

**UNIVERZITET SINGIDUNUM**

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER PROGRAM: SAVREMENE INFORMACIONE TEHNOLOGIJE

Slaven Ijačić

**Primena kvantne mehanike u kriptografiji, kvantno  
računarstvo i post-kvantni šifarski sistemi**

- Master rad -



**Beograd, 2014.**



**UNIVERZITET SINGIDUNUM**

**-MASTER STUDIJSKI PROGRAM-  
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Slaven Ijačić

**Primena kvantne mehanike u kriptografiji, kvantno  
računarstvo i post-kvantni šifarski sistemi**

- Master rad -

**Mentor:**  
**prof. dr Mladen Veinović**

**Student: Slaven Ijačić**  
**br.indeksa: 410154/2012**



**Beograd, 2014.**

## **Primena kvantne mehanike u kriptografiji, kvantno računarstvo i post-kvantni šifarski sistemi**

### **Sažetak**

Ovaj rad istražuje primenu kvantne mehanike u kriptografiji, principe kvantnog računarstva, moguće napade na moderne šifarske sisteme sa javnim ključem primenom Šorovog kvantnog algoritma na rešavanje problema faktORIZACIJE prirodnih brojeva i diskretnih logaritama u realnom vremenu. Istražena je tehnologija kvantne distribucije ključeva (QKD) koja omogućuje bezuslovno sigurnu razmenu tajnih ključeva između dve strane primenom kvantno-mehaničkih fenomena. Opisana je klasa takozvanih post-kvantnih šifarskih sistema koji su otporni na napade primenom kvantnih računara i data preporuka za njihovu primenu u sigurnosnim protokolima za internet komunikaciju.

Ključne reči: RSA/ECDH, SSL/TLS, šifarski sistemi sa javnim ključem, faktORIZACIJA prirodnih brojeva, diskretni logaritmi, klase kompleksnosti algoritama, kvantna mehanika, kvantni računari, kvantne operacije, kvantni algoritmi, kubiti, kvantana superpozicija, kvantno korelisani sistemi, dekoherencija kvantnog sistema, reverzibilna logika, unitarne operatori, Šorov algoritam, kvantna simulacija, Kvantna distribucija ključeva, BB84, ERP/E91, SARG04, post-kvantni šifarski sistemi, NTRU, GGH, Mekelis, Niderajter, Merkel

## **Application of quantum mechanics in cryptography, quantum computing and post-quantum crypto-systems**

### **Abstract**

This paper explores application of quantum mechanics in cryptography, principles of quantum computing, potential attacks on contemporary public-key crypto-systems applying Schor's quantum algorithm to solving problems of integer factorization and discrete logarithms in real time. Quantum Key Distribution technology is explored, which enables unconditionally secure generation and distribution of secret keys between two parties using quantum mechanics phenomena. Class of so-called post-quantum public-key systems, resistant to attacks using quantum computers, is described and recommendations provided for their application in contemporary internet security protocols.

Keywords: RSA/ECDH, SSL/TLS, public-key crypto-systems, integer factorization, discrete logarithm, algorithm complexity classes, quantum mechanics, quantum computer, quantum operations, quantum algorithms, qubit, quantum superposition, entanglement, quantum system decoherence, reversible logic, unitary operators, expected values, Shor's algorithm, quantum simulation, quantum key distribution (QKD), BB84, ERP/E91, SARG04, post-quantum crypto-systems, NTRU, GGH, McEliece, Niederreiter, Merkel

## Sadržaj:

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| 1. Metodologija istraživačkog rada .....                                        | 9  |
| 1.1. Uvodne napomene .....                                                      | 9  |
| 1.2. Predmet istraživanja .....                                                 | 9  |
| 1.3. Hipotetički okvir .....                                                    | 9  |
| 1.4. Ciljevi istraživanja .....                                                 | 9  |
| 1.5. Metode istraživanja i tok istraživačkog procesa .....                      | 10 |
| 2. Opšti pojmovi u kriptografiji .....                                          | 10 |
| 2.1. Simetrični šifarski sistemi .....                                          | 11 |
| 2.2. Šifarski sistemi sa javnim ključem (public-key) .....                      | 12 |
| 2.3. SSL/TLS protokoli za sigurnu komunikaciju na internetu .....               | 14 |
| 3. Osnovne ideje kvantne mehanike .....                                         | 14 |
| 3.1. Hilbertovi prostori i stanja kvantnog sistema .....                        | 18 |
| 3.2. Očekivane vrednosti i linearni operatori .....                             | 22 |
| 3.3. Unitarni operatori .....                                                   | 24 |
| 3.4. Nemogućnost kopiranja stanja i dekoherencija kvantnog sistema .....        | 25 |
| 4. Kvantno generisanje i distribucija ključeva (Quantum Key Distribution) ..... | 26 |
| 4.1. BB84 protokol .....                                                        | 28 |
| 4.2. EPR/E91 (Einstein- Podolsky-Rosen) protokol .....                          | 32 |
| 4.3. SARG04 protokol .....                                                      | 35 |
| 4.4. Praktična ograničenja QKD tehnologije .....                                | 37 |
| 4.5. Implementacije QKD tehnologije .....                                       | 38 |
| 5. Osnove kvantnog računarstva .....                                            | 39 |
| 5.1. Kvantni bit – Kubit (Qubit) .....                                          | 41 |
| 5.2. Kvantni registri .....                                                     | 44 |
| 5.3. Kvantno korelisani sistemi (entanglement) .....                            | 46 |
| 5.4. Kvantne operacije i logička kola .....                                     | 48 |
| 5.5. Dijagrami kvantnih kola .....                                              | 58 |
| 5.6. Priroda rezultata i ograničenja kvantnih računara .....                    | 60 |

|        |                                                                         |    |
|--------|-------------------------------------------------------------------------|----|
| 5.7.   | Kvantni algoritmi: Dojč-Joža, Grover, QFT, Kvantna simulacija .....     | 64 |
| 5.8.   | Šorov algoritam .....                                                   | 66 |
| 5.9.   | Simulacija rada kvantnog računara .....                                 | 72 |
| 5.10.  | Primer komercijalnog kvantnog uređaja .....                             | 73 |
| 5.11.  | Perspektive kvantnog računarstva.....                                   | 74 |
| 6.     | Post-kvantna kriptografija .....                                        | 77 |
| 6.1.   | Šifarski sistemi na bazi rešetke (Lattice-based Cryptography) .....     | 78 |
| 6.1.1. | NTRU šifarski sistem .....                                              | 83 |
| 6.1.2. | GGH šifarski sistem.....                                                | 87 |
| 6.2.   | Šifarski sistemi na bazi kodova (Code-based Cryptosystems).....         | 88 |
| 6.2.1. | Mekelis šifarski sistem (McEliece) .....                                | 89 |
| 6.2.2. | Niderajter šifarski sistem (Niederreiter).....                          | 93 |
| 6.3.   | Drugi post-kvantni sistemi .....                                        | 93 |
| 6.3.1. | Merkle šema za digitalni potpis.....                                    | 93 |
| 6.3.2. | Šifarski sistemi na bazi multivariabilnih kvadratnih polinoma (MQ)..... | 95 |
| 7.     | Zaključak .....                                                         | 97 |
| 8.     | Reference .....                                                         | 99 |

## Spisak slika:

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Slika 1 – Oblik Šredingerove jednačine zavisne od vremena .....                                             | 16 |
| Slika 2 – Oblik Šredingerova jednačine nezavisne od vremena .....                                           | 16 |
| Slika 3 - Orbitale atoma hidrogena su ajgen-funkcije energije – plot verovatnoće pozicije elektrona .....   | 17 |
| Slika 4 – Matematički izraz Hajzenbergovog principa neodređenosti .....                                     | 18 |
| Slika 5 - Jedinični vektori $i, j, k$ formiraju ortonormalni basis u Euklidskom prostoru $R^3$ .....        | 19 |
| Slika 6 - Linearna polarizacija svetlosti .....                                                             | 27 |
| Slika 7- Moguće pozicije Bobovog polarizacionog detektora: vertikalna i dijagonalna orijentacija .....      | 28 |
| Slika 8 - Moguće polarizacije Alisinih emitovanih fotona .....                                              | 29 |
| Slika 9 - Deflekcija fotona na “vertikalnom” detektoru, “vertikalni” foton levo, “horizontalni” desno ..... | 29 |
| Slika 10 - Fotoni sa dijagonalnom polarizacijom, 50:50 verovatnoća za promenu polarizacije u v. ili h ...   | 29 |
| Slika 11 - Odnos razdaljine između Alise i Boba i realne stope generisanja ključeva (bps) .....             | 38 |
| Slika 12 - Blohova sfera – model qubita .....                                                               | 43 |
| Slika 13 - Hadamardovo kolo .....                                                                           | 50 |
| Slika 14 - Paulijevo X kolo .....                                                                           | 50 |
| Slika 15- Paulijevo Y kolo .....                                                                            | 50 |
| Slika 16 - Paulijevo Z kolo .....                                                                           | 50 |
| Slika 17 - S kolo .....                                                                                     | 51 |
| Slika 18 - T kolo .....                                                                                     | 51 |
| Slika 19 - $R(\theta)$ kolo .....                                                                           | 51 |
| Slika 20 - Swap kolo .....                                                                                  | 52 |
| Slika 21 - CNOT kolo .....                                                                                  | 52 |
| Slika 22 - Tofolijevo kolo .....                                                                            | 53 |
| Slika 23 - Fredkinovo kolo .....                                                                            | 54 |
| Slika 24 - $R_k$ kolo .....                                                                                 | 54 |
| Slika 25 - $R_x$ kolo .....                                                                                 | 54 |
| Slika 26 - $R_y$ kolo .....                                                                                 | 55 |
| Slika 27 - $R_z$ kolo .....                                                                                 | 55 |
| Slika 28 - Identitet .....                                                                                  | 55 |
| Slika 29 - Merenje stanja .....                                                                             | 56 |
| Slika 30 - Kolo za Volšovu transformaciju .....                                                             | 56 |
| Slika 31 - Kolo za kontrolisano U sa jednim kontrolnim i $(n-1)$ ciljnih kubita .....                       | 56 |
| Slika 32 - Kolo za kontrolisano U sa $(n-1)$ kontrolnih i jednim ciljnim kubitom .....                      | 57 |
| Slika 33 - QFT kolo .....                                                                                   | 57 |
| Slika 34 - Inveržno QFT kolo .....                                                                          | 58 |
| Slika 35 - Kolo za promenu redosleda kubita .....                                                           | 58 |
| Slika 36 - Identitet na $n$ kubita .....                                                                    | 58 |
| Slika 37 - Dijagram kvantnog kola sa 3 kubita i 3 proizvoljne kvantne operacije .....                       | 59 |
| Slika 38 - Kontrolni kubit $q_0$ kvalifikuje izvršavanje operacije X na ciljnom kubit $q_1$ .....           | 59 |
| Slika 39 - Kontrolni kubit $q_0$ , ciljni kubit $q_2$ , kubit $q_1$ ne učestvuje u operaciji .....          | 59 |

|                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------|----|
| Slika 40 - Kubit $q_0$ stavljen u superpoziciju stanja primenom Hadamardovog kola, sa merenjem stanja . | 60 |
| Slika 41 - Primenom Hadamardovog kola na $q_0$ , i CNOT na $q_1$ nastaje EPR par .....                  | 60 |
| Slika 42 - Proces izvršavanja programa na kvantnom i konvencionalnom (klasičnom) računaru .....         | 61 |
| Slika 43 - Odnos BQP klase i klasičnih klasa kompleksnosti problema .....                               | 64 |
| Slika 44 - Prikaz toka Šorovog algoritma po fazama .....                                                | 67 |
| Slika 45 - Dijagram kvantnog kola za implementaciju faze 2 Šorovog algoritma .....                      | 71 |
| Slika 46 - Primena Hadamardove operacije nad $n$ kubita .....                                           | 71 |
| Slika 47 - Dijagrami kvantnih kola za sumu, prenos, i inverzni prenos kod implementacije $U_f$ .....    | 72 |
| Slika 48 - Dijagram kvantnog kola za QFT .....                                                          | 72 |
| Slika 49 - D-Wave 2 - adiabatiski kvantni računarski sistem i verzija Rainer procesora sa 128 qb .....  | 74 |
| Slika 50 - D-Wave 2 – detalji kriogenog postrojenja .....                                               | 74 |
| Slika 51 - Gartnerova skala novih tehnologija i pozicija kvantnog računarstva .....                     | 76 |
| Slika 52 - Pet osnovnih tipova rešetki u Euklidskoj ravni .....                                         | 79 |
| Slika 53 - Primer SVP problema na rešetci $L$ generisanoj na $\mathbb{R}^2$ .....                       | 80 |
| Slika 54 - Primer CVP problema na rešetci $L$ generisanoj na $\mathbb{R}^2$ .....                       | 80 |
| Slika 55 - Prvobitni bazis $(v_1, v_2)$ i redukovani bazis $(u_1, u_2)$ .....                           | 81 |
| Slika 56 - Primer Merkle drveta .....                                                                   | 94 |

## Spisak Tabela:

|                                                                                                   |    |
|---------------------------------------------------------------------------------------------------|----|
| Tabela 1 - Primer kvantnog alfabeta.....                                                          | 27 |
| Tabela 2 - Mapiranje kvantnih stanja u polarizacije fotona i odgovarajuće binarne vrednosti ..... | 28 |
| Tabela 3 - Slanje informacije kroz kvantni kanal uz odbacivanje nekorelisanih bitova .....        | 29 |
| Tabela 4 - Međusobno neortogonalni kvantni alfabeti .....                                         | 34 |
| Tabela 5 - Primer sekvence bitova sa objavljenim stanjima – SARG04 .....                          | 36 |
| Tabela 6 - Varijable u Šorovom algoritmu .....                                                    | 66 |
| Tabela 7 - Preporučene vrednosti parametara za NTRUEncrypt .....                                  | 86 |

## **1. Metodologija istraživačkog rada**

### **1.1. Uvodne napomene**

Osnovni zadatak ovog rada je istraživanje prostora kvantne mehanike i njena primena u domenu kriptografije, kako bi se razumele mogućnosti i ograničenja, kao i prvenstveno potencijalni uticaj na današnje public-key šifarske sisteme odnosno sigurne komunikaciju putem interneta.

### **1.2. Predmet istraživanja**

Predmet istraživanja je analiza i potpuno sagledavanje teorijske osnove kvantnih računara sa naglaskom na primenu Šorovog algoritma, odnosno mogućnost rešavanje problema faktorizacije velikih brojeva i diskretnih logaritama, u polinomijalnom vremenu, u kontekstu napada na postojeće public-key algoritme. Istraživanje uključuje i postojeće protokole kvantne distribucije javnog ključa, kao i glavne kadidate za klasične post-kvantne šifarske sisteme, odnosno sisteme koji se smatraju otpornim na napade primenom posebnih algoritama koji se izvršavaju na kvantnim računarima.

### **1.3. Hipotetički okvir**

Generalna ili opšta hipoteza: Mogućnost sigurne razmene podataka na internetu je od ključne važnosti za trgovinu putem interneta kao i za zaštitu privatnosti svih korisnika.

Posebna ili radna hipoteza: Postoji realna opasnost da se današnji public-key šifarski sistemi koji se koriste u današnjim protokolima za sigurne komunikacije na internetu, kao što su RSA i EC Helman-Difi, kompromituju primenom kvantih računara u realnom vremenu.

Pojedinačna hipoteza: Danas postoje public-key šifarski sistemi koji su otporni na napade primenom kvantnih računara i koji su praktični i primenjivi na obezbeđivanje sigurnosti internet komunikacija, kao i tehnologije za generisanje i distribuciju javnih ključeva primenom fenomena kvantne mehanike.

### **1.4. Ciljevi istraživanja**

Naučni cilj ovog istraživanja je analiza i razumevanje uticaja kvantnih računara u domenu public-key šifarskih sistema radi predviđanja trendova u razvoju budućih šifarskih sistema odnosno obezbeđivanja sigurnih internet komunikacija u budućnosti.

Konkretni cilj ovog istraživanja je pronalaženje odgovora na sledeća pitanja:

- Koje izazove donosi razvoj kvantnih računara u domenu public-key šifarskih sistema?
- Koji su osnovni principi rada kvantih računara i na koji način primena kvantnih računara može da ugrozi današnje public-key šifarske sisteme?
- Šta je kvantno generisanje i distribucija ključeva i kakve su mogućnosti odnosno ograničenja ove tehnologije?

- Šta su post-kvantni šifarski sistemi i kakve su karakteristike i praktične mogućnosti ovih public-key šifarskih sistema?

### **1.5. Metode istraživanja i tok istraživačkog procesa**

Osnovne metode: Istražen je teorijski prostor kvantnog računarstva, tehnologija i nivo razvoja postojećih implementacija kvantnih računara, kao i procena trendova razvoja ove oblasti. Za potrebe istraživanja izvršena je analiza postojećih tehnologija, algoritama i protokola i teorijski uticaj kvantnih računara na sadašnje public-key šifarske sisteme. Analizirani su postojeći protokoli za kvantno generisanje i distribuciju ključeva, njihove prednosti i ograničenja kao i postojeće komercijalne implementacije. Istražena je dostupna literatura u vezi glavnih kandidata za post-kvantne šifarske sisteme i date preporuke za primenu u sadašnjim sigurnosnim protokolima na internetu.

Statističke metode: Korišćeni su podaci iz literature u vezi kompleksnosti različitih public-key algoritama kao i njihove uporedne kompleksnosti iz radova i izvora koji su dati u sekciji literatura.

Eksperimenti: U cilju lakšeg razumevanja principa rada kvantnih računara detaljno je objašnjen Šorov algoritam a zatim i prikazan primer faktorizacije relativno malog proizvoda prirodnih brojeva primenom ovog algoritma sa klasičnom i kvantnom QFT fazom uporedo. Detaljno je objašnjen princip rada protokola BB84 za kvantno generisanje i distribuciju ključeva, uz odgovarajuće primere. Dati su principi rada glavnih post-kvantnih algoritama sa detaljnim primerima generisanja ključeva, kao i šifrovanjem i dešifrovanjem poruka.

Tok istraživačkog procesa: Na početku je izvršena analiza današnjih protokola za sigurnu komunikaciju na internet, kao i odgovarajući public-key šifarski sistemi koji su osnova navedenih protokola. Potom je izvršeno prikupljanje informacija kako bi se definisala hipoteza o potencijalnom uticaju kvantnih računara na ove sisteme. Nakon toga je izvršeno obimno istraživanje u domenu kvantne mehanike i principa rada kvantnih računara i tehnologije i protokola kvantne distribucije ključeva. Zatim je izvršena analiza glavnih kandidata za potencijalne post-kvantne šifarske sisteme kao i detaljno istraživanje pojedinačnih sistema u ovom domenu. Na kraju rada dat je zaključak u pogledu procenjenog rizika kao i definisanje potrebnih koraka kako bi se osigurao kontinuitet sigurnih internet komunikacija u kontekstu novih post-kvantnih šifarskih sistema koji bi zamenili postojeće potencijalno ranjive public-key šifarske sisteme, kao i preporuka u vezi primene sistema za kvantno generisanje i distribuciju ključeva, sa njihovim mogućnostima i ograničenjima.

## **2. Opšti pojmovi u kriptografiji**

Kriptografija se bavi istraživanjem i primenom tehnika sigurne komunikacije u prisustvu treće strane, kojoj generalno nije dozvoljen uvid u komunikaciju. Kriptografija je deo šireg polja kriptologije, koja uključuje i kriptanalizu koja obuhvata tehnike razbijanja kodova. Osnovni cilj

kriptografije je da se omogući zaštićena komunikacija između dve strane i da se obezbedi autentičnost poruke, odnosno da se onemogući da treća strana, protivnik, izmeni sadržaj poruke. Da bi se postigli ovi zahtevi koriste se šifarski algoritmi (transformacije) koje kombinuju poruku (otvoreni tekst) sa dodatnom informacijom koja se zove šifarski ključ, i proizvode šifrat. Potreban uslov je da je nemoguće dešifrovati šifrat bez odgovarajućeg ključa, ali i uslov da se korišćenjem adekvatnog algoritma izgube određene karakteristike otvorenog teksta, kao što je frekvencija karaktera u datom jeziku, koje bi mogle olakšati napad na šifrat. U principu, da bi dešifrovao poruku, primalac mora da izvrši obrnutu transformaciju (dešifrovanje ili dekripciju) koristeći odgovarajući ključ. Iako je poverljivost poruke tradicionalni cilj kriptografije, danas je važno i kreiranje digitalnih potpisa radi obezbeđivanja autentičnosti, integriteta i neporecivost informacija kod komunikacije.

Postoje dve osnovne grupe algoritama, zavisno od toga da li Alisa (pošiljalac) i Bob (primalac) koriste dva različita ali povezana ključa ili oboje koriste isti ključ za šifrovanje i dešifrovanje. U prvom slučaju to su asimetrični šifarski sistemi, dok se u drugom slučaju govori o simetričnim šifarskim sistemima. Neophodno je istaći da se asimetrični sistemi koji generalno intenzivnije koriste računarske resurse, najčešće koriste za generisanje i razmenu tajnog ključa između Alise i Boba putem sigurnog kanala. Potom se tajni ključ koristi u simetričnom šifarskom sistemu, koji generalno troši znatno manje računarskih resursa, i na kome se bazira zaštićena komunikacijska sesija između Alise i Boba. (Striktno, Alisa i Bob razmenjuju sirovi ključ na osnovu kog se, uz određene javne i/ili tajne informacije, generiše sesijski ključ koji se koristi za šifrovanje otvorenog teksta). Način generisanja, razmene i upravljanja tajnim ključevima svakog simetričnog šifarskog sistema je ključni izazov u kriptografiji.

## **2.1. Simetrični šifarski sistemi**

Simetrični šifarski sistemi koji koriste isti ključ za šifrovanje i dešifrovanje poruka su bili jedini sistemi u primeni do pronalaska asimetričnih šifarskih sistema sa javnim ključem (public-key). Ovi konvencionalni algoritmi se tradicionalno zasnivaju na metodama zamene i/ili transpozicije karaktera odnosno bita u otvorenom tekstu, često u više sukcesivnih faza, kako bi se dobio šifrat. Fundamentalni zahtev je da su ove operacije reverzibilne, i da nema gubitaka informacija iz poruke. Tajni ključ je uvek nezavisan od algoritma koji se koristi, kao i sadržaja poruke. Korišćeni simetrični šifarski algoritam, ako se primene dva različita ključa, mora od istog teksta poruke uvek proizvesti dva potpuno različita i nekorelisana šifrata, što zavisi i od kvaliteta algoritma i pravilnog izbora i dužine ključa. S druge strane korišćenje ključeva velike dužine i veoma komplikovanih algoritama je ograničeno dostupnim računarskim resursima, potrebi resinhronizacije sigurnog komunikacionog kanala, i drugim faktorima, koji zajedno utiču na smanjenje propusnog opsega kanala.

Današnji simetrični algoritmi se dalje dele na blok šifarske algoritme (block cipher) koji se primenjuju na blokovima podataka, i šifarske algoritme koji se primenjuju na nizovima bitova (stream cipher). Standardni blok algoritmi su DES, 3DES, IDEA, AES. Standardni "stream" algoritmi su RC4 i drugi. Bitno je istaći da je šifarski algoritam bezuslovno siguran samo ako šifrat koji je generisan

nikad ne sadrži dovoljno informacija da bi se jedinstveno odredio njegov odgovarajući otvoreni tekst, bez obzira na količinu šifrata koji je na raspolaganju kriptanalistu.

Kao ekstreman slučaj koji je jedini zaista bezuslovno siguran poznat je algoritam sa tablicom za jednokratnu upotrebu (engl. one-time pad), poznata kao Vernamova šifra otkrivena 1926. godine. Otvoreni tekst se posmatra kao niz bitova koji se bit-po-bit sabira sa tajnim ključem. Praktično se primenjuje XOR operacija između sukcesivnih bitova poruke i ključa. Navedeni šifarski sistem je bezuslovno siguran ali postoje ozbiljni problem u vezi generisanja, distribucije i upravljanja ključevima. Generisani ključ mora biti potpuno slučajan niz bitova, što nije jednostavan zadatak, a ključ mora da bude dug koliko i poruka, i što je jako važno može da se koristi samo jednom. Evidentan je problem distribucije tajnog ključa između Alise i Boba, te se svaki ključ mora distribuirati jednoj ili obema stranama sigurnim kanalom (kurir, predefinisani nizovi ključeva, diplomatska pošta). Ovo je ekstremni primer problema razmene ključeva koji je problem za sve konvencionalne šifarske sisteme, a kao jedno rešenje ovog problema 70-ih godina pojavljuju se asimetrični šifarski sistemi.

## **2.2. Šifarski sistemi sa javnim ključem (public-key)**

Jedan od najtežih problema u kriptografiji je problem efikasne razmene tajnih ključeva. Bez obzira koliko je neprobojan pojedini šifarski algoritam, pitanje efikasnog i sigurnog generisanja, distribucije, i upravljanja ključevima je od nemerljivog značaja za funkcionisanje celog sistema. Drugi izazov je pitanje digitalnih potpisa, koji osiguravaju autentičnost, integritet i neporecivost poruka, što je posebna klasa problema i predmet mnogih istraživanja. Sredinom 1970-ih godina se pojavljuju šifarski sistemi sa javnim ključem (engl. public-key), koji donose određena rešenja za ove probleme. Smatra se da je to jedan od najvažnijih proboja u istoriji kriptologije.

Prvi protokol sa javnim ključem (engl. public-key") su 1976 objavili Difi i Helman (Whitfield Diffie, Martin Hellman) sa Univerziteta Stanford, po kojima je i dobio ime. Kod šifarskog sistema sa javnim ključem, jedan ključ se koristi za šifrovanje a drugi ključ, koji je vezan za prvi, za dešifrovanje poruka. Suština efektnosti DH šifarskog sistema je nemogućnost lakog izračunavanja diskretnih logaritama. 1978. godine Rivest, Šamir, i Adlema sa MIT-a. (Rivest, Adi Shamir, Leonard Adleman) su objavili RSA algoritam, koji je dobio ime po inicijalima pronalazača. Ovaj public-key šifarski sistem radi na principu složenosti faktORIZACIJE proizvoda dva velika prosta broja. Poznati šifarski sistemi iz ove klase koji se više ili manje koriste su El Gamal, YAK, DSS (digital signature standard), razne šeme sa eliptičnim krivama (engl. elliptic curves), Paillier, i drugi sistemi.

### **Princip rada public-key šifarskih sistema**

Sledeći primer komunikacije između Alise i Boba možeda se odvija putem bilo kojeg medijuma, telefona ili čak pisanih poruka, iako bi danas najverovatnije koristili internet. Ako Bob želi da prima poruke šifrovane javnim ključem on prvo generiše svoj privatni ključ koji je poznat samo

njemu. Zatim on generiše javni ključ, na osnovu svog privatnog ključa, i objavljuje javni ključ svim zainteresovanim stranama. Alisa koristi Bobov javni ključ da šifrue svoju poruku, šalje je Bobu koji poruku dešifrue svojim privatnim ključem. Moguće je da Alisa takođe generiše svoj privatni ključ i javni ključ koji deli sa Bobom. Na ovaj način oni bez prethodne definisane zajedniče tajne razmenjuju određene podatke na siguran način kroz neki javni kanal za komunikaciju.

U realnoj situaciji mogu se prepoznati dve faze u komunikaciji između Alise i Boba. U prvoj fazi komunikacije oni koriste public-key šifarski sistemi kao što je RSA ili (EC)DH da bi se pripremila sigurna komunikacija. Alisa i Bob u ovoj fazi razmenjuju određene podatke koristeći javni i privatni ključ preko otvorenog kanala kako bi oboje na početku dogovorili parametre simetričnog šifarskog sistema koji će da koriste (npr. AES/DES/3DES) i razmenili odgovarajući zajednički tajni ključ. Nakon toga počinje druga faza komunikacije putem simetričnog šifarskog sistema korišćenjem izabranog tajnog ključa koja traje dok neka od strana ne želi da prekine komunikaciju ili eventualno promeni parametre ili generiše novi tajni ključ. U tom slučaju ponavlja se prva faza komunikacije. Suština je da je nemoguće je od Alisinog javnog ključa na neki način dobiti Bobov privatni ključ. Važno je napomenuti da su sve ove public-key šeme sigurne samo ako je autentičnost javnog ključa osigurana. Time se onemogućuje man-in-the-middle napad, gde napadač preuzima ulogu Boba dok je Alisa uverena da komunicira sa Bobom. Jedan od načina je korišćenje sertifikata od takozvanih autoriteta za sertifikate (X.509 standard) i mreža poverenja. Zajedno ti protokoli i pravila se nazivaju PKI (engl. public-key infrastructure), što predstavlja javni i transparentni način verifikacije identiteta nekog entiteta (organizacije/kompanije) kao stvarnog vlasnika izdatih javnih ključeva.

Drugi važan aspekt public-key sistema je autentifikacija poruka kojom se obezbeđuje integritet (poruka nije promenjena u tranzitu), autentičnost (poruka je od poznatog pošiljaoca) i neporecivost poruke (ne može se reći da je neko drugi poslao poruku umesto pošiljaoca). Ovaj process uključuje kreiranje takozvanog dajžesta (engl. digest) ili heša (engl. hash) na osnovu sadržaja poruke, odnosno kratkog sadržaja ili otiska poruke, dužine do par stotina bita. Važno je istaći da se minimalnom promenom poruke odgovarajući heš drastično menja i da je u praktičnim uslovima nemoguće dobiti isti heš za dve različite poruke, niti se može iz heša dobiti neka korisna informacija u vezi sadržaja poruke. Za kreiranje heša koriste se takozvane heš funkcije kao što su SHA-1/2. Heš te poruke se zatim širuje privatnim ključem pošiljaoca i sada kao digitalni potpis šalje uz šifrovanu poruku. Primalac koristi svoj javni ključ kako bi dešifrovao digitalni potpis i poruku, izračunao heš na osnovu dešifrovane poruke uporedio sa prvobitnim hešom i potvrdio da je digitalni potpis validan.

### **Matematička osnova public-key šifarskih sistema**

Sigurnost public-key sistema počiva na posebnim klasama jednosmernih (engl. one-way) funkcija kod kojih je lako izračunati svaku vrednost u domenu funkcije  $f(x)$  ali je veoma teško rešiti inverznu funkciju  $f^{-1}$  za slučajnu vrednost funkcije  $f(x)$ . Pod pojmom "težina rešavanja inverzne funkcije" podrazumeva se činjenica da vreme koje je potrebno da se korišćenjem bilo kojih računarskih resursa reši zadata funkcija raste najmanje eksponencijalno sa porastom veličine argumenta funkcije. Pojam

težine rešavanja problema, pod određenim uslovima koje obično znače dovoljno veliki privatni ključ, može da bude ekvivalentan radu svih današnjih računarskih resursa u svetu idućih 1000 godina.

Kod navedenih klasa jednosmernih funkcija takođe postoje tajna vrata (engl. trap door) koja omogućuju trivijalno lako rešenje, ako je poznata određena informacija. RSA algoritam koristi faktorisanje velikih prostih brojeva kao one-way funkciju dok DH koristi problem rešavanja diskretnog logaritma. Oba problema su teška ali nikada nije bezuslovno dokazano da ne postoji efikasan algoritam koji omogućuje rešavanje problema u polinomijalnom vremenu.

### **2.3. SSL/TLS protokoli za sigurnu komunikaciju na internetu**

Sigurnost komunikacija na internetu danas je realna potreba svih korisnika, bilo da je to plaćanje računa putem interneta (e-banking), povezivanje mobilnim uređajima na internet putem wifi mreža, ili prijavljivanje na web sajtove koji sadrže privatne podatke poput socijalnih mreža. TLS/SSL protokoli su osnova sigurnih komunikacija na internetu, uključujući web (https), email, IM (instant messaging), i VoIP, a TLS 1.2 je poslednja verzija novijeg od dva protokola.

Oba protokola koriste varijacije RSA i DH public-key šifarskih sistema, kao i X.509 sertifikate za autentifikaciju učesnika u komunikaciji. TLS/SSL se inicijalizuju na nivou 5 OSI modela a rade na nivou 6. TLS/SSL implementira inicijalizaciju zaštićene komunikacije putem takozvanog hendšejka (engl. handshake), procesa kojim se definišu parametri razmene podataka, razmenjuju odgovarajući sertifikati i prelazi u fazu razmene podataka između klijenta i server korišćenjem javnih i privatnih ključeva, kako bi se generisao zajednički tajni ključ koji će se koristiti za komunikaciju korišćenjem dogovorenog simetričnog šifarskog sistema. Zaključak je da sigurnost komunikacija na internetu zavisi direktno od public-key sistema kao što su Difi-Helman i RSA, pa se ovaj rad fokusira na istraživanje sigurnosti ova dva sistema.

## **3. Osnovne ideje kvantne mehanike**

Do kraja 19. veka fizički svet je mogao biti objašnjen, principima njutnovske (engl. Isaac Newton) klasične mehanike. Početkom 20. veka postavljaju se nova pitanja o fizičkom svetu zahvaljujući rezultatima eksperimenata koje klasična teorija nije mogla da objasni. Javlja se teorija relativiteta i kvantne mehanike, teorije koje pokušavaju da objasne pojedine eksperimentalne rezultate. Teorija relativiteta se pojavljuje prva, pokušavajući da objasni fiziku masivnih i brzih objekata. Za njom se tokom 1920-ih pojavljuje kvantna mehanika kako bi opisala fiziku veoma malih objekata.

Ni jedna od navedenih teorija ne omogućava lak i intuitivan način razumevanja sveta pošto su kontradiktorne pretpostavkama koje pruža poznata njutnovska mehanika u disciplinama koje te

teorije pokušavaju da objasne. Ipak obe teorije mogu da ponove rezultate već opisane njutnovskom mehanikom kad se primene na svakodnevni svet. Da bi se razumela fizika poluprovodnika na atomskom nivou, mora se poći od okvira kvantne mehanike jer njutnovska mehanika nije adekvatna

### **Talasi, čestice i princip dualnosti**

Na makroskopskom nivou navikli smo na dva opšta tipa fenomena: talase i čestice. Čestice su lokalizovani fenomeni koji prenose masu i energiju krećući se u nekom referentnom okviru. Talasi su nelokalizovani fenomeni "razvučeni" u prostoru, koji prenose energiju ali ne i masu prilikom propagacije u prostoru. Analogija čestici u makro svetu može da bude fudbalska lopta koja leti ka jezeru, dok analogija talasu može da bude niz kružnih nabora na površini jezera nastalih udarom fudbalske lopte koji se kreću radijalno od mesta udara – kod talasa postoji prenos energije radijalno putem talasa, ali ne postoji neto prenos mase, jer molekuli vode osciluju oko neke tačke.

U kvantnoj mehanici ne postoji ova uredna razlika između talasa i čestica. Subjekti koje bismo obično smatrali česticama, kao na primer elektroni, mogu da ispoljavaju određena talasna svojstva u određenim situacijama, dok se subjekti za koje se obično misli da su talasi mogu ponašati kao čestice – fotoni kao čestice EM energije odnosno svetlosti. U poznatom eksperimentu u kojem snopovi elektrona koji prolaze kroz proreze na prepreci stvaraju se difrakcione šare na zaslonu veoma slične talasima na površini jezera koji se šire i interferiraju, što navodi na pomisao da elektroni u suštini imaju talasnu prirodu. Na drugoj strani, fotoelektrični efekat u kome elektroni apsorbuju svetlost isključivo diskretnim količinama (kvantima) prikazuju kvantnu prirodu svetlosti, uvodeći koncept fotona.

Ove ideje su dovele francuskog fizičara DeBroglia (DeBroglie) do zaključka, koji je izneo u svojoj doktorskoj tezi 1924. godine, da svi subjekti imaju i talasne i korpuskularne aspekte, kao i da se ti različiti aspekti subjekta manifestuju zavisno od tipa procesa koji se subjektu dešava. Ova teza je postala poznata kao Princip talasno-korpuskularne dualnosti. DeBroglie je nadalje našao odnos momenta čestice i talasne dužine talasa koji odgovara toj čestici:  $p = h/\lambda$ , gde je  $p$  momenat čestice u referentnom okviru, proizvod mase i vektora brzine čestice ( $p=mv$ ) ;  $h$ -tzv. Plankova konstanta, fundamentalna veličina u fizici ;  $\lambda$  – talasna dužina talasa koji odgovara opisanoj čestici. Na osnovu ove relacije moguće je izračunati kvantnu talasnu dužinu čestice na osnovu njenog momenta.

Taj rezultat je veoma značajan jer su talasni fenomeni, kao što je difrakcija, veoma važni kada talasi međusobno dejstvuju sa objektima veličina uporedivih sa talasnim dužinama tih talasa. Na osnovu DeBrogliejeve relacije, talasne dužine svakodnevnih objekata koji se kreću oko nas su veoma male da kvantno-mehanički efekti ne mogu da se primete na makroskopskoj skali na kojoj ljudi spoznaju svet. Na taj način je potvrđeno da je njutnovska mehanika sasvim pogodna za svakodnevnu primenu, što je bitno sa stanovišta opšteg Principa korespondencije. Obrnuto, mali objekti kao što su elektroni imaju talasne dužine uporedive sa mikroskopskim atomskim strukturama (npr. rešetkama) u

čvrstim telima. Kvantno mehanički opisi subjekata, poput elektrona, su neophodni da bi se razumela njihova suština. Sledeće važno pitanje je kako je moguće matematički opisati elektron odnosno njegovu talasnu prirodu.

### Talasna funkcija i Šredingerova jednačina

Austrijski fizičar Ervin Šredinger (Erwin Schrödinger) je 1926. godine predložio talasnu funkciju  $\Psi(\mathbf{r}, t)$  (engl. wave function) čije će promenljive biti vreme i prostorne koordinate, i koja će u sebi da nosi informaciju o čestici, odnosno kvantnom sistemu. Kao rezultat ovog predloga nastala je čuvena Šredingerova jednačina - parcijalna diferencijalna jednačina koja koristi talasnu funkciju  $\Psi$  da opiše pojedini kvantni sistem. Postoje dve forme Šredingerove jednačine, zavisno od fizičkog stanja kvantnog sistema koji se opisuje: forma jednačine koja zavisi od vremena i forma koja ne zavisi od vremena i opisuje stacionarna stanja sistema. (engl. time-dependent/time-independent).

Sledeća jednačina je oblik Šredingerove jednačine za nerelativističke čestice, koja zavisi od vremena (engl. "time-dependant") i ona daje mogućnost predviđanja ponašanja talasne funkcije kada je poznato stanje njene okoline:

$$i\hbar \frac{\partial}{\partial t} \Psi(\mathbf{r}, t) = \left[ \frac{-\hbar^2}{2m} \nabla^2 + V(\mathbf{r}, t) \right] \Psi(\mathbf{r}, t)$$

Slika 1 – Oblik Šredingerove jednačine zavisne od vremena

Informacija o okolini je data u formi potencijala koji bi delovao na česticu u skladu sa klasičnom mehanikom. Ova forma Šredingerove jednačine za nerelativističke čestice koja ne uzima u obzir vreme (engl. "time-independent") opisuje stacionarna stanja čestica odnosno kvantnog sistema:

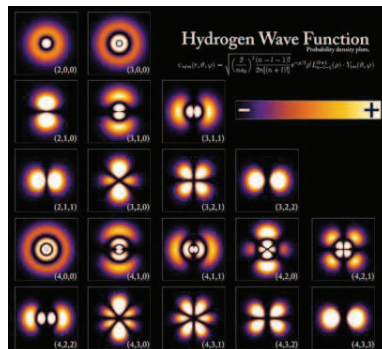
$$E\Psi(\mathbf{r}) = \frac{-\hbar^2}{2m} \nabla^2 \Psi(\mathbf{r}) + V(\mathbf{r})\Psi(\mathbf{r})$$

Slika 2 – Oblik Šredingerova jednačine nezavisne od vremena

### Merenje kvantnih sistema i Hajzenbergov princip neodređenosti

Kad god se izvrši merenje kvantnog sistema, npr. merenje momenta ili pozicije elektrona, rezultat zavisi od talasne funkcije u trenutku u kome je merenje obavljeno. Pokazano je da za svaku moguću veličinu koju bismo da merimo, tzv. merena promenljiva, (engl. observable) postoji skup posebnih funkcija poznatih kao dozvoljene ili ajgen-funkcije (engl. eigenfunctions) koje će uvek vraćati iste dozvoljene (karakteristične) ili ajgen-vrednosti (engl. eigenvalues) za datu merenu

promenljivu. Kažemo i da je talasna funkcija superpozicija dve ili više dozvoljenih funkcija, odnosno matematička linearna kombinacija dozvoljenih funkcija sa odgovarajućim koeficijentima.



Slika 3 - Orbitale atoma hidrogena su ajgen-funkcije energije – plot verovatnoće pozicije elektrona

Šta se dešava tokom merenja stanja kvantnog sistema? Talasna funkcija će naglo da pređe u jednu od dozvoljenih funkcija koje je sačinjavaju. Ovaj događaj se zove kolaps talasne funkcije. Verovatnoća kolapsa talasne funkcije u jedno od dozvoljenih funkcija zavisi od toga koliko dozvoljena funkcija doprinosi prvobitnoj superpoziciji. Nadalje verovatnoća da će data dozvoljena funkcija biti izabrana je proporcionalna kvadratu koeficijenta te dozvoljene funkcije u datoj superpoziciji. Koeficijenti su normalizovani tako da je ukupna verovatnoća suma kvadrata koeficijenata, jedinična. Očigledno postoji ograničen broj diskretnih stanja koja merena promenljiva može da uzme. Pri tome kažemo da je sistem kvantizovan. U trenutku kad je talasna funkcija kolabirala u određenu dozvoljenu funkciju ona će ostati u tom stanju dok je vanjski uticaj ne promeni.

Jedno suštinsko ograničenje kvantne mehanike je izraženo kroz Hajzenbergov princip neodređenosti, kojim se tvrdi da je određena kvantna merenja mogu da poremete sistem i prebace talasnu funkciju ponovo u superponirano stanje. Kao primer uzmimo merenje pozicije čestice koja se kreće u prostoru. Pre nego što je merenje izvršeno talasna funkcija čestice predstavlja superpoziciju dozvoljenih funkcija, gde svaka funkcija odgovara različitoj dozvoljenoj (vrednosti) poziciji čestice. Kada je merenje izvršeno, talasna funkcija kolabira u jedno od dozvoljenih stanja, sa verovatnoćom određenom sastavom prvobitne superpozicije. Tačno jedna pozicija će biti izmerena, i to ona koja je data odgovarajućom dozvoljenom funkcijom, izabranom od čestice.

Ako se merenje pozicije čestice koja se kreće u prostoru izvrši odmah nakon prethodnog merenja, talasna funkcija će biti ista kao i nakon prethodnog merenja jer se ništa novo nie desilo što bi je promenilo. Ako se pak pokuša merenje momenta čestice ( $p=mv$ , proizvod mase i vektora brzine), talasna funkcija čestice će da pređe u neku od dozvoljenih funkcija momenta čestice, koja nije ista kao i dozvoljena funkcija pozicije. Dalje, ako se još kasnije izvrši merenje pozicije čestice, čestica će opet biti u superpoziciji dozvoljenih funkcija pozicije, tako da će izmerena pozicija ponovo zavisiti od verovatnoće. Zaključak je da se ne može izmeriti pozicija i moment čestice u istom trenutku sa

proizvoljnom preciznošću jer se merenjem jedne vrednosti poremeti druga vrednosti. Matematički Hajzenbergov princip za poziciju i moment je izražen sledećom formulom:

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

Slika 4 – Matematički izraz Hajzenbergovog principa neodređenosti

Već pomenuti oblik Šredingerove jednačine koja zavisi od vremena (engl. time-dependant) omogućuje da se izračuna talasna funkcija čestica kad je poznat potencijal u kome se kreću. Važno je istaći da se sva rešenja ove jednačine menjaju u vremenu na neki "talasni" način ali samo određena rešenja se menjaju na predvidljiv sinusoidalni način. Ova posebna rešenja oblika Šredingerove jednačine koja zavisi od vremena su u stvari energetske dozvoljene funkcije (engl. energy eigenfunctions) i mogu se izraziti kroz proizvod faktora koje ne zavisi od vremena i sinusoidalnog faktora koji se menja periodično u vremenu, koji se odnosi na energiju (frekvencija sinusoidalnog talasa je povezana energijom relacijom  $E = h \cdot \nu$ ).

Ne postoji fizičko objašnjenje suštine talasne funkcije, ali talasna funkcija jednostavno sadrži informacije u vezi kvantnog sistema koji ona opisuje. Suštinski jedna od najbitnijih karakteristika talasne funkcije, za primer stacionarne nerelativističke čestice, je da je kvadrat magnitude talasne funkcije te čestice mera verovatnoće nalaženja čestice na određenoj poziciji.

### 3.1. Hilbertovi prostori i stanja kvantnog sistema

Matematički koncept Hilbertovih prostora, nazvan po Dejvidu Hilbertu (engl. David Hilbert), je struktura koja uopštava pojam euklidskog prostora i proširuje metode vektorske algebra i funkcionalne analize sa dvodimenzionalne Euklidske ravni i trodimenzionalnog prostora na prostore bilo koje konačne ili beskonačne dimenzionalnosti. Hilbertov prostor je apstraktni vektorski prostor koji sadrži strukturu unutrašnjeg proizvoda (engl. inner product) koja omogućava merenje dužine i ugla u datom prostoru. Dalje, Hilbertov prostor mora biti kompletan, što znači da postoji dovoljan broj ograničenja na tom apstraktnom prostoru koja omogućuju primenu matematičke analize. Formalno Hilbertov prostor  $\mathcal{H}$  je vektorski prostor na skupu kompleksnih brojeva  $\mathcal{C}$ , sa unutrašnjim proizvodom (engl. "inner product", "dot product") koji proizvodi kompleksne vrednosti

$$(\_, \_) : \mathcal{H} \times \mathcal{H} \rightarrow \mathcal{C}$$

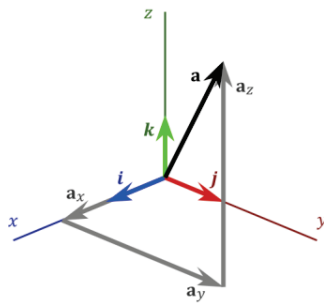
Hilbertov prostor je kompletan s obzirom na normu  $\|u\| = \sqrt{(u,u)}$  nastalu na osnovu definisanog unutrašnjeg proizvoda za svaki element "u", sa sledećim osobinama:

1. Pozitivna konačnost  $(u,u) \geq 0$  ;  $(u, u) = 0$  ako i samo ako je  $u = 0$

2. Simetrični konjugat  $(u,v) = (v,u)^*$  (\* označava konjugat)
3. Linearnost u prvom argumentu  $(u + w, v) = (u,v) + (w,v)$
4. Iz (2) i (3) sledi da je  $(\lambda u, v) = \lambda (u,v)$ , dok je  $(u, \lambda v) = \lambda^* (u,v)$  ( $\lambda \in \mathbb{C}$ )

### Bazisi Hilbertovog prostora

Dimenzionalnost Hilbertovog prostora zavisi od kompleksnosti tog sistema jer svaka dimenzija ovog vektorskog prostora odgovara nekom od nezavisnih fizičkih stanja sistema. Dva vektora u vektorskom prostoru sa definisanim unutrašnjim proizvodom se nazivaju ortonormalnim ako su oba jedinični vektori i međusobno su normalni (okomiti). Skup vektora formira ortonormalni skup ako su svi vektori u skupu međusobno normalni i jedinične dužine. U linearnoj algebri bazis je po definiciji skup linearno nezavisnih vektora kojima se pak, u linearnoj kombinaciji, može izraziti bilo koji vektor u tom vektorskom prostoru. Jedna jednostavnija definicija bazisa je da "definiše koordinatni sistem".



Slika 5 - Jedinični vektori i, j, k formiraju ortonormalni basis u Euklidskom prostoru  $\mathbb{R}^3$

Za svaki Hilbertov prostor možemo da definišemo ortonormalni bazis i svaki vektor stanja u Hilbertovom prostoru može se izraziti kao linearna kombinacija ovog bazisa, s tim da prostor može imati više bazisa. Dva bazisa Hilbertovog prostora su konjugovana ako svaki vektor jednog bazisa ima jednake dužine projekcija na sve vektore drugog bazisa. Dva vektora  $|\alpha\rangle$  i  $|\beta\rangle$  u Hilbertovom prostoru odgovaraju jednakom kvantno-mehaničkom stanju ako postoji kompleksni broj  $\lambda$  takav da je  $|\alpha\rangle = \lambda |\beta\rangle$ .

### Stanja kvantnog sistema

U kvantnoj mehanici kvantno stanje se odnosi na stanje nekog kvantno-mehaničkog sistema. Kao jedan primer takvog sistema je elektron u atomu koji može zauzeti određena stanja u smislu pozicije u atomu, što zavisi direktno od energije elektrona. Primer je i polarizacija fotona kao njegovo unutrašnje stanje koje može da se meri. Nadalje, stanje svakog kvantnog sistema može biti predstavljeno vektorom u Hilbertovom prostoru, koji se tada naziva vektor stanja. Vektor stanja sistema teoretski sadrži statističke informacije o kvantnom sistemu. U matematički striktnoj formulaciji kvantne mehanike dozvoljena stanja (tzv. "čista" stanja) kvantno-mehaničkog sistema su predstavljena jediničnim vektorima, vektorima stanja, koji postoje u kompleksnom separabilnom

Hilbertovom prostoru, koji se naziva i prostorom stanja. Drugim rečima, moguća stanja su tačke u projektivizaciji Hilbertovog prostora, koji se obično naziva kompleksni projektivni prostor.

Stvarna priroda ovog Hilbertovog prostora zavisi od fizičkog kvantnog sistema. Uz Hilbertov prostor može da se definiše i tzv pridruženi ili adžoint (engl. adjoint) prostor nad linearnim funkcijama koji je jednake dimenzije i sa istim bazisom kao i prvobitni Hilbertov prostor.

Svaka posmatrana promenljiva sistema (engl. observable) je nadalje predstavljena sopstvenim linearnim operatorom (engl. self-adjoint linear operator) koji deluje na dati prostor. Suštinski to je linearna funkcija koja deluje na stanja sistema. Svaka dozvoljena vrednost (engl. eigenstate) promenljive sistema odgovara karakterističnom vektoru (engl. eigenvector) operatora, a pridružena karakteristična (dozvoljena) vrednost (engl. eigenvalue) odgovara upravo vrednosti te promenljive u datom dozvoljenom stanju. Takav kvantni sistem je linearna kombinacija dozvoljenih stanja koji u sebi nosi inherentu kvantnu neizvesnost.

Jedan takav sistem može se predstaviti sledećim izrazom u kome je vektor stanja sistema  $|\psi(t)\rangle$ , dozvoljene vrednosti  $|\Phi_n\rangle$ , a koeficijenti  $C_n(t)$  kompleksni brojevi koji omogućuju kvantnu interferenciju između dozvoljenih stanja:

$$|\psi(t)\rangle = \sum_n C_n(t) |\phi_n(t)\rangle$$

Kvantna interferencija je fenomen prisutan isključivo u kvantnoj mehanici i nije vidljiv na makro nivou. Neizvesnost ishoda merenja stanja je evidentna u kvantnoj mehanici, a koeficijenti  $C_n$  nazivaju se amplitude verovatnoće. Kvadrat apsolutne vrednosti svakog od datih koeficijenata (normalizovan) predstavlja verovatnoću da sistem nakon merenja zauzme tu dozvoljenu vrednost.

### Dirakova bra-ket notacija

U kontekstu kvantne mehanike elementi Hilbertovog prostora  $\mathcal{H}$ , po Dirakovoj (Paul Dirac) notaciji se zovu "ketovi" stanja odnosno vektori stanja, a označavaju se sa " $|x\rangle$ " gde je "x" niz karaktera koji u datom kontekstu označava određeno stanje – na primer  $|A\rangle$ ,  $|\psi\rangle$ ,  $|\lambda\rangle$ , ili  $|\uparrow\rangle$ . Dirakova notacija je konvencija i jednostavniji način prezentacije vektora.

Neka je  $\mathcal{H}$  određeni Hilbertov prostor a  $|\psi\rangle$  vektor u tom prostoru koji opisuje stanje nekog kvantnog sistema. Neka je  $|i\rangle$  ortonormalni bazis tog Hilbertovog prostora. U tom slučaju kvantno stanje sistema dato je linearnom kombinacijom ketova datog bazisa

$$|\psi\rangle = \sum_i a_i |i\rangle$$

Koeficijenti  $a_1, a_2 \dots a_n$  su kompleksni brojevi, i važi sledeće:

- $\forall i, a_i = \langle \psi | i \rangle$
- $a_i$  je amplituda verovatnoće da se sistem može naći u stanju  $|i\rangle$
- $|a_i|^2$  je verovatnoća nalaženja kvantnog sistema u stanju  $|i\rangle$
- $\sum_i |a_i|^2 = 1$

U opštem slučaju kvantno stanje sistema predstavljenog gornjim izrazom odgovara superpoziciji svih dozvoljenih stanja kvantnog sistema, od kojih će se merenjem dobiti određeni rezultat. Kvadrati modula koeficijenata  $a_i$  predstavljaju verovatnoće sa kojima će se dobiti mogući (dozvoljeni) rezultati merenja. Neodređenost (verovatnoća) merenja ne počiva na nesavršenost mernih uređaja kojima merimo kvantni sistem nego je ona nerazdvojiva od fizičke situacije.

Neka  $\mathcal{H}^*$  bude skup svih mogućih morfizama (mapiranja odnosno funkcija/linearnih transformacija između dve matematičke strukture),  $\mathcal{H}$  u Hilbertov prostor svih kompleksnih brojeva,  $\mathcal{C}$ .

$$\mathcal{H}^* = H_{\text{omc}}(\mathcal{H}, \mathcal{C})$$

Elementi  $\mathcal{H}^*$  se nazivaju "bra" vektori, označeni sa  $\langle x |$  (gde "x" ima isto značenje u kontekstu kao i odgovarajući naziv za ket) i pripadaju pridruženom (engl. adjoint) prostoru  $\mathcal{H}^*$  koji je jednake dimenzije nad jednakim bazisom kao i prvobitni prostor  $\mathcal{H}$ . Svaki ket  $|\psi\rangle$  ima jedinstveni odgovarajući bra  $\langle \psi |$ , koji odgovara tom fizičkom kvantnom stanju. Striktno bra  $\langle \psi |$  je adžoint (engl. adjoint) keta. Ket se takođe može predstaviti kao vektor kolone, a bra kao a vektor vrste. Uzimajući u obzir zajednički bazis  $|i\rangle$  Hilbertovog prostora i njegovog pridruženog prostora (adžointa), po definiciji je  $\langle i | i \rangle = 1$  dok je  $\langle i | j \rangle = 0$  ako je  $\langle i \neq j \rangle$ . Nadalje, ako je:

$$|\psi\rangle = \sum_i a_i |i\rangle$$

, onda je

$$\langle \psi | = \sum_i a_i^* \langle i |$$

, gde  $a_i^*$  označava konjugat kompleksne amplitude  $a_i$ .

Evaluacija funkcije bra na ket, se može jednostavnije pretstaviti kao  $\langle x_1 | x_2 \rangle$ , odnosno bra-ket proizvod bra  $\langle x_1 |$  i keta  $|x_2\rangle$ . Bra-ket  $\langle \psi | \psi \rangle$  odgovara unutrašnjem proizvodu, odnosno dužini vektora  $|\psi\rangle$  na osnovu sledećeg izraza:

$$\langle \psi | \psi \rangle = \left( \sum_i a_i \langle i | \right) \left( \sum_i a_i^* |i\rangle \right) = \sum_i |a_i|^2 \geq 0$$

Može se dokazati da ako postoje dva keta za bilo koja dva stanja

$$|\psi\rangle = \sum_i a_i |i\rangle \quad , \quad |\phi\rangle = \sum_i b_i |i\rangle$$

, takva da vredi sledeće

$$\langle\phi|\psi\rangle = \left( \sum_i b_i^* a_i \right)$$

, iz čega sledi da je

$$\langle\psi|\phi\rangle = (\langle\phi|\psi\rangle)^*$$

, gde \* označava konjugat. Kvantno-mehanička stanja sistema mogu se takođe predstaviti matricama kompleksnih brojeva kao u sledećem primeru. Ako su bra A i ket B dati sa:

$$|B\rangle = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} \quad , \quad \langle A| = (A_1^* \ A_2^* \ \dots \ A_n^*)$$

, tada je  $\langle A|B\rangle$  unutrašnji proizvod keta  $|A\rangle$  i keta  $|B\rangle$ , jednak

$$\langle A|B\rangle = A_1^* B_1 + A_2^* B_2 + \dots + A_n^* B_n = (A_1^* \ A_2^* \ \dots \ A_n^*) \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

### 3.2. Očekivane vrednosti i linearni operatori

Matematički okvir merenja kvantnog sistema, odnosno konkretnih merenih promenljivih kvantnog sistema (engl. observables), počiva na takozvanim Hermitijan (engl. Hermitian) linearnim operatorima koji deluju na ketove u nekom Hilbetovom prostoru.

Linearni operator na vektorskom prostoru  $V$  je objekat  $Q$  koji linearno transformiše jedan ket u drugi ket - dakle imamo ket  $|\psi\rangle$ , i još jedan ket  $|\phi\rangle = Q|\psi\rangle$ . Ako je  $|\chi\rangle$  treći ket, a  $\alpha$  i  $\beta$  kompleksni brojevi, vredi sledeće:

$$Q(\alpha|\psi\rangle + \beta|\chi\rangle) = \alpha(Q|\psi\rangle) + \beta(Q|\chi\rangle)$$

Neka je  $I$  linearni operator

$$I = \sum_i |i\rangle\langle i|$$

, gde je  $|i\rangle$  neki bazis. "I" je linearni operator zato što ako se primeni na neki ket  $|\psi\rangle$  dobije se linearna kombinaciju ketova što ke po definiciji keta još jedan ket.

$$I = \sum_i |i\rangle\langle i|\psi\rangle$$

Faktor  $\langle i|\psi\rangle$  može slobodno pomerati jer je to običan kompleksni broj. Da bi se utvrdilo šta je ket  $I|\psi\rangle$ , može se razviti  $|\psi\rangle$  po definiciji,

$$|\psi\rangle = \sum_i a_i |i\rangle$$

, a na osnovu odnosa ortogonalnosti, gde je  $\langle i|\psi\rangle = \delta_{ij}$ , a  $\delta_{ij} = 1$  ako je  $i = j$ , odnosno  $\delta_{ij} = 0$  ako je  $i \neq j$ , važi sledeće

$$I|\psi\rangle = \sum_i |i\rangle\langle i| \left( \sum_j a_j |j\rangle \right) = \sum_i a_i |i\rangle = |\psi\rangle$$

Ovo dokazuje da operator  $I$  primenjen na slučajni ket  $|\psi\rangle$  daje taj isti ket  $|\psi\rangle$ . Ovaj operator naziva se operator identiteta (engl. identity operator) i to je najtrivijalniji operator.

Neka je  $H$  neki linearni operator definisan na sledeći način.

$$H = \sum_i E_i |E_i\rangle\langle E_i|$$

Ovo je najvažniji operator u kvantnoj mehanici, takozvani Hamiltonian operator, nazvan u čast W.R. Hamiltona, koji je predložio analogni operator u klasičnoj fizici. Zbog korišćenja  $H$  operatora u definisanju evolucije kvantnih sistema u vremenu, ovaj operator je od fundamentalne važnosti za većinu formulacija u kvantno mehaničkoj teoriji.

Operator  $H$  može da se primeni na neki proizvoljni ket  $|\psi\rangle$  kako bi se dobio ket  $H|\psi\rangle$ , a zatim se dalje može primeniti bra  $\langle\psi|$  od  $|\psi\rangle$  na ket  $H|\psi\rangle$ , tako da je

$$\langle\psi|H|\psi\rangle = \sum_i E_i \langle\psi|E_i\rangle\langle E_i|\psi\rangle$$

Neka je kvantno stanje sistema  $|k\rangle$  takvo da možemo da budemo sigurni da će izmerena vrednost energije (stanje sistema) biti jednako  $E_k$ , koje zovemo stanje dobro definisane energije. Pošto znamo da je  $\langle E_i|\psi\rangle = a_i$ , dok je  $\langle\psi|E_i\rangle = a_i^*$ , sledi da je:

$$\langle\psi|H|\psi\rangle = \sum_i E_i |a_i|^2 = \sum_i p_i E_i = \langle E \rangle$$

Ovo je rezultat od velikog značaja – ako se Hamiltonian primeni između stanja  $|\psi\rangle$  i njegovog bra, dobije se očekivana vrednost energije sistema (engl. expectation value) za konkretno stanje  $E_i$ .

Ovaj rezultat za očekivanu vrednost energije sistema se može opravdano generalizovati i na druge merene vrednosti. Ako je  $Q$  neka merena promenljiva (engl. observable), i njen spektar mogućih vrednosti  $\{q_i\}$ , moguće je razviti bilo koji ket  $|\psi\rangle$  u linearnu kombinaciju stanja  $|q_i\rangle$  u kojima je vrednost  $Q$  dobro definisana

$$Q = \sum_i a_i |q_i\rangle$$

,a sa  $Q$  se vezuje istoimeni operator

$$Q = \sum_i q_i |q_i\rangle\langle q_i|$$

Tada je po analogiji  $\langle\psi|Q|\psi\rangle$  očekivana vrednost merene promenljive  $Q$  kada je kvantni sistem u nekom stanju  $|\psi\rangle$ .

Za svaki linearni operator  $R$  koji se javlja u opštim matematičkim problemima, korisno je ispitati njegove karakteristične vrednosti (engl. eigenvalues) i karakteristične vektore (engl. eigenvectors). Karakteristični vektor je vektor koga linearni operator  $R$  skalira (množi), a karakteristična vrednost je jednostavno faktor skaliranja. Ako je  $|r\rangle$  karakteristični vektor operatora  $R$ , a  $r$  karakteristična vrednost, sledi da je:

$$R|r\rangle = r|r\rangle$$

Vraćajući se na Hamiltonian operator  $H$ , pitanje je šta su njegove karakteristične vrednosti i karakteristični vektor? Ako se primeni  $H$  na  $|E_k\rangle$ , dobija se

$$H|E_k\rangle = \sum_i E_i |E_i\rangle\langle E_i|E_k\rangle = E_k |E_k\rangle$$

Dakle karakteristični vektori Hamiltoniana  $H$  su dobro definisana energetska stanja, a odgovarajuće karakteristične vrednosti predstavljaju moguće rezultate merenja energije sistema.

Nadalje, ova zapažanja takođe mogu direktno da se primene na opšti linearni operator  $Q$ , koji odgovara nekoj izabranoj merljivoj vrednosti kvantnog sistema. Ovim je data matematička osnova za merenje rezultata neke osobine kvantnog sistema, i odgovarajuće karakteristične (dozvoljene) vrednosti koje je moguće dobiti operacijom merenja u opštem slučaju.

### 3.3. Unitarni operatori

Unitarni operator je ograničen (engl. bounded) linearni operator  $U: \mathcal{H} \rightarrow \mathcal{H}$  na Hilbertovom prostoru  $\mathcal{H}$  za koje važi sledeće:

$$UU^* = U^*U = I$$

, gde je  $U^*$  adžoint (engl. adjoint) od  $U$ , a  $I: \mathcal{H} \rightarrow \mathcal{H}$  operator identiteta (engl. identity operator). Navedene osobine su ekvivalentne sledećim:

- $U$  održava unutrašnji proizvod  $\langle, \rangle$  Hilbertovog prostora, odnosno, za sve vektore  $X$  i  $Y$  Hilbertovog prostora  $\mathcal{H}$  važi  $\langle Ux, Uy \rangle = \langle x, y \rangle$ .

- $U$  je surjekcija.

U prethodnim sekcijama već pomenuti operator identiteta  $I$  je trivijalni unitarni operator. Rotacija vektora na  $\mathbb{R}^2$  odnosno  $\mathbb{R}^3$  je jednostavan primer unitarne operacije, koja ne menja dužinu vektora (održava unutrašnji proizvod) odnosno ugao između komponentnih vektora. Ako posmatramo vektorski prostor  $\mathbb{C}$  kompleksnih brojeva, množenje kompleksnim brojem apsolutne vrednosti 1 tj. brojem u obliku  $e^{i\theta}$  za neko  $\theta \in \mathbb{R}$ , je takođe unitarna operacija koja isključivo menja fazu.

Unitarne matrice su unitarni operatori na Hilbertovim prostorima konačne dimenzije. Trivijalan primer je unitarna matrica koja definiše rotaciju vektora u  $\mathbb{R}^2$  za neki ugao  $\theta$

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

Unitarne operacije, koje su takođe po sebi reverzibilne, imaju ključnu ulogu u kvantnom računarstvu i u sledećim poglavljima će biti više reči o njima.

### 3.4. Nemogućnost kopiranja stanja i dekoherencija kvantnog sistema

Teorema o nemogućnosti kopiranja stanja kvantnog sistema (engl. no-cloning theorem) je princip kvantne mehanike koji ne dozvoljava pravljenje identičnih kopija nekog nepoznatog kvantnog stanja. Autori Wootters, Zurek, i Dieks su 1982. godine objavili ovu teoremu, koja ima velike implikacije u kvantnoj mehanici i srodnim oblastima. Striktno, teorema tvrdi da ne postoji uređaj koji može da pripremi tačnu kopiju kvantnog stanja. Jedna analogija u klasičnoj fizici koja može da objasni navedenu teoremu je sledeća – ne može se, na osnovu samo jednog rezultata bacanja novčića (koji može biti podešen da favorizuje jednu stranu), simulirati sledeće nezavisno bacanje istog novčića.

Ovaj teorem dodatno sprečava korišćenje "klasičnih" tehnika za korekciju greške (engl. error correction techniques) na kvantnim stanjima. Dakle ne mogu se napraviti kopije stanja kvantnog sistema u toku kvantne operacije na tom sistemu, i te kopije eventualno iskoristiti kako bi se ispravile naknadne greške. Tehnike korekcije greške su pak neophodne za praktično kvantno računarstvo, tako da je ovo dugo vremena smatrano za ključno ograničenje. 1995. godine autori Šor i Stin (Shor, Steane) su nezavisno razvili prve tehnike za kvantnu korekciju greške koja zaobilaze ova ograničenja.

### Dekoherencija kvantnog sistema

U kvantnoj mehanici, kvantna dekoherencija predstavlja fenomen gubitka povezanosti ili redosleda faznih uglova među komponentama (kvantnog) sistema koji se nalazi u kvantnoj

superpoziciji. Jedna posledica ovog gubitka faze je klasična odnosno stohastički aditivno ponašanje. Dekohherencija se manifestuje istovetno kao i kolaps talasne funkcije pri merenju stanja sistema, ali ona ne generiše kolaps talasne funkcije. Dekohherencija samo daje objašnjenje o uočavanju kolapsa talasne funkcije, kada kvantna priroda sistema "curi" u okolinu. U stvari komponente talasne funkcije se odvajaju od koherentnog sistema i uzimaju faze njihove neposredne okoline.

Dekoherencija je suštinski mehanizam na osnovu koga se pojavljuju klasična ograničenja u odnosu na kvantno početno stanje, i ona povlači granice između klasičnog i kvantnog sveta. Dekohherencija nastaje povodom interakcije sistema sa okolinom na nepovratan način u termodinamičkom smislu. Može da se posmatra kao beg informacije iz sistema ka okolini, pošto je svaki sistem uvek slabo povezan sa energetske stanjem okruženja. Dekohherencija se takođe može modelirati kao neunitarni proces kojim se (kvantni) sistem spaja sa okolinom. Kako je u ovom slučaju dinamika sistema ireverzibilna, svaka informacija prisutna u kvantnom sistemu se gubi u okolini. Smatra se da je to proces kojim se informacija u kvantnom sistemu gubi u interakciji sa okolinom tako što nastaje kvantna korelacija (engl. entanglement) sistema i okoline na neki nepoznat način, tako da se sam sistem više ne može opisati bez reference na stanje njegove okoline. Dekohherencija predstavlja ogroman izazov za sve eksperimentalne realizacije kvantnih sistema pa i kvantni računara koji se oslanjaju na neometanu evoluciju kvantnih koherencija. Zbog toga gotovo svaka eksperimentalna implementacija kvantnog računara uključuje kriogene stepene i raznovrsne šeme izolacije sistema od okoline da bi se zadržala neophodna koherencija.

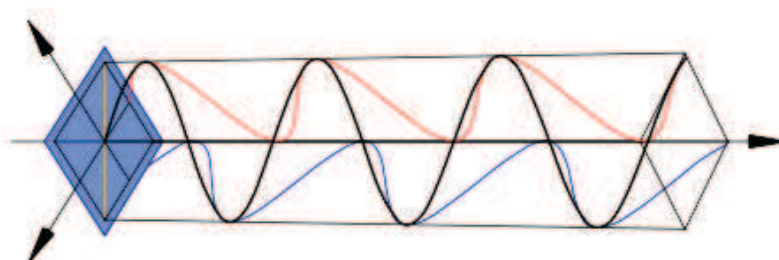
#### **4. Kvantno generisanje i distribucija ključeva (Quantum Key Distribution)**

Sigurno generisanje i razmena kriptografskih ključeva je cilj svakog šifarskog sistema. Postoje mnoge šeme koje omogućuju razmenu ključeva kao što su sistemi sa javnim ključem, ali se zna da RSA niti DH nisu bezuslovno sigurni. Jedan od pravaca razvoja su istraživanja u ovom pogledu je polje kvantne kriptografije (QC), preciznije, kvantne razmene ključeva (QKD). Istraživanja na ovom polju se odvijaju zadnjih 30 godina i danas već postoje komercijalni uređaji kao i implementacije državnih i korporativnih sigurnih komunikacionih mreža koje primenjuju QKD tehnologije.

