Potencijali upotrebe kvantnih računala u polju kriptologije

Markušić-Novosel, Kristijan

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2019./ 2020.

Kristijan Markušić-Novosel

Potencijali upotrebe kvantnih računala u polju kriptologije

Završni rad

Mentor: Dr. sc. Vjera Lopina

Zagreb, lipanj 2020.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

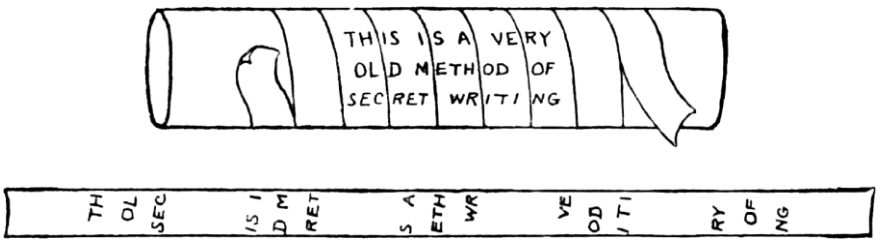
_____

(potpis)

Sadržaj

1. Uvod

Ljudska potreba za čuvanjem tajni, privatnom komunikacijom i zaštitom znanja stara je gotovo koliko i čovjek sam. Ljubavnici su razmjenjivali pisma pisana nevidljivom tintom od soka limuna ili mlijeka, Indijanci su kao sredstvo komunikacije koristili dimne signale, a ishodi mnogih povijesnih bitaka ovisili su o kuririma čiji je zadatak bio prenijeti poruku od točke A do točke B. Tijekom povijesti razvijene su mnoge kriptografske tehnike, a zapisi i ostaci najranijih sežu još iz doba drevnih civilizacija Mezopotamije i Egipta. Jedan od takvih sustava je skitala – prvi kriptografski sustav upotrabljan u vojne svrhe. Skitala se sastoji od cilindra oko kojeg je omotana vrpca od kože ili sličnog materijala koja na sebi sadrži poruku. Poruka može biti isčitana isključivo uz posjedovanje cilindra unaprijed određenog promjera. Ovaj sustav koristili su spartanski generali u 5. stoljeću prije Nove ere.



Slika 1. Scytale. Ohaver M.E. Solving cipher secrets. // Flynn's, 1924.

Britanski kriptoanalitičari su u vrijeme Drugog svjetskog rata koristili Colossus - prvo programabilno digitalno računalo, kako bi dešifrirali i iščitavali tajne poruke njemačke vojske. Uz Colossus su za dešifriranje poruka dizajnirana i druga računala, poput američkog ENIAC-a. Izum Turingovog stroja i probijanje njemačkog kriptološkog sustava Enigma označio je svojevrsni presedan za budućnost informacijskog ratovanja, ali i kriptološku znanost općenito. Dvadeset godina kasnije prvo računalo za osobnu upotrebu postaje komercijalno dostupno. To računalo temelji se na tehnologijama i metodama koje se upotrebljavaju i danas, poput korištenja tranzistora, dioda i otpornika za prijenos informacija, a koristila ga je NASA pri

planiranju slijetanja na Mjesec. Razvoj Interneta uzrokovao je preseljenje velikog dijela komunikacije u digitalnu domenu. Eksponencijalno ubrzani razvoj informacijskih tehnologija u pitanje dovodi pouzdanost široko upotrebljavanih digitalnih komunikacijskih kanala i predstavlja izazove za daljni razvoj znanstveno-istraživačkog područja kriptologije.

Velik dio danas korištenih algoritama i protokola temelji se na nedokazanim matematičkim pretpostavkama, a razvoj dovoljno snažnog super-računala mogao bi ozbiljno ugroziti njihovu sigurnost. Stoga se posljednjih desetljeća razvijaju nove grane kriptologije – kvantna kriptologija i post-kvantna kriptologija. Cilj je protokole temeljene na matematičkim zakonitostima barem dijelom zamijeniti onima temeljenim na fizičkim i mehaničkim fenomenima i tako informacije zaštititi zakonima prirode.

Osnovne tehnološke komponente u informacijskoj eri u kojoj se nalazimo, poput tranzistora, integriranih strujnih krugova i lasera, direktne su aplikacije kvantne mehanike na makroskopskom nivou. Prema Mooreovom zakonu, broj tranzistora u računalnim procesorima udvostručuje se svake dvije godine. Međutim, zbog nezaobilaznih problema pri proizvodnji taj zakon prestaje vrijediti. Uslijed postupnog fizičkog smanjivanja veličine komponenti, mikroskopski kvantno-mehanički fenomeni počinju utjecati na njihov rad. Jedna od paradigmi alternativnih klasičnom računarstvu kojom bi se ove prepreke mogle premostiti je paradigma znanosti o kvantnoj informaciji, čiji je cilj iskoristiti kvantnomehaničke efekte pri obradi, manipulaciji i prijenosu informacija. Razvoj kvantnih informacijskih tehnologija zaokuplja pažnju mnogih svjetskih znanstvenika, ali njihova praktična implementacija podrazumijeva izgradnju izuzetno skupe infrastrukture, kao i razvoj kvantnih algoritama namijenjenih rješavanju praktičnih problema. Prvi tvrdi disk kompanije IBM, sa memorijom od 5 megabajta, težio je jednu tonu i koštao preko 50.000 dolara, što je neusporedivo sa današnjim standardima. Ako se trend razvoja koji prati klasična računala prenese i na kvantne tehnologije, možemo biti relativno sigurni da će kvantna računala, odnosno računala osnažena kvantnim sklopovljem uskoro postati dio tehnološke stvarnosti.

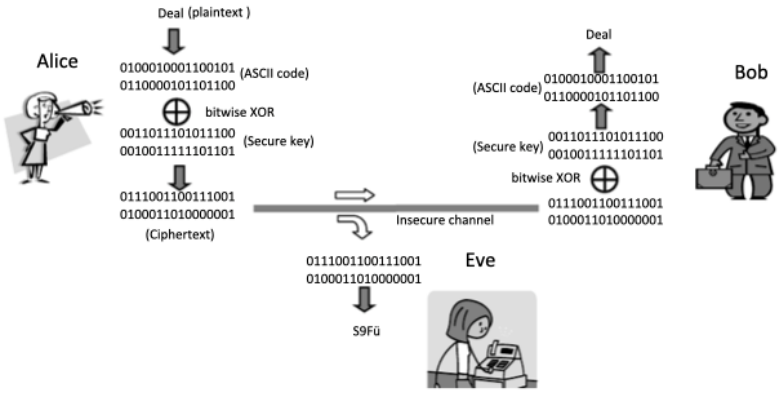
Kvantna fizika, kao jedna od najuspješnijih znanstvenih teorija iz temelja mijenja ljudsko poimanje prirodnog svijeta i svakodnevnog života. Kvantno računarstvo je znanstveno područje koje se bavi proučavanjem upotrebe kvantnomehaničkih efekata, poput superpozicije i prepletenosti prilikom obrade informacija. Područje kvantnog računarstva u koherentnu cjelinu spaja ideje iz područja teorije informacija, računarstva i kvantne fizike. Kako bismo

shvatili ideju iza koncepata kvantne fizike, valja se u jednu ruku odreći klasičnog načina razmišljanja. Postoji niz pravila i fenomena u kvantnoj fizici koje nije moguće razumjeti kroz paradigmu klasične fizike, od kojih su tri od osobite važnosti pri proučavanju veze između kvantne mehanike i kriptologije: "no-cloning" teorem prema kojem nije moguće kreirati kopiju nepoznatog kvantnog stanja, nemogućnost mjerenja stanja sustava bez njegovog remećenja, te Heisenbergov princip neodređenosti, prema kojem nije moguće istovremeno mjerenje komplementarnih varijabli (poput položaja čestice u sustavu i njezine brzine kretanja) s visokom preciznošću. Već na prvi pogled vidljiva je sličnost između ova tri fenomena - sva tri govore o onom što nije moguće. Iako se to može činiti kao svojevrsni hendikep kvantne teorije, stručnjaci iz područja kriptografije ističu načine na koje se upravo ova svojstva mogu iskoristiti u svrhu pospješivanja sigurnosti i privatnosti komunikacijskih sustava.

2. Klasična kriptografija

Umijeće stvaranja i razbijanja kodova ima veliku ulogu u ljudskoj povijesti. Vjeruje se da su kriptoanalitički pothvati saveznika, poput probijanja njemačkog kriptografskog sustava Enigma skratili II. svjetski rat za dvije godine. Kriptografske metode enkripcije tradicionalno se dijele u dvije skupine: transpozicijske i supstitucijske. Transpozicijske metode podrazumijevaju obradu teksta poruke određenom permutacijom. Primjer takvog sustava je ranije spomenuti sustav skitala. Kod supstitucijskih metoda vrijednost znaka i slova se mijenja, ali njihov redoslijed u poruci ostaje nepromijenjen. Takav sustav koristio je Julije Cezar za razmjenu poruka vojnog karaktera. U njegovim porukama svako je slovo bilo zamijenjeno slovom udaljenim tri mjesta u abecednom nizu. Slovo A tako bi postalo slovo D, slovo B slovo E i tako dalje. Danas, kada su internet općenito i elektroničko poslovanje sve popularniji, kriptografija postaje esencijalni dio svakodnevice. Uz dobro razvijeni kriptografski protokol, možemo biti relativno sigurni da su naše osobne informacije zaštićene prilikom provođenja bilo kakvih elektronskih transakcija. Evolucija kriptografije zasnovana je na vječnim bitkama između kriptografa i kriptoanalitičara, među kojima se nalaze neki od najsvjetlijih umova na svijetu. Čim je postojeći kod probijen, zadaća kriptografa je osmisliti i implementirati novi protokol koji omogućava nastavak sigurne komunikacije, što potencira razvitak novih metoda za njihovo probijanje od strane kriptoanalitičara. Apsolutni cilj kriptografije je razvitak potpuno sigurne sheme kodiranja koja je u potpunosti zaštićena od napadača sa neograničenom moći obrade podataka. Taj cilj je u teoriji postignut kada je Gilbert Vernam izumio metodu jednokratnog ključa "One Time Pad", odnosno OTP 1917. godine. Kao i kod mnogih drugih modernih kriptografskih sustava u OTP se prilikom procesa enkripcije i dekripcije koristi siguran kriptografski ključ. Enkripcijski algoritam je javno dostupan, a sigurnost kriptografskog sustava zajamčena je tajnošću ključa. OTP je enkripcijski algoritam gdje je osnovna poruka, koja je razumljiva svima, kodirana tajnim nasumično generiranim ključem koji je iste duljine kao i sama poruka. Primatelj poruke koristi isti ključ kako bi dešifrirao poruku. Grafički prikaz ovog protokola prikazan je na slici 1. Ako uzmemo u obzir da se ključ koristi samo jedanput, apsolutnu sigurnost OTP protokola dokazao je Claude Shannon.

