

UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I INXHINIERISË ELEKTRIKE DHE KOMPJUTERIKE

PROGRAMI: INXHINIERI KOMPJUTERIKE



PUNIM DIPLOME

**KRIPTOGRAFIA E SFIDUAR NGA KOMPJUTERËT
KUANTIK**

Mentori:

Prof. Dr. Blerim Rexha

Kandidati:

Nehar Jashari

Prishtinë, Janar 2022

Falenderime

Falenderoj familjen time për përkrahjen dhe motivimin e vazhdueshëm. Falenderoj babain për shembullin e dhënë se si të jem i suksesshëm në jetë dhe studime. Falënderim i veçantë për Prof. Dr.Blerim Rexha për durimin e tij, ndihmën dhe këshillimet gjatë gjithë studimeve të mia, gjithashtu e falenderoj në emër të të gjithë studentëve të Inxhinierisë Kompjuterike për vullnetin e pakufishëm që të jetë në krahun tonë.

Abstrakti

Digjitalizimi nuk ka kufi, si rrjedhojë e saj edhe nevojat për revolucione të mëdha në këtë fushë. Një nga termat më aktuale në botën teknologjike tani është Quantum Computing. Duke zgjidhur problemet më misterioze në botën e fizikës kuantike, tashmë duket se ka ardhur koha që ato mësimet të përdoren në vazhdimin e zhvillimin teknologjik të botës njerëzore. Tashmë ekzistojnë shumë mite e legjenda për kompjuterët kuantik, për fuqinë e madhe të tyre si dhe shkencën themelore me të cilën funksionojnë ata. Kjo ka krijuar një ndjenjë kurioziteti dhe po ashtu frike në komunitetet tona. Çka është realiteti i këtyre kompjuterëve, si funksionojnë ata, dhe cilat janë mundësitë e përdorimit të tyre? Këto janë disa nga pyetjet që ky punim do të mundohet ti shtjellojë dhe të hedhi dritë mbi to. Gjatë punës sime në këtë punim kam zbuluar fuqinë e madhe të kësaj teknologjie, duke filluar me gjenerimin e numrave të vërtetë random dhe duke përfunduar me faktorizimin e numrave prime duke përdorur algoritmin e Shor-it, algoritëm i cili thyen algoritmin e enkriptimit të të dhënave RSA.

Abstract

Digitalization has no limits, as a result of which a never ending need for great revolutions in this field. One of the most current terms in the tech world right now is Quantum Computing. By solving the most mysterious problems in quantum physics world, it now seems that the time has come for those lessons to be used in the continuation of the technological development of the human world. There are already many myths and legends about quantum computers, about their great potencial and the fundamental science they're build with. This has created a sense of curiosity and also fear in our communities. What is the reality of these computers, how do they work, and what are the possibilities of using them? These are some of the questions that this paper will try to elaborate and shed light upon. During my work in this paper I have discovered the great power of this technology, starting with generating real random numbers and ending with the factorization of prime numbers using Shor's algorithm, an algorithm which promises to crack RSA encryption.

Përmbajtja

Abstrakti	3
Përmbajtja	5
Lista e Figurave	6
Lista e shkurtesave	7
Lista e pjesëve të kodit	7
1. Hyrje	8
1.1. Hyrje	8
1.2. Motivimi	8
1.3. Përshkrimi i problemit	9
2. Gjendja e tanishme	11
3. Quantum Computing	13
3.1. Quantum Properties	15
3.1.1. Quantum Superposition	15
3.1.2. Quantum Entanglement	16
3.2. Qubit	18
3.3. Quantum Computation	19
3.3.1. Ruajtja dhe marrja e informacionit	19
3.3.2. The Big Picture	20
4. Quantum Cryptography	23
4.1. Quantum Key Distribution	24
4.2. Quantum Encryption	26
4.3. Quantum-Safe Cryptography	27
4.5. Pse kriptografia kuantike është e rëndësishme?	28
6. Rasti i studimit – Programimi i kompjuterëve kuantik	29
6.1. Metodologjia dhe veglat e përdorura	29
6.2. Ndërtimi i një qarku të thjeshtë kuantik	31
6.3. Gjenerimi i numrave vërtet të rastësishëm - Shembulli i Monedhës	33
6.4. Cracking RSA ëith Shor's Algorithm	35
7. Diskutime dhe Konkluzione	39
7.1. Reflektimi kritik	39
7.2. Përmisimet e mundshme	40
Bibliografia dhe referencat	41

Lista e Figurave

Figura 1. Rritja eksponenciale [4].....	9
Figura 2. Faktorizimi i numrave të mëdhen, dallimi në mes kompjuterëve klasik dhe kuantik [5].....	10
Figura 3. Algoritmi i Shor-it [5].....	10
Figura 4. IBM Q System One [7].....	12
Figura 5. Tranzistorët klasik NPN dhe PNP [1].....	13
Figura 6. Ligji i Moore-it [8]	14
Figura 7. Vetitë e grimcave kuantike njëkohësisht si valë dhe si grimca [10].....	16
Figura 8. Opinioni i Albert Einstein për vetitë kuantike të grimcave [11].....	17
Figura 9. Vetia e grimcave kuantike e quajtur Quantum Entanglement [12]	17
Figura 10. Dallimi në mes bitëve klasik dhe kuantik [13]	18
Figura 11. Dekoherenca Kuantike [15].....	20
Figura 12. Arkitektura e propozuar për kompjuterët kuantik [17].....	21
Figura 13. Quantum Key Distribution Process [19]	25
Figura 14. Procesi i enkriptimit kuantik [20].....	26
Figura 15. Lista e certifikatave kuantike [19]	27
Figura 16. Portat logjike kuantike [10].	30
Figura 17. Procesi i simulimit të programeve kuantike përmes IBM Research Programme [21]	31
Figura 18. Hadamard Gate [21]	32
Figura 19. CNOT Gate [21].....	32
Figura 20. Rezultati i qarkut kuantik të koduar në Python	33
Figura 21. Rezultati i programit të hedhjes së monedhës në Python	35
Figura 22. Rezultatet e eksperimentit të faktorizimit të numrit $N=15$	38
Figura 23. Koha e faktorizimit me rritjen e inputit, dallimi në mes të algoritmit klasik dhe atij të Shor-it [25].....	39

Lista e shkurtesave

IT	Information Technology
ALU	Arithmetic Logic Unit
CPU	Central Processing Unit
QKD	Quantum Key Distribution
PKI	Public key infrastructure

Lista e pjesëve të kodit

Kodi 1. Inicializimi i librarive dhe krijimi i regjistrave të kubitëve dhe bitëve	32
Kodi 2. Ndërtimi i qarkut kuantik dhe ruajtja e tij në një variabël	33
Kodi 3. Procesimi i Qubits përmes portave Hadamard dhe CNOT	33
Kodi 4. Printimi i qarkut kuantik	33
Kodi 5. Instalimi i librarisë qiski dhe përdorimi i saj për të ndërtuar qarkun kuantik	34
Kodi 6. Pjesa e kodit të eksperimentit me monedhë përmes kompjuterëve kuantik.....	34
Kodi 7. Importimi i librarive të Python për zhvillimin e eksperimentit të dekriptimit të RSA	35
Kodi 8. Implementimi i gjetjes së periodës nga Peter Shor	36
Kodi 9. Implementimi i Transformimit Furie Kuantik në Python	36
Kodi 10. Ndërtimi final i algoritmit të Shor-it	37
Kodi 11. Pjesa e kodit për faktorizimin e numrit $N=15$	38

Hyrje

1.1. Hyrje

Ndryshimet teknologjike që nga vitet 60-ta kanë pasë rritje eksponenciale, duke lejuar kompjuterët që të bëhen gjithnjë e më të vogël, por ky zhvillim së shpejti do të mbërrij limitet e veta fizike. Madhësia e disa pjesëve kompjuterike është duke ju afruar madhësisë së atomit dhe kjo paraqet një problem të ri për zhvillimin e kompjuterëve akoma më të fuqishëm [1].

Duke iu afruar madhësisë së atomit ne jemi duke hyrë në botën e fizikës kuantike. Në këtë botë nuk vlejnë të njëjtat ligje fizike që janë shfrytëzuar deri tani nga kompjuterët tradicional. Në fizikën kuantike nuk mund të kontrollojmë rrjedhën e elektroneve siq bëjmë me transistorë sepse elektroni mund të kalojë ato barriera shumë më lehtë. Si rrjedhojë e kësaj ka ardhur koha e zhvillimit të Kompjuterëve Kuantik. Megjithatë fushë shumë e re në botën e sotme, deri më tani ka pasur me mijëra studime dhe miliona investime për zhvillimin e këtyre kompjuterëve. Tërë ky potencial i Kompjuterëve Kuantik ka bërë që edhe kompjuterët më të fuqishëm të zhvilluar deri më tani të fillojnë të quhen nga komuniteti shkencorë si Kompjuterë “Klasik”.

Ky punim, do të tentojë të shpjegojë këtë fushë të re në botën teknologjike e aq më shumë e re në komunitetin tonë universitar. Në këtë punim unë do të shqyrtoj se si punojnë këta kompjuterë dhe cilat janë bazat që këta kompjuterë mbështeten. Në pjesën e parë të punimit do të shfrytëzoj mundësinë për të shpjeguar më hollësisht se çka janë kompjuterët kuantik, çfarë ligje fizike vlejnë për ta, cilat janë vetitë e tyre, si dhe pse janë të nevojshëm ata. Në pjesën e dytë të punimit do të fokusohem në një nga trajtimet më të rëndësishme të kompjuterëve kuantik e cila është kriptografia kuantike. Ku do të hedhim dritë në implementimin e kompjuterëve kuantik në një ndër fushat më të rëndësishme të teknologjisë informative. Në kapitullin kryesorë do të ndaj disa eksperimente dhe punime të bëra nga unë duke programuar në këta kompjuterë. Do të shohim si mund të zhvillojmë shtresat abstrakte në ta dhe të programojmë duke përdorur logjikën e njëjtë të gjuhëve programuse të përdorura deri më tani. Në fund do të diskutoj gjetjet e mia se si do të ndikojë ky lloj i ri i zhvillimit të kompjuterëve në botën teknologjike, cilat janë nevojat, premisat si dhe mundësitë e saj.

1.2. Motivimi

Duke parë se sa shumë mendime ekzistojnë për këtë teknologji por jo dhe aq opinione të sakta apo bazuara në punime shkencore, vërehet se mungojnë informacione të sakta në komunitetin tonë lokal deri më tani për këtë teknologji. Si rrjedhojë e kësaj paraqitet një nevojë për kuptimin e kësaj teknologjie, të kuptojmë se si do të ndikojë ky zhvillim në jetët tona, çfarë duhet të dimë ne si komunitet i teknologjisë informative dhe cili është realiteti i kësaj teknologjie.

Kompjuterët kuantik mbështeten në parimet dhe vetitë kuantike cilat bëjnë të gjithë ndryshimin në aftësinë e tyre për të zgjidhur probleme në dukje të pakapërcyeshme. Duke përdorur këto veti kuantike kompjuterët kuantik janë jashtëzakonisht superiorë ndaj kompjuterëve klasik. Në rastin më të thjeshtë për kërkimin e bazave së të dhënave, një kompjuter normal mund t'i duhet të testojë çdo një nga hyrjet e tij. Algoritmet e kompjuterëve kuantikë kanë nevojë vetëm për rrënjën katrore të asaj kohe, e cila për bazat e të dhënave të mëdha, është një ndryshim i madh. Falë vetive kuantik si superposition dhe entanglement, një kompjuter kuantik mund të përpunojë një numër të madh llogaritjesh në të njëjtën kohë.

Motivimi im do të ishte testimi i secilës teknologji të re dhe aq më shumë një teknologji me aq potencial siç është Quantum Computing, të provoj se çka mund të ndërtojmë duke përdorur parimet e saj dhe të shikoj

se cili është realiteti i kësaj teknologjie. Misioni tjetër i këtij punimi është gjithashtu motivimi i studentëve që të interesohen më shumë për këtë temë. Të kuptojnë se si mund të inkuadrohen në këtë rreth inovacioni, çfarë mund të ofrojnë ata për komunitetin, si dhe a mund të hecin në karrierën e tyre duke ndjekur këtë fushë. Mundësia e ndjekjes së lëmive të reja teknologjike në botën e sotme për ne është shumë më e lehtë se sa i prindërve tanë dhe inkuadrimi jonë në këtë botë nuk ka qenë kurrë më i mundur.

1.3. Përshkrimi i problemit

Pavarësisht sukseseve të mëdha të botës teknologjike dhe revolucionit digjital, ka një mori problemesh llogaritëse të mëdha të cilat kompjuterët klasikë nuk duket se do të mund t'i zgjidhin. Megjithatë kompjuterët konvencionalë kanë dyfishuar fuqinë dhe shpejtësinë e përpunimit pothuajse çdo dy vjet për dekada me rradhë, ata ende nuk duket se po i afrohen zgjidhjes së këtyre problemeve të vazhdueshme [2].

Kjo ngecje e zgjidhjeve të këtyre problemeve të mëdha mund të pengojnë përparimet kryesore shkencore, madje edhe ekonominë globale në të ardhmen. Për të kuptuar ngecjen e kompjuterëve klasik, le të marrim si shembull “thembrën e Akilit” të tyre: gjetja e prime factors për numra të plotë shumë të mëdhenj [3]. Gjetja e prime factors të një numri është një funksion që ka rritje eksponenciale, do të thotë kompleksiteti i algoritmit është $O(2^n)$. Rritja eksponenciale është një funksion matematikorë që tregon rritje më të mprehta me kalimin e kohës, funksioni fillon relativisht ngadalë, por së shpejti arrin deri në numra që asnjë kompjuter klasik nuk do të jetë në gjendje t'i llogarisë me madhësi të dhënash mjaft të mëdha [4].

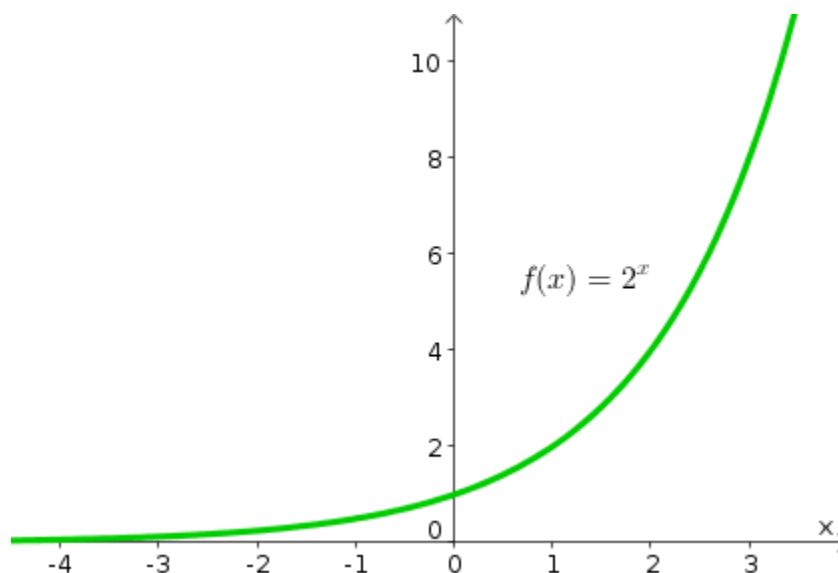


Figura 1. Rritja eksponenciale [4]

Ky proces në dukje i thjeshtë, qëndron në zemër të ekonomisë dixhitale dhe është baza për algoritmet tona më të sigurta të enkriptimit të të dhënave. Arsyeja pse e përdorim këtë teknikë në enkriptim është sepse duke u bërë numrat e përdorur në faktorizimin prim gjithnjë e më të mëdhenj, bëhet gjithnjë e më vështirë për kompjuterët konvencionalë që t'i faktorizojnë ato. Në problemin e faktorizimit të numrave prim bazohet dhe algoritmi i famshëm i enkriptimit të të dhënave RSA, i cili përbën një nga algoritmet më të rëndësishme prej të cilës bazohet shumica e kriptografisë moderne.

Në vitin 1994, një matematikan nga Instituti i Teknologjisë i Massachusetts (MIT) Peter Shor, i cili punonte në AT&T në atë kohë, zbuloi se nëse një kompjuter kuantik plotësisht funksional ishte i disponueshëm, ai mund të faktorizonte lehtësisht numra të mëdhenj në kohë sekondash [5].

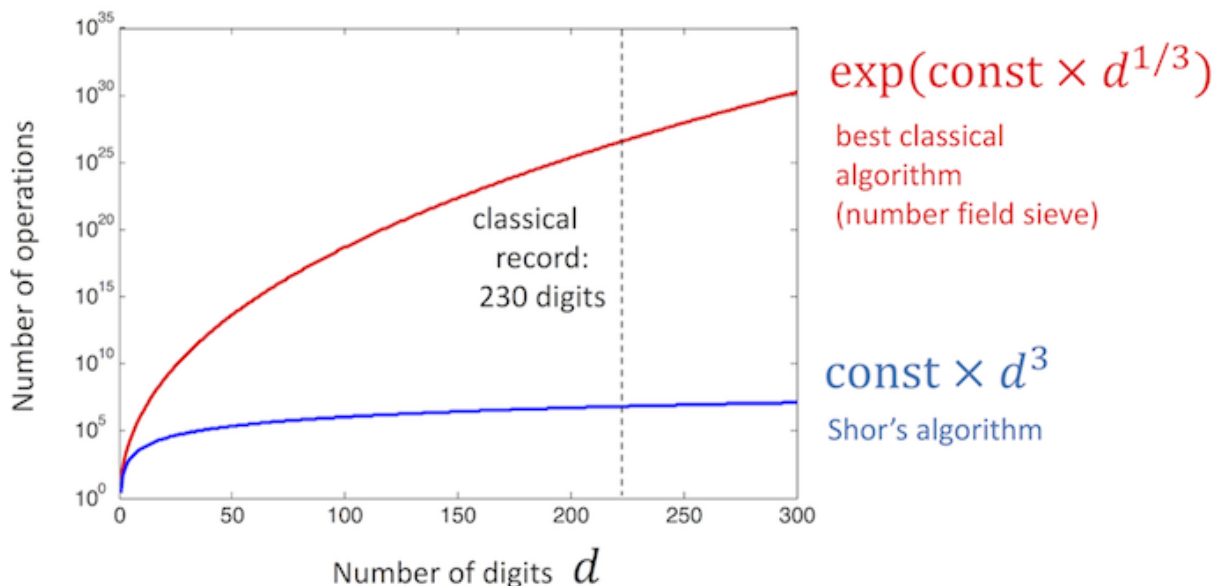


Figura 2. Faktorizimi i numrave të mëdhenj, dallimi në mes kompjuterëve klasik dhe kuantik [5]

Algoritmi i shkencëtarit të famshëm Peter Shor është arritur që të modelohet edhe duke përdorur strukturën e portave logjike në kompjuterët kuantik dhe përbën një prej algoritmeve më me potencial në kompjuterikën kuantike.

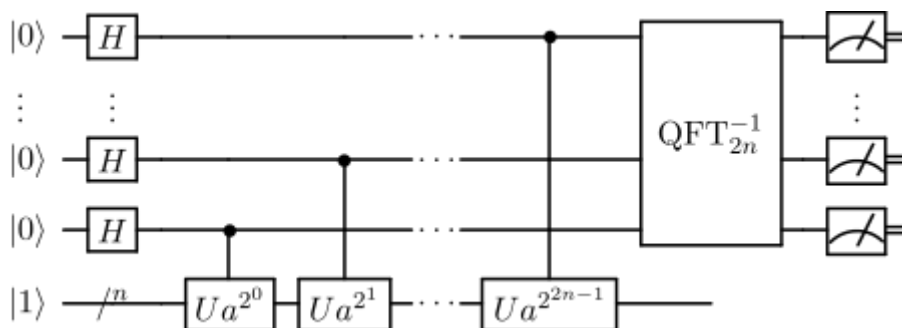


Figura 3. Algoritmi i Shor-it [5]

Përmes këtij algoritmi kompjuterët kuantikë mund të shkatërrojnë sigurinë e IT-së pasi që përmes tij edhe enkriptimi RSA mund të thyhet [6]. Kjo paraqet një rrezik të madh për kriptografinë moderne sepse ljo do të sillte probleme të reja për botën teknologjike. Kjo është një ndër problemet që do të shtjellohen në këtë temë, përveç zgjidhjes së faktorizimit të numrave prime do të shohim se si do të mund të mbroheshim nga kjo.

2. Gjendja e tanishme

Kompjuterët kuantikë na ofrojnë një perspektivë të shkëlqyeshme por ka edhe shumë zhurmë të rreme rreth tyre. Kjo zhurmë është e natyrshme duke pasur parasysh se çdo e re në teknologji sjell edhe një sasi të konsiderueshme të trillimeve shkencore. Realiteti qëndron se Kompjuterët kuantikë janë këtu për të zgjidhur disa probleme më të mëdha, probleme që kërkojnë fuqi dhe hapësirë jashtëzakonisht të madhe llogaritëse, si p.sh., gjetja e faktorëve të numrave prim shumë të mëdhenj, simulimi i molekulave, simulimi i fenomeneve kuantike, etj.

Për momentin pjesa më e madhe e kërkimit të informatikës kuantike është përqendruar në thyerjen e kriptografisë, për shkak të implikimeve të saj. Kjo është për arsye të algoritmit të Shor, por është joreale të pritet që kompjuterët kuantikë të thyejnë kriptografinë në të ardhmen e afërt pasi na duhen mijëra kubit për të thyer kriptografinë moderne, dhe numri i tanishëm i tyre është vetëm dyshifrorë [7]. Me kalimin e kohës janë shfaqur edhe shumë ide për aplikacione të reja për kompjuterët kuantikë, duke filluar nga interneti kuantik deri te simulimi i sistemeve mekanike kuantike, të cilat mund të çojnë në formimin e materialeve të reja që mund të përdoren për të luftuar kancerin, për të bërë nano-grimca, për të bërë materiale superpërçuese, etj. Megjithatë kriptografia kuantike po shfaqet si një nga fushat më të avancuara në aplikimet e efekteve kuantike deri tani.

Me investime miliardshe nga gjigande teknologjik si IBM, Google dhe Microsoft, shkencëtarët kryesorë eksperimentalë të kompjuterave në botë janë ende duke luftuar për të ndërtuar një "çip" kompjuteri kuantik me më shumë se një grusht kubitësh. Vetëm për t'ju dhënë një kuptim se sa herët jemi në historinë e informatikës kuantike, një revolucion që u cilësua ishte nga IBM, që zbuloi së fundmi kompjuterin kuantik më të madh në botë me vetëm 50 kubit [7]. Tani për tani, pothuajse çdo kompjuter kuantik është një projekt me shuma miliona dollarësh. Në përgjithësi i gjeni në departamentet e R&D (Research and Development) në kompanitë e mëdha të IT si IBM, Google, Microsoft ose në krahun e fizikës eksperimentale të universiteteve të mëdha kërkimore si MIT.

Arsyeja kryesore që kompjuterët kuantikë nuk janë përhapur ende është se mendjet dhe shpikësit më të mirë në botë janë ende duke luftuar me shkalla të larta gabimi dhe numër të ulët të kubitëve. Problem që normalisht do të merr vite dhe investime më të mëdha për zgjidhjen e tyre. Kjo i bën këta kompjuterë që të mos mund të përdoren për qëllime praktike. Është shumë e vështirë të rritet numri i kubitëve në kompjuterët kuantikë për shkak të dekoherencës, dhe megjithëse cilësia e kubitëve është rritur në dekadën e fundit, ka ende një nevojë të madhe për kërkime dhe fokusim në kompjuterët kuantikë dhe nevojën për të edukuar njerëzit përpara se të presim disa rezultate nga kompjuterët kuantikë. Jian-Wei Pan i Universitetit të Shkencës dhe Teknologjisë të Kinës, shpreson që deri në vitin 2030 komunikimet kuantike do të shtrihen në shumë vende, në rreth 10 vjet, ju mund të prisni edhe internetin kuantik. Intel njoftoi së fundmi një kompjuter kuantik 49-bit të quajtur "Tangle Lake", Google thuhet se ka ndërtuar një çip kompjuterik kuantik 72-bit të quajtur "Bristlecone", kurse IBM zbuloi kompjuterin e parë kuantik komercial në botë të quajtur IBM Q System One [7].

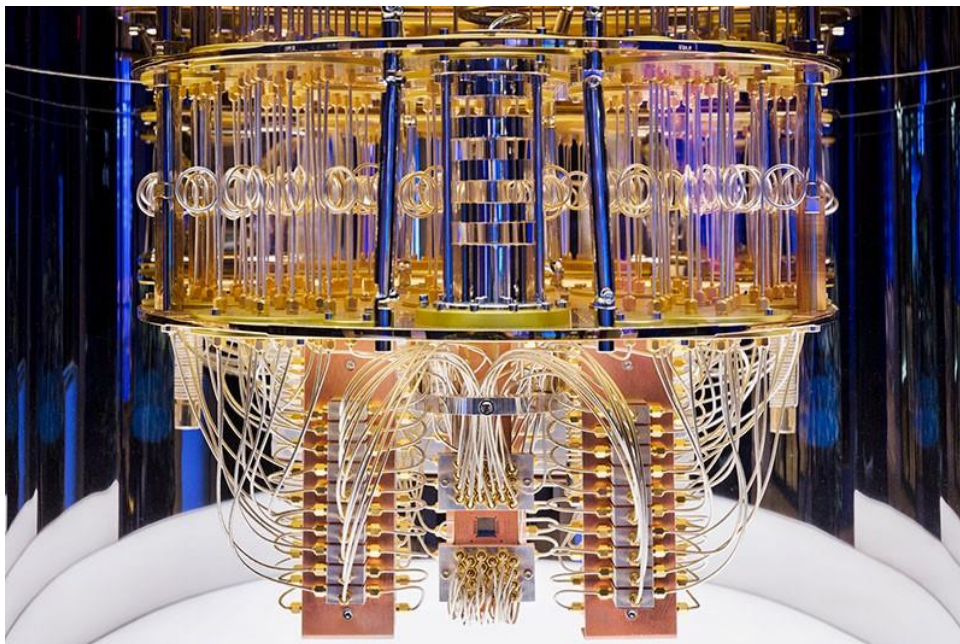


Figura 4. IBM Q System One [7]

Në përgjithësi, rruga përpara për kompjuterët kuantikë duket e ndritur, duke parë edhe konkurrencën e madhe në mes kompanive gjigante si IBM, Google dhe Microsoft. Kjo konkurrencë garanton gjithmonë rezultate të mëdha në çfarëdo fushe.

3. Quantum Computing

Kompjuteri është i përbërë nga disa komponente shumë të thjeshta, të cilat bëjnë punë të lehta si reprezentimi i të dhënave, procesimi i tyre, si dhe mekanizmat kontrollues. Një çip kompjuteri përmban module, të cilat përmbajnë porta logjike, të cilët në vete janë të përbërë nga transistorë. Tranzistori është forma më e thjeshtë e procesimit të të dhënave në kompjuterë, që në parim është thjeshtë një çelës që bllokun ose lejon kalimin e informatës. Kjo informatë është e përbërë nga të ashtuquajturit bits, të cilët mund të jenë “0” ose “1”. Kombinimi i këtyre bits mund të përdoret për reprezentimin e të dhënave më komplekse si numra, shkronja, fjalë, fjali, fotografi, e kështu me rradhë deri në reprezentimin e formulave më të komplikuar matematikore.

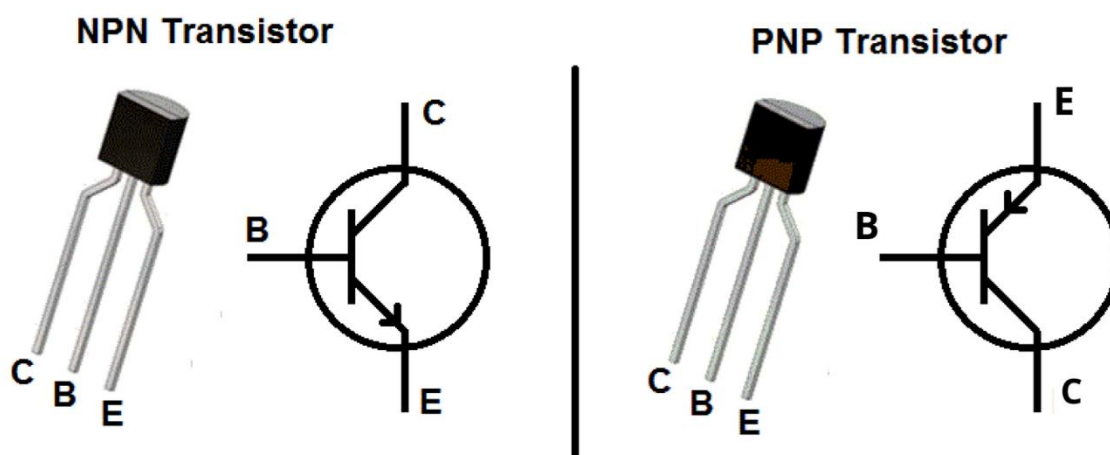


Figura 5. Tranzistorët klasik NPN dhe PNP [1]

Potenciali i kompjuterëve ishte i madh që në fillimet e tij dhe konkurrenca e madhe bëri që kjo fushë të zhvillohet gjithmonë e më shumë. Kompjuterët filluan të zvogëlohen në madhësi gjithmonë e më të vogla, si dhe bashkë me ta edhe transistorët. Këtë dukuri e vërejti edhe shkencëtari Gordon Moore, dhe e formuloi në këtë mënyrë tezën e tij: “Numri i transistorëve në një qark të integruar do të dyfishohet çdo dy vjet” [8]. Rezultatet e gjetura nga ai mund të vërehen edhe në figurën e treguar më poshtë, ku shihet zvogëlimi i madhësisë së transistorëve me kalimin e viteve. Gordon Moore emëroi këtë ligj sipas emrit të tij.

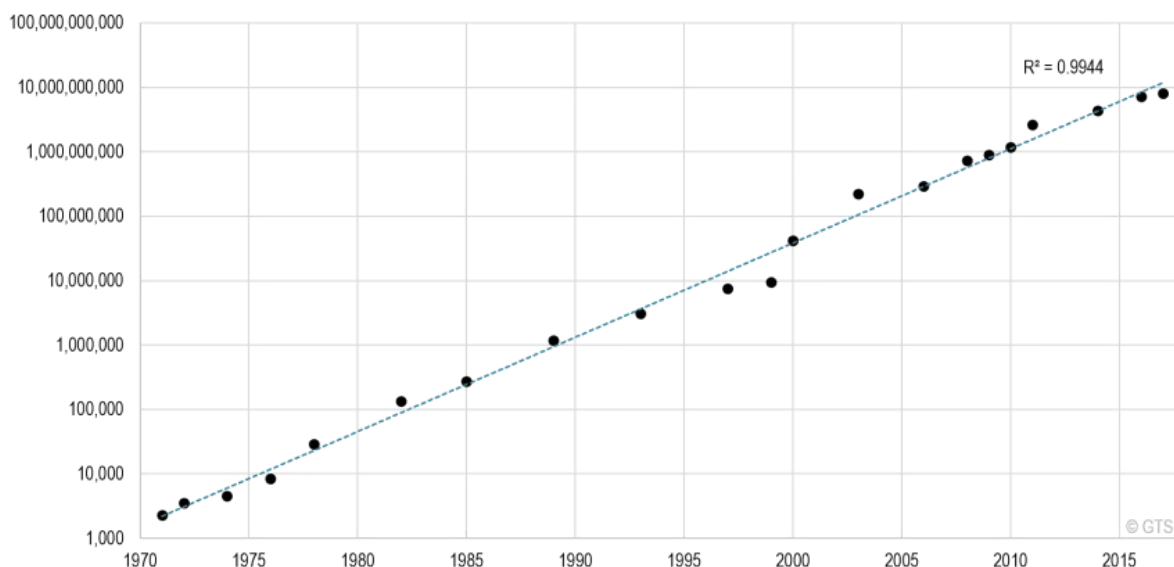


Figura 6. Ligji i Moore-it [8]

Ligji i Moore-it doli shumë i vertetë për shumë vite me rradhë dhe është akoma. Sot madhësia e zakonshme e transistorëve ka arritur diku rreth 14 nanometra, që i bjen 8 herë më i vogël se diametri i HIV virusit dhe 500 herë më i vogël se qelizat e kuqe të gjakut. Sipas kësaj prespektive, madhësia e transistorëve është duke mbërritur ditë mbas dite edhe në vet madhësinë e atomit. Atomi është njësia më e vogël e materies së zakonshme dhe arritja e madhësisë së tranzistorë në këtë dimension paraqet një problem të madh. Në botën e Fizikës Kuantike ajo madhësi aq e vogël e transistorit do të thotë se elektronet në atë rast do të mund të kalonin bllokadën e tyre përmes një procesi të quajtur Quantum Tunneling, sepse kjo është mënyra se si funksionojnë materiet në madhësi aq të vogla si të atomit. Kjo do të thotë se parimi fundamental i tranzistorëve, që është bllokimi apo lejimi i kalimit të një elektroni përgjatë një qarku nuk do të funksiononte më. Sipas një studimi të IEEE Spectrum ata kishin parashikuar në vitin 2021 tranzistorët do të ndalojnë zvogëlimin e tyre fizik dhe duket se kemi mbërritur këtë kohë [9].

Bota teknologjike është duke e arritur kufirin e vet fizik, prandaj tani shkenca është duke u munduar që ti shfrytëzojë këto veti të botës kuantike në avantazhin e tyre duke filluar të ndërtojnë Kompjuterë Kuantik. Kjo paraqet edhe fillimin i një fushe të re në komunitetin e IT-së të quajtur Quantum Computing dhe potenciali i kësaj fushe padyshim është revolucionar. Quantum Computing në thelb është shfrytëzimi i ligjeve të fizikës kuantike për të procesuar të dhëna dhe të zgjidhë disa probleme të caktuara. Ka disa probleme që kërkojnë fuqi dhe hapësirë jashtëzakonisht të madhe llogaritëse, si p.sh., gjetja e faktorëve të numrave të thjeshtë shumë të mëdhenj, simulimi i molekulave, simulimi i fenomeneve kuantike, etj. Një ndër problemet më të mëdha është si faktorizimi kryesor për numra të mëdhenj, ku këto mund të zgjidhen nga kompjuterët klasikë për një numër shumë të vogël inputesh, por për vlera të mëdha të N , koha e marrë për llogaritjen bëhet shumë e madhe dhe kështu llogaritja bëhet e pamundur. Probleme tjera si prishja e enkriptimit RSA si dhe problemet ku nevojitet një zgjidhje kuantike si modelimi kuantik gjithashtu do të ishin të pamundshme nga kompjuterët klasikë. Për këtë qëllim mund të përdoren kompjuterët kuantik, për të zgjidhur probleme që do të jenë të pazgjidhshme nga kompjuterët klasikë.

3.1. *Quantum Properties*

Për të kuptuar më mirë se si funksionojnë Kompjuterët Kuantik, fillimisht duhet të kuptojmë disa fenomene bazike të fizikës kuantike. Më specififikisht do të flasim për dy vetitë kryesore të kompjuterëve kuantik: Superposition dhe Entanglement.

3.1.1. *Quantum Superposition*

Superpozicioni kuantik është një fenomen fizik që mund të cilësohet si shumë kundër-intuitiv, pasi që ai sugjeron që grimcat kuantike si elektronet mund të shfaqen në më shumë se një gjendje në të njëjtën kohë. Për të kuptuar më lehtë këtë teori mund të marrim njërin shembull të grimcave kuantike që është elektroni dhe të themi se një elektron mund të jetë në dy gjendje, momentume apo energji të ndryshme në të njëjtën kohë. Kjo nuk vërehet në jetën tonë të përditshme, pasi në jetën tonë të përditshme një materie duhet të jetë vetëm në një vend, nuk mund të jetë në dy gjendje në të njëjtën kohë. Nëse do të ishte në shumë gjendje në të njëjtën kohë, nuk do t'u bindej ligjeve të fizikës klasike.

Kjo në fakt është e vërtetë dhe e mundur me grimcat kuantike për shkak të natyrës së tyre të dyfishtë, të ngjashme me valën dhe të ngjashme me grimcat. Grimcat kuantike thuhet se janë valë dhe grimca në të njëjtën kohë (duhet të theksohet se "e njëjta kohë" është vetëm për ta kuptuar si koncept, sepse në botën kuantike nuk ka koncept të kohës) prandaj kanë natyrë të dyfishtë. Tani valët kanë parimin e superpozicionit apo edhe interferimit siç mund ta dimë nga fizika e mësuar deri tani. Kjo do të thotë se dy valë mund të mbivendosen (superposed) mbi njëra-tjetrën për të prodhuar një valë tjetër.

Ky është përkufizimi i superpozicionit kuantik sipas Dirac [10]:

Njësoj si valët në fizikën klasike, çdo dy (ose më shumë) gjendje kuantike mund të shtohen së bashku ("superposed") dhe rezultati do të jetë një gjendje tjetër kuantike e vlefshme; dhe anasjelltas, se çdo gjendje kuantike mund të përfaqësohet si një shumë e dy ose më shumë gjendjeve të tjera të dallueshme.

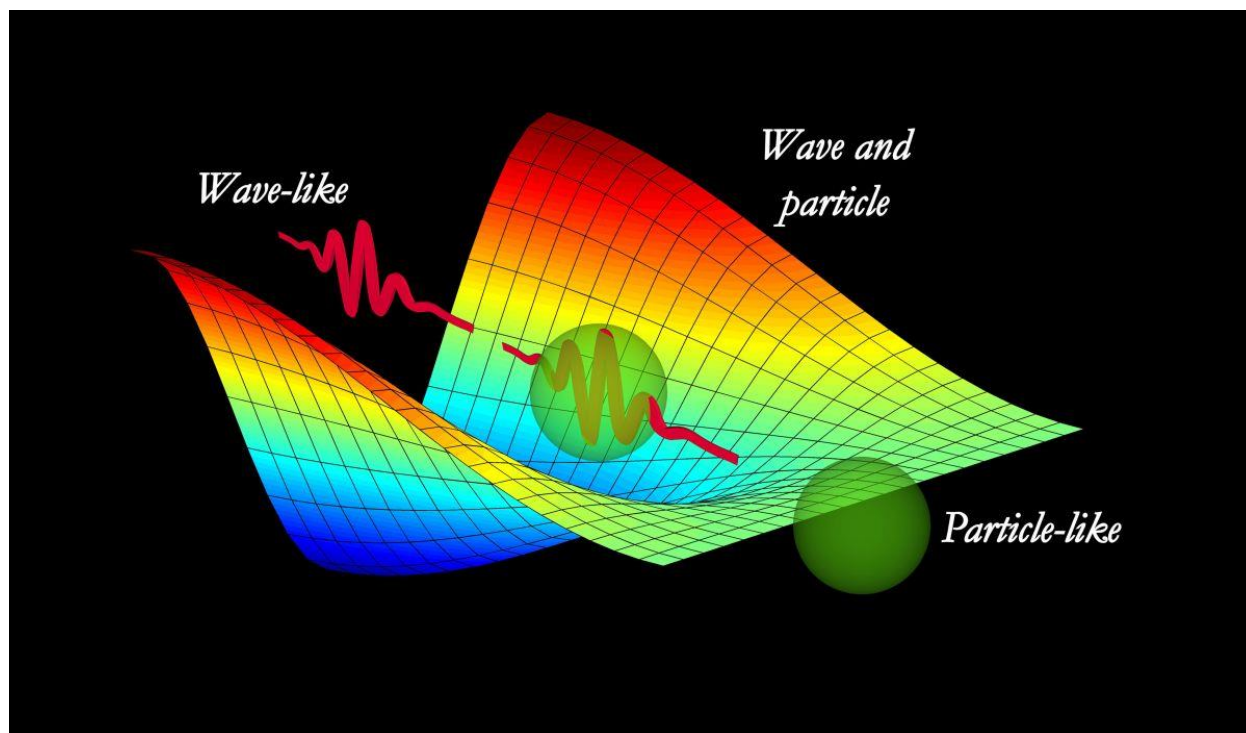


Figura 7. Vetitë e grimcave kuantike njëkohësisht si valë dhe si grimca [10]

Matematikisht, ky definicion i referohet një vetie të zgjidhjeve të ekuacionit të Schrödinger-it, ku meqenëse ekuacioni i Shrodingerit është linear, çdo kombinim linear i zgjidhjeve do të jetë gjithashtu një zgjidhje. Një shpjegim tjetër më matematikor i superpozicionit kuantik i marrur nga libri i Dirac [10] është si në vijim:

1. Konsideroni mbivendosjen e dy gjendjeve, A dhe B, të cilat në vëzhgim japin rezultate a dhe b.
2. Vëzhgimi i bërë në sistemin në gjendje të mbivendosur (superposed) do të jetë ndonjëherë a dhe ndonjëherë b, i bazuar sipas ligjit të probabilitetit në varësi të peshave relative të A dhe B në procesin e mbivendosjes (superpozicionit).

3.1.2. Quantum Entanglement

Quantum Entanglement është një nga fenomenet kuantike më magjepsëse, është një nga arsytet që Ajnshtajni ishte skeptik ndaj mekanikës kuantike dhe e bëri atë ta quante “spooky action at a distance” [11].

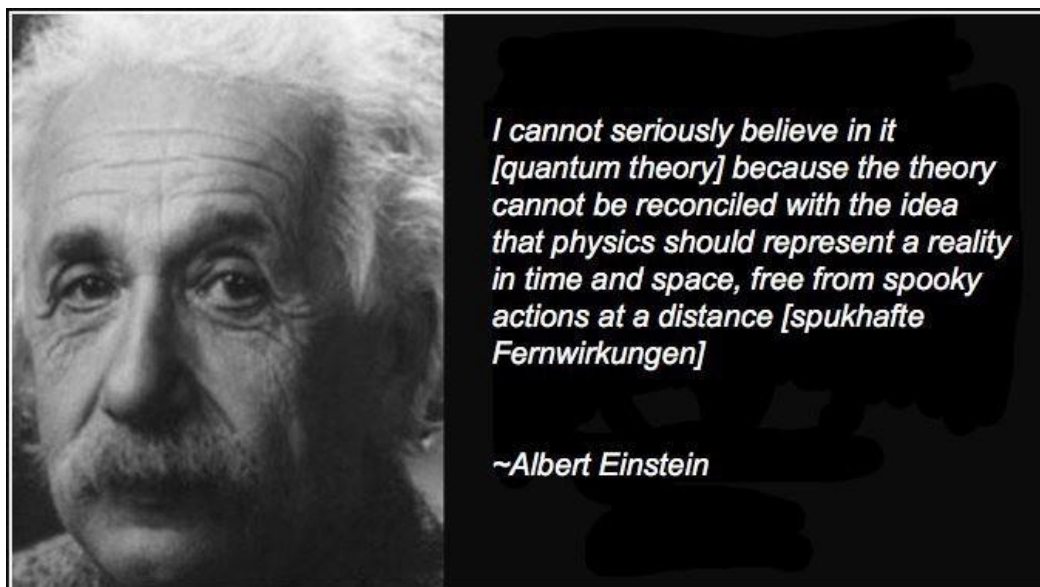


Figura 8. Opinioni i Albert Einstein për vetitë kuantike të grimcave [11]

Le të themi se keni dy grimca në një univers të izoluar të krijuar vetëm nga energjia, tani le të shqyrtojmë momentin e tyre këndor, shumën e momentit të tyre këndor duhet të jetë konstante (Ligji i ruajtjes së momentit këndor) [12]. Le të themi se ato ndahen më pas me një distancë shumë të madhe, përsëri shumën e momentit këndor të tyre duhet të jetë e njëjtë (pasi momenti këndor është i ruajtur). Kështu për shembull nëse një grimcë është në drejtim lart, atëherë grimca tjetër duhet të jetë në drejtim të kundërt. Tani le të marrim parasysh se matim rrotullimin e grimcës së parë dhe zbulojmë se ajo është në drejtim lart, atëherë rrotullimi i grimcës tjetër duhet të jetë në drejtim poshtë (ruajtja e momentit këndor), duke kontaktuar njëri-tjetrin me ndihmën e një kalimi të panjohur (spooky action) ose ata janë duke komunikuar me diçka më të shpejtë se drita (gjë që nuk është e mundur për shkak të fizikës). Kjo paraqet vetinë e famshme të Fizikës Kuantike të quajtur Quantum Entanglement [12].

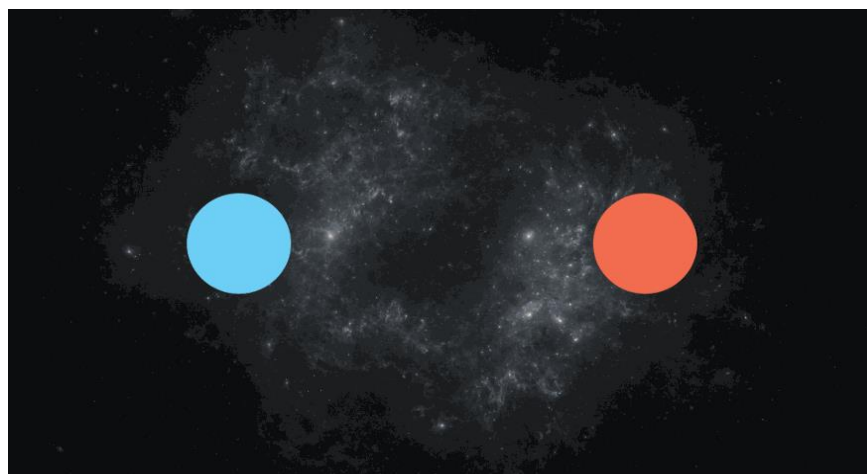


Figura 9. Vetia e grimcave kuantike e quajtur Quantum Entanglement [12]

Një përkufizimi më zyrtar për Quantum Entanglement do të ishte kështu:

Quantum Entanglement është një fenomen fizik që ndodh kur çiftet ose grupet e grimcave krijohen, ndërveprojnë ose ndajnë afërsinë hapësinore në mënyra të tilla që gjendja kuantike e secilës grimcë nuk mund të përshkruhet në mënyrë të pavarur nga gjendja e tjetrës, edhe kur grimcat janë të ndara me një distancë të madhe [12].

Ngatërrimi kuantik është demonstruar eksperimentalisht me fotone, neutrino, elektrone, molekula më të mëdha dhe madje edhe diamante të vegjël. Përdorimi i kësaj vetie në komunikim dhe llogaritje është një fushë shumë aktive e punimeve shkencore ndërkombëtare. Edhe pse ngatërrimi kuantik duket i çuditshëm, ai ende funksionon dhe kjo është ajo që ka rëndësi kur bëhet fjalë për kompjuterët kuantikë për të cilët do të vazhdojmë të hyjmë në më shumë detaje.

3.2. Qubit

Një kompjuter klasik ruan dhe proceson të dhënat duke përdorur bits, që mund të jetë 0 ose 1. Në teknologji moderne bitët janë të reprezentuar me mungesën ose prezencën e sinjalit elektrik përmes tranzistorëve elektrik, të enkoduar si 0 dhe 1. Ne kemi zhvilluar sisteme shumë të sofistikuara vetëm duke përdorur këtë formë të thjeshtë ruajtjeje të informacionit, por ne mund të bëjmë akoma shumë më mirë me një bit kuantik (Quantum Bit) apo ndryshe të quajtum Qubit. Ndryshe nga bitët që mund të ruajnë vetëm 0 dhe 1, Qubits mund të ruajnë një gjendje të tretë dhe shumë të rëndësishme që është superpozicioni i 0 dhe 1. Ky superpozicion i gjendjeve është ajo që ndihmon një kompjuter kuantik të bëjë gjëra që një kompjuter klasik nuk mund t'i bëjë në asnjë moment.

Kur një Qubit është në një nga gjendjet e superpozicionit, mund të thuhet se është në të dy gjendjet 0 dhe 1 në të njëjtën kohë. Kjo është për shkak të parimit të Quantum Superposition që është përmendur më parë. Për të kuptuar më lehtë mund të marrim një shembull të thjeshtë. Nëse marrim parasysht që do të lëvizim 3 m në Veri dhe më pas 4 m në Perëndim, tani jeni 5 m në drejtimin veri-perëndim ose jeni në një mbivendosje të Veriut dhe Perëndimit. E thënë ndryshe - "Jemi në veri dhe perëndim në të njëjtën kohë!". E njëjta gjë vlen edhe për superpozicionin e gjendjeve kuantike. Edhe pse një kubit nuk është në asnjë nga gjendjet 1 ose 0, por mund të themi se është në gjendjen 1 me një përqindje 60% dhe 40% gjendjen 0. Prandaj, është në superpozicionin e dy gjendjeve njëherësh.



Figura 10. Dallimi në mes bitëve klasik dhe kuantik [13]

Sa të fuqishëm mund të jenë Qubits në krahasim me bitët klasik? Nëse marrim 4 bits, ne mund të ruajmë deri në 2^4 , do të thotë 16 kombinime të tyre. Kurse nëse marrim 4 Qubits në superpozicion, atëherë do të jenë 16 kombinime të ndryshme përnjëherësh. Ky numër rritet në mënyrë eksponenciale me çdo Qubit

shtesë. Njëzet prej tyre tashmë mund të ruajnë 1 milion vlera paralelisht. Duke marrë parasysh këto kalkulime mund të vërejmë se sa të fuqishëm mund të jenë Qubits në ruajtjen e të dhënave të mëdha dhe rritjen e performancës së algoritmeve komplekse.

Për të ndërtuar kompjuterë kuantik na duhen objekte kuantike që do të luanin rolin e një Qubit. Shkencëtarët kanë mësuar të shfrytëzojnë dhe kontrollojnë shumë sisteme fizike që mund të përdoren si Qubits. Disa nga Qubit-ët më të zakonshëm që përdoren tani janë [14]:

- Spin
- Trapped Atoms and Ions
- Photons
- Superconducting Circuits

3.3. *Quantum Computation*

3.3.1. *Ruajtja dhe marrja e informacionit*

Një nga gjërat më të rëndësishme që bën një makinë të quhet kompjuterike është leximi dhe shkrimi i të dhënave, pasi që nëse ajo është e mundur atëherë një makinë e tillë mund të bëjë “gjithçka”, siç tregohet nga matematicienti i famshëm si dhe i cilësuar babai i shkencave kompjuterike Alan Turing. Koncepti i Makinerisë Turing është marrë më tej edhe për Kompjuterët Kuantikë dhe janë propozuar Makinat Turing Kuantike.

Fillimisht, le të kuptojmë se si një kompjuter kuantik lexon dhe shkruan të dhëna. Kubitët janë të ngulitur (embedded) midis transistorëve. Tani të gjithë kubitët kanë energji, le të themi se kemi një elektron në gjendje poshtë (doën), atëherë ai do të ketë energji të ulët, tani me një mikrovalë precize (precize do të thotë të jesh në vendin e duhur me frekuencën e duhur) ne mund t'i japim atij elektron energji të mjaftueshme për ta bërë atë të rrotullohet në drejtimin lart. Kjo do të rezultojë në një ndryshim të tensionit në tranzistor dhe tani mund të themi në bazë të tij, se ai me të vërtetë është rritur. Prandaj ne kemi ndryshuar gjendjen e një kubit nga 0 në 1 dhe tani kemi shkruar me sukses në një kubit.

Leximi nga një kubit është i ngjashëm, por duhet të kemi parasysh se nuk është aq e lehtë. Nuk mund të kemi thjesht një gjenerator të mirë mikrovalë dhe të lexojmë/shkruajmë nga/në Qubit. Meqenëse në temperaturën e dhomës, ka shumë energji për një grimcë kuantike dhe ajo do të gjenerojë modele të rastësishme, por ne kemi nevojë për modele shumë të sakta, kështu që ne duhet ta ftohim substancën në pothuajse zero kelvin në mënyrë që të mund të regjistrojmë të dhënat e qubitit. Ky fenomen i nevojës së ftohjes së substancës për ta ruajtur gjendjen e tyre kuantike quhet Quantum Decoherence [15].

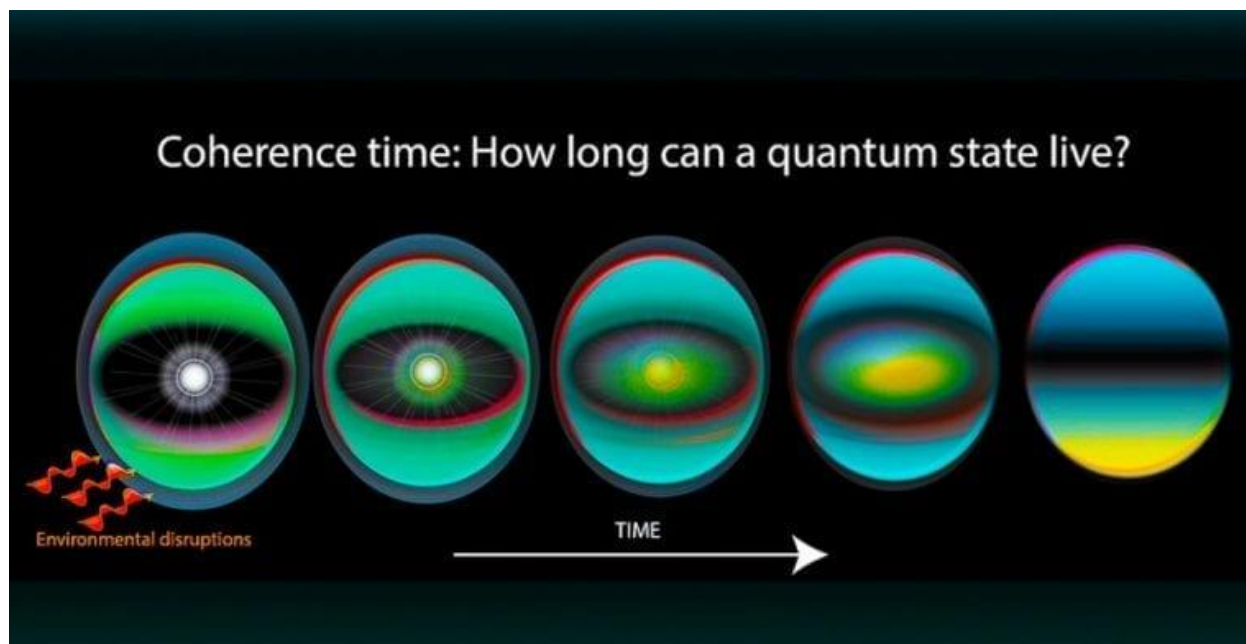


Figura 11. Dekoherenca Kuantike [15]

3.3.2. The Big Picture

Pasi kemi parë operationet bazë si leximi dhe shkrimi në një kubit, tani jemi gati të kuptojmë se si kompjuterët kuantikë kryejnë operacione logjike. Kjo bëhet me ndihmën e portave logjike kuantike. Portat logjike kuantike janë qarqe kuantike bazë që veprojnë në një numër të vogël kubitësh. Ato janë blloqet ndërtuese të qarqeve kuantike, siç janë portat logjike klasike për qarqet digjitale konvencionale. Por ndryshe nga portat klasike, portat kuantike kanë një veti të veçantë - ato janë të kthyeshme. Kjo do të thotë që dalja mund të gjenerohet nga hyrja dhe anasjelltas. Për shembull, duke ditur se në një Portë NOT (NOT GATE) dalja është 1, ne e dimë se hyrja duhet të jetë 0. Në mënyrë të ngjashme, nëse dimë se dalja është 0, atëherë hyrja duhet të jetë 1. Prandaj, Porta NOT është e kthyeshme.

Portat kuantike duhet të jenë të kthyeshme pasi mekanika kuantike kërkon që një sistem kuantik të mos humbasë kurrë informacionin me kalimin e kohës dhe duhet gjithmonë të jetë e mundur të rindërtohet e kaluara [3].

Ka shumë porta kuantike në dispozicion. Këtu do të japim një përmbledhje të shkurtër të disa prej portave kuantike më të rëndësishme [16]:

- **CNOT Gate:** ose Controlled NOT është një nga Portat më themelore për kompjuterët kuantikë. Çdo qark kuantik mund të simulohet në një shkallë arbitrare saktësie duke përdorur një kombinim të portave CNOT dhe rrotullimeve të vetme të Qubit. Mund të përdoret për të ngatërruar (entangle) dhe shkëputur (disentangle) gjendjet EPR (entangled pairs of qubits). Porta CNOT funksionon në një regjistrer kuantik të përbërë nga 2 Qubit. Porta CNOT kthen Qubit-in e dytë (Qubit-in e synuar) nëse dhe vetëm nëse Qubiti i parë (Qubiti i kontrollit) është $1>$.
- **Toffoli Gate:** Porta Toffoli është një portë logjike e kthyeshme universale, që do të thotë se çdo qark i kthyeshëm mund të ndërtohet nga portat Toffoli. Ka hyrje dhe dalje 3-bit; nëse dy bitët e parë janë vendosur të dy në 1, ai përmbys bitin e tretë, përndryshe të gjithë bitët qëndrojnë të njëjtë.

- **Hadamard Gate:** Porta Hadamard është një operacion me një Qubit që harton gjendjen bazë $|0\rangle$ në $(|0\rangle + |1\rangle)/\sqrt{2}$ dhe $|1\rangle$ në $(|0\rangle - |1\rangle)/\sqrt{2}$, duke krijuar kështu një mbivendosje të barabartë të dy gjendjeve bazë. Porta Hadamard mund të shprehet gjithashtu si një rrotullim 90° rreth boshtit Y, i ndjekur nga një rrotullim 180° rreth boshtit X.

Me njohuritë e mësipërme për funksionimin e brendshëm të kompjuterëve kuantikë, ne mund t'i kombinojmë këto për të formuar pjesë më të gjera dhe më të dobishme të një kompjuteri ashtu sikurse në kompjuterët klasikë. Pastaj na duhen të gjitha gjërat që janë të disponueshme në një kompjuter klasik, duke filluar nga një compiler, sistem operativ, gjuhët e programimit, etj. Meqenëse kompjuterët klasikë kanë një histori të pasur, ne mund ta shfrytëzojmë këtë në avantazhin tonë dhe pa shumë punë, të ndërtojmë një softuer të dobishëm për kompjuterë kuantik. Aktualisht, shumica e kompanive kanë arkitekturat e tyre, por kjo duhet të ndryshojë së shpejti nëse duam të rrisim shpejtësinë e kërkimit në këtë fushë. Ne kemi nevojë për arkitektura të standardizuara, kështu që është e lehtë për studiuesit të zhvillojnë dhe testojnë gjëra të reja.

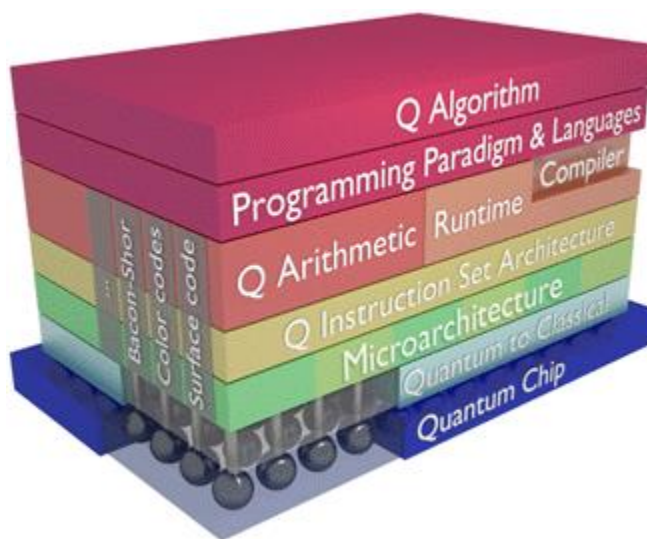


Figura 12. Arkitektura e propozuar për kompjuterët kuantik [17]

Siç mund të shihet kjo duket si një arkitekturë klasike kompjuterike me termin kuantik të lidhur me të, dhe në të vërtetë është ashtu. Tani jemi në gjendje të kuptojmë se si t'i përdorim këta komponentë dhe të bëjmë diçka të dobishme me ta duke ndërtuar algoritme të ndryshme që do të jenë revolucionare për botën teknologjike.

Disa nga algoritmet kuantike që janë propozuar në komunitetin e kësaj fushe janë [18]:

- **Algoritmi i Shor-it**, i cili mund të përdoret për faktorizimin e numrave të plotë. Ai përdor teorinë e numrave për ta arritur këtë dhe teorikisht mund të thyejë enkriptimin RSA.
- **Algoritmi i Grover-it** është një algoritëm kuantik që gjen me probabilitet të lartë hyrjen unike në një funksion të kutisë së zezë që prodhon një vlerë të caktuar dalëse, duke përdorur vetëm një kompleksitet $O(N)$ të funksionit, ku N është madhësia e domenit të funksionit. Ajo u krijua nga Lov Grover në 1996.
- **Problemi Deutsch-Jozsa**, i cili merr vlera binare n -shifrore si hyrje dhe prodhon një 0 ose një 1 si dalje për secilën vlerë të tillë. Na premtohet se funksioni është ose konstant (0 në të gjitha daljet

ose 1 në të gjitha daljet) ose i balancuar, detyra më pas është të përcaktojmë nëse f është konstante apo e balancuar duke përdorur orakullin (black box quantum computer).

Shumica e këtyre algoritmeve gjejnë përdorimin më të madh në Kriptografinë Kuantike, e cila cilësohet si fusha më e zhvilluar e Quantum Computing deri më tani.

4. Quantum Cryptography

Nga shumë degë të ndryshme të kompjuterikës kuantike, kriptografia kuantike është ndoshta më e njohura. Përparësitë e kriptografisë kuantike përfshijnë sigurinë e pathyeshme, që do të thotë se mund të ketë aplikime pothuajse në çdo industri. Përderisa studiuesit dalin me algoritme dhe parime të reja për t'u zbatuar në kriptografinë kuantike, kjo pa dyshim do të revolucionarizojë të ardhmen e sigurisë në internet. Kriptografia është procesi i enkriptimit të të dhënave, ose i konvertimit të tekstit të thjeshtë në tekst të pakuptueshëm apo të enkriptuar, në mënyrë që vetëm dikush që ka "çelësin" e duhur mund ta lexojë atë. Kjo lloj kriptografie është arsyeja që ne mund të ju dërgojmë email privatisht miqve tanë pa pasur nevojë të shqetësohemi nëse dikush tjetër do të jetë në gjendje t'i lexojë ato.

Kriptografia kuantike, në bazamentet e saj, thjesht përdor parimet e mekanikës kuantike për të enkriptuar të dhënat dhe për t'i transmetuar ato në një mënyrë që nuk mund të deshifrohen. Sipas përkufizimit zyrtarë, kriptografia kuantike është shkenca e shfrytëzimit të vetive mekanike kuantike për të kryer detyra kriptografike. Ekzistojnë dy lloje të shpërndarjes së çelësit në kriptografinë e rregullt:

- çelësi simetrik - i cili mbështetet në një çelës sekret të përbashkët që vetëm palët lejohen të lexojnë të dhënat
- çelësi asimetrik - i cili përdor çifte çelësash publik/privat të krijuar matematikisht.

Edhe pse matematika e përdorur për gjenerimin e këtyre çelësve është shumë e ndërlikuar, është e mundur të thuhet nëse mund të faktorizoni një numër shumë të madh (çelës publik) në dy faktorët e tij të numrit kryesor (çelës privat). Arsyeja pse ne i besojmë këtij lloji të kriptimit është se do të duhej një kohë jopraktike që edhe kompjuterët klasikë më të fuqishëm të kryejnë llojin e llogaritjeve të nevojshme për të gjetur dy numrat e thjeshtë të saktë. Problemi me kriptografinë e rregullt është se, sado i ndërlikuar dhe kohëmarrës të jetë procesi, është e mundur që në një moment të zbulohen çelësat privatë me numrin kryesor që mbrojnë sekretet tona. Kjo informatë për qeveritë dhe bizneset me informacione shumë të vlefshme, tregon se zhvillimi i shpejtë i kompjuterëve dhe fuqia e tyre përpunuese përbën një rrezik të madh.

Kriptografia kuantike është siç thamë përdorimi i parimeve të mekanikës kuantike për të krijuar dhe transmetuar të dhëna në një mënyrë që nuk mund të dekriptohen kurrë. Vetë natyra e grimcave të kompjuterëve kuantikë, me vetitë e tyre speciale, e bën kriptografinë kuantike jashtëzakonisht të sigurt.

Ka katër parime kryesore në të cilat do të përqendrohet kriptografia kuantike [19]:

1. Të gjitha grimcat janë të pasigurta. Mekanika kuantike ndalon njohjen e vetive të caktuara të grimcave kuantike pa sakrifikuar njohurinë e disa vetive të tjera. Kjo nuk ka të bëjë fare me instrumentin matës apo me kompetencën e vëzhguesit, por me natyrën e vetë sistemit.
2. Grimcat kuantike mund të ekzistojnë në më shumë se një gjendje ose vend. Fotonet mund të ekzistojnë në dy gjendje të ndryshme kuantike: rrotullimi lart dhe rrotullimi poshtë. Linja midis të dyjave shpesh është e paqartë, kështu që këto gjendje përdoren në llogaritjen kuantike si homologu kuantik i njësheve dhe zero në bit klasikë binare.
3. Ju nuk mund të matni një sistem kuantik pa e shqetësuar ose pa bërë që sistemi të shembet në vetvete (dekoherenca kuantike).
4. Ju mund të klononi disa veti të një grimce kuantike, por jo të gjitha.

Këto veti janë secila të nevojshme që kriptografia kuantike të funksionojë, me role kyçe në shpërndarjen e çelësit kuantik (Quantum Key Distribution) dhe enkriptimin aktual. Ndryshe nga sistemet klasike kriptografike, këto veti të përmedura përfundojnë natën e sistemet kriptografike kuantike si vërtet të pahakueshme.

Ndërsa shumë fusha të kriptografisë kuantike janë konceptuale dhe jo realitet sot, disa aplikacione të rëndësishme ku sistemet e enkriptimit kryqëzohen me llogaritjen kuantike janë thelbësore për të ardhmen e afërt të sigurisë kibernetike.

Dy aplikacione kriptografike të njohura, por dukshëm të ndryshme në zhvillim duke përdorur vetitë kuantike janë [6]:

- **Quantum Key Distribution (Shpërndarja e çelësit kuantik):** Procesi i përdorimit të komunikimit kuantik për të vendosur një çelës të përbashkët midis dy palëve të besuara në mënyrë që një përgjues i pabesueshëm të mos mund të mësojë asgjë për atë çelës.
- **Quantum Encryption (Enkriptimi Kuantik):** Procesi i përdorimit të mekanikës kuantike për të kriptuar vetë të dhënat, jo vetëm çelësin e përdorur për t'i lexuar ato.
- **Quantum-safe Cryptography (Kriptografia kuantike e sigurt):** Zhvillimi i algoritmeve kriptografike, të njohura gjithashtu si kriptografia post-kuantike, që janë të sigurta kundër një sulmi nga një kompjuter kuantik dhe përdoren në gjenerimin e certifikatave të sigurta kuantike.

Shembulli më i njohur i kriptografisë kuantike është shpërndarja e çelësit kuantik, e cila ofron një zgjidhje teorikisht të sigurt informacioni për problemin e shkëmbimit të çelësve (Quantum Key Distribution).

4.1. Quantum Key Distribution

Kriptografia Kuantike zakonisht ka të bëjë me shpërndarjen e çelësit kuantik, ose QKD. Shpërndarja e çelësit kuantik nuk i kodon të dhënat aktuale, por përkundrazi i lejon përdoruesit të shpërndajnë në mënyrë të sigurt çelësat klasikë të cilët më pas mund të përdoren për komunikim të koduar.

Pra, si funksionon QKD? Duke u mundur të mos devijojmë nga shembujt e zakonshëm të kriptografisë, imagjinojmë se kemi një përdorues të quajtur Alice që dëshiron t'i tregojë me siguri Bobit se ajo mendon se Toby është personazhi më i mirë në The Office. Alice e di se dhunuesi i saj, Eva, po përpiqet të përgjojë bisedën e tyre në mënyrë që ajo të mund ta ekspozojë Alice-n në të gjithë shkollën. Por Alice dhe Bob janë të zgjuar: ata vendosin të përdorin QKD për të siguruar bisedën e tyre. Alice përdor një sekuençë të rastësishme filtrash për t'i dërguar Bobit një seri fotonesh të polarizuara përmes një kabloje me fibër optike (Parimi 2), të cilin ai duhet ta lexojë më pas duke përdorur dy lloje të ndryshme filtrash.

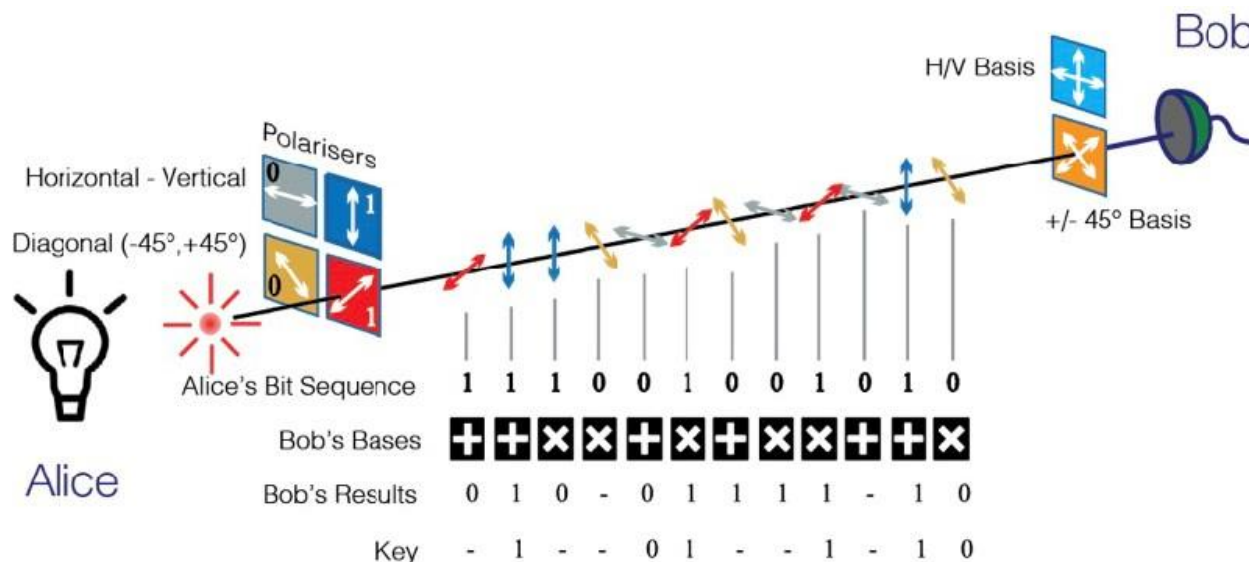


Figura 13. Quantum Key Distribution Process [19]

Ekzistojnë katër lloje të ndryshme të rrotullimit të fotonit: horizontale, vertikale, diagonale me pamje përpara dhe diagonale me pamje prapa. Rrotullimet diagonale vertikale dhe mbropa përfaqësojnë një bit që zë gjendjen "1", ndërsa rrotullimet diagonale horizontale dhe përpara përfaqësojnë një bit që zë gjendjen "0". Rrotullimi horizontal dhe vertikal mund të lexohet vetëm nga një filtër drejtvizor, dhe rrotullimi diagonal me drejtim përpara dhe prapa mund të lexohet vetëm nga një filtër diagonal (siç tregohet në grafikun e mësipërm). Nëse Bob do të përdorte filtrin e gabuar për një foton të caktuar, ai do të kishte marrë një matje të gabuar. Ky ishte një telash që në fakt studiuesve iu desh shumë kohë për ta kuptuar, sepse e bënte mesazhin aq të sigurt sa që edhe marrësi i synuar nuk do të ishte në gjendje ta lexonte atë.

Zgjidhja e tyre ishte e thjeshtë por gjeniale: pasi të ndodhte transaksioni i fotonit, Alice do të telefononte Bobin dhe do t'i tregonte se cilën sekuencë filtrash përdori për të krijuar polarizimin origjinal. Fotonet për të cilat Bob përdori filtrin e gabuar më pas hidhen, dhe sekuenca e mbetur e njësheve dhe zerove bëhet çelësi që ata përdorin për të koduar bisedën e tyre. Pjesa më befasuese është se, edhe nëse Eva do të dëgjonte bisedën e tyre, ajo nuk do të ishte në gjendje të zbulonte çelësin aktual, sepse ajo di vetëm filtrat e përdorur nga Alice, jo vetë gjendjet e polarizimit. Në mënyrë që ajo të kuptojë saktë çelësin, ajo duhet të dijë se cilët filtra kanë përdorur Alice dhe Bob përpara se të ishin dërguar ndonjëherë fotonet (Parimi 1).

Për më tepër, për të matur rrotullimin e fotoneve që Alice dërgoi përgjatë kabllit, Evës do t'i duhej ta kalonte atë përmes sekuencës së saj të filtrit. Nëse ajo përdor filtrin e gabuar për çdo foton të caktuar, rrotullimi i tij përkatës do të ndryshonte. Pra, sapo Alice i thotë Bobit se cilën sekuencë filtrash përdori, ajo dhe Bob do ta dinin menjëherë se çelësi i tyre është komprometuar sepse sekuenca e biteve të tyre nuk do të përputhej (Parimi 3). Më pas Alice do t'i dërgonte një çelës të ri, të pakompromis Bobit, të cilin ai mund ta përdorte më pas për të lexuar sekretin e saj.

Tani mund të pyesni: nëse QKD është kaq e sigurt, atëherë pse nuk është në përdorim të gjerë? Përgjigja kryesore për këtë pyetje është se vetë procesi është shumë i shtrenjtë. Pra, përdoret për transaksione të rëndësishme si komunikimi ndërbankar dhe transmetimi i rezultateve të zgjedhjeve ku kostoja e lartë ka kuptim, por nuk do të mbrojë privatësinë e mesazheve tuaja me tekst. Pavarësisht nga pengesat që mund të jenë përgjatë rrugës, një gjë është e qartë se QKD është e ardhmja e afërt e kriptografisë.

4.2. Quantum Encryption

Ndryshe nga QKD, kriptimi kuantik është procesi i përdorimit të mekanikës kuantike për të kriptuar vetë të dhënat, jo vetëm çelësin e përdorur për t'i lexuar ato. Kjo detyrë është shumë më e vështirë se QKD, por megjithatë është një mundësi eventuale. Aktualisht, qasja më popullore ndaj kriptimit kuantik është Protokoli KAK: një version kuantik i algoritmit të rregullt të bllokimit të dyfishtë, i cili është një proces me katër hapa që lejon përdoruesit të komunikojnë të dhëna pa ndarë asnjë çelës [19].

Le të supozojmë të njëjtin skenar Bob-Alice-Eve nga më parë, ku Alice nuk dëshiron që Eva të lexojë sekretin që i dërgon Bobit. Alice mbyll mesazhin e saj në një kuti dixhitale duke përdorur një çelës sekret të koduar dhe ia dërgon Bobit. Më pas Bob vendos bllokimin e tij në kasë dhe ia dërgon atë Alice, e cila e heq bllokimin e saj. Pasi çështja t'i kthehet Bobit, ai mund ta zhblokojë atë dhe të lexojë mesazhin brenda. I gjithë ky shkëmbim ndodhi pa pasur nevojë që Alice apo Bob të ndajnë asnjë çelës, gjë që e bën atë shumë të sigurt.

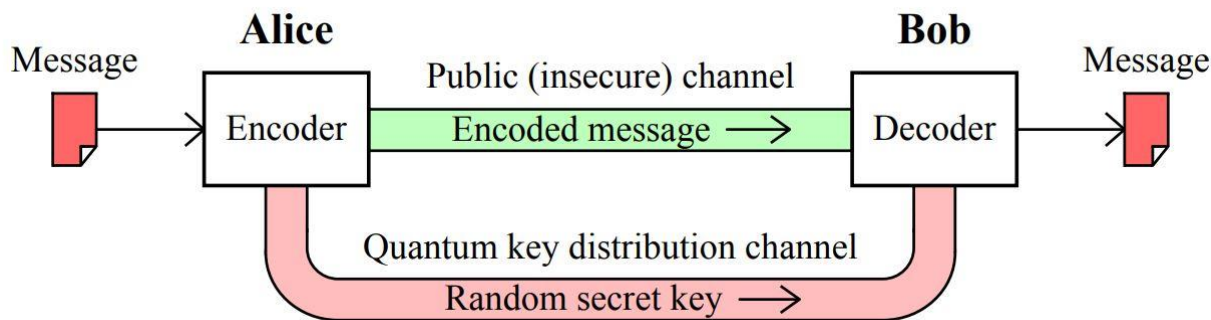


Figura 14. Procesi i enkriptimit kuantik [20]

Transferimi bëhet pak më i komplikuar kur përfshijmë enkriptimin digjital, për disa arsye. Së pari, çështja duhet të shkëmbehet në një sekuencë specifike kronologjike në mënyrë që të funksionojë: Alice duhet të vendosë bllokimin e saj në kasë përpara se Bob ta bëjë këtë, dhe më pas ajo duhet të jetë në gjendje ta heqë atë përpara se Bob të heqë të tijën. Për më tepër, meqenëse enkriptimi i zakonshëm përfshin shumëzimin me një numër të madh, Eva mund të nxjerrë hipotetikisht çelësat sekretë përkatës të Alice dhe Bob duke matur të dhënat e shumëzuara me çelësin e Alice, të dhënat e shumëzuara me të dy çelësat dhe të dhënat e shumëzuara me çelësin e Bobit ndërsa paketa kthehet prapa. dhe me radhë.

Për të zgjidhur këtë problem, shkencëtari kompjuterik Subhash Kak propozoi përdorimin e disa rrotullimeve kuantike si bravë në vend të numrave të shumfishuar të mëdhenj [20]. Këto rrotullime duhet të zbatohen në çdo mënyrë, sepse sistemet kuantike mund të zënë disa gjendje në të njëjtën kohë (Parimi 2), i cili zgjidh problemin e mëparshëm të "bloqeve" që duhen zbatuar në mënyrë komutative. Meqenëse matja e sistemeve kuantike shkakton kolapsin e tyre (Parimi 3) dhe është e pamundur të klonohen të gjitha vetitë kuantike-mekanike të një sistemi kuantik (Parimi 4), çdo përpjekje e Evës për të matur të dhënat e ndërmjetme do të bënte që mesazhi të korruptohej. Dhe kështu nuk ka asnjë mënyrë të mundshme që Eva të lexojë sekretin e Alices.

Studiuesit përveç Kak kanë vazhduar të zhvillojnë protokollin dhe ta bëjnë atë më rezistent ndaj ndërhyrjeve, por për fat të keq, ne nuk kemi parë ende ndonjë zbatim komercial të enkriptimit kuantik. Megjithatë kriptimi i vërtetë i bazuar në kuantik do të kërkojë kompjuterë shumë më të fuqishëm, studiuesit po afrohen më shumë për ta bërë atë realitet.

4.3. Quantum-Safe Cryptography

Kriptosistemet e mira kërkojnë një problem të vështirë për t'u zgjidhur. Kriptimi kuantik vjen nga zgjedhja e një qasjeje matematikore që është e vështirë për t'u zgjidhur si për kompjuterët tradicionalë ashtu edhe për ato kuantike. Algoritmet aktuale kriptografike RSA dhe ECC bazohen në probleme algjebrike duke përdorur numra të rastësishëm shumë të gjatë dhe aplikohen si për çelësat publikë ashtu edhe për çelësat privatë në një mënyrë që çelësi privat, i cili është çelësi sekret, nuk mund të rrjedhë nga çelësi publik përmes brute force attacks. Sulmet në këso raste bëhen të paefektshme sepse janë shumë të shtrenjta nga pikëpamja llogaritëse. Me llogaritjen kuantike, këto supozime themelore, mbi të cilat është ndërtuar e gjithë arkitektura jonë e sigurisë, nuk janë më të vërteta. Kompjuterët kuantikë mund të nxjerrin çelësin privat nga një çelës publik në një kohë të arsyeshme.

Kriptografia e sigurt kuantike bazohet në zgjidhjen e problemeve krejtësisht të ndryshme. Për shembull, kriptografia e bazuar në rrjetë bazohet në një qasje gjeometrike dhe jo në atë algjebrike, duke i bërë vetitë speciale të një kompjuteri kuantik më pak efektive në thyerjen e sistemeve të enkriptimit kuantik. Kriptografia e bazuar në rrjetë është e vështirë për t'u zgjidhur si për kompjuterët klasikë ashtu edhe për ato kuantike, duke e bërë atë një kandidat të mirë për të qenë baza e qasjes për një algoritëm kriptografik post-kuantik. Janë propozuar algoritme të sigurta kuantike dhe aktualisht po i nënshtrohen një procesi përzgjedhjeje nga Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST), agjencia federale e SHBA-së që mbështet zhvillimin e standardeve të reja, me plane për të nxjerrë standardin fillestar për kriptografinë rezistente ndaj kuantike në vitin 2022 [19].

Ndërsa zhvillohet kriptografia kuantike e sigurt, ndërmarrjet tani duhet të marrin në konsideratë se cilat certifikata të sigurta kuantike do të zbatohen. Ekzistojnë katër lloje të certifikatave dixhitale që janë të rëndësishme për çdo diskutim rreth sistemeve të kriptografisë kuantike. Çdo lloj është ende i përmbahet standardeve të certifikatës dixhitale X.509 që janë thelbësore për kriptografinë e çelësit publik. Këto lloje ndryshojnë dukshëm sipas qëllimit dhe algoritmit të enkriptimit të përdorur për të krijuar certifikatën.

Certificate Type	Encryption Algorithms	Description	Purpose
Traditional	RSA or ECC	Traditional non-Quantum-Safe certificates	Traditional PKI and identity systems
Quantum-Safe	New Quantum-Safe algorithms	Quantum-Safe certificates	Implementing Quantum-Safe PKI and identity systems
Hybrid	Traditional (ECC or RSA) and quantum- safe algorithms	Contains both traditional and Quantum-Safe keys	Used for migration to Quantum-Safe algorithms. Systems can use either the traditional or Quantum-Safe keys
Composite	Multiple Traditional (ECC or RSA) and/or Quantum Safe algorithms	Contains multiple traditional and/or Quantum-Safe keys	Used for systems requiring the highest level of security and protection while recognizing the provenance of some encryption algorithms is still unknown

Figura 15. Lista e certifikatave kuantike [19]

4.5. Pse kriptografia kuantike është e rëndësishme?

Teknologjia premton të bëjë disa lloje problemesh kompjuterike shumë, shumë më të lehta për t'u zgjidhur sesa me kompjuterët klasikë të sotëm. Një nga këto probleme është thyerja e disa llojeve të enkriptimit, veçanërisht metodat e përdorura në infrastrukturën e sotme të çelësit publik (PKI), e cila qëndron në themel të pothuajse të gjitha komunikimeve të sotme në internet.

Organizatat akademike, teknologjike dhe të sektorit publik në mbarë botën kanë përshpejtuar përpjekjet për të zbuluar, zhvilluar dhe zbatuar algoritme të reja kriptografike të sigurt kuantike. Objektivi është krijimi i një ose më shumë algoritmeve që mund të jenë rezistente në mënyrë të besueshme ndaj llogaritjes kuantike.

Kompjuterët kuantikë komercialë të disponueshëm sot janë ende larg aftësisë për ta bërë këtë. Realiteti i kriptografisë kuantike është se teoritë kanë avancuar më shumë se sa vet hardueri. Megjithatë këto probleme gjithmonë kan motivuar njerëzit që të kalojnë këtë bllokadë sa më shpejtë.

5. Rasti i studimit – Programimi i kompjuterëve kuantik

5.1. Metodologjia dhe veglat e përdorura

Kompjuterët kuantikë ekzistojnë dhe funksionojnë sot, megjithëse me shkallë gabimesh mjaft të larta. Përderisa zbatimi fizik i këtyre makinerive ndryshon në mënyrë thelbësore midis kompanive të ndryshme, shumë nga konceptet për programimin e tyre mbeten të njëjta. Për shkak të potencialit të kompjuterëve kuantikë, gjigantët e teknologjisë si Google dhe IBM janë duke ofruar mundësinë përdoruesve që nuk kanë kompjuterë kuantik të mësojnë se si të programojnë dhe manipulojnë qarqet kuantike duke përdorur gjuhë të ndryshme programimi.

Gjuhët kuantike të programimit të zhvilluara deri më tani përdoren për:

- menaxhimin e pajisjeve fizike ekzistuese
- parashikimin e kostove të ekzekutimit të algoritmeve kuantike në pajisjet e mundshme
- shqyrtimin e koncepteve të llogaritjes kuantike (qubits, superposition, entanglement)
- testimin dhe verifikimin e algoritmeve kuantike dhe zbatimin e tyre

Gjuhët aktuale të programimit kuantik dhe përpiluesit janë të fokusuar kryesisht në optimizimin e qarqeve të nivelit të ulët të përbërë nga portat kuantike. Portat kuantike janë blloqet ndërtuese të qarqeve kuantike, ato janë të ngjashme me portat logjike të kompjuterëve klasik [16].














Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Figura 16. Portat logjike kuantike [10].

Por për programimin e këtyre kompjuterëve lindin disa vështirësi:

- Vështirësi në formulimin e gjuhëve universale
- Paplotësia dhe ndryshoret e fshehura në mekanikën kuantike
- Kompjuterët kuantikë janë ende në fillimet e tyre duke punuar në <100 Qubits, prandaj, nuk janë mjaftueshëm të fuqishëm për të ekzekutuar algoritme komplekse kuantike.

Megjithatë, disponueshmëria e SDK-ve me burim të hapur po i lejon komunitetet të gjejnë zgjidhje për sfidat e programimit dhe të gjejnë aplikacione më praktike për llogaritjen kuantike. Unë do të përdorë dokumentimin dhe udhëzimet e IBM për programimin e kompjuterëve kuantik dhe ndërtimin e qarqeve kuantike, duke shfrytëzuar një modul të gjuhës programuse Python që quajtur Qiskit. Modul i zhvilluar nga IBM Research për ta bërë më të lehtë për këdo ndërfaqen me një kompjuter kuantik.

Për të simuluar qarqe apo zgjidhje të probleme kuantikë përmes Python ne mund të përdorim simulatorët QasmSimulator që synon të imitojë një pajisje të vërtetë kuantike ose mund të lidhemi direkt me kompjuterët kuantik të IBM përmes një API Token [21].

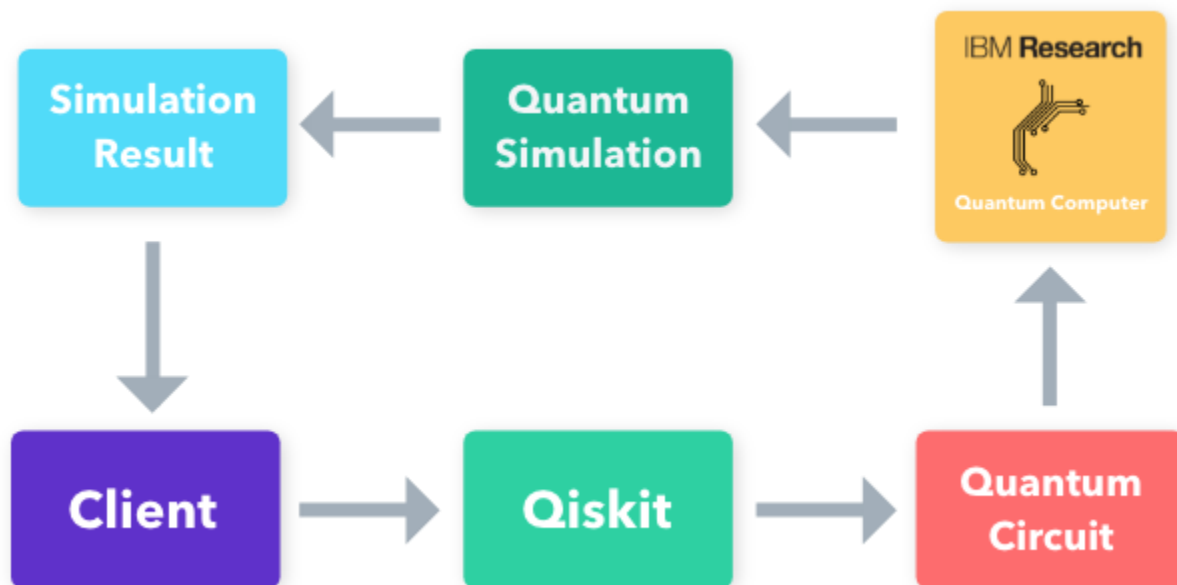


Figura 17. Procesi i simulimit të programeve kuantike përmes IBM Research Programme [21]

Për të analizuar se si mund të programojmë në një kompjuterë kuantik do të ndjekim disa shembuj të zhvilluar nga unë, duke filluar nga shembuj më të thjeshtë deri në më të komplikuar:

1. Ndërtimi i një qarku kuantik përmes Portës Hadamard dhe Portës së Kontrolluar-NOT
2. Gjenerimi i vlerave reale të rastësishme me shembullin e monedhës kuantik
3. Faktorizimi i numrave prim përmes algoritmit të Shor-it, i cili vërteton thyerjen e RSA-së nga kompjuterët kuantik

5.2. Ndërtimi i një qarku të thjeshtë kuantik

Ndërtimin e një qarku të thjeshtë kuantik mund ta bëjmë duke përdorur dy porta kuantike:

1. Porta Hadamard
2. Porta e Kontrolluar-NOT

Porta Hadamard merr një Qubit të vetëm dhe nxjerr një bit me një probabilitet të barabartë për t'u bërë 1 ose 0 [21].



Figura 18. Hadamard Gate [21]

Porta e Kontrolluar-NOT (Controlled-NOT) (CNOT) merr 2 Qubit dhe e kthen një Qubit nga një gjendje e ket 0 në ket 1 vetëm nëse kontrolli Qubit është ket 1. Përndryshe, ai e lë atë të pandryshuar.



Figura 19. CNOT Gate [21]

Ndërtimi i këtyre Portave kuantike përmes Qiskit do të ishte si në vazhdim. Fillimisht bëhet inicializimi i librarive përkatëse dhe krijimi i regjitrave të kubitëve dhe bitëve:

```
import qiskit as qk

# Creating Qubits
q = qk.QuantumRegister(2)

# Creating Classical Bits
c = qk.ClassicalRegister(2)
```

Kodi 1. Inicializimi i librarive dhe krijimi i regjitrave të kubitëve dhe bitëve

Regjistrat mbajnë një rekord të kubitëve dhe biteve që po përdoren nga qarku ynë. Duke pasur Kubitët dhe Bitët në duart tona, le të ndërtojmë qarkun tonë:

```
circuit = qk.QuantumCircuit(q, c)
```

Kodi 2. Ndërtimi i qarkut kuantik dhe ruajtja e tij në një variabël

Le të shtojmë disa porta në qarkun tonë për të manipuluar dhe punuar me Kubitët dhe Bitët tanë dhe në fund të masim Kubitët përfundimtarë:

```
# Hadamard Gate on the first Qubit
circuit.h(q[0])
# CNOT Gate on the first and second Qubits
circuit.cx(q[0], q[1])
# Measuring the Qubits
circuit.measure(q, c)
```

Kodi 3. Procesimi i Qubits përmes portave Hadamard dhe CNOT

Le të vizualizojmë qarkun tonë në mënyrë që të kemi një ide të përafërt të transformimeve të aplikuara në Qubitët tanë:

```
print (circuit)
```

Kodi 4. Printimi i qarkut kuantik

Nëse e printojmë këtë qark, mund të shohim një diagram qarku të printuar për qëllime lehtësie, i cili do të duket diçka si kjo:

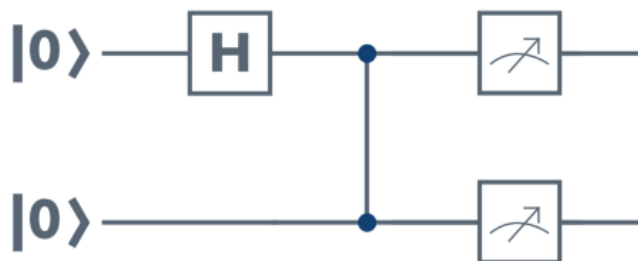
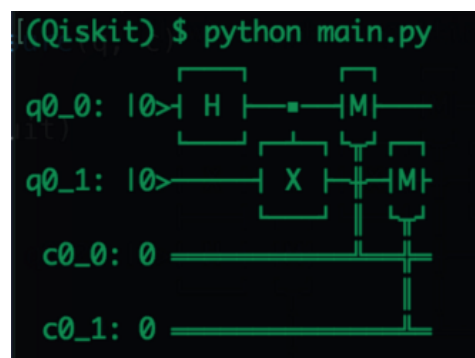


Figura 20. Rezultati i qarkut kuantik të koduar në Python

Ky do të ishte qarku më i thjeshtë kuantik që mund të ndërtojmë, por është e rëndësishme kuptimi i koncepteve bazike kuantike para se të fillojmë më probleme më të vështira.

5.3. Gjenerimi i numrave vërtet të rastësishëm - Shembulli i Monedhës

Një ndër problemet më të veçanta që kompjuterët kuantik mund të përdoren është gjenerimi i numrave vërtet të rastësishëm. Kjo është diçka që një kompjuter tradicional nuk mund ta bëjë pa u mbështetur në burime të jashtme. Kompjuterët tradicionalë mund të gjenerojnë vetëm numra që duken të rastësishëm, por në realitet, llogariten sipas rregullave fikse. Këta numra quhen pseudo të rastësishëm. Nëse gjenerojmë mjaft nga këta numra pseudo të rastësishëm, do të vërejmë se ata përfundimisht përsëriten. Për të gjeneruar numra vërtet të rastësishëm, një kompjuter tradicional mat ngjarjet e jashtme si zhurma atmosferike ose kohën e saktë kur shtypni tastet.

Kompjuterët kuantikë janë në thelb të rastësishëm, gjë që është mund të jetë edhe e keqe edhe e mirë. Nga njëra anë, mund të jetë shumë e vështirë të kuptojmë mënyrën se si një kompjuter kuantik arrin në një rezultat të caktuar për shkak të natyrës së tyre të rastësishme. Nga ana tjetër, fenomenet kuantike të rastësishme janë ato që i bëjnë këta kompjuterë kaq të fuqishëm.

Qarku ynë kuantik do të përbëhet nga vetëm një kubit i vetëm (bit kuantik) që përfaqëson monedhën tonë. Ne do të manipulojmë kubitin që të jetë në një mbivendosje prej 0 (koka) dhe 1 (bishti). *Ashtu si macja e Shrodingerit e vdekur dhe e gjallë në të njëjtën kohë, monedha jonë do të jetë koka dhe bishti në të njëjtën kohë.* Kur masim monedhën, kur hedhim një vështrim, monedha do të përfundojë rastësisht ose kokë ose bishtë me probabilitet 50%.

Së pari, ne instalojmë librarinë qiskit: `pip install qiskit`. Pastaj ne përdorim qiskit për të ndërtuar qarkun tonë kuantik.

```
import qiskit as qk

qk.IBMQ.load_account()

# Create circuit with 1 quantum and 1 classical bit
circuit = QuantumCircuit(1, 1)

# Apply Hadamard gate to quantum bit --> Superposition
circuit.h(0)

# Measure quantum bit and store result in classical bit
circuit.measure(0, 0)
```

Kodi 5. Instalimi i librarisë qiskit dhe përdorimi i saj për të ndërtuar qarkun kuantik

Në rreshtin 4, ne krijojmë qarkun tonë kuantik me një bit kuantik (monedhën tonë) dhe një bit klasik për të ruajtur rezultatin e matjes. Rreshti tjetër aplikojmë portën Hadamard në monedhën tonë, e cila e vendos atë në një mbivendosje të kokave dhe bishtave. Rreshti i fundit mat monedhën tonë dhe ruan rezultatin në bitin tonë klasik. Kodi nuk i ekzekuton operacionet, por thjesht përcakton se si duhet të duket qarku ynë kuantik. Ne mund të ekzekutojmë qarkun në kompjuterët kuantikë të IBM me kodin e mëposhtëm:

```
provider = IBMQ.enable_account(API_KEY)

quantum_computer = provider.get_backend("ibmq_armonk")

job = execute(circuit, quantum_computer, shots=1)

counts = job.result().get_counts()

result = "heads" if next(iter(counts.keys())) == "0" else "tails"

print(f"The quantum coin is: {result}")
```

Kodi 6. Pjesa e kodit të eksperimentit me monedhë përmes kompjuterëve kuantik

Programi fillimisht krijon një lidhje të vërtetuar me IBM Quantum API me çelësin e dhënë. Më pas specifikojmë se duam të ekzekutojmë qarkun tonë në kompjuterin kuantik me emrin "ibmq_armonk". Parametri "shots" specifikon se ne duam të ekzekutojmë qarkun vetëm një herë - ne duam të bëjmë vetëm

një rrokullisje monedhë. Pas kësaj, programi nxjerr rezultatin e rrokullisjes së monedhës nga objekti i rezultetit dhe e printon atë. Duke gjeneruar një rezultat real të rastësishëm.



Figura 21. Rezultati i programit të hedhjes së monedhës në Python

5.4. Cracking RSA with Shor's Algorithm

RSA është algoritmi standard kriptografik në internet i cili bazohet në problemin të faktorizimit të numrave prime. Algoritmi më i mirë në treg do të kërkonte kohë super polinomiale për të faktorizuar numrat prime [22], por kompjuterët kuantikë mund ta bëjnë këtë në një kohë polinomiale me ndihmën e algoritmit të Shor-it [5]. Algoritmi i Shor është i famshëm për faktorizimin e numrave të plotë në kohë polinomiale.

Në këtë shembull do të fokusohemi në pjesën kuantike të algoritmit të Shorit, i cili në fakt zgjidh problemin e gjetjes së periodave (Period Finding). Meqenëse një problem faktorizimi mund të shndërrohet në një problem për gjetjen e periudhës në kohë polinomiale, një algoritëm efikas i gjetjes së periodës mund të përdoret gjithashtu për të faktorizuar në mënyrë efikase numrat e plotë. Tani për tani është e mjaftueshme për të treguar se nëse mund të llogarisim periodën e $a^x \bmod N$ në mënyrë efikase, atëherë ne gjithashtu mund të faktorizojmë në mënyrë efikase [23].

Zgjidhja e Shor-it për gjetjen e periudhës ishte përdorimi i vlerësimit të fazës kuantike në operatorin unitar [23]:

$$U|y\rangle \equiv |ay \bmod N\rangle$$

Në këtë shembull do të zgjidhim problemin e gjetjes së periodës për $a=7$ dhe $N=15$. Ne ofrojmë qarqet për U ku:

$$U|y\rangle \equiv |ay \bmod 15\rangle$$

Fillimisht, importojmë libraritë e nevojshme të Python dhe Qiskit për të zhvilluar eksperimentin.

```
import matplotlib.pyplot as plt
import numpy as np
from qiskit import QuantumCircuit, Aer, transpile, assemble
from qiskit.visualization import plot_histogram
from math import gcd
from numpy.random import randint
import pandas as pd
from fractions import Fraction
print("Imports Successful")
```

Kodi 7. Importimi i librarive të Python për zhvillimin e eksperimentit të dekriptimit të RSA

Që të krijojmë U^x , ne do të aplikojmë operatorin unitar me fuqi të ndryshme në kubitët e synuar duke e kontrolluar atë me secilin nga kubitët e ndryshëm të matjes [22]. Në këtë rast implementimi i zgjidhjes së Shor-it për gjetjen e periodës do të ishte fillimisht funksioni `c_amod15`, i cili kthen portën e kontrolluar-U për a , të përsëritur $power$ herë.

```
def c_amod15(a, power):
    """Controlled multiplication by a mod 15"""
    if a not in [2,7,8,11,13]:
        raise ValueError("'a' must be 2,7,8,11 or 13")
    U = QuantumCircuit(4)
    for iteration in range(power):
        if a in [2,13]:
            U.swap(0,1)
            U.swap(1,2)
            U.swap(2,3)
        if a in [7,8]:
            U.swap(2,3)
            U.swap(1,2)
            U.swap(0,1)
        if a == 11:
            U.swap(1,3)
            U.swap(0,2)
        if a in [7,11,13]:
            for q in range(4):
                U.x(q)
    U = U.to_gate()
    U.name = "%i^%i mod 15" % (a, power)
    c_U = U.control()
    return c_U
```

Kodi 8. Implementimi i gjetjes së periodës nga Peter Shor

Implementimi i algoritmit të Shor-it gjithashtu kërkon aplikimin invers të Quantum Fourier Transform (QFT) në qubitët e matur [22].

```
def qft_dagger(n):
    qc = QuantumCircuit(n)
    for qubit in range(n//2):
        qc.swap(qubit, n-qubit-1)
    for j in range(n):
        for m in range(j):
            qc.cp(-np.pi/float(2**(j-m)), m, j)
        qc.h(j)
    qc.name = "QFT†"
    return qc
```

Kodi 9. Implementimi i Transformimit Furie Kuantik në Python

Pjesa e algoritmit të Shor-it që e bën kompleksitetin polinomial dhe që në fakt është pjesa ku fizika kuantike e bën të mundshme është se operatori unitar në këtë rast zbaton fuqizimin modular (modular

exponentiation) [22]. Kjo do të thotë se do të ishim duke kalkuluar periodën $a^2 \bmod N$, që përmes kompjuterëve kuantik bëhet shumë më e lehtë [23]. Përfundimisht implementimi i algoritmit të Shor-it duke përdorur funksionet e ndërtuara deri më tani do të merrte këtë formë:

```
def qpe_amod15(a):
    n_count = 8
    qc = QuantumCircuit(4+n_count, n_count)
    for q in range(n_count):
        qc.h(q) # Initialize counting qubits
    qc.x(3+n_count)
    for q in range(n_count): # Do controlled-U operations
        qc.append(c_amod15(a, 2**q),
                  [q] + [i+n_count for i in range(4)])
    qc.append(qft_dagger(n_count), range(n_count)) # Do inverse-QFT
    qc.measure(range(n_count), range(n_count))
    # Simulate Results
    aer_sim = Aer.get_backend('aer_simulator')
    t_qc = transpile(qc, aer_sim)
    qobj = assemble(t_qc, shots=1)
    result = aer_sim.run(qobj, memory=True).result()
    readings = result.get_memory()
    print("Register Reading: " + readings[0])
    phase = int(readings[0], 2) / (2**n_count)
    print("Corresponding Phase: %f" % phase)
    return phase
```

Kodi 10. Ndërtimi final i algoritmit të Shor-it

Mund të vëreni se në këtë pjesë të kodit bëhet edhe simulimi i rezultateve duke përdorur simuluesit e kompjuterëve kuantik të IBM, që në këtë rast është *aer_simulator*. Nëse caktojmë $N=15$, tani na mbetet që të përsëritim algoritmin derisa të gjendet të paktën një faktor prej 15.

```
N=15

a = 7
factor_found = False
attempt = 0
while not factor_found:
    attempt += 1
    print("\nAttempt %i:" % attempt)
    phase = qpe_amod15(a)
    frac = Fraction(phase).limit_denominator(N)
    r = frac.denominator
    print("Result: r = %i" % r)
    if phase != 0:
        guesses = [gcd(a**(r//2)-1, N), gcd(a**(r//2)+1, N)]
        print("Guessed Factors: %i and %i" % (guesses[0], guesses[1]))
        for guess in guesses:
```

```
if guess not in [1,N] and (N % guess) == 0:  
    print("*** Non-trivial factor found: %i ***" % guess)  
    factor_found = True
```

Kodi 11. Pjesa e kodit për faktorizimin e numrit $N=15$

Nëse ekzekutojmë kodin e mësipërm, pas disa përpjekjeve do të fitojmë faktorët e numrit $N=15$ që janë 3 dhe 5.

```
Attempt 1:  
Register Reading: 00000000  
Corresponding Phase: 0.000000  
Result: r = 1  
  
Attempt 2:  
Register Reading: 11000000  
Corresponding Phase: 0.750000  
Result: r = 4  
Guessed Factors: 3 and 5  
*** Non-trivial factor found: 3 ***  
*** Non-trivial factor found: 5 ***
```

Figura 22. Rezultatet e eksperimentit të faktorizimit të numrit $N=15$

Në këtë rast duke gjetur faktorët e një numri teoritikisht ne mund edhe të dekriptojmë algoritmin RSA duke gjetur çelësin privat përmes faktorizimit të çelësit publik, që përmes zgjidhjes së Shor-it kjo do të merrte një kohë polinomiale.

6. Diskutime dhe Konkluzione

6.1. Reflektimi kritik

Duke marrë parasysh të gjitha eksperimentet e treguara mund të shohim se çfarë fuqie të madhe kanë kompjuterët kuantik. Quantum Computing ka potencial shumë të madh dhe do të përdoren për të kryer detyra dhe për të trajtuar probleme që dikur konsideroheshin të pamundura për t'u zgjidhur siç janë gjenerimi i numrave të vertetë të rastësishëm si dhe faktorizimi i numrave prim.

Algoritmi RSA bazohet në parimin e vështirësisë së faktorizimit të numrave prim. Në vitin 2014, WraithX përdori një buxhet prej 7,600 dollarësh në Amazon EC2 dhe burimet e tij/saj për të faktorizuar një numër 696-bit [24]. Ne mund të thyejmë një çelës 1024-bit me një buxhet të konsiderueshëm brenda muajve ose një viti. Për fat të mirë, kompleksiteti i problemit të faktorizimit kryesor rritet në mënyrë eksponenciale me gjatësinë e çelësit. Pra, ne jemi mjaft të sigurt nga kompjuterët klasik pasi kemi kaluar tashmë në çelësat 2048-bit, ku dekriptimi i këtij çelësi do të merrte me mijëra vite por kjo nuk vlen për kompjuterët kuantik sepse faktorizimi i këtyre numrave do të mund të bëhej në një kohë polinomiale [25].

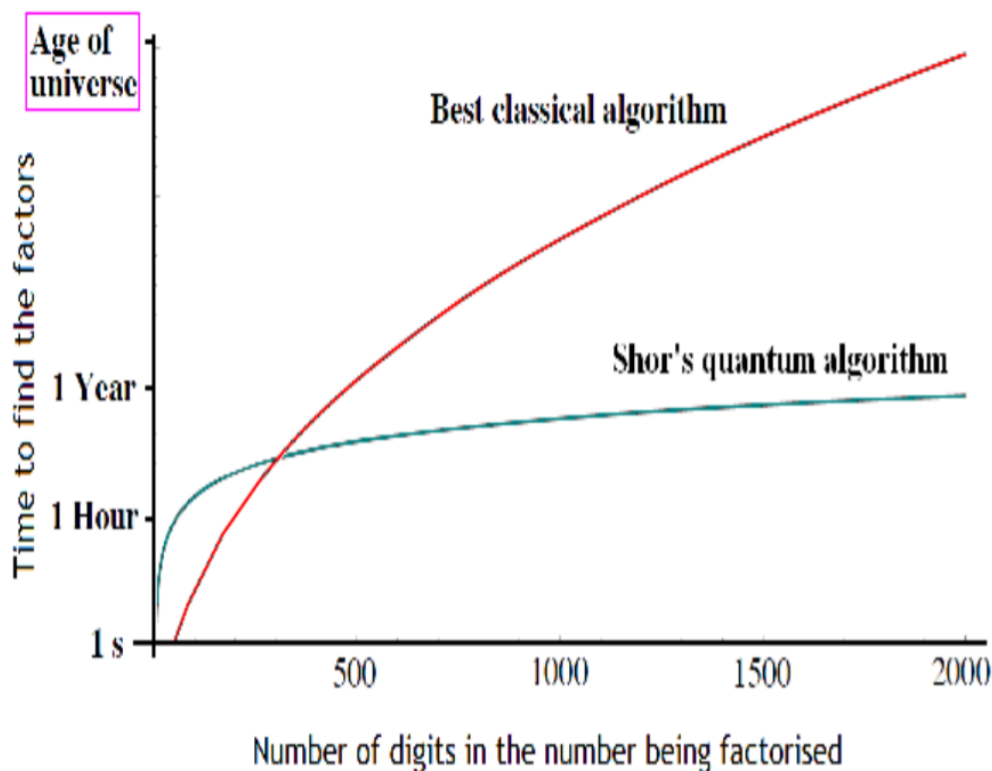


Figura 23. Koha e faktorizimit me rritjen e inputit, dallimi në mes të algoritmit klasik dhe atij të Shor-it [25]

Mund të vërejmë se në eksperimentin e zhvilluar për dekriptimin e RSA përdoren vetëm 8 qubit për të ruajtur rezultatet pasi që jemi duke gjetur faktorizimin e një numri të vogël të plotë që është 15.

Më sipër thamë se tani standardi i algoritmit RSA është përdorimi i çelësave 2048-bit dhe në mënyrë që realisht të dekriptojmë një RSA enkriptim do të na duhej një kompjuterë kuantik më shumë se shumë qubit. Gjendja e tanishme është ajo që kompjuterin kuantik më të madh në botë të zhvilluar nga IBM e kemi me vetëm 50 kubit, që nuk do të ishin të mjaftueshme për thyerjen e enkriptimit RSA të tanishëm.

Ne mund të përfundojmë se përkundër nevojës së madhe të kompjuterëve kuantik si dhe potencialit të tyre të madh, realiteti qëndron se kompjuterët kuantikë nuk do të zëvendësojnë kurrë kompjuterët tanë shtëpiak. Ata janë goxha të ndryshëm nga kompjuterët klasikë dhe kanë stilin e tyre të llogaritjes. Ata nuk mund të jenë kurrë në gjendje të mposhtin kompjuterët normalë në shumicën e problemeve që ne zgjidhim me kompjuterët klasikë. Kompjuterët kuantik nuk do të mund të jenë të qasshëm nga të gjithë dhe do të ishte ide e keqe të përdoren për pune ordinere, të përditshme tonat, probleme të cilat zgjidhen në mënyrë perfekte nga kompjuterët që veç i kemi në dispozicion. Qëllimi i përdorimit të këtyre makinave do të mund të ishte në kriptografi duke u munduar të thyejmë algoritmet e përdorura deri më tani. Realiteti i thyerjes së këtyre algoritmeve tani për tani është larg, siç e cekëm më lart se nuk kemi qubit të mjaftueshëm për ta bërë atë, por nëse diçka si ligji i Moores zbatohet edhe për kompjuterët kuantikë, kjo do të arrihet shumë shpejt.

6.2. *Përmisimet e mundshme*

Duke marrë parasysh se Quantum Computing është një temë e re jo vetëm në vendin tonë por edhe globalisht, realizimi i këtij punimi ishte mjaft sfidues për mua. Fillisht ishte e nevojshme njohuria e disa fenomeneve bazike të fizikës kuantike për të kuptuar thelbin e funksionimit të kompjuterëve kuantik dhe pastaj duke hyrë më thellë në algoritmet kuantik, puna kërkimore bëhej gjithnjë e më e vështirë.

Fatmirësisht nuk ka pasë mungesë të informacionit në këtë drejtim dhe kam pasur mundësinë të përdorë vegla të zhvilluara nga gjigandë kompjuterik si IBM për të realizuar me sukses eksperimentet e mia për programimin e këtyre kompjuterëve.

Megjithatë hapësira për përmisime është e madhe, Quantum Computing paraqet një temë shumë më të gjerë se sa kam mundur unë të paraqes në këtë punim. Mundësia e shtjellimit të algoritmeve të tjera kuantike është më e gjerë dhe secila prej tyre paraqet një revolucion të ri në botën e IT-së. Sugjerimi im do të ishte që të ketë punime më shumë rreth Kompjuterikës Kuantike, ku thapësira për implementimin e algoritmeve të tjera kuantike siç janë Algoritmi i Glover-it apo Problemi Deutsch-Jozsa, do të mund të ishte një pjesë shumë atraktive për studentët tanë.

Gjithë kjo punë për mua ishte një mundësi shumë e mirë që të mësoj diçka të re për profesionin tim dhe të zhvillohem më tej në karrierën time si inxhinier i kompjuterikës, qëllime të cila do të vlejnjë gjithmonë për mua.

Bibliografia dhe referencat

- [1] “Moore's Law: Transistors per microprocessor”, January 2022. Gjendet në: <https://ourworldindata.org/grapher/transistors-per-microprocessor>.
- [2] E. C. G. Sudarshan, The promise of quantum computing, 2003.
- [3] C. Lee, “How Quantum Computing Works and Why It’s Important”, 23 August 2017. Gjendet në: <https://medium.com/@laserboy/how-quantum-computing-works-and-why-its-important-c596376209d5>.
- [4] “The exponential function”, Gjendet në: https://mathinsight.org/exponential_function.
- [5] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, 1994.
- [6] N. Gisin, G. Ribordy, W. Tittel dhe H. Zbinden, Quantum cryptography, 2002.
- [7] J. Roell, “The Need, Promise, and Reality of Quantum Computing”, 1 February 2018. Gjendet në: <https://towardsdatascience.com/the-need-promise-and-reality-of-quantum-computing-4264ce15c6c0>.
- [8] G. E. Moore, Cramming more components, 1965.
- [9] “Transistors Will Stop Shrinking in 2021, Moore’s Law Roadmap Predicts The last ITRS report forecasts an end to traditional 2D scaling”, 22 July 2016. Gjendet në: <https://spectrum.ieee.org/transistors-will-stop-shrinking-in-2021-moores-law-roadmap-predicts>.
- [10] P. Dirac, The Principles of Quantum Mechanics (2nd ed.), 1947.
- [11] M. Born, The Born-Einstein letters: correspondence between Albert Einstein and Max and Hedwig Born from 1916–1955, 1971.
- [12] E. Schrödinger, Discussion of probability relations between separated systems, 1935.
- [13] M. A. Nielsen dhe I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2010.
- [14] U. o. Waterloo, “INSTITUTE FOR QUANTUM COMPUTING”, Gjendet në: <https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/what-qubit>.
- [15] K. S. B. Hasan, “Towards Data Science”, 8 April 2019. Gjendet në: <https://towardsdatascience.com/understanding-quantum-computers-ecb9d375b46f>.
- [16] J. Roell, “Towards Data Science”, 26 February 2018. Gjendet në: <https://towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640>.
- [17] R. V. M. A. G. F. P. L. M. J. K. T. D. L. a. Y. Y. N. Cody Jones, Layered Architecture for Quantum Computing, 2012.
- [18] A. O. Pittenger, An Introduction to Quantum Computing Algorithms, 2001.
- [19] P. S. R. J. Aditya, Quantum Cryptography, 2018.
- [20] S. Kak, A Three-Stage Quantum Cryptography Protocol, 2006.
- [21] R. Anand, “Building Your Own Quantum Circuits in Python”, 2019. Gjendet në: <https://towardsdatascience.com/building-your-own-quantum-circuits-in-python-e9031b548fa7>.
- [22] “Shor's Algorithm - Qiskit”, January 2022. Gjendet në: <https://qiskit.org/textbook/ch-algorithms/shor.html>.
- [23] M. Hayward, Quantum Computing and Shor’s Algorithm, 2005.
- [24] “QC — Cracking RSA with Shor’s Algorithm”, 13 December 2018. Gjendet në: <https://jonathan-hui.medium.com/qc-cracking-rsa-with-shors-algorithm-bc22cb7b7767>.
- [25] S. R. Sihare dhe D. V. V. Nath, Analysis of Quantum Algorithms with Classical, MECS, 2017.

