime.com/%CE%B5%CE%BA%CE%B4%CE%BF%CF%84%CE%B9%CE%BA%CE%AE-%CF%86%CF%89%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF-%CF%8C%CE%B9-atomichron-image53075797
61. http://physics4u.gr/blog/2018/02/15/%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9-%CE%B3%CE%B9%CE%B1-%CF%80%CE%BB%CE%BF%CE%AE%CE%B3%CE%B7%CF%83%CE%B7-%CF%83%CF%84%CE%BF-%CE%B2%CE%B1%CE%B8%CF%8D-%CE%B4%CE%B9/
62. http://www.physics4u.gr/news/2005/scnews1983.html

63. https://physics4u.wordpress.com/2018/02/15/%CF%86%CE%BF%CF%81%CE%B7%CF%84%CF%8C-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%81%CE%BF%CE%BB%CF%8C%CE%B9-%CF%80%CE%BF%CF%85-%CE%BC%CE%B5%CF%84%CF%81%CE%AC%CE%B5%CE%B9-%CF%84%CE%B7%CE%BD-%CE%B2/
64. https://www.newspepper.gr/dite-to-atomiko-roloi-gia-tin-ploigisi-sto-diastima-foto/
65. https://physicsgg.me/2014/06/24/το-απόλυτο-παγκόσμιο-ρολόι-και-η-κβαντ/
66. http://ikee.lib.auth.gr/record/129871/files/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%95%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%20%CE%97%CE%BB%CE%B9%CE%BF%CF%80%CE%BF%CF%8D%CE%BB%CE%BF%CF%85%20%CE%95%CE%BB%CF%80%CE%AF%CE%B4%CE%B1%CF%82.pdf
67. https://el.wikipedia.org/wiki/%CE%9A%CE%BF%CF%83%CE%BC%CE%B9%CE%BA%CE%AD%CF%82_%CE%B1%CE%BA%CF%84%CE%AF%CE%BD%CE%B5%CF%82
68. https://el.wiktionary.org/wiki/%CF%87%CF%81%CE%BF%CE%BD%CE%B9%CF%83%CE%BC%CF%8C%CF%82
69. https://el.wikipedia.org/wiki/%CE%91%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C_%CF%81%CE%BF%CE%BB%CF%8C%CE%B9
70. https://www.kathimerini.gr/553437/article/epikairothta/episthmh/neo-rekor-akriveias-apo-peiramatiko-amerikaniko-roloi
71. https://www.rizospastis.gr/story.do?id=308579&textCriteriaClause=%2B%CE%91%CE%A4%CE%9F%CE%9C%CE%99%CE%9A%CE%9F+%2B%CE%A1%CE%9F%CE%9B%CE%9F%CE%99
72. https://www.chemist.gr/%CF%81%CE%BF%CE%BB%CF%8C%CE%B3%CE%B9%CE%B1-%CF%83%CF%84%CF%81%CE%BF%CE%BD%CF%84%CE%AF%CE%BF%CF%85-87/
73. https://physics4u.wordpress.com/2010/02/17/%CE%AD-%CE%AC-%CF%8C-%CE%AC/

74. http://www.tsiridesfoundation.com/cgibin/hweb?-A=140,printer.html&-V=webcontent
75. http://www.newsnowgr.com/article/1103301/forito-atomiko-roloi-pou-metraei-tin-varytita.html
76. https://techblog.gr/gadgets/new-atomic-clock-doesnt-lose-a-sec-6391/
77. https://newpost.gr/tech/5c1257cb56dccb7e13df744a/neo-optiko-atomiko-roloi-ypsisths-akribeias
78. https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B9%CE%B1%CE%BA%CE%AE_%CE%AD%CE%BA%CE%BB%CE%B1%CE%BC%CF%88%CE%B7
79. http://www.enet.gr/?i=news.el.article&id=411420
80. https://www.tovima.gr/2014/06/21/science/kaisio-yliko-gia-to-teleio-roloi/
81. https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/2590/gegasa_ins.pdf?sequence=3
82. https://www.mdpi.com/1424-8220/18/10/3205/htm
83. http://www.physics4u.gr/news/2004/scnews1289.html
84. https://www.darpa.mil/news-events/2013-08-29
85. http://physics4u.gr/blog/2010/02/17/%CE%AD-%CE%AC-%CF%8C-%CE%AC/
86. http://cosray.phys.uoa.gr/conference%20proc./E123.pdf
87. https://slideplayer.gr/slide/11638534/
88. https://www.naftemporiki.gr/story/689205
89. https://xhmeiapedia.blogspot.com/2017/10/oct02.html
90. https://tinanantsou.blogspot.com/2018/02/blog-post_15.html
91. https://www.eef.edu.gr/el/arthra/iliaki-drastiriotita/

Κβαντικοί Αισθητήρες:

1. https://el.wikipedia.org/wiki/%CE%98%CF%8C%CF%81%CF%85%CE%B2%CE%BF%CF%82
2. https://docplayer.gr/7041938-Syntheti-antistasi-i-empe-isi.html
3. http://moag.phys.uoa.gr/moag_gr/sites/default/files/moag_files/Telecom_Chapter_2.pdf