Iako je OTP u teoriji u potpunosti sigurna metoda, postoji problem kod njene uporabe u praksi: jednom kada osoba A kao pošiljatelj i osoba B kao primatelj poruke iskoriste svoj unaprijed generirani ključ, sigurna komunikacija je prekinuta sve dok se ne generira novi ključ. Rješenje ovog problema uključuje dva zadatka neizvediva korištenjem principa klasične fizike: generaciju istinski nasumičnih brojeva i bezuvjetno sigurnu distribuciju ključa nesigurnim kanalom.



Slika 2. Grafički prikaz OTP protokola. Qi, B., Qian, Li., Lo, H. A brief introduction of quantum cryptography for engineers. // Arxiv

Deterministička priroda klasične fizike isključuje postojanje istinski nasumičnih brojeva u svojim kaotičnim, ali klasičnim procesima. Ali istinski nasumični brojevi mogu se generirati osnovnim kvantnim procesima. U svijetu u kojem su informacije kodirane na klasičan način ne postoji siguran proces distribucije ključa nesigurnim kanalom. Kada bi to bilo moguće, ne bi bilo potrebe za generiranjem ključa već bi se poruke mogle prenositi direktno. Osnovni razlog je taj što se u klasičnoj fizici informacije mogu kopirati odnosno klonirati. Nije moguće dokazati da ključ etabliran putem nesigurnog kanala nije kopiran od strane potencijalnog prisluškivača.

Jedini način za premošćivanje ovog problema, koji je ujedno izuzetno neisplativ, bio bi slanje pouzdanog kurira kao što su to nekad bili golubovi pismonoše. Zbog ovog problema distribucije ključa, protokoli poput OTP-a koriste se samo u slučajevima gdje je apsolutna sigurnost prioritet. Ali čak i OTP protokol može biti kompromitiran njegovom nepravilnom implementacijom. Za vrijeme hladnog rata KGB-ovi špijuni rutinski su koristili OTP za

kodiranje prioritetnih tajnih poruka. Neke od nasumično generiranih ključeva Sovjeti su zabunom koristili više puta. To je omogućilo američkim i britanskim kriptoanalitičarima da dešifriraju neke poruke od izuzetne važnosti, poput onih koje su otkrile prisutnost sovjetskih špijuna u nacionalnim laboratorijima u Los Alamosu.

Alternativa simetričnim kriptografskim sustavima jesu asimetrični kriptografski sustavi, odnosno sustavi sa javnim ključem, gdje se različiti ključevi koriste za šifriranje i dešifriranje. Kod većine modernih kriptografskih sustava poput "Data Encryption Standard" (DES) i "Advanced Encryption Standard (AES), kraći ključevi koriste se za enkripciju dugačkih poruka. Ti protokoli nažalost nisu sigurni poput OTP. Kriptografski algoritmi s javnim ključem izumljeni su kako bi se eliminirao problem distribucije ključa, a najpoznatiji i najzastupljeniji od njih je RSA koji su izumili Ron Rivest, Adi Shamir i Leonard Adleman prema čijim inicijalima je i sam algoritam dobio naziv.

RSA funkcionira na sljedeći način: primatelj poruke (osoba B) priprema dva kriptografska ključa - javni i privatni ključ. Osoba B potom odašilje javni ključ kanalom te je on dostupan bilo kome tko prima informacije kroz njega. Pošiljatelj poruke (osoba A) kodira poruku tim javnim ključem i šalje ju javnim kanalom. Ovaj algoritam dizajniran je na način da se poruka šifrirana javnim ključem može dešifrirati samo uz poznavanje odgovarajućeg privatnog ključa. Ovakav sustav može se vizualizirati kao svojevrsni lokot i ta analogija može biti od pomoći pri dočaravanju načina na koji on funkcionira. Bilo tko može zaključati otvoreni lokot, ali samo osoba koja ima odgovarajući ključ može ga ponovo otključati. Osoba A može proizvesti mnogo kopija otvorenog lokota koji predstavljaju javni ključ u ovom sustavu. Osoba B koja želi osobi A poslati privatnu poruku primit će svoj otvoreni lokot. Jednom kada se lokot zaključa, samo osoba A može ga ponovno otključati budući da jedino ona ima pravi privatni ključ. Posljednjih desetljeća ovakvi sustavi postali su izuzetno popularni i danas se veliki dio internetske sigurnosti temelji na njima. Iako se procesi kriptografskih algoritama s javnim ključem u teoriji čini jednostavnim, bilo je potrebno nekoliko godina da se pronađu matematičke funkcije koje odgovaraju svim sigurnosnim kriterijima, a kod RSA i sličnih sustava to je jednosmjerna funkcija faktoriziranja brojeva. I na prvi pogled jasno je da je puno lakše izračunati umnožak dvaju brojeva nego rastaviti rezultat množenja na faktore. Vrijeme potrebno za izvršavanje tog zadatka povećava se eksponencijalno s brojem ulaznih bitova. Problem kod ovakvih sustava je što se njihova sigurnost temelji na nedokazanim matematičkim pretpostavkama. Na primjer, sigurnost RSA bazirana je na pretpostavci da ne postoji efikasan način za rastavljanje velikih

brojeva na proste faktore. Ipak, ta pretpostavka nije dokazana unatoč brojnim pokušajima. S obzirom da je RSA sam po sebi bio neočekivano otkriće, ne treba isključiti mogućnost da bi netko mogao otkriti efikasan algoritam za faktorizaciju i tako ugroziti mnoge javne kriptografske sustave. Brz razvoj tehnologije i tehnika proizvodnje kvantnih računalnih sustava predstavlja problem za sigurnost RSA i sličnih sustava u bliskoj budućnosti. Teorijska superiornost kvantnog računala u ovoj disciplini temeljena je na Shorovom kvantnom algoritmu. Zanimljiv je podatak da je cijelo desetljeće prije razvitka ideje razbijanja sigurnosti kriptografskih sustava korištenjem kvantnog računala, pronađeno rješenje za takav "kvantni napad" - kvantna distribucija ključa (QKD). Temeljena na osnovnim principima kvantne fizike, QKD predstavlja bezuvjetno siguran način distribucije ključa nesigurnim kanalom. Stoga bi povratak na korištenje simetričnih kriptografskih sustava ojačanim uspješno implementiranim kvantno mehaničkim fenomenima mogao biti najisplativije i najsigurnije rješenje.

3. Kvantno računalo

Pionirom kvantnog računarstva smatra se Richard Feynman, poznati američki teorijski fizičar. Feynman je osamdesetih godina prošlog stoljeća počeo istraživati načine za simulaciju kvantnih sustava pomoću drugih kvantnih sustava umjesto klasičnim računalom i promišljao je kako realizirati koncepte klasičnih računala, poput binarnih brojeva, upotrebom kvantnih sustava. Britanski fizičar David Deutsch je 1985. godine opisao koncepte univerzalnog kvantnoga računala. Deutsch je pokazao da je upotrebom univerzalnog kvantnoga računala moguće simulirati bilo koji fizički sustav, te je opisao koncept jednostavnih kontroliranih operacija nad kvantnomehaničkim sustavom kojima je moguće utjecati na evoluciju tog sustava. Te su jednostavne operacije u biti kvantna vrata koja su analogna logičkim vratima kod klasičnih računala. Danas Deutschov model predstavlja osnovu za izradu kvantnih algoritama i proučavanje računalne snage kvantnih računala. Kvantno računalo je uređaj za obradu informacija koji prilikom izvršavanja operacija nad podacima koristi kvantnomehaničke efekte poput superpozicije i prepletenosti. Osim teorijskih aspekata vezanih uz kvantno računarstvo kojima se bave teorijski fizičari, eksperimentalni fizičari pokušavaju izgraditi prvo kvantno računalo većih razmjera. Velik problem u izgradnji kvantnoga računala većih razmjera predstavlja kvantna dekoherencija, odnosno utjecaj okoline na kvantno računalo. Kvantna dekoherencija narušava stanje kvantne informacije unutar računala, a njeno izbjegavanje još uvijek je teško fizički izvedivo. Današnji kvantni uređaji zahtijevaju operacijske temperature bliske apsolutnoj nuli, tako da se kao obećavajući poslovni model ističe usluga kvantnog računarstva u oblaku. Takav oblik usluge pretpostavlja pitanje pouzdanosti rezultata primljenih iz oblaka ako se komunikacija vrši putem internetske veze, čijem komunikacijskom kanalu druga kvantna računala potencijalno mogu pristupiti. Istraživači su trenutno fokusirani na razvoj masovne proizvodnje više-kubitnih procesora kako bi se omogućila svojevremena konstrukcija kvantnih računala sa više milijuna kvantnih bitova. Jednako je važno stvoriti kvantni ekosustav sastavljen od standardiziranog kvantnog programskog jezika, kompajlera i sloja apstrakcije kvantnog hardware-a, koji različitim odredišnim platformama omogučava kompajliranje unificiranog kvantnog programa kao što je to slučaj kod klasičnih računala. Kod razvoja kvantnih računala potrebno je posvetiti posebnu pažnju detektiranju i ispravljanju pogrešaka, s obzirom da su sva trenutno dostupna kvantna rješenja još uvijek relativno nepouzdana za korištenje. Prije kraja dvadesetog stoljeća vodeći stručnjaci iz područja kvantnog računarstva vjerovali su kako su kvantna stanja previše