##### **Linearna polarizacija i kvantna stanja fotona**

Sa stanovišta klasične fizike svetlosni talasi u vakumu su transferzalni elektromagnetski (EM) talasi sa vektorima električnog i magnetnog polja okomitim na pravac prostiranja i u odnosu na jedan drugog. Na osnovu konvencije polarizacija svetla se definiše orijentacijom električnog polja u tački u prostoru preko jednog perioda oscilacije. Svetlost propagira kao transferzalni talas te je polarizacija okomita u odnosu na pravac prostiranja talasa. Električno polje može biti orijentisano u jednom pravcu (linearna polarizacija), ali u generalnom slučaju može da rotira oko ose prostiranja talasa što odgovara kružnoj ili eliptičnoj polarizaciji svetlosti zavisno od faze između komponenti el. polja.

Na sledećoj slici prikazan je primer promene vektora električnog polja (crno) u vremenu (horizontalna osa), u određenoj tački u prostoru, uz odgovarajuće komponente vektora po X osi i po Y osi (crveno i plavo). Te dve komponente vektora po X i Y osi su u fazi i tako da je pravac vektora električnog polja (vektorska suma komponenti) je konstantan. Kako vrh vektora opisuje liniju u polju, ovaj poseban slučaj se naziva linearna polarizacija. Pravac po kome se proteže ova linija zavisi samo od međusobnog odnosa amplituda dve komponente. U tom smislu mogu se prepoznati dva zraka svetlosti koji imaju (relativnu) vertikalnu ili horizontalnu polarizaciju ako su vektori njihovih električnih polja ortogonalni.



Slika 6 - Linearna polarizacija svetlosti

Može da se govori i o vertikalno, horizontalno ili dijagonalno polarizovanim fotonima. U opštem slučaju ugao polarizacije fotona je relativna stvar i može biti arbitran.

Kvantni sistemi za generisanje i distribuciju ključeva (engl. Quantu Key Distribution – QKD) se oslanjaju na transmisiju pojedinačnih fotona kroz optička vlakna, od tačke do tačke, i koriste stanja polarizacije pojedinačnih fotona, u prostoru kvantnih stanja fotona, za enkodiranje binarnih vrednosti. Takve šeme kodiranja informacija nazivaju se kvantni alfabeti. Ukoliko su odgovarajuća stanja ortogonalna, poput vertikalne i horizontalne polarizacije, kvantni alfabet je ortogonalan, a kao primer mogu da se koriste sledeći alfabeti:

| polarizacija  | mapirana vrednost |
|---------------|-------------------|
| pravolinijska |                   |
| ↕             | 0                 |
| ↔             | 1                 |
| dijagonalna   |                   |
| ↗             | 0                 |
| ↘             | 1                 |

Tabela 1 - Primer kvantnog alfabeta

QKD tehnologije koristi neklasične, kvantno-mehaničke fenomene kako bi se omogućilo sigurno generisanje i razmena ključeva između dva čvora optičke mreže. Smatra se da će organizacije koje zahtevaju visok nivo sigurnosti u kritičnim aplikacijama u bliskoj budućnosti veoma brzo preći a korišćenje QKD tehnologije. Postoji više protokola QKD a najpoznatiji su BB84, SARG04, i EPR/E91,

koji već imaju komercijalne i/ili eksperimentalne implementacije. U sledećim poglavljima dati su njihovi principi rada, ograničenja i implementacije.

#### 4.1. BB84 protokol

BB84 je prvi QKD protokol, koji su 1984. godine kreirali Čarls Benet i Žil Brasar (engl. Charles H. Bennett i Gilles Brassard) sa Montrealskog Univerziteta. Protokol koristi 4 kvantna stanja koja grade dva bazisa, sa stanjima gore  $|\uparrow\rangle$ , dole  $|\downarrow\rangle$ , levo  $|\leftarrow\rangle$  i desno  $|\rightarrow\rangle$ . Navedeni bazisi su maksimalno konjugovani, što znači da su međusobne projekcije vektora iz dva bazisa jednake, tj.  $|\langle\uparrow|\leftarrow\rangle|^2 = \frac{1}{2}$ .

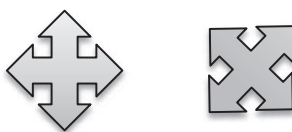
Vrednost "0" dodeljena je stanjima  $|\uparrow\rangle$  i  $|\rightarrow\rangle$ , a vrednost "1" stanjima  $|\downarrow\rangle$  and  $|\leftarrow\rangle$ . U fizičkom smislu moguće je pridružiti pojedine vrste polarizacije fotona navedenim kvantnim stanjima, konkretno, koristeći u prethodnoj sekciji pomenute pravolinijske i dijagonalne kvantne alfabete.

| kvantno stanje        | polarizacija fotona      | vrednost |
|-----------------------|--------------------------|----------|
| $ \uparrow\rangle$    | $\uparrow$ : (90°)       | 0        |
| $ \downarrow\rangle$  | $\leftrightarrow$ : (0°) | 1        |
| $ \rightarrow\rangle$ | $\nearrow$ : (45°)       | 0        |
| $ \leftarrow\rangle$  | $\nwarrow$ : (135°)      | 1        |

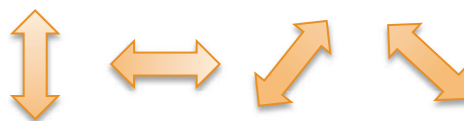
Tabela 2 - Mapiranje kvantnih stanja u polarizacije fotona i odgovarajuće binarne vrednosti

U prvom koraku Alisa šalje pojedinačne fotone sa određenom polarizacijom Bobu u stanjima koja su izabrana na potpuno slučajan način iz skupa 4 moguća stanja. Za svaki pojedinačni foton i Alisa i Bob vode evidenciju u vezi poslate/primljene polarizacije. Alisa i Bob moraju da imaju nezavisne generatore potpuno slučajnih brojeva (kvantne generatore) kako se ne bi stvarala bilo kakva dodatna korelacija između njihovih trenutno izabranih bazisa.

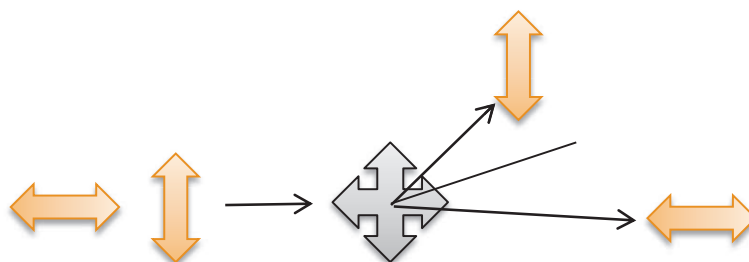
Bob zatim meri polarizaciju dolaznog fotona u jednom od dva bazisa (dve pozicije detektora fotona) koji je slučajno izabran. Bobov prijemni bazis odgovara u fizičkom smislu detektoru na koji pada foton koji je poslala Alisa. Kao primer uzmimo jednu komercijalnu implementaciju uređaja kompanije IDQuantique koji podržava ovaj protokol. Kad emitovani vertikalno polarizovan foton padne na vertikalni detektor, on će proći ali će biti deflektovan na predvidiv način, uvek u jednom, npr. levom smeru, dok će horizontalno polarizovani foton isto tako proći ali će da bude deflektovan uvek u drugom smeru, npr. desno od pravca kretanja. Ako foton sa dijagonalnom linearnom polarizacijom padne na vertikalni detektor on će proći kroz njega izmenjen na slučajan način, sa jednakim šansama da postane vertikalno ili horizontalno polarizovan, odnosno on gubi svoju prvobitnu linearnu polarizaciju i biva deflektovan u levo ili desno sa 50% šansi za oba ishoda.



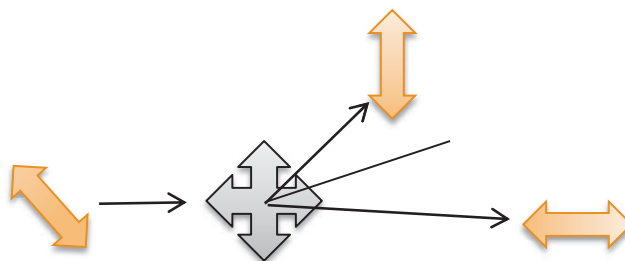
Slika 7- Moguće pozicije Bobovog polarizacionog detektora: vertikalna i dijagonalna orijentacija



Slika 8 - Moguće polarizacije Alisinih emitovanih fotona



Slika 9 - Defleksija fotona na "vertikalnom" detektoru, "vertikalni" foton levo, "horizontalni" desno



Slika 10 - Fotoni sa dijagonalnom polarizacijom, 50:50 verovatnoća za promenu polarizacije u v. ili h

Sledeća tabela prikazuje primer razmene bitova između Boba i Alise sa odgovarajućim kodiranjima:

| Alisa:<br>poslata<br>sekvenca | Alisa:<br>polarizacija<br>emitovanog<br>fotona | Bob:<br>orijentacija<br>filtera | Bob:<br>polarizacija<br>fotona na<br>izlazu | Bob:<br>primljena<br>sekvenca | Prosejani ključ:<br>prihvaćeni i<br>odbaćeni<br>bitovi |
|-------------------------------|------------------------------------------------|---------------------------------|---------------------------------------------|-------------------------------|--------------------------------------------------------|
| 0                             | ↑↓                                             | ⊗                               | ↖↗                                          | 1                             | odbaćen                                                |
| 1                             | ↔                                              | ⊕                               | ↔                                           | 1                             | 1                                                      |
| 1                             | ↖↗                                             | ⊕                               | ↑↓                                          | 0                             | odbaćen                                                |
| 0                             | ↗↘                                             | ⊗                               | ↗↘                                          | 0                             | 0                                                      |
| 1                             | ↖↗                                             | ⊗                               | ↖↗                                          | 1                             | 1                                                      |
| 0                             | ↗↘                                             | ⊕                               | ↑↓                                          | 0                             | odbaćen                                                |
| 0                             | ↑↓                                             | ⊕                               | ↑↓                                          | 0                             | 0                                                      |
| 1                             | ↔                                              | ⊗                               | ↖↗                                          | 1                             | odbaćen                                                |
| 1                             | ↔                                              | ⊗                               | ↗↘                                          | 0                             | odbaćen                                                |
| 1                             | ↖↗                                             | ⊗                               | ↖↗                                          | 1                             | 1                                                      |
| 0                             | ↑↓                                             | ⊗                               | ↗↘                                          | 0                             | odbaćen                                                |
| 1                             | ↔                                              | ⊕                               | ↔                                           | 1                             | 1                                                      |

Tabela 3 - Slanje informacije kroz kvantni kanal uz odbacivanje nekorelisanih bitova

Kad Alisa i Bob koriste isti bazis oni uvek dobiju perfektno korelisan rezultat. Ukoliko koriste različit bazis dobijaju potpuno nekorelisan rezultat. Za svaki bit Bob objavljuje putem javnog kanala koji bazis je koristio za određeni kubit, ali Bob ne objavljuje rezultat koji je dobio. Alisa zatim javlja putem javnog kanala da li stanje u kojem je ona kodirala taj bit kompatibilno sa bazisom koji je objavio Bob ili ne. Ako je stanje kompatibilno bit se sačuva, a ako nije bit se napušta. Na ovaj način se odbaci oko 50% bitova a dobijeni niz bitova se zove "prosejani ključ".

Korišćenje javnog komunikacionog kanala je veoma često u ovakvim protokolima. Takav javni kanal ne mora da bude poverljiv ali mora da bude autentičan. U tom pogledu bilo koji protivnik "Eva" može da prisluškuje komunikaciju na javnom kanalu ali ne može da ga modifikuje. U praksi Alisa i Bob mogu da koriste isti transmisioni kanal kao kvantni i javni kanal, kao na primer optičko vlakno. Ni Alisa ni Bob ne mogu da se opredele koji ključ će biti prozveden protokolom – ključ je u stvari proizvod njihovih slučajnih odluka.

### **Prisluškivanje QKD sistema**

Sledeće pitanje je ponašanje ovog protokola u neidealnim uslovima u pristustvu šuma na kvantnom kanalu i prisluškivanja. Pretpostavimo da Eva, protivnik koji prisluškuje kanal, preuzme kubit koji je Alisa poslala ka Bobu. To je veoma jednostavno, ali ako Bob ne primi očekivani bit on će jednostavno putem javnog kanala javiti Alisi da je taj bit ispušten. U tom smislu Eva može samo da smanji stopu proizvodnje bitova ali Eva u tom slučaju ne dobija ništa od korisnih informacija. Da bi Eva zaista prisluškivala komunikaciju tokom razmene ključa ona mora da pošalje bit Bobu. U idealnom slučaju ona mora da pošalje Bobu bit u izvornom obliku i da sačuva kopiju za sebe.

Tu dolazimo do fundamentalne osobine kvantnih sistema koja je ključna za QKD, gde je kopiranje kvantnog stanja sistema nemoguće, kao što se tvrdi prethodno pomenutom "no-cloning" teoremom. Čitanje stanja kvantnog sistema uništava prvobitno stanje sistema. Ova nemogućnost preciznog kopiranja kvantnog stanja sistema na fundamentalnom nivou sprečava Evu da na idealan način prisluškuje komunikaciju, što omogućuje da kvantna kriptografija bude potencijalno sigurna.

### **Strategija "presretni i pošalji"**

Jedna jednostavna strategija napada koju Eva može da primeni naziva se "presretni i pošalji". Ova strategija podrazumeva da Eva meri svaki bit u jednom od bazisa, kao što to radi i Bob. Ona zatim šalje Bobu drugi bit u stanju koje odgovara rezultatu njenog merenja. U 50% slučajeva Eva će biti u stanju da pogodi bazis koji je kompatibilan sa stanjem bita koje je pripremila i poslala Alisa. Kod navedenih slučajeva Eva mora ponovo da pošalje bit koji je u odgovarajućem stanju ka Bobu, a Alisa i Bob neće biti u stanju da primete da je ona intervenisala.

U ostalih 50% slučajeva Eva koristi bazis koji nije kompatibilan sa stanjem bita koji je poslala Alisa. Naravno ovo se dešava usled toga što je Eva ne zna stanja bita koje je Alisa pripremila, koristeći generator potpuno slučajnih brojeva. U tim slučajevima biti koje je poslala Eva su u novim stanjima uz preklapanje od  $\frac{1}{2}$  sa prvobitnim korektnim stanjima. Alisa i Bob time mogu da otkriju Evinu

intervenciju u blizu pola slučajeva jer su dobili nekorelisane rezultate. Iako Eva koristi opisanu strategiju radi prisluškivanja, ona dobija 50% informacije, dok Alisa i Bob istovremeno dobiju 25% stopu greške u svom prosejanom ključu – dakle nakon što eliminišu slučajeve nekompatibilnih stanja postoji još 25% greške u njihovoj komunikaciji na osnovu čega oni lako detektuju Evinu intervenciju na kanalu. Ako Eva primeni opisanu strategiju na samo 10% saobraćaja, greška će biti samo 2.5% dok će Eva zadržati 5% informacije.

### **Korekcija greške, povećanje privatnosti i porast kvantne tajne**

Nakon razmene bitova putem BB84 Alisa i Bob dele takozvani prosejani ključ. Ovaj ključ sadrži i greške nastale usled tehničkih nepravilnosti kanala ali i potencijalne Evine intervencije. Realna stopa greške u prosejanom ključu nastala usled primenjene tehnologije je reda veličine nekoliko procenata dužine ključa. Tih nekoliko procenata može se svesti korišćenjem klasičnih algoritama za korekciju greške, u odgovarajućem delu protokola, na stopu manju od  $10^{-9}$  koja odgovara redu veličine greške kod svih komunikacija kroz optička vlakna. U tom smislu se definišu dve vrste greške: QBER (quantum bit error rate) za grešku na kvantnom kanalu, i BER (bit error rate) koja odgovara grešci nastaloj u standardnoj komunikaciji. Situacija u kojoj legitimni učesnici u komunikaciji dele klasičnu informaciju sa visokom ali ne i 100-procentnom korelacijom, uz moguću korelaciju sa trećom stranom (Eva), je česta u svim kvantnim šifarskim sistemima.

Kao poslednji korak, protokol BB84 koristi klasične algoritme za korekciju greške, a zatim i da smanji procenat informacije o ključu do koje je došla Eva - ovaj proces se naziva povećanje privatnosti. U tom smislu pretpostavimo da Alisi, Bobu, i Evi pripadaju respektivno slučajne promenljive  $\alpha$ ,  $\beta$ ,  $\epsilon$ , sa zajedničkom raspodelom verovatnoće  $P(\alpha, \beta, \epsilon)$ . Alisi i Bobu je naravno dostupna samo marginalna raspodela verovatnoće  $P(\alpha, \beta)$ . Na osnovu toga oni moraju da izvedu zaključak o teorijskoj maksimalnoj količini informacija koje su dostupne Evi, Uz poznatu  $P(\alpha, \beta, \epsilon)$ ; potrebni i dovoljni uslov za pozitivnu stopu tajnog ključa,  $S(\alpha, \beta || \epsilon)$ , nisu poznati. Korisna donja granica je data razlikom između Alisine i Bobove zajedničke Šenonove informacije (mutual Shannon information)  $I(\alpha, \beta)$ . i Evine zajedničke informacije.

$$S(\alpha, \beta || \epsilon) \geq \max \{ I(\alpha, \beta) - I(\alpha, \epsilon), I(\alpha, \beta) - I(\beta, \epsilon) \}$$

Intuitivno ovaj rezultat tvrdi da je odvajanje sigurnog ključa moguće ako Bob poseduje veću količinu informacija od Eve. Gornja nejednakost je sigurna ako Alisa i Bob koriste jednostranu komunikaciju ali ako je komunikacija obostrana onda se odvajanje sigurnog ključa može izvršiti i pod uslovima gde gornja nejednakost nije ispunjena.

U trenutku kad je dobijen prosejani ključ Alisa i Bob javno upoređuju nasumično izabrani podskup dobijenog ključa. Na ovaj način oni procenjuju stopu greške, odnosno u opštem slučaju marginalnu raspodelu verovatnoće  $P(\alpha, \beta)$ . Ovi javno dostupni bitovi se nakon procene odbacuju. Kao sledeći korak je, ukoliko gornja nejednakost nije ispunjena, protokol se zaustavlja. Ukoliko je nejednakost pak zadovoljena na ključ može da se primeni neki od standardnih algoritama za korekciju greške kako bi se dobio kraći ključ bez grešaka. Kod najjednostavnijeg algoritma za

korekciju greške Alisa nasumice bira par bitova, primenjuje XOR operaciju i objavljuje tu vrednost. Bob odgovara sa "prihvatam" ako i on dobije istu vrednost kod tih bitova, odnosno "odbijam" u suprotnom slučaju. U prvom slučaju Alisa i Bob čuvaju prvi bit iz para bitova a u drugom slučaju odbacuju oba bita. U praksi se koriste mnogo komplikovaniji i efikasniji algoritmi. Ovaj postupak se ponavlja sve dok se greške ne smanje toliko da se Alisin i Bobov ostatak prosejanog ključa mogu smatrati identičnim. Nakon prikazane korekcije greške Alisa i Bob imaju identične ključeve ali Eva još uvek može da poseduje određenu količinu informacija o ključu. Alisa i Bob i dalje moraju da umanje Evinu informaciju do određenog izabranog nivoa koristeći neki od protokola za povećanje privatnosti.

Jedan od algoritama za povećanje privatnosti radi na sledećem principu – Alisa nasumično bira par bitova i izračunava njihovu XOR vrednost, ali za razliku od prethodnog koraka ne objavljuje tu vrednost već objavljuje koje je bitove u nizu prosejanog ključa je izabrala. (npr. bit 150 i bit 678) Alisa i Bob zatim zamenjuju ta dva bita sa njihovim XOR rezultatom. Eva ima samo delimičnu informaciju o dva bita ali informacija koju ona poseduje nakon primene operacije XOR na njih i zamene postaje još manja. Postoje i efikasniji algoritmi za povećanje privatnosti, a svi su "klasične" prirode.

QKD ne obezbeđuje kompletno rešenje za sve svrhe u koje se koristi kriptografija, ali ona može da se koristi kao dopuna za standardne simetrične šifarske sisteme. Tajni ključ generisan i distribuiran pomoću kvantnog protokola može dalje da se koristi kao jednokratni ključ za šifrovanje poruke u šifarskom sistemu sa tablicom za jednokratnu upotrebu (engl. one-time pad).

#### **4.2. EPR/E91 (Einstein- Podolsky-Rosen) protokol**

EPR protocol poznat još i pod nazivom E91 je varijacija BB84 protokola i on ima poseban konceptualni istorijski značaj. EPR protokol je 1991 osmislio Artur Ekert sa Univerziteta u Oksfordu, i osnovna ideja je da kvantnim kanalom prenose parovi fotona iz jedinstvenog izvora - foton za Alisu i foton za Boba. Prva opcija je da izvor emituje dva fotona uvek u istom kvantnom stanju izabranom nasumično iz skupa od četiri kvantna stanja koja se koriste u BB84 protokolu. Alisa i Bob bi, zatim, oboje merili svoje fotone pomoću jednog od dva bazisa, izabrana nasumično i nezavisno jedan od drugog. Izvor zatim objavljuje bazise i Alisa i Bob u tom slučaju zadržavaju informaciju samo ako su merenje izvršena pomoću istog bazisa. Ako je izvor pouzdan, protokol je ekvivalentan prethodno opisanom protokolu BB84. Ukoliko Eva kontroliše izvor nastaje dodatni izazov, zbog čega je Ekert svoj protokol bazirao na principu kvantne korelacije (engl. quantum entanglement), što je jedan od fundamentalnih pojava u kvantnoj mehanici i nema analogije u makro svetu.

##### **Kvantno korelisani fotoni**

Dva kvantna sistema kao što su par fotona (pa i elektroni i molekule), mogu da postanu kvantno korelisani i time se omogućuju određene interakcije između dva fotona čak i na udaljenosti

koje daleko premašuju skalu veličine čestica. Eksperimentalno je dokazano da one ostaju povezane i da merenje stanje jedne čestice, može da nedvosmisleno odredi i stanje druge upletene čestice, iako su čestice razdvojene stotinama kilometara. Kao jedan od primera možem uzeti merenje polarizacije para korelisanih fotona u pravolinijskom basisu. Ako je polarizacija prvog fotona horizontalna, za drugi foton iz para možemo sigurno da tvrdimo da je vertikalne polarizacije.

Praktično korelisanje para fotona nije lak zadatak. Poznat je metod "spontane parametričke konverzije na dole" (engl. spontaneous parametric down-conversion – SPDC), kod kog se prolaskom kroz određeni materijal nelinearan incidentni foton razdvaja na par fotona koji, na osnovu zakona o održanju energije, imaju kombinovane energije i momente jednake energiji i momentu prvobitnog fotona, i uz to imaju korelisane polarizacije. Ako fotoni imaju jednake polarizacije spadaju u tip I. Kao rezultat ovog procesa nastaje i kategorija fotona nazvana tip 2, koji imaju okomite polarizacije i koji su korelisani. Razlog navedenog razbijanja fotona na par korelisanih fotona, fenomen koji se dešava samo za mali broj incidentnih fotona, nije potpuno jasan.

Suštinski postoji veza između rezultata merenja jednog od para korelisanih fotona (merenje rezultira kolapsom talasne funkcije koja opisuje prvi foton), i što je veoma važan eksperimentalno dokazan rezultat, ovo merenje će se odraziti istovremeno i na drugi korelisani foton iz para u istom trenutku bez obzira na međusobnu udaljenost fotona. Očigledno je da se informacija prenela brzinom većom od brzine svetlosti, tzv. "dejstvo na daljinu" što se kosi sa klasičnom teorijom relativita.

Ajnštajn, Podolski i Rouzen (EPR) su u svom poznatom radu iz 1935. godine ukazali na ovaj paradoks "sablasnog dejstva na daljinu" što je po njima ukazalo na nekompletnost teorije kvantne fizike. EPR su tvrdili da je da postoje skrivene varijable koje nisu zapažene u eksperimentima i pomoću kojih može da se objasni navedeno paradoksalno „sablasno dejstvo na daljinu“. Džon Bel (John S. Bell) je 1964. godine dokazao da sve teorije skrivenih varijabli (lokalnost i realnost) moraju da zadovolje matematički model tzv. Belovu nejednakost. Pokazalo se da kvantna fizika narušava tu nejednakost, čime je matematički dokazano da u kvantnoj fizici ne postoje skrivene varijable. Teorema je eksperimentalno dokazana i važi za svaki kvantni sistem sa dva korelisana kvantna bita. Ovim teoremom se ne dokazuje kompletnost kvantne mehanike ali se odbacuju tvrdnje o lokalnosti i/ili realnosti. Još uvek postoje rezerve u odnosu na interpretaciju ovog fenomena.

### Osnovni principi protokola EPR/E91

EPR protokol je protokol sa tri stanja koji koristi Belovu nejednakost za detekciju Evinog prisustva kao skrivene varijable. Ovaj protokol se može opisati pomoću polarizacionih stanja kvantno korelisanog para fotona. Kao tri moguća polarizaciona stanja kvantno korelisanog para fotona izabraćemo:

$$|S_0\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle_1 \left| \frac{3\pi}{6} \right\rangle_2 - \left| \frac{3\pi}{6} \right\rangle_1 |0\rangle_2 \right),$$

$$|S_1\rangle = \frac{1}{\sqrt{2}} \left( \left| \frac{\pi}{6} \right\rangle_1 \left| \frac{4\pi}{6} \right\rangle_2 - \left| \frac{4\pi}{6} \right\rangle_1 \left| \frac{\pi}{6} \right\rangle_2 \right),$$

$$|S_2\rangle = \frac{1}{\sqrt{2}} \left( \left| \frac{2\pi}{6} \right\rangle_1 \left| \frac{5\pi}{6} \right\rangle_2 - \left| \frac{5\pi}{6} \right\rangle_1 \left| \frac{2\pi}{6} \right\rangle_2 \right)$$

Za svako od ovih stanja mogu se izabrati odgovarajući međusobno neortogonalni kvantni alfabeti  $A_0$ ,  $A_1$  i  $A_2$ , koji su dati u sledećim tabelama:

| kvantni alfabet | polarizacija (radijana) | vrednost |
|-----------------|-------------------------|----------|
| $A_0$           | 0                       | 0        |
|                 | $3\pi/6$                | 1        |
| $A_1$           | $\pi/6$                 | 0        |
|                 | $4\pi/6$                | 1        |
| $A_2$           | $2\pi/6$                | 0        |
|                 | $5\pi/6$                | 1        |

**Tabela 4 - Međusobno neortogonalni kvantni alfabeti**

Kao i kod BB84 protokola, postoje dve faze EPR protokola: komunikacija preko kvantnog i komunikacija preko javnog kanala. U prvoj fazi EPR protokola, najpre se iz skupa stanja  $\{|S_0\rangle, |S_1\rangle, |S_2\rangle\}$  nasumično i sa podjednakom verovatnoćom bira stanje  $|S_j\rangle$ . Zatim se kreira kvantno koorelisani par u izabranom stanju  $|S_j\rangle$ . Jedan foton kreiranog para šalje se Alisi, a drugi Bobu. Alisa i Bob nasumično sa podjednakom verovatnoćom, odvojeno i nezavisno jedan od drugog, biraju jedan od tri operatora merenja  $O_0, O_1$  i  $O_2$ , i vrše merenje svog fotona. Koristeći odgovarajući kvantni alfabet Alisa beleži izmereni bit. Sa druge strane, Bob beleži komplement svog izmerenog bita. Ova procedura se ponavlja više puta. U prvom koraku druge faze, Alisa i Bob obavljaju komunikaciju preko javnog kanala kako bi odredili one bitove za koje su koristili iste operatore merenja. Oni zatim dele svoje nizove bitova na dva podniza. Jedan podniz, koji se naziva prosejani ključ, sastoji se od onih bitova za koje su koristili iste operatore merenja, pošto su u tom slučaju rezultati njihovih merenja identični. Drugi podniz, koji se naziva odbaćeni ključ, sastoji se od svih ostalih bitova.

Za razliku od BB84 protokola, EPR protokol, umesto da odbaci bitove kod kojih se Alisin i Bobov izbor operatora merenja ne slažu i koji sačinjavaju odbaćeni ključ, koristi ih za detekciju Evinog prisustva. Upoređuju zatim odbaćeni ključ kako bi se odredilo da li je Belova nejednakost zadovoljena. Ako je Belova nejednakost zadovoljena dokazano je da je Eva prisluškivala komunikaciju između Alise i Boba. Za EPR protokol, Belova nejednakost može da se formuliše u sledećem obliku. Ako je  $P(\neq | i, j)$  verovatnoću da se dva odgovarajuća bita Alisinog i Bobovog odbaćenog ključa ne poklapaju, uz uslov da su operatori merenja koje su izabrali Alisa i Bob, respektivno ili  $O_i$  i  $O_j$ , ili  $O_j$  i  $O_i$ . Iz verovatnoće  $P(= | i, j) = 1 - P(\neq | i, j)$ . Uzmimo da je  $\Delta(i, j) = P(\neq | i, j) - P(= | i, j)$ . Konačno, neka je:  $\beta = 1 + \Delta(1,2) - |\Delta(0,1) - \Delta(0,2)|$ . Belova nejednakost u ovom slučaju se svodi na  $\beta \geq 0$ . Kako je u

kvantnoj mehanici  $\beta = -1/2$ , ovo narušava Belovu nejednakosti. Sledeći korak u realnim uslovim podrazumeva procese korekcije greške i povećanje privatnosti, na isti način koji je opisan u BB84 protokolu.

### 4.3. SARG04 protokol

SARG04 protokol je verovatno najznačajniji protokol za kvantnu distribuciju ključa koji se pojavio u poslednje vreme. Nastao je 2004. godine kao plod rada naučnika Scarani, Acín, Ribordy i Gisin, po čemu je dobio naziv, na osnovu saznanja da se korišćenjem 4 kvantna stanja kao kod BB84 uz primenu različitog sistema kodiranja može razviti novi protokol koji će biti otporniji u slučaju korišćenja slabih laserskih pulseva umesto izvora pojedinačnih fotona. Osnovni način rada zahteva da protokol koristi isti hardver kao kod sistema sa BB84 uz izmenjeno kodiranje. SARG04 protokol je dakle modifikacija BB84 protokola i koristi ista četiri ortogonalna kvantna stanja kao i BB84, uz izmenjenu proceduru za izdvajanje prosejanog ključa. Bob ne objavljuje svoje bazise koje je koristio za merenje kvantnih stanja Alisinih fotona, kao u BB84. Umesto ovog već poznatog načina rada Alisa objavljuje preko javnog kanala jedan od četiri skupa stanja,  $\{|\rightarrow\rangle, |\nearrow\rangle\}$ ;  $\{|\uparrow\rangle, |\nearrow\rangle\}$ ;  $\{|\rightarrow\rangle, |\nwarrow\rangle\}$ ;  $\{|\uparrow\rangle, |\nwarrow\rangle\}$ , koji sadrži stanje fotona koji je poslala.

Ako je foton u stanju  $|\uparrow\rangle$ , Alisa preko javnog kanala objavljuje da stanje pripada skup  $\{|\uparrow\rangle, |\nearrow\rangle\}$  ili skup  $\{|\uparrow\rangle, |\nwarrow\rangle\}$ . Pretpostavimo da je Bob koristio pravougaoni bazis za merenje stanja  $|\uparrow\rangle$ . U tom slučaju je rezultat merenja dobio vrednost '1'. Na osnovu poznatih činjenica o BB84 postoji mogućnost da Bob dobije vrednost '1' i u slučaju kad je stanje fotona koji meri  $|\nearrow\rangle$  ili  $|\nwarrow\rangle$ . Samim tim Bob ne može da odredi pomoću tog jednog merenja kvantno stanje Alisinog fotona rukovodeći se isključivo skupom stanja koji je Alisa objavila putem javnog kanala. Na osnovu toga on javlja Alisi da se bit koji odgovara ovom merenju odbacuje. Nadalje ako Bob meri stanje  $|\uparrow\rangle$  pomoću u tom trenutku odabranog dijagonalnog bazisa, on kao rezultat merenja može da dobije vrednost bita '1' ili '0' sa verovatnoćom jednakom 50% za svaki ishod. Pod pretpostavkom da je rezultat Bobovog merenja '0', ako Alisa objavi da je tekući skup stanja  $\{|\uparrow\rangle, |\nearrow\rangle\}$  onda Bobovo merenje nije jednoznačno zato što stanje  $|\nearrow\rangle$  izmereno pomoću dijagonalnog bazisa uvek daje rezultat '0'. Stoga Alisa i Bob moraju da odbace bit koji odgovara tom merenju.

S druge strane ako Alisa objavi skup stanja  $\{|\uparrow\rangle, |\nwarrow\rangle\}$ , tada Bob sigurno zna da stanje Alisinog fotona ne može da bude  $|\nwarrow\rangle$ , zato što stanje  $|\nwarrow\rangle$  izmereno pomoću dijagonalnog bazisa uvek daje kao rezultat merenja '0'. Alisa i Bob će stoga zadržati bit koji odgovara ovom merenju. Sledeća tabela prikazuje sve moguće slučajeve u kojima će Alisa i Bob zadržati bit iz binarne sekvence.

| Alisina polarizacija | Alisin objavljeni skup stanja | Bobov bazis | Bobov primljeni bit |
|----------------------|-------------------------------|-------------|---------------------|
|----------------------|-------------------------------|-------------|---------------------|

|                              |                                             |           |   |
|------------------------------|---------------------------------------------|-----------|---|
| $\uparrow: (90^\circ)$       | $\{ \uparrow\rangle,  \nearrow\rangle\}$    | $\otimes$ | 1 |
| $\uparrow: (90^\circ)$       | $\{ \uparrow\rangle,  \nwarrow\rangle\}$    | $\otimes$ | 0 |
| $\leftrightarrow: (0^\circ)$ | $\{ \rightarrow\rangle,  \nearrow\rangle\}$ | $\otimes$ | 1 |
| $\leftrightarrow: (0^\circ)$ | $\{ \rightarrow\rangle,  \nwarrow\rangle\}$ | $\otimes$ | 0 |
| $\nearrow: (45^\circ)$       | $\{ \rightarrow\rangle,  \nearrow\rangle\}$ | $\oplus$  | 1 |
| $\nearrow: (45^\circ)$       | $\{ \uparrow\rangle,  \nearrow\rangle\}$    | $\oplus$  | 0 |
| $\nwarrow: (135^\circ)$      | $\{ \rightarrow\rangle,  \nwarrow\rangle\}$ | $\oplus$  | 1 |
| $\nwarrow: (135^\circ)$      | $\{ \uparrow\rangle,  \nwarrow\rangle\}$    | $\oplus$  | 0 |

Tabela 5 - Primer sekvence bitova sa objavljenim stanjima – SARG04

Interesantno je napomenuti da je SARG04 protokol otporan na napade polovljenjem broja fotona (engl. photon-number-splitting attack). Pretpostavimo da Alisa u jednom vremenskom intervalu šalje Bobu dva ili više fotona istog kvantnog stanja usled nesavršenosti izvora fotona koji može da emituje isključivo jedan foton u zadatom vremenskom intervalu.

Neka Eva presretne i sačuva jedan od dva identična fotona dok Alisa i Bob odluče da zadrže bit koji odgovara tom fotonu. Kod BB84 Bob javlja Alisi putem javnog kanala koji bazis je korišten za merenje fotona. Javni kanal je dostupan Evi i ona jednostavno meri sačuvani foton istim bazisom i dobije vrednost koju imaju Bob i Alisa, što predstavlja očiglednu slabost BB84 protokola u navedenom napadu. Kod SARG04 protokola Eva bi znala samo, iz Alisine i Bobove javne komunikacije, da se foton nalazi u jednom od dva neortogonalna stanja iz skupa stanja koji je objavila Alisa. Eva, u ovom slučaju, ne može da odredi stanje fotona koji je uskladištila, zbog toga što ne zna koji bazis da upotrebi prilikom merenja. SARG04 protokol stoga uspešno umanjuje Evinu mogućnost da sazna tačno stanje fotona koji je uskladištila.

Istraživači Branciard i Gisin su 2005. godine pokazali su da u praktičnim eksperimentalnim uslovima SARG04 protokol funkcioniše bolje nego BB84 protokol kad je u pitanju stvarna efikasnost distribucije tajnog ključa, unatoč prikazanoj manjoj efikasnosti ovog protokola usled odbacivanja 75% bitova u nizu sirovog ključa, dok BB84 odbacuje pola bitova.

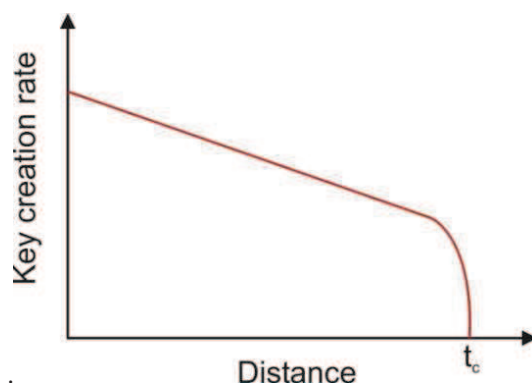
## Ostali kvantni protokoli

BB84 protokol koristi 4 kvantna stanja (dva puta dva ortogonalna stanja). Dokazano je da su dva neortogonalna kvantna stanja (protokol B92) dovoljna za sigurnu distribuciju ključa. Četiri kvantna stanja su standard, dok protokol sa šest kvantnih stanja sa tri bazisa pruža teoretski verovatnoću da Alisa prilikom slanja i Bob prilikom prijema fotona izaberu isti bazis u samo jednom od tri slučaja ( $P=0.333333$ ). Istovremeno to važi i za Evu jer strategija presretanja svih Alisinih fotona i merenja svakog od njih pomoću nasumično izabranog bazisa, i slanja fotona u izmerenom stanju ka Bobu, ona će teoretski pogoditi ispravni bazisa u samo jednoj trećini slučajeva, sa verovatnoćom  $P=0.333333$ . ovo je bitna razlika u odnosu na BB84 protokol gde je verovatnoća da će Eva prilikom merenja odabrati ispravan bazis je jednaka  $P=0.5$ . Na osnovu toga u sistemu sa 6 kvantnih stanja maksimalna teorijska količina informacije do koje Eva može da dođe prisluškivanjem je manja, a time je povećana otpornost protokola na prisluškivanje.

Čarls Benet je 1992. godine otkrio da za kvantnu distribuciju ključa dovoljna samo dva neortogonalna kvantna stanja, protokol poznat pod imenom B92. Sigurnost sistema proizilazi iz toga da Eva ne može nedvosmisleno i bez narušavanja stanja da razlikuje dva kvantna stanja koja Alisa koristi za predstavljanje bitova i koja zatim šalje Bobu, zato što su ta kvantna stanja neortogonalna. Kao i u BB84 protokolu, Alisa i Bob komuniciraju u dve faze, u prvoj preko jednosmernog kvantnog komunikacionog kanala, a u drugoj preko dvosmernog javnog komunikacionog kanala.

### 4.4. Praktična ograničenja QKD tehnologije

Prvu eksperimentalnu demonstraciju kvantne kriptografije su 1989 godine prikazali Benet i Brassard. Ključ je razmenjen kroz vazduh na udaljenosti od 30 cm, dok je prva demonstracija QKD kroz optički kabl je izvedena 1993. godine na Univerzitetu Ženeve. Praktični izvori fotona se danas oslanjaju na slabe laserske impulse ili kvantno korelisane parove fotona. Praktično svi moderni QKD sistemi koriste mono-modalna optička vlakna kao medijum za kvantni kanal, sa prečnikom jezgra od  $8\mu\text{m}$ , za telekomunikacione talasne dužine od 1300 nm i 1500 nm. Performanse QKD sistema mogu se opisati brzinom kojom je ključ generisan između uređaja na određenoj daljini. Neidealni izvori pojedinačnih fotona i detektori doprinose smanjenju broja fotona koji će se detektovati na prijemniku, odnosno smanjenju efektivne stope generisanja ključeva. Kako se povećava razdaljina između dva QKD uređaja, postoje dva glavna efekta koji dopunjavaju jedan drugog i smanjuju efektivnu stopu generisanja ključa - mogućnost da pojedinačni foton dostigne prijemnik se smanjuje, kao i odnos signala i šuma se smanjuje, što znači da se stopa greške povećava i na taj način se smanjuje efektivna stopa generisanja ključeva.



Slika 11 - Odnos razdaljine između Alise i Boba i realne stope generisanja ključeva (bps)

Tipične brzine generisanja ključeva kod postojećih QKD sistema se kreću od nekoliko stotina kilobita u sekundi za kraće razdaljine do nekoliko stotina bitova u sekundi za veće razdaljine. Na slici. je data kritična udaljenost  $t_c$  nakon koje propusna moć tipičnog QKD sistema naglo pada. Pošto se nizovi bitova koji bivaju razmenjeni između QKD uređaja koriste za kreiranje relativno kratkih ključeva za šifriranje (128 odnosno 256 bita), brzina razmene bitova je dovoljna da se održi stalna stopa osvežavanja bezuslovno sigurnih i potpuno slučajnih ključeva. Poruke se nadalje šifruje dobijenim ključevima i šalju u realnom vremenu do opsega od 10Gbps.

Raspon današnjih QKD sistema je ograničen providnošću optičkih veza i u principu dostiže oko 150 kilometara. U klasičnoj telekomunikaciji putem magistralnih optičkih linija umanjeње signala se rešava optičkim repetitorima na svakih 80 kilometara. Kod QKD protokla nije moguće ubaciti repetitor je bi takav uređaj praktično imao ulogu Eve i izazvao korupciju ključa. S druge strane moguće je napraviti mrežu poznatih QKD uređaja koji se mogu koristiti da se poveća razdaljina između čvorova koji zahtevaju zaštićenu komunikaciju.

#### 4.5. Implementacije QKD tehnologije

##### Eksperimentalne implementacije

Najbrži eksperimentalni QKD sistem na bazi BB84 protokola do sada ostvario je brzinu razmene ključeva od 1Mbps preko 20 kilometara optičke linije, kao rezultat saradnje između Univerziteta u Kembridžu i Tošibe. Od marta 2007. godine najveća razdaljina između čvorova među kojima je demonstrirana QKD tehnologija iznosi 148.7 kilometara optičkog vlakna, u okviru eksperimenta tima iz Los Alamos National Laboratory/NIST, uz korišćenje BB84 protokola. Značaj ovog eksperimenta je da je ova razdaljina uporediva sa većinom razdaljina između čvorova glavnih optičkih linija koje su danas u upotrebi, što implicira mogućnosti stvaranja mreže QKD čvorova.

Najveća razdaljina kod primene QKD u praznom prostoru iznosi 144 kilometra, između dva Kanarska ostrva, korišćenjem EPR protokola 2006, a BB84 protokola sa lažnim (engl. decoy) stanjima 2007. godine. Ovaj eksperiment je ukazao na mogućnost QKD komunikacije sa satelitima ako se

zemaljske stanice nalaze na većoj nadmorskoj visini usled razređenog vazduha koji smanjuje atenuaciju signala koja je ubedljivo dominantna u prvih par kilometara iznad zemljine površine

### **Komercijalne implementacije**

Trenutno u svetu postoje tri kompanije koje nude komercijalne QKD sisteme: ID Quantique, Švajcarska; MagiQ Technologies, SAD i Quintessence Labs, Australija. Velike korporacije kao što su Toshiba, HP, IBM, Mitsubishi, NEC, i NTT, aktivno ulažu u razvoju QKD tehnologija. Prva bankarska transakcija u svetu korišćenjem QKD je izvršena u Beču 2004. godine, a tehnologija kompanije ID Quantique je već korišćena tokom izbora u Ženevskom kantonu za siguran prenos glasova do centralne glasačke komisije.

### **QKD mreže**

DARPA kvantna mreža koja predstavlja QKD sistem od 10 čvorova je u funkciji od 2004. godine u saveznoj državi Masačusets, SAD. Na razvoju ove mreže rade kompanije BN Technologies i QinetiQ, kao i Harvardski i Bostonski univerziteti. Prva računarska mreža u svetu koja je zaštićena QKD tehnologijom implementirana je u oktobru 2008. godine na naučnoj konferenciji u Beču. Mreža pod nazivom SECOQC (Secure Communication Based on QC) napravljena je sredstvima EU. SECOQC koristi 200 km standardnog optičkog kabla da bi se povezalo 6 lokacija u Beču sa gradom St.Poelten, koji se nalazi 69 kilometara zapadno od Beča.

Kompanija ID Quantique je objavila završetak najdužeg eksperimenta za testiranje QKD tehnologije. Glavni cilj SwissQuantum mreže instalirane u Ženevi u martu 2009. godine bio je da se verifikuje pouzdanost i otpornost QKD sistema u neprekidnom radu pod realnim uslovima. Kvantni sloj je radio stabilno gotovo 2 godine, do januara 2011. godine, kada je projekat završen.

Tokio QKD mreža je započela rad prvog dana UQCC2010 konferencije. Ova mreža uključuje međunarodnu saradnju između 7 partnera: EC, Mitsubishi Electric, NTT, NICT, Toshiba Research Europ, Id Quantique, All Vienna.

## **5. Osnove kvantnog računarstva**

Počeci razmišljanja vezani za ideje kvantnog računarstva vezane su za problem simulacija određenih klasa fizičkih sistema koje su zahtevale ogromne računarske resurse za relativno jednostavne probleme. Primer takvih fizičkih sistema su turbulencija u fluidima i određeni kvantno-mehanički sistemi. Fizičar Ričard Fejnman (Richard Feynman) je 1982. godine u svom radu izneo argument da bi simulacije fenomena kvantne mehanike zahtevale ogromne količine računarskih resursa koje bi rasle eksponencijalno sa težinom problema, bez obzira na moguće efikasne algoritme koji mogu da ubrzaju takvu vrstu izazova, kao i da je, uprkos pozitivnim rezultatima kod određenih kvantno-mehaničkih sistema, simulacija generičkog kvantnog sistema veoma težak problem. Juri Manin (Yuri Manin) je nezavisno došao do slične ideje 1980. godine u Sovjetskom savezu. Fejnman je

takođe predložio u svom radu iz 1982. godine da bi se izazov simulacije kvanto-mehaničkih sistema mogao rešiti primenom kvantnog računara - hipotetičkog uređaja koji bi radio na principima fundamentalnih kvatno-mehaničkih fenomena.

### **Apstraktni model kvantnog računara**

1985. godine autor Dejvid Dojč (David Deutch) je u svom radu izneo apstraktni model kvantnog računarstva, postavio teoriju kvantnih logičkih kola, i postavio pitanje da li bi univerzalni kvantni računar mogao da se koristi u rešavanju određenih klasa teških klasičnih problema. Kasnijim istraživanjem došlo se do skupa problema koje bi kvantni računari teoretski mnogo bolje rešavali u odnosu na klasične računare. Jedan primer je faktorizacija prirodnih brojeva korišćenjem Šorovog (Peter W. Shor) algoritma, i simulacija kvantnih sistema sa više tela (engl. quantum many-body systems). Po definiciji kvantni računar je hipotetički uređaj koji neposredno koristi kvantno-mehaničke fenomene kao što su superpozicija i kvantno korelisanje (engl. entanglement) kako bi izvršio određene (unitarne) operacije na podacima. Teoretski model kvantnog računara je takozvana kvantna Turingova mašina, poznata još i kao univerzalni kvantni računar. Kvantni računari dele određene teoretske sličnosti sa nedeterminističkim i stohastičkim računarskim sistemima - jedan primer je mogućnost kvantnog računara da zauzme više dozvoljenih stanja istovremeno.

Piteru Šor (Peter W. Shor) je u svom radu o faktorizaciji prirodnih brojeva na kvantnom računaru istakao prvi put glavnu prednost kvantnog računarstva u odnosu na klasično: "...kvantno računarstvo dobija dodatnu računarsku snagu na osnovu eksponencijalne dimenzionalnosti pošto za sistem od  $n$  kubita dimenzionalnost prostora kvantnih stanja postaje  $\mathbb{C}^{2^n}$  ..."

### **Izazovi klasične simulacije**

Dokazano je da bi svaki današnji konvencionalni digitalni računar mogao izvršavati bilo koji današnji kvantni algoritam s obzirom da kvantni računari ne dovode u pitanje Čurč-Turingovu (Church-Turing) hipotezu koja tvrdi da se svaka funkcija algoritamski može izračunati ako i samo ako se može izračunati na Turingovoj mašini. Ključno ograničenje kod izvršavanja kvantnih algoritama (odnosno simulacije rada kvantnih računara) na klasičnom računaru je činjenica da se klasični računarski resursi potrebni za takvu simulaciju povećavaju eksponencijalno sa količinom informacija koja se obrađuje. Ako neki kvantni računar izvršava operacije na registru od 200 kvantnih bita, što je neophodan red veličine za rešavanje mnogih realnih problema, odgovarajuća simulacija bi zahtevala klasičnu memoriju koja mora da sadrži  $2^{200}$  kompleksnih vrednosti. Radi poređenja terabajt (TB) digitalnih podataka jednak je  $2^{43}$  bita. Na osnovu postojećih teorija, budući kvantni računari koji će raditi nad značajno većim skupom podataka (većim brojem kvantnih bita - kubita) od onoga koji podržavaju današnji eksperimentalni sistemi, moći će da rešavaju složene probleme iz raznih kritičnih oblasti za redove veličina brže nego što to mogu današnji konvencionalni računarski sistemi, koristeći najefikasnije postojeće algoritme.

## Osnovne komponente kvantnog računarstva

Sledeće komponente su neophodne da bi se izvršila računaska operacija na kvantnom računararu:

- Kvantni tip podataka. Kubit (engl. qubit) odnosno kvantni bit, i kvantni registri koji predstavljaju kolekcije kubita.
- Kvantne operacije. Sve kvantne operacije koje su isključivo unitarne pa samim tim i reverzibilne, što znači da je moguće je reverzibilno dobiti ulazne podatke na osnovu rezultata te operacije. Primer unitarne operacije je rotacija vektora u Euklidskom prostoru  $\mathbb{R}^2$ .
- Konverzija u klasične tipove podataka. Pre izvršenja jedne ili više kvantnih operacija neophodno je inicijalizacija kubita, odnosno registra kubita, na bazi nekog klasičnog tipa podataka kao što je npr. UINT32. Rezultat čitanje stanja registra je niz klasičnih bita koje je zatim neophodno prebaciti u tip koji je kompatibilan sa višim programskim jezicima.

### 5.1. Kvantni bit – Kubit (Qubit)

Američki naučnik Klod Šenon za koga se vezuje nastanak teorije informacija (Claude E. Shannon) prvi put je koristio reč "bit" u svom radu o Matematičkoj teoriji komunikacija iz 1948, kao akronim za binarni broj (engl. binary digit). Šenon je u svojoj master tezi na MIT iz 1937 pokazao da korišćenje električnih uređaja za implementiranje Bulove algebra bi omogućilo rešavanje bilo kojeg logičkog odnosno numeričkog problema, a time je postavljena osnova digitalnih kola i računara.

Podatak u formi bita kao najmanje količina informacije, se može predstaviti bilo kojim sistemom koji ima dva stabilna stanja – dva nivoa napona, dva nivoa intenziteta svetlosti, polarizacija svetlosti, smer magnetnog polja, i slično, i takav čuvati u memoriji, kopirati, ili razmenjivati putem nekog komunikacionog kanala. Svaki bit uvek uzima vrednost "0" ili "1" ali nikad istovremeno. Kao što je navedeno ranije, matrična reprezentacija nekog kvantnog sistema prikazuje verovatnoće da će sistem biti u nekom od datih stanja kad se izvrši merenje. Po analogiji vrednost klasičnog bita se može predstaviti, po Dirakovoj odnosno matričnoj notaciji, na sledeći način:

$$0 = |0\rangle = \begin{bmatrix} 1 + i0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad , \quad 1 = |1\rangle = \begin{bmatrix} 0 \\ 1 + i0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Ako uzmemo da su vrednosti u gornjim matricama, amplitude verovatnoća, mora biti da je zbir verovatnoća da je klasični bit u stanju  $|0\rangle$  ili  $|1\rangle$  jedinična, a klasični bit uzima vrednosti "0" i "1", ali nikad u isto vreme.

Kubit je kvantno-mehanički (kvantni) sistem koji je analogan bitu u klasičnom računarstvu. Naziv je nastao skraćivanjem fraze "kvantni bit". (engl. qubit – quantum bit). Striktno, kubit je po definiciji kvantni sistem  $\mathcal{Q}$  čije stanje (vektor) leži u nekom dvodimenzionalnom Hilbertovom prostoru  $\mathcal{H}$ . Čisto stanje kubita je linearna kombinacija bazisa stanja. Kao što je ranije rečeno, kubit može biti predstavljen kao linearna kombinacija bazisa stanja  $|0\rangle$  i  $|1\rangle$  sa amplitudama verovatnoće  $\alpha$  i  $\beta$ .

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ ili u matričnoj notaciji, } |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Bitno je napomenuti da su amplitude verovatnoće  $\alpha$  i  $\beta$  su kompleksni brojevi koji naravno mogu biti pozitivni i negativni, što omogućuje da se verovatnoće poništavaju/sabiraju tokom operacija.

Ako kažemo da je kubit u superpoziciji dva stanja, "0" =  $|0\rangle$ , i "1" =  $|1\rangle$ , i da je verovatnoća da je kubit u svakom od stanja jednaka odnosno 50% za oba slučaja, stanje kubita se tada može opisati sledećom matricom:

$$|\psi\rangle = \begin{bmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{bmatrix},$$

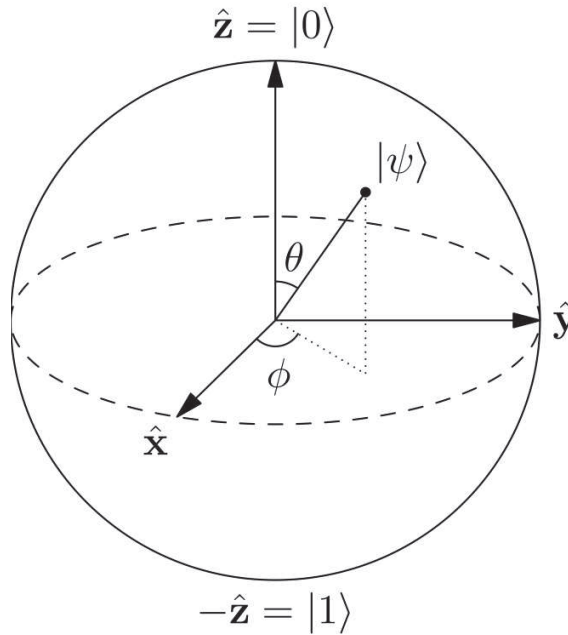
, ili u Dirakovoj notaciji

$$|\psi\rangle = \frac{\sqrt{2}}{2}|0\rangle \pm \frac{\sqrt{2}}{2}|1\rangle$$

Kažemo da se kubit istovremeno nalazi u 50% - 50% superpoziciji stanja  $|0\rangle$  i  $|1\rangle$ , odnosno da je mogućnost dobijanja vrednosti "0" i "1" kao rezultata merenja kubita podjednako verovatna. Kubit se može postaviti u stanje superpozicije primenom tzv. Hadamardove operacije, što će u kasnijim poglavljima biti detaljno objašnjeno.

### Reprezentacija kubita - Blohova sfera

Blohova sfera (engl. Felix Bloch) je geometrijska reprezentacija tzv. "čistih" stanja kubita. Sfera je jedinična sa parom naspramnih tačaka koji predstavljaju uzajamno ortogonalne vektore stanja. Severni i južni pol Blohove sfere su po konvenciji izabrani da predstavljau respektivno bazis vektore  $|0\rangle$  i  $|1\rangle$ , što u fizičkom smislu može biti spin-up i spin-down stanje elektrona, ili horizontalna i vertikalna polarizacija fotona. Tačke na površini sfere odgovaraju tzv. "čistim" stanjima, dok tačke unutar sfere odgovaraju tzv. "mešanim" kvantnim stanjima. Blohova sfera može predstavljati svaki kvantni sistem od n-nivoa ali je vizualizacija takvog sistema nepraktična.



Slika 12 - Blohova sfera – model qubita

Važi da se svako čisto stanje  $|\psi\rangle$  kvantnog sistema sa dva nivoa može se predstaviti superpozicijom bazis vektora  $|0\rangle$  i  $|1\rangle$ , sa koeficijentima  $\alpha$  i  $\beta$  koji su kompleksni brojevi:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Kako u ovom slučaju samo relativne faze među koeficijentima dva bazis vektora imaju neko fizičko značenje, koeficijent  $\alpha$  može se smatrati realnim i nenegativnim. Po definiciji, ukupna verovatnoća svih ishoda mora da bude jedinična, pa važi da je  $\langle\psi^*|\psi\rangle = 1$ , odnosno  $\alpha^2 + \beta^2 = 1$ . Na osnovu datih ograničenja  $|\psi\rangle$  se može izraziti kao:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + (\cos\phi + i\sin\phi)\sin\left(\frac{\theta}{2}\right)|1\rangle$$

, za neko  $0 \leq \theta \leq \pi$  i  $0 \leq \phi \leq 2\pi$ .

Parametri  $\theta$  i  $\phi$  određuju tačku na jediničnoj sferi u  $\mathbb{R}^3$ , kao sferne koordinate jediničnog vektora. Kao primer, jedno čisto stanje kubita,  $1/\sqrt{2}(|0\rangle + i|1\rangle)$ , odgovara tački koja leži na secištu ekvatora sfere i pozitivnog dela y-ose.

### Tenzorski proizvod Hilbertovih prostora

Tenzorski proizvod se primenjuje u različitim kontekstima u matematici, uključujući i Hilbertove prostore. U određenim kontekstima tenzorski proizvod, koji se označava simbolom " $\otimes$ ",

naziva se i vanjskim proizvodom. (engl. "outer product). Tenzorski proizvod  $\mathcal{H} \otimes \mathcal{K}$  dva Hilbertova prostora  $\mathcal{H}$  i  $\mathcal{K}$  je jednostavno najprostiji Hilbertovo prostor za koji važe sledeća pravila:

- $(h_1 + h_2) \otimes k = (h_1 \otimes k) + (h_2 \otimes k), \forall h_1, h_2 \in \mathcal{H}, \forall k \in \mathcal{K}$
- $h \otimes (k_1 + k_2) = (h \otimes k_1) + (h \otimes k_2), \forall h \in \mathcal{H}, \forall k_1, k_2 \in \mathcal{K}$
- $\lambda (h \otimes k) \equiv (\lambda h) \otimes k = h \otimes (\lambda k), \forall \lambda \in \mathbb{C}, \forall h \in \mathcal{H}, \forall k \in \mathcal{K}$

Na osnovu navedenog sledi, ako su  $\{e_1, e_2, e_3, \dots, e_m\}$  i  $\{f_1, f_2, f_3, \dots, f_n\}$  respektivno bazisi Hilbertovih prostora  $\mathcal{H}$  i  $\mathcal{K}$ , onda je  $\{e_i \otimes f_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$  basis tenzorskog proizvoda  $\mathcal{H} \otimes \mathcal{K}$ . Dimenzija tenzorskog proizvoda  $\mathcal{H} \otimes \mathcal{K}$  je proizvod dimenzija Hilbertovih prostora  $\mathcal{H}$  i  $\mathcal{K}$ :

$$\text{Dim}(\mathcal{H} \otimes \mathcal{K}) = \text{Dim}(\mathcal{H}) \cdot \text{Dim}(\mathcal{K})$$

Na kraju, ako su  $|u\rangle$  i  $|v\rangle$  ketovi na Hilbertovi prostorima  $\mathcal{H}_1$  i  $\mathcal{H}_2$ , njihov tenzorski proizvod se uobičajeno obeležava po nekoj od sledeće tri konvencije:

$$|u\rangle \otimes |v\rangle, \quad |u, v\rangle, \quad |u\rangle|v\rangle$$

Ako su ketovi  $u, v$  dati sa

$$u = (u_1, u_2, \dots, u_n), \quad v = (v_1, v_2, \dots, v_m)$$

, njihov tenzorski proizvod je

$$u \otimes v = \begin{bmatrix} u_1 v_1 & u_1 v_2 & \dots & u_1 v_n \\ u_2 v_1 & u_2 v_2 & \dots & u_2 v_n \\ \dots & \dots & \dots & \dots \\ u_m v_1 & u_m v_2 & \dots & u_m v_n \end{bmatrix}$$

## 5.2. Kvantni registri

Kvantni registar je skup logički grupisanih kubita. Analogija sa registrima digitalnih računara i logičkim operacijama nad podacima u njima ostaje u pogledu držanja ulaznih podataka u registrima, operacija nad podacima u registrima, i predstavljanju rezultata tih operacija. Kvantni registri mogu takođe da sadrže grupe dodatnih, kontrolnih kubita (engl. ancilla qubits), koji su neophodni za izvršavanje operacija. Važno je reći da inicijalne vrednosti registara pre primene kvantne operacije mogu da sadrže navedene dodatne kubite koji mogu biti pripremljeni u određenim stanjima. Slično tome, izlazne vrednosti nakon izvršene kvantne operacije mogu sadržati kubite koji nisu relevantni za rezultat operacije. Sledi formalna definicija registra kubita sa određenim osobinama i posledicama koje nisu prisutne u konvencionalnim registrima.

Neka  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$  su dva kvantna sistema koji su odvojeno pripremljeni i nalaze se u respektivnim stanjima  $|\psi_1\rangle$  i  $|\psi_2\rangle$  i koji su u jednom trenutku sjedinjeni, bez međusobnog uticaja. Pošto su  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$  pripremljeni nezavisno, bez međusobne interakcije, njihova stanja  $|\psi_1\rangle$  i  $|\psi_2\rangle$  leže u odvojenim Hilbertovim prostorima  $\mathcal{H}_1$  i  $\mathcal{H}_2$ . Pošto su ovi kvantni sistemi nezavisno pripremljeni ne postoji nikakva fizička pretpostavka da postoji zavisnost između stanja  $|\psi_1\rangle$  i  $|\psi_2\rangle$ .

Globalni kvantni sistem  $\mathcal{Q}$  koji se sastoji od ova dva kvantna sistema,  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$ , naziva se kombinacija (grupisanje) (engl. juxtaposition) kvantnih sistema  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$ . Stanje ovog globalnog kvantnog sistema  $\mathcal{Q}$  je po definiciji tenzorski (spoljni) proizvod stanja  $|\psi_1\rangle$  i  $|\psi_2\rangle$  kvantnih sistema  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$ . Drugim rečima stanje kvantnog sistema  $\mathcal{Q}$  je dato sledećim izrazom:

$$|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

Na osnovu date definicije, ako su kvantni sistemi  $\mathcal{Q}_1$  i  $\mathcal{Q}_2$  kubiti sa odgovarajućim zajedničkim bazisom, u tom slučaju kvantni sistem  $\mathcal{Q}$  odgovara kvantnom registru dva kubita. Ovo kombinovanje kvantnih sistema (kubita) u strukturu koja he praktično registar kubita ima važnu implikaciju na ključne osobine kvantnog računara.

Neka je  $\mathcal{H}$  dvodimenzionalni Hilbertov prostor i neka  $\{|0\rangle, |1\rangle\}$  predstavlja proizvoljno izabrani ortonormalni bazis. Neka su  $\mathcal{H}_{n-1}, \mathcal{H}_{n-2}, \dots, \mathcal{H}_0$  posebni Hilbertovi prostori, svaki izomorfan na  $\mathcal{H}$ , sa indukovanim ortonormalnim bazisima, respektivno:

$$\{|0_{n-1}\rangle, |1_{n-1}\rangle\}, \{|0_{n-2}\rangle, |1_{n-2}\rangle\}, \dots, \{|0_0\rangle, |1_0\rangle\}$$

Posmatrajmo  $n$  kubita  $\mathcal{Q}_{n-1}, \mathcal{Q}_{n-2}, \dots, \mathcal{Q}_0$  koji su odvojeno pripremljeni (bez međusobne interakcije), u sledećim stanjima, respektivno:

$$\frac{1}{\sqrt{2}}(|0_{n-1}\rangle + |1_{n-1}\rangle), \frac{1}{\sqrt{2}}(|0_{n-2}\rangle + |1_{n-2}\rangle), \dots, \frac{1}{\sqrt{2}}(|0_0\rangle + |1_0\rangle)$$

Neka  $\mathcal{Q}$  predstavlja globalni sistem odnosno registar koji se sastoji od grupe posebno pripremljenih  $n$  kubita  $\mathcal{Q}_{n-1}, \mathcal{Q}_{n-2}, \dots, \mathcal{Q}_0$ . U tom slučaju stanje  $|\psi\rangle$  registra  $\mathcal{Q}$  je tenzorski proizvod:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|0_{n-1}\rangle + |1_{n-1}\rangle) \otimes \frac{1}{\sqrt{2}}(|0_{n-2}\rangle + |1_{n-2}\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0_0\rangle + |1_0\rangle) = \\ &= \left(\frac{1}{\sqrt{2}}\right)^n (|0_{n-1}0_{n-2} \dots 0_1 0_0\rangle + |0_{n-1}0_{n-2} \dots 0_1 1_0\rangle + \dots + |1_{n-1}1_0 \dots 1_1 1_0\rangle) \end{aligned}$$

, koji leži u Hilbertovom prostoru  $\mathcal{H} = \mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \dots \otimes \mathcal{H}_0$ .

Dakle kubit registar  $\mathcal{Q}$ , koji se sastoji od  $n$  kubita  $\mathcal{Q}_{n-1}, \mathcal{Q}_{n-2}, \dots, \mathcal{Q}_0$ , je u stanju

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^n (|00 \dots 00\rangle + |00 \dots 01\rangle + \dots + |11 \dots 11\rangle)$$

Važno je primetiti da je  $n$ -kubit registar  $\mathcal{Q}$  u superpoziciji ketova sa labelama koje odgovaraju svim binarnim  $n$ -tuplovima. Ako posmatramo svaki binarni  $n$ -tuple kao binarni broj, stanje registra  $\mathcal{Q}$  može se predstaviti kao

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle + |2\rangle + |3\rangle + \dots + |2^n - 1\rangle)$$

Drugim rečima vidi se da ovaj  $n$ -kubitni registar sadrži sve prirodne brojeve od 0 do  $2^n - 1$  u superpoziciji, i što je još važnije sadrži sve navedene prirodne brojeve istovremeno. To je upravo primer masivnog paralelizma koji je svojstven kvantnom računaru.

Ako izvršimo očitavanje registra, što je ekvivalentno merenju stanja kvantnog sistema  $\mathcal{Q}$ , ova osobina masivnog paralelizma nestaje i registar kolabira u jedno od stanja koje odgovara nekom od  $2^n$  prirodnih brojeva sa verovatnoćom:

$$p = \left| \left(\frac{1}{\sqrt{2}}\right)^n \right|^2 = \left(\frac{1}{2}\right)^n$$

Kao što je ranije predstavljeno, merenje sistema izaziva kolaps kvantnog registra u neko od stanja sa verovatnoćom  $p$  na osnovu inherentne kvantne neizvesnosti, što nije preterano korisno te je neophodan nešto složeniji pristup, sa takozvanim kvantnim korelisanjem kubita u registru.

### 5.3. Kvantno korelisani sistemi (entanglement)

Kvantno korelisanje (engl. entanglement) dva kvantna sistema je kvantno-mehanički fenomen koji je potpuno specifičan, i nema nikakve analogije u klasičnom svetu. Sledi striktna matematička definicija.

Neka su  $\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_n$  kvantni sistemi sa svojim Hilbertovim prostorima  $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$  respektivno. Onda se za kvantni registar  $\mathcal{Q}$  koji se sastoji od kvantnih sistema  $\mathcal{Q}_1, \mathcal{Q}_2, \dots, \mathcal{Q}_n$  kaže da je kvantno korelisan, ako se njegovo stanje

$$|\psi\rangle \in \mathcal{H} = \bigotimes_{j=1}^n \mathcal{H}_j$$

ne može napisati u formi tenzorskog proizvoda ketova

$$|\psi\rangle = \bigotimes_{j=1}^n |\psi_j\rangle$$

, gde svaki ket  $|\psi_j\rangle$  leži u Hilbertovom prostoru za  $j = 1, 2, \dots, n$ . Možemo reći za takvo stanje  $|\psi\rangle$  da je kvantno korelisano.

Kao primer uzmimo registar koji se sastoji od 2 kubita. Sva stanja registra možemo izvesti na sledeći način, na osnovu teorije date u prethodnom poglavlju:

$$\left\{ \begin{array}{l} |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ |1\rangle = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\ |2\rangle = |10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\ |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{array} \right.$$

Pretpostavimo da je početno stanje  $|\psi\rangle_{t=0}$  ovog registra sledeće:

$$|\psi\rangle_{t=0} = \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \otimes |0\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |01\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |2\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

Pretpostavimo da je od trenutka  $t=0$  do  $t=1$  dinamičko ponašanje registra određeno Hamiltonianom  $H$ , koji se može opisati u smislu bazisa  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$  sledećom matricom, sa redovima i kolonama u datom poretku:

$$H = \frac{\pi\hbar}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 \end{pmatrix}$$

Kao posledica Šredingerove jednačine, Hamiltonian  $H$  određuje unitarnu transformaciju  $U_{cnot}$

$$U_{cnot} = e^{-\frac{i}{\hbar}H} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 3| + |3\rangle\langle 2|$$

Koja transformiše 2-kubitni registar iz početnog stanja  $|\psi\rangle_{t=0}$  u trenutku  $t=0$ , u stanje  $|\psi\rangle_{t=1}$  u trenutku  $t=1$ :

$$\begin{aligned}
|\psi\rangle_{t=1} &= U_{cnot}|\psi\rangle_{t=0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle)
\end{aligned}$$

Novo stanje se više ne može predstaviti tenzorskim produktom dva stanja i novo stanje ne odgovara stanju dva grupisana kubita. Kao što se tvrdi u gornjoj definiciji, govori se o paru kvantno korelisanih kubita primenom operacije  $U_{cnot}$  o kojoj će kasnije biti više reči.

Kvantnim korelisanjem dva kubita u registru su izgubila svoje odvojene identitete i ponašaju se spregnuto – merenje jednog kubita izazvaće kolaps oba kubita sa 50% verovatnoće da će par uzeti jednu od vrednosti  $|0\rangle$  ili  $|3\rangle$  ali istovremeno. Dakle promena stanja jednog kubita izaziva istovremenu promenu stanja u drugom kubitu ovog kvantno-korelisano para. Ovo stanje najjednostavnijeg sistema maksimalno korelisanih kubita se naziva i Belovo stanje (engl. Bell state).

#### 5.4. Kvantne operacije i logička kola

Kvantni računar može se modelirati unitarnom transformacijom  $U$  koja je sastavljena od sekvence konačno mnogo lokalnih unitarnih transformacija:

$$U = U_{n-1}U_{n-2} \dots U_1U_0$$

Svaka unitarna transformacija  $U_j$ , odnosno konkretnije kvantna operacija, predstavlja jedan korak u izračunavanju rezultata zadatog problema na hipotetičkom kvantnom računaru.

U svakom kvantnom računarstvu kvantno logičko kolo je osnovni uređaj koji operiše nad jednim ili više kubita, i svako takvo kolo implementira određenu unitarnu transformaciju  $U_j$ , tj. kvantnu operaciju. Kvantna logička kola su dakle osnovni gradivni elementi kvantnih računara, analogno konvencionalnim logičkim kolima u digitalnim računarima (AND, OR, NOT, NAND, NOR). Ključna razlika je da kvantna logička kola implementiraju takozvane reverzibilne logičke operacije.

Reverzibilna logička kola se proučavaju još od 1960-ih godina, a prvobitna motivacija za proučavanje je taj da reverzibilna kola gube manje, odnosno teoretski, nikako ne gube energiju u vidu toplote tokom izvršavanja operacija na njima. Konvencionalna logička kola gube ulazna stanja (informacija) pa je tako količina informacija na izlazu manja nego na ulazu. Takav gubitak informacije odaje energiju u okolinu u obliku toplote, usled termodinamičke entropije. Jedan način da se ovaj

proces shvati je da je električni naboj u konvencionalnim logičkim kolima uzemljen i da otiče u trenutku kad se menja stanje u kolu odnoseći određenu količinu energije sa sobom. Nasuprot tome svako reverzibilno kolo isključivo pomera stanje napred-nazad, tako da ne postoji gubitak informacije i zbog toga nema gubitka energije.

Kvantna logička kola su predstavljena odgovarajućim unitarnim matricama. Najčešće kvantna logička kola operišu nad jednim ili dva kubita, analogno konvencionalnim logičkim kolima. To znači da kvantna logička kola mogu biti opisana unitarnim matricama dimenzija  $2 \times 2$ , odnosno  $4 \times 4$ , za unarne, odnosno binarne kvantne operacije respektivno. Polazeći tom logikom uopšte kvantna logička kola nad  $n$  kubita mogu biti predstavljena odgovarajućim  $2^n \times 2^n$  matricama.

Operacija na kubit u predstavljena nekom  $2 \times 2$  matricom može biti bilo šta, sve dok je operacija (matrica) unitarna. Ako posmatramo operaciju na jednom kubit u na Blohovoj sferi, mnoge od ovih operacija su rotacije oko  $x, y, z$  osa. Ovi principi važe i kad se operacija primenjuje na više kubita.

Neka je početno stanje našeg kubita dato prvim izrazom, a zatim neka sledi operacija data odgovarajućom  $2 \times 2$  matricom:

$$|0\rangle \mapsto a|0\rangle + b|1\rangle, |1\rangle \mapsto c|0\rangle + d|1\rangle$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$$

$$(ax + by)|0\rangle + (cx + dy)|1\rangle.$$

Kao i kod konvencionalnih računara u kvantnom računarstvu postoji skup kvantnih univerzalnih kola kojima se sve ostale transformacije mogu izvesti. To su CNOT, Hadamard, i Phase-shift kola. Sledi definicija niza kvantnih logičkih kola.

### Hadamardovo kolo

Hadamardovo kolo deluje na jedan kubit, mapirajući basis stanja  $|0\rangle$  i  $|1\rangle$  u  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  i  $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ , respektivno. Operacija implementirana ovim kolom na Blohovoj sferi predstavlja rotaciju od  $\pi$  radiana oko ose  $\frac{\vec{x} + \vec{z}}{\sqrt{2}}$ , predstavljena je odgovarajućom matricom i simbolom.

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



Slika 13 - Hadamardovo kolo

### Paulijevo X kolo

Paulijevo X kolo deluje na jedan kubit, mapirajući  $|0\rangle$  u  $|1\rangle$  i  $|1\rangle$  u  $|0\rangle$ . Ova operacija predstavlja rotaciju od  $\pi$  radijana oko x ose na Blohovoj sferi, efektivno implementirajući kvantni ekvivalent NOT kola. Paulijevo X kolo predstavljeno je odgovarajućom matricom i simbolom.

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



Slika 14 - Paulijevo X kolo

### Paulijevo Y kolo

Paulijevo Y kolo deluje na jedan kubit, mapirajući  $|0\rangle$  u  $i|1\rangle$  i  $|1\rangle$  u  $-i|0\rangle$ . Ova operacija predstavlja rotaciju od  $\pi$  radijana oko y ose na Blohovoj sferi. Paulijevo Y kolo predstavljeno je odgovarajućom matricom i simbolom.

$$\begin{bmatrix} 1 & -i \\ i & 0 \end{bmatrix}$$



Slika 15- Paulijevo Y kolo

### Paulijevo Z kolo

Paulijevo Z kolo deluje na jedan kubit i nema uticaja na bazis stanje  $|0\rangle$  ali mapira  $|1\rangle$  u  $-|1\rangle$ . Ova operacija predstavlja rotaciju od  $\pi$  radijana oko z ose na Blohovoj sferi, pa predstavlja poseban slučaj kola za pomeranje faze (engl. phase shift). Kolo je predstavljeno odgovarajućom matricom i simbolom.

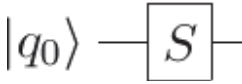
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Slika 16 - Paulijevo Z kolo

### S (fazno) kolo

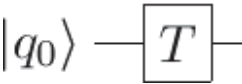
S (fazno ) kolo deluje na jedan kubit i predstavljeno je odgovarajućom matricom i simbolom.

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$


Slika 17 - S kolo

### T ( $\pi/8$ fazno) kolo

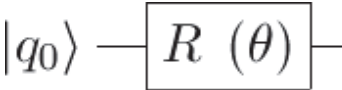
T kolo deluje na jedan kubit i predstavljeno je odgovarajućom matricom i simbolom.

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$


Slika 18 - T kolo

### R( $\theta$ ) rotacija

Ovo je porodica kola koji deluju na jedan kubit i ne utiču na basis stanje  $|0\rangle$ , ali mapiraju  $|1\rangle$  u  $e^{i\theta}|1\rangle$ . Verovatnoća merenja stanja  $|0\rangle$  i  $|1\rangle$  se ne menja nakon primene kola ali se menja faza kvantnog stanja. Ova operacija je ekvivalentna iscrtavanju horizontalnog kruga na Blohovoj sferi za  $\theta$  radijana. Kolo je predstavljeno odgovarajućom matricom i simbolom.

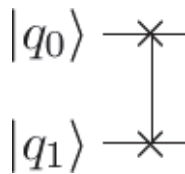
$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$


Slika 19 - R( $\theta$ ) kolo

### Swap kolo (swap gate)

Swap kolo izmenjuje redosled dva kubita. Predstavljeno je sledećom matricom i simbolom.

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

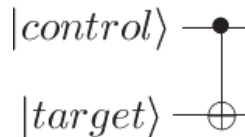


Slika 20 - Swap kolo

### CNOT kolo

Kontrolisano NOT kolo (CNOT) radi sa 2 kubita, tako što izvršava NOT operaciju na drugom kubit (target) samo ako je prvi kubit (control) u stanju  $|1\rangle$  – u suprotnom slučaju stanje drugog kubita ostaje nepromenjeno. CNOT pripada podskupu tzv. univerzalnih kvantnih logičkih kola.

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



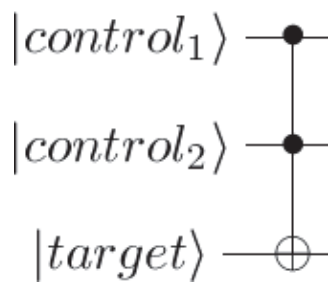
Slika 21 - CNOT kolo

### Tofolijevo kolo (Toffoli gate)

Tofolijevo kolo, takođe nazvano CCNOT kolo, radi sa 3 bita i to je univerzalno reverzibilno kolo u klasičnom računarstvu. Kvantno Tofolijevo kolo je ekvivalentno konvencionalnom, za 3 kubita. Ako su prva dva kubita (control1 i control2) u stanju  $|1\rangle$  primenjuje se Paulijeva X transformacija na trećem kubit (target) – u suprotnom nema promene.

| Input |   |   | output |   |   |
|-------|---|---|--------|---|---|
| 0     | 0 | 0 | 0      | 0 | 0 |
| 0     | 0 | 1 | 0      | 0 | 1 |
| 0     | 1 | 0 | 0      | 1 | 0 |
| 0     | 1 | 1 | 0      | 1 | 1 |
| 1     | 0 | 0 | 1      | 0 | 0 |
| 1     | 0 | 1 | 1      | 0 | 1 |
| 1     | 1 | 0 | 1      | 1 | 1 |
| 1     | 1 | 1 | 1      | 1 | 0 |

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



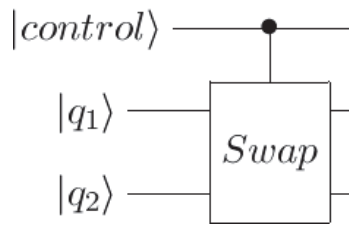
Slika 22 - Tofolijevo kolo

### Fredkinovo kolo (Fredkin gate)

Fredkinovo kolo, poznato još kao CSWAP kolo, je univerzalno klasično reverzibilno kolo koje radi sa 3 bita i izvodi kontrolisanu zamenu bita. Kvantni ekvivalent kola predstavljen je sledećom tabelom stanja, matricom, i odovarajućim simbolom svojstvenim Fredkinovom kolu.

| input    |                      |                      | output   |                      |                      |
|----------|----------------------|----------------------|----------|----------------------|----------------------|
| <b>C</b> | <b>I<sub>1</sub></b> | <b>I<sub>2</sub></b> | <b>C</b> | <b>O<sub>1</sub></b> | <b>O<sub>2</sub></b> |
| 0        | 0                    | 0                    | 0        | 0                    | 0                    |
| 0        | 0                    | 1                    | 0        | 0                    | 1                    |
| 0        | 1                    | 0                    | 0        | 1                    | 0                    |
| 0        | 1                    | 1                    | 0        | 1                    | 1                    |
| 1        | 0                    | 0                    | 1        | 0                    | 0                    |
| 1        | 0                    | 1                    | 1        | 1                    | 0                    |
| 1        | 1                    | 0                    | 1        | 0                    | 1                    |
| 1        | 1                    | 1                    | 1        | 1                    | 0                    |

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



Slika 23 - Fredkinovo kolo

### Rk kolo

$R_k$  kolo se koristi u kvantnim Furijeovim transformacijama što je i najbitniji deo Šorovog algoritma za faktORIZACIJU prirodnih brojeva. Ovoj operaciji odgovara sledeća matrica sa pripadajućim simbolom:

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2k} \end{bmatrix}$$

Slika 24 -  $R_k$  kolo

### $R_x(\theta)$ rotacija

Rotacija oko X ose Blohove sfere, može se opisati sledećom matricom, sa pripadajućim simbolom za  $R_x$  kolo:

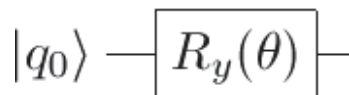
$$\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Slika 25 -  $R_x$  kolo

### Ry (θ) rotacija

Rotacija oko Y ose Blohove sfere može se opisati sledećom matricom, sa pripadajućim simbolom za Ry kolo:

$$\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

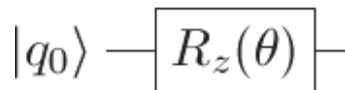


Slika 26 - Ry kolo

### Rz (θ) rotacija

Rotacija oko Z ose Blohove sfere može se opisati sledećom matricom, sa pripadajućim simbolom za Rz kolo:

$$\begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

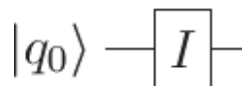


Slika 27 - Rz kolo

### Identitet (neutralna operacija)

Operacija na jednom kubit u koja je neutralna tj. identitet, ne utiče na kubit, sa odgovarajućom matricom i simbolom za kolo:

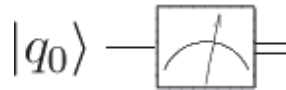
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



Slika 28 - Identitet

### Operacija merenja stanja kubita

Operacija merenja određuje stanje kubita na kraju sekvencijalne primene ostalih operacija, predstavljena je sledećim simbolom:



Slika 29 - Merenje stanja

### Volšova transformacija (Walsh Transformation)

Volšova transformacija primenjuje Hadamard operaciju nad  $n$  kubita. Opisana je tensorskim proizvodom  $n$  Hadamard matrica:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \dots \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

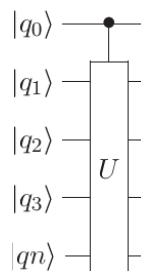


Slika 30 - Kolo za Volšovu transformaciju

### Kontrolisano U sa jednim kontrolnim i (n-1) ciljnih kubita

Operacija primenjuje operaciju  $U$  na  $n-1$  ciljnih kubita, sa jednim kontrolnim kubitom. Ako je jedinstveni kontrolni kubit u stanju  $|0\rangle$  nema promena. Ako je kontrolni kubit u stanju  $|1\rangle$ , kolo  $U$  se primenjeno istovremeno na  $n-1$  ciljnih kubita. Ovoj operaciji odgovara sledeća matrica i simbol:

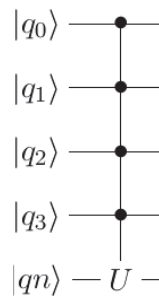
$$\begin{bmatrix} I_2 & 0 \\ 0 & U \end{bmatrix}$$



Slika 31 - Kolo za kontrolisano U sa jednim kontrolnim i (n-1) ciljnih kubita

### Kontrolisano U sa (n-1) kontrolnih i jednim ciljnim kubitom

Operacija primenjuje operaciju  $U$  na jedan ciljni kubit, uz  $n-1$  kontrolnih kubita. Ukoliko je svih  $n-1$  kontrolnih kubita u stanju  $|1\rangle$  kolo  $U$  je primenjeno na jedinstveni ciljni kubit. Ovoj operaciji odgovaraju različite matrice, zavisno od  $n$ , uz pripadajući simbol:

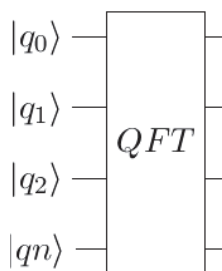


Slika 32 - Kolo za kontrolisano U sa (n-1) kontrolnih i jednim ciljnim kubitom

### Kvantna Furijeova transformacija (QFT)

Operacija se primenjuje u Šorovom algoritmu za faktorisanje prirodnih brojeva. Faktor  $\omega$  odgovara  $2^n$ -tom jediničnom korenu (engl. root of unity)  $e^{\frac{2\pi i}{2^n}}$ . QFT operaciji odgovara sledeća matrica i simbol.

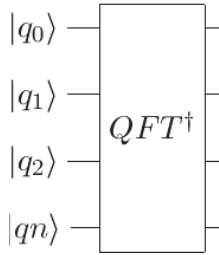
$$\frac{1}{\sqrt{2^n}} \begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 & \dots \\ \omega^0 & \omega^1 & \omega^2 & \omega^3 & \dots \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 & \dots \\ \omega^0 & \omega^3 & \omega^6 & \omega^9 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$



Slika 33 - QFT kolo

### Inverzna kvantna Furijeova transformacija (QFT\*)

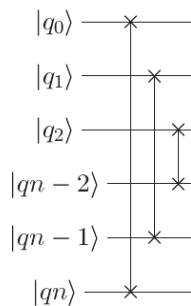
Operacija inverzna prethodnoj, kvantnoj Furijeovoj transformaciji, sa pripadajućim simbolom:



Slika 34 - Inveržno QFT kolo

### Promena redosleda kubita - n kubita (Reverse order of n qubits)

Operacija na n kubit koja menja redosled kubita u registru, sa odgovarajućim simbolom:

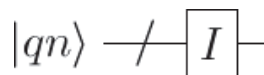


Slika 35 - Kolo za promenu redosleda kubita

### Identitet operacija na n kubita (Identity - n qubits)

Neutralna Identitet operacija na n kubita sa odgovarajućom matricom i simbolom.

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

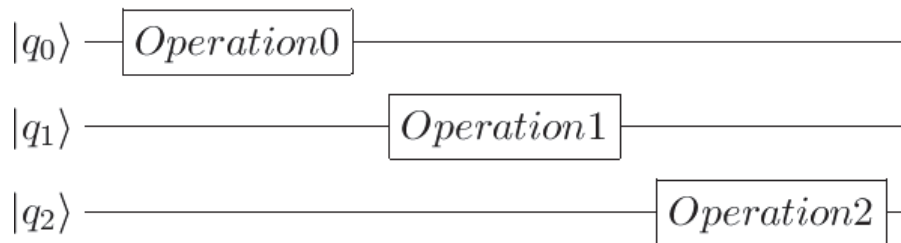


Slika 36 - Identitet na n kubita

## 5.5. Dijagrami kvantnih kola

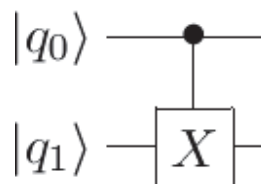
U literaturi se često koriste dijagrami kvantnih kola kako bi se ilustrovalo izvršavanje elementarnih operacije nad pojedinim kubitima u okviru različitih algoritama. Kod dijagrama kvantnih

kola kubit su predstavljeni horizontalnim linijama, operacije su predstavljene oznakama na pojedinim linijama, sa odgovarajućim simbolima kola, kao što je navedeno u poglavlju o kvantnim operacijama. Dijagram se čita sa leva na desno, kako i teče redosled operacija u vremenu.



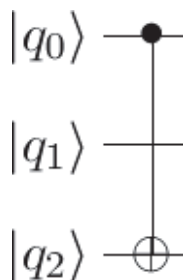
Slika 37 - Dijagram kvantnog kola sa 3 kubita i 3 proizvoljne kvantne operacije

Operacije koje se izvršavaju na više kubita su vezane na odgovarajuće kubite vertikalnim linijama na dijagramu. Puni krug na presecanju horizontalne i vertikalne linije predstavlja kontrolni kubit, dok se neka proizvoljna operacija X izvodi na ciljnom kubit, u zavisno od vrednosti kontrolnog kubita.



Slika 38 - Kontrolni kubit  $q_0$  kvalifikuje izvršavanje operacije X na ciljnom kubit  $q_1$

Operacije se često izvršavaju na podskupu kubita u registru. Ako se operacija ne izvršava na određenom kubit, vertikalna linija koja se na kraju završava na ciljnom kubit može da pređe preko ovog kubita tako da nema efekta na njega. Obično ciljni kubit ima određenu oznaku kako bi se istaklo da se operacije odnosi na njega. Primer je CNOT kolo sa  $q_0$  i  $q_2$ , koje zaobilazi  $q_1$ .



Slika 39 - Kontrolni kubit  $q_0$ , ciljni kubit  $q_2$ , kubit  $q_1$  ne učestvuje u operaciji

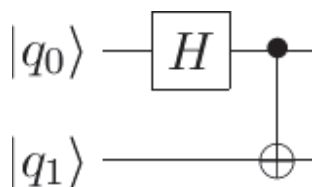
Praktični primer neka bude dijagram jednog od osnovnih kvantnih kola, kolo za "kvantno bacanje novčića". U suštini potrebno je postaviti jedan kubit u stanje superpozicije kad su ishodi

“pismo” i “glava” podjednako mogući a zatim i izmeriti stanje tog kubita. Jednostavni dijagram prikazuje primenu Hadamardovog kola na kubit, zajedno sa operacijom merenja.



Slika 40 - Kubit  $q_0$  stavljen u superpoziciju stanja primenom Hadamardovog kola, sa merenjem stanja

Drugi primer je kvantno korelisanje, odnosno uplitanje stanja dva kubita što je čisti kvantno-mehanički fenomen. (nastaje tzv. EPR par) Da bi se izvršilo korelisanje kubita, prvi bit se podigne u superpoziciju stanja primenom Hadamardovog kola, a zatim se isti bit uzima kao kontrolni bit za operaciju CNOT nad drugim, ciljnim kubitom. Rezultat ove dve operacije je par kvantno korelisanih kubita. Merenje jednog kolabira i drugi kubit istovremeno, u određena stabilna stanja.



Slika 41 - Primenom Hadamardovog kola na  $q_0$ , i CNOT na  $q_1$  nastaje EPR par

## 5.6. Priroda rezultata i ograničenja kvantnih računara

Današnje digitalne računare zovemo klasičnim ili konvencionalnim računarima. Principi rada konvencionalnih računara se nisu menjali od kada je te principe predložio Alan Turing 1930. godine. Klasični računar će za iste ulazne podatke i isti program uvek dati jednake rezultate, dok kvantni računar može redovno da daje potpuno različite rezultate prilikom više uzastopnih izvršavanja istog kvantnog programa nad istim ulaznim podacima, jer je suštinski stohastičke prirode. Na apstraktnom nivou kvantni računari mogu da vrše kalkulacije nad velikim brojem ulaza u isto vreme i ta mogućnost masovnog paralelnog procesiranja predstavlja glavni kvalitet kvantnog računara. Postoje pravila i teoretska ograničenja mogućnosti kvantnih računara koja se ne mogu izbeći, o čemu se govori u sledećim sekcijama.

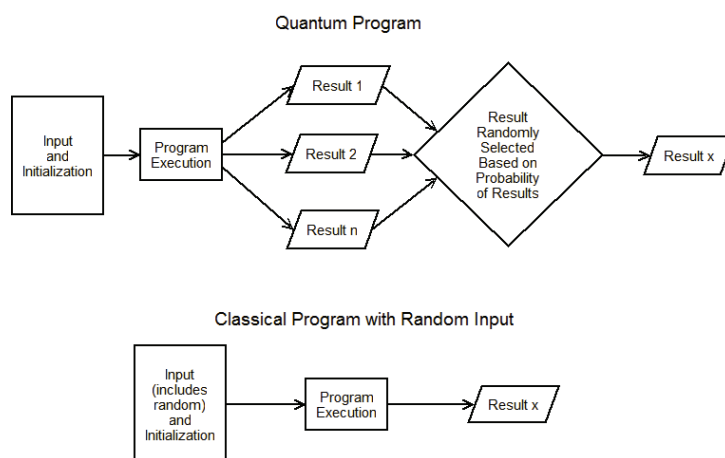
### Stohastička priroda rezultata

Prvo ograničenje je da je izlaz kvantnog računara stohastičke prirode – izvršavanje jednog kvantnog program više puta za redom može dati različite rezultate. Nakon što je merenjem dobijen rezultat kvantnog programa jedini način da se generiše sledeći rezultat je da se kvantni program ponovo izvrši, jer se sistem ne može ponovo vratiti u stanje u kome je bio pre merenja. Rezultat koji

je dobijen zavisi od verovatnoća mogućih odgovora. Postavlja se pitanje koliko je korisno kvantno računarstvo ako su rezultati u velikoj meri slučajni, odnosno ne-egzakti? Postoje dva razloga:

Prvi je da se verovatnoće ishoda mogu menjati ka željenom rezultatu, tako da određeni rezultati na kraju imaju veću verovatnoću ishoda od drugih. Drugi razlog je što je za izvršavanje većine algoritama koji se smatraju "teškim" potrebno mnogo računarskih resursa i po pravilu "težina" algoritma raste eksponencijalno sa povećanjem veličine ulaza. Nasuport tome provera valjanosti rešenja je trivijalna operacija! Verovatnoće ishoda u kvantnom računarstvu mogu međusobno interferirati konstruktivno i destruktivno. Povećanje verovatnoća ka odgovarajućem rezultatu se zove konstruktivna interferencija za razliku od negativne interferencije koja predstavlja minimiziranje verovatnoća netačnih ishoda.

Ideja da se verovatnoća dobijanja određenog rešenja može menjati analogna je (nelegalnom) podešavanju težišta kockica koje se koriste u igrama na sreću kako bi se u nizu bacanja dobio određeni željeni rezultat mnogo češće nego očekivano. Primer je podešavanje para kockica kako bi se povećala verovatnoća dobijanja zbira jednakog 7. U praksi će se izabrati skup rezultata izvršavanja programa na kvantnom računarstvu kao skup mogućih traženih rešenja nakon N uzastopnih izvršavanja kvantnog programa, a zatim će se izvršiti validacija tih rezultata konvencionalnim metodama kako bi se dobilo konačno rešenje datog problema.



Slika 42 - Proces izvršavanja programa na kvantnom i konvencionalnom (klasičnom) računarstvu

### Nemogućnost očitavanja rezultata uzastopnih operacija

Rezultati pojedinih operacija koje se sukcesivno izvršavaju na kvantnom računarstvu se ne mogu očitavati tokom izvršenja kvantnog programa. Ovo ograničenje je fundamentalno za kvantno računarstvo jer sistem ne sme imati interakciju sa okolinom tokom izvršenja programa - svaka interakcija izazvala bi dekoherenciju sistema što je ekvivalentno merenju rezultata i prekidu izvršenja programa. To je jedan od razloga zašto je veoma teško konstruisati praktičan kvantni računar.

Važno je napomenuti da se ovo ograničenje ne može zaobići eventualnim kopiranjem stanja kvantnog računara u pomoćni registar u trenutku merenja međurezultata, a zatim restauracijom kopiranog stanja kako bi se nastavio niz kvantnih operacija. Kao što je navedeno u teoremi o nemogućnosti kopiranja kvantnog stanja (eng. no-cloning theorem) koja je data u prethodnom tekstu, ne postoji način da se kopira stanje kvantnog sistema jer svaka obzervacija sistema dovodi do kolapsa u određeno stanje. Jedino što je preostalo je ponovno pokretanje programa.

U odnosu na navedeno ograničenje kod kvantnih računara, savim je moguće i poželjno zaustavljanje izvršenja programa koji se izvršava na konvencionalnom računaru. Jedan od realnih scenarija je debugovanje klasičnog programa ili kontrolisano zaustavljanje izvršenja u slučaju greške što omogućuje uvid u stanje sistema u tom trenutku izvršenja programa. (npr. try /catch). Implikacija je da je priprema kvantnog programa koji se izvršava bez grešaka složen zadatak, te je potrebno razmotriti ideju razvoja kvantnih programa na simulatoru kvantnog računara. Naravno neophodno je imati u vidu da zahtevi resursa eksponencijalno rastu sa povećanjem veličine ulaznih podataka.

### **Reverzibilnost kvantnih operacija**

Sve operacije na kvantnim računarima moraju biti reverzibilne - po definiciji, moguće je ponovo dobiti sve ulazne podatke na osnovu bilo svakog od rezultata reverzibilne operacije. U suštini kvantni program koji je niz sukcesivnih kvantnih operacija može se izvršiti unazad, da bi se došlo do početnih podataka. Kod nereverzibilnih operacija postoji neto utrošak energije potrebne za brisanje informacije iz sistema, što je poznato kao Landauerov princip. Suprotno tome kvantne logičke operacije ne gube informacije i nema izmene energije sa okolinom, što bi izazvalo dekoherenciju. Ovo ograničenje izgleda striktno ali je moguće dokazati da sve ireverzibilne operacije u klasičnom računarstvu mogu biti transformisane u reverzibilne, što se može postići korišćenjem pomoćnih kontrolnih bita. Formalno sve kvantne logičke operacije su tzv. unitarne operacije koje su opisane u prethodnom tekstu, a unitarne operacije su po definiciji i reverzibilne. Nadalje, postoji neograničen broj dozvoljenih kvantnih operacija jer je svaka unitarna operacija je dozvoljena a stanja kubita su opisana kontinualnim verovatnoćama.

### **Veze sa klasičnim računarstvom**

Kvantni algoritmi (programi) su dizajnirani da rešavaju jedan složeni segment kalkulacije na kvantnom računaru koji se ne može optimalno rešiti na klasičnom računaru, a koji je deo niza koraka većeg konvencionalnog algoritma. To znači da će konvencionalni računar uvek okruživati kvantni stepen. Princip rada je da se svaka kalkulacija koja se izvršava na kvantnom računaru prethodno prebaci, u konvencionalnom domenu, u poseban oblik koji može da se izvrši na kvantnom računaru. Kvantni sistem se zatim na određeni način inicijalizuje na osnovu klasičnih podataka pre nego što se pokrene kvantni program. Nakon izvršene sekvence kvantnih operacije (kvantnog programa),

merenjem kvantni sistem kolabira u neko stanje koje se mora predstaviti na klasičan način. Jednostavno, zatečeno stanje u registru kubita se pretvara u bitove odnosno u neki od tipova podataka kao što su Uint32. Klasični program dalje preuzima taj rezultat, verifikuje i transformiše u sledećem koraku algoritma.

Važna je pretpostavka da će budući kvantni računari biti retki, kompleksni i skupi tehnološki sistemi sa kriogenim elementima i EM zaštitom koji će se deliti između raznih grupa istraživača, analogno sa ranim mejnfrejm računarima iz 1950-ih godina. Može se pretpostaviti da će uvek biti neophodan klasični računarski sistem za prijavljivanje i kontrolisanje redosleda i prioriteta izvršenja poslova, koji okružuje kvantni sistem. Na osnovu današnjih saznanja pretpostavka je da primena klasičnih računara nikad neće biti napuštena a oni potpuno zamenjeni kvantnim računarima.

### **BQP klasa kompleksnosti problema**

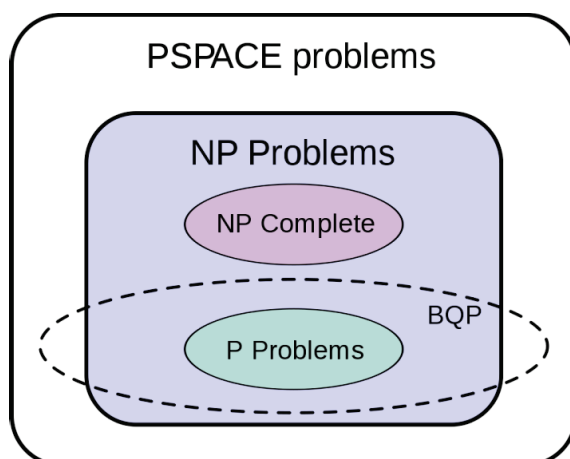
Teorija kompleksnosti izračunavanja (engl. Computational Complexity Theory) je deo teorijske računarske nauke i matematike koja se bavi klasifikacijom problema odnosno algoritama koji se izvršavaju na računaru na osnovu njihove težine, odnosno kompleksnosti, i njihovom međusobnom poređenju. Problem se smatra teškim ako njegovo rešavanje zahteva znatne resurse bez obzira na algoritam koji se koristi. Ova teorija praktično formalizuje intuitivni stav o težini određenog problema na taj način što kvantifikuje potrebne računarske resurse kao što su vreme i memorija u zavisnosti od povećanja ulaznih podataka. Druge metrike kojima se klasifikuju problemi bave se brojem I/O operacija u jedinici vremena, brojem osnovnih logičkih kola potrebnih za implementaciju određenog algoritma na čipu, brojem procesora (jezgara) neophodnih za izvršavanje određenog zadatka u nekom vremenu  $T$ , itd. Razlog izučavanja kompleksnosti problema i definisanja klasa problema je praktičan - potrebno je saznati da li se problem može rešiti na računaru u realnom vremenu, sa datim resursima, a ako može za koje vreme i kakva je zavisnost od povećanja veličine ulaza. Poređenje efikasnosti novih i postojećih algoritama se takođe zasniva na navedenim metrikama. Neke od fundamentalnih klasa su  $P$  i  $NP$  klase kompleksnosti problema.

$P$  klasa kompleksnosti problema sadrži sve probleme odluke (engl. decision problems) koji mogu da se reše u polinomijalnom vremenu na determinističkoj Turingovoj mašini - tj. vreme potrebno da se reši određeni  $P$  problem raste polinomijalno sa povećanjem veličine ulaza.  $NP$  klasa kompleksnosti problema (engl.  $NP$ : non-deterministic polynomial) sadrži sve probleme odluke gde potvrđan odgovor može da se verifikuje u polinomijalnom vremenu na determinističkoj Turingovoj mašini.  $P$  klasa kompleksnosti je sadržana u  $NP$  klasi.  $NP$  klasa sadrži i najteže probleme koji se nazivaju  $NP$ -kompletni (engl.  $NP$ -complete) problemi. Problem se naziva  $NP$ -kompletnim ako istovremeno pripada klasi  $NP$  problema i  $NP$ -teških problema (engl.  $NP$ -hard problems), u čiju definiciju nećemo ulaziti. Za probleme  $NP$ -kompletne klase ne postoje rešenja koja se mogu efikasno pronaći, odnosno ne zna se za efikasna rešenja, dok samo verifikovanje rešenja ostaje trivijalan zadatak. Suštinski vreme potrebno za rešavanje tih problema na računaru raste velikom brzinom kako

se povećava veličina problema (ulaznih podataka). Vreme potrebno za rešavanje problema može da raste eksponencijalno sa linearnom rastom veličine problema, i realno može da bude milion godina.

Klasa problema koji se mogu efikasno rešavati na kvantnim računarima se zove BQP klasa kompleksnosti, odnosno klasa ograničene greške, kvantnog, polinomialnog vremena (engl. bounded error, quantum, polynomial time). Kako kvantni računari izvršavaju stohastičke algoritme, BQP na kvantnom računarima je srodna klasi problema BPP (bounded error, probabilistic, polynomial time) na klasičnim računarima. BPP klasa je skup problema koji se mogu rešavati u polinomijalnom vremenu, čija je verovatnoća greške teži da bude manja od jedne polovine. Shodno tome, na osnovu već opisane stohastičke prirode rezultata kvantnog računara nastala je BQP klasa.

Pretpostavka je da BQP klasa nema preseka sa klasom NP-kompletnih problema, i da je nadskup klase P, ali ova tvrdnja nije dokazana. Problem nalaženja diskretnog logaritma i faktorizacija prirodnih brojeva su BQP problemi. Oba ova problema su NP problemi, a sumnja se da ne pripadaju klasi NP-kompletnih problema. Često je pogrešno shvatanje da kvantni računari mogu da rešavaju problem iz klase NP-kompletnih problema u polinomijalnom vremenu. Za to nema dokaza i generalno se sumnja da to nije tačno. Sledeći dijagram daje odnose među nabrojanim klasama kompleksnosti.



Slika 43 - Odnos BQP klase i klasičnih klasa kompleksnosti problema

### 5.7. Kvantni algoritmi: Dojč-Joža, Grover, QFT, Kvantna simulacija

Istraživanje kvantnih kompjuterskih algoritama neprekidno traje od sredine 80-ih godina prošlog veka, paralelno sa razvojem kvantnih računarskih uređaja koji koriste raznovrsne kvantne fenomene u različitim konfiguracijama. Do pojave čuvenog Šorovog algoritma 1994. godine nije bilo kvantnih algoritama koji su dizajnirani da rešavaju konkretne problem. Piter Šor, istraživač sa MIT-a (Peter W. Shor) je tad objavio kvantni algoritam za faktorizaciju prirodnih brojeva i rešavanje

diskretnih logaritama u polinomijalnom vremenu, koji je i danas jedan od najpoznatijih kvantnih algoritama.

Ostali kvantni algoritmi koji dokazano mogu efikasnije rešavati određene problem su simulacija kvantnih sistema (savijanje molekula proteina, dinamika hemijskih reakcija), pretraživanje nesortiranih nizova objekata, i kvantna Furijeova transformacija - algoritmi opisani u sledećoj sekciji.

### **Dojč-Joža algoritam**

Dojč-Joža algoritam (Deutsch-Josza) je generalizovana verzija Dojčovog algoritma skalirana na  $n$  bita, deterministički algoritam koji je objavljen 1992. godine i nema posebnu primenu osim što predstavlja primer ranog kvantnog algoritma. Algoritam implementira funkciju  $f: \{0,1\}^n \rightarrow \{0,1\}$  koja uzima binarni broj od  $n$  bita i daje 0 ili 1 na izlazu. U slučaju  $n=1$ , algoritam omogućuje određivanje rezultata  $f(0) \text{ xor } f(1)$  sa samo jednim proračunom vrednosti  $f(x)$  dok bi klasični algoritam zahtevao dve kalkulacije, odnosno u slučaju  $n$  bita  $2^{n-1} + 1$  kalkulacija.

### **Grover algoritam**

Lov Grover (Lov Grover) je 1996. godine objavio efikasan kvantni algoritam, poznat kao Groverov algoritam, koji pretražuje niz od  $n$  nesortiranih objekata u bazi podataka za vreme  $O(\sqrt{n})$ , koristeći  $O(\log n)$  kubita, što je znatno efikasnije nego obično pretraživanje niza za vreme  $O(n)$ , a ovaj algoritam je najefikasniji kvantni algoritam koji rešava navedeni problem. Groverov algoritam je kao i većina kvantnih algoritama stohastičke prirode, što znači da će dati tačno rešenje sa velikom verovatnoćom koja se može povećati ponovnim izvršavanjem algoritma. Modifikacija algoritma poznata kao parcijalno kvantno pretraživanje je objavljena 2004. godine i odnosi se na pretraživanje gornjih bitova adrese objekta, kako bi se odredio blok objekata u kome se nalazi traženi objekat.

### **Kvantna Furijeova transformacija (QFT)**

Kvantna Furijeova transformacija (QFT) je kvantni analog diskretne Furijeove transformacije, a koristi se u mnogim kvantnim algoritmima kao što je Šorov, kod kvantne procene karakterističnih vrednosti unitarnih operatora (engl. estimating eigenvalues of unitary operator), i algoritma za pronalaženje skrivenih podgrupa (engl. finding hidden subgroup). Algoritam se može implementirati sa  $O(n^2)$  Hadamard kola i kola za promenu faze (engl. controlled phase shift gate), za razliku od klasične implementacije diskretne Furijeove transformacije koja treba  $O(n2^n)$  logičkih kola, za  $n$  bita, što je očigledno eksponencijalno više nego kod QFT implementacije.

### **Kvantne simulacije**

Ričard Fejnman je prvobitno došao na ideju kvantni računari mogu eksponencijalno brže izvršavati simulacije kvantnih sistema sa više čestica (engl. many-particle quantum systems) u odnosu

na klasične računare. Od tada su razvijeni efikasni kvantni algoritmi za simulaciju bozonskih i fermionskih sistema koji se izvršavaju u polinomijalnom vremenu. Teoretski simulacije dinamike hemijskih reakcija, koje zahtevaju računarske resurse daleko iznad postojećih klasičnih super računara, bi se efikasno obavljale na hipotetičkom kvantnom računaru kapaciteta nekoliko stotina kubita.

## 5.8. Šorov algoritam

Diskretni algoritmi i faktORIZACIJA prirodnih brojeva se smatra teškim problemima u klasičnom računarstvu, bez poznatih efikasnih algoritama koji bi rešavali ove probleme u vremenu manjem od eksponencijalnog. Navedeni problemi se koriste u modernim šifarskim sistemima – faktORIZACIJA prirodnih brojeva se koristi u RSA, asimetričnom kriptografskom algoritmu, koji je osnova većine komercijalnih algoritama za sigurnu komunikaciju.

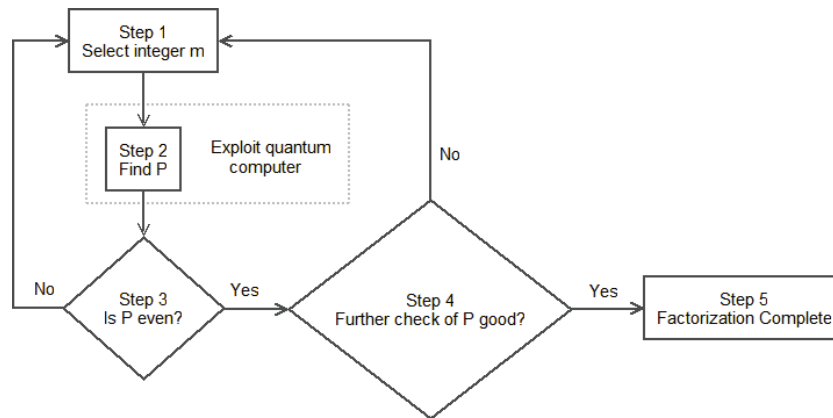
Kada se reše inženjerski problemi implementacije efikasnih kvantnih računara, Šorov algoritam može učiniti većinu navedenih šifarskih sistema zastarelim, uz ogromne implikacije na e-komerc, nacionalnu bezbednost, i druge važne aplikacije. U Novembru 2011. godine kineski istraživači su uspeli da faktORIZUJU broj 143 primenom ovog algoritma.

Šorov algoritam pronalazi dva prosta broja,  $p$  i  $q$ , na osnovu poznatog  $N$ , gde je  $N=pq$ , što je u suštini problem faktORIZACIJE velikih prirodnih brojeva. Sledeća tabela opisuje varijable koje se koriste u opisu samog algoritma.

| simbol | značenje                                                                   |
|--------|----------------------------------------------------------------------------|
| $N$    | Broj koji se faktoriše                                                     |
| $p, q$ | Činioci broja $N$                                                          |
| $P$    | Period                                                                     |
| $m$    | Jedinstveni slučajni broj u svakoj iteraciji                               |
| $n$    | Broj kubita u registru potrebnih da sadrži $N$                             |
| $f$    | Funkcija nad prirodnim brojevima koja je periodična za operaciju sabiranja |

Tabela 6 - Varijable u Šorovom algoritmu

Algoritam se sastoji iz klasičnog i kvantnog dela. Ključni deo algoritma gde se koristi kvantni računar je pronalaženje perioda  $P$  funkcije  $f$ , funkcije u domenu prirodnih brojeva koja je periodična kod sabiranja, i gde je  $f(x) = f(y)$  za različito  $x, y$ . U ovom slučaju  $x, y$  se razlikuju za množilac  $P$ , odnosno  $f(x + P) = f(x)$ . Sledeća slika daje prikaz toka algoritma u 5 odvojenih faza. Kao što je prikazano na slici kvantni računar se koristi isključivo u fazi 2 radi povećanja efikasnosti.



Slika 44 - Prikaz toka Šorovog algoritma po fazama

**Faza 1** U prvoj fazi bira se slučajan prirodni broj  $m$ , i  $m < N$ , a  $N$  je broj koji faktorišemo. Zatim se bira najveći zajednički delilac  $N$  i  $m$  (engl. gcd) korišćenjem Euklidovog algoritma koji je dovoljno efikasan na klasičnim računarima. Ako je  $\neq 1$ ,  $m = p$  ili  $m = q$ . U tom slučaju smo sasvim slučajno izabrali jedan od faktora na sreću, i algoritam je završen. U većini slučajeva to se ne dešava.

**Faza 2** U drugoj fazi, u kojoj se jedino koristi kvantni računar radi efikasnosti, pokušavamo da nađemo period  $P$  kako bi se dobio faktor. Funkcija  $f(x) = m^x \bmod N$  ima period  $P$ , gde je  $P \leq N$ . Period  $P$  je najmanji prirodni broj za koji važi  $f(x + P) = f(x)$ , za svako  $x$ . Kada se izračunava  $f(x)$ , mora da se proba dovoljno vrednosti  $x$  kako bi se našao period  $P$ . Važno je napomenuti da kod izračunavanja  $m^x$  u  $f(x)$  brzo može doći do overflow-a, u većini programskih jezika koji ne podržavaju proizvoljne veličine tipova za prirodne brojeve. Postoji način da se izbegne ovaj problem, i da bi se izračunala sledeća vrednost  $f(x)$  može da se iskoristi sledeći identitet:

$$m^x \bmod N = ((m^{x-1} \bmod N)m) \bmod N$$

**Faza 3** U trećoj fazi neophodno je proveriti da li je  $P$  paran broj. Ako je neparan počinjemo algoritam ispočetka, od faze 1, sa novim slučajnim brojem  $m$ , gde je  $m < N$ . Ova faza se ponavlja sa novim slučajnim brojem  $m$  sve dok se ne dobije parna vrednost za  $P$ .

**Faza 4** U četvrtoj fazi mora da se proveriti da li je  $(m^{\frac{P}{2}} + 1) = 0 \bmod N$ , na osnovu datih vrednosti  $P$  i  $N$ . Ako je ovo tačno počinjemo algoritam iz početka, od faze 1, pošto je  $\gcd(m^{\frac{P}{2}} - 1, N) = 1$ , te nije pronađen faktor. Kao i kod faze 3, neophodno je naći novo  $m$  koje nismo probali, uz uslov da  $m < N$ . Ako je  $(m^{\frac{P}{2}} + 1) \neq 0 \bmod N$ , idemo u fazu 5.

**Faza 5** Peta faza zaključuje algoritam. Sad je  $\gcd(m^{\frac{P}{2}} - 1, N)$  ili  $\gcd(m^{\frac{P}{2}} + 1, N)$  faktor broja  $N$  koji je veći od 1 (možda i oba) - dakle  $\gcd(m^{\frac{P}{2}} - 1, N)$  i/ili  $\gcd(m^{\frac{P}{2}} + 1, N)$  je jedan od faktora,  $p$  ili  $q$ .

Pošto imamo jedan faktor lako je dobiti drugi faktor broja  $N$ , na osnovu  $q = N/p$ , što predstavlja kraj izvršavanja algoritma.

## Primena kvantnog računara u fazi 2

U ovom delu će biti opisana primena kvantnog računara u fazi 2 Šorovog algoritma, kako bi se našao period  $P$  funkcije. Pretpostavićemo da su definisani unitarni operatori bez detaljnih objašnjenja kako su konstruisane odgovarajuće operacije, o čemu će biti reči kasnije.

Za kvantnu verziju faze 2, potrebna su dva registra koja ćemo nazvati Registar 1 i Registar 2,  $|REG1\rangle$  i  $|REG2\rangle$ .  $|REG1\rangle$  će sadržati moguće vrednosti varijable  $x$ , dok će  $|REG2\rangle$  sadržati rezultat evaluacije funkcije  $f(x)$ . Kao što je uobičajeno,  $n$  predstavlja broj kubita potrebnih da se izrazi broj  $N$  koji se faktoriše, gde je  $n = \log_2 N$ . Kako moramo prikazati sve moguće vrednosti  $x$  ( $0 \leq x \leq N^2$ ) unutar registra  $|REG1\rangle$ , on mora da se sastoji od minimalno  $2n$  kubita. Udvostručavanjem broja kubita u  $|REG1\rangle$  postojeće najmanje  $N$  perioda funkcije  $f(x)$ . Rezultat evaluacije funkcije  $f(x)$  će uvek biti manji od  $N$ , te je stoga potrebno da se  $|REG2\rangle$  sastoji od najmanje  $n$  kubita. Zajedno potrebno je  $3n$  kubita kako bi se implementirao ovaj kvantni algoritam.

Važno je takođe napomenuti da iako postoje dva registra,  $|REG1\rangle$  i  $|REG2\rangle$ , oni su u suštini jedan registar od  $3n$  kubita. Ovo je važan zaključak jer algoritam zahteva kvantno korišćenje kubita oba registra – drugim rečima iako postoje dva logički odvojena registra na njima se u istom trenutku vrše operacije. Oba registra su inicijalizovana na nulu,  $|0 \dots 0\rangle$ , a radi lakšeg snalaženja stanja kubita će biti prikazana kao nizovi binarnih brojeva koji predstavljaju pozitivni prirodni broj. Za primer  $|00111\rangle$  znači da registar od 5 kubita predstavlja decimalni broj 7, u trenutku merenja stanja registra.

Nakon inicijalizacije registara, primenjuje se Hadamard operacije na svih  $2n$  kubita u registru  $|REG1\rangle$ , Nakon primene Hadamarda  $|REG1\rangle$  se nalaze u superpoziciji svih vrednosti ( $0 \leq x \leq N^2 - 1$ ). U Dirakovoj notaciji ovo stanje se može predstaviti na sledeći način:

$$\frac{|0 \dots 00\rangle + |0 \dots 01\rangle + |0 \dots 10\rangle + |0 \dots 11\rangle + \dots + |1 \dots 11\rangle}{\sqrt{2^n}}$$

Dalje, definišemo operaciju  $U_f = |REG1\rangle|REG2\rangle \rightarrow |REG1\rangle|f(|REG1\rangle)\rangle$  i primenjujemo je na oba registra ( $f(x)$  je definisana u prethodnom poglavlju). Operacija  $U_f$  uzima vrednost  $x$  iz registra  $|REG1\rangle$  i upisuje sve rezultate funkcije  $f(x)$  u  $|REG2\rangle$ . Nakon primene operacije  $U_f$ , kubiti registara  $|REG1\rangle$  i  $|REG2\rangle$  su kvantno korelisani. Može se smatrati da  $|REG1\rangle$  sadrži sve moguće vrednosti  $x$ , a  $|REG2\rangle$  sve vrednosti  $f(x)$  za svako  $x$ . Ova činjenica objašnjava prednosti kvantnog računarstva – sve moguće vrednosti argumenta i funkcije su sadržane u registrima kvantnog računara istovremeno.

U trenutku kad se izmeri stanje  $|REG2\rangle$ , nastaje i kolaps registra  $|REG1\rangle$  u neko stabilno stanje, jer su registri kvantno korelisani.  $|REG1\rangle$  sada sadrži vrednost  $x$  koja odgovara vrednosti u

$|REG2\rangle$ . U sledećem koraku kvantna Furijeova transformacija (QFT) je primenjena na  $|REG1\rangle$  i  $|REG1\rangle$  je zatim izmeren. Dobijeni rezultat predstavlja period  $P$  funkcije, prirodni broj koji zadovoljava jednakost  $m^P = 1 \bmod N$ . Nakon što je period  $P$  dobijen kvantni deo algoritma je završen i nastavlja se ka fazi 3 koja se izvršava na klasičnom računaru.

### Primer faktorizacije za $N = 15$

Radi lakšeg razumevanja algoritma možemo prikazati nalaženje faktora broja 15 korišćenjem Šorovog algoritma:

**Faza 1** U prvoj fazi bira se slučajan prirodni broj  $m$ , i  $m < 15 = N$ , Za ovaj primer izaberimo  $m = 8$ . Proverimo da je  $\gcd(8,15) = 1$ , što znači da se može nastaviti u fazu 2.

**Faza 2** U drugoj fazi izračunavamo vrednosti  $f(x)$ , za svako  $(0 \leq x \leq 15^2 - 1)$ , gde je  $f(x) = m^x \bmod N$ . Kao što je rečeno krajnji cilj je naći period  $P$  date funkcije, gde je  $P \leq N$ , a mora biti da je  $(x + P) = f(x)$ . Nekoliko kalkulacija od mogućih 225 je dato ovde:

$$f(0) = 8^0 \bmod 15 = 1$$

$$f(1) = 8^1 \bmod 15 = 8$$

$$f(2) = 8^2 \bmod 15 = 4$$

$$f(3) = 8^3 \bmod 15 = 2$$

$$f(4) = 8^4 \bmod 15 = 1$$

$$f(5) = 8^5 \bmod 15 = 8$$

$$f(6) = 8^6 \bmod 15 = 4$$

$$f(7) = 8^7 \bmod 15 = 2$$

$$f(8) = 8^8 \bmod 15 = 1$$

$$f(9) = 8^9 \bmod 15 = 8$$

$$f(10) = 8^{10} \bmod 15 = 4$$

$$f(11) = 8^{11} \bmod 15 = 2$$

...

Kao što se jasno može primetiti na sekvenci vrednosti funkcije kod ovog jednostavnog primera, uočava se da je period  $P = 4$  jer funkcija za sekvencijalni niz argumenata uzima vrednosti 1, 8, 4, 2, koje se ponavljaju sa periodom 4 za svih 225 argumenata.

Kada se klasična faza 2 zameni kvantnom, svih 225 (255) mogućih vrednosti argumenta  $x$  predstavljeno je u registru  $|REG1\rangle$  istovremeno, kako bi se našle sve vrednosti  $f(x)$ . Da bi se predstavio broj 15, potrebna su 4 kubita, pa je  $n = 4$ . Na osnovu toga potrebno je alocirati 8 kubita za  $|REG1\rangle$ , i 4 kubita za  $|REG2\rangle$ . Zatim su svi kubiti inicijalizovani na 0 -  $|REG1\rangle = |00000000\rangle$ ,  $|REG2\rangle = |0000\rangle$ . Dalje, nakon primene Hadamard operacije na svih 8 kubita registar  $|REG1\rangle$  se nalazi u superpoziciji svih 255 stanja istovremeno.

$$\frac{|00000000\rangle + |00000001\rangle + |00000010\rangle + |00000011\rangle + \dots + |11111111\rangle}{\sqrt{256}}$$

Nakon što se  $|\text{REG1}\rangle$  nađe u superpoziciji, primenjuje se operacija  $U_f$ , nakon koje  $|\text{REG2}\rangle$  sadrži sve vrednosti  $f(x)$  za sve vrednosti  $x$  u  $|\text{REG1}\rangle$ .  $f(x)$  teoretski može da bude broj od 0 do 15 ali kako je već prikazano u klasičnoj fazi 2,  $f(x)$  će samo uzimati vrednosti 1, 2, 4, ili 8, za svako  $x$ . U ovom trenutku  $|\text{REG2}\rangle$  može da kolabira u jedno od stanja 1, 2, 4, ili 8 sa jednakom verovatnoćom za svaki ishod,  $p = 0.25$ .

$$\begin{aligned} & \frac{1}{\sqrt{16}}|0001\rangle + \frac{1}{\sqrt{16}}|0010\rangle + \frac{1}{\sqrt{16}}|0100\rangle + \frac{1}{\sqrt{16}}|1000\rangle + \\ & \frac{1}{\sqrt{16}}|0001\rangle + \frac{1}{\sqrt{16}}|0010\rangle + \frac{1}{\sqrt{16}}|0100\rangle + \frac{1}{\sqrt{16}}|1000\rangle + \\ & \frac{1}{\sqrt{16}}|0001\rangle + \frac{1}{\sqrt{16}}|0010\rangle + \frac{1}{\sqrt{16}}|0100\rangle + \frac{1}{\sqrt{16}}|1000\rangle + \\ & \frac{1}{\sqrt{16}}|0001\rangle + \frac{1}{\sqrt{16}}|0010\rangle + \frac{1}{\sqrt{16}}|0100\rangle + \frac{1}{\sqrt{16}}|1000\rangle = \\ & = \frac{1}{\sqrt{4}}|0001\rangle + \frac{1}{\sqrt{4}}|0010\rangle + \frac{1}{\sqrt{4}}|0100\rangle + \frac{1}{\sqrt{4}}|1000\rangle = |\text{REG2}\rangle \end{aligned}$$

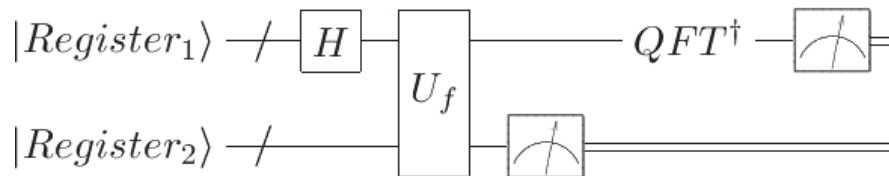
Uzmimo da je merenjem  $|\text{REG2}\rangle$  kolabirao u stanje 4 ( $|0100\rangle$ ). Merenje stanja  $|\text{REG2}\rangle$  takođe uzrokuje kolaps  $|\text{REG1}\rangle$  pošto su dva registra prethodno kvantno korelisana primenom operacije  $U_f$ . Na osnovu pretpostavke da je  $|\text{REG2}\rangle$  kolabirao u stanje 4, u  $|\text{REG1}\rangle$  će se biti svako  $x$  za koje je  $f(x) = 4$ , dakle u superpoziciji stanja  $x = 2, 6, 10, 14, \dots x \leq 255$ .

$$\begin{aligned} & \frac{|00000010\rangle + |000001110\rangle + |00001010\rangle + |00001110\rangle + \dots}{\sqrt{64}} = \\ & \frac{|2\rangle + |6\rangle + |10\rangle + |14\rangle + \dots}{\sqrt{64}} \end{aligned}$$

Na kraju je neophodno iz superpozicije rešenja u  $|\text{REG1}\rangle$ , za  $f(x) = 4$ , naći period  $P$ . Za ovo se koristi kvantna Furijeova transformacija (QFT), uz konačno merenje rezultata. Ovim se završava kvantna faza 2, i nastavlja klasični algoritam fazom 3, sa periodom  $P = 4$  funkcije  $f(x)$ , kao što je objašnjeno u prethodnoj sekciji.

### Dijagram kvantnog dela Šorvog algoritma

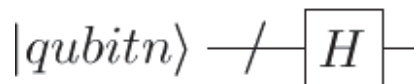
Kvantni deo Šorovog algoritma je implementiran u polinomijalnom broju kvantnih kola,  $O(\log N)$ , rešavajući problem kroz tri dela kola koja rešavaju svaki svoj poseban zadatak. Na slici je dat kompletan postupak iz tri dela, Hadamardovo kolo, implementacija funkcije  $f(x)$  putem kvantne operacije  $U_f$ , i kvantna Furijeova transformacija (QFT) sa finalnim merenjem stanja oba registra.



Slika 45 - Dijagram kvantnog kola za implementaciju faze 2 Šorovog algoritma

### Primena Hadamard operacije

Prvi deo kola se odnosi na stavljanje registra  $|REG1\rangle$  u supepoziciju primenom Hadamard kola na  $2n$  kubita  $|REG1\rangle$ . Ispod je odgovarajući dijagram sa kosom linijom koja predstavlja  $n$  kubita.

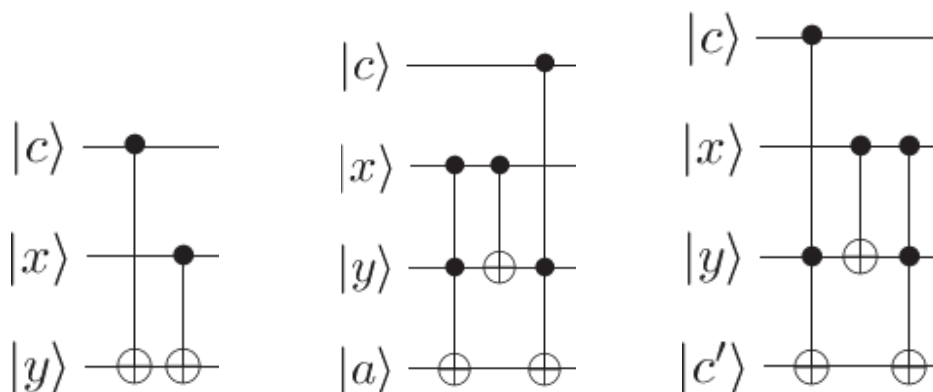


Slika 46 - Primena Hadamardove operacije nad  $n$  kubita

### Implementacija funkcije $f(x)$ - kvantna operacija $U_f$

Drugi deo kola implementira funkciju  $f(x)$  putem kvantne operacije  $U_f$  na register  $|REG1\rangle$  i  $|REG2\rangle$ .  $U_f$  je veom kompleksna operacija i to je najsloženiji deo kvantnog algoritma koji se implementira velikim brojem elementarnih kvantnih kola – u suštini bazira se na implementaciji modularnog sabirača koj se koristi u implementaciju modularnog multipleksa, koji je na kraju osnova za implementaciju funkcije modularni eksponent korišćenjem metode "repeated squaring".

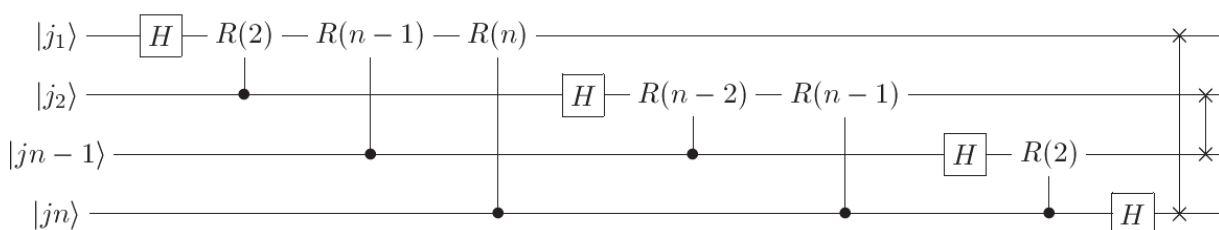
Pošto je ovo veoma složena i obimna operacija, opisana su tri osnovna kola: suma, prenos, i inverzni prenos (prenos<sup>-1</sup>) koja se koriste za implementaciju elementarnog modularnog 2-kubitnog sabirača. U donjim dijagramima kubiti  $|x\rangle$  i  $|y\rangle$  se sabiraju (mod 2), prenos je označen sa  $|c\rangle$  (engl. carry), dok je  $|a\rangle$  pomoćni, tzv. ansila, kubit (engl. ancilla) koji ne predstavlja nikakav rezultat ali se koristi kao skreć-bit ili međurezultat kod nekih kvantnih operacija.



Slika 47 - Dijagrami kvantnih kola za sumu, prenos, i inverzni prenos kod implementacije  $U_f$

### Implementacija kvantne Furijeove transformacije

Kvantna Furijeova transformacija je poslednji korak u kvantom delu Šorovog algoritma, sa poznatim Hadamardovim kolom, swap kolima, kao i ranije opisanim  $R_k$  kolima koje su za  $k=2$  i  $k=3$  ekvivalentne S i T kvantnim kolima.



Slika 48 - Dijagram kvantnog kola za QFT

### 5.9. Simulacija rada kvantnog računara

Procenjuje se da će praktični kvantni računari postati javno dostupni za 10 ili više godina. U međuvremenu je neophodno naći način za razvoj i testiranje novih kvantnih algoritama. Jedno od rešenja ovog problema je razvoj softvera za simulaciju kvantnih računara na klasičnim računarima. Simulacija kvantnih računara može biti korisna kako istraživačima radi testiranja novih, tako i studentima radi razumevanja postojećih kvantnih algoritama. U trenutku kada se pojave praktični kvantni računari još uvek neće biti lako doći do računarskih resursa, slično kao kod pojave prvih velikih računara u 1950-im godinama. Klasična simulacija će i tada biti neophodna mnogim korisnicima koji neće imati priliku da pristupe novim resursima.

## **Praktična ograničenja simulacije**

Ključno ograničenje klasične simulacije je eksponencijalan rast potrebnih računarskih resursa usled povećanja veličine ulaznih podataka. Prednost kvantnog računara je upravo mogućnost paralelnog izvršavanja operacija. Registar od 8 kubita u sebi istovremeno sadrži 256 stanja sa određenim pridruženim verovatnoćama. U klasičnoj simulaciji neophodno je čuvati svih 256 vrednosti verovatnoća u nekoj memorijskoj strukturi. Kvantne kalkulacije se zasnivaju na povećanju verovatnoća potencijalnih rešenja odnosno smanjenju verovatnoća preostalih rezultata. Drugim rečima verovatnoće svih stanja postepeno evoluiraju primenom odgovarajućih kvantnih operacija. Povećanjem broja kubita, npr. na 9 ili 10 kubita, eksponencijalno se povećava veličina memorije potrebne za čuvanje vrednosti verovatnoća svih stanja sistema na 512, odnosno 1024, respektivno. To je veliko ograničenje koje implicira da svaka simulacija mora da radi sa razumnim ulaznim podacima kako bi se završila u prihvatljivom vremenu.

## **Prednosti simulacije**

Kvantni računar radi na principu evolucije vrednosti verovatnoća a rezultati sekvencijalnih kalkulacija sa istim početnim uslovima su uvek veoma različiti. U principu kvantni program se izvršava veliki broj puta da bi se odvojili određeni kandidati za rešenja datog problema, koji se zatim testiraju klasičnim putem (provera rešenja uvek zahteva najviše polinomijalno vreme). Klasična simulacija omogućuje ranije identifikovanje mogućih rešenja, bez velikog broja uzastopnih simulacija.

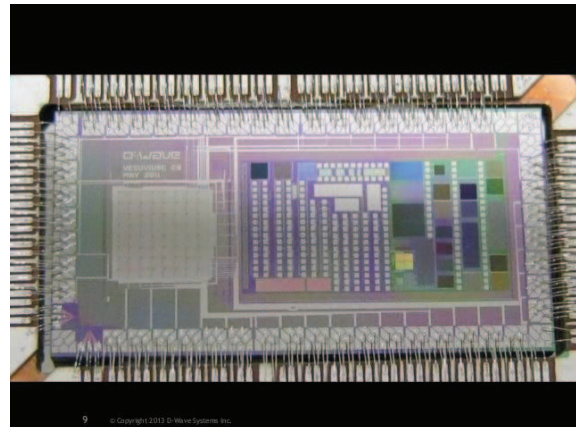
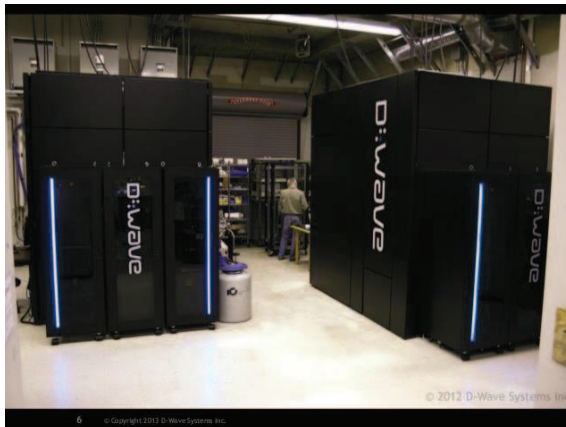
Druga značajna prednost simulacija kvantnog računara je mogućnost debugovanja kvantnog algoritma zaustavljanjem simulacije i očitanjem međurezultata kako bi se osiguralo da algoritam radi na način na koji je dizajniran. Na pravom kvantnom računaru ovo teoretski nije moguće jer očitavanje međurezultata kolabira registre u neko od stanja i jedino što preostaje je ponovno pokretanje izvršavanja kvantnog programa

### **5.10. Primer komercijalnog kvantnog uređaja**

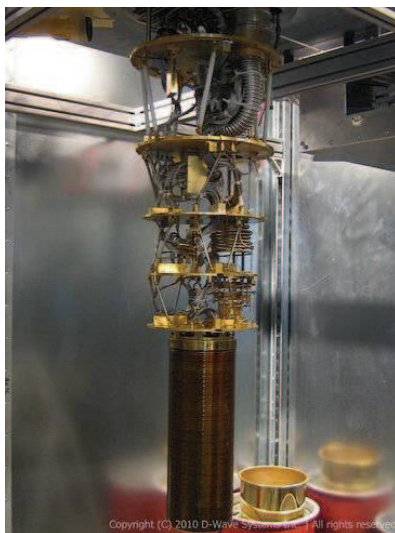
Prvi komercijalni kvantni uređaj od 128 kubita koji koristi metode kvantnog "prekaljivanja" (engl. quantum annealing) napravila je kanadska kompanija D-Wave Systems (D-Wave Systems). Njihov poslednji proizvod predstavljen 2013 godine je komercijalni kvantni uređaj D-Wave Two. Sa procesorom Vesuvius koji sadrži 512 kubita, nalazi se unutar velikog kriogenog postrojenja zaštićen od EM zračenja u prostoriji od 10 m<sup>2</sup>. Prve uređaje po ceni od 10 miliona američkih dolara već su su nabavile kompanije Lockheed-Martin, Boeing, ali i američka NASA.

Navedeni kvantni uređaj ne može se smatrati univerzalnim kvantnim računarom ali on koristi određene kvantne efekte kako bi optimizacijom dao rešenja posebne klase problema. Konkretno uređaj radi na principu adiabatske kvantne optimizacije, gde se kubiti polako podešavaju iz početnog

stanja superpozicije u klasično stanje 0 ili 1. Ovaj process se odvija u prisustvu programiranih memorijskih elemenata na procesoru, a vrednosti 0 i 1 u koje kubiti polako prelaze postaju rešenja zadanog problema. Sva kola na uređaju su napravljena od tzv. super-provodničkih materijala koji su hlađeni na radnu temperaturu od 20 mK (miliKelvina  $\sim -273^\circ\text{C}$ ).



Slika 49 - D-Wave 2 - adiabatski kvantni računarски sistem i verzija Rainer procesora sa 128 qb



Slika 50 - D-Wave 2 – detalji kriogenog postrojenja

### 5.11. Perspektive kvantnog računarstva

Postoje brojni modeli kvantnog računarstva koji se razlikuju na osnovu načina razlaganja procesa izračunavanja rešenja za dati problema, a glavna četiri pravca razvoja su:

- "Quantum gate array", kvantno računanje se sastoji iz primene niza kola nad više kubita.

- "One-way quantum computer", kvantno računanje se sastoji iz niza merenja pojedinačnih kubita koje se primenjuju na visoko-korelisano prvobitno stanje ili klaster stanje.
- "Adiabatic quantum computer" – računar radi na bazi kvantnog "prekaljivanja" (engl. quantum annealing) gde se kalkulacije sastoje od spore neprekidne transformacije provobitnog Hamiltoniana u konačni Hamiltonian operator čija bazna stanja sadrže rešenje.
- "Topological quantum computer" – kvantno računanje se zasniva na uplitanju aniona 2D rešetke.

### **Postojeće tehnologije implementacije**

Dosadašnji pokušaji implementacije praktičnog kvantnog računara razlikuju se na osnovu tehnologije fizičke implementacije kubita, i dele na sledeće važnije kategorije:

- Interferencija superprovodnika (engl. SQUID), kubiti su implementirani stanjima malih superprovodnih kola, tzv. Josephson junctions.
- Zarobljeni joni (engl. trapped ion quantum computer), kubiti su implementirani unutrašnjim stanjima zarobljenih jona
- Optičke rešetke (engl. optical lattices), kubiti su implementirani unutrašnjim stanjima neutralnih atoma zarobljenih u optičkoj rešetci.
- Kvantne tačke (engl. quantum dots), kubiti su implementirani pozicijom elektrona unutar dvostruke kvantne tačke, ili spina elektrona.
- Nuklearna magnetna rezonanca (engl. NRI), kubiti su implementirani nuklearnim spinovima molekula u nekom rastvoru

### **Pretpostavke i izazovi**

U ovom trenutku ne postoji praktični univerzalni kvantni računar. Najjači postojeći eksperimentalni kvantni računar radi sa najviše 12 kubita. Razlog za to su tehnoloških izazovi vezani za izolovanje uređaja od okoline, prvenstveno da bi se kontrolisala dekoherencija, te se primenjuju raznovrsni pristupi arhitekturi eksperimentalnih kvantnih računara. Praktični i teoretski razvoj u ovoj oblasti je neprekidan od pojave prvih ideja o kvantnom računarstvu sredinom 1980-ih. Preovladava mišljenje da će kvantni računari sa 50 kubita po sirovoj računarskoj snazi biti ekvivalentni današnjim konvencionalnim superračunarima.

Osim faktORIZACIJE prirodnih brojeva i rešavanja diskretnih algoritama, pojedini autori smatraju da će se veoma važni problemi optimizacije (NP-kompletni) moći izvršavati u realnom vremenu na budućim kvantnim uređajima - problemi kao što su tzv. problem punjenja ruksaka (engl. Knapsack problem), trgovačkog putnika (engl. Traveling salesman problem), izomorfizma podgrafa (engl. Subgraph isomorphism), problem sume podskupa (engl. Subset sum), i nekoliko desetina sličnih

problema. Rešavanje navedenih problema optimizacije u realnom vremenu bi predstavljao istinski revolucionarni proboj u nauci.

Simulacija kvantnih fizičkih procesa iz hemije i fizike čvrstog stanja predstavljaju najvažniju klasu problema koja će se u teoriji optimalno rešavati na budućim kvantnim računarima. Mogućnosti simulacija složenih kvantnih procesa će takođe imati ogromnog uticaja i izazvati revoluciju u nauci. Kao primer može se uzeti simulacija ponašanja velikih molekula kao što su proteini. Na ovaj način bi se procesi kao što su npr. delovanje lekova u organizmu mogli simulirati u realnom vremenu. To bi predstavljalo jedno od najvećih dostignuća u biohemiji i medicine uopšte.

Većina izvora tvrdi da će praktično kvantno računarstvo biti dostupno najranije za 10 do 15 godina. Gartner, poznata svetska kompanija koja se bavi analizom i predviđanjem tehnoloških trendova u svetu, na skali nadolazećih tehnologija za 2013. godinu procenila je da će praktično kvantno računarstvo biti u širokoj upotrebi tek za 10 i više godina.



Slika 51 - Gartnerova skala novih tehnologija i pozicija kvantnog računarstva

Polje kvantnog računarstva je veoma novo i dinamično i u tom smislu je potreban dalji rad na razvoju novih kvantnih algoritama koji će rešavati ključne probleme u nauci. Paralelno mora teći razvoj kvantnih računara na bazi novih arhitektura i tehnologija koje će omogućiti implementaciju kubita sa dovoljno dugim vremenom dekoherencije i skaliranje ka registrima od par hiljada kubita.

Mnoge državne agencije za nauku i bezbednost kao i velike svetske korporacije ulažu ogromna finansijska sredstva u razvoj kvantnog računarstva. Kvantno računarstvo pripada onim remetilačkim (engl. disruptive) tehnologijama poput nuklearnih tehnologija, interneta ili mobilnih komunikacija, koja može da izazove revoluciju u modernoj nauci ali i u društvenim odnosima u najširem smislu, i potpuno promene način života koji poznajemo.

## 6. Post-kvantna kriptografija

Pojam post-kvantna kriptografija podrazumeva kriptografske algoritme odnosno odgovarajuće šifarske sisteme koji se ne mogu kompromitovati primenom kvantnog računara. Važno je istaći da je većina simetričnih šifarskih sistema otporna na primenu kvantnih računara, pa se stoga post-kvantna kriptografija ne bavi simetričnim algoritmima.

### Izazovi za post-kvantne šifarske sisteme

Postavlja se pitanje zašto se već danas mora voditi računa o opasnosti od razbijanja postojećih šifarskih sistema primenom kvantnog računara, iako je ta tehnologija tek u začetku?

U principu je moguće globalno zaštititi sve komunikacije primenom nekog od postojećih šifarskih sistema koji su otporni na napade kvantnim računarima, kao što je NTRU ili Mekelis. Zamena šifarskih sistema koji se trenutno koriste, kao što su razne varijante RSA i DH, post-kvantnim sistemima može sačekati do trenutka kad bude izvesno da je tehnologija kvantnih računara dostigla zrelost, što je prema trenutnim procenama 10-15 godina u budućnosti. Sa druge strane postoje jaki argumenti zašto je već danas neophodno ulagati u istraživanja post-kvantnih šifarskih sistema, argumenti koji su relevantni u svim poljima kriptografije, od početaka do danas.

### Efikasnost algoritama

Spor šifarski sistem koji zahteva značajne računarske resurse može biti prihvatljiv za neke korisnike ali takav sistem sigurno ne može biti primenjiv u scenarijima pristupa internet server koji mora da obradi desetine hiljade klijenata svake sekunde. Kao primer uzmimo siguran pristup veb serveru (https protokol), gde postoje dodatni koraci za početno uspostavljanje parametara i razmenu ključeva, i na kraju šifrovanja/dešifrovanja podataka. Navedeni koraci moraju da budu mnogo manje zahtevni što se tiče potrebnog vremena i resursa (overhead) u poređenju sa resursima vezanim za regularnom pristupu serveru i razmeni podataka putem http-a. Drugi primer je sigurna komunikacija između servera i mobilnih odnosno embedded sistema koji imaju ograničene resurse - to je jedno od ograničenja koje usmerava razvoj algoritama u ovoj oblasti.

### Poverenje u valjanost algoritama

Merkle heš-drvo (engl. hash tree) sistem za potpisivanje sa javnim ključem i Mekelisov istem sa Gopa kodovima (engl. hidden-Goppa code) su objavljeni pre više od trideset godina ali još uvek nisu kompromitovani unatoč nebrojenim pokušajima kriptanalista. Relativno novi šifarski sistemi kao što su sistemi na bazi rešetke nad celim brojevima (engl. lattice), predstavljaju post-kvantne šifarske sisteme koji su kandidati za široku primenu na internetu. Realno je moguće da u skoroj budućnosti neki od navedenih šifarskih sistema bude potpuno diskvalifikovan primenom novih tehnika, ali je moguće i da se nađu rešenja koje će značajno poboljšati robusnost sistema na napade. Da bi se izgradilo široko poverenje javnosti u nove post-kvantne šifarske sisteme potrebno je da ti

sistemi izdrže godine analiza i napada kriptanalista. U tom period potencijalni korisnici kao što su programeri, analisti sistema, stručnjaci za zaštitu podataka, i drugi, mogu da upoznaju nove sisteme, njihove prednosti i ograničenja. Na taj način bi se omogućila masovna primena komercijalnih rešenja na bazi ovih šifarskih sistema u svakodnevnim komunikacijama.

### Primenjivost algoritama

Uzimajući istorijski razvoj RSA šifarskih sistema može se uzeti kao primer činjenica da je primenjivost ranog algoritma bila na eksperimentalnom odnosno akademskom nivou sve dok nije napuštena primena velikih eksponenata, čime su do tada neopravdano usporavali algoritam bez ikakve koristi. Kasniji razvoj šifarskih sistema je značajno izmenio određene delove algoritma nakon uspešnih napada, koji su opet doveli do primene odgovarajućih kontra-mera, što praktično znači da je današnji šifarski sistem postepeno značajno evoluirao dok su rane verzije bile daleko od idealnih.

Nakon što je detaljno definisan jedan takav šifarski sistem, potrebno je obratiti pažnju na softversku i/ili hardversku implementaciju, kako bi se on uspešno integrisao u različite aplikacije. Neophodno je obezbediti tačnost i brzinu ali i sačuvati otpornost na razne vidove napada u realnim primenama. Zatim sledi standardizacija kako bi se svi sistemi na bazi takvih algoritama ponašali u skladu sa specifikacijama koje su prihvaćene svuda. Sve navedene mere neophodno je primeniti na postojeća i buduća rešenja post-kvantnih šifarskih sistema.

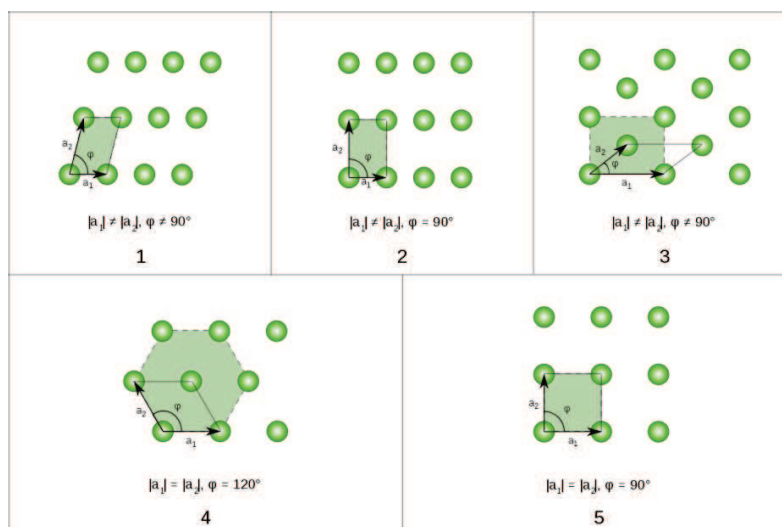
#### 6.1. Šifarski sistemi na bazi rešetke (Lattice-based Cryptography)

Prva opšta istraživanja rešetki počeli su poznati matematičari Džozefa Lui Lagranž (engl. Joseph Louis Lagrange) i Karl Fridrih Gaus (engl. Carl Friedrich Gauss), dok je istraživač Mikloš Ajtai (engl. Miklós Ajtai) 1996. godine prvi put prikazao mogućnosti primene rešetki u kriptografiji.

Rešetka  $L$  je skup tačaka u  $n$ -dimenzionalnom euklidskom prostoru  $\mathbb{R}^n$  koji pokazuje jaku periodičnost. Striktno, rešetka u  $\mathbb{R}^n$  je diskretna podgrupa prostora  $\mathbb{R}^n$  nad realnim vektorskim prostorom  $\mathbb{R}^n$ . Svaka rešetka u  $\mathbb{R}^n$  može biti generisana kao linearna kombinacija basis vektora tog prostora sa koeficijentima koji su celi brojevi. Tipična rešetka u  $\mathbb{R}^n$  može se opisati na sledeći način:

$$L = \left\{ \sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z} \right\}$$

gde je  $\{v_1, v_2, v_3, \dots, v_n\}$  basis vektorskog prostora  $\mathbb{R}^n$ . Različiti bazisi mogu generisati istu rešetku, ali je apsolutna vrednost determinante vektora  $v_i$  jedinstveno određena rešetkom  $L$  i označava se  $d(L)$ . Ako se rešetka zamisli kao delioc prostora  $\mathbb{R}^n$  u jednake polihedre (kopije  $n$ -dimenzionalnog paralelopipeda), onda je  $d(L)$  jednaka  $n$ -dimenzionalnoj zapremini jednog polihedra. Radi ilustracije sledećih 5 tipova rešetki se može definisati u euklidskoj ravni  $\mathbb{R}^2$ , sa bazisom  $(a_1, a_2)$ :



Slika 52 - Pet osnovnih tipova rešetki u Euklidskoj ravni

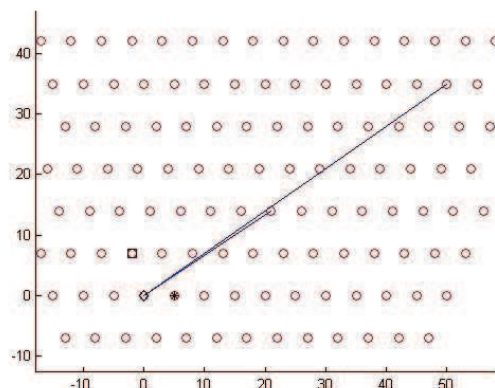
Sve rešetke u  $\mathbb{R}^2$  imaju, naravno, beskonačno mnogo elemenata, dok se u kriptografiji na bazi rešetki razmatraju rešetke nad konačnim poljem. Dva matematička problema koji se koriste kao primitive u post-kvantnim šifarskim sistemima na bazi rešetki su problem najkraćeg vektora (engl. Shortest Vector Problem - SVP) i problem najbližeg vektora (engl. Closest Vector Problem - CVP). SVP problem sastoji se iz pronalaženja najkraćeg vektora u nekoj rešetci, za dati basis rešetke. CVP problem zahteva da se, za dati basis rešetke i neki vektor  $v$  koji nije deo rešetke, pronađe najkraći vektor koji pripada toj rešetci a koji je najmanje udaljen od navedenog vektora  $v$ .

### Problem najkraćeg vektora (SVP)

Neka je basis vektorskog prostora  $V$ , i norme  $N$  (euklidska norma  $l^2$ ) dat za rešetku  $L$ . SVP problem se sastoji u pronalaženju najkraćeg ne-nula vektora u  $V$ , izmerenog normom  $N$  u rešetci  $L$ , odnosno  $\lambda(L)$ , gde je  $\lambda(L) = \min(\|v\|_N \mid v \in L, v \neq 0)$ .

Tačna verzija SVP problema je NP-teška (engl. NP-hard). Algoritam Lenstra-Lenstra-Lovaš (engl. Lenstra–Lenstra–Lovász), poznat i kao LLL algoritam za redukciju bazisa, omogućuje pronalaženje relativno kratkog vektora u polinomijalnom vremenu, ali ne rešava problem u potpunosti. Pošto za sada ne postoji efikasan algoritam koji će da reši SVP (CVP) u potpunosti u bilo kojoj izabranoj višoj dimenziji, ovi problem se uobičajno definišu kao aproksimacija početnog problema, gde faktor aproksimacije  $\gamma \geq 1$  može da bude funkcija dimenzije ili ranga rešetke. U navedenoj  $\gamma$ -aproksimaciji SVP-a, takozvanom  $SVP_\gamma$  problemu, neophodno je pronaći ne-nula vektor rešetke takav da je njegova dužina ne veća od  $\gamma \cdot \lambda(L)$ .

Kao primer uzmimo sledeću rešetku koja je generisana vektorima  $i = (50, 35)$   $j = (21, 14)$  na  $\mathbb{R}^2$ . Najkraći vektor koji nije jednak nuli je  $a = (5, 0)$ . Sledeći najkraći je  $b = (-2, 7)$ . U opštem slučaju rešetka je generisana na  $\mathbb{R}^n$ , što čini ovaj problem NP-teškim.

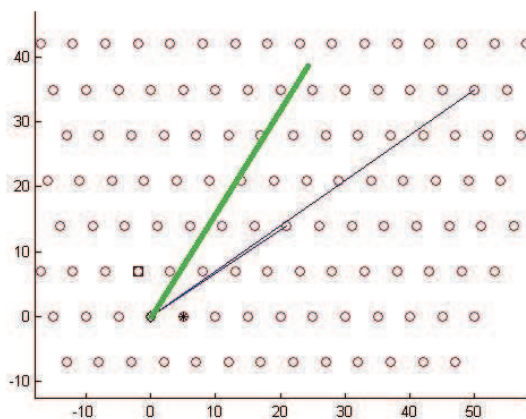


Slika 53 - Primer SVP problema na rešetki  $L$  generisanoj na  $\mathbb{R}^2$

### Problem najbližeg vektora (CVP)

U CVP je basis vektorskog prostora  $V$  i norme  $N$  (euklidska norma  $l^2$ ), dat za rešetku  $L$  kao i za vektor  $v$  tog prostora  $V$ , koji ne pripada rešetki  $L$ . Problem se sastoji u pronalaženju vektora koji pripada rešetki  $L$  koji je najbliži datom vektoru  $v$ . Kao što je pomenuto u prethodnom poglavlju u slučaju SVP, postoji takođe i  $\gamma$ -aproksimacija CVP problema, CVP  $\gamma$ , gde je neophodno pronaći vektor koji pripada rešetki na distance od najviše  $\gamma$ .

Kao primer uzmimo rešetku  $L$  koja je generisana kao u primeru SVP problema u prethodnom poglavlju, i slučajni vektor  $v$  (deblja linija) koji ne pripada rešetki  $L$ . Potrebno je pronaći vektor koji pripada rešetki  $L$ , a koji je najbliži vektoru  $v$ .



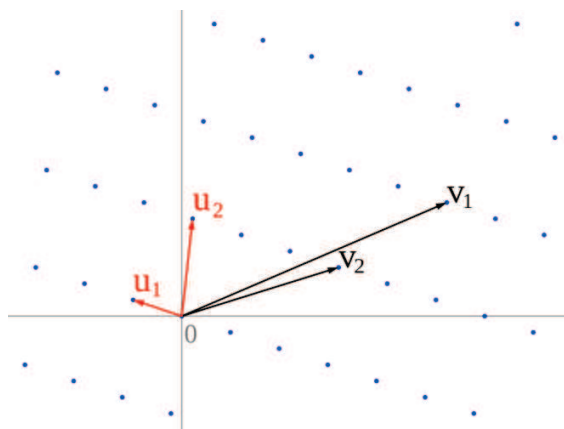
Slika 54 - Primer CVP problema na rešetki  $L$  generisanoj na  $\mathbb{R}^2$

## Rešavanje SVP i CVP primenom LLL algoritma

Za mnoge probleme u vezi rešetki se pretpostavlja ili je već dokazano da su teški u prosečnom slučaju, i zbog toga su takvi pogodni kandidati za osnove pojedinih šifarskih sistema. Nadalje, težina najgoreg slučaja određenih problema zasnovanih na rešetkama se koristi kao osnova za šifarske sisteme. Upravo ta činjenica ističe ove probleme kao potencijalne kandidate za sisteme koji su najverovatnije otporni na napade primenom kvantnog računara.

Algoritmi na bazi redukovanja bazisa rešetke imaju za cilj da se na osnovu početnog bazisa nekom transformacijom dođe do novog bazisa iste rešetke koji se sastoji iz relativno kratkih i ortogonalnih (okomitih) vektora. LLL algoritam je jedan od ranih primera efikasnih algoritama sa redukcijom bazisa u polinomijalnom vremenu. Algoritam je uz dodatna poboljšanja korišćen za razbijanje nekoliko šifarskih sistema, i tako dobio status ozbiljnog alata u kriptanalizi. Uspeh LLL algoritma na eksperimentalnim podacima je doveo do toga da se verovalo da je redukcija rešetke relativno lak zadatak u praksi. Sredinom devedesetih godina prošlog veka došlo se do novih rezultata koji su potvrdili težinu problema sa rešetkama, opovrgavajući tvrdnje o relativnoj lakoći rešavanja navedenih problema korišćenjem algoritama na bazi redukcije rešetke. U svom radu iz 1996. godine, Mikloš Ajtai je dokazao da je SVP problem NP-težak i otkrio određene veze između kompleksnosti određenih problema sa rešetkama u najgorem i prosečnom slučaju. Na osnovu prikazanih rezultata Ajtai i Dwork (engl. Dwork) su predstavili šifarski sistem sa javnim ključem čija sigurnost je mogla biti dokazana primenom najgoreg slučaja određene verzije SVP problema, što predstavlja prvi rezultat gde je korištena težina najgoreg slučaja problema kako bi se obezbedila sigurnost sistema.

LLL algoritam su 1982. godine pronašli Ardžen Lenstra, Henrik Lenstra i Laslo Lovaš (engl. Arjen Lenstra, Hendrik Lenstra, László Lovász). Ako je dat bazis  $V = \{v_1, v_2, v_3, \dots, v_d\}$  vektorskog prostora  $V$ , sa  $n$ -dimenzionalnim celobrojnim koordinatama, za rešetku  $L \subset \mathbb{R}^n$ , gde je  $d \leq n$ , LLL algoritam obezbeđuje LLL-reducirani (kraći, gotovo ortogonalan) bazis rešetke u vremenu  $O(d^5 n \log^3 V)$ , gde je  $V$  najveća vrednost  $v_i$  u smislu euklidske norme.



Slika 55 - Prvobitni bazis  $(v_1, v_2)$  i redukovani bazis  $(u_1, u_2)$

LLL algoritam postiže i više od pronalaženja relativno kratkog vektora u rešetci, on nalazio takozvani redukovani basis za ulaznu rešetku, odnosno celi basis za relativno kratke vektore koji pripadaju rešetci. Ubrzo nakon otkrića LLL algoritma Babaji (engl. Babai) je dokazao da redukovano basis može biti korišćen za efikasno rešavanje CVP problema, uz slične aproksimativne faktore.

Za obe aproksimacije problema, SVP i CVP, se zna da su NP-teške ako je faktor  $\gamma = 1$  ili čak aproksimacije za male vrednosti  $\gamma$ , odnosno za konstantno  $\gamma$  koje ne zavise od dimenzija prostora  $V$ . Ovim se implicira da verovatno ne postoji efikasan algoritam za rešavanje ovih problema u slučaju bilo kojoj slučajno izabrane dimenzije rešetke  $N$ . Za neku fiksnu dimenziju  $n$  oba SVP i CVP mogu se potpuno rešiti problem korišćenjem tzv. Kananovog algoritma, tzv. HKZ redukcija bazisa algoritma (engl. Kannan), ali je zavisnost vremena izvršenja algoritma za dimenziju vektorskog prostora  $n$  jednaka  $n^{\frac{n}{2e} + o(N)}$  što je neprihvatljivo za veće dimenzije. Ako se zahteva tačno rešenje za SVP, ili čak aproksimacija, vreme izvršavanja najboljeg poznatog algoritma je  $2^{O(n)}$ . Zahtevi resursa takođe rastu eksponencijalno što ga čini suštinski nepraktičnim. Neki drugi algoritmi koji rešavaju SVP zauzimaju resurse polinomijalno, ali s druge strane vreme izvršavanja raste sa  $2^{O(n \log n)}$

U zadnje vreme metod redukcije bazisa rešetke je veoma često korišćen u rešavanju mnogih problema u kriptanalizi i teoriji kodiranja (engl. coding theory), uključujući i kompromitovanje nekoliko varijanti RSA i DSA, nalaženja malih rešenja modularnih jednačina, i sličnih problema. Poslednja klasa problema je kreiranje šifarskih sistema (heš funkcija otpornih na kolizije, šema sa javnim ključem i drugih primena) na osnovu očigledne težine rešavanja SVP problema sa malim faktorima aproksimacije  $\gamma$ . Jedna bitna karakteristika navedenih problema na bazi rešetki je da je moguće dokazati da su oni teški za rešavanje u tipičnom slučaju, do čega se došlo na osnovu pretpostavke o težini rešavanja tog problema u najgorem slučaju.

### **Kvantno računarstvo i problemi rešetke**

Kao što je već pomenuto, problemi rešetki su u tipičnom slučaju teški. Najbolji algoritmi za rešavanje ovih problema izvršavaju se korektno u eksponencionalnom vremenu, ili daju aproksimativne rezultate, u polinomijalnom vremenu, koji nisu primenjivi. Shodno ovim zaključcima postavlja se pitanje da li su problemi sa rešetkama rešivi primenom kvantnih računara, odnosno da li su navedeni problemi mogući kandidati za primenu u post-kvantnim šifarskim sistemima?

U ovom trenutku odgovor na ovo pitanje je „verovatno da“ jer do sada nisu pronađeni kvantni algoritmi koji bi rešavali probleme iz ove klase u polinomijalnom vremenu i resursima. Od otkrića Šorovog algoritma 1994. godine naučnici pokušavaju da pronađu rešenja, ali ovi pokušaji do danas ostaju bez rezultata. Osnovni problem je da tehnika pronalaženja periodičnosti, koja se koristi u Šorovom algoritmu, izgleda kao da ne može da se primeni na probleme sa rešetkom. Na osnovu ove pretpostavke smatra se da su problemi sa rešetkama kandidati za primitive post-kvantnih šifarskih sistema.

### 6.1.1. NTRU šifarski sistem

NTRU šifarski sistem je patentiran open-source sistem sa javnim ključem koji koristi kriptografiju na bazi rešetke. Akronim NTRU je nastao od naziva algoritma "N<sup>th</sup> Degree Truncated Polynomial Ring Units". Sastoji se iz dva algoritma, NTRUEncrypt koji se koristi za šifrovanje, i NTRUSign koji se koristi za digitalni potpis. Postoje i komercijalna rešenja razvijena od strane privatnih kompanija kao što su Security Innovation, koji nude softverske biblioteke i alat u C/C++ i Java programskim jezicima za implementaciju SSL/TLS sa NTRU, a naročito rešenja za mobilne uređaje.

Prvu verziju ovog šifarskog sistema, pod nazivom NTRU, razvili su 1996. godine matematičari J. Hofštajn, J. Pajper i Silverman. (engl. J. Hoffstein, J. Pipher, Silverman). Iste godine oni su u saradnji sa D. Limanom (engl. D. Lieman) ustanovili kompaniju NTRU Cryptosystems Inc. i obezbedili patent za ovaj šifarski sistem. 2009. godine ova kompanija je prodana kompaniji Security Innovations.

Uz jednak nivo krypto-zaštite NTRU izvršava složene operacije šifrovanja i dešifrovanja značajno brže nego RSA. Kod RSA obe operacije jednako su zahtevne. Kod NTRU se dešifrovanje znatno brže izvršava od šifrovanja, što dolazi posebno do izražaja kako raste dužina poruke. Dokazano je da vreme izvršena ovih operacija kod NTRU raste sa  $O(n \log n)$  dok je za RSA to  $O(n^3)$ , u odnosu na poruku. Ovo je očigledna prednost NTRU, uz isti nivo zaštite, te je ovaj sistem izuzetno pogodan za aplikacije na mobilnim uređajima i pametnim karticama (engl. smart cards).

Navedeni šifarski sistem se u suštini zasniva na težini faktorisanja određenih polinoma u prstenu na dva polinoma sa veoma malim koeficijentima. Napad na ovakav sistem je usko povezan, ali ne i ekvivalentno, sa algoritamskim problemom redukcije rešetke, odnosno već pomenutog rešavanja problema najbližeg vektora (CVP) nad izabranim rešetkama. Pametan izbor parametara sistema je ključan u tom slučaju za onemogućavanje određenih napada. Kod NTRU i šifrovanje i dešifrovanje koristi jednostavno množenje polinoma pa se zbog toga obe operacije izvršavaju znatno brže nego kod drugih šifarskih sistema kao što su RSA, EEC, i El Gamal.

Kao što je ranije pomenuto smatra se da je NTRU otporan na napade korišćenjem kvantnog računarstva, za razliku od poznatih RSA i ECC sistema. Smatra se da je NTRU najpraktičniji šifarski sistem iz navedene klase. Standardom IEEE 1363.1 iz 2008. godine definisani su šifarski sistem sa javnim ključem, konkretno NTRUEncrypt. Standard X9.98 takođe standardizuje ovaj šifarski sistem, kao deo grupe standarda X za industriju finansijskih usluga.

#### NTRUEncrypt

NTRUEncrypt je NTRU algoritam za šifrovanje koji se zasniva na problemu najkraćeg vektora (SVP) u rešetci. Operacije su zasnovane na objektima u skraćenom polinomijalnom prstenu

$R = \frac{\mathbb{Z}[X]}{(X^N-1)}$  sa konvolutivnim množenjem a svi polinomi u prstenu imaju celobrojne koeficijente stepena do  $N - 1$ .

$$a = a_0 + a_1X + a_2X^2 + \dots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}$$

NTRU je u stvari parametrizovana porodica šifarskih sistema, a svaki sistem je definisan sa tri celobrojna parametra  $(N, p, q)$  koji predstavljaju maksimalni stepen  $N - 1$  za sve polinome u skraćenom prstenu  $R$ , a zatim mali i veliki modulus  $p, q$  respektivno, gde se podrazumeva da je  $N$  prost broj,  $q$  je uvek veće od  $p$ ,  $q$  i  $p$  su uzajamno prosti brojevi ( $\gcd(p, q) = 1$ ), a četiri skupa polinoma  $L_f, L_g, L_m, L_r$  su: polinomijalni deo privatnog ključa, polinomi za generisanje javnog ključa, poruka i polinomi za zaklanjanje (sakrivanje) poruke, respektivno.

## Generisanje ključeva

Slanje tajne poruke od Alise do Boba zahteva generisanje privatnog i javnog ključa. Javni ključ naravno poseduju i Alisa i Bob dok je privatni ključ poznat samo Bobu. Da bi se generisao privatni-javni par ključeva, potrebna su dva polinoma  $f$  i  $g$  sa koeficijentima mnogo manjim od  $q$ , najvećeg stepena  $N - 1$ , is a koeficijentima iz skupa  $\{-1, 0, 1\}$ . Polinom  $f \in L_f$  mora da zadovolji dodatni zahtev da postoje inverzni moduo  $q$  i inverzni moduo  $p$ , što znači da je  $f \cdot f_p = 1 \pmod{p}$  i  $f \cdot f_q = 1 \pmod{q}$ . Ako dati polinom  $f$  nije invertibilan potrebno je izabrati drugi polinom koji jeste. Oba polinoma  $f$  i  $f_p$  su Bobovi privatni ključevi. Javni ključ  $h$  je generisan sledećim izrazom:

$$h = p \cdot f_q \cdot g \pmod{q}$$

Kao realni primer procesa generisanja ključeva neka su izabrani sistemski parametri  $(N, p, q)$  sledeći:  $N = 11$ ,  $p = 3$ ,  $q = 32$ . Navedeni sistemski parametri neka su uvek svima poznati. Polinomi  $f$  i  $g$  su u ovom slučaju najviše reda 10, i oni mogu biti izabrani potpuno slučajno. U ovom primeru to su:

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$$

$$g = -1 + x^2 + x^3 + x^5 - x^8 - x^{10}$$

Korišćenjem Euklidovog algoritma izračunate su inverzne vrednosti  $f \pmod{p}$  i  $f \pmod{q}$ :

$$f_p = 1 + 2x + 12x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9 \pmod{3}$$

$$f_q = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10} \pmod{32}$$

Na osnovu dobijenog inverza polinoma  $f_q$  i drugog polinoma  $g$  dobije se javni ključ  $h$ :

$$h = p \cdot f_q \cdot g \pmod{32} = 8 + 25x + 22x^2 + \dots + 19x^9 + 16x^{10} \pmod{32}$$

## Šifrovanje

Alisa šalje tajnu poruku Bobu u obliku polinoma  $m$  sa koeficijentima  $\{-1,0,1\}$ . Ovaj polinom može da se reprezentuje u binarnom ili ternarnom obliku. Potom Alisa bira slučajan polinom  $r$  sa malim koeficijentima, koji ne moraju biti ograničeni na skup  $\{-1,0,1\}$ , koji se koristi da poruku učini nerazumljivom. Uz pomoć Bobovog javnog ključa  $h$ , izračunata je poruka  $e$ .

$$e = r \cdot h + m \pmod{q}$$

Neka je tajna poruka koju Alisa šalje u obliku sledećeg polinoma  $m$ .

$$m = -1 + x^3 - x^4 + x^5 - x^8 + x^9 + x^{10}$$

Neka je polinom  $r$  koji će da učini poruku nečitljivom.

$$r = -1 + x^2 + x^3 + x^4 - x^5 - x^7$$

Šifrovana poruka  $e$  koju Alisa šalje Bobu je u tom slučaju:

$$\begin{aligned} e &= r \cdot h + m \pmod{32} = \\ &= 14 + 11x + 26x^2 + 24x^3 + 14x^4 + 16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10} \pmod{32} \end{aligned}$$

## Dešifrovanje

Na osnovu polinoma  $r$  može se izračunati poruka  $m$ , pa prema tome Alisa mora da održava polinom  $r$  tajnim. Uz sve poznate parametre Bob poseduje i svoj privatni ključ. Da bi dešifrovao poruku  $m$ , on prvo množi šifrovanu poruku  $e$  i deo svog privatnog ključa  $f$ .

$$a = f \cdot e \pmod{q}$$

Na osnovu primera dobija se da je

$$\begin{aligned} a &= f \cdot e \pmod{32} = \\ &= 3 - 7x - 10x^2 - 11x^3 + 10x^4 + 7x^5 + 6x^6 + 7x^7 + 5x^8 - 3x^9 - 7x^{10} \pmod{32} \end{aligned}$$

Sledeći korak podrazumeva izračunavanje  $a \pmod{p}$ .

$$b = a \pmod{p} = f \cdot m \pmod{p}, \text{ zato što je } p \cdot r \cdot g \pmod{p} = 0.$$

Na osnovu primera dobija se

$$b = a \pmod{3} = -x - x^2 + x^3 + x^4 + x^5 + x^7 - x^8 - x^{10} \pmod{3}$$

Znajući vrednost  $b$ , Bob može iskoristiti drugi deo svog privatnog ključa  $f_p$  kako bi množenjem  $b$  i  $f_p$  dobio poruku.

$$c = f_p \cdot b = f_p \cdot f \cdot m \pmod{p}$$

,što znači da je  $c = m \pmod{p}$  zbog uslova  $f_p \cdot f = 1 \pmod{p}$  za  $f_p$ .

Na osnovu primera dobija se

$$\begin{aligned} c &= m \pmod{3} = \\ &= -1 + x^3 - x^4 + x^5 - x^8 + x^9 + x^{10} \end{aligned}$$

, što je zaista poruka koju je Alisa poslala Bobu u gornjem primeru.

### Sigurnost

Od pojavljivanja NTRU šifarskog sistema primećeno je nekoliko značajnih napada. Većina napada se fokusira na nalaženje tajnog ključa  $f$  umesto dešifrovanja poruke. Ako je poznato da  $f$  ima veoma mali broj ne-nula koeficijenata, napadač može da primeni napad grubom silom (engl. brute force) tako što će pokušati da proba sve moguće vrednosti  $f$ . Moguće je primeniti napad čovek-u-sredini koji je napredniji od napada grubom silom, jer je moguće da skрати vreme pretraživanja proporcionalno kvadratnom korenu. Ovaj napad se zasniva na činjenici da je  $f \cdot h = g \pmod{p}$ .

Najpoznatiji je napad koji se zasniva na redukciji rešetke, ujedno i najpraktičniji način da se kompromituje NTRUEncrypt sistem, i u tom smislu je uporediv sa faktorizacijom kod RSA: Najčešće korišćeni algoritam za redukciju rešetke je prethodno opisani Lenstra-lenstra-Lovaš (LLL) algoritam. Rezultat uspešnog napada redukcijom rešetke je potpun pad sistema jer se kompromituje privatni ključ. Napad redukcijom rešetke je teži ukoliko je dimenzija rešetke veća i najkraći vektor duži, pa je ova vrsta napada otežana ako se izaberu dovoljno sigurni početni parametri. U tom smislu se u većini komercijalnih primena parametru  $N$  zadaje vrednost 251, a polinomi  $f$  i  $g$  imaju po 72 ne-nula koeficijenta. Na osnovu relativno skoriš istraživanja u sledećoj tabeli prikazane su predložene vrednosti  $N, p, q$  parametara u zavisnosti od željenog (relativnog) nivoa zaštite.

| nivo zaštite | $N$ | $q$ | $p$ |
|--------------|-----|-----|-----|
| umereni      | 167 | 128 | 3   |
| standardni   | 251 | 128 | 3   |
| visoki       | 347 | 128 | 3   |
| najviši      | 503 | 256 | 3   |

Tabela 7 - Preporučene vrednosti parametara za NTRUEncrypt

### NTRUSign

NTRUSign, poznat kao NTRU algoritam za potpisivanje, je zasnovan na Goldrajh-Goldvasser-Halevi (engl. Goldreich–Goldwasser–Halevi), odnosno GGH šemi za digitalno potpisivanje. Prvi put je predstavljen 2001. godine na konferenciji Asiacrypt, dok je 2003. godine objavljen na RSA

konferenciji, gde su predloženi parametri algoritma koji odgovaraju 80-bitnoj zaštiti. 2005. godine predloženi su parametri za 112, 128, do 256 bita ekvivalentne zaštite, a dat je i opis algoritma za izvođenje parametara za bilo koji željeni nivo zaštite.

NTRUSign podrazumeva mapiranje poruke u slučajno izabranu tačku  $2N$ -dimenzionalnog prostora, gde je  $N$  jedan od parametara algoritma, i rešavanje problema najbližeg vektora u rešetki (CVP) koja je usko povezana sa NTRUEncrypt rešetkom. Ova rešetka ima osobinu da se njen privatni  $2N$ -dimenzionalni bazis može opisati sa 2 vektora, oba sa  $N$  koeficijenta, dok se javni bazis može opisati sa jednim  $N$ -dimenzionalnim vektorom. To omogućuje da se javni ključ reprezentuje u  $O(N)$  prostoru, za razliku od nekih drugih šema za potpis na bazi rešetke čiji javni ključ se definiše u  $O(N^2)$  prostoru. Kod ove šeme operacije sa privatnim ključem uzimaju vreme u zavisnosti od  $O(N^2)$ , za razliku od  $O(N^3)$  kod ECC (engl. elliptic curve cryptography) i RSA. NTRUSign se zbog ovoga smatra bržim kod nižih nivoa zaštite, dok je kod većih nivoa zaštite značajno brži od pomenutih šema. NTRUSign je trenutno u procesu standardizacije u okviru aktivnosti radne grupe IEEE P1363.

## Sigurnost

Kompanija NTRU Cryptosystems je 2003. godine prvi put prikazala efikasnu šemu digitalnog potpisa pod nazivom NTRUSign. NTRUSign nije zero-knowledge šema za digitalni potpis i 2006. godine je dokazano da se iz celog transkripta potpisa može izvući privatni ključ u nekim slučajevima nakon samo 400 potpisa. Tekuće rešenje da se izbegne navedena slabost sistema je da se ubace perturbacije kako bi se povećala minimalna veličina transkripta koja omogućuje nalaženje ključa. NTRU tvrdi da bi u tom slučaju bilo potrebno najmanje  $2^{30}$  potpisa pre nego što bi se stvorile šanse za koristan napad na ovu šemu.

### 6.1.2. GGH šifarski sistem

Goldrajh-Goldvasser-Halevi (engl. Goldreich–Goldwasser–Halevi) (GGH) je asimetrični šifarski sistem na bazi rešetke koji je prvi put prikazan 1997. godine, koji takođe implementira i šemu digitalnog potpisa. GGH kao i drugi sistemi na bazi rešetke koristi CVP problem, odnosno jednosmernu tajnu funkciju koja se oslanja na težinu problema redukcije rešetke. Osnovna ideja je da je za bilo koji bazis rešetke jednostavno generisati vektor koji je blizu neke tačke koja pripada rešetki, na primer uzimanjem neke tačke u rešetki i dodavanjem nekog malog vektora greške. S druge strane, da bi iz ovog novog vektora dobili prvobitni vektor koji pripada rešetki potreban je poseban bazis.

Privatni ključ u GGH je bazis  $B$  rešetke  $L$  koji poseduje "povoljna" svojstva – kratki, gotovo ortogonalni vektori, i unimodularnu matricu  $U$ . To je po definiciji kvadratna matrica sa celobrojnim elementima i determinantom jednakom  $+1$  ili  $-1$ . Javni ključ je drugi bazis rešetke  $L$  oblika  $B' = UB$ . Za neku poruku  $M$ , prostor poruke se sastoji od vektora  $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$  u intervalu  $-M < \lambda_i < M$ .

## Šifrovanje

Ako je poruka  $M = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ , greška  $e$ , a javni ključ  $B'$ , neophodno je izračunati

$$v = \sum \lambda_i b'_i$$

U matricnoj notaciji gornji izraz jednak je  $v = m \cdot B'$ . Pošto se poruka  $m$  sastoji od celobrojnih vrednosti, a  $b'$  je tačka u rešetci  $L$ , izvesno je da  $v$  takođe pripada rešetci  $L$ . Šifrovana poruka je u tom slučaju  $c = v + e = m \cdot B' + e$ .

## Dešifrovanje

Dešifrovanje se svodi na izračunavanje sledećeg izraza:

$$c \cdot B^{-1} = (m \cdot B' + e) \cdot B^{-1} = m \cdot U \cdot B \cdot B^{-1} + e \cdot B^{-1} = m \cdot U + e \cdot B^{-1}$$

Babai tehnika zaokruživanja u rešetci, koja se sastoji od jednostavnog zaokruživanja koordinata na najbližu celobrojnu vrednost ka redukovanoj bazi, može da se iskoristi da se ukloni faktor  $e \cdot B^{-1}$  ako je dovoljno mali. Na kraju da bi se dobilo tekst poruke potreban je poslednji korak:

$$m = m \cdot U \cdot U^{-1}$$

## Sigurnost

Poznati istraživač u ovoj oblasti, Fong Njong (engl. Phong Q. Nguyen), je 1999. godine na Crypto konferenciji dokazao da GGH sistem ima nedostatak tako da svaka šifrovana poruka odaje informaciju o tekstu, kao i da se problem dešifrovanja može pretvoriti u poseban CVP problem.

## GGH šema za digitalni potpis

GGH šema digitalnog potpisa je prvi put objavljena 1997. godine, i zasniva se na rešavanju CVP problema na rešetci. Potpisnik demonstrira poznavanje "dobrog" bazisa na rešetci korišćenjem tog bazisa za rešavanje CVP-a za tačku koja predstavlja poruku. Verifikator koristi loš bazis na istoj rešetci da bi dokazao da je potpis koji se razmatra u stvari tačka u rešetci, i da je dovoljno blizu tački rešetke koja predstavlja poruku. GGH potpisi predstavljaju osnovu NTRUSign algoritma.

## 6.2. Šifarski sistemi na bazi kodova (Code-based Cryptosystems)

U ovom poglavlju se razmatraju aspekti šifarskih sistema na bazi kodova. Ovi šifarski sistemi koriste neke od kodova za korigovanje grešaka (engl. error correcting code) kao algoritamske primitive.

### 6.2.1. Mekelis šifarski sistem (McEliece)

Mekelis šifarski sistem je 1978. godine predstavio Robert Mekelis (Robert McEliece). To je bio prvi sistem koji koristi randomizaciju u procesu šifrovanja. Algoritam nikada nije bio široko prihvaćen u kriptografskim krugovima ali je to ipak izvestan kandidat za post-kvantnu kriptografiju usled dokazane otpornosti na napade primenom Šorovog algoritma. Algoritam se zasniva na težini dekodiranja generalnog (slučajnog) linearnog koda, problema koji je dokazano NP-težak. To je stari problem u teoriji kodiranja za koji isključivo postoje rešenja sa eksponencijalnom vremenskom zavisnošću.

Takozvano sindrom dekodiranje linearnih kodova je NP-kompletni problem ako broj grešaka nije ograničen, ali postoje i klase linearnih kodova sa veoma brzim algoritmima za dekodiranje. Osnovna ideja Mekelis sistema je da se uzme jedan od linearnih kodova i da se maskira tako da je potencijalni napadač prinuđen da koristi sindrom dekodiranje, dok primalac koji poznaje sistem zna kako da ukloni maskiranje i primeni brzi algoritam za dekodiranje. Mekelis je u tu svrhu predložio korišćenje binarnih Goppa kodova (Goppa), linearnih kodova sa brzim algoritmom za dekodiranje. U suštini tajna funkcija primenjena u Mekelis sistemu svodi se na poznavanje efikasnih algoritama za korigovanje greške za izabranu klasu kodova zajedno sa permutacijom.

#### Linearni kodovi

U teoriji kodiranja linearni kod je kod za korigovanje greške (engl. error-correcting code) za koji je bilo koja linearna kombinacija kodnih reči takođe kodna reč. Linearni kodovi se tradicionalno dele na dve klase, blok kodovi i konvolucionni kodovi. Linearni kodovi omogućuju algoritme za kodiranje i dekodiranje koji su relativno efikasni. Linearni kodovi se koriste u korekciji grešaka unapred (engl. forward error correction FEC) i primenjuju se kod slanja simbola (bitova) kroz bilo koji praktični komunikacioni kanal. Time je omogućena, u određenoj meri, detekcija i ispravljanje grešaka koje se dešavaju tokom transmisije informacija kroz takav kanal. Kodne reči u linearnom blok kodu su blokovi simbola (tj. bitova) koje su enkodirane sa više simbola nego što je potrebno za prvobitnu informaciju.

Poznat je Hamingov (Hamming) kod koji enkodira 4 bita poruke sa kodnom reči od 7 bitova. Dve posebne kodne reči ovog koda se razlikuju u najmanje 3 bita. Hamingov kod se sastoji od 16 kodnih reči. Posledica ovog specifičnog kodiranja informacije je da je na mestu prijema informacije moguće detektovati grešku ako su primljena maksimalno 2 pogrešna bita u kodnoj reči, dok je najviše jedan pogrešan bit moguće i korigovati. Neki od poznatih linearnih kodova su i Reed-Mueller i Walsh-Hadamard kao poseban slučaj prethodnog koda.

#### Sindrom dekodiranje

Sindrom dekodiranje je veoma efikasan sistem dekodiranja linearnog koda sa kanala sa šumom, odnosno kanala na kome se javljaju greške tokom prenosa informacija. U suštini sindrom dekodiranje je takozvano dekodiranje sa minimalnom distancom koje koristi redukovanu referentnu

tabelu. (engl. lookup table). Važno je istaći da linearnost koda dozvoljava redukovanje referentne tabele. Najjednostavniji primer sindrom dekodiranja je već pomenuti Hamingov kod.

### Binarni Gopa kodovi

Binarni Gopa kod je kod za korekciju grešaka koji pripada klasi opštih Gopa kodova, prvobitno opisanih u naučnom radu ruskog matematičara Valerija Denisoviča Gope (Valerii Denisovich Goppa), čija binarna struktura daje nekoliko matematičkih prednosti u odnosu na nebinarne varijante, kao i praktične prednosti u primenama u računarstvu i telekomunikacijama. Binarni Gopa kodovi imaju interesantne osobine koje su prijemčive za upotrebu u kriptografiji u šifarskim sistemima sličnim Mekelisu i srodnim sistemima. Dekodiranje binarnog Gopa koda se tradicionalno obavlja Patersonovim algoritmom, koji je jednostavan za implementaciju i omogućuje dobre mogućnosti za korigovanje greške.

### Šifrovanje

Neka je  $C$   $(n,k)$ -linearni kod sa brzim algoritmom za dekodiranje koji može da koriguje najviše  $t$  grešaka. Neka je  $G$  generator matrica za  $C$ . Da bi se obezbedilo maskiranje neka je  $S$  invertibilna matrica dimenzija  $k \times k$ , i neka je  $P$  slučajna matrica permutacije (koja ima isključivo vrednost "1" u svakom redu i koloni), dimenzija  $n \times n$ . Sledeća matrica:

$$G' = SG P$$

je javna dok su  $S$ ,  $G$  i  $P$  tajne koje zna samo Bob. Ako Alisa želi da pošalje poruku Bobu, ona će da podeli poruku u binarne vektore dužine  $k$ . Ako je  $x$  jedan takav blok, ona će na slučajan način konstruisati binarni  $n$ -vektor težine  $t$  (tj. Alisa će da na slučajan način podeli  $t$  1-inica u nula-vektor dužine  $n$ ), neka se taj vektor zove  $e$ , a zatim će Bobu poslati sledeći vektor:

$$y = xG' + e$$

### Dešifrovanje

Napadač će presresti ovu poruku i pokušati da pronađe najbližu kodnu reč sa  $y$ , koda generisanog sa  $G'$ . To implicira izračunavanje sindroma od  $y$  i poređenje sa sindromima svih vektora greške težine  $t$ . Pošto postoji  $\binom{n}{k}$  takvih vektora greške, za dobro izabrane vrednosti  $n$  i  $k$ , ovo izračunavanje je nepraktično odnosno nemoguće u realnom vremenu. a druge strane Bob bi izračunao sledeće:

$$yP^{-1} = (xG' + e)P^{-1} = xSG + eP^{-1} = xSG + e'$$

Gde je  $e'$  vektor težine  $t$ . ( $P^{-1}$  je takođe matrica permutacije kao i  $P$ ). Bob primenjuje brzi algoritam za dekodiranje da ukloni vektor greške  $e'$  i dobije kodnu reč  $(xS)G$ . Vektor  $x$  može da se dobije množenjem izraza sa desne strane matricom  $G^{-1}$ , a zatim i matricom  $S^{-1}$ , što je prvobitni blok poruke koju je poslala Alisa.

Za primer Mekelis Gopa koda, sa početnim parametrima  $n = 1024$  and  $t = 50$ , napadač mora da proveriti preko  $10^{80}$  sindroma što je suština algoritma.

### Primer

Kao primer uzmimo Hamingov kod koji može da koriguje jedan bit u kodnoj reči. Generator matrica  $G$  može da bude sledeća.

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

Bob bira matricu za maskiranje  $S$ .

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

Izabrana matrica permutacije  $P$  neka je definisana na sledeći način.

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

Bob izračunava javnu generator matricu  $G'$  koja je vidljiva svima.

$$G' = SG = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Ako Alisa želi Bobu da pošalje poruku  $x = |1\ 1\ 0\ 1|$ , ona prvo kreira vektor greške težine 1, npr.  $e = |0\ 0\ 0\ 0\ 1\ 0\ 0|$ , a zatim izračuna sledeći izraz i šalje Bobu:

$$y = xG' + e = |0\ 1\ 1\ 0\ 0\ 1\ 0| + |0\ 0\ 0\ 0\ 1\ 0\ 0| = |0\ 1\ 1\ 0\ 1\ 1\ 0|$$

Bob prima  $y$  i izračuna  $y' = yP^{-1}$ :

$$P^{-1} = \begin{vmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{vmatrix}$$

Tako je dobijena vrednost  $y' = |1\ 0\ 0\ 0\ 1\ 1\ 1|$ . Nadalje Bob dekodira  $y'$  koristeći brzi algoritam za dekodiranje, u ovom primeru je to Haming dekodiranje. Sindrom od  $y' = |1\ 1\ 1\ 0|^T$ , tako da se greška pokazuje u poziciji 7. (detalji zaobiđeni). Bob sad ima kodnu reč  $y'' = |1\ 0\ 0\ 0\ 1\ 1\ 0|$ . Zbog dobrog izbora generator matrice  $G$ , (množenje odgovarajućom inverznom matricom) lako se izračuna da je  $xS = |1\ 0\ 0\ 0|$ , i sada je moguće dobiti  $x$  prostim množenjem ovog izraza inverznom matricom  $S^{-1}$ .

$$S^{-1} = \begin{vmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{vmatrix}$$

Dobijena vrednost bloka  $x = |1\ 0\ 0\ 0|S^{-1} = |1\ 1\ 0\ 1|$ , kao što je predviđeno u teoretskom delu.

### Nedostatci

Postoje tri osnovna problema u vezi praktične primene Mekelis sistema. Najbitniji problem je veličina ključeva koji su u suštini velike matrice. Korišćenjem Gopa koda sa parametrima koji se predlažu, javni ključ ( $G'$ ) bi se sastojao od  $2^{19}$  bita (512 Kb). To je jedan od razloga zašto je ovaj algoritam retko korišten u praksi. Sledeći izazov je veličina šifrovane poruke koja je mnogo duža nego sam tekst. Treći razlog je što se dugo vremena smatralo da Mekelis ne može da se koristiti za potpisivanje, što je ograničavalo njegovu praktičnu korisnost. Na kraju je otkriveno da je funkcija potpisivanja moguća primenom Niderajterove šeme (engl. Niederreiter), što je u suštini varijacija Mekelisa.

### Sigurnost

Mekelis sistem sa Gopa kodovima do danas nije kompromitovan. Najefektivniji poznati napad koristi algoritme za dekodiranje na osnovu skupa informacija, za koji postoji odbrana. Mekelis šifarski sistem poseduje određene prednosti u odnosu na RSA, konkretnije brže šifrovanje i dešifrovanje, a dokazano je da sa povećanjem ključa sigurnost sistema se uvećava značajno brže nego kod Mekelis sistema u poređenju sa RSA. Jedna primena Mekelis sistema bila je kod Entropy peer-to-peer platforme za sigurno čuvanje i razmenu podataka, koja je prestala sa radom sredinom 2004. godine usled otvorenih sumnji u sigurnost sistema.

### 6.2.2. Niderajter šifarski sistem (Niederreiter)

Niderajter šifarski sistem je varijacija Mekelis sistema koju je 1986. godine predložio Harald Niderajter (Harald Niederreiter). Oba algoritma su ekvivalentnog nivoa sigurnosti a napadač koji je u stanju da kompromituje jedan sistem u stanju je da kompromituje i drugi. Kod Niderajtera sindrom je šifrovana poruka dok je tekst sadržan u grešci. Šifrovanje poruke kod Niderajtera je blizu deset puta brža nego kod Mekelisa, a za razliku od Mekelisa sistem podržava digitalno potpisivanje.

#### Generisanje ključeva

Alisa bira binarni  $(n, k)$ -linearni Gopa kod  $G$  koji može da ispravi najviše do  $t$  grešaka a poseduje efikasan algoritam za dekodiranje. Alisa generiše  $(n - k) \times n$  matricu  $H$  za proveru kodnih reči (engl. parity check matrix) koja odgovara kodu  $G$ . Alisa nadalje bira slučajnu nesusingularu matricu  $S$  dimenzije  $(n - k) \times (n - k)$  i uzima neku matricu permutacije  $P$ , dimenzije  $n \times n$ . Ona zatim izračunava  $H^{pub} = SHP$ , matricu dimenzije  $(n - k) \times n$ . Konačno, Alisin javni ključ je  $(H^{pub}, t)$ , dok je privatni ključ  $(S, H, P)$ . Važno je istaći da su preporučene vrednosti korišćenih parametara sledeće:  $n = 1024, t = 38, k = 644$ .

#### Šifrovanje

Ako Bob želi da pošalje poruku  $m$  Alisi on koristi prethodno generisani javni ključ da bi izračunao  $c = H^{pub} m^T$ , i to je šifrovana poruka.

#### Dešifrovanje

Kada Alisa primi Bobovu poruku  $c = H^{pub} m^T$ , ona izračuna  $S^{-1}c = HPm^T$ , i primeni sindrom dekodiranje za kod  $G$  kako bi došla do  $Pm^T$ . Na kraju je potrebno da izračuna  $m^T = P^{-1}Pm^T$  kako bi došla do prvobitne poruke  $m$ .

### 6.3. Drugi post-kvantni sistemi

#### 6.3.1. Merkle šema za digitalni potpis

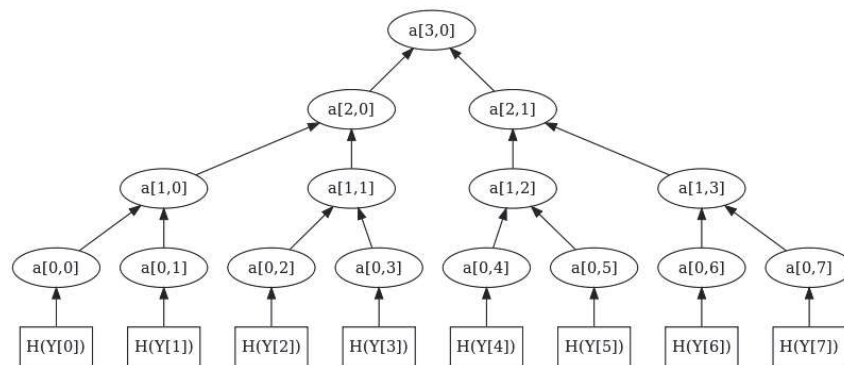
Merkle šema za potpis koristi Lamportovu šemu za jednokratni potpis i heš drvo (engl. hash tree) koja se ponekada zovu i Merkleovo drvo. Merkle šemu je razvio Ralph Merkle tokom kasnih 70-ih godina, i ona predstavlja jednu od alternativnih šemu u odnosu na DSA ili RSA šeme za potpis. Merkle šema je interesantna u kontekstu post-kvantum kriptografije jer se smatra da je ona otporna na napade primenom Šorovog algoritma zbog toga što zavisi samo od postojanja sigurnih heš funkcija, npr. SHA-1/2. Time se implicira da je ova šema veoma prilagodljiva i otporna na napade primenom kvantnog računara.

## Generisanje ključeva

Šema može biti korištena za potpisivanje ograničenog broja poruka sa jednim javnim ključem  $P$ . Broj mogućih poruka mora biti eksponent od 2, tako da je broj poruka koje mogu biti potpisane tim ključem  $N = 2^n$ . Prvi korak u generisanju javnog ključa  $P$  je generisanje skupa javnih ključeva  $X_i$  i skupa privatnih ključeva  $Y_i$  koji odgovaraju  $2^n$  jednokratnih potpisa primenom Lampartove šeme. Potom se za svaki javni ključ  $X_i$ , gde je  $1 \leq i \leq 2^n$ , izračuna heš vrednost  $h_i = X_i = H(Y_i)$  primenom heš funkcije SHA-1 koja daje 160-bitnu vrednost. U najjednostavnijoj formi generiše se 160  $X_i$  i 160  $Y_i$  vrednosti.

Na osnovu ovih heš vrednosti  $h_i$  generiše se odgovarajuće heš drvo. Svaki čvor tog heš drveta se može predstaviti sa  $a_{i,j}$  gde je indeks  $i$  definiše visinu čvora a indeks  $j$  odgovara poziciju čvora s leva na desno. Visina čvora je definisana kao daljina od čvora do lista drveta tako da list ima visinu  $i = 0$ , dok je visina korena drveta  $i = n$ . Čvorovi sa istom visinom su zatim nabrojani s leva na desno, tako da je na primer krajnji levi čvor visine  $i$  označen sa  $a_{i,0}$

U Merkleovom drvetu heš vrednosti  $h_i$  su listovi binarnog drveta tako da postoji mapiranje  $h_i = a_{0,i}$ . Svaki unutrašnji čvor drveta je heš vrednost konkatencije (operacija ||) njegove dece. Kao primer može se uzeti da je  $a_{1,0} = H(a_{0,0} || a_{0,1})$ , dok je  $a_{2,0} = H(a_{1,0} || a_{1,1})$ .



Slika 56 - Primer Merkle drveta

Na ovaj način izgrađeno je drvo sa  $2^n$  listova i  $2^{n+1} - 1$  čvorova, a koren drveta  $a_{n,0}$  je javni ključ  $P$  koji je zamišljen na početku.

## Generisanje potpisa

Alisa prvo potpisuje poruku  $M$  jednokratnim šemom, na osnovu koje se dobije potpis  $S'$  korišćenjem para javnih i privatnih ključeva  $(X_i, Y_i)$ . Odgovarajući list drveta za jednokratni javni ključ  $X_i$  je  $a_{0,i} = H(X_i)$ . Označimo putanju kroz drvo od čvora  $a_{0,i}$  do korena sa  $A$ . Putanja  $A$  sastoji se od  $n + 1$  čvorova,  $A_0, \dots, A_n$ , gde je  $A_0 = a_{0,i}$  list, a  $A_n = a_{n,0} = P$ , koren drveta. Da bi Alisa izračunala navedenu putanju potrebni su svaki od čvorova  $A_1, \dots, A_n$ , uzimajući u vidu da je svako  $A_i$  dete čvora  $A_{i+1}$ . Da bi izračunala sledeći čvor  $A_{i+1}$ , ona treba da zna oba čvora  $A_i$  i njegov bratski

čvor na istom nivou,  $s_i$ , te izračunati  $A_{i+1} = H(A_i || s_i)$ . Na osnovu ovog algoritma traverziranjem putanje A i jednokratnog potpisa  $S'$ , Alisa izračunava krajnji potpis  $S$  na osnovu sledećeg izraza.

$$S = (S' || s_0 || s_1 || \dots || s_{n-1})$$

### Verifikacija potpisa

Bob poseduje javni ključ  $P$ , poruku  $M$ , i potpis  $S$ . Na početku on verifikuje jednokratni potpis  $S'$  poruke, a ako je on korektan, Bob nastavlja sa izračunavanjem  $A_0 = H(X_i)$  heširanjem javnog ključa jednokratnog potpisa. Za svako  $j = 1, \dots, n - 1$ , čvorovi  $A_j$  putanje  $A$  su izračunati na osnovu izraza  $A_j = H(A_{j-1} || s_{j-1})$ . Ako je  $A_n$  jednako javnom ključu  $P$ , Bob je uspešno verifikovao potpis Alisine poruke.

### 6.3.2. Šifarski sistemi na bazi multivariabilnih kvadratnih polinoma (MQ)

Ova klasa šifarskih sistema podrazumeva asimetrične šifarske primitive na bazi polinoma sa više promenljivih nad konačnim poljem. (engl. Multivariate Quadratic Cryptosystems) Rešavanje sistema jednačina sa više promenljivih je NP-teško ili NP-kompletno. U ovom trenutku ne postoje rezultati koji bi dokazali rešivost ovog problema za kvadratne polinome korišćenjem kvantnih algoritama, te se smatra da su šeme na bazi kvadratnih polinoma kandidati za post-quantnu kriptografiju. Na žalost do sada ne postoje sigurne šeme za šifrovanje, dok su šeme za digitalni potpis već prikazane. Moguće generisati efikasan potpis koji je dugačak samo 128 bita. Istraživanja u ovoj oblasti su stoga veoma značajna, iako se navedene šeme za potpisivanje ne koriste u praksi.

T. Macumoto i H. Imai (T. Matsumoto and H. Imai) su 1988. godine prvi put predložili Macumoto-Imai šemu na konferenciji Eurocrypt. Značajne šeme za potpis u ovoj oblasti je predložio J. Patarin u svoji radovima iz 1996. i 1997. godine – HFE, "Balanced Oil and Vinegar" respektivno, a zatim je 1999. godine razrađena i šema "Unbalanced Oil and Vinegar" u saradnji sa Aviad Kipnisom i Lui Gubinom. (Aviad Kipnis, Louis Goubin) Rešavanje sistema kvadratnih jednačina sa više promenljivih, kao što je sistem u sledećem primeru, je NP-teško nad bilo kojim poljem.

$$y_1 = x_1^2 + x_1x_4 + x_3x_4 + \dots$$

$$y_2 = x_{13} + x_2x_4 + \dots$$

...

$$y_n = x_1x_2 + x_1x_3 + x_2^2 + x_2x_3 + x_n^2 + x_3x_n + \dots$$

Šeme sa javnim ključem koje se zasnivaju na problemu rešavanja sistema jednačina sa kvadratnim polinomima sa više promenljivih, kao i izomorfizmu polinoma, predstavljaju suštinu takozvane MQ kriptografije. Moguće je korišćenje polinoma nad malim poljima kao što su GF(2), GF(128), ili GF(256).

## Generisanje ključeva

Privatni ključ kod MQ šifarskih sistema sastoji se iz tri affine transformacije  $(S, P', T)$ , gde je  $P'$  transformacija koja je posebno napravljena za svaku od šema. Ona je takođe maskirana sa dve tajne matrice  $S$  i  $T$ , a zatim primenjene ovim redosledom:

1.  $S$  transformiše iz  $GF^n$  u  $GF^n$ .
2.  $P'$  mapira elemente iz  $GF^n$  u  $GF^m$
3.  $T$  transformiše iz  $GF^m$  u  $GF^m$ .

Notacija  $GF^n$  podrazumeva konačno ili Galoaovo polje (Évariste Galois). To su su polja koja sadrže konačan broj elemenata, u datom slučaju  $n$  elemenata. ( $n$  se naziva i red polja). Po definiciji polje je skup nad kojim su definisane operacije komutativnog množenja, sabiranja, oduzimanja, i deljenja (osim nulom). Svaka od navedenih transformacija mora biti invertibilna. Ponekad se  $(S, P', T)$  naziva "tajnim vratima", pa se privatni ključ  $P$  može formulisati i na sledeći način:  $P = S \cdot P' \cdot T$ , dok je sistem jednačina javni ključ.

## Generisanje potpisa

Potpis se generiše primenom privatnog dok se verifikacija potpisa obavlja primenom javnog ključa. Na početku Alisa uzima poruku i interpretira je kao vektor u malom polju. (kao primer, ako se polje sastoji od 2 elementa, onda je poruka bit vektor). Neka transformacija  $S$  uzima  $x = \langle x_1, x_2, \dots, x_n \rangle$  kao ulaz. U kontekstu primene transformacije  $S$ ,  $x$  se množi sa matricom  $M_S$ , a zatim se dodaje vektor  $v_s$  dužine  $n$ . Na sličan način se primenjuje i transformacija  $T$  tako da se matematički ove dve transformacije mogu izraziti sa

$$S = M_s * x + v_s$$

$$T = M_t * x + v_t$$

Nakon transformacije  $S$  primenjuje se privatna transformacija  $P'$ , a zatim i transformacija  $T$ , što predstavlja na kraju traženi potpis  $y$ . Navedeni algoritam može se opisati sledećim izrazom.

$$\langle x_1, x_2, \dots, x_n \rangle \xrightarrow{S} \langle \dots \rangle \xrightarrow{P'} \langle \dots \rangle \xrightarrow{T} \langle y \rangle$$

## Verifikacija potpisa

Bob poseduje javni ključ u formi sistema jednačina na osnovu koga može se verifikovati da je  $y$  adekvatan potpis poruke  $x$ . Kompletan potpis sastoji se od elemenat  $(x, y)$  kao bit vektora. Na kraju je dovoljno da Bob proveri da li su zadovoljene sve jednačine sistema datim rešenjem  $(x, y)$ . Kao primer javnog ključa može se posmatrati sledeći sistem:

$$y_1 = x_1x_2 + x_1x_4 + x_3x_4$$

$$y_2 = x_{13} + x_2x_4$$

$$y_3 = x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

$$y_4 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

U opštem slučaju sistem jednačina je definisan sledećim izrazom:

$$p_i(x_1, \dots, x_n) = \sum_{1 \leq j \leq k \leq n} \gamma_{i,j,k} x_k x_j + \sum_{j=1} \beta_{i,j} x_j + \alpha_i$$

## 7. Zaključak

U radu je razmatrana sigurnost komunikacija na internetu kao realna potreba svih korisnika i pri tome uzeti u obzir najpoznatiji šifarski sistemi sa javnim ključem, opisan princip rada kvantnih računara i kvantna distribucija ključeva, kao i napad kvantnim računarima na navedene šifarske sisteme. Na kraju je predložena klasa takozvanih post-quantum sistema sa javnim ključem koji su, smatra se, otporni na napade kvantnim računarima.

Moderna trgovina, bankarstvo, razmena osetljivih podataka, kao i uopšte zaštita privatnosti podataka svih strana na internetu zasniva na protokolima kao što su SSL/TLS, GPG, i PGP. Suština ovih sigurnosnih protokola počiva na šifarskim sistemima sa javnim ključem kao što su RSA i Difi-Helman. Navedeni sistemi sa javnim ključem se baziraju na matematičkim problemima koji su praktično nerešivi u realnom vremenu u nedostatku odgovarajućeg tajne informacije odnosno ključa. To su problem faktORIZACIJE proizvoda dva velika prosta broja i nalaženje diskretnog logaritma. Za ove probleme ipak nije matematički dokazano da se ne mogu rešiti na neki drugi način, u realnom vremenu bez tajnog ključa, tako da ovi sistemi nisu bezuslovno sigurni. Buduća istraživanja u ovom domenu mogu da otkriju metode rešavanja navedenih matematičkih problema u realnom vremenu. korišćenjem dostupnih prosečnih računarskih resursa. Suštinski, oslanjanje na par poznatih problema nije dobra dugoročna strategija i potrebna je diversifikacija primenom novih nepovezanih algoritama.

Drugi veliki izazov za današnje sigurne internet komunikacije je postao evidentan otkrićem Šorovog algoritma 1994. godine, kao i njegovih kasnijih modifikacija, koje otvaraju mogućnost primene navedenog algoritma na kvantnom računaru za rešavanje pomenutih problema faktORIZACIJE i diskretnog logaritma u polinomijalnom vremenu. U ovom trenutku kvantni računari nisu na nivou razvoja koji bi predstavljao opasnost za postojeće sisteme. Sa druge strane kvantno računarstvo se neprestano razvija a problem izgradnje kvantnog računara je tehnološke prirode, isključivo u inženjerskom smislu i kontekstu stabilnosti odnosno dekoherencije i primene odgovarajućih kvantnih operacija. Mnogi istraživači, uključujući i projekcije Gartnera, smatraju da će se do primenjivog kvantnog računara kapaciteta 1000+ kubita doći u roku od 10 do 15 godina. U tom trenutku svi današnji sistemi sa javnim ključem mogu postati prevaziđeni, pa je već danas neophodno da se investira u razvoj sistema koji su otporni na navedene napade primenