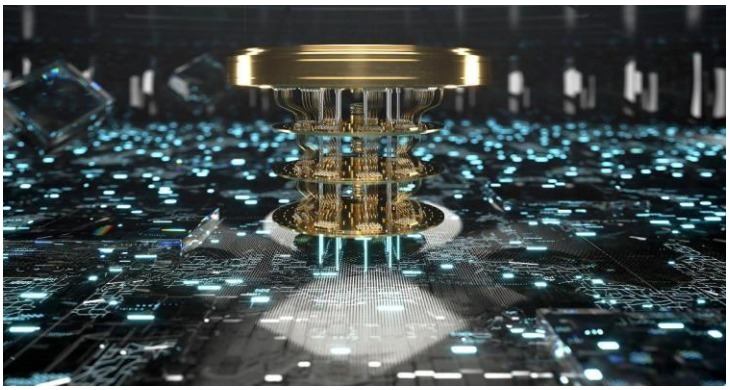
ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ ΜΗΧΑΝΙΚΗ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΔΙΑΔΙΚΤΥΑΚΕΣ ΚΑΙ ΦΟΡΗΤΕΣ ΕΦΑΡΜΟΓΕΣ

Κβαντική Υπολογιστική: Παρούσα κατάσταση και μελλοντικές τάσεις.



MSc Thesis

Μαντώς Παναγιώτης

Αριθμός Γενικού Μητρώου: M013121018

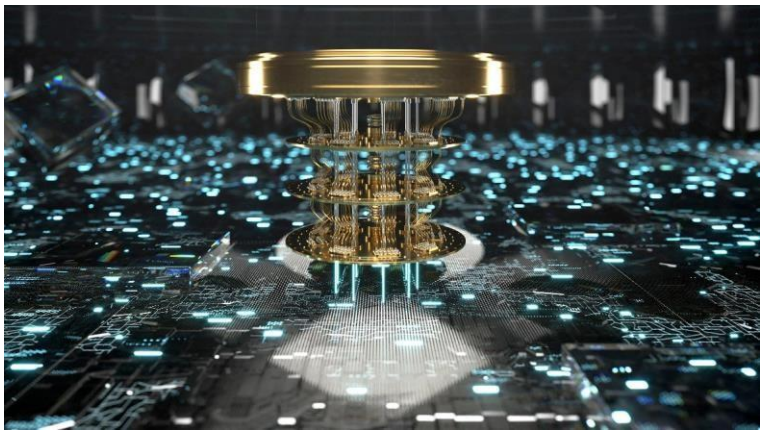
Επιβλέπων Καθηγητής: Σάββας Ηλίας

Λάρισα, Φεβρουάριος 2023.

University of Thessaly
School Of Technology
Digital Systems Department

MSc: Software Engineering for Web and Mobile Applications

Quantum Computation: Present state and future trends.



MSc Thesis

Mantos Panagiotis

RN: M013121018
Supervisor Professor: Savvas Ilias

Larissa, Greece, February 2023.

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

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

Ο Δηλών

(Υπογραφή)

Μαντώς Παναγιώτης

Ημερομηνία

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων **Ηλίας Σάββας**

Βαθμίδα/ιδιότητα επιβλέποντα,

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Μέλος **Ονοματεπώνυμο Μέλους 1**
Βαθμίδα/ιδιότητα μέλους 1, Τμήμα/Ιδρυμα μέλους 1

Μέλος **Ονοματεπώνυμο Μέλους 2**
Βαθμίδα/ιδιότητα μέλους 2, Τμήμα/Ιδρυμα μέλους 2

Ημερομηνία έγκρισης:

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους με βοήθησαν κατά την συγγραφή της μεταπτυχιακής διπλωματικής μου εργασίας, καθώς και τον επιβλέποντα καθηγητή μου κ. Ηλία Σάββα, για την συνεχής επιτήρηση και τις πολύτιμες συμβουλές του.

Μαντώς Παναγιώτης

Περίληψη

Η κβαντική πληροφορική αποτελεί μία επανάσταση όσον αφορά την ανάπτυξη της πληροφορικής. Έχει ως βάση του τις αρχές της κβαντικής μηχανικής και λόγω αυτών μπορεί και επιλύνει προβλήματα που δεν μπορούν να αντιμετωπίσουν οι κλασικοί υπολογιστές. Ξεκίνησε το 1980, όταν ο Richard Feynmann είχε θέσει την ιδέα να χρησιμοποιήσει κβαντικά συστήματα με σκοπό την εκτέλεση υπολογισμών. Αυτή η ιδέα αποτέλεσε το εναρκτήριο λάκτισμα για την ανάπτυξη των κβαντικών αλγορίθμων και του κβαντικού υλικού και συνεπώς στους κβαντικούς υπολογιστές.

Στη περίπτωση των κβαντικών υπολογιστών, η ειδοποιός διαφορά είναι ότι χρησιμοποιούνται qubits αντί για τα bits που υπάρχουν στους κλασικούς υπολογιστές. Τα qubits έχουν το χαρακτηριστικό ότι μπορούν να υπάρχουν σε πολλές καταστάσεις ταυτοχρόνως, δηλαδή και 0 και 1 την ίδια στιγμή, σε αντίθεση με τα bits, τα οποία μπορούν να υφίστανται στη κατάσταση 0 ή 1. Αυτό δίνει τη δυνατότητα στους κβαντικούς υπολογιστές να εκτελούν πολλούς υπολογισμούς την ίδια στιγμή, κάτι το οποίο τους καθιστά πολύ πιο γρήγορους από τους κλασικούς υπολογιστές.

Επιπροσθέτως, η κβαντική υπολογιστική καλύπτει ένα μεγάλο εύρος εφαρμογών, όπως η κρυπτογραφία, μηχανική μάθηση, βελτιστοποίηση προβλημάτων κ.α.

Μάλιστα, το πεδίο που προβλέπεται ότι θα επωφεληθεί περισσότερο είναι η κρυπτογραφία, διότι υπάρχουν πιθανότητες να σπάσει μέχρι και τους πιο ισχυρούς αλγορίθμους κρυπτογράφησης. Κάτι τέτοιο όμως, γεννά φόβους σχετικά με την ασφάλεια που πρέπει να προβλεφθούν και να επιλυθούν.

Μεγάλες εταιρείες από την πλευρά τους, έχουν επενδύσει αρκετά χρήματα στην ανάπτυξη των κβαντικών υπολογιστών και τεχνολογιών, με σκοπό τη δημιουργία αξιόπιστων και σταθερών κβαντικών υπολογιστών και μαζί με αυτούς, την εκτέλεση πιο σύνθετων υπολογισμών και προσομοιώσεων.

Μία από τις μεγαλύτερες, αν όχι η μεγαλύτερη πρόκληση που αντιμετωπίζει η κβαντική υπολογιστική, είναι το πως θα καταφέρει να κάνει τους κβαντικούς υπολογιστές να αναπτυχθούν σε μεγάλη κλίμακα, κάτι το οποίο απαιτεί πολύ δυνατό κβαντικό υλικό αλλά και λογισμικό, από το οποίο θα μπορούν να αντλήσουν όφελος οι άνθρωποι από τις τεράστιες και μη προηγούμενες ιδιότητες των κβαντικών υπολογιστών, λύνοντας έτσι σημαντικά και πολύπλοκα προβλήματα, πέρα από τα όρια που υπάρχουν αυτή τη στιγμή.

Abstract

Quantum computing is a revolution in the development of information technology. It is based on the principles of quantum mechanics and because of these it can solve problems that classical computers cannot deal with; it began in 1980, when Richard Feynmann had put the idea to use quantum systems to perform calculations. This idea was the starting point for the development of quantum algorithms and quantum material and thus quantum computers.

In the case of quantum computers, the notified difference is that qubits are used instead of the bits present in classical computers. qubits have the characteristic that they can exist in many states simultaneously, i.e. 0 and 1 at the same time, as opposed to bits, which can exist in state 0 or 1. This enables quantum computers to perform many calculations at the same time, which makes them much faster than classical computers.

In addition, quantum computing covers a wide range of applications, such as cryptography, machine learning, problem optimization, and so on.

In fact, the field that is predicted to benefit most is cryptography, because there are chances to break up even the most powerful encryption algorithms. This, however, raises fears about the safety which must be foreseen and resolved.

Large companies, for their part, have invested a lot of money in the development of quantum computers and technologies, in order to create reliable and stable quantum computers and, with them, perform more complex calculations and simulations.

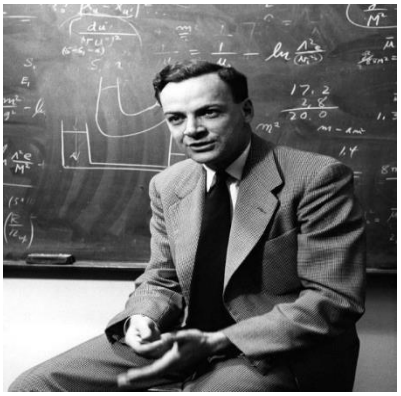
One of the biggest, if not the biggest, challenges facing quantum computing is how to make quantum computers grow on a large scale, which requires very powerful quantum hardware as well as software, from which people can benefit from the submissive and non-prior properties of quantum computers, thus solving important and complex problems beyond the limits that exist at the moment.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

1.1 Ιστορική Αναδρομή

Τα τελευταία χρόνια, η Κβαντική Πληροφορική αποτελεί χωρίς καμία αμφιβολία, μία τεχνολογία η οποία έχει τις μεγαλύτερες απαιτήσεις όσον αφορά την αλλαγή παραδείγματος από τη πλευρά των προγραμματιστών. Τη δεκαετία του 1980, προτάθηκαν για πρώτη φορά οι Κβαντικοί Υπολογιστές από τους **Richard Feynmann** και **Yuri Manin**.



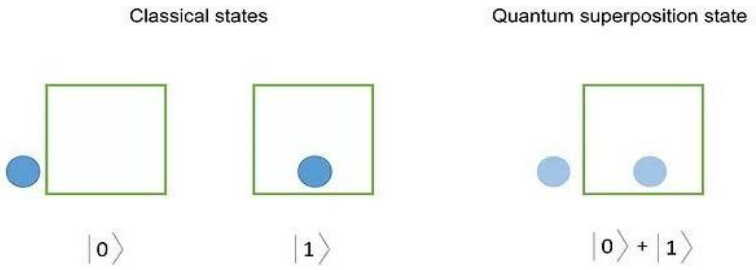
Εικόνα 1. : Richard Feynmann (Πηγή: https://www.caltech.edu/about/news/remembering-richard-feynman-81875)

Η κβαντική μηχανική γνώρισε μεγάλη ανάπτυξη μεταξύ του 1900 και 1925 και μέχρι και σήμερα αποτελεί τον σημαντικότερο παράγοντα στον οποίο στηρίζεται η χημεία, η φυσική συμπυκνωμένης ύλης και τεχνολογίες που έχουν να κάνουν με τα chip υπολογιστών και με τον φωτισμό LED. Παρόλα αυτά, στη περίπτωση της κβαντικής μηχανικής, ακόμα και τα πιο απλά συστήματα, παρουσίαζαν δυσκολία στο να μοντελοποιηθούν με αυτή. Αυτό έχει να κάνει με το γεγονός ότι για να γίνει προσομοίωση συστημάτων απαιτεί πολύ μεγάλη υπολογιστική ισχύ, περισσότερη από όση παρέχει ένας συμβατικός υπολογιστής για χιλιάδες χρόνια.

Ο **Richard Feynmann** είχε σημειώσει ότι όταν τα ηλεκτρονικά συστατικά δημιουργούν μικροσκοπικές κλίμακες, τότε συμβαίνουν φαινόμενα τα οποία υπάρχουν στη κβαντική μηχανική και έτσι είχε την ιδέα να προτείνει να χρησιμοποιηθούν για τον σχεδιασμό πιο ισχυρών υπολογιστών. Επίσης, είχε ξεκινήσει να κάνει υποθέσεις ότι οι υπολογιστές θα μπορούσαν να υπολογίσουν κβαντικά συστήματα με πάνω από 2 καταστάσεις, όπως έκαναν οι κλασικοί υπολογιστές (Εικασία Feynmann). Την εικασία αυτή του Feynmann υποστήριξε ο φυσικός **Paul Beni-off**, όπου βρισκόταν στο ίδιο συνέδριο μαζί του(MIT).

Στόχος των κβαντικών ερευνητών είναι να «τιθασεύσουν» το φαινόμενο «υπέρθεση» (superposition). Ένα κβαντικό σύστημα «υπάρχει» σε όλες τις πιθανές καταστάσεις, πρώτού μία μέτρηση «καταρρεύσει» στο σύστημα σε μία μόνο κατάσταση.

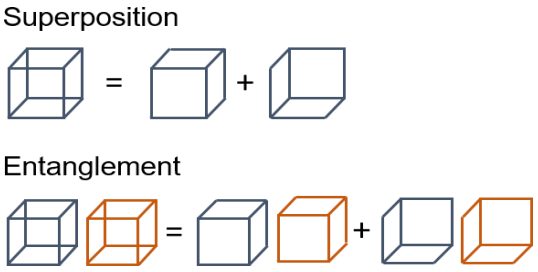
Με βάση αυτό το φαινόμενο η υπολογιστική ισχύ σε ένα υπολογιστή μπορεί να επεκταθεί σε μεγάλο βαθμό. Συμπέρανε ότι οι κβαντικοί υπολογιστές θα είχαν την δυνατότητα να προσομοιώσουν κβαντικά συστήματα με αποτελεσματικότητα. Έως τη σημερινή εποχή, δεν έχουν ανακαλυφθεί αποτελεσματικοί παραδοσιακοί αλγόριθμοι, στη περιοχή της κβαντικής προσομοίωσης η οποία παρουσιάζει προβλήματα.



Εικόνα 2. : Quantum States (Πηγή: https://physics.stackexchange.com/questions/582737/has-it-been-practically-proven-that-quantum-superposition-exists-if-yes-how-d)

Με βάση κάποιες έννοιες που έχουν να κάνουν με τη χημεία, οι επιστήμονες της κβαντικής φυσικής κατασκεύασαν τα θεμέλια που αργότερα θα οδηγούσαν στη κβαντική υπολογιστική. Ένα αξιοσημείωτο παράδειγμα είναι το πείραμα του **Faraday** το οποίο μας έδειξε ότι υπάρχουν φορτισμένα υποατομικά σωματίδια.

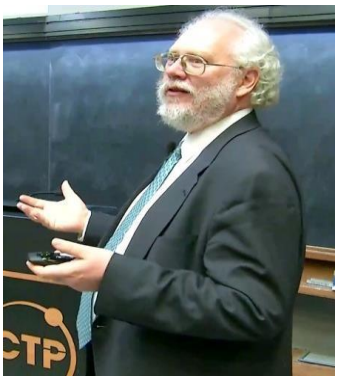
Πολλές ιδιότητες οι οποίες ανακαλύφθηκαν, όπως η διεμπλοκή (entanglement), υπέρθεση(superposition) και άλλες, είναι αυτές οι οποίες έγινε οι βασικές αρχές για τη κβαντική υπολογιστική και ταυτόχρονα θεμελιώδεις αρχές της κβαντικής φυσικής.



Εικόνα 3. : Superposition-Entanglement (Πηγή: https://qt.eu/discover-quantum/introduction-to-quantum-physics/)

Μεταξύ της δεκαετίας του 1980 και του 1990, αναπτύχθηκε σημαντικά η θεωρία των κβαντικών υπολογιστών. Μετά από τον Feynmann, το 1985 ο **David Deutsch** έκανε μία περιγραφή περί της κατασκευής των πυλών της κβαντικής λογικής για ένα κβαντικό υπολογιστή. Επίσης, πρότεινε την μηχανή Κβαντικού Turing(QTM), η οποία ήταν μία θεωρητική μηχανή και αυτό που έκανε ήταν να μοντελοποιεί τα μαθηματικά πίσω από τον κβαντικό υπολογισμό με τη χρήση κβαντικών πυλών, οι οποίες αποτελούν ένα σύνολο λειτουργιών όπου επιτρέπουν την ύπαρξη πολλαπλών καταστάσεων σε ένα υπολογιστή.

Έπειτα το 1994 ο **Peter Shor** δημιούργησε έναν αλγόριθμο ώστε να μπορεί να παραγοντοποιεί αριθμούς σε έναν κβαντικό υπολογιστή ο οποίος θα απαιτούσε μόνο 6 qubits, παρότι πολλά περισσότερα qubits χρειάζονται για τη παραγοντοποίηση μεγάλων αριθμών σε ένα διάστημα.



Εικόνα 4. : Peter Shor speaking after receiving the 2017 Dirac Medal (Πηγή: https://en.wikipedia.org/wiki/Peter_Shor)

Το 1981 το MIT έθεσε το δίλλημα, ότι οι κλασικοί υπολογιστές που υπήρχαν δεν μπορούσαν να προσομοιώσουν την εξέλιξη των κβαντικών συστημάτων με τρόπο ο οποίος να έχει αποτέλεσμα. Προτάθηκε λοιπόν, ένα βασικό μοντέλο για έναν κβαντικό υπολογιστή ο οποίος θα είχε την ικανότητα να κάνει τέτοιες προσομοιώσεις. Έτσι, περιεγράφηκε η πιθανότητα να ξεπεραστούν εκθετικά οι κλασικοί υπολογιστές. Παρόλα αυτά, χρειάστηκαν πάνω από 10 χρόνια ώστε να δημιουργηθεί ένας ειδικός αλγόριθμος ο οποίος θα άλλαζε τη άποψη σχετικά με τη κβαντική υπολογιστική, ο αλγόριθμος Shor.

Το 1994, ο λεγόμενος αλγόριθμος από τον Peter Shor, ο οποίος αυτό που έκανε ήταν να επιτρέπει στους κβαντικούς υπολογιστές να παραγοντοποιήσουν με αποτελεσματικότητα τους μεγάλους ακέραιους που είναι εκθετικά ταχύτεροι από τον κλασικό αλγόριθμο στις παραδοσιακές μηχανές. Από θεωρητική πλευρά, ο αλγόριθμος Shor έχει τη δυνατότητα να σπάσει πολλά από τα κρυπτοσυστήματα που υπάρχουν σήμερα. Ενσωμάτωσε τόσο την εμπλοκή (entanglement) όσο και την υπέρθεση (superoposition) ώστε να μπορεί να καθορίσει τους πρώτους παράγοντες ενός ακεραίου, κάτι το οποίο απασχολεί σε μεγάλο βαθμό τους κρυπτογράφους και τους επιστήμονες υπολογιστών. Αποτέλεσε φλέγον ζήτημα η πιθανότητα να μπορούν να διασπαστούν κρυπτοσυστήματα σε ώρες αντί για εκατομμύρια χρόνια με τη χρυσή κβαντικών υπολογιστών.

Το 1996, ένας αλγόριθμος αναζήτησης κβαντικής βάσης δεδομένων εφευρέθηκε από τον Lov Grover (Bell Labs), ο οποίος παρουσίασε μία τετραγωνική επιτάχυνση για ένα εύρος προβλημάτων. Οποιοδήποτε πρόβλημα έπρεπε να λυθεί με τυχαία η brute-force αναζήτηση, τώρα θα γινόταν 4x πιο γρήγορα. Ο συγκεκριμένος αλγόριθμος είχε στόχο την αναζήτηση σε database και επιπλέον μπορούσε να εφαρμοστεί σε ευρύτερη κλίμακα.

Το 1998, κατασκευάστηκε ένας κβαντικός υπολογιστής 2 qubit, ο οποίος ήταν λειτουργικός και έλυσε τους πρώτους κβαντικούς αλγορίθμους όπως ο αλγόριθμος του Grover. Κάπου εκεί ξεκίνησε να έρχεται μία νέα εποχή για την ισχύ των υπολογιστών και ήταν ένα διάστημα όπου όλο και περισσότερες εφαρμογές αναπτύσσονταν.

Έπειτα, το 1998, ο **Isaac Chuang** (Los Alamos National Laboratory, ο **Neil Gershenfeld** (MIT), και ο **Mark Kubinec** του πανεπιστημίου της Καλιφόρνια στο Berkeley, δημιούργησαν **τον πρώτο κβαντικό υπολογιστή** με 2 qubit ο οποίος θα μπορούσε να έχει τη δυνατότητα να πάρει κάποια δεδομένα και να βρει μία λύση. Παρότι το σύστημα που είχαν δημιουργήσει είχε συνοχή για λίγα nanoseconds, κατέδειξε τις αρχές του κβαντικού υπολογισμού και ήταν κάτι πολύ σημαντικό.

Εικόνα 5. : Isaac Chuang- Test-tube solution (Πηγή: https://physicsworld.com/a/quantum-computing-with-solids/)

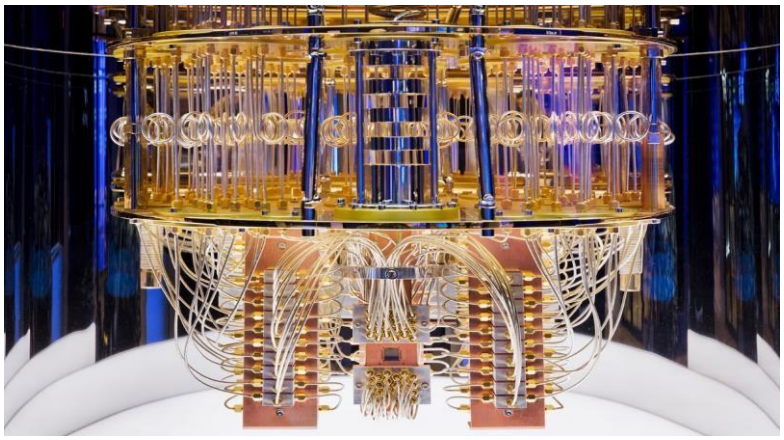
Το Μάρτιο του 2000, οι **Emanuel Knill**, **Raymond Laflamme**, και ο **Rudy Martinez** από το Los Alamos και MIT, δημιούργησαν ένα κβαντικό υπολογιστή 7 qubit, που υλοποιήθηκε βασισμένος σε μία νέα εναλλακτική μέθοδο όπου υπήρχε εμπλοκή ατόμων βηρυλλίου παρότι υπήρχαν πολλές δυσκολίες στην εφαρμογή της, αλλά εν τέλει αυτό απέδειξε ότι οι κβαντικοί υπολογιστές όντως υπάρχουν.

Αξίζει να σημειωθεί όμως ότι ένα μεγάλο μέρος ερευνητών είναι επιφυλακτικοί όσον αφορά τη επέκταση των μαγνητικών τεχνικών πέρα από τα 10 με 15 qubits λόγω της μειωμένης συνοχής

μεταξύ των πυρήνων (decoherence) , μειώνουν την αξιοπιστία και την αποτελεσματικότητά τους ταυτόχρονα.

Μία εβδομάδα πριν ανακοινωθεί ο κβαντικός υπολογιστής με 7 qubit, ο **David Wineland** και οι συνεργάτες του (NIST), είχαν ανακοινώσει την δημιουργία ενός κβαντικού υπολογιστή 4 qubit χρησιμοποιώντας μία ηλεκτρομαγνητική «παγίδα». Αυτό έγινε με ένα λέιζερ το οποίο μετά τον περιορισμό των ιόντων σε γραμμική διάταξη, ψύχρανε τα σωματίδια σχεδόν σε θερμοκρασίες απόλυτου μηδενός και συγχρονίζοντας τις καταστάσεις περιστροφής τους. Έπειτα, χρησιμοποιήθηκε ακόμα ένα λέιζερ ώστε να εμπλέξει τα σωματίδια, φτιάχνοντας έτσι μία υπέρθεση (superposition) καταστάσεων spin-up και spin-down ταυτοχρόνως και για τα 4 ιόντα. Αυτό, είχε ως αποτέλεσμα ξανά να αποδειχθούν οι βασικές αρχές της κβαντικής πληροφορικής.

Το 2017, η IBM παρουσίασε τον πρώτο κβαντικό υπολογιστή, ο οποίος ήταν εμπορικά χρησιμοποιήσιμος, και πλέον όλος αυτός ο αγώνας έχει φτάσει σε άλλο επίπεδο.



Εικόνα 6. : IBM Quantum Computer (Πηγή: https://www.engadget.com/ibm-quantum-computing-speedup-050134678.html)

Χρονολογικό Διάγραμμα Κβαντικής Εξέλιξης

- ***1998***

  Έλαβε μέρος η πρώτη επίδειξη της διόρθωσης κβαντικού σφάλματος. Αποδείχθηκε για πρώτη φορά, ότι μπορεί να γίνει προσομοίωση αποτελεσματικά με τους κλασικούς υπολογιστές, μία συγκεκριμένη υποκλάσικη κβαντικών υπολογισμών.

- ***1999***

  ο Yasunobu Nakamura από το Πανεπιστήμιο του Tokyo και ο Jaw-Shen Tsai του Πανεπιστημίου Επιστημών του Tokyo , καταφέρνουν να αποδείξουν ότι ένας υπεραγώγιμο κύκλωμα μπορεί να χρησιμοποιηθεί ως qubit.

- ***2002***

  Γίνεται η δημοσίευση της πρώτης έκδοσης του Quantum Computation Roadmap, ένα ζωντανό έγγραφο που αποτελείται από βασικούς ερευνητές της κβαντικής υπολογιστικής.

- ***2004***

  Αποδείχθηκε η πρώτη εμπλοκή (entanglement) 5 φωτονίων από την ομάδα του Jian-WeiPan στη Κίνα, στο πανεπιστήμιο επιστήμης και τεχνολογίας.

- ***2011***

  Ο πρώτος εμπορικά διαθέσιμος κβαντικός υπολογιστής προσφέρεται από την D-Wave Systems. Σήμερα, η συγκεκριμένη εταιρεία αποτελεί μία από τις ελάχιστες που διαθέτουν το hardware. Από την άλλη πλευρά, η IBM και η Rigetti, πωλούν υπολογιστικό χρόνο, αποκλειστικά στους υπολογιστές τους, quantum gate.

Εικόνα 7. : D-wave quantum computer (Πηγή: https://www.wired.co.uk/article/d-wave-2000q-quantum-computer)

- ***2012***

  Ιδρύθηκε η πρώτη εταιρεία η οποία ήταν αφιερωμένη στο λογισμικό κβαντικής πληροφορικής, η 1QBit.

- ***2014***

  Στο Πανεπιστήμιο Τεχνολογίας Delft, φυσικοί στο Ινστιτούτο Νανοεπιστήμης, τηλεμετέφεραν πληροφορίες μεταξύ 2 κβαντικών bits, τα οποία χωρίζονταν από σχεδόν 3,5 μέτρα με μηδενικό ποσοστό σφάλματος.

- ***2017***

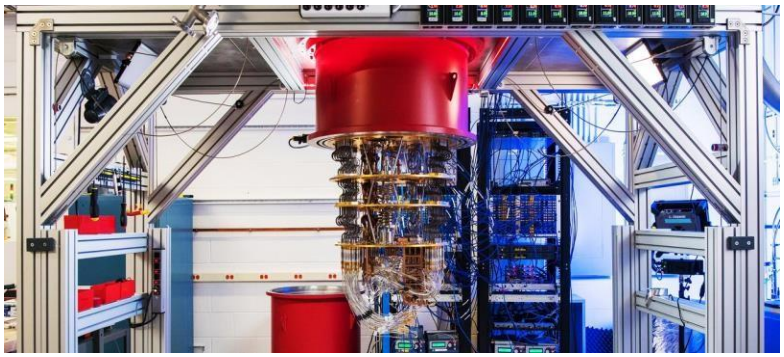
  Η πρώτη κβαντική τηλεμεταφορά ανεξάρτητων μονοφωτονίων qubits αναφέρεται από Κινέζους ερευνητές, μέσα από ένα παρατηρητήριο στη γη, σε ένα δορυφόρο χαμηλής τροχιάς με απόσταση έως 1400km.

- ***2018***

  Ο Donald Trump υπέγραψε την Εθνική Κβαντική Πρωτοβουλία(National Quantum Initiative Act) , καθορίζοντας έτσι τους στόχους και τις προτεραιότητες για ένα σχέδιο το οποίο ήταν 10-ετές και είχε σκοπό την επιτάχυνση της ανάπτυξης της κβαντικής επιστήμης των πληροφοριών και των εφαρμογών της τεχνολογίας στις ΗΠΑ.

- ***2019***

  Η Google υποστηρίζει ότι κατέχει τη κβαντική υπεροχή, διότι εκτέλεσε μία σειρά από λειτουργίες σε 200 δευτερόλεπτα, κάτι το οποίο ένας υπερυπολογιστής θα χρειαζόταν περίπου 10.000 χρόνια για να τις ολοκληρώσει. Δεν άργησε να έρθει η απάντηση της IBM,καθώς πρότεινε ότι θα γινόταν να διαρκέσει 2,5 μέρες αντί για 10.000 χρόνια, τονίζοντας τις τεχνικές που μπορεί να χρησιμοποιήσει ένας υπερυπολογιστής, για να μεγιστοποιήσειτη υπολογιστική ταχύτητα.



Εικόνα 8. : Google Quantum Computer (Πηγή: https://blog.google/perspectives/sundar-pichai/what-our-quantum-computing-milestone-means/)

Ο σκοπός όλης αυτής της διαδρομής και της εξέλιξης της κβαντικής υπεροχή, είναι να επιδείξει μία πρακτική κβαντική συσκευή η οποία μπορεί να λύσει ένα πρόβλημα όπου ένας κλασικός υπολογιστής δεν θα μπορεί να το κάνει σε οποιοδήποτε εφικτό χρονικό διάστημα, το επόμενο βήμα της πληροφορικής είναι πάντα η ταχύτητα και η βιωσιμότητα.

2. Qiskit,Pyquill

2.1 Qiskit

Το **qiskit** αποτελεί ένα software development kit το οποίο χρησιμοποιείται για εργασία με κβαντικούς υπολογιστές όσο έχει να κάνει με αλγόριθμους, κυκλώματα και παλμούς. Παρέχει μια γκάμα εργαλείων για να μπορούμε να δημιουργήσουμε και να χειριστούμε κβαντικά προγράμματα είτε μέσω προσομοίωσης σε τοπικό υπολογιστή, είτε σε πρωτότυπες κβαντικές συσκευές μέσω του IBM Quantum Experience.

Το μοντέλο που ακολουθείται είναι το μοντέλο κυκλώματος για καθολικούς κβαντικούς υπολογισμούς και έχει την ιδιότητα ότι μπορεί να χρησιμοποιηθεί για οποιοδήποτε κβαντικό υλικό.

Η IBM δημιούργησε το Qiskit και στόχος της ήταν να επιτρέψει την ανάπτυξη λογισμικού για το cloud computing service της.

Η Python έχει τον πρώτο λόγο στη κύρια έκδοση του Qiskit, ενώ στα πρώτα στάδια των εκδόσεων του διερευνήθηκαν εκδόσεις που χρησιμοποιούσαν Swift και Javascript, αλλά πλέον έχει σταματήσει η ανάπτυξη τους.

Επίσης για την εφαρμογή των απαραίτητων χαρακτηριστικών μόνο , υπάρχει η εφαρμογή MicroQiskit , η οποία έχει ως χαρακτηριστικό τη εύκολη μεταφορά σε διαφορετικές και εναλλακτικές πλατφόρμες.

Ουσιαστικά, το Qiskit, έχει ως σκοπό την εκμάθηση των βασικών χαρακτηριστικών του κβαντικού προγραμματισμού προς τους ανθρώπους.

Το Qiskit απαρτίζεται από στοιχεία τα οποία μέσω της συνεργασίας τους ενεργοποιούν την κβαντική υπολογιστική. Ο κύριος στόχος του είναι η δημιουργία μίας στοίβας λογισμικού η οποία θα κάνει εύκολη τη χρήση κβαντικών υπολογιστών σε όλους, χωρίς να έχει να κάνει το κατά πόσο σχετικοί είναι με το συγκεκριμένο αντικείμενο. Επιπλέον, επιτρέπει τη σχεδίαση εύκολων πειραμάτων και διαφόρων εφαρμογών στους χρήστες, ακόμη και να μπορούν να τα τρέξουν σε πραγματικούς κβαντικούς υπολογιστές είτε σε κλασικούς προσομοιωτές. Έπειτα, μέσω του OpenQASM, δύναται η ανάπτυξη κβαντικού λογισμικού, για ανέμπειρους χρήστες στο τομέα της κβαντικής υπολογιστικής.

Qiskit Terra

Το υπόλοιπο qiskit είναι βασισμένο πάνω στο στοιχείο Terra. Το Qiskit Terra παρέχει μία γκάμα εργαλείων, τα οποία χρησιμοποιούνται για την υλοποίηση κβαντικών κυκλωμάτων σε κβαντικό κώδικα μηχανής ή παρόμοιο με αυτόν.

Επιπλέον, παρέχονται εργαλεία τα οποία βελτιστοποιούν τα κβαντικά κυκλώματα για μία συσκευή συγκεκριμένη, και για τη διαχείριση εργασιών όσον αφορά την εκτέλεσή τους σε προσομοιωτές αλλά και σε κβαντικές συσκευές οι οποίες έχουν απομακρυσμένη πρόσβαση.

Παρακάτω, ένα παράδειγμα Qiskit Terra.

Αναπαρίσταται ένα κβαντικό κύκλωμα για 2 qubits, το οποίο αποτελείται από κβαντικές πύλες που είναι απαραίτητες για μια κατάσταση Bell(Bell state). Το κύκλωμα τελειώνει με κβαντικές μετρήσεις, από τις οποίες εξάγεται ένα bit από κάθε qubit.

```
from qiskit import QuantumCircuit

qc = QuantumCircuit(2, 2)

qc.h(0)
qc.cx(0, 1)
qc.measure([0,1], [0,1])
```

Εικόνα 9. : Qiskit Terra (Πηγή: https://en.wikipedia.org/wiki/Qiskit)

Qiskit Aer

Αυτό που κάνει το στοιχείο Aer είναι ότι διαθέτει προσομοιωτές κβαντικής υπολογιστής με πολύ μεγάλη απόδοση, με μοντέλα θορύβου που είναι αρκετά ρεαλιστικά. Επίσης, παρέχει προσομοιωτές οι οποίοι "στεγάζονται" τοπικά στη συσκευή αυτού που τα χρησιμοποιεί, αλλά και μέσω cloud, υπάρχει διαθεσιμότητα σε πόρους HPC. Ένα χαρακτηριστικό των προσομοιωτών είναι ότι μπορούν να προσομοιώσουν τις επιπτώσεις του θορύβου για πιο απλά αλλά και για πιο σύνθετα και εξελιγμένα μοντέλα θορύβου.

Αφότου γίνει η δημιουργία ενός κβαντικού κυκλώματος, έπειτα μπορεί να εκτελεστεί σε backend(κβαντικό υλικό ή προσομοίωση). Παρακάτω χρησιμοποιείται ένας τοπικός προσομοιωτής.

```
from qiskit import Aer, execute

backend = Aer.get_backend("qasm_simulator")
job = execute(qc, backend)
result = job.result()
print(result.get_counts(qc))
```

Εικόνα 10. : Qiskit Aer (Πηγή: https://en.wikipedia.org/wiki/Qiskit)

Qiskit Ignis

Από τις 6 Δεκεμβρίου 2021, τη θέση του Qiskit Ignis έχει πάρει το Qiskit Experimental.

Τα εργαλεία που παρέχονται, βοηθάνε σο χαρακτηρισμό του θορύβου, στη διόρθωση σφαλμάτων αλλά και στη επαλήθευση του κβαντικού υλικού. Επίσης, τα εργαλεία αυτά χρησιμοποιούνται για το χαρακτηρισμό του θορύβου σε συσκευές με μικρή διάρκεια. Επίσης περιλαμβάνεται η συγκριτική αξιολόγηση συσκευών οι οποίες είναι μακροπρόθεσμες, στις οποίες εφαρμόζεται μείωση και διόρθωση σφάλματος.

Ουσιαστικά, το Ignis είναι σχεδιασμένο για τους ανθρώπους που σκοπό έχουν τη σχεδίαση κώδικα διόρθωσης κβαντικού σφάλματος, ή που ενδιαφέρονται στη μελέτη τρόπων χαρακτηρισμών σφαλμάτων μέσω τομογραφίας ή για χρήση πυλών με βέλτιστο έλεγχο.

Qiskit Aqua

Από τις 2 Απριλίου 2021, έχει γίνει υποβάθμιση του Qiskit Aqua.

Το στοιχείο Aqua διέθετε μία βιβλιοθήκη με cross-domain algorithms, όπου μπορεί να γίνει η δημιουργία εφαρμογών όσον αφορά συγκεκριμένους τομείς. Πλέον το Qiskit Aqua διαχωρίζεται σε ενότητες εφαρμογής που έχουν να κάνουν με τη χρηματοδότηση, τη βελτιστοποίηση τη φύση(Φυσική, Χημεία) και τη μηχανική μάθηση(ML). Κάποιοι αλγόριθμοι και άλλες λειτουργίες μεταφέρθηκαν στο Qiskit Terra πλέον.

Έπειτα, πλέον οι αλγόριθμοι λειτουργούν με βάση ένα ενοποιημένο πρότυπο: Ταξινομούνται ανάλογα με το τι προβλήματα έχουν να λύσουν, ενώ μέσα σε ένα application class, έχουν την δυνατότητα να εναλλάσσονται για να επιλύσουν κοινά προβλήματα.

Qiskit Optimization

Αποτελεί ένα open-source framework το οποίο περιλαμβάνει όλο το έυρος υψηλού επιπέδου μοντελοποίησης προβλημάτων βελτιστοποίησης, χρησιμοποιώντας αυτόματη μετατροπή προβλημάτων, σε μία σουίτα από εύχρηστους αλγόριθμους κβαντικής βελτιστοποίησης και μάλιστα καθίσταται δυνατό να μπορούν να τρέξουν σε κλασικούς προσομοιωτές αλλά και σε κβαντικές συσκευές που υπάρχουν μέσα από το Qiskit. Με τη χρήση του docplex, υλοποιείται εύκολη και αποτελεσματική μοντελοποίηση των προβλημάτων βελτιστοποίησης μέσω της μονάδας βελτιστοποίησης.

Qiskit Finance

Αποτελεί και αυτό ένα open-source framework , το οποίο έχει να κάνει με προβλήματα stocks και securities και με στοιχεία αβεβαιότητας. Επίσης, παρέχει άντληση πραγματικών ακόμη και τυχαίων δεδομένων όσον αφορά τη χρηματοδότηση πειραμάτων.

Qiskit Machine Learning

Παρέχει σχετικά απλά δείγματα από σύνολα δεδομένων, μέχρι στιγμής. Περιέχει αλγορίθμους ταξινόμησης(classification), όπως VQC,QSVM. Υπάρχει δυνατότητα τα data να χρησιμοποιηθούν για πειράματα. Ένας πολύ ενδιαφέρον αλγόριθμος που υπάρχει επίσης είναι ο QGAN(Quantum Generative Adversarial Network).

Qiskit Nature

Ακόμη ένα open-source framework από τη Qiskit, όπου αυτό που κάνει είναι να αντιμετωπίζει προβλήματα που έχουν να κάνουν με υπολογισμούς ενέργειας κατάστασης εδάφους, διεγερμένες καταστάσεις και άλλα. Όσον αφορά τον κώδικα, υπάρχουν drivers χημείας, οι οποίοι όταν παρέχονται σε μοριακή διαμόρφωση, τότε επιστρέφουν ολοκληρώματα 1 και 2 σωμάτων, αλλά και δεδομένα που έχουν υπολογιστεί κλασικά. Έπειτα, αυτά τα data, δύναται να χρησιμοποιηθούν σαν είσοδο στο Qiskit Nature και μεταφράζονται μέσω αυτού σε μορφή κατάλληλη για να χρησιμοποιηθούν από κβαντικούς αλγορίθμους.

2.2 Pyquill

Η κβαντική υπολογιστική πρόκειται για μία έννοια η οποία προσφάτως έχει εισαχθεί στις ζωές μας και βασίζεται στη κβαντική φυσική.

Η Rigetti Computing πρόκειται για έναν πάροχο κβαντικών συστημάτων υπολογιστών και δραστηριοποιείται σε κβαντικά κυκλώματα υλικού αλλά και σε στρώματα λογισμικού. Αυτό που κάνει είναι ότι δίνει τη δυνατότητα στο ευρύ κοινό, χωρίς να έχει άμεση πρόσβαση σε κβαντικούς υπολογιστές, να χρησιμοποιεί **κβαντική μηχανική μάθηση**.

Εικόνα 11. : Forest Software Development Kit (Πηγή: https://ml2quantum.com/pyquil/)

Το Forest Software Development Kit έχει αναπτυχθεί από τη Rigetti και περιέχει τα παρακάτω:

PyQuil: Αποτελεί μία βιβλιοθήκη Python, η οποία είναι ανοιχτού κώδικα(open source) και σκοπός της είναι να βοηθάει τους χρήστες να μπορούν να γράφουν και συνάμα να εκτελούν κβαντικά προγράμματα. Αξιοσημείωτο είναι ότι το source βρίσκεται στο github.

Quil: Το Quil(Quantum Instruction Language) περιέχει κάποιες οδηγίες, οι οποίες δύναται να εκτελεστούν σε οποιαδήποτε εφαρμογή μίας αφηρημένης κβαντικής μηχανής, πχ QVM ή QPU.

QVM: Αποτελεί τη Κβαντική Εικονική Μηχανή και επιτρέπει στους χρήστες να προσομοιώσουν ένα μικρό κβαντικό υπολογιστή, μέσω ενός κανονικού υπολογιστή και να εκτελούν προγράμματα Quil.

QPU: Αποτελεί τη Μονάδα Κβαντικής Επεξεργασίας και είναι το chip με το οποίο τρέχουν τα κβαντικά προγράμματα.

Quil Compiler: Το Quil το οποίο είναι γραμμένο για ένα QAM(κβαντικό αφηρημένο μηχάνημα), μεταγλωττίζεται από τον quilc(μεταγλωττιστή), σε ένα άλλο. Αυτό γίνεται αυτόματα, καθώς ο μεταγλωττιστής που έχουμε παίρνει Quil και το μεταγλωττίζει για το δεδομένο QAM που υπάρχει.

Ο συνδυασμός των Pyquil,quilc,QVM και άλλων βιβλιοθηκών, απαρτίζουν το SDK Forest.

Forest SDK: Αποτελεί ένα software development kit, όπου έχει βελτιστοποιηθεί για τη σχέση μεταξύ συνεπεξεργαστών κβαντικών υπολογιστών και παραδοσιακών επεξεργαστών, ώστε να γίνει η εκτέλεση υβριδικών αλγορίθμων.

Με τη χρήση του Forest SDK, μπορεί να πραγματοποιηθεί προσομοίωση της λειτουργίας ενός πραγματικού κβαντικού επεξεργαστή(QPU).

Το PyQuil έχει **3** κύριες λειτουργίες:

Παράγει προγράμματα Quil σχετικά εύκολα, μέσω κβαντικών πυλών και κλασικών λειτουργιών.

Μεταγλωττίζει και προσομοιώνει προγράμματα Quil, χρησιμοποιώντας τον quilc και το QVM.

Εκτελεί προγράμματα Quil σε QPUs χρησιμοποιόντας Quantum Cloud Services(QCS).

QCS(Quantum Cloud Services): Παρέχει σε αυτούς που τις χρησιμοποιούν, ένα μοναδικό σημείο πρόσβασης(on-premise), από όπου μπορούν να έχουν πρόσβαση σε κβαντικούς υπολογιστές.

Μία πλήρως διαμορφωμένη εικονική μηχανή η οποία λέγεται εικόνα κβαντικού μηχανήματος(QMI), αποτελεί αυτό το σημείο πρόσβασης.

Για να προγραμματιστεί ο χρόνος υπολογιστικής λειτουργίας ενός QMI στους κβαντικούς υπολογιστές, υπάρχει ομαδοποίηση του QMI με το ίδιο SDK και με μια CLI(διασύνδεση γραμμής εντολών).

Definitions

QCS: Quantum Cloud Services

QMI: Quantum Machine Image

QAM: Quantum Abstract Machine

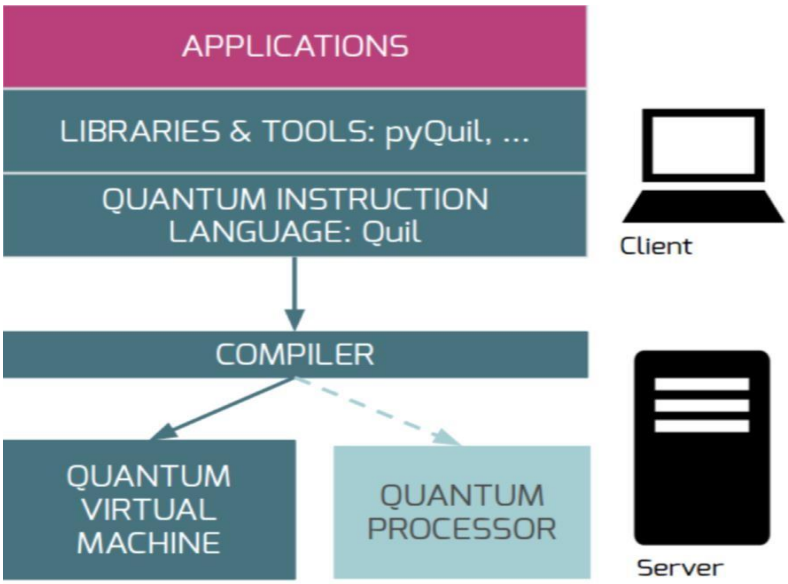
QVM: Quantum Virtual Machine

QPU: Quantum Processing Unit

QCS⇒Code⇒QMI⇒QAM⇒Quil(PyQuil)⇒QVM or QPU.

QCS--> Στέλνεται ο κώδικας στο QMI, χρησιμοποιείται η QAM ώστε να τρέξει ο κώδικας με βάση τις οδηγίες του Quil, χρησιμοποιείται το PyQuil στη QVM ή στη QPU.

Μέσω QCS στέλνουμε τον κώδικα στο QMI, χρησιμοποιούμε τη διεπαφή QAM για να τρέξουμε τον κώδικα με οδηγίες Quil, χρησιμοποιώντας τη βιβλιοθήκη PyQuil είτε στη QVM είτε στη QPU.



Εικόνα 12. : Artistic view on quantum. Photo by Michael Dziedzic on Unsplash (Πηγή: https://medium.com/swlh/exploring-quantum-computing-with-rigetti-pyquil-mid-2020-edition-70b28f917670)

<<We shouldn't wait quantum computers to become mainstream before developing quantum programming languages, algorithms and community around quantum computing. Modern programming languages were not developed over night and I guess the quantum case will be no different.>>

Aki Kutvonen

Η Rigetti Computing, δίνει τη δυνατότητα στους χρήστες μέσω της cloud computing πλατφόρμας της, να γράψουν κβαντικές υπολογιστικές οδηγίες στη Python σε ένα προσομοιωμένο κβαντικό υπολογιστή, ο οποίος χρησιμοποιεί πολλούς κλασικούς υπολογιστές.

Στο πρακτικό κομμάτι, εφόσον ανάμεσα σε ένα κβαντικό και σε ένα κλασικό υπολογιστή απαιτούνται αλληλεπιδράσεις, κρίνεται απαραίτητο να υπάρχει αρκετά στενή σύνδεση μεταξύ τους. Αυτό λόγω του ότι μία κβαντική κατάσταση αποσυντίθεται σε microseconds ώστε να μη χάνεται χρόνος και συνάμα χρειάζεται μία κλασική αναπαράσταση των αποτελεσμάτων της για καλύτερη κατανόηση, η οποία αναπαράσταση αποτυπώνεται στη μορφή κλασικών πραγματικών αριθμών.

Quantum Hybrid Cloud

Όταν χρειάζεται ένας κλασικός και ένας κβαντικός υπολογιστής να αλληλοεπιδράσουν, και αυτό γίνεται μέσω APIs(Application Programming Interface).

Αν για παράδειγμα κάποιος θέλει να βελτιστοποιήσει μία παρατηρήσιμη τιμή σε σύγκριση με άλλες ορισμένες παραμέτρους ενός συστήματος, πρακτικά θα έπρεπε να δοκιμάζει συνεχώς από ένα μεγάλο εύρος παραμέτρων, και αφού δει τα αποτελέσματα να επιλέξει τις καλύτερες τιμές για αυτές. Το QCS όμως έχει πολύ χρήσιμες λειτουργίες για αυτά.

Όταν εφαρμόζουμε μία πύλη, τότε καταρρέουμε την κβαντική κατάσταση και την ορίζουμε σε συγκεκριμένη κατάσταση αποτελεσματικώς.

Υπάρχει ένα εύρος πυλών, με τις βασικές πύλες να υπάρχουν γύρω από τους κύριους άξονες.

Από το εύρος πυλών που υπάρχουν, στη πραγματικότητα λίγες είναι αυτές που μπορούν να εφαρμοστούν, αναλόγως και με την ακριβή φυσική εφαρμογή του QPU.

GROVE

Πρόκειται για μία Python βιβλιοθήκη η οποία είναι open-source και περιέχει κβαντικούς υλοποιημένους αλγορίθμους που χρησιμοποιούν τη βιβλιοθήκη PyQuil και το Rigetti Forest toolkit.

Ένας από αυτούς είναι ο αλγόριθμος του Grover ο οποίος αποτελεί έναν αλγόριθμο αναζήτησης και η διαφορά του είναι ότι μέσω αυτού μπορούμε από εκεί που με μία κλασική αναζήτηση θα απαιτούνταν O(N) εκτιμήσεις, χάρη στο κβαντικό κόσμο μπορούμε να κάνουμε μία αναζήτηση στο O(sqrt(N)), αφού ουσιαστικά ελέγχουμε ταυτοχρόνως πολλαπλές καταστάσεις μέσω της υπέρθεσης.

3. ΚΒΑΝΤΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ

3.1 Bra, ket

Σημειογραφία Ντιράκ – Dirac Notation

Ο συμβολισμός Dirac αποτελεί μία γλώσσα η οποία έχει σχεδιαστεί ώστε οι ανάγκες των καταστάσεων έκφρασης στη κβαντική μηχανική να "εφαρμόζουν" με αυτή.

Ο ορισμός **Bracket** μεταφράζεται ως αγκύλη. Ως εκ τούτου, τα σύμβολα όπου χρησιμοποιούμε για να περικλείουμε φράσεις και σήματα πληροφορίας είναι αγκύλες και απεικονίζονται με « > » και « < ». Ο συμβολισμός τους προέκυψε από τον ευρέως γνωστό φυσικό **Paul Dirac**, ο οποίος όρισε αυτά τα διανύσματα κατάστασης των κβαντικών συστημάτων με μισές αγκύλες , <| και |>. Το πρώτο σύμβολο, πήρε τη ονομασία bra, από το πρώτο συνθετικό της λέξης "bracket" , και το δεύτερο από το δεύτερο συνθετικό της.

Εικόνα 13. : Paul Dirac

Πηγή: (https://www.nature.com/articles/459326a) Credit: BETTMAN/CORBIS

Τα διανύσματα ket έχουν την ιδιότητα ότι γίνεται να γραφούν σαν πίνακες με μία στήλη, οι οποίοι ονομάζονται πίνακες κατάστασης. Συγκεκριμένα, στη περίπτωση των κβαντικών συστημάτων δύο καταστάσεων, αυτοί οι πίνακες αποτελούνται από 2 στοιχεία.

Περιορισμοί της σημειογραφίας διανύσματος στήλης

Παρότι στη γραμμική άλγεβρα η σημειογραφία που υπάρχει στα διανύσματα των στηλών είναι κοινή, στους κβαντικούς υπολογιστές παρατηρείται μία δυσκινησία, ιδιαιτέρως όταν έχουν να κάνουν με πολλά qubits.

Παράδειγμα

Όταν πάμε να ορίσουμε ένα διάνυσμα, δεν είναι σαφές αν αυτό το διάνυσμα είναι γραμμής ή αν είναι στήλης. Συνεπώς αυτό σημαίνει πως πχ αν έχουμε φ και ψ διανύσματα, πάλι δεν είναι σαφές αν ορίζονται, τα σχήματα αυτών των διανυσμάτων υπάρχει περίπτωση να είναι ασαφή στο πλαίσιο.

Ακόμη και η περίπτωση της έκφρασης απλών διανυσμάτων, μπορεί να είναι δυσκίνητη αν χρησιμοποιηθεί γραμμική αλγεβρική σημειογραφία.

Παράδειγμα

Στη περίπτωση της περιγραφής μίας κατάστασης n-qubit, όπου κάθε qubit παίρνει την τιμή 0, η κατάσταση θα εκφραστεί:

$$\begin{bmatrix}1\\0\end{bmatrix}\otimes\cdots\otimes\begin{bmatrix}1\\0\end{bmatrix}.$$

Σημείωση

Λόγω του μεγάλου εκθετικά χώρου όπου υφίσταται το παραπάνω διάνυσμα, η αξιολόγηση του γινομένου τανυστή δεν είναι πρακτικά ορθή.

Παρόλα αυτά, ο συγκεκριμένος συμβολισμός είναι η καλύτερη περιγραφή όπου μπορούμε να δώσουμε χρησιμοποιώντας τη σημειογραφία που αναφέραμε.

Τύποι διανυσμάτων σε σημειογραφία Dirac

Δύο τύποι διανυσμάτων: Bra και ket.

Όταν συνδυαστούν σχηματίζουν ένα εσωτερικό γινόμενο και από εκεί προκύπτει και η ονομασία τους.

Αν ψ διάνυσμα στήλης, αναγράφεται ως |ψ⟩, όπου |⟩ ουσιαστικά δηλώνει ότι πρόκειται για διάνυσμα μοναδικής στήλης, όπως ένα διάνυσμα ket.

Αν ψ διάνυσμα γραμμής, με παρόμοια λογική, το διάνυσμα αναγράφεται ως ⟨ψ|.

Το bra-ket notation σημαίνει ότι το ⟨ψ|ψ⟩ , αποτελεί το εσωτερικό γινόμενο του φορέα ψ με τον ίδιο του τον εαυτό, κάτι που από προεπιλογή είναι 1.

Με βάση τα προαναφερθέντα, εφόσον έχουμε ψ και φ , τα οποία αποτελούν και τα δύο διανύσματα κβαντικής κατάστασης, τότε το εσωτερικό τους γινόμενο θα είναι ⟨φ|ψ⟩.

Συμπερασματικά, η πιθανότητα η κατάσταση |ψ⟩ να είναι |φ⟩ είναι |⟨φ|ψ⟩|2.

Παρακάτω γίνεται χρήση της συγκεκριμένης σύμβασης ώστε να γίνει περιγραφή των κβαντικών καταστάσεων που κωδικοποιούν τις τιμές του μηδενός και του ενός.

$$\begin{bmatrix}1\\0\end{bmatrix} = |0\rangle\,, \qquad \begin{bmatrix}0\\1\end{bmatrix} = |1\rangle\,.$$

Καταστάσεις qubit

Ketbra

Ketbra ή αλλιώς εξωτερικό γινόμενο είναι όταν τα bra και τα ket είναι στη αντίθετη σειρά από ότι τα braket. Αναπαρίσταται ως |ψ⟩ ⟨φ|.

Το εξωτερικό γινόμενο ορίζεται ως πολλαπλασιασμός πινάκων :

$|\psi\rangle \langle\phi| = \psi\phi^{\dagger}$ για διανύσματα κβαντικής κατάστασης ψ και ϕ.

Παράδειγμα του συγκεκριμένου συμβολισμού :

$$|0\rangle \langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad |1\rangle \langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

3.2 Qubit

Τι είναι;

Qubit ονομάζεται το bit της κβαντικής μηχανικής. Ένα κλασικό **bit** όπου κωδικοποιεί τις πληροφορίες σε έναν κλασικό υπολογιστή, έχει τη δυνατότητα να είναι είτε μηδέν είτε ένα. Όμως, στο κβαντικό υπολογισμό αυτό αλλάζει, καθώς στη περίπτωση του **qubit** το οποίο κωδικοποιεί τις πληροφορίες, έχει την ιδιότητα να είναι και μηδέν και ένα ταυτόχρονα. Αυτό το φαινόμενο είναι γνωστό ως **υπέρθεση** (superposition).

Οι δύο καταστάσεις qubit αναγράφονται ως: |0⟩ και |1⟩.

Εικόνα 14. : Representation of the qubit project (Πηγή: Jackie Niam -stock.adobe.com)

Τεχνολογίες Qubit

Υπάρχει πληθώρα διαφόρων φυσικών υλοποιήσεων των qubits, όπως οι πολώσεις ενός φωτονίου, η περίπτωση ενός υπεραγώγιμου qubit Transmon, οι καταστάσεις spin ενός ηλεκτρονίου, οι καταστάσεις του πυρηνικού σπιν ενός ατόμου και πολλές άλλες.

"QM είναι σε καθημερινή χρήση και εξαιρετικά επιτυχής στην κατανόηση, πρόβλεψη και τον υπολογισμό παρατηρούμενων φαινομένων - Van Kampen"

Όσον αφορά την αρχιτεκτονική, κάποιες από τις υλοποιήσεις χρειάζονται τα qubit να βρίσκονται σε θερμοκρασία κοντά στο απόλυτο μηδέν ώστε να επιτευχθεί η διατήρησή τους.

Οι καταστάσεις qubit ην ιδιότητα να αλληλοεπιδρούν μεταξύ τους, διότι κάθε κατάσταση μπορεί να περιγραφεί από πολλές πιθανότητες, όπως συμβαίνει και στα πλάτη των κυμάτων, αυτό ονομάζεται παρεμβολή και είναι συνέπεια της υπέρθεσης.

Εμπλοκή

Πολλά qubits έχουν την δυνατότητα να δείξουν κβαντική διεμπλοκή, ουσιαστικά σχηματίζουν ένα ενιαίο σύστημα. Και σε περιπτώσεις που έχουν άπειρη απόσταση μεταξύ τους, αρκεί να γνωρίζουμε τη μέτρηση της κατάστασης από ένα qubit, ώστε να γνωρίζουμε τη κατάσταση του άλλου, δίχως να χρειάζεται άμεση μέτρηση.

Μέλλον

Μέσω της εξέλιξης και της προόδου των κβαντικών τεχνολογιών, η ανθρωπότητα φτάνει όλο και πιο κοντά στη εύρεση λύσεων σε μερικά από τα πιο δύσκολα προβλήματα που αντιμετωπίζει.

Ένα πολύ σημαντικό πρόβλημα που αντιμετωπίζουν τα qubits είναι η ευθραυστότητα που τα χαρακτηρίζει. Όταν το σύστημα qubit εμπλέκεται με το περιβάλλον του, τότε υπάρχει πολύ μεγάλή πιθανότητα να προκληθεί αποσυνοχή και να διαταραχθεί το σύστημα. Αυτό έχει ως αποτέλεσμα να γίνονται συνεχώς πρόοδοι και εξελίξεις όσον αφορά τη κατασκευή υλικού κβαντικής υπολογιστικής και στις μεθόδους διόρθωσης σφαλμάτων.

Στη περίπτωση των τοπολογικών qubits υπάρχει μεγαλύτερη σταθερότητα. Για αυτό και χρησιμοποιούνται πιο πολύ από τη Microsoft για να αντιμετωπιστεί η ευθραυστότητα,

καθώς αυτά σταθεροποιούνται και προστατεύονται από μολύνσεις λόγω του περιγύρου τους. Έπειτα, χάρη στο quasisωματίδιο που διαθέτουν προστατεύονται από τον θόρυβο. Αυτό έχει ως

αποτέλεσμα η κβαντική κλίμακα υπολογιστή να έχει τη δυνατότητα να ολοκληρώσει πολύ πιο συνθέτους υπολογισμούς και να βρει περισσότερες λύσεις.

Ότι είναι το bit για τους κλασικούς υπολογιστές, τον ίδιο ρόλο έχει το qubit για τους κβαντικούς υπολογιστές, καθώς αποτελεί την μονάδα πληροφορίας τους.

Αυτό που χαρακτηρίζει τα qubits είναι μία υπέρθεση πολλών πιθανών καταστάσεων.

Χρησιμοποιεί το φαινόμενο της υπέρθεσης και πετυχαίνει ένα γραμμικό συνδυασμό από 2 καταστάσεις. Στη περίπτωση του κλασικού bit, αυτό μπορεί να υπάρξει μόνο είτε σε κατάσταση 0, είτε μόνο σε κατάσταση 1. Από την άλλη πλευρά, ένα qubit μπορεί να βρίσκεται και στις 2 καταστάσεις ταυτόχρονα, και 0 και 1, είτε ένα οποιοδήποτε ποσοστό του 0 και του 1 λόγω της υπέρθεσης.

Ένα qubit σύστημα μπορεί να χρησιμοποιήσει έναν όγκο πληροφοριών, ο οποίος αυξάνεται με εκθετικό ρυθμό.

πχ: Στη περίπτωση ενός κλασικού υπολογιστή θα χρειαζόταν εκατομμύρια χρόνια για να βρεθούν οι πρώτοι παράγοντες ενός αριθμού με 2048 bit, ενώ με qubits θα χρειαζόταν λίγα λεπτά.

3.3 Κβαντικές Πύλες(Quantum Gates)

Hadamard Gate (H)

Η πύλη **Hadamard**, έχει το χαρακτηριστικό ότι δρα σε ένα qubit. Αυτό σημαίνει πως μέσα σε μια σφαίρα Bloch, η πύλη H περιστρέφει το διάνυσμα κατάστασης ενός qubit. Συνεπώς, υπάρχει μεταβολή των γωνιών θ και φ. Αξιοσημείωτο είναι, ότι υπάρχει άπειρος αριθμός κβαντικών πυλών που εφαρμόζονται σε ένα qubit, όμως χρησιμοποιούνται κατά κύριο λόγο οι **3** από αυτές, εκ των οποίων μία είναι η Hadamard.

- Απεικονίζεται με τον τελεστή **H**.
- Ο πίνακας που αναπαριστά τον τελεστή αυτής της πύλης:

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

Στη περίπτωση όπου ένα qubit βρίσκεται στη κατάσταση $|0\rangle$ **(βασική)**, τότε η εφαρμογή της πύλης Hadamard σε αυτό, έχει ως αποτέλεσμα:

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

Ενώ αν ένα qubit βρίσκεται στη κατάσταση $|1\rangle$ **(βασική)** , τότε:

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

Συμπερασματικά, όταν εφαρμόζεται η πύλη Hadamard σε qubits τα οποία βρίσκονται σε μία από τις 2 βασικές καταστάσεις , τότε αυτά θέτονται σε **υπέρθεση**(superposition).

Αυτό σημαίνει , ότι η πιθανότητα ένα qubit, αφού μετρηθεί, να βρίσκεται στη κατάσταση $|0\rangle$, είναι ίση με το να βρίσκεται στη κατάσταση $|1\rangle$. Συνεπώς, και οι δύο πιθανότητες είναι ισόποσες (0,5).

Παρακάτω φαίνεται τι συμβαίνει όταν εφαρμόζεται η πύλη Hadamard σε ένα qubit όπου είναι στη υπέρθεση καταστάσεων με βάση:

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

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

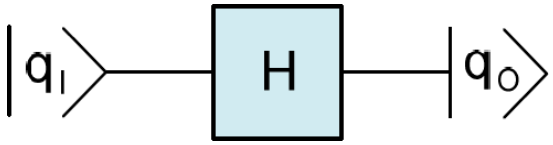
Παρακάτω φαίνεται τι συμβαίνει όταν εφαρμόζεται η πύλη Hadamard σε ένα qubit όπου είναι στη

$$: \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

υπέρθεση καταστάσεων με βάση:

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

Η πύλη Hadamard επιστρέφει τα qubits στις **βασικές** τους καταστάσεις.



Σχήμα 3-3. Το σύμβολο της κβαντικής πύλης Hadamard, Η.(ΚΒΑΝΤΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗ)

$\|q_I\rangle$	$\|q_O\rangle$
$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$
$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	$\|0\rangle$
$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\|1\rangle$

Πίνακας 3-3. *Η δράση της κβαντικής Hadamard στις καταστάσεις ενός qubit.*

Τέλος, η πύλη Hadamard, αποτελεί μία πολύ σημαντική πύλη, καθώς θέτει τα qubit από τις βασικές τους καταστάσεις σε υπέρθεση και το αντίθετο. Αυτό, αποτελεί το βασικό λόγο που θεωρείται η κύρια πύλη για τη διασύνδεση μεταξύ κλασικών και κβαντικών υπολογιστών μελλοντικά.

CNOT Gate (CNOT)

Ορισμός: Controlled-NOT(CNOT)

Το **χαρακτηριστικό** της συγκεκριμένης πύλης, είναι ότι έχει δράση πάνω σε 2 qubits.

Το ένα qubit αναφέρεται ως qubit ελέγχου και αναπαρίσταται με "c", ενώ το άλλο qubit συμβολίζεται με "t" και ονομάζεται qubit στόχος.

Πρώτού εφαρμοστεί η πύλη, τα 2 qubits βρίσκονται στις καταστάσεις $|c_i\rangle$ και $|t_i\rangle$.

Αφότου δράσει η πύλη, τα qubits βρίσκονται στις καταστάσεις $|c_o\rangle$ και $|t_o\rangle$.

Στη περίπτωση όπου η κατάσταση του qubit ελέγχου είναι $|1\rangle$, τότε η πύλη CNOT αλλάζει τη κατάσταση του qubit στόχου.

Αντιθέτως, όταν η κατάσταση του qubit ελέγχου είναι $|0\rangle$, τότε δεν αλλάζει τη κατάσταση του qubit στόχου.

Επιπλέον, όσον αφορά τη κατάσταση του qubit ελέγχου $|c_i\rangle$,δεν υπάρχει πότε μεταβολή , καθώς ισχύει **πάντα** ότι

$$|c_i\rangle = |c_o\rangle$$

.

Αναπαράσταση της πύλης CNOT:

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

Όταν η πύλη CNOT εφαρμόζεται πάνω σε ένα κβαντικό καταχωρητή που αποτελείται από 2 qubits, τότε ισχύει το εξής:

$$CNOT\,|c_i t_i\rangle = |c_o t_o\rangle$$

Αν η κατάσταση του κβαντικού καταχωρητή πριν δράσει η πύλη είναι $|10\rangle$.

Τότε :

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

Παρατηρούμε ότι η κατάσταση του qubit **στόχου** άλλαξε από $|0\rangle$ σε $|1\rangle$, καθώς η κατάσταση του qubit **ελέγχου** είναι $|1\rangle$.

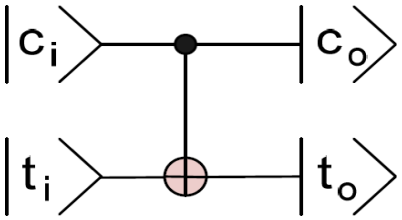
Στην άλλη περίπτωση, $|01\rangle$:

τότε:

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

Αυτή τη φορά παρατηρούμε ότι η κατάσταση του qubit **στόχου** δεν μεταβάλλεται καθώς η κατάσταση του qubit **ελέγχου** είναι $|0\rangle$.

Συμβολισμός CNOT



Αξιοσημείωτο είναι, ότι με τις πύλες CNOT,H και Φ, μπορεί να γίνει πράξη οποιοσδήποτε κβαντικός υπολογισμός, καθώς αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών.

Η κβαντική πύλη αδράνειας

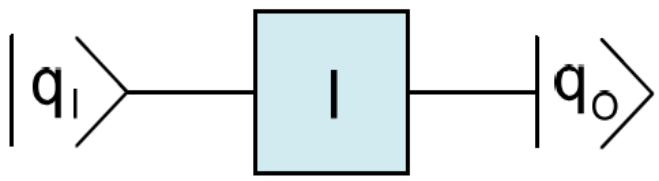
Συμβολίζεται με I και ο συγκεκριμένος τελεστής λέγεται τελεστής αδράνειας.

Πίνακας για τον τελεστή I:

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

Το χαρακτηριστικό της πύλης αδράνειας, είναι ότι μετά την εφαρμογή της, αφήνει **ανεπηρέαστη** τη κατάσταση του qubit στο οποίο εφαρμόζεται.

$$I \left| q \right\rangle = \left| q \right\rangle$$

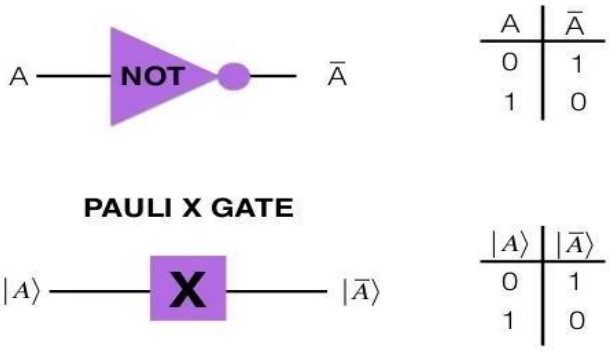


Σχήμα 3-1. Το σύμβολο της κβαντικής πύλης αδρανείας, I.

Με $\left| q_I \right\rangle$ συμβολίζεται η κατάσταση του qubit πριν να δράσει η πύλη και με $\left| q_O \right\rangle$ συμβολίζεται η κατάσταση του qubit αφότου δράσει η πύλη.

Η Κβαντική πύλη X-gate

Η κβαντική πύλη Pauli X χαρακτηρίζεται από την άρνηση. Δεν υφίστανται φανταστικοί αριθμοί σε αυτή τη πύλη. Συνεπώς η κβαντική πύλη Pauli X είναι μία πύλη NOT.



Εικόνα 15. : Pauli X-gate(Πηγή: https://www.quantum-inspire.com/kbase/pauli-x/)

Αξιοσημείωτο είναι, πως στη πραγματική ζωή αυτό που κάνει η πύλη X είναι ότι μετατρέπει την κατάσταση spin-up |0> ενός ηλεκτρονίου σε μία κατάσταση αναπτυσσόμενης λίστας |1> και αντίστροφα.

```
|0>  -->  |1>  OR  |1> --> |0>
```

Η πύλη Pauli X συμβολίζεται με «X»

Οι Κβαντικές πύλες Y και Z

Η πύλη Y παρουσιάζει μεγάλη ομοιότητα με τη πύλη X, αλλά η ειδοποιός διαφορά είναι ότι υπάρχει και ένα i στη θέση του 1 και ένα αρνητικό πρόσημο βρίσκεται πάνω δεξιά.

Είναι μία πύλη NOT με i πολλαπλάσιο.

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Η πύλη Z μοιάζει με την πύλη X αλλά υπάρχει και ένα αρνητικό πρόσημο.

/ 1 0 \

\ 0 -1 /

Gate	Transformation on Bloch sphere (defined for single qubit)
X	π-rotation around the X axis, Z→−Z. Also referred to as a bit-flip.
Z	π-rotation around the Z axis, X→−X. Also referred to as a phase-flip.
H	maps X→Z, and Z→X. This gate is required to make superpositions.

Συμπερασματικά, η πύλες Y και Z αλλάζουν τη περιστροφή του του ηλεκτρονίου qubit.

Swap Gate

Η πύλη SWAP λειτουργεί πάνω σε δύο qubit. Εκφράζεται σε καταστάσεις βάσης και ουσιαστικά ανταλλάσσει τη κατάσταση δύο qubits:

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

3.4 Κβαντικοί καταχωρητές(Quantum Registers)

Η χρήση των καταχωρητών υπόκειται στο να αποθηκεύουν τις τιμές ορισμένων μεταβλητών. Στη περίπτωση των κλασικών υπολογιστών, ένα σύνολο από bits αποτελεί έναν καταχωρητή. Επομένως, στη περίπτωση των κβαντικών υπολογιστών, ένας κβαντικός καταχωρητής απαρτίζεται από ένα σύνολο qubits. **Αξιοσημείωτο** αποτελεί το γεγονός ότι η αρίθμηση των qubits εφαρμόζεται από τα δεξιά προς τα αριστερά και κατά κύριο λόγο η διάταξη τους είναι σε σειρά.

Η κύρια διαφορά μεταξύ ενός κλασικού και ενός κβαντικού καταχωρητή, είναι ότι στον δεύτερο υπάρχει η δυνατότητα αποθήκευσης πολύ **μεγαλύτερου** όγκου πληροφορίας.

Παράδειγμα

Κβαντικός καταχωρητής που αποτελείται από 2 qubits $|q_1\rangle$ και $|q_0\rangle$.

Μέσω του τανυστικού γινομένου από τις καταστάσεις των qubit που το αποτελούν , δίνεται η κατάσταση του κβαντικού καταχωρητή, και απεικονίζεται ως:

$$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = |q_1\rangle|q_0\rangle = |q_1 q_0\rangle$$

Το $\otimes$ αποτελεί το συμβολισμό του **τανυστικού γινομένου**.

Αν έχουμε δύο πίνακες, Α και Β

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

Τότε, το τανυστικό τους γινόμενο πρόκειται για ένα τρίτο πίνακα με μία στήλη, τον πίνακα C , όπου :

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

Κατά συνέπεια, αυτό σημαίνει ο αριθμός των στοιχείων του πίνακα C, είναι όσα έχουν ο Α και ο Β **αθροιστικά**.

Έπειτα,

Το 1ο στοιχείο, αποτελεί το γινόμενο των πρώτων στοιχείων του **A** και **B**.

Το 2ο στοιχείο, αποτελεί το γινόμενο του πρώτου στοιχείου του A και του δεύτερου στοιχείου του B.

Αντίστοιχα, το 3ο και 4ο στοιχείο του C, αποτελούν το δεύτερο στοιχείο του A επί το 1ο και το 2ο στοιχείο του B.

Παραδείγματα

Δυό καταστάσεις qubits:

q1:

$$|q_1\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

q0:

$$|q_0\rangle = c|0\rangle + d|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$$

Τότε, η κατάσταση του κβαντικού καταχωρητή, θα δίνεται από:

$$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

$$= (a\cdot c)|0\rangle\otimes|0\rangle + (a\cdot d)|0\rangle\otimes|1\rangle + (b\cdot c)|1\rangle\otimes|0\rangle + (b\cdot d)|1\rangle\otimes|1\rangle$$

$$= c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Ουσιαστικά, αυτό που έγινε είναι η αντικατάσταση από το a*c, a*d, b*c, b*d, που κάναμε στο προηγούμενο παράδειγμα, με τα c0, c1, c2 και c3.

Αυτό σημαίνει, πως εφόσον έχουμε 2 qubits, ο κβαντικός καταχωρητής που προκύπτει, αποτελείται από ένα σύστημα 4 βασικών καταστάσεων, οι οποίες προκύπτουν από το τανυστικό γινόμενο των βασικών καταστάσεων των qubits.

ΒΑΣΙΚΕΣ ΚΑΤΑΣΤΑΣΕΙΣ

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

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

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

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

Superposition: Υπέρθεση είναι η ικανότητα ενός κβαντικού συστήματος να βρίσκεται σε πολλαπλές καταστάσεις ταυτόχρονα μέχρι να μετρηθεί.

Bell state: Είναι συγκεκριμένη κβαντική κατάσταση 2 qubits που αντιπροσωπεύει τα απλούστερα και μέγιστα παραδείγματα της κβαντικής εμπλοκής(entaglement).

Quantum entanglement: Η κβαντική διεμπλοκή είναι το φαινόμενο που συμβαίνει όταν μια ομάδα σωματιδίων παράγονται, αλληλοεπιδρούν, ή μοιράζονται χωρική εγγύτητα με τέτοιο τρόπο ώστε η κβαντική κατάσταση κάθε σωματιδίου της ομάδας δεν μπορεί να περιγράφει ανεξάρτητα από την κατάσταση των άλλων.

GHZ stage: Μια κατάσταση Greenberger-Horne-Zeilinger (κατάσταση GHZ) είναι ένας συγκεκριμένος τύπος διεμπλεγμένης κβαντικής κατάστασης που περιλαμβάνει τουλάχιστον τρία υποσυστήματα (καταστάσεις σωματιδίων, qubits, ή qubit).

Quantum state: Είναι ένα σύνθετο διάνυσμα των διαστάσεων 2^n , όπου n είναι ο αριθμός των qubits.

Για να προσομοιώσουμε ένα κύκλωμα χρησιμοποιούμε την quant_info ενότητα στο Qiskit.

Ground state: Η βασική κατάσταση ενός κβαντομηχανικού συστήματος είναι η σταθερή κατάσταση της χαμηλότερης ενέργειας, η ενέργεια της κατάστασης του εδάφους είναι γνωστή ως ενέργεια μηδενικού σημείου του συστήματος.

4. ΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ-ΠΡΟΓΡΑΜΜΑΤΑ

4.1 Grover's Algorithm

Πολύ συχνά, στην περίπτωση των Κβαντικών Υπολογιστών ο αλγόριθμος Grover ονομάζεται αλλιώς και αλγόριθμος αναζήτησης. Αυτό που κάνει είναι ότι βρίσκει με πολύ μεγάλη πιθανότητα τη μοναδική είσοδο σε μία συνάρτηση μαύρου κουτιού η οποία δημιουργεί μια συγκεκριμένη τιμή εξόδου.

Χρησιμοποιείται μαζί με διάφορες παραλλαγές, όπως η ενίσχυση πλάτους με σκοπό τη επιτάχυνση ενός μεγάλου φάσματος αλγορίθμων.

Επίσης, ακόμη μία χρησιμότητα του συγκεκριμένου αλγορίθμου είναι ότι μπορεί να εκτιμήσει τη μέση τιμή ενός συνόλου αριθμών και να βοηθήσει στη επίλυση του προβλήματος σύγκρουσης (collision problem). Επιπλέον, χρησιμοποιείται για τη επίλυση NP-complete προβλήματα, κάνοντας πολλές πάρα πολλές αναζητήσεις στο σύνολο των πιθανών λύσεων.

Τέλος, είναι πιθανολογικός αλγόριθμος, δηλαδή δίνει τη σωστή απάντηση με μεγάλη πιθανότητα. Με κάθε επανάληψη μειώνεται η πιθανότητα αποτυχίας.

Παράδειγμα

```
from qiskit import *

from qiskit.visualization import plot_histogram

s = [0, 1] # το s μπορεί να πάρει οποιαδήποτε τιμή 2 bits

n = 2

grover_circuit = QuantumCircuit(n)

for i in range(n):

   grover_circuit.h(i)

grover_circuit.cz(0,1)

for i in range(n):

grover_circuit.h(i)
```

```
for i in range(n):
    if s[i] == 1:
        grover_circuit.z(i)
grover_circuit.cz(0,1)
for i in range(n): grover_circuit.h(i)
grover_circuit.draw(output='mpl')
grover_circuit.measure_all()
aer_sim = Aer.get_backend('aer_simulator')
qobj = assemble(grover_circuit)
result = aer_sim.run(qobj).result()
simulation_counts = result.get_counts()
plot_histogram(simulation_counts)
```

4.2 MyFirstCircuit

1. import QuantumCircuit

2. Δημιουργούμε ένα κβαντικό κύκλωμα από 3 qubits.

3. Προσθέτουμε λειτουργίες στο κύκλωμα, μία προς μία.

qubit 0: H gate-->Superposition

qubits(0,1): CX(CNOT)--> Bell state

qubits(0,2): CX(CNOT)-->GHZ state

Superposition: Υπέρθεση είναι η ικανότητα ενός κβαντικού συστήματος να βρίσκεται σε πολλαπλές καταστάσεις ταυτόχρονα μέχρι να μετρηθεί.

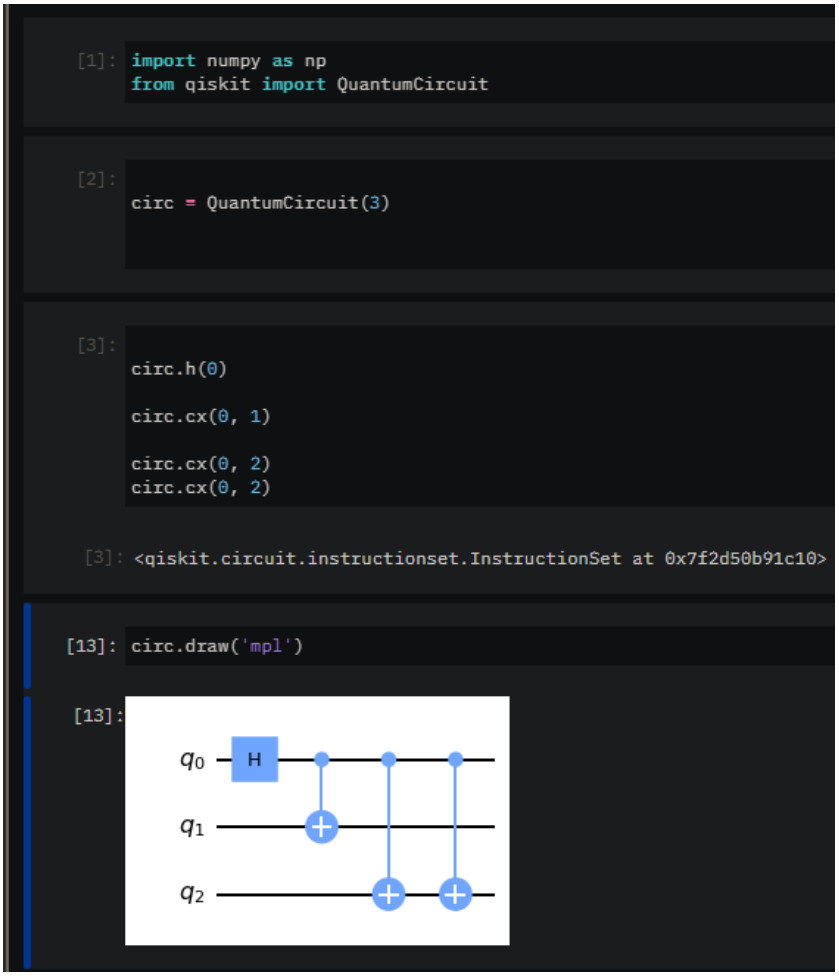
Bell state: Είναι συγκεκριμένη κβαντική κατάσταση 2 qubits που αντιπροσωπεύει τα απλούστερα και μέγιστα παραδείγματα της κβαντικής εμπλοκής (entaglement).

GHZ stage: Μια κατάσταση Greenberger-Horne-Zeilinger (κατάσταση GHZ) είναι ένας συγκεκριμένος τύπος

διεμπλεγμένης κβαντικής κατάστασης που περιλαμβάνει τουλάχιστον τρία υποσυστήματα (καταστάσεις σωματιδίων, qubits, ή qudit).

4. Visualize Circuit μέσω circ.draw('mpl').

Στο συγκεκριμένο κύκλωμα, η τοποθέτηση των qubits γίνεται με τη σειρά, με το qubit 0 στη κορυφή και το qubit 2 στο κάτω μέρος.(Διαβάζεται από αριστερά στα δεξιά, με αποτέλεσμα οι πύλες που βρίσκονται πιο αριστερά, να εφαρμόζονται πιο νωρίς).



Simulation

Η ενότητα quant_info χρησιμοποιείται ώστε να γίνει η προσομοίωση ενός κυκλώματος στο Qiskit. Μέσω αυτού του προσομοιωτή, επιστρέφεται η κβαντική κατάσταση η οποία αποτελεί ένα πολύπλοκο διάνυσμα διαστάσεων 2^n, με n τον αριθμό των qubits.

Δύο στάδια: 1. Ορίζεται η κατάσταση εισόδου

2. Εξέλιξη της κατάστασης από το κβαντικό κύκλωμα.

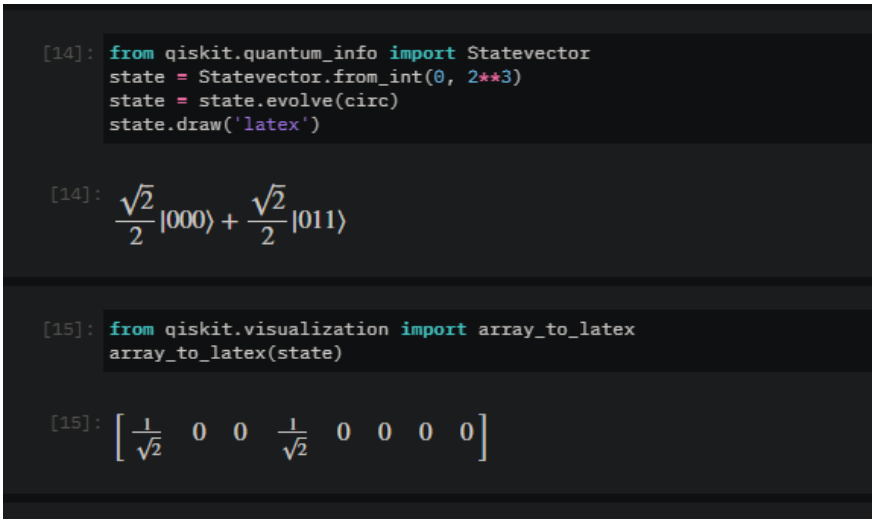
1. Import statevector

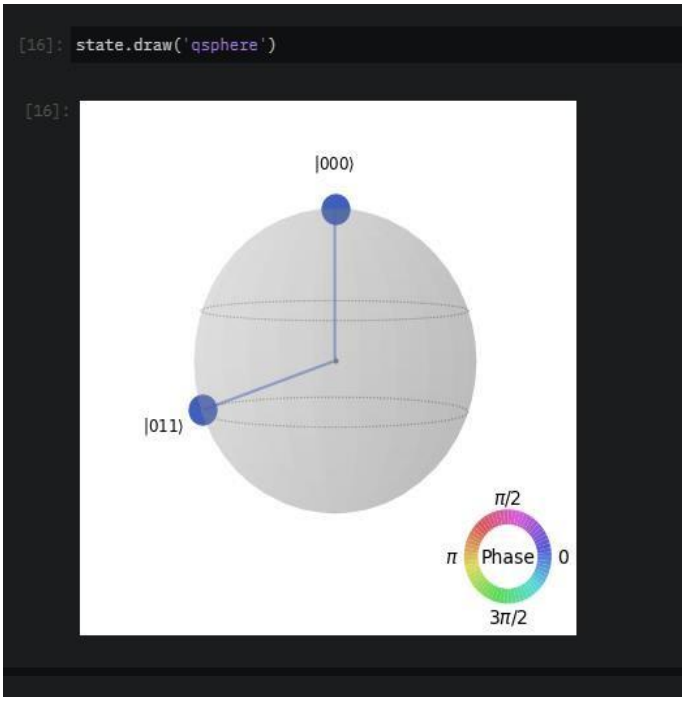
2. Ορισμός της αρχικής κατάστασης του προσομοιωτή στο ground state με τη χρήση του front_int.

ground state: Η βασική κατάσταση ενός κβαντομηχανικού συστήματος είναι η σταθερή κατάσταση της χαμηλότερης ενέργειας, η ενέργεια της κατάστασης του εδάφους είναι γνωστή ως ενέργεια μηδενικού σημείου του συστήματος.

3. Εξέλιξη της κατάστασης από το κβαντικό κύκλωμα.

4. draw using latex.





4.3 Fourier Checking Circuit

Import qiskit.quantum_info as qi(Αυτό θα κάνει τους υπολογισμούς).

Import library

Import visualizer

Κάνουμε ορισμό δύο συναρτήσεων f και g (inputs).

Το Fourier Checking Circuit μας αποκαλύπτει πόσο συσχετιζόμενος είναι ο μετασχηματισμός fourier του g με τη συνάρτηση f.

Οπότε το κύκλωμα θα εξάγει μία πιθανότητα για την μηδενική κατάσταση.

Και αν η πιθανότητα είναι μεγαλύτερη από 0,05, τότε ο μετασχηματισμός Fourier της συνάρτησης g συσχετίζεται με τη συνάρτηση f μας.

Το συμπέρασμα είναι ότι ένας κβαντικός υπολογιστής, μπορεί να κάνει αυτόν τον υπολογισμό πολύ πιο γρήγορα από ένα κλασικό υπολογιστή.

Κάνουμε set τα circuits circ = FourierChecking(f=f,g=g).

circuit for calculation

```
In [4]: zero = qi.Statevector.from_label('00')
        sv = zero.evolve(circ)
```

Αυτό εκτελεί το κύκλωμα με τον προσομοιωτή στατικού μηχανισμού.

Μας ενδιαφέρει μόνο η 00 πιθανότητα.

```
probs = sv.probabilities_dict()
plot_histogram(probs)
```

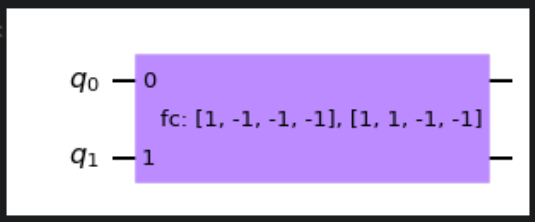
outputs

Με βάση το histogram, αυτό σημαίνει ότι ο μετασχηματισμός Fourier της συνάρτησης g μου είναι συσχετισμένος με τη συνάρτηση f μου.

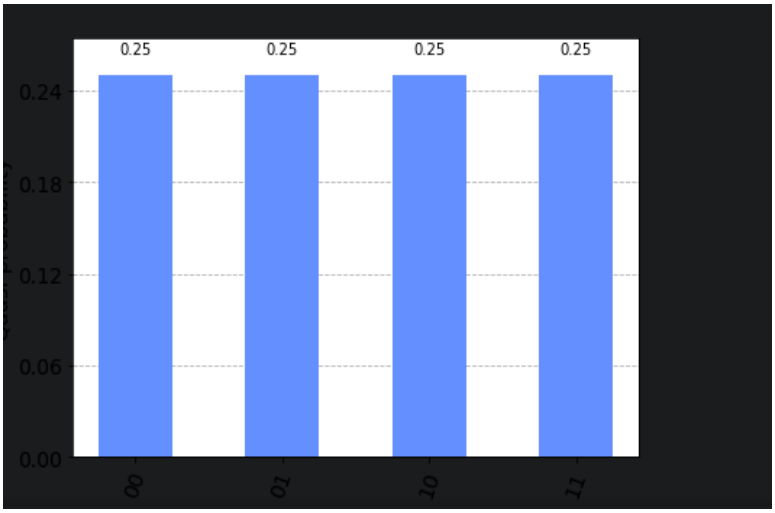
Τα outputs αλλάζουν με βάση το input που βάζουμε στις συναρτήσεις.

```
[1]: import qiskit.quantum_info as qi
     from qiskit.circuit.library import FourierChecking
     from qiskit.visualization import plot_histogram

[2]: f=[1,-1,-1,-1]
     g=[1,1,-1,-1]

[3]: circ = FourierChecking(f=f,g=g)
     circ.draw()
```

[3]:




```
[4]: zero = qi.Statevector.from_label('00')
     sv = zero.evolve(circ)
     probs = sv.probabilities_dict()
     plot_histogram(probs)
```



Ο κβαντικός μετασχηματισμός Fourier έχει δράση πάνω σε ένα κβαντικό διάνυσμα κατάστασης. Αποτελεί μία ακολουθία πιθανοτήτων κατά τη διάρκεια της μέτρησης για όλα τα κβαντικά αποτελέσματα. Παρόλα αυτά, λόγω της σύμπτυξης της κβαντικής κατάστασης σε μία κατάσταση βάσης, δεν είναι εφικτό να επωφεληθεί με την ίδια επιτάχυνση του κβαντικού μετασχηματισμού Fourier, κάθε εργασία που χρησιμοποιεί τον κλασικό μετασχηματισμό Fourier.

4.4 Shor's Algorithm

Ο αλγόριθμος του Shor χρησιμοποιείται για την εύρεση των πρώτων παραγόντων ενός ακεραίου και δημιουργήθηκε το 1994 από τον Peter Shor.

Αποτελεί ένα πολύ σημαντικό αλγόριθμο, διότι λέει ότι η κρυπτογράφηση δημοσίου κλειδιού (public key) είναι δυνατό να σπάσει σχετικά εύκολα, αν υπάρχει ένας αρκετά μεγάλος κβαντικός υπολογιστής.

Αν υπάρχει ένας κβαντικός υπολογιστής με επαρκή αριθμό qubits, τότε η λειτουργία του θα υπήρχε δίχως να υποπέσει σε κβαντικό θόρυβο (noise) και κάποια ακόμη φαινόμενα που έχουν να κάνουν με τη κβαντική αποσυνοχή (decomposition) και έτσι θα ήταν δυνατό να σπάσει η κρυπτογράφηση δημοσίου κλειδιού, όπως

Το καθεστώς RSA

Πρωτόκολλο Diffie-Hellman

Η ελλειπτική ανταλλαγή κλειδιών Diffie-Hellman.

Το πρόβλημα που προσπαθούμε να λύσουμε είναι ότι, δεδομένου ενός ακεραίου N, προσπαθούμε να βρούμε έναν άλλο ακέραιο p μεταξύ του 1 και του N που διαιρεί το N.

Ο αλγόριθμος του Shor αποτελείται από δύο μέρη:

Μια μείωση του προβλήματος παραγοντοποίησης στο πρόβλημα της εύρεσης παραγγελίας, η οποία μπορεί να γίνει σε έναν κλασσικό υπολογιστή.

Ένας κβαντικός αλγόριθμος για να λύσει το πρόβλημα εύρεσης διάταξης.

5. ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Η διαφορά που υφίσταται μεταξύ αυτών των δύο, είναι πως η μετα-κβαντική κρυπτογραφία έχει να κάνει με κρυπτογραφικούς αλγορίθμους, οι οποίοι θεωρούνται ασφαλείς απέναντι σε επιθέσεις από κβαντικούς υπολογιστές. Αυτό σημαίνει πως οι κλασικοί υπολογιστές μπορεί να χρειαστούν μήνες και χρόνια για να σπάσουν αυτές τις εξισώσεις.

Σημείωση: Μέσω του αλγορίθμου του Shor, γίνεται οι κβαντικοί υπολογιστές να καταφέρουν να σπάσουν αυτά τα μαθηματικά συστήματα.

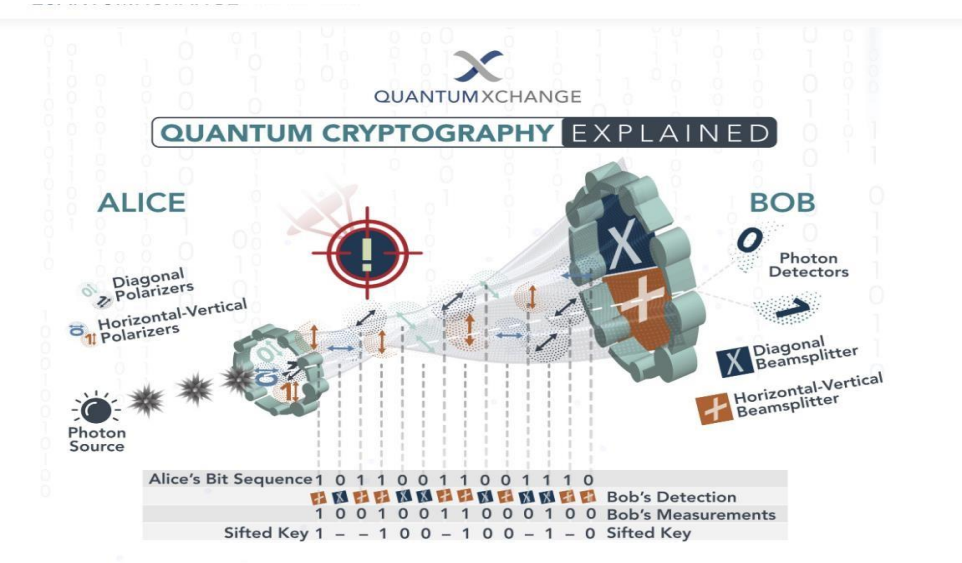
Από την άλλη, στη περίπτωση της κβαντικής κρυπτογραφίας χρησιμοποιούνται οι αρχές της κβαντικής μηχανικής με σκοπό την αποστολή ασφαλών μηνυμάτων, κάτι που τη καθιστά αρκετά πιο εύκολο να παραβιαστεί.

5.1 Πως λειτουργεί η Κβαντική Κρυπτογραφία

Ο τρόπος που λειτουργεί η κβαντική κρυπτογραφία ή αλλιώς και διανομή κβαντικού κλειδιού(QKD) , είναι πως χρησιμοποιεί σωματίδια φωτός με σκοπό τη μετάδοση δεδομένων από μια θέση σε μία άλλη μέσω καλωδίου οπτικών ινών. Αυτό έχει ως αποτέλεσμα, έπειτα από σύγκριση μετρήσεων των ιδιοτήτων ενός κλάσματος αυτών των φωτονίων, τα δύο τελικά σημεία να καθορίζουν ποιο είναι το πιο ασφαλές κλειδί ώστε να χρησιμοποιηθεί.

Παράδειγμα

Υποθέτουμε ότι υπάρχουν δύο άνθρωποι Α και Β , οι οποίοι θέλουν να στείλουν ένα μυστικό ο ένας στον άλλον, δίχως να μπορεί να υποκλαπεί από κάποιον. Με τη χρήση του QKD, ο Α στέλνει στον Β μία σειρά πολωμένων φωτονίων μέσω ενός καλωδίου οπτικών ινών όπως προαναφέρθηκε. Το σημαντικό κομμάτι είναι πως το καλώδιο αυτό δεν χρειάζεται να είναι στερεωμένο διότι τα φωτόνια έχουν μία τυχαιοποιημένη κβαντική κατάσταση.



Εικόνα 16. : Quantum Cryptography Explained (Πηγή: https://quantumxc.com/blog/quantum-cryptography-explained/)

Αν ένας τρίτος θελήσει να «ακούσει» ή να υποκλέψει τη συζήτηση, τότε θα πρέπει να διαβάσει κάθε φωτόνιο ώστε να το καταφέρει.

Έπειτα, θα πρέπει να δώσει το φωτόνιο στον Β. Αφού ο C διαβάσει το φωτόνιο, μεταβάλλεται η κβαντική κατάσταση του φωτονίου και αυτό έχει ως αποτέλεσμα να εισάγονται σφάλματα στο key. Έτσι προειδοποιούνται ο Α και ο Β ότι κάποιος προσπαθεί να παραβιάσει το key και το απορρίπτουν. Τέλος, αυτό που πρέπει να γίνει μετά είναι ο Α να στείλει στον Β ένα νέο κλειδί που δεν έχει εκτεθεί και έτσι να ακούσει το μυστικό.

Λόγω των qubits και των ιδιοτήτων τους να διατηρούν διαφορετικές καταστάσεις ταυτοχρόνως(0 και 1), οι κβαντικοί υπολογιστές έχουν τη δυνατότητα να εκτελούν υπολογισμούς με πολλαπλές πράξεις την ίδια στιγμή, κάτι το οποίο δεν μπορεί να κάνει ένας κλασικός υπολογιστής. Κατ' επέκταση, αυτό σημαίνει πως η κρυπτογράφηση που χρησιμοποιείται για τη ψηφιακή ασφάλεια των ανθρώπων σε ότι έχει να κάνει με τη κατηγορία των προσωπικών δεδομένων, «απειλείται».

Ένα παράδειγμα για τη κατανόηση του πώς διαχειρίζονται προβλήματα τα οποία έχουν πολλές πιθανές απαντήσεις οι κβαντικοί υπολογιστές, είναι ότι σε αντίθεση με τους κλασικούς οι οποίοι θα κάνουν πάρα πολλές προσπάθειες, μπορούν να δοκιμάσουν όλες τις πιθανές λύσεις του προβλήματος ταυτόχρονα, με αποτέλεσμα ο χρόνος που απαιτείται για να βρεθεί η λύση να μειώνεται κατά πολύ.

Αυτό το «πλεονέκτημα» των κβαντικών υπολογιστών, μπορεί να βρει εφαρμογή και να επιτεθεί στις δύο πιο γνωστές μορφές κρυπτογράφησης σήμερα, την συμμετρική και ασύμμετρή.

5.2 Συμμετρική Κρυπτογράφηση-Symmetric Encryption

Ο τρόπος που λειτουργεί η συμμετρική κρυπτογράφηση είναι χρησιμοποιώντας ένα κλειδί ώστε να κλειδώσει τα data και έπειτα ένα ίδιο κλειδί για να τα ξεκλειδώσει.

Ένας τρόπος λοιπόν, ώστε να παραβιαστεί αυτή η μέθοδος κρυπτογράφησης, είναι το να δοκιμάζονται συνεχώς πιθανά κλειδιά μέχρι να βρεθεί αυτό που ξεκλειδώνει τα data.

Οι καλοί συμμετρικοί αλγόριθμοι είναι έτσι σχεδιασμένοι, ώστε η «πλήρης επίθεση» που προαναφέρθηκε, να είναι ο πιο αποτελεσματικός τρόπος να «σπάσει» η κρυπτογράφηση.

Αυτό συμβαίνει διότι ο αριθμός των πιθανών κλειδιών είναι τόσο μεγάλος που ουσιαστικά ένας κλασικός υπολογιστής, είναι πρακτικά αδύνατον να αποκρυπτογραφήσει τα δεδομένα και κατ' επέκταση είναι μη πρακτική λύση. Αυτό συμβαίνει καθώς ο όγκος της εργασίας που απαιτείται για αυτή την «επίθεση», τη υπολογιστή ισχύ, η ενέργεια και το χρηματικό ποσό, είναι πολύ μεγάλα. Έπειτα, οι λανθασμένες απαντήσεις είναι τόσες πολλές που το καθιστά πρακτικά αδύνατο.

Κάπου εδώ, όπως προαναφέρθηκε, με τη χρήση των κβαντικών υπολογιστών αυτή όλη η ενέργεια και η εργασία που απαιτείται, μειώνεται σε τεράστιο βαθμό καθώς μπορούν να δοκιμάσουν πολλά κλειδιά ταυτόχρονα και να βρεθεί με πολύ μεγαλύτερη ευκολία, το σωστό κλειδί, χωρίς να υπάρχει αυτή η τεράστια κατανάλωση, πόρων, ενέργειας και χρημάτων που απαιτούνται από τους κλασικούς υπολογιστές.

Ένα αξιοσημείωτο παράδειγμα για τη κατανόηση της διαφοράς αυτής, είναι ότι πχ αν το μήκος του κλειδιού είναι κοντά στις 10.000 δοκιμές, με ένα κβαντικό υπολογιστή ο παράγοντας εργασίας θα μειωνόταν στα 100 πιθανά κλειδιά.

5.3 Ασύμμετρη Κρυπτογράφηση-Asymmetric Encryption

Από την άλλη πλευρά, η ασύμμετρη κρυπτογράφηση έχει να κάνει μαθηματικά. Συγκεκριμένα, με πράξεις οι οποίες μπορεί να υλοποιούνται σχετικά εύκολα, αλλά στη περίπτωση που χρειάζεται να αντιστραφούν, τότε είναι πολύ πιο δύσκολο.

Όταν γίνεται η προσπάθεια επιθέσεων σε αυτό το είδος κρυπτογράφησης, τότε ουσιαστικά προσπαθούν να επιλύσουν αυτές τις μαθηματικές πράξεις και προβλήματα. Παρόλα αυτά, όπως και στη συμμετρική κρυπτογράφηση, όταν εμπλέκονται κβαντικοί υπολογιστές στη επίλυση αυτών των προβλημάτων, τότε μειώνεται πάλι ο χρόνος, οι πόροι και οι προσπάθειες, σε πολύ σημαντικό και μεγάλο βαθμό.

Παράδειγμα

Η επίλυση του 1303x1307 είναι πολύ πιο εύκολη από το να πρέπει να ψάξουμε ποιους 2 αριθμούς πρέπει να πολλαπλασιάσουμε για να βρούμε το 1,703,021.

5.4 Μελλοντικές απειλές και αντιμετώπιση

Στα αρχικά του στάδια βρίσκεται ένα Πρόγραμμα Προτυποποίησης της Μετα-Κβαντικής Κρυπτογραφίας , το οποίο έχει αναλάβει το Ινστιτούτο Προτύπων και Τεχνολογίας(NIST) και στόχο έχει τον εντοπισμό νέων αλγορίθμων οι οποίοι έχουν την δυνατότητα να αντισταθούν στις απειλές που τίθενται από τους κβαντικούς υπολογιστές.

Μέσω αυτού του προγράμματος, ερευνητές από την IBM έχουν πάρει μέρος στην ανάπτυξη τριών κβαντοασφαλών κρυπτογραφικών αλγορίθμων οι οποίοι είναι βασισμένοι στη κρυπτογραφία πλέγματος(lattice cryptography).

Όλη η μετάβαση που γίνεται στη νέα κρυπτογραφία κάθε άλλο παρά απλή είναι και σίγουρα χρειάζεται χρόνος και επενδύσεις. Αυτό σημαίνει πως δεν μπορεί να προβλεφθεί ή να υπολογιστεί με ακρίβεια το πότε θα υφίσταται ένας κβαντικός υπολογιστής μεγάλης κλίμακας ο οποίος θα έχει τη ικανότητα να μπορεί να σπάει κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού. Το μόνο σίγουρο είναι πως υπάρχει χρόνος για την εύρεση κβαντικοασφαλών λύσεων, χωρίς αυτό να σημαίνει ότι πρέπει να εφησυχαστούμε.

Από την πλευρά τους, οι hackers πλέον έχουν την δυνατότητα συλλογής κρυπτογραφημένων δεδομένων με σκοπό να τη χρήση τους αργότερα, όταν θα έχουν την δυνατότητα να τα αποκρυπτογραφήσουν μέσω ενός κβαντικού υπολογιστή. Μάλιστα η BSI, που αποτελεί ένα γερμανικό ομοσπονδιακό οργανισμό, έχει την απαίτηση της χρήσης υβριδικών συστημάτων, κάτι που σημαίνει ότι χρησιμοποιούνται και κλασικοί και κβαντικοί υπολογιστές, με σκοπό τη προστασία σε εφαρμογές υψηλής ασφάλειας. Τέλος, ο Λευκός Οίκος είχε εκδώσει ένα υπόμνημα το οποίο έχει ως απαίτηση από τις ομοσπονδιακές υπηρεσίες να ξεκινήσουν το κβαντικό σχεδιασμό εκσυγχρονισμού.

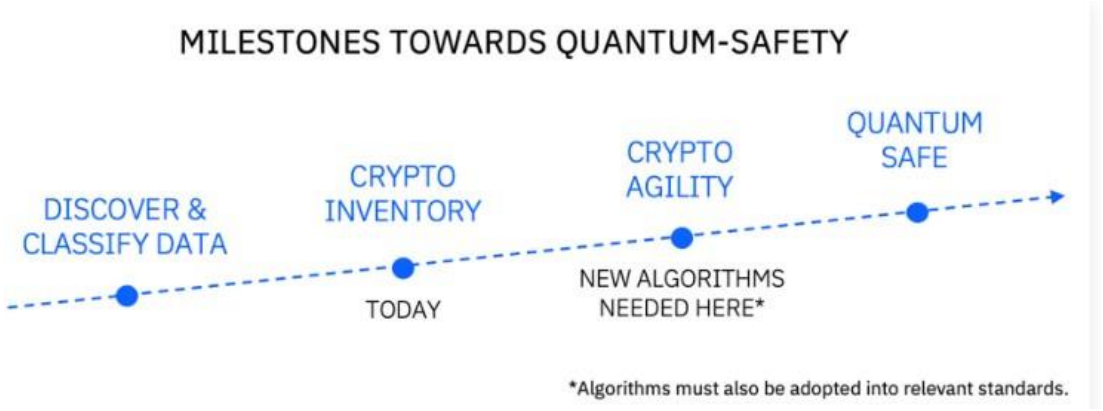
5.5 Προετοιμασία για την υιοθέτηση προτύπων ασφάλειας από την κβαντική ακτινοβολία

Αρχικά, πρέπει να γίνει ανακάλυψη και ταξινόμηση των δεδομένων, δηλαδή να ταξινομηθούν τα δεδομένα μας με βάση την αξία τους και έπειτα να κατανοηθούν οι απαιτήσεις συμμόρφωσης. Με αυτά τα πρώτα βήματα δημιουργείται ένα απόθεμα δεδομένων.

Έπειτα, πρέπει να δημιουργηθεί μία απογραφή κρυπτογράφησης. Αυτό σημαίνει πως αφότου ταξινομηθούν τα δεδομένα, είναι αναγκαίο να προσδιοριστεί ο τρόπος που θα κρυπτογραφηθούν,

όπως και άλλες χρήσεις που θα έχει η κρυπτογράφηση, ώστε να δημιουργηθεί μία απογραφή κρυπτογράφησης η οποία βοηθάει στο προγραμματισμό της μετεγκατάστασης.

Αυτή η μετάβαση από τα κλασικά στα πρότυπα κβαντικής ασφάλειας αποτελεί ένα χρονοβόρο και μεγάλο «δρόμο» και αυτό συμβαίνει γιατί υπάρχει συνεχής εξέλιξη των προτύπων. Συνεπώς, κάτι τέτοιο σημαίνει πως πρέπει να χρησιμοποιούμε πάντα ευέλικτες προσεγγίσεις για κάθε αντικατάσταση που μπορεί να προκύψει. Συνίσταται συνήθως η εφαρμογή υβριδικής προσέγγισης διότι λειτουργεί συνδυαστικά.



Εικόνα 17. : Milestones towards quantum-safety (Πηγή: https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it)

5.6 Κλάδοι που επηρεάζονται

Στο τομέα της αυτοκινητοβιομηχανίας χρησιμοποιείται η τεχνολογία δημοσίου κλειδιού(public key) σε συνδεδεμένα αυτοκίνητα για τις επικοινωνίες vehicle-to-everything(V2X). Από εδώ και στο εξής, όσα αυτοκίνητα κατασκευάζονται πλέον θα είναι σχεδιασμένα έτσι ώστε να μπορούν να υιοθετήσουν τη κβαντική ασφαλή τεχνολογία.

Αξιοσημείωτο είναι, πως όσα οχήματα έχουν περιορισμούς στους πόρους του υλικού τους, θα πρέπει οι πελάτες να δοκιμάζουν νέους αλγορίθμους κβαντικής ασφάλειας, ώστε να υπάρχει μεγαλύτερη σιγουριά στο τι μπορούν να υιοθετήσουν αργότερα.

Όσον αφορά τις τράπεζες, εδώ κυρίαρχο ρόλο αναλαμβάνει η συμμετρική κρυπτογραφία καθώς μέσω αυτής εξασφαλίζουν την εμπιστευτικότητα των δεδομένων στις τραπεζικές εφαρμογές. Υπάρχουν άτομα που προσπαθούν να υποκλέψουν τα προσωπικά δεδομένα που έχουν οι πελάτες των τραπεζών. Για αυτό το λόγο οι πελάτες έχουν ξεκινήσει να δημιουργούν δεδομένα και κρυπτο αποθέματα ώστε να υλοποιηθεί μία κβαντική-ασφαλή προστασία όσον αφορά τα ευαίσθητα δεδομένα. Επιπροσθέτως, οι τράπεζες χρησιμοποιούν και αυτές τη κρυπτογράφηση δημοσίου κλειδιού, όπως πχ στη περίπτωση των ψηφιακών υπογραφων για τη πιστοποίηση και επαλήθευση λογισμικού.

6. ΚΒΑΝΤΙΚΑ ΠΑΙΧΝΙΔΙΑ-QUANTUM GAMES

Τα κβαντικά παιχνίδια αποτελούν ένα τρόπο μέσω της ψυχαγωγίας στην εκμάθηση της κβαντικής μηχανής. Είναι σχεδιασμένα έτσι ώστε να αναπαριστούν βασικές αρχές της κβαντικής μηχανικής όπως η υπέρθεση(superposition), εμπλοκή(entanglement) και κβαντική αβεβαιότητα.

Υπάρχει μεγάλη ποικιλία κβαντικών παιχνιδιών και παρακάτω παρουσιάζονται μερικά από αυτά:

1. Hello Quantum

Το συγκεκριμένο παιχνίδι πρόκειται για παζλ, το οποίο έχει σχεδιαστεί από την IBM. Στόχο έχει την διδαχή των βασικών αρχών της κβαντικής υπολογιστικής. Οι παίκτες μαθαίνουν να ελέγχουν τα qubits και μέσα από αυτό αναπτύσσεται μία λογική αίσθηση ώστε να μπορούν να γράψουν κβαντικά προγράμματα.

Πως παίζεται;

Στόχος είναι η αλλαγή της τοποθέτησης στο χρώμα των κύκλων σε ένα πλέγμα για να ταιριάζει με ένα καθορισμένο μοτίβο. Ένα ζευγάρι από qubits συμβολίζουν το πλέγμα, ενώ αν είναι λευκό το χρώμα των κύκλων σημαίνει πως η κατάσταση είναι on και το μαύρο off, ενώ αν είναι clear συμβολίζει το τυχαίο.

Μέσω του παιχνιδιού μαθαίνουμε για τις εντολές χειρισμού qubit , τις αλληλεπιδράσεις μεταξύ τους καθώς και την αβεβαιότητα των μη μετρημένων qubits.

2. Particle in A box.

Το συγκεκριμένο παιχνίδι έχει αναπτυχθεί από το Design and Interaction Studio της Georgia Tech, με σκοπό να δείξει τη εισαγωγική Κβαντική Μηχανική με ένα πιο απλό τρόπο.

Χωρίζεται σε δύο κόσμους: την κβαντική και την κλασική μηχανική.

Στη περίπτωση του Κβαντικού κόσμου, μία λέξη η οποία μπορεί να τον χαρακτηρίσει , είναι αδιαμφισβήτητα η τυχαιότητα. Τα αντικείμενα λοιπόν, στο κβαντικό κόσμο παρουσιάζουν τυχαιότητα, σε αντίθεση με τον κλασικό κόσμο όπου οι συμπεριφορές που παρουσιάζονται είναι

τυπικές και προσδοκώμενες. Στόχος του παιχνιδιού είναι να αυξήσουμε τη ενέργεια ενός σωματιδίου και στους 2 κόσμους.

Στο κλασικό κόσμο, αυτό μπορεί να επιτευχθεί κυλώντας την ενέργεια με σκοπό να ωθήσει ένα μοχλό πιο πάνω και να πάει στο επόμενο επίπεδο. Από την άλλη, στον κβαντικό κόσμο, θα χρειαστεί να συναρμολογήσετε λαμπτήρες που έχουν το σωστό χρώμα και να βάλετε φως στο κβαντικό καλώδιο ενός ηλεκτρονίου. Έτσι, μπορείτε να αυξήσετε την ενέργεια ενός ηλεκτρονίου έως και τρία επίπεδα. Αξιοσημείωτο είναι οι σχεδιαστές του συγκεκριμένου παιχνιδιού κέρδισαν το Student's Choice Award στο Serious Showcase & Challenge το 2015.

3. PSI and Delta

Όπως και στο προηγούμενο παιχνίδι, το PSI and Delta αποτελείται από δύο μέρη.

Ο παίκτης χτίζει μοντέλα τα οποία βασίζονται στην υπέρθεση αλλά και στη πιθανότητα στο πρώτο μέρος, αλλά και στην ανάπτυξη μοντέλων στα επίπεδα ενέργειας στο δεύτερο μέρος.

Η φυσική εξηγεί πως σε ένα περιορισμένο χώρο, ένα ηλεκτρόνιο θα φτάσει σε υπέρθεση ή θα υπάρχει σε πολλά μέρη ταυτοχρόνως. Για να φτάσει αυτή η υπέρθεση στο τέλος της, ο παίκτης πρέπει να τραβήξει ένα επίπεδο ώστε να λάβει τις απαραίτητες μετρήσεις, έτσι να προκαλέσει την κατάρρευση του ηλεκτρονίου από την κατάσταση υπέρθεσης σε μία τυχαία θέση στο καλώδιο.

Έτσι, ένα συμπτυγμένο ηλεκτρόνιο αυτό που κάνει είναι ότι θα «σοκάρει» το robot ή τον παίκτη όπου στέκεται πάνω από αυτό, και προκαλώντας τους έτσι να χάσουν. Την πιθανότητα να μετρηθεί κάτω από την πλατφόρμα ένα ηλεκτρόνιο, αυξάνει το μήκος και το ύψος της καμπύλης που βρίσκεται πάνω από αυτό. Μετά από το φαινόμενο της υπέρθεσης συνεχίζεται η κάθε μέτρηση σε αυτό.

Έπειτα, το αντίπαλο robot, διαθέτει μία ασπίδα η οποία είναι ανθεκτική σε κραδασμούς και αυτό έχει ως αποτέλεσμα την απαίτηση περισσότερης ενέργειας από την πλευρά του ηλεκτρονίου, ώστε να σπάσει μέσα από αυτό.

4. Qcard

Αυτό το παιχνίδι είναι σχεδιασμένο από τη QPlayLearn, μια ομάδα που αποτελείται από επιστήμονες και επικοινωνιολόγους οι οποίοι έχουν σαν στόχο τη εκπαίδευση των ανθρώπων και την εισαγωγή τους στις βασικές αρχές της κβαντικής πληροφορικής.

Για το συγκεκριμένο παιχνίδι, χρησιμοποιείται το Qiskit της IBM και μιμείται τα κβαντική κυκλώματα. Στόχος του παιχνιδιού είναι ο παίκτης να αυξήσει τη πιθανότητα ότι το qubit γυρίσει από 0 σε 1 στο τέλος του κάθε γύρου.

5. Photonic Trail

Η QPlayLearn συνεργάστηκε με τη Quantum Flytrap και δημιούργησαν ένα παιχνίδι το οποίο ονομάζεται Photonic Trail και είναι ένα παιχνίδι κβαντικής μουσικής. Παίζεται μόνο με ένα παίκτη και σκοπός είναι το κυνήγι θησαυρού που αποτελείται από 6 αποστολές και καλύπτουν έτσι τα βασικά της κβαντικής οπτικής. Υπάρχει ένας συνδυασμός τέχνης, επιστήμης και μυθοπλασίας και έτσι διδάσκει τις θεμελιώδεις ιδέες της κβαντικής οπτικής, πως υπάρχει αλληλεπίδραση μεταξύ φωτός και ατόμων και μορίων.

Επειδή αυτό το παιχνίδι βασίζεται κυρίως στο ένστικτο, κάνει εφικτή τη πρόσβαση του σε μαθητές και της πρωτοβάθμιας και της δευτεροβάθμιας εκπαίδευσης. Με κάθε αποστολή που ολοκληρώνεται, πλησιάζουν οι παίκτες περισσότερο στη τελειοποίηση του Hilbert Spade και γίνονται "Master of Light".

6. Virtual Lab By Quantum Flytrap

Αυτό που κάνει το Quantum Flytrap είναι μέσω γραφικών διεπαφών να φέρνει κοντά τους χρήστες στις κβαντικές τεχνολογίες. Διαθέτει ένα παιχνίδι προσομοιωτή, το Virtual Lab, το οποίο σε πραγματικό χρόνο αποτελεί μία διαδικτυακή προσομοίωση ενός οπτικού πίνακα όπου υποστηρίζει μέχρι και τέσσερα μπερδεμένα φωτόνια. Χρησιμοποιεί μία λειτουργία μεταφοράς και απόθεσης ώστε να τοποθετεί οπτικά στοιχεία όπως πηγές φωτονίων και περιστροφείς Faraday.

Το virtual lab προσφέρει τη δυνατότητα διερεύνησης της φύσης της κβαντικής φυσικής όπως κατάσταση εξέλιξης, εμπλοκή και μέτρηση. Επίσης προσφέρεται η δυνατότητα χρήσης της κβαντικής κρυπτογραφίας.

Τέλος, προσφέρει ένα εύρος μεθόδων για τη διερεύνηση ενός πειράματος, των αποτελεσμάτων του και της κβαντικής κατάστασης που επικρατεί. Οι παίκτες έχουν τη δυνατότητα να εξετάσουν το πείραμα, συμπεριλαμβανομένων όλων τα δυνατοτήτων των μετρήσεων, με τη χρήση ενός πολυκάναλου εργαλείου δέντρου(multiverse tree tool). Με βάση την ερμηνεία της Κοπεγχάγης, όλοι οι κλάδοι συνδέονται με τα πιθανά αποτελέσματα και αποτελούν μία συνυπάρχουν πτυχή της κβαντικής κατάστασης, κάτι το οποίο σημαίνει πως η περίπτωση οι κόσμοι να έρθουν σε σύγκρουση, αποτελεί κάτι απίθανο.

7. Quantum Odyssey

Σχεδιάστηκε από το Quarks Interactive και αποτελεί το συνδυασμό της εμπειρίας ενός βιντεοπαιχνιδιού και μίας πολύ καλής οπτικής εκμάθησης όσον αφορά την διδασκαλία της Universal Quantum Computing. Διδάσκει κβαντική υπολογιστική μέσω μιας πλήρως οπτικής εμπειρίας.

Το παιχνίδι παίζεται ως εξής: Μία ομάδα ειδικών μέσω ενός πλοίου “Starship” το οποίο σχεδιάστηκε από τον Elon Musk, για να συλλέξει ένα εξωγήινο τεχνούργημα. Αν τα πράγματα δεν πάνε καλά, τότε η ομάδα αυτή πρέπει να μπορέσει να επιβιώσει. Αυτό που πρέπει να κάνουν είναι να δουλέψουν με ένα AI το οποίο ονομάζεται AXIOM, έτσι ώστε να μπορούν να φτιάξουν φαγητό στο διάστημα, να συμβάλλουν στην ανακάλυψη πόρων και έπειτα να βρουν τρόπο ώστε να γυρίσουν σπίτι.

8. Quantum Moves

Δημιουργήθηκε από το ScienceAtHome, μία ομάδα ερευνητών, επιστημόνων δεδομένων αλλά και προγραμματιστές παιχνιδιών, οι οποίοι στόχο έχουν να φέρουν την επανάσταση στη επιστημονική έρευνα μέσω των βιντεοπαιχνιδιών.

Το παιχνίδι αυτό προσφέρει εφαρμογή στη κβαντική έρευνα τεχνολογίας. Επίσης, σε ένα πολύ σημαντικό θέμα που αντιμετωπίζεται, αυτό της βελτιστοποίησης, οι έρευνες που έχουν διεξαχθεί έχουν δείξει ότι παράγονται λύσεις από παίκτες όπου είναι πιο αποτελεσματικές σε σύγκριση με τη τυχαία σπορά (random seeding) και μάλιστα αυτό παρατηρείται ακόμη και σε πιο περίπλοκα προβλήματα.

Μέσω του Quantum Movement , οι παίκτες έχουν την δυνατότητα της εξερεύνησης του τοπίου λύσης με μεγαλύτερη αποτελεσματικότητα και μπορούν να συλλάβουν τεχνικές λύσης όπου οι αλγόριθμοι ενδεχομένως παραβλέπουν. Αυτό δεν σημαίνει ότι οι αλγόριθμοι είναι υποδεέστεροι ως προς την αποδοτικότητά τους, αλλά ότι μπορεί οι ιδέες των ανθρώπων να λειτουργήσουν ευεργετικά ως προς το πως αποφασίζουν να επιλύσουν ένα συγκεκριμένο κβαντικό πρόβλημα. Το παιχνίδι βρίσκεται σε beta στάδιο και πολλοί πιστεύουν ότι αποτελεί ένα σημαντικό βήμα ως προς την υβριδική νοημοσύνη (hybrid intelligence).

9. Quantum Chess

Δημιουργήθηκε από τον μεταπτυχιακό φοιτητής φυσικής Chris Cantwell σε συνεργασία με το qcraft. Αποτελεί το πρώτο παιχνίδι που δημιουργήθηκε στη κορυφή μίας μηχανής κβαντικής φυσικής και ουσιαστικά δείχνει πως ένα παραδοσιακό παιχνίδι μπορεί να αναπροσαρμοστεί ώστε να αναδείξει τα κβαντικά φαινόμενα.

Στο Κβαντικό Σκάκι, τα κομμάτια δεν διατηρούν μία φυσική θέση αλλά βρίσκονται σε υπέρθεση διαφορετικών τετραγώνων στον πίνακα. Έτσι, στη περίπτωση όπου ένα κομμάτι δέχεται επίθεση, τότε λαμβάνει χώρα μία προβολική μέτρηση(projective measurement). Το στοιχείο υπέρθεση

συμβολίζεται με ένα δακτύλιο και δείχνει τη πιθανότητα που υπάρχει το κομμάτι αυτό να βρίσκεται σε ένα ορισμένα τετράγωνο.

Στη διάρκεια μετακίνησης ενός κομματιού, κάθε ενέργεια μπορεί να καθοδηγείται από πιθανότητα. Αξιοσημείωτο είναι, πως πολλοί υπολογισμοί εκτελούνται παρασκηνιακά όταν ένα κομμάτι παίρνει προτεραιότητα ώστε να καθορίσει το τελικό αποτέλεσμα, το οποίο υπάρχει περίπτωση να μη είναι προσδοκώμενο. Παρόλα αυτά, τα κινήματα υπακούουν στις βασικές αρχές και κανόνες του κλασικού σκακιού (μαζί με το ροκέ).

10. Quantum Tic-Tac-Toe

Στο συγκεκριμένο παιχνίδι, στόχος είναι η απεικόνιση της υπέρθεσης(superposition).

Οι παίκτες τοποθετούν τα κομμάτια τους σε ένα πλέγμα 3x3 και στόχος είναι να πάρουν τρείς στη σειρά όπως στο κλασικό tic tac toe. Όμως η διαφορά στο Κβαντικό παιχνίδι είναι ότι κάθε χώρος στο πλέγμα μπορεί να υφίσταται σε πολλαπλές καταστάσεις ταυτοχρόνως λόγω της υπέρθεσης και έτσι επιτρέπεται στους παίκτες να καταλαμβάνουν πολλαπλούς χώρους την ίδια στιγμή.

7. ΤΟ ΜΕΛΛΟΝ ΤΟΥ ΚΒΑΝΤΙΚΟΥ ΥΠΟΛΟΓΙΣΜΟΥ

Οι κβαντικοί υπολογιστές αποτελούν μία επανάσταση της πληροφορικής, προσφέροντας μία μεγάλη καινοτομία στη καθημερινή μας ζωή.

Η κβαντική υπολογιστική βρίσκεται πολύ κοντά στο να εμπορευματοποιηθεί στη καθημερινότητα μας. Κάτι τέτοιο θα επιφέρει ένα τεράστιο αντίκτυπο στη ζωή των ανθρώπων, καθώς πολλές αναδυόμενες τεχνολογίες θα αναπτυχθούν με πολύ μεγαλύτερη ταχύτητα, όπως οι μπαταρίες EV, η βιοτεχνολογία και η τεχνητή νοημοσύνη.

Η IBM προχώρησε σε ανακοίνωση της κατασκευής ενός νέου κβαντικού υπολογιστή με όνομα Os-prey, ο οποίος αποτελείται από 433 qubits και είναι τριπλάσια από τα στοιχεία επεξεργασίας δεδομένων συγκριτικά με τον περσινό. Έπειτα, η IBM ανακοίνωσε ότι υπάρχουν βελτιώσεις σε σχέση με παλαιότερες εκδόσεις ενός παλαιότερου υπολογιστή, του Eagle.

Χάρη στη Κβαντική Πληροφορική, θα υπάρξει γρηγορότερη επεξεργασία σε τεράστιους όγκους δεδομένων, μία πολύ καλύτερη και ουσιαστική προσέγγιση στη μηχανική μάθηση αλλά θα επιτραπούν και προσομοιώσεις όπου σήμερα μοιάζουν μακρινές. Θα υπάρξει πρόοδος στη γονιδιωματική, τη διαχείριση ασθενειών και στις τεχνολογίες ανανεώσιμων πηγών ενέργεια, δηλαδή μια συνολική αναμόρφωση στον κόσμο γύρω μας.

7.1 Τι θα συμβεί στο μέλλον της κβαντικής υπολογιστικής;

Κάποια από τα προβλήματα όπου οι κβαντικοί υπολογιστές θα είχαν τη δυνατότητά να χρησιμοποιηθούν, έχουν να κάνουν με τη πρόβλεψη της ροής κυκλοφορίας σύνθετα αστικά περιβάλλοντα καθώς και στη επεξεργασία από πολύ μεγάλή ποσότητα δεδομένων που έχουν να κάνουν με τη τεχνητή νοημοσύνη και στη μηχανική μάθηση. Επίσης, φαίνεται ότι αν πότε η ανθρωπότητα φτάσει στην υλοποίηση ενός πολύπλοκου βιολογικού εγκεφάλου, αυτό σίγουρα θα είναι μέσω της κβαντική υπολογιστικής.

Ο Gasman αναφέρει:
«*Το συναρπαστικό για μένα είναι οι καινοτομίες που είναι πιθανό να συμβούν. Για να αναμείξουμε μεταφορές, ο κόσμος είναι το στρείδι της κβαντικής υπολογιστικής. Υπάρχουν πολλοί καλοί λόγοι ν α βρίσκεσαι στους κλασσικούς υπολογιστές, αλλά αν ψάχνεις για μαζικές καινοτομίες δεν πρόκειτα ι να συμβεί. Αυτός είναι ο ενθουσιασμός των κβαντικών υπολογιστών.*»

7.2 Πώς θα αλλάξει η κβαντική υπολογιστική την τεχνητή νοημοσύνη;

Λόγω της πολύ μεγάλης εξέλιξης που έχει η τεχνητή νοημοσύνη τα τελευταία χρόνια, υπάρχει πλέον η δυνατότητα δημιουργίας ρεαλιστικών 3D εικόνων αλλά και βίντεο. Επίσης, η κβαντική πληροφορική έχει αρχίσει να εμπλέκεται ενεργά στη τεχνητή νοημοσύνη και αυτό έχει πυροδοτήσει τη αφορμή για τη κβαντική τεχνητή νοημοσύνη. Κάτι τέτοιο εγκυμονεί πολλά πλεονεκτήματα, καθώς θα υπάρχει η δυνατότητα χειρισμού πολύ μεγάλων συνόλων δεδομένων με πολλή περισσότερη αποτελεσματικότητα αλλά και ταχύτητα. Επιπλέον, θα μπορεί να αναγνωρίσει μοτίβα που είναι δύσκολο να αναγνωριστούν από τους κλασικούς υπολογιστές. Τέλος, θα μπορεί να κάνει συνδυασμό και αναδιοργάνωση υπάρχουν ιδεών, δηλαδή να δημιουργεί νέες ιδέες με τρόπους όπου ο κάθε άνθρωπος είναι αδύνατο να φανταστεί ότι υπάρχουν.

7.3 Πότε Θα Έρθει Η Κβαντική Υπολογιστική;

Υπολογίζεται ότι τομείς όπως η οικονομία θα αρχίσουν να έχουν κέρδη από τη Κβαντική Πληροφορική έως το 2025 και με τη σειρά τους θα ακολουθήσουν και άλλες βιομηχανίες λόγω της προσβασιμότητας που θα αποκτηθεί μέσω cloud.

Η McKinsey & Company έχει πραγματοποιήσει κάποιες προβλέψεις σχετικά με την άφιξη της κβαντικής υπολογιστικής και το ρεαλιστικό σενάριο λέει πως αναμένεται τουλάχιστον σε 10 χρόνια να υπάρξει μαζική υιοθέτηση. Οι εκτιμήσεις αναφέρουν ότι θα μπορούσαν να υπάρχουν από 2000 έως 5000 κβαντικού υπολογιστές στο κόσμο εν έτει 2030.

Παρόλα αυτά, τα εργαλεία που απαιτούνται για να αντιμετωπιστούν επιχειρησιακά θέματα, υπολογίζεται ότι θα υπάρχουν το 2035, λόγω των πολλών κομματιών του υλικού λογισμικού που απαιτείται για τη δημιουργία τους. Αξιοσημείωτο είναι πως ο κλάδος των οικονομικών θα υποστεί το μεγαλύτερο όφελος.

Η χρηματοδότηση των start-up εταιρειών είχε ως βασικό στόχο τις κβαντικές τεχνολογίες με πάνω από 1.4 δις δολάρια από το 2020 στο 2021. Υπολογίζεται ότι ο Κβαντικός Υπολογισμός έχει τη δυνατότητα να πάρει αξία πάνω από 700 δις δολάρια από το έτος 2035, και μάλιστα να ξεπεράσει τα 90 δις δολάρια έως το 2040. Με βάση αυτό, οι πιο ισχυροί κβαντικοί υπολογιστές θα ήταν πολύ πιθανό να θέσουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο.

7.4 Προβλέψεις για το μέλλον της τεχνητής νοημοσύνης με κβαντική πληροφορική

Ένα εμπόδιο που προβλέπεται ότι θα μπορέσει να ξεπεράσει η τεχνητή νοημοσύνη χάρη στη κβαντική πληροφορική, είναι το γλωσσικό. Τα μοντέλα της τεχνητής νοημοσύνης θα μπορούν να κατανοήσουν μία γλώσσα που χρησιμοποιούν ώστε να εκπαιδευτούν. Άρα, αυτό υποδηλώνει ότι θα πρέπει να διδαχθεί από τη αρχή η εκάστοτε γλώσσα. Κάπου εδώ έρχεται η κβαντική πληροφορική και ξεπερνάει αυτό το εμπόδιο, προσφέροντας εκπαίδευση των μοντέλων σε μία γλώσσα και μετάφρασή της σε μία άλλη γλώσσα χωρίς κόπο.

Αυτό θα επιτρέπει στη τεχνητή νοημοσύνη, την κατανόηση και ερμηνεία διαφορετικών γλωσσών ταυτοχρόνως. Ακόμη μία πρόβλεψη είναι η δυνατότητα δημιουργίας μοντέλων με αρκετά ακριβείς δεξιότητες λήψης αποφάσεων. Αυτό σημαίνει πως θα λαμβάνονται ακριβείς αποφάσεις, οι οποίες θα διαδραματίζουν σημαντικό ρόλο, ιδιαιτέρως στα οικονομικά μοντέλα, τα οποία έχουν συνήθως υψηλό ποσοστό ανακρίβειας, λόγω των περιορισμένων δεδομένων που χρησιμοποιούνται για τη κατάρτισή τους.

Συμπερασματικά, οι δυνατότητες που προσφέρουν οι κβαντικοί υπολογιστές είναι απεριόριστες και σε συνδυασμό με την τεχνητή νοημοσύνη η τεχνολογία που θα παραχθεί θα είναι πολύ ισχυρή. Κάτι τέτοιο θα επιτρέψει στις μηχανές να εξελίσσονται από μόνες τους και θα καταστήσει την επίλυση πολύ σύνθετων προβλημάτων πολύ πιο εύκολη, όπως και την ανάπτυξη των αλγορίθμων αυτό-μάθησης (self-learning) οι οποίοι βοηθάνε στη χρηματοδότηση και την υγειονομική περίθαλψη.

Τέλος, αυτό που πρέπει οπωσδήποτε να λάβουν όλοι οι άνθρωποι υπόψη τους, είναι ότι εφόσον θα υπάρχει αυτή η αλληλεπίδραση της τεχνητής νοημοσύνης και των κβαντικών υπολογιστών με τους ανθρώπους στο μέλλον, θα πρέπει να υπάρχει ενημέρωση ώστε να είμαστε προετοιμασμένη για τις αλλαγές που ενδεχομένως θα επέλθουν και έτσι να μπορούμε να τις αξιοποιήσουμε σωστά.

ΣΥΜΠΕΡΑΣΜΑΤΑ-CONCLUSION

Συνοψίζοντας, η Κβαντική Υπολογιστική δεν αποτελεί απλώς μια εξέλιξη, αλλά μία **επανάσταση** της πληροφορικής παγκοσμίως. Ο τρόπος που μεγαλώνει και εξελίσσεται είναι εκθετικός σε σχέση με τους κλασικούς υπολογιστές του σήμερα. Παρόλα αυτά, ακόμη βρίσκονται σε πρώιμο στάδιο και υπάρχουν πολλά ζητήματα που πρέπει να προβλεφθούν και να ξεπεραστούν, με κύριο το να αναπτυχθεί ανθεκτικό και σταθερό κβαντικό υλικό καθώς και το θέμα της αξιοπιστίας στον τομέα της επίλυσης προβλημάτων και της εξάλειψης σφαλμάτων.

Αφότου ξεπεραστούν αυτά τα εμπόδια και κατανοηθούν οι συνέπειες της κβαντικής υπολογιστικής σε σημαντικούς τομείς της κοινωνίας όπως στη κρυπτογραφία, τότε θα βρισκόμαστε στο σημείο που πρέπει ώστε να εκμεταλλευτούμε και να επωφεληθούμε σε μεγάλο βαθμό από τις δυνατότητες της κβαντικής υπολογιστικής.

Εν κατακλείδι, οι δυνατότητες της κβαντικής υπολογιστής είναι πέρα από τα σύνορα που έχουν οριοθετηθεί στη μέχρι τώρα πληροφορική και πρέπει να με προσοχή να τη διαχειριστούμε και να αποκομίσουμε όλα τα οφέλη και τις δυνατότητες που μας προσφέρει, αλλάζοντας έτσι τον κόσμο, προς το καλύτερο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Microsoft, “Quantum Computing History and Background”, url: https://docs.microsoft.com/en-us/azure/quantum/concepts-overview, Αύγουστος 2022.

[2] Q-munity, “History of Quantum Computing”, url: https://www.qmunity.tech/post/history-of-quantum-computing-simplified, Αύγουστος 2022.

[3] Britannica, “Quantum Computer”, url: https://www.britannica.com/technology/quantum-computer, Αύγουστος 2022.

[4] Medium, “A brief History of Quantum Computing”, url: https://medium.com/@markus.c.braun/a-brief-history-of-quantum-computing-a5babea5d0bd, Αύγουστος 2022.

[5] Forbes, “27 Milestones In The History Of Quantum Computing”, url: https://www.forbes.com/sites/gilpress/2021/05/18/27-milestones-in-the-history-of-quantum-computing/, Αύγουστος 2022.

[6] Wikipedia, “Qiskit”, url: https://en.wikipedia.org/wiki/Qiskit, Σεπτέμβριος 2022.

[7] Ml2quantum,”Pyquil”, url: https://ml2quantum.com/pyquil/, Σεπτέμβριος 2022.

[8] Github, “Pyquil”, url: https://github.com/rigetti/pyquil, Σεπτέμβριος 2022.

[9] Medium, “Exploring quantum computing with Rigetti & pyQuil”, url: https://medium.com/swlh/exploring-quantum-computing-with-rigetti-pyquil-mid-2020-edition-70b28f917670, Νοέμβριος 2022.

[10] Ιωάννης Καραφυλλίδης, «Κβαντική Υπολογιστική», Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών,2015, Νοέμβριος 2022.

[11] Microsoft, “Dirac Notation”, url: https://learn.microsoft.com/en-us/azure/quantum/concepts-dirac-notation, Νοέμβριος 2022.

[12] Quantum Inspire, “What is a qubit”, url: https://www.quantum-inspire.com/kbase/what-is-a-qubit/, Δεκέμβριος 2022.

[13] Microsoft, “Qubit explained”, url: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit/#qubit-vs-bit, Δεκέμβριος 2022.

[14] Towardsdatascience “Demystifying Quantum Gates”, url: https://towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640, Δεκέμβριος 2022.

[15] Quantum-Inspire, “Swap Gate”, url: https://www.quantum-inspire.com/kbase/swap/, Δεκέμβριος 2022.

[16] IBM, “What Is Quantum-Safe Cryptography”, url: https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it?fbclid=IwAR3_PZtTVUVkMhk5nw9altHl7Acq4zo7qejrgRl8LvP9YNZASJPIboshvE0, Ιανουάριος 2023.

[17] Quantum Zeitgeist, “10 Quantum Games”, url: https://quantumzeitgeist.com/10-quantum-games-that-can-help-you-learn-the-field-of-quantum-computing/, Ιανουάριος 2023.

[18] Nasdaq, “What Is Quantum Computing and How Will It Transform the Future?”, url: https://www.nasdaq.com/articles/what-is-quantum-computing-and-how-will-it-transform-the-future, Ιανουάριος 2023.

[19] Forbes, “Quantum Computing Now And In The Future: Explanation, Applications, And Problems”, url: https://www.forbes.com/sites/bernardmarr/2022/08/26/quantum-computing-now-and-in-the-future-explanation-applications-and-problems/?sh=15e16dc71a6b, φεβρουάριος 2023.

[20] Readwrite, “What Quantum Computing Will Mean for the Future Artificial Intelligence”, url: https://readwrite.com/what-quantum-computing-will-mean-for-the-future-artificial-intelligence/, Φεβρουάριος 2023.

[21] gmo-research, “Future is Quantum Computing”, url: https://gmo-research.com/news-events/articles/future-quantum-computing, Φεβρουάριος 2023.

[22] Cryptomathic, “When Will Quantum Computing Arrive and How Will It Impact Cybersecurity?”, url: https://www.cryptomathic.com/news-events/blog/when-will-quantum-computing-arrive-and-how-will-it-impact-cybersecurity, Φεβρουάριος 2023.

[23] Internet Society, “Fact Sheet: Quantum Physics and Computing”, url: https://www.internetsociety.org/resources/doc/2020/does-quantum-computing-put-our-digital-security-at-risk/?gclid=CjwKCAiAzp6eBhByEiwA_gGq5FBeAhbs_FlMNdiQKgfG-3ookO5ZjQOeRaW-tBvC2IPslASJnqlSJFBoCpSkQAvD_BwE, Φεβρουάριος 2023.