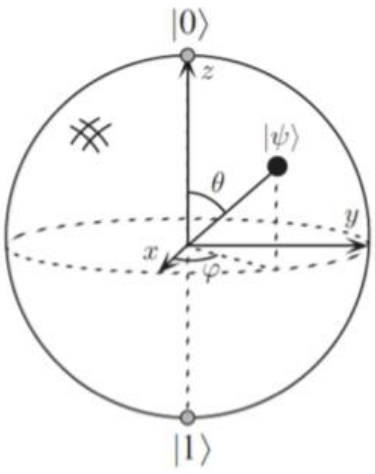
nestabilna i podložna akumulaciji pogrešaka da bi kvantni algoritmi funkcionirali na dovoljno visokoj razini. Taj stav vrlo se brzo promijenio izumom kodova i teorema za kvantno ispravljanje pogrešaka. Tim teoremima dokazano je da, ukoliko se količina pogrešaka po logičkoj operaciji (kvantnim vratima) snizi do određene razine, proizvoljno duge kvantne operacije mogu biti izvršene pouzdano uz pravilnu implementaciju metoda ispravke pogrešaka. Tijekom godina eksperimentalni znanstvenici postupno razvijaju poboljšani kvantni hardware sa sve manjom stopom pogreške po kvantnim vratima. Istodobno teorijski istraživači razvijaju nove procedure kvantne ispravke pogrešaka sa većom tolerancijom na pogreške. Eksperimentima u proizvodnji kvantnih vrata korištenjem tehnologija ionskih zamki i sklopova supervodiča demonstrirana je funkcija kvantnog sklopovlja sa stopom pogreške daleko nižom od gornje granice. Ta postignuća uzrokovala su znatno povećan interes i investicije od strane vladinih organizacija, ali i mnogih privatnih kompanija.

2011. godine tvrtka D-wave systems proizvela je komercijalno dostupan kvantni procesor sa 128 kvantnih bitova. Tim predvođen Matthiasom Troyerom i Danielom Lidarom došao je do zaključka da ovaj procesor koristi kvantnomehaničke efekte, ali ne rješava praktične probleme brže u odnosu na klasična računala. Cijena ovakvog procesora bila je oko 10 milijuna dolara.

Google je 2013. godine osnovao laboratorij za kvantnu umjetnu inteligenciju, opremljen kvantnim računalom sa 512 kvantnih bitova istog proizvođača. Svrha ovog laboratorija bila je okupiti znanstvenike koji za cilj imaju poboljšavanje računalnog učenja upotrebom kvantnog računala.

3.1. Kvantni bit

Kvantni bit (eng. *qubit*) je kvantno mehanički analog klasičnom bitu. Kod klasičnog računarstva informacije su kodirane u bitovima, gdje svaki bit može imati jednu od dvije vrijednosti - nula ili jedan. Kvantni bit je kvantni sustav na dvije razine, a njegova dva osnovna stanja obično označavamo kao |0⟩ i |1⟩. Kvantni bitovi mogu postojati u stanju |0⟩, |1⟩, ili (za razliku od klasičnih bitova) u linearnoj kombinaciji tih dvaju stanja. Taj fenomen naziva se superpozicija. Kako bismo što bolje razumjeli razliku između klasičnih bitova i qubita kao metoda vizualizacije, koristi se imaginarni raspon odnosno prostor mogućih vrijednosti koje oni mogu nositi. Kod klasičnih bitova taj prostor lako je zamisliti kao sklopku s dvije vrijednosti od kojih jedna predstavlja vrijednost 0, a druga vrijednost 1. Svaki bit postoji u jednom od ta dva stanja. Kvantni bit pak, hipotetski rečeno, postoji na površini sferičnog oblika, a njegova je vrijednost određena koordinatama na toj apstraktnoj sferi, upravo kao što bismo odredili određenu geografsku lokaciju na planeti. Sjeverni i južni pol sfere obično se izdvajaju te su im dodjeljene vrijednosti 0 i 1, što odgovara vrijednostima koje nalazimo kod klasičnih bitova.



Slika 3. Vizualizacija vektora stanja kvantnoga bita sa kompleksnim amplitudama. Qubit. // Wikipedija: slobodna enciklopoedija. 14.10.2020. Dostupno na: https://en.wikipedia.org/wiki/Qubit

Iako vrijednost kvantnog bita može ležati bilo gdje na sferi, sam čin mjerenja njegovog stanja postavit će njegovu vrijednost na jedan od polova, što znači da kvantni bit u tom slučaju prenosi informaciju ekvivalentu klasičnom bitu. Ipak, iz ovog kvantno mehaničkog fenomena lako je zaključiti koliki potencijal leži u korištenju kvantnih sustava u polju kriptologije, imajući na umu da su originalna nepromatrana stanja kvantnih bitova zaštićena zakonima prirode. Individualni kvantni bit nije moguće kopirati. To njegovo svojstvo postaje od izuzetne koristi kada se želi sačuvati tajnost informacije.

Različiti fizički sustavi mogu se koristiti za kodiranje kvantnih bitova, a za njihovu proizvodnju potrebno je detaljno poznavanje tih platformi. Apstraktno viđenje kvantnih bitova kao sfere kvantnih stanja omogućava znanstvenicima da ih pri proučavanju i eksperimentiranju tretiraju na univerzalan način.

Krajem 2012. godine australski znanstvenici su uspjeli realizirati kvantni bit pomoću jednog atoma, a u Vancouveru je osnovana prva programska tvrtka 1QBit koja proizvodi programska rješenja za kvantna računala uključujući ona za „D-Wave Two“ procesor.

3.2. Kvantna prepletenost

Kvantna prepletenost odnosno kvantno sprezanje je fizički resurs kojeg dijele kvantni sustavi i može se mjeriti. Za par ili grupu čestica kažemo da se nalaze u sprezi kada kvantno stanje svake pojedine čestice nije moguće opisati neovisno o stanju ostalih čestica. Kvantno stanje sustava u cjelini može se definirati, ali kvantno stanje njegovih djelova ne. Kada se dva kvantna bita nalaze u sprezi između njih postoji posebna veza koja postaje jasna iz rezultata mjerenja vrijednosti njihovih stanja. Rezultat mjerenja stanja svakog kvantnog bita može biti 0 ili 1, a taj rezultat direktno će utjecati na stanje kvantnog bita s kojim se nalazi u sprezi čak i kada su oni udaljeni kilometrima jedan od drugog.

1964. godine, John Stewart Bell objavljuje rad s naslovom "On the Einstein-Podolsky-Rosen Paradox" i razvija Bellov teorem. Veza između kriptografije i Bellovog teorema nije vidljiva na prvi pogled. Stoga valja detaljnije proučiti EPR protokol s obzirom da je i sam Bellov teorem nastao kao svojevrsna reakcija na njega. 1935. godine Albert Einstein, Boris Podolsky i Nathan

Rosen (zajedno EPR) objavljuju rad s naslovom „*Can quantum-mechanical description of physical reality be considered complete?*“ kojim su pod upitnik stavili kompletnost teorije kvantne mehanike i opisali "EPR paradoks" kojim su to htjeli pokazati. U svom radu krenuli su od dvije pretpostavke:

Realnost - Mjerena vrijednost važeća je i prije kvantno-mehaničkog mjerenja.

Lokalnost - Čin mjerenja jedne čestice ne može utjecati na postojeću realnost druge čestice na udaljenoj lokaciji.

U kvantnoj mehanici pretpostavke su formulirane kroz termin vjerojatnosti. Na primjer, vjerojatnost da će se elektron naći u određenom dijelu prostora ili vjerojatnost da će njegov spin biti u smjeru prema gore ili dolje. Ipak, prije dokazivanja Bellovog teorema, postojala je ideja da elektron ima definitivno određenu poziciju i spin te da je mana kvantne mehanike nemogućnost preciznog određivanja tih vrijednosti. Trio EPR iznio je teoriju da bi neka, do tada nepoznata ali validnija teorija (teorija skrivene varijable) mogla precizno predvidjeti spomenute vrijednosti, a opet u isto vrijeme odgovarati probabilističkim odgovorima koje daje kvantna mehanika. Kada bi teorija skrivene varijable bila istinita, a te varijable ne bi bile opisane kvantnom mehanikom, to bi značilo da je teorija kvantne mehanike nepotpuna. John Stewart Bell osmislio je misaoni eksperiment koji je omogućio da se eksperimentalno utvrdi je li kvantna mehanika odnosno "EPR paradoks" doista način na koji priroda funkcionira ili postoje skrivene varijable, kako su u svojem radu tvrdili Einstein, Podolsky i Rosen. To je za posljedicu imalo otkrivanje fenomena nazvanog kvantna prepletenost odnosno kvantna sprega.

Bellov teorem predstavlja važan primjer usporedbe kvantne mehanike i klasične fizike. Bell je u svojem radu dokazao da princip lokalnosti nije konzistentan sa teorijom skrivene varijable predloženom u EPR paradoksu. Svoj teorem dokazao je stvaranjem Bellovih nejednakosti. Te nejednakosti važeće su za korelacije proizašle iz bilo koje teorije koja je u skladu sa lokalnim realizmom. Ipak, kvantna mehanika predviđa kršenje Bellovih nejednakosti kod određenih kvantnih stanja u sprezi.

Bellova stanja su:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

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

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

3.3. Superpozicija

Jedno od svojstava po kojima se qubit razlikuje od klasičnog bita jest njegova mogućnost postojanja u superpoziciji. Superpozicija je jedan od fundamentalnih principa kvantne mehanike. U klasičnoj fizici, val koji opisuje glazbeni akord možemo promatrati kao nekoliko valova različitih frekvencija povezanih u cjelinu odnosno superpozicioniranih. Slično tome, kvantno stanje u superpoziciji možemo promatrati kao linearnu kombinaciju različitih posebnih kvantnih stanja. To kvantno stanje u superpoziciji tvori novo važeće kvantno stanje. Kvantni bitovi mogu se nalaziti u superpoziciji dvaju osnovnih stanja $|0\rangle$ i $|1\rangle$. Kada nad kvantnim bitom izvršimo čin mjerenja, njegovo stanje zauzet će jednu od tih vrijednosti. Na primjer, kada se qubit nalazi u superpoziciji vrijednosti jednakih težina, mjerenje će uzrokovati njegovo zauzimanje vrijednosti jednog od osnovnih stanja $|0\rangle$ i $|1\rangle$ sa vjerojatnošću od 50%.

Koncept superpozicije stanja i ulogu mjerenja najlakše je opisati poznatim Schrödingerovim misaonim eksperimentom: Zamislimo živu mačku zatvorenu u metalnoj kutiji u kojoj se nalaze radioaktivna supstanca, bočica otrova, čekić i mjerač radijacije. Vrijeme raspada radioaktivne supstance nasumičan je faktor i nije moguće predvidjeti u kojem trenutku će se on dogoditi. Kada se rasprad dogodi, mjerač radijacije poslat će signal čekiću, koji će potom razbiti bočicu otrova koji je smrtonosan za mačku. Promatrač ne može znati je li mačka živa ili mrtva dok ne otvori kutiju. Do tog trenutka mačka se nalazi u superpoziciji stanja između živog i mrtvog.

Kvantna superpozicija fundamentalno se razlikuje od superpozicije klasičnih valova. Kvantno računalo koje se sastoji od n kubita može se nalaziti u superpoziciji 2^n stanja: od $|000...0\rangle$ do $|111...1\rangle$. Superpozicioniranje n broja klasičnih valova različitih frekvencija pak rezultira superpozicijom n frekvencija. Superpozicioniranje klasičnih valova stoga je skalarno linearno, a superpoziciranje kvantnih stanja skalarno eksponencijalno.

4. Kvantna kriptografija

Jedna informacija može biti izražena i reprezentirana na mnogo različitih načina i pritom zadržati svoja osnovna obilježja. To svojstvo otvara mogućnost automatske manipulacije informacijama. Stroj mora biti u mogučnosti upravljati samo krajnje jednostavnim faktorima, poput binarnih brojeva, kako bi izvodio prilično složene procese procesuiranja informacija poput pripreme dokumenta ili prevođenja prirodnih jezika. Danas su ovi fenomeni poznati svima, ali prije samo pola stoljeća ovolika važnost automatskog upravljanja informacijama nije se mogla ni naslutiti. Sve metode izražavanja informacije imaju nešto zajedničko: koriste se fizičkim fenomenima za obavljanje funkcije. Zvuk i glas prenose se fluktuacijama u pritisku zraka, pisani tekst ovisi o rasporedu molekula tinte na papiru, a ljudske misli o neuronima. Može se reći da nema informacije bez njene fizičke reprezentacije. Neovisnost o načinu izražavanja i mogućnost slobodnog mjenjanja oblika informaciju čine očitim kandidatom za bitnu ulogu u znanosti fizike, uz energiju, moment sile i ostale slične apstrakcije. Povijesno je velik dio rada u polju fizike bio usmjeren na otkrivanje najmanjih čestica u prirodi i jednadžbi koje opisuju njihovo kretanje i interakcije. Danas se čini da bi drugačiji pristup mogao biti od jednake važnosti: otkriti načine na koje priroda omogućava izražavanje i manipuliranje informacijom. Praksa matematičkog tretiranja informacija, osobito matematičko procesiranje informacija postoji tek od sredine dvadesetog stoljeća, što znači da prava važnost tretiranja informacije kao osnovnog koncepta fizike biva otkrivena tek sada. Ta je važnost osobito vidljiva pri proučavanju koncepata kvantne mehanike, a teorija o kvantnoj informaciji i kvantnom računarstvu dovela je do istinski uzbudljivih saznanja o načinu na koji prirodni svijet funkcionira.

Neki od procesa kvantne obrade informacija su korištenje kvantnih stanja za siguran prijenos klasičnih informacija (kvantna kriptografija), korištenje fenomena kvantne prepletenosti u svrhu pouzdane transmisije kvantnog stanja (teleportacija), mogućnost očuvanja kvantne koherentnosti uz prisutnost buke u komunikacijskom kanalu (kvantno ispravljanje pogrešaka) i korištenje kontrolirane kvantne evolucije za izvedbu računarskih algoritama (kvantno računarstvo). Ono zajedničko ovim procesima je upotreba fenomena kvantne prepletenosti kao računskog resursa.

Područje kvantne kriptografije za cilj ima opisati procese ostvarivanja sigurne komunikacije i zaštite podataka upotrebom fundamentalnih principa fizike poput kvantno mehaničkog fenomena kvantne prepletenosti i Heisenbergovog načela neodređenosti. Posljednjih desetljeća ostvaren je značajan napredak u teorijskom razumijevanju kvantne kriptologije, a sve bržim tehnološkim napretkom i razvojem kvantnih računala njezin je potencijal i eksperimentalno dokazan. Područje kvantne kriptografije stoga se smatra jednim od najperspektivnijih kandidata za široku implementaciju kvantnih tehnologija.

4.1. „No-cloning“ teorem

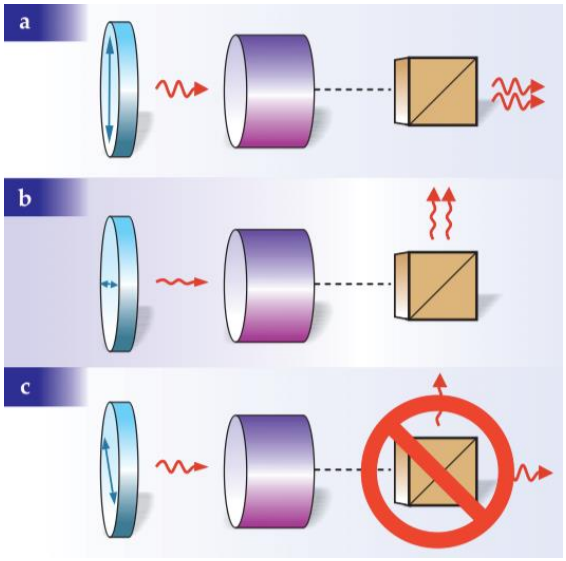
„No-cloning“ teorem proizašao je iz kvantne mehanike koja onemogućava kreiranje identičnih kopija nepoznatog kvantnog stanja. Ovaj teorem formulirali su Wootters, Zurek i Dieks 1982. godine i time bitno pridonijeli razvoju kvantnog računarstva i uz njega vezanih znanstvenih disciplina. „No-cloning“ teorem proizlazi iz činjenice da sve kvantne operacije moraju biti unitarne linearne transformacije stanja.

Teoremom o nemogućnosti kloniranja kvantnog stanja onemogućeno je korištenje klasičnih metoda ispravljanja pogrešaka nad kvantnim stanjima. Na primjer, nije moguće kreirati dodatne kopije stanja tokom obavljanja kvantne operacije te ih koristiti za ispravljanje eventualnih pogrešaka tijekom izvedbe. Mogućnost ispravljanja pogrešaka od izuzetne je važnosti za praktičnost upotrebe kvantnog računarstva, a njen nedostatak dugo se smatrao velikim ograničenjem. 1995. godine Peter Shor i Andrew Steane ponovo ističu potencijale kvantnog računarstva tako što neovisno jedan o drugome razvijaju prve kodove za kvantno ispravljanje pogrešaka koji zaobilaze teorem o nemogućnosti kloniranja stanja.

Ipak, "no cloning" teorem jedan je od vitalnih dijelova u području kvantne kriptografije jer onemogućava kopiranje kvantnog kriptografskog ključa od strane prisluškivača. "No cloning teorem" zastupa Heisenbergov princip neodređenosti (načelno je nemoguće istovremeno odrediti točan položaj i brzinu neke čestice) u kvantnoj mehanici. Heisenbergovo je stajalište sljedeće: elektron postoji neovisno o opažaču, ali se promatranjem na njega utječe onako kako je to formulirano matematičkom shemom relacija neodređenosti. Niti jedan do sada izveden pokus kojim ih se htjelo narušiti ili opovrgnuti nije uspio izbjeći relacije neodređenosti. Kada bismo mogli klonirati fundamentalno nepoznato stanje, mogli bismo napraviti neograničen broj njegovih kopija i mjeriti svaku dinamičku varijablu sa proizvoljnom preciznošću i tako

premostiti princip neodređenosti. Dokazivanjem validnosti teorema o nemogućnosti kloniranja kvantnog stanja ta je mogućnost isključena.

Ovaj teorem ističe nemogućnost superluminalnog prijenosa informacija (prijenosa informacija bržeg od brzine svjetlosti) uzrokovanu, u prethodnim poglavljima spomenutim fenomenom - kvantne sprege. "No cloning" teorem u kombinaciji sa EPR paradoksom pokazuje nam kako je ne-relativistička kvantna mehanika konzistentna teorija jer, da je kloniranje moguće, EPR korelacije bismo mogli koristiti za komunikaciju bržu od brzine svjetlosti, što je kontradiktorno principima specijalne relativnosti.



Slika 4. Wooters, W., Zurek, W. The no-cloning theorem. // Physics Today, 2009, str. 76-77.

Umjesto matematičkog dokazivanja ovog teorema, dovoljno je navesti dva primjera koji prikazuju način na koji on funkcionira. U prvom slučaju proučava se foton čija je polarizacija vertikalna ili horizontalna. Kako bi se odredilo njegovo polarizacijsko stanje može se upotrijebiti polarizacijski razdjelnik, nakon kojeg se nalaze dva detektora fotona. Ako detektor na putu refleksije daje signal jasno je da je ulazni foton vertikalno polariziran, dok je u protivnom polariziran horizontalno. Jednom kada je polarizacijsko stanje fotona poznato, može se proizvesti proizvoljan broj fotona sa istim polarizacijskim stanjem i tako postići savršeno kloniranje istog. To je izvedivo jer su dva moguća polarizacijska stanja ulaznog fotona međusobno ortogonalna.

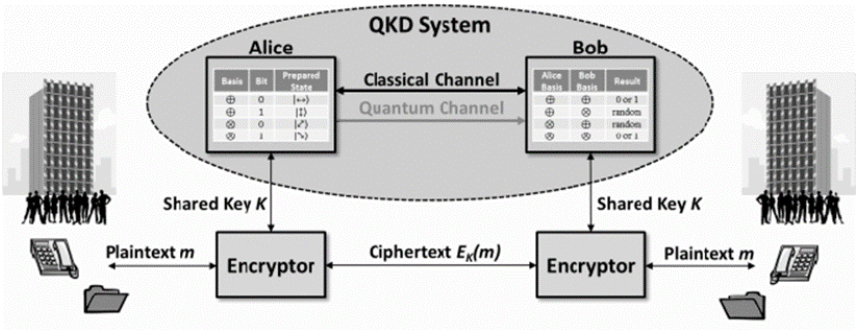
U drugom slučaju promatra se foton čija je polarizacija nasumično određena iz seta {horizontalno, vertikalno, 45˚, 135˚}. Polarizacijsko stanje ovog fotona nije moguće odrediti bilo kakvim eksperimentom. Kada bismo koristili identičan polarizacijski razdjelnik kao u prvom slučaju foton polariziran pod, na primjer, 45˚ bio bi reflektiran ili prenešen sa polovičnom vjerojatnošću, pa iz tog razloga njegovo polarizacijsko stanje nije moguće odrediti sa sigurnošću, što je vidljivo iz *slike 4*.

4.2. Kvantna distribucija ključa

Kvantna kriptografija bavi se istraživanjem i realizacijom nekoliko ideja od kojih je trenutno najraširenija ideja kvantne distribucije ključa. To je metoda gdje se kvantna stanja koriste za provedbu komunikacijske funkcije gdje se između dvije lokacije prenosi par identičnih, ali nasumično odabranih sekvenci binarnih brojeva bez mogućnosti prisluškivanja sa treće strane. Ta metoda od izuzetne je važnosti jer se nasumična sekvenca može koristiti kao kriptografski ključ za ostvarivanje sigurne komunikacije. Bitno svojstvo kvantne distribucije ključa je da principi kvantne mehanike garantiraju očuvanje tajnosti kvantne informacije što znači da je rizik kompromitiranja tajnosti ključa u potpunosti izbjegnut korištenjem zakona prirode.

Jedno od neobičnih svojstava kriptografije jest da nije moguće eksperimentom dokazati da je kriptografska procedura sigurna. Pouzdanje u funkcionalnost metoda mora biti zasnovano na matematičkim dokazima sigurnosti, a na tom polju je od začetka discipline puno napravljeno te su predstavljeni mnogi dokazi koji podržavaju sigurnost pravilno implementirane kvantne distribucije ključa. Kao što je ranije spomenuto, kvantna distribucija ključa je metoda gdje se kvantna stanja koriste za generiranje nasumičnog tajnog kriptografskog ključa. Osnovne ideje su sljedeće: Osoba "A" i osoba "B" nalaze se na velikoj fizičkoj udaljenosti jedna od druge i žele zasnovati komunikacijski kanal. Osoba A šalje osobi B *2n* qubita, svaki od njih pripremljen u jednom od stanja $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, nasumce odabranih. Osoba B mjeri stanja primljenih bitova na temelju nasumično odabrane baze između vrijednosti $\{|0\rangle , |1\rangle\}$ i $\{|+\rangle,|-\rangle\}$. Osoba A i B zatim javno dijele informaciju o bazi koju su koristili za pripremu odnosno mjerenje svakog kvantnog bita. Na taj način saznaju kod kojih su slučajeva nasumce odabrali istu bazu, što se u prosjeku događa u 50% slučajeva i zadržavaju samo te rezultate. Ukoliko nije bilo grešaka ili smetnji u prijenosu osoba A i B dijele isti niz nasumce odabranih klasičnih bitova (podrazumijeva se da je unaprijed dogovoreno da se, naprimjer, kvantne vrijednosti $|0\rangle$

i $|+\rangle$ vežu uz vrijednost 0, a vrijednosti $|1\rangle$ i $|-\rangle$ uz 1). Taj niz klasičnih bitova naziva se "sirova kvantna transmisija" (*raw quantum transmission*, RQT). Do sada u ovom procesu nisu iskorištene prednosti korištenja kvantnih bitova, ali treba napomenuti kako ne postoji mogućnost da itko osim osobe A i B otkrije rezultate mjerenja qubita bez ostavljanja dokaza svoje prisutnosti. Grafički prikaz ovog procesa prikazan je na slici 5. Najjednostavniji način na koji prisluškivač može otkriti ključ jest da presretne kvantne bitove u komunikacijskom kanalu, izmjeri njihovo stanje i proslijedi osobi B. Prisluškivač će u prosjeku za pola kvantnih bitova pogoditi bazu koju je osoba A koristila i u tom slučaju neće promijeniti njegovo stanje. Ipak, prisluškivač će pogoditi baze na različitim kvantnim bitovima od osobe B, pa će saznati stanja pola od n kvantnih bitova koje će osoba A i B kasnije smatrati pouzdanima, dok će drugoj polovici promijeniti stanja (naprimjer poslati osobi B $|+\rangle$ za originalno stanje $|0\rangle$ poslano od strane osobe A). Pola kvantnih bitova kojima je prisluškivač promijenio stanje vratit će se u originalno stanje činom mjerenja od strane osobe B, tako da prisluškivač korumpira ukupno *n/4* bitova RQT. Osobe A i B sada mogu detektirati prisutnost prisluškivača tako da nasumce odaberu *N/2* RQT bita i javno obznane njihove vrijednosti. Ako se njihove vrijednosti slažu za sve bitove, mogu biti sigurni da je njihov ključ siguran, budući da je vjerojatnost da je prisluškivač bio prisutan i da su nasumce odabrali *n/2* nekorumpiranih bitova $(3/4)^{n/2} \simeq 10^{-125}$ za $n=1000$. U praksi je ovaj protokol nešto kompliciraniji za izvedbu jer prisluškivač može koristiti i druge strategije, a buka u komunikacijskom kanalu može korumpirati neke kvantne bitove čak iako prisluškivač nije prisutan. Umjesto da odbace ključ ako se mnogi kvantni bitovi razlikuju, osoba A i B zadržat će ga sve dok je kvota pogreške manja od 25% te će ga naknadno procesuirati.



Slika 5. grafički prikaz kvantne distribucije ključa. Mailloux, L., Hodson, D., Grimaila, M. Using Modeling and Simulation to Study Photon Number Splitting Attacks. // IEEE Access, 1(Travanj 2016), str. 2188-2197. Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7456202

Opisani protokol nije jedini način kvantne distribucije ključa. Drukčiji pristup opisao je 1991. godine Artur Ekert. Kod njegovog protokola koriste se EPR parovi koje osoba A i B mjere na jednoj od tri različite osi. Kako bi isključili mogućnost prisluškivanja, provjeravaju Bell-EPR korelacije u svojim rezultatima.

Protokoli kvantne distribucije ključa (QKD protokoli) obično se provode u dvije faze: faza kvantne transmisije i faza klasičnog post-procesiranja. Prva faza uključuje pripremu kvantnog stanja, transmisiju i detekciju, a druga usporedbu baza mjerenja, ispravku pogrešaka i amplifikaciju privatnosti.

QKD ne mora biti jedino rješenje za premošćivanje slabosti javnih kriptografskih sustava. Ljudi bi mogli prihvatiti povratak na staru shemu distribucije ključa pouzdanim kurirom. Na tradicionalne tvrde diskove i dalje se može pohraniti višestruko veći broj nasumičnih bitova nego što bilo koji trenutno dostupan QKD sustav može generirati. Ipak, napredak novih tehnologija otvara nebrojene mogućnosti i uz uloženi trud stručnjaka pitanje je trenutka kada će visoko efikasni i komercijalno dostupni QKD sustavi biti stavljeni u upotrebu.

4.3. Shorov algoritam

Ranih devedesetih godina prošlog stoljeća nekoliko je autora (Deutsch i Jozsa 1992, Berthiaume i Brassard 1992, Bernstein i Vazirani 1993) kroz svoje radove istraživalo postojanje računskih problema pri čijem bi rješavanju korištenje kvantnog računala bilo brže i efikasnije od korištenja bilo kojeg klasičnog računala. Takav bi kvantni algoritam imao veliku konceptualnu ulogu, definirajući nešto od esencijalne prirode kvantne mehanike. Daniel Simon je na ovom polju 1994. godine postigao izvjestan uspjeh, opisavši kvantni algoritam za rješavanje (relativno apstraktnog) problema koji je bio nerješiv na dotad poznate klasične načine. To je inspiriralo Petera Shora, profesora primjenjene matematike na Američkom sveučilištu MIT, koji je iste godine predstavio algoritam koji ne samo da je efikasan na kvantnim računalima, već se dotiče centralnog problema u računarstvu: rastavljanja velikih brojeva na proste faktore, na čijoj se nerješivosti temelji sigurnost mnogih današnjih sigurnosnih sustava. Shorov algoritam znatno je brži od najbržeg poznatog algoritma za rješavanje istog problema na klasičnom računalu te se danas smatra najznačajnijim algoritmom za kvantna računala jer rješava bitan problem u računarstvu i dokazuje da bi kvantna računala svojevremeno mogla imati znatno više računske snage od klasičnih. Shorov algoritam u pitanje dovodi Church-Turingovu vezu, prema kojoj je bilo koji algoritam za bilo koje fizički izvedivo računalo moguće simulirati na Turingovom stroju, što za Shorov algoritam nije slučaj. Kada bi kvantno računalo sa dovoljnim brojem kvantnih bitova moglo funkcionirati bez kvantne buke i drugih fenomena kvantne dekoherencije, Shorov algoritam mogao bi se koristiti kao metoda probijanja kriptografskih sustava sa javnim ključem, poput široko upotrebljavane RSA sheme. Trenutno nije poznat niti jedan klasičan algoritam koji može rastavljati velike brojeve na proste faktore u polinomnom vremenu. Shor svojim algoritmom dokazuje da je rješenje tog problema dokučivo konstrukcijom kvantnog računala sa dovoljnom količinom kvantnih bitova. Njegov rad potaknuo je razvoj arhitekture i unaprjeđenje dizajna kvantnih računala i uzrokovao povećan interes za istraživanje novih sigurnosnih sustava koji su sigurni od napada kvantnim računalom kolektivno poznatih pod nazivom „post-kvantna kriptografija“. Shorov algoritam sastoji se od dva dijela. Prvi dio algoritma pretvara proces faktoriziranja u problem pronalaska perioda funkcije i može ga se implementirati na klasičnom računalu. U drugom dijelu period funkcije se pronalazi koristeći Fourierovu kvantnu transformaciju koja je odgovorna za kvantno ubrzanje. Shorov algoritam oslanja se na mogućnost kvantnog računala da se nalazi u mnogo stanja istovremeno, odnosno da se nalazi u superpoziciji stanja. Kako bi se izračunao period funkcije *f*, vrijednost funkcije računa se u svim točkama istovremeno. Ipak, kvantna

fizika ne dozvoljava direktan pristup rezultatima. Mjerenje će uzrokovati uništenje svih osim jedne od mogućih vrijednosti. Da ne vrijedi teorem o nemogućnosti kloniranja, bilo bi moguće mjerenje funkcije *f(x)* bez mjerenja *x*. Potom bi se moglo napraviti nekoliko kopija rezultirajućeg stanja, što je superpozicija stanja od kojih sva imaju identičnu vrijednost *f(x)*. Mjerenje varijable *x* nad tim stanjima rezultiralo bi različitim vrijednostima koje daju isti *f(x)* što bi vodilo do perioda funkcije. S obzirom da nije moguće napraviti identične kopije kvantnih stanja, ova metoda ne funkcionira, već je potrebno pažljivo pretvoriti superpoziciju u drugo stanje koje će davati točan odgovor sa visokom vjerojatnošću. To se postiže korištenjem kvantne Fourierove transformacije koju je izumio Don Coppersmith.

Znanstvenici Vandersypen, Steffen, Breyta, Yannoni, Sherwood i Chuang su 2001. godine uspjeli demonstrirati Shorov algoritam na kvantnom računalu sa 7 kvantnih bitova konstruiranih korištenjem tehnologije nuklearne magnetske rezonance.

2010. godine tim znanstvenika sa Sveučilišta u Bristolu uspio je kreirati kvantni čip temeljen na kvantnoj optici i na njemu demonstrirati Shorov algoritam.

4.4. BB84 protokol

Prvi protokol kvantne kriptografije predstavili su 1984. godine Charles H. Bennet i Gilles Brassard (iz čega proizlazi naziv BB84). Ovim protokolom predstavili su potencijalno nove temelje same kriptografije, temeljene na kvantnoj mehanici i zakonima prirode umjesto na matematičkoj kompleksnosti. BB84 protokol koristi pulseve polariziranog svijetla, gdje svaki puls predstavlja jedan foton. Osnovna ideja iza BB84 protokola iznenađujuće je jednostavna. Pretpostavimo da su osoba A i osoba B povezane relativno nesigurnim kvantnim komunikacijskim kanalom, na primjer optičkim vlaknom i klasičnim javnim kanalom poput telefonske linije ili internetske veze. Pitanje je kako mogu dijeliti dugi niz brojeva koji će koristiti kao kriptografski ključ s apsolutnom sigurnošću. Imajući na umu "no cloning" teorem, osoba A kodira svoje nasumične bitove polarizacijskim stanjem fotona i prosljeđuje ih osobi B nesigurnim kvantnim kanalom. U ovom slučaju koristimo naziv "kvantni kanal" kako bismo naglasili činjenicu da su informacije koje putuju tim kanalom kodirane kvantnim stanjem fotona. Osoba A koristi horizontalno polarizirani foton za kodiranje bita "0" i vertikalno polarizirani foton za kodiranje bita "1". Osoba B može raskriti nasumičan bit provođenjem mjerenja polarizacije. Ali ova metoda nije sigurna zato jer potencijalni prisluškivač može presresti fotone u komunikacijskom kanalu, izmjeriti polarizaciju fotona, zapisati rezultat i

prema njemu pripremiti novi foton koji će proslijediti osobi B i tako doći do iste informacije kao osoba B. Problem u ovom slučaju predstavlja nedostatak koncepta baze koja predstavlja način na koji će foton biti kodiran. Kako bi ovaj model funkcionirao, koriste se dvije baze: horizontalno-vertikalna, gdje horizontalna polarizacija fotona predstavlja vrijednost bita "0", a vertikalna vrijednost "1" i dijagonalna baza, gdje polarizacija fotona od 45˚ predstavlja vrijednost "0", a polarizacija od 135˚ vrijednost "1". Za svaki prijenos, osoba A nasumce odabire bazu koju će koristiti za kodiranje svog nasumičnog broja. Sada je polarizacija svakog fotona nasumce odabrana iz seta {horizontalno, vertikalno, 45˚, 135˚} i ne postoji način na koji prisluškivač može odrediti njegovo polarizacijsko stanje. BB84 protokol grafikčki je prikazan na slici 6. Ukoliko prisluškivač odluči mjeriti foton po horizontalno-vertikalnoj bazi, uništit će informacije kodirane fotonom u dijagonalnoj bazi budući da foton, polariziran pod 45˚ ili 135˚ ima jednake šanse da bude projiciran u horizontalno ili vertikalno stanje. Bez poznavanja baze, koju je osoba A koristila za pojedini foton, osoba B nasumce bira bazu koju će koristiti za mjerenje svakog dolazećeg fotona. Ako je korištena ista baza za isti foton mogu se generirati odgovarajući bitovi, a ako su korištene različite baze, vrijednosti njihovih bitova neće si međusobno odgovarati. Nakon što osoba B izmjeri sve fotone, korištene baze uspoređuju se kroz pouzdani javni kanal. Zadržavaju se samo vrijednosti nasumičnih bitova generiranih odgovarajućim bazama. Uz izostanak buke u kanalu, nesavršenosti sistema ili prisutnosti prisluškivača, njihove vrijednosti su identične i mogu biti korištene kao kriptografski ključ.

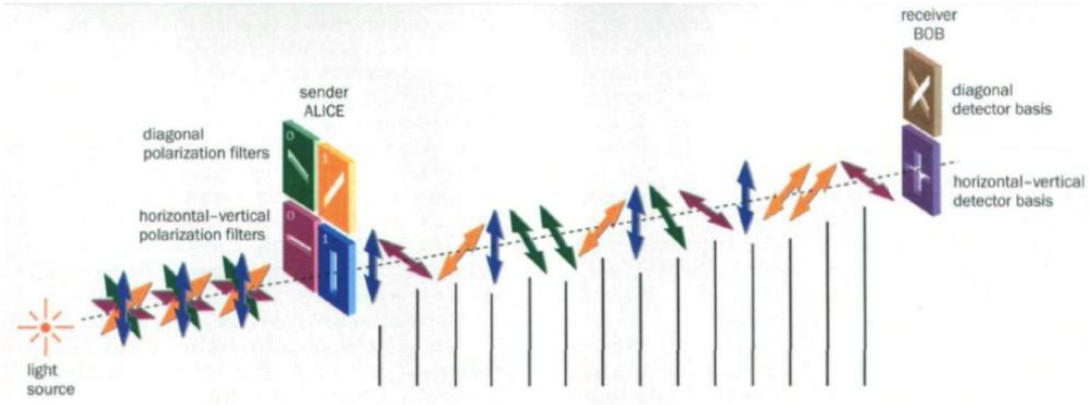
Tablica 1: prikaz BB84 QKD protokola

Alice's random bits	1	0	0	1	0	1	1	1	0	1
Alice's encoding bases	×	×	+	×	+	+	+	×	+	+
Alice's photon polarization	135°	45°	H	135°	H	V	V	135°	H	V
Bob's measurement bases	+	×	+	×	×	+	×	+	+	+
Bob's measurement result	H	45°	H	*	135°	V	45°	*	H	V
Bob's raw data	0	0	0		1	1	0		0	1
Sifted key from matched bases		0	0			1			0	1
+: rectilinear basis; ×: diagonal basis; H: horizontal polarization; V: vertical polarization; *: no detection										

Što će se dogoditi ako prisluškivač presretne fotone poslane od strane osobe A, izmjeri ih po nasumično odabranoj bazi i proslijedi novi foton osobi B?

Usredotočimo se samo na slučajeve gdje osoba A i osoba B koriste istu bazu, s obzirom da će ostale vrijednosti ionako biti odbačene. Ukoliko prisluškivač, igrom slučaja, koristi ispravnu bazu on i osoba B dekodirat će vrijednost bita poslanu od osobe A ispravno. Ukoliko prisluškivač upotrijebi pogrešnu bazu za mjerenje, njegova vrijednost bit će nasumična. U tom slučaju osoba A i B će prilikom usporedbe vrijednosti bitova primijetiti veliku količinu pogrešaka. Ovakav pokušaj prisluškivanja rezultirat će sa 25% pogrešaka kvantnog bita (*quantum bit error rate*, QBER).

Ovaj primjer ilustrira osnovni princip kvantne distribucije ključa: prisluškivač može dobiti informacije samo tako da pritom uzrokuje pogreške u sustavu koje će otkriti njegovu prisutnost.



Slika 6: BB84 protokol. Labouchere, P., Behrens, A. // Ppt prezentacija: Quantum Cryptography, 3. Prosinca 2007.

5. Implementacija protokola kvantne kriptografije

Kroz posljednja tri desetljeća kriptografski protokoli s javnim ključem postali su integralni dio svjetske digitalne komunikacijske infrastrukture. Ove mreže podržavaju niz procesa važnih za ekonomiju, sigurnost i način života koji uključuje korištenje mobilnih uređaja, internetsko poslovanje, društvene mreže i računarstvo u oblaku. U ovako povezanom svijetu potreba za sigurnom komunikacijom od izuzetno je velike važnosti. Mnogi od najzastupljenijih komunikacijskih protokola ovise o tri jezgrene kriptografske funkcije: enkripciji javnim ključem, digitalnim potpisima i razmjeni ključa. Trenutno su ove funkcionalnosti u većini ostvarene korištenjem Diffie-Hellman-ovom razmjenom ključa, RSA (Rivest-Shamir-Adleman) kriptološkim sustavom i kriptografijom eliptičkih krivulja. Sigurnost ovih protokola ovisi o težini određenih matematičkih problema, poput faktorizacije velikih brojeva. Peter Shor je 1994. godine dokazao da kvantno računalo može učinkovito rješiti svaki od njih i tako ugroziti sigurnost javnih kriptoloških sustava temeljenih na matematičkim pretpostavkama. Od tada je znanost o teoriji kvantnih algoritama značajno napredovala. Otkriveni su kvantni algoritmi koji omogućavaju eksponencijalno ubrzanje pri rješavanju problema vezanih uz simuliranje fizičkih fenomena, teoriju brojeva i topologiju. Skromnija, ali ipak značajna ubrzanja ostvarena su pri rješavanju različitih klasa problema vezanih uz pretraživanje neoznačenih listi, pronalaženje kolizija i Booleove formulacije.

Tablica 2: Utjecaj kvantnog računarstva na sigurnost popularnih kriptografskih algoritama

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

U ne tako dalekoj prošlosti kvantna računala kao dio tehnološke stvarnosti nisu bila zamisliva, a danas mnogi znanstvenici vjeruju kako njihova izgradnja predstavlja ništa više nego izazov za inžinjere. Neki stručnjači predviđaju da će kroz narednih 20 godina biti proizvedena kvantna računala dovoljno snažna da ugroze sigurnost svih danas korištenih kriptoloških sustava sa javnim ključem. Predviđa se da će do 2030. godine biti proizvedeno kvantno računalo dovoljne snage da ugrozi sigurnost RSA protokola sa 2000 bitova u samo nekoliko sati.

Za razvoj moderne kriptografske infrastrukture bilo je potrebno gotovo dvadeset godina, a za sigurnu migraciju na kriptološke sustave prilagođene kvantno-mehaničkom informacijskom okruženju potrebna su mnoga ulaganja. Iako nije moguće predvidjeti točno vrijeme početka ere kvantnog računarstva, sa pripremom sustava za sigurnost potrebno je početi sada, kako bi se oni mogli održati i tada.

Skup procesa namijenjenih ostvarivanju tih ciljeva u akademskom je svijetu poznat pod nazivom „Post-Kvantna Kriptografija“. To je aktivno područje istraživanja sa serijom konferencija pod nazivom PQCrypto, koje su sa održavanjem počele 2006. godine. Razvoj znanosti poduprt je financijskim donacijama mnogih udruga, posebice iz Europe i Japana, velikim dijelom kroz projekte Europske Unije PQCrypto i SAFECrypto, te CREST Crypto-Math projekt u Japanu. U proteklih nekoliko godina organizacije za standarde i industriju započele su sa raznim aktivnostima u polju post-kvantne kriptografije: od 2013. godine European Telecommunications Standards Institute (ETSI) održao je tri radionice pod nazivom „Quantum-Safe Cryptography“, National Institute of Standards and Technology (NIST) u SAD-u je 2015. godine održao radionicu pod nazivom „Cybersecurity in a Post-Quantum World“, koju je pohađalo preko 140 ljudi iz vladinih organizacija, industrije i akademske zajednice. Post-kvantnu kriptografiju ne treba miješati sa kvantnom kriptografijom (ili kvantnom distribucijom ključa), gdje se svojstva kvantne mehanike koriste za stvaranje sigurnog komunikacijskog kanala.

Prvi eksperiment kvantne distribucije ključa izvela je IBM-Montreal grupacija 1989. godine. Od tada je ostvaren velik eksperimentalni i tehnološki napredak na polju kvantne kriptografije, pa danas već postoje komercijalno dostupni sustavi kvantne distribucije ključa. Provođenjem dvaju eksperimenata kvantne distribucije ključa kvantnim satelitom 2017. i 2018. godine, gdje je kriptografski ključ uspješno prenesen između dvije točke udaljene 1200km u Kini i 7600km između Kine i Austrije demonstrirana je zrelost i upotrebljivost tehnologija za implementaciju

QKD protokola. Na unaprjeđenju tehnologije kvantne komunikacije putem satelita intezivno se radi i u Europi, SAD-u, Kanadi, Japanu i Singapuru. Uspješan proces kvantne distribucije ključa optičkim vlaknima do sada je ostvaren na udaljenosti od 500km. Za praktičnu implementaciju, uz velike udaljenosti, potrebna je i velika brzina prijenosa ključa. 2018. godine demonstiran je prijenos brzine od 10 Mbits/s, putem optičkih vlakana duljine 50km, za razliku od prijašnjih 1 Mbits/s.

U praksi su fotoni trenutno najbolji kandidat za prijenos različitih kvantnih stanja. Fotone je jednostavno proizvesti, a njihova interakcija sa okolišem može se kontrolirati. Stručnjaci i istraživači također imaju benefit korištenja rezultata tridesetogodišnjeg razvoja optičke telekomunikacije. Neke od kompanija koje u svojoj ponudi imaju komercijalno dostupna QKD rješenja su ID Quantique, Quantum CTek, Qasky i Toshiba Europe. Nekoliko instituta, poput European Telecommunications Standards Instituta (ETSI), International Organization for Standardization (ISO) i International Telecommunication Union (ITU) poduzimaju mjere kako bi se procesi kvantne distribucije ključa što bolje standardizirali. Sve u svemu, tehnologija kvantne distribucije ključa dovoljno je zrela za široku implementaciju. Na primjer, QKD tehnologija korištena je za ostvarivanje sigurne komunikacije u vrijeme predsjedničkih izbora u Švicarskoj 2007. godine i za određivanje ždrijeba na svjetskom nogometnom prvenstvu 2010. godine. U Kini QKD već ima široku sferu upotrebe, a koriste ga mnoge vladine i financijske institucije (People's Bank of China, The China Banking Regulatory Commission, Industrial and Commercial Bank of China i druge), kao i organizacije iz polja energetike.

Početkom 2014. godine objavljen je podatak da je Nacionalna sigurnosna agencija u SAD-u pokrenula projekt vrijedan 79,9 milijuna dolara, kojemu je cilj sagledati upotrebu kvantnoga računala u kriptološke svrhe. Nastanak komercijalno dostupnih kvantno kriptoloških rješenja i povećano zanimanje i financijsko ulaganje velikih tehnoloških kompanija u razvitak upućuju na mogućnost upotrebe kvantnih sustava u mnogo šire svrhe nego što je to bilo do sada.

5.1. DARPA kvantna mreža

DARPA model sigurnosti je kriptografska Virtualna Privatna Mreža (VPN). Tradicionalne VPN mreže koriste kriptografske sustave sa javnim ključem i simetrične kriptografske sustave kako bi postigli integritet i pouzdanost mreže. Iz tog razloga njihova sigurnost ne ovisi o javnoj mreži koja povezuje dvije krajnje točke u komunikacijskom kanalu. U radu DARPA-e, postojeće znamenke VPN ključa nadograđene su ili potpuno zamjenjene vrijednostima koje daju kvantni kriptološki mehanizmi. Ostatak VPN arhitekture ostaje nepromijenjen, pa je DARPA mreža, osigurana kvantnom distribucijom ključa, potpuno kompatibilna sa konvencionalnim internetskim hostovima, usmjernicima, vatrozidima i ostalim.

5.2. MagiQ Technologies

Jedna od kompanija koja nudi komercijalno dostupne proizvode i razvija rješenja bazirana na kvantnoj kriptografiji je MagiQ Technologies, tehnološki start-up sa sjedištem u New Yorku. Velik broj njihovih klijenata je iz financijske industrije, ali njihovi proizvodi koriste se i u akademskim i državnim laboratorijima. Stajalište ove kompanije je da kvantna kriptografija ne predstavlja zamjenu za tradicionalne tehnike enkripcije, već svojevrsni dodatak postojećim algoritmima, kako bi se stvorio hibridni model koji pospješuje sigurnost sustava. Njihov sustav kvantne distribucije ključa smatra se prvim komercijalno dostupnim QKD sustavom. Fizičke jedinice ovog sustava sastoje se od odašiljača i primatelja fotona i elektroničkih komponenti kojima upravlja računalni algoritam odgovoran za proces kvantne distribucije ključa. Te jedinice međusobno su povezane optičkim vlaknom gdje je implementiran Brassardov i Benettov BB84 protokol za kvantnu enkripciju. Ovaj sustav funkcionira na način da mijenja nasumično odabrane brojeve jednom u sekundi kako bi spriječio neautoriziran pristup podacima koji putuju optičkim vlaknima. Cijena jedne ovakve MagiQ "Navajo QPN Security Gateway" jedinice je oko 50,000 američkih dolara.

6. Zaključak

Uslijed sve bržeg tehnološkog razvoja na području kvantnog računarstva i kvantne teorije informacija, svijet ulazi u proces druge kvantne revolucije. Bruce Schneider, jedan od vodećih svjetskih stručnjaka za sigurnost, jednom je izjavio: "Sigurnost je lanac koji je toliko jak koliko i njegova najslabija karika." Kriptološki protokoli temeljeni na matematičkim algoritmima trenutno se smatraju najsnažnijim karikama većine modernih sigurnosnih lanaca, ali eventualni razvoj dovoljno snažnog kvantnog računala mogao bi to vrlo brzo promijeniti. Prateći razvoj kriptografije kao znanstvene discipline kroz povijest lako je primjetiti da je kad god bi novi način probijanja sigurnosnog sustava bio otkriven, njegova sigurnost morala biti temeljito preispitana te je često bilo potrebno razviti nove sheme kodiranja kako bi se njegova sigurnost očuvala. Shorovim algoritmom faktoriziranja brojeva u teoriji je dokazano kako će sigurnost mnogih javnih kriptografskih sustava biti ozbiljno ugrožena jednom kada kvantno računalo postane dostupno i bude dovoljno snažno. To je samo jedan od primjera kojima se pokazuje utjecaj kvantne mehanike na klasičnu kriptologiju. Imajući na umu osnovne razlike između klasične i kvantne fizike, sigurnost svake karike u cijelim lancima kriptografskih sustava mora biti temeljito preispitana kako bismo znali hoće li ti sustavi preživjeti kvantnu eru.

Kvantna kriptografija predstavlja skup najnaprednijih tehnoloških procesa u području proučavanja kvantnih informacija. Ona je prvi kvantni koncept koji postupno dobiva industrijsku primjenu i manifestira se u vidu komercijalno dostupnih proizvoda. Iz tog razloga stručnjaci posljednjih godina rade na pouzdanosti tih sustava i njihovoj prilagodbi krajnjem korisniku koji ne mora nužno biti upoznat sa konceptima kvantne mehanike.

Shorov i slični algoritmi potiču stručnjake na razvitak i implementaciju metoda koje bi osigurale sigurnost sustava u slučaju takvog kvantnog napada, objedinjenih pod nazivom "post-kvantna kriptografija". Prvi kvantni kriptološki protokol razvili su Charles H. Benett i Gilles Brassard 1984. godine. Neovisno o njihovom BB84 teoremu, Artur K. Ekert objavljuje svoj Ekert protokol temeljen na česticama u kvantnoj sprezi i Bellovim teoremom kao metodom otkrivanja prisutnosti prisluškivača.

Tehnološki razvoj na polju kvantne kriptografije još je uvijek vrlo ograničen, ali u posljednjem desetljeću provedeni su mnogi eksperimenti koji dokazuju funkcionalnost kvantnih kriptoloških sustava izvan laboratorija. To potvrđuje ideju da će kvantna tehnologija biti široko upotrebljavana u bliskoj budućnosti. Ako promatramo kriptologiju kao znanstvenu disciplinu

u cjelini, možemo primijetiti da ona prolazi kroz svojevrsnu renesansu, razvijajući se paralelno s novom paradigmom o kvantnoj teoriji informacija kao alternativi dosada široko prihvaćenoj klasičnoj teoriji. Tehnologije za proizvodnju kvantnih računala posljednjih godina razvijaju se izuzetno brzo. Google je 2019. godine objavio podatak da je postignuta "kvantna nadmoć", što znači da je kvantno računalo prvi puta rješilo problem koji je nerješiv korištenjem klasičnog računala. Naime, prema Googleu njihov je Sycamore procesor sa 54 kvantna bita u 200 sekundi rješio problem za čije bi rješavanje najmoćnijem super računalu na svijetu trebalo 10000 godina. Nekoliko kompanija i svjetskih laboratorija u utrci su kako bi proizveli prvo kvantno računalo sa širokom upotrebom. Kvantni procesor sa 16 kvantnih bitova kompanije IBM Q već je dostupan za korištenje putem mrežnog sučelja, kompanija Rigetti nudi usluge kvantnog računarstva u oblaku, a Chinese Academy of Sciences (CAS) i Alibaba osnovali su laboratorij za kvantno računarstvo kako bi ubrzali razvoj kvantnih tehnologija. Ostale kompanije (Intel, Microsoft, Baidu, Tencent, IonQ, Xanadu, Zapata i druge) također sudjeluju u utrci za kvantnu nadmoć. U Kini se trenutačno gradi nacionalni laboratorij za znanost o kvantnoj informaciji, a u SAD-u je 2018. godine predstavljen nacionalni akt za kvantne inicijative (National Quantum Initiative Act). Sve ovo jasni su znakovi da se rizik za kriptološke protokole uzrokovan potencijalnom uspješnom proizvodnjom snažnog kvantnog računala u sljedećem desetljeću više ne može ignorirati. Iako su uvjeti za proizvodnju kvantnih računala sa širokom upotrebom još uvijek daleko od idealnih, pred svjetskim stručnjacima za sigurnost leže mnogi izazovi. Ukoliko kriptografski protokoli ne budu pratili tehnološki razvoj kvantnih računala, ovakvi bi sustavi u pogrešnim rukama mogli rezultirati krahom globalne sigurnosti. Pravilno implementirani kvantni kriptološki sustavi za razliku od klasičnih jamče sigurnu komunikaciju, ali ta njihova snaga vrlo se lako može pretvoriti u njezinu najveću slabost. Stoga ne bi bilo pogrešno reći da se znanost kriptologije nalazi u jednom od uzbudljivijih razdoblja u svojoj dosadašnjoj povijesti.

Literatura

Bell, J.S. On the Einstein-Podolsky-Rosen Paradox // Physics 1, (1964) str. 195-200.

Bennett, C.H., Besette, F., Brassard, G. Experimental quantum cryptography // Journal of Cryptology 5, (1992), str. 3 – 28.

Bennett, C.H., Brassard, G. Quantum Cryptography: Public key distribution and coin tossing. // Bangalore: Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, 1984.

Bouwmeester, D., Ekert, A., Zeilinger, A. The physics of Quantum Information. Berlin: Springer-Verlag, 2000.

Colin, R., Johnson MagiQ employs quantum technology for secure encryption. // EE Times, (2002)

Einstein, A., Podolsky, B., Rosen, N. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? // Phys. Rev. 47, 10(1935), str. 777 – 780.

Ekert, A.K. Quantum Cryptography Based on Bell's Theorem // Phys. Rev. Lett. 67, (1991) str. 661-663.

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. Quantum Cryptography // Rev. Mod. Phys. 74, 145(2002) str. 145-195.

Poppe, A. Practical quantum key distribution with polarization entangled photons. // Optics Express 12, 16(2004), str. 3865 – 3871.

Qi, B., Qian, L., Lo, H. A brief introduction of quantum cryptography for engineers. Ontario: University of Toronto, 2010.

Rivest, R., Shamir, A., Adleman, L. On Digital Signatures and Public-Key Cryptosystems. // Technical Report, MIT/LCS/TR-212. MIT Laboratory for Computer Science : 1979.

Scarani, V., Iblisdir, S., Gisin, N., Acin, A. Quantum Cloning // Rev. Mod. Phys. 77, 1225 (2005)

Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. // Santa Fe: Proceedings of the 35th Annual Symposium of Computer Science, 1994.

Shor, P.W, Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. //, Physical Review Letters 85, 2(2000)

Steane, A. Quantum computing. Oxford: University of Oxford Clarendon Laboratory, Department of Atomic and Laser Physics, 1997.

Wootters, W.K., Zurek, W.H. The no-cloning theorem", Physics Today, (2009), str. 76-77.

Potencijali upotrebe kvantnih računala u polju kriptologije

Sažetak

Kvantna računala uslijed naglog tehnološkog napretka uzrokovanog sve većim financijskim ulaganjima kompanija (još uvijek većinom iz privatnog sektora) postaju dio tehnološke stvarnosti, te se za njih pronalazi praktična primjena. Izgradnja takvog računala dovoljne snage mogla bi bitno utjecati na daljnji razvoj kriptologije kao znanosti. Cilj istraživanja je kroz upoznavanje sa algoritmima kvantne i post-kvantne kriptografije (s naglaskom na Shorov algoritam i kvantnu distribuciju ključa) ukazati na potencijale upotrebe kvantnih računala u polju kriptologije. Razmatraju se kvantnomehanički principi koji se primjenjuju u teoriji o kvantnim računalima i teoriji o kvantnoj informaciji koje se na nizu razina razlikuju od klasičnih informacija. Uvodi se pojam kvantnog bita (eng. *Qubit*), višequbitnih stanja, tenzorskih produkata stanja i operatora. Kroz povijesni pregled formalno-logičke i fizičke realizacije kvantnih računala ukazuje se na trenutačna tehnološka ograničenja i prepreke za njihovu implementaciju u šire svrhe, te se predlažu potencijalna rješenja za njihovo premošćivanje.

Ključne riječi: kriptologija, kvantno računalo, kvantna distribucija ključa, kvantna kriptografija

Potential of using quantum computers in the field of cryptology

Summary

Following fast technical advances caused by financial investment of large comapanies (still mostly private) quantum computers are becoming a part of technological reality and practical use for them is being found. Building a large scale quantum computer could strongly affect the development of cryptology as a science. Goal of the reasearch is to point out the potentials of using quantum computers for cryptological purposes by getting familiar with algorithms of quantum and post-quantum cryptography, with special emphasis on Shor's algorithm and quantum key distribution. Quantum mechanical principles on which quantum computing and the theory of quantum information (which is much different than classical information) are based are being discussed and explained. Current technological barriers for a wide implementation of the technology are highlighted through the process of historical overview of its development and possible solutions are discussed.

Key words: cryptology, quantum computer, quantum key distribution, quantum cryptography