4. https://www.nature.com/articles/s41378-019-0089-7
5. http://ikee.lib.auth.gr/record/290567/files/Diplwmatikh_Kydonopoulos_5080.pdf
6. https://physics4u.wordpress.com/2009/06/29/%ce%ae-%cf%8d-%ce%ac/
7. http://147.102.192.206/ergasthria/askhseis_ergasthrion/magnhtikes_metrhseis.pdf
8. https://eoc.org.cy/en/index.php?id=1001
9. digilabcfu.weebly.com/uploads/1/0/2/3/10237615/14_syntheth_antistash.pdf
10. https://illustrationprize.com/el/298-photodiode.html
11. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5317166/
12. http://www.physics4u.gr/articles/2006/susy.html
13. https://thesis.ekt.gr/thesisBookReader/id/16359#page/1/mode/2up
14. https://el.bccrwp.org/solution/heat-vs-specific-heat/
15. http://195.134.76.37/old_site_10-7-2016/courses/organologia/PDF/Ch05_1xxy.pdf
16. http://users.teiath.gr/kskourol/heat.pdf
17. https://iopscience.iop.org/book/978-0-7503-1635-4/chapter/bk978-0-7503-1635-4ch1
18. https://sites.google.com/site/squiddevices/home
19. https://www.slac.stanford.edu/econf/C0604032/talks/snic_ullom.pdf
20. https://www.sense-pro.org/lll-sensors/more-lll-sensors
21. http://web.mit.edu/figueroagroup/ucal/ucal_tes/
22. https://arxiv.org/pdf/1907.06480.pdf
23. https://www.mdpi.com/1424-8220/16/7/953/htm
24. https://www.sciencedaily.com/releases/2020/03/200319161529.htm
25. https://en.wikipedia.org/wiki/SQUID
26. https://arxiv.org/ftp/arxiv/papers/1407/1407.0691.pdf
27. http://giryd.de/en/projects.php/_/1/
28. http://venus.ifca.unican.es/~xray/XEUS/archivopapers/TESIrwinHilton.pdf
29. https://www.wired.com/story/quantum-physicists-found-a-new-safer-way-to-navigate/
30. https://tel.archives-ouvertes.fr/tel-01735459/document
31. https://iopscience.iop.org/article/10.1088/1361-6455/ab56a9
32. http://www.physics4u.gr/news/2003/scnews1138b.html

33. https://www.nature.com/articles/s41598-018-37655-8
34. https://repository.kallipos.gr/bitstream/11419/5052/1/02_chapter_%2004.pdf
35. https://onlinelibrary.wiley.com/doi/full/10.1002/qute.201900134
36. http://physics4u.gr/blog/2010/07/22/%CE%AD-%CF%8D-%CE%AE-p/
37. https://www.scientificamerican.com/article/what-are-josephson-juncti/
38. https://www.alfavita.gr/epistimi/288052_ta-pano-kato-stin-epistimoniki-koinotita-apo-ti-mystiriodi-skoteini-energeia
39. https://www.cnn.gr/style/politismos/story/121502/neo-psifiako-planitario-ayti-ti-deytera-mas-kalei-se-mia-katadysi-sto-mystirio-tis-skoteinis-ylis
40. https://iopscience.iop.org/article/10.1088/0953-4075/48/20/202001
41. https://science.fandom.com/el/wiki/%CE%A3%CE%BA%CE%BF%CF%84%CE%B5%CE%B9%CE%BD%CE%AE_%CE%95%CE%BD%CE%AD%CF%81%CE%B3%CE%B5%CE%B9%CE%B1
42. https://eclass.uniwa.gr/modules/document/file.php/ET240/%CE%A3%CE%97%CE%9C%CE%95%CE%99%CE%A9%CE%A3%CE%95%CE%99%CE%A3%20%CE%9C%CE%91%CE%98%CE%97%CE%9C%CE%91%CE%A4%CE%9F%CE%A3/A%CE%A3%CE%9A%CE%97%CE%A3%CE%97_4/%CE%A0%CE%91%CE%A1%CE%9F%CE%A5%CE%A3%CE%99%CE%91%CE%A3%CE%97.pdf
43. https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%8E%CE%B8%CE%B5%CF%81%CE%BC%CE%B7_%CE%B1%CE%BD%CF%84%CE%AF%CE%B4%CF%81%CE%B1%CF%83%CE%B7
44. https://www.secnews.gr/170574/gps-pyksida-kvantiki/
45. https://www.kathimerini.gr/994728/article/epikairothta/episthmh/dhmioyrgh8hke-h-prwth-kvantikh-py3ida-ston-kosmo
46. https://www.ethnos.gr/kosmos/3996_kbantiki-pyxida-gia-ploigisi-aney-doryforon
47. https://www.offsite.com.cy/eidiseis/tech/dimioyrgithike-i-proti-kbantiki-pyxida
48. https://www.news247.gr/technologia/dimioyrgithike-proti-ston-kosmo-kvantiki-pyxida.6666501.html
49. https://sputniknews.gr/texnologia/201811121366447-kvantiki-pixida-gps-imperial-college/
50. https://www.fortunegreece.com/article/dimiourgithike-i-proti-kvantiki-pixida-ston-kosmo-vinteo/

51. https://www.iefimerida.gr/news/457837/poio-gps-dimioyrgithike-i-proti-ston-kosmo-kvantiki-pyxida-eikona
52. https://ecozen.gr/2018/11/proti-kvantiki-pyxida/
53. https://opencourses.uoa.gr/modules/document/file.php/CHEM103/%CE%94%CE%B9%CE%B4%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CF%8C%20%CE%A0%CE%B1%CE%BA%CE%AD%CF%84%CE%BF/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/pdf/%CE%95%CE%BD%CF%8C%CF%84%CE%B7%CF%84%CE%B1%205%3A%20%CE%9C%CE%AD%CE%B8%CE%BF%CE%B4%CE%BF%CE%B9/%CE%95%CF%80%CE%B9%CE%BA%CF%8D%CF%81%CF%89%CF%83%CE%B7-%CE%95%CF%80%CE%B1%CE%BB%CE%AE%CE%B8%CE%B5%CF%85%CF%83%CE%B7%20%CE%91%CE%BD%CE%B1%CE%BB%CF%85%CF%84%CE%B9%CE%BA%CF%8E%CE%BD%20%CE%9C%CE%B5%CE%B8%CF%8C%CE%B4%CF%89%CE%BD%202.pdf
54. https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2018-11/Responsible%20Innovation%20in%20Quantum%20Technologies%20applied%20to%20Defence%20and%20National%20Security%20PDFNov18.pdf
55. http://physics4u.gr/blog/2018/05/29/%CF%8C%CF%83%CE%B1-%CE%B8%CE%B1-%CE%B8%CE%AD%CE%BB%CE%B1%CF%84%CE%B5-%CE%BD%CE%B1-%CE%BC%CE%AC%CE%B8%CE%B5%CF%84%CE%B5-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD-%CF%83%CE%BA%CE%BF%CF%84%CE%B5%CE%B9%CE%BD/
56. https://physicsgg.me/2018/11/10/%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CF%85%CE%BE%CE%AF%CE%B4%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%80%CE%BB%CE%BF%CE%AE%CE%B3%CE%B7%CF%83%CE%B7-%CE%AC%CE%BD%CE%B5%CF%85-%CE%B4/
57. https://en.wikipedia.org/wiki/Quantum_sensor
58. http://mil-embedded.com/news/arl-scientists-make-progress-in-quantum-sensing-research/

59. https://www.fierceelectronics.com/sensors/quantum-sensor-covers-entire-rf-range
60. https://www.army.mil/article/212935/army_researchers_make_giant_leap_in_quantum_sensing
61. https://hackaday.com/2020/03/24/quantum-sensor-receives-from-0-hz-to-1000-ghz/
62. https://incompliancemag.com/quantum-sensor-could-help-soldiers-communicate-over-entire-radio-frequency-spectrum/
63. https://en.wikipedia.org/wiki/Josephson_effect
64. https://en.wikipedia.org/wiki/Pi_Josephson_junction
65. https://whatis.techtarget.com/definition/Josephson-junction
66. https://www.sciencedirect.com/topics/materials-science/josephson-junction
67. https://www.ellines.com/good-news/34600-ellinas-ereunitis-dimiourgise-protoporiaki-psifiaki-kamera-pou-blepei-to-aorato/
68. http://www.avgi.gr/article/10965/8196837/protoporiake-psephiake-kamera-pou-blepei-to-aorato-demiourgese-ellenas-ereunetes
69. https://www.amna.gr/anarussia/article/160994/Protoporiaki-psifiaki-kamera-pou-blepei-to-aorato-dimiourgise-Ellinas-ereunitis
70. https://www.sigmalive.com/news/scitech/technology/434273/psifiaki-kamera-me-aisthitira-cmos-vlepei-ta-aorata
71. http://www.ecgs.lu/wulg/gravimeters/
72. https://www.sciencedirect.com/topics/earth-and-planetary-sciences/gravimeter
73. https://www.altsantiri.gr/texnologia/349747/gia-proti-fora-kamera-vlepi-aorato-exetias-enos-tsip-grafenio-video/
74. https://www.electronicdesign.com/industrial-automation/article/21127094/army-scientists-create-innovative-quantum-sensor
75. https://www.evaluationengineering.com/applications/article/21131337/army-scientists-create-innovative-quantum-sensor
76. https://science.slashdot.org/story/20/03/21/0014219/scientists-create-quantum-sensor-that-covers-entire-radio-frequency-spectrum
77. https://en.wikipedia.org/wiki/Transition-edge_sensor
78. https://www.researchgate.net/publication/324150773_Quantum_Sensing_for_High_Energy_Physics

79. https://www.computerweekly.com/opinion/Quantum-sensing-a-new-frontier-for-revolutionary-technology
80. https://www.darpa.mil/program/quantum-assisted-sensing-and-readout
81. https://www.tanea.gr/2017/09/07/science-technology/i-pio-isxyri-iliaki-eklampsi-edw-kai-12-xronia/
82. https://www.cnn.gr/tech/story/96419/h-pio-isxyri-iliaki-eklampsi-tis-teleytaias-12etias-vid
83. http://www.physics4u.gr/faq/solarflares.html
84. https://www.iefimerida.gr/kosmos/iliakes-eklampseis-kai-diastimikes-kataigides
85. http://www.indeepanalysis.gr/episthmes/anichneyontas-thn-skoteinh-ylh
86. https://www.in.gr/2020/06/18/tech/skoteini-yli-ypogeios-anixneytis-stin-italia-parexei-tin-proti-endeiksi-tis-yparksis-tou-aksioniou/
87. https://en.wikipedia.org/wiki/Gravimeter
88. https://www.britannica.com/technology/gravimeter
89. https://en.wikipedia.org/wiki/Quantum_imaging
90. https://www.naftemporiki.gr/story/1412062
91. https://www.onera.fr/en/news/a-first-for-a-cold-atom-accelerometer
92. https://physicsgg.me/2018/03/17/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-%CF%85%CF%80%CE%B5%CF%81%CE%B1%CE%B3%CF%8E%CE%B3%CE%B9%CE%BC%CE%B7-%CF%83%CF%85%CF%83%CE%BA%CE%B5%CF%85%CE%AE-%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9/
93. https://www.birmingham.ac.uk/research/quest/emerging-frontiers/quantum-sensors.aspx
94. https://www.osa-opn.org/home/articles/volume_30/september_2019/features/quantum_sensors_a_revolution_in_the_offing/
95. https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html
96. https://en.wikipedia.org/wiki/Rydberg_atom
97. http://physics4u.gr/blog/2018/11/11/%CE%B7-%CF%80%CF%81%CF%8E%CF%84%CE%B7-%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE

%AE-%CF%80%CF%85%CE%BE%CE%AF%CE%B4%CE%B1-%CF%80%CE%BF%CF%85-%CF%87%CF%81%CE%B7%CF%83%CE%B9%CE%BC%CE%BF%CF%80%CE%BF/
98. https://core.ac.uk/download/pdf/38467782.pdf
99. https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%B9%CE%BA%CE%AE_%CE%B4%CE%B9%CF%80%CE%BF%CE%BB%CE%B9%CE%BA%CE%AE_%CF%81%CE%BF%CF%80%CE%AE
100. https://el.wikipedia.org/wiki/%CE%98%CE%B5%CF%81%CE%BC%CE%BF%CF%87%CF%89%CF%81%CE%B7%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1
101. http://pesxm10.chemeng.upatras.gr/sites/default/files/papers/P01/Alatas_extended_abstract_10thPESXM.pdf
102. http://opencourses.teiwest.gr/modules/document/file.php/CIED106/%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CE%B9%CF%82%202016%20-%202017/Telecom_Systems_I_Lectures_3.pdf
103. https://eclass.uoa.gr/modules/document/file.php/MATH378/16_%CE%9A%CE%9F%CE%A3%CE%9C%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%91_%CE%9A%CE%9F%CE%A3%CE%9C%CE%91%CE%A3_%CE%93%CE%91%CE%96%CE%95%CE%91%CE%A3_2017.pdf
104. https://el.wikipedia.org/wiki/%CE%A6%CF%89%CF%84%CE%BF%CE%B4%CE%AF%CE%BF%CE%B4%CE%BF%CF%82
105. https://el.wikipedia.org/wiki/%CE%97%CF%87%CE%BF%CF%83%CE%B7%CE%BC%CE%B1%CE%BD%CF%84%CE%AE%CF%81%CE%B1%CF%82
106. https://startupper.gr/vipnews/55751/%CE%B7-%CE%B5%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1-%CF%83%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CE%AD%CF%87%CE%B5%CE%B9-%CF%83%CF%84%CE%BF-%CE%AD%CF%81%CE%B3%CE%BF-%CE%B1%CE%BD%CE%AC%CF%80%CF%84%CF%85%CE%BE%CE%B7/

107. https://science.fandom.com/el/wiki/%CE%98%CE%B5%CF%81%CE%BC%CE%BF%CF%87%CF%89%CF%81%CE%B7%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1
108. http://ikee.lib.auth.gr/record/290517/files/%CE%94%CE%99%CE%A0%CE%9B%CE%A9%CE%9C%CE%91%CE%A4%CE%99%CE%9A%CE%97_%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%99%CE%91.pdf
109. http://amitos.library.uop.gr/xmlui/bitstream/handle/123456789/4661/%CE%A0%CF%84%CF%85%CF%87%CE%B9%CE%B1%CE%BA%CE%AE_%CE%93%CE%B1%CF%81%CE%B1%CE%BD%CF%84%CE%B6%CE%B9%CF%8E%CF%84%CE%B7%CF%82%20%CE%A0%CE%B5%CF%81%CE%B9%CE%BA%CE%BB%CE%AE%CF%82_%CE%A0%CE%9C%CE%A3%20%CE%A4%CE%B7%CE%BB%CE%B5%CF%80%CE%B9%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%B1%CE%BA%CE%AC%20%CE%A3%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1.pdf?sequence=1&isAllowed=y
110. https://el.wikipedia.org/wiki/%CE%98%CE%B5%CF%81%CE%BC%CE%B9%CE%BA%CE%AE_%CE%B1%CE%B3%CF%89%CE%B3%CE%B9%CE%BC%CF%8C%CF%84%CE%B7%CF%84%CE%B1
111. https://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%BF%CF%84%CE%B5%CE%B9%CE%BD%CE%AE_%CE%B5%CE%BD%CE%AD%CF%81%CE%B3%CE%B5%CE%B9%CE%B1
112. https://ocp.teiath.gr/modules/document/file.php/NAFP_UNDER107/%CE%95%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CF%8C%20%CF%85%CE%BB%CE%B9%CE%BA%CF%8C/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/05_%CE%95%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CF%83%CF%83%CF%8C%CE%BC%CE%B5%CE%BD%CE%B1_%CE%BA%CF%85%CE%BA%CE%BB%CF%8E%CE%BC%CE%B1%CF%84%CE%B1_%CE%BC%CF%8C%CE%BD%CE%B9%CE%BC%CE%B7%CF%82_%CE%BA%CE%B1%CF%84%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7%CF%82%28%CE%95%CE%B1%CF%81%CE%B9%CE%BD%CF%8C_2015%29.pdf
113. https://www.researchgate.net/publication/266973951_Giant_Rydberg_excitons_in_the_copper_oxide_Cu2O

114. https://el.mort-sure.com/blog/difference-between-specific-heat-capacity-and-heat-capacity/
115. https://el.wikipedia.org/wiki/%CE%92%CE%B1%CF%81%CF%85%CF%84%CE%AE%CE%BC%CE%B5%CF%84%CF%81%CE%BF
116. https://thmarblog.wordpress.com/2018/11/26/%CE%B2%CE%B1%CF%81%CF%85%CF%84%CF%8C%CE%BC%CE%B5%CF%84%CF%81%CE%B1/
117. https://science.fandom.com/el/wiki/%CE%A5%CF%80%CE%B5%CF%81%CF%83%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%AF%CE%B1
118. https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/u.s._army_scientists_create_innovative_quantum_sensor.html
119. https://www.army.mil/article/233809/army_scientists_create_innovative_quantum_sensor
120. https://www.techbriefs.com/component/content/article/tb/techbriefs/electronics-and-computers/25970
121. https://el.wikipedia.org/wiki/%CE%98%CE%B5%CF%81%CE%BC%CE%AF%CF%83%CF%84%CE%BF%CF%81
122. http://www.physics.ntua.gr/POPPHYS/software/MICROCOSM/PARTICLES/darkmatter.html
123. https://el.wikipedia.org/wiki/%CE%A3%CE%BA%CE%BF%CF%84%CE%B5%CE%B9%CE%BD%CE%AE_%CF%8D%CE%BB%CE%B7
124. https://gre.legatechnics.com/small-inexpensive-high-frequency-comb-signal-generator-222713
125. https://www.kathimerini.gr/992637/article/epikairothta/episthmh/skoteinh-ylh-pws-oi-episthmones-prospa8oyn-na-fwtisoyn-ena-megalo-mysthrio
126. https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%B5%CF%81%CF%83%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%AF%CE%B1
127. https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%B9%CE%BA%CE%AE_%CE%B5%CE%BC%CF%80%CE%AD%CE%B4%CE%B7%CF%83%CE%B7
128. https://www.real.gr/texnologia/arthro/kinezoi_epistimones_espasan_to_rekor_kryptografimenon_kbantikon_epikoinonion_meso_doryforou_se_apostasi_1_120_xlm-646246/

129. https://www.cnn.gr/tech/story/152611/quantum-flagship-h-emvlimatiki-protovoylia-tis-ee-gia-tis-kvantikes-texnologies
130. https://eclass.aspete.gr/modules/document/file.php/EHN223/TELECOM_notes_06_noise.pdf
131. https://m.naftemporiki.gr/story/1412062/kbantiki-puksida-gia-ploigisi-aneu-doruforon
132. https://www.techgear.gr/quantum-compass-2184
133. https://el.wikipedia.org/wiki/%CE%A3%CF%89%CE%BC%CE%B1%CF%84%CE%AF%CE%B4%CE%B9%CE%BF_%CE%AC%CE%BB%CF%86%CE%B1
134. http://www.physics.ntua.gr/POPPHYS/software/MICROCOSM/PARTICLES/grandunification.html
135. http://www.physics4u.gr/news/2006/scnews2328.html
136. https://www.bbc.com/news/business-47294704
137. https://technology.nasa.gov/patent/GSC-TOPS-32
138. https://phys.org/news/2019-03-quantum-sensor-cancer-treatment.html
139. https://link.springer.com/chapter/10.1007/10933596_3
140. https://www.eef.edu.gr/el/arthra/i-skoteini-energeia-to-kbantiko-keno-kai-to-problima-tis-kosmologikis-statheras/
141. https://www.sofokleousin.gr/rekor-kryptografimenon-kvantikon-epikoinonion-se-apostasi-1120-xl
142. https://qudev.phys.ethz.ch/static/content/science/Documents/phd/PhD-TobiasThiele.pdf
143. https://ecozen.gr/2019/04/symfonia-ee-kai-esa-gia-asfali-paneyropaiko-diktyo-kvantikon-epikoinonion/
144. https://illustrationprize.com/el/59-difference-between-photodiode-amp-phototransistor.html
145. https://school.astronomos.gr/c-class-less-13/
146. https://www.energia.gr/article/103419/pano-apo-400-ereynhtes-ypografoyn-to-kvantiko-manifesto-gia-thn-eyroph-
147. https://emea.gr/epicheiriseis/578679/symvoli-tis-thales-stin-anaptyxi-ton-eyropaikon-ypodomon/
148. https://physics4u.wordpress.com/2011/03/22/%CE%AF-%CE%AF-%CE%AF-lamb/

149. https://www.semanticscholar.org/paper/Studies-of-transition-edge-sensor-physics-%3A-thermal-Kinnunen/6b04052d0231b9d777c3dc78acc440926eb6bec3?p2df
150. https://www.semanticscholar.org/paper/Studies-of-transition-edge-sensor-physics-%3A-thermal-Kinnunen/6b04052d0231b9d777c3dc78acc440926eb6bec3?p2df
151. http://www.physics.ntua.gr/POPPHYS/60/susy.html
152. https://atlas.physicsmasterclasses.org/gr/zpath_supersym.htm
153. https://m.naftemporiki.gr/story/983751/ena-akomi-pligma-gia-tin-upersummetria
154. https://www.azosensors.com/article.aspx?ArticleID=299
155. https://physicstoday.scitation.org/doi/10.1063/PT.3.3995
156. https://seis.bristol.ac.uk/~phmgt/quantip/Tuto_SSPD.html
157. https://www.sciencedirect.com/science/article/abs/pii/S0304885308012328
158. https://enallaktikiagenda.gr/einai-skotini-energeia-epistimones-exigoun/
159. https://www.forth.gr/index_main.php?l=g&c=28&i=1546
160. https://www.mozaweb.com/el/Extra-Montela_3D-Pws_leitoyrgei_to_sonar-139779
161. https://el.wikipedia.org/wiki/%CE%A3%CF%8C%CE%BD%CE%B1%CF%81
162. https://www.nature.com/articles/s41598-018-30608-1
163. https://m.naftemporiki.gr/story/1097146
164. http://physics4u.gr/blog/2009/06/29/%CE%AE-%CF%8D-%CE%AC/
165. https://americanhistory.si.edu/collections/search/object/nmah_865075
166. https://zaguan.unizar.es/record/64440/files/texto_completo.pdf
167. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119552215.ch5
168. https://www.ceid.upatras.gr/webpages/faculty/alexiou/ahts/notes/kef02.pdf
169. https://arxiv.org/ftp/arxiv/papers/1807/1807.00729.pdf
170. https://physicstoday.scitation.org/doi/full/10.1063/PT.3.3995
171. https://www.epixeiro.gr/article/157898
172. http://www.ece.ucy.ac.cy/courses/ece305/lectures/7/ECE305_7.pdf
173. http://ikee.lib.auth.gr/record/292092/files/thesis_georgiadis_alexandros.pdf
174. http://www.supracon.com/cms/html/2/browse/232

175. http://library.tee.gr/digital/diplomatikes/athanasiou_ioannou_66782.pdf

Κβαντικό Ραντάρ:

1. http://www.dealnews.gr/roi/item/228743-Καναδάς-Κβαντικό-ραντάρ-για-εντοπισμό-stealth-αεροσκαφών#.XdWyBG5uJjo
2. http://pdplab.it.uom.gr/teaching/ince_2e_gr/Text/C14/Designprinciples_3.htm
3. http://www.securnet.gr/2017/06/blog-post_67.html
4. https://www.thetech.gr/2016/11/stealth.html
5. https://www.naftemporiki.gr/story/1598336
6. http://securityexpert.gr/2016/09/22/%CF%84%CE%BF-%CF%84%CE%AD%CE%BB%CE%BF%CF%82-%CF%84%CE%B7%CF%82-%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1%CF%82-stealth-%CE%BD%CE%AD%CE%BF-%CE%BA%CE%B9%CE%BD%CE%B5%CE%B6%CE%B9%CE%BA/
7. https://physics4u.wordpress.com/2016/09/26/%CE%B7-%CE%BA%CE%AF%CE%BD%CE%B1-%CE%B4%CE%BF%CE%BA%CE%B9%CE%BC%CE%AC%CE%B6%CE%B5%CE%B9-%CF%84%CE%BF-%CF%80%CF%81%CF%8E%CF%84%CE%BF-%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C-%CF%81%CE%B1/amp/
8. https://www.naftemporiki.gr/story/1344281/kbantiko-rantar-gia-ton-entopismo-stealth-aeroskafon-anaptussei-o-kanadas
9. https://www.ptisidiastima.com/quantum-radars/
10. https://www.onalert.gr/eksoplismoi/quantum-radar-etsi-h-kina-skopeuei-na-paroplisei-ta-stealth-f22-kai-f35-tvn-hpa/144391/
11. https://www.ptisidiastima.com/china-quantum-radar/
12. https://tecky.eu/to-neo-anti-stealth-yperoplo-legete-kvantiko-rantar/
13. https://www.limenikanea.gr/gr/kosmos/erxontai-ta-kbantika-rantar-–-giati-tha-allaksoun-ton-tropo-pou-ginetai-o-polemos-8368
14. https://eandt.theiet.org/content/articles/2019/04/could-quantum-radars-expose-stealth-planes/

15. https://www.fanaticalfuturist.com/2018/07/canada-and-uk-partner-to-develop-the-wests-first-quantum-radar/
16. http://www.dealnews.gr/roi/item/228743-%CE%9A%CE%B1%CE%BD%CE%B1%CE%B4%CE%AC%CF%82-%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C-%CF%81%CE%B1%CE%BD%CF%84%CE%AC%CF%81-%CE%B3%CE%B9%CE%B1-%CE%B5%CE%BD%CF%84%CE%BF%CF%80%CE%B9%CF%83%CE%BC%CF%8C-stealth-%CE%B1%CE%B5%CF%81%CE%BF%CF%83%CE%BA%CE%B1%CF%86%CF%8E%CE%BD#.X1kmdufivIU
17. https://www.kathimerini.gr/280011/article/epikairothta/kosmos/sta-skaria-to-ypertato-rantar
18. https://www.kathimerini.gr/world/280011/sta-skaria-to-ypertato-rantar/
19. https://www.limenikanea.gr/gr/kosmos/erxontai-ta-kbantika-rantar-%E2%80%93-giati-tha-allaksoun-ton-tropo-pou-ginetai-o-polemos-8368
20. https://egno.gr/2020/05/entopizontas-antikoimena-me-ena-neo-kvantiko-rantar/
21. https://www.popularmechanics.com/military/a28818232/quantum-radar/
22. https://newatlas.com/physics/quantum-radar-entangled-photons/
23. https://www.sciencealert.com/physicists-are-investigating-ways-to-use-entanglement-as-a-fancy-new-kind-of-radar
24. https://spie.org/news/quantum-radar?SSO=1
25. https://www.technologyreview.com/2019/08/23/75512/quantum-radar-has-been-demonstrated-for-the-first-time/
26. https://phys.org/news/2020-05-scientists-quantum-radar-prototype.html
27. https://www.fanaticalfuturist.com/2019/09/quantum-radar-that-neutralises-stealth-technology-demonstrated-for-first-time/
28. https://www.311institute.com/chinas-new-ghost-imaging-satellites-will-make-us-stealth-obsolete/
29. https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547
30. https://www.tovima.gr/2017/03/11/science/kbanta-enantion-stealth/
31. https://www.tovima.gr/2016/09/26/science/i-kina-dokimazei-to-prwto-kbantiko-rantar/

32. https://www.eef.gr/articles/entopizontas-antikeimena-me-ena-neo-kbantiko-rantar
33. https://kostasvakouftsis.blogspot.com/2017_05_30_archive.html
34. https://iellada.gr/kosmos/ta-pio-apisteyta-mystika-opla-ston-kosmo
35. https://m.naftemporiki.gr/story/1344281
36. https://edromos.gr/tis-epistimis-kai-tis-koinonias-f-408/
37. https://phys.org/news/2019-08-nanoworld.html
38. https://www.nature.com/articles/d41586-020-01588-y
39. https://arxiv.org/ftp/arxiv/papers/1908/1908.06850.pdf

Γενικά:

1. http://www.icsd.aegean.gr/website_files/metaptyxiako/618564813.pdf
2. http://ikee.lib.auth.gr/record/291310/files/diplomatiki.pdf
3. https://static.eudoxus.gr/books/52/chapter-2252.pdf
4. https://crypto.stanford.edu/~dabo/pubs/papers/quantum.pdf
5. http://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/1166-29.pdf
6. https://www.dsei.co.uk/__media/libraries/global-theatre/Dr-Paul-Kealy.pdf
7. https://dspace.lib.uom.gr/bitstream/2159/912/1/AggourasMsc2003.pdf
8. https://core.ac.uk/download/pdf/52104043.pdf
9. https://www.slideshare.net/marynasta/quantum-cryptography-mnastakou
10. https://docplayer.gr/30478762-Panepistimio-aigaioy-kvantiki-kryptografia-kvantiki-kryptanalysi-iplomatiki-ergasia.html
11. https://el.wikipedia.org/wiki/%CE%9C%CE%AD%CE%BB%CE%B1%CE%BD_%CF%83%CF%8E%CE%BC%CE%B1
12. https://docplayer.gr/amp/30478762-Panepistimio-aigaioy-kvantiki-kryptografia-kvantiki-kryptanalysi-iplomatiki-ergasia.html
13. http://www.klouras.chem.upatras.gr/attachments/article/9/12_Measurements%20and%20Heisenberg%27s%20uncertainty%20principle.pdf

14. https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/6048/tsetsilam_quantum.pdf
15. http://apothesis.teicm.gr/xmlui/bitstream/handle/123456789/829/vronteli.pdf?sequence=1&isAllowed=y
16. http://www.physics4u.gr/news/2004/scnews1377.html
17. 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
18. https://www.newsbeast.gr/weekend/arthro/3306993/ti-ine-o-kvantikos-ipologistis-ke-pos-tha-allaxi-tin-kathimerinotita-mas
19. https://gorganews.gr/i-nea-epanastasi-stis-stratiotikes-ypotheseis/
20. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/8058/1/Quantum%20Error%20Correction%20Diploma.pdf
21. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/4136/7/Stamatiou-PhD-UPatras-2010.pdf
22. https://drops.dagstuhl.de/opus/volltexte/2018/8660/pdf/dagrep_v007_i010_p001_17401.pdf
23. http://physics4u.gr/blog/2019/07/06/%CE%B7-%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE-%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE

%B3%CE%B9%CE%BA%CE%AE-%CE%B5%CF%80%CE%B1%CE%BD%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7-%CE%BE%CE%B5/

24. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%B1%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7
25. https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/6048/tsetsilam_quantum.pdf
26. http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/2633/cse_39095.pdf?sequence=5&isAllowed=y
27. http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/3445/%CE%97%20%CE%95%CE%9E%CE%95%CE%9B%CE%99%CE%9E%CE%97%20%CE%A4%CE%97%CE%A3%20%CE%9A%CE%A1%CE%A5%CE%A0%CE%A4%CE%9F%CE%93%CE%A1%CE%91%CE%A6%CE%99%CE%91%CE%A3.pdf
28. https://dspace.lib.uom.gr/bitstream/2159/13404/2/KourtelisMsc2008.pdf
29. http://olympias.lib.uoi.gr/jspui/bitstream/123456789/6998/1/M.E.%20-%20ΠΑΣΧΑΛΗΣ%20ΠΑΠΑΝΙΚΟΛΑΟΥ.pdf
30. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/11560/1/ΜΔΕ%20Αλγόριθμοι%20Κρυπτογράφησης%20Διαμοιραζόμενου%20Κλειδιού%20Θεωρία%20και%20Εφαρμογές.pdf
31. https://repository.kallipos.gr/bitstream/11419/5439/1/main-KOY.pdf
32. https://www.researchgate.net/publication/328475176_E_Kbantike_Technologia_sten_Aichme_tes_Amyntikes_Ereunas_Kbantiko_rantar_Kbantike_kryptographia_Quantum_Technologies_in_the_Frontier_of_Defence_Research_Quantum_Radar_Quantum_Cryptography_in_Greek

33. https://peopleinaction.wordpress.com/2012/10/19/%CF%83%CE%B5-%CE%B1%CE%BC%CF%86%CE%B9%CE%B2%CE%BF%CE%BB%CE%AF%CE%B1-%CE%B7-%CE%B1%CF%80%CF%81%CE%BF%CF%83%CE%B4%CE%B9%CE%BF%CF%81%CE%B9%CF%83%CF%84%CE%AF%CE%B1-%CF%84%CE%BF%CF%85-heisenberg/
34. http://users.auth.gr/ganoulis/quantum/THMMY-2020/26-%CE%9A%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%AE%20%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1.pdf
35. https://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CF%84%CE%B7%CF%82_%CE%B1%CF%80%CF%81%CE%BF%CF%83%CE%B4%CE%B9%CE%BF%CF%81%CE%B9%CF%83%CF%84%CE%AF%CE%B1%CF%82
36. https://science.fandom.com/el/wiki/%CE%91%CF%81%CF%87%CE%AE_%CE%91%CF%80%CF%81%CE%BF%CF%83%CE%B4%CE%B9%CE%BF%CF%81%CE%B9%CF%83%CF%84%CE%AF%CE%B1%CF%82
37. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1554/1/Κείμενο%20διπλωματικής.pdf
38. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs-16-18-quantum-technologies-report.pdf
39. http://dspace.lib.ntua.gr:8080/xmlui/bitstream/handle/123456789/6048/tsetsilam_quantum.pdf?sequence=3&isAllowed=y
40. https://www.australiandefence.com.au/defence/cyber-space/quantum-sensors-to-make-australia-safer

41. http://amitos.library.uop.gr/xmlui/bitstream/handle/123456789/952/358_000014m.pdf?sequence=1&isAllowed=y
42. https://eclass.aueb.gr/modules/document/file.php/INF208/Διαλέξεις/crypto13-01-introduction.pdf
43. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2017-11/SR112%20Quantum%20technologies.pdf?Xjl6YKv9JduL_0f_dw3C4wfAVCYl6ebv
44. http://www.physics4u.gr/news/2002/scnews517.html
45. http://83.212.168.57/jspui/bitstream/123456789/358/1/022013108.pdf
46. https://en.calameo.com/books/003094022c7b636f6d34c
47. https://el.wikipedia.org/wiki/%CE%9A%CE%B2%CE%AC%CE%BD%CF%84%CE%BF
48. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%B1%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7
49. http://docplayer.gr/55073850-Panepistimio-makedonias-diatmimatiko-programma-metaptyhiakon-spoydon-sta-pliroforiaka-systimata-aggoyras-vasileios-i-ilektroniki-ypografi.html
50. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/1554/1/%ce%9a%ce%b5%ce%af%ce%bc%ce%b5%ce%bd%ce%bf%20%ce%b4%ce%b9%cf%80%ce%bb%cf%89%ce%bc%ce%b1%cf%84%ce%b9%ce%ba%ce%ae%cf%82.pdf
51. https://hellanicus.lib.aegean.gr/bitstream/handle/11610/12627/file0.pdf
52. https://docplayer.gr/9181518-Vasika-themata-kryptografias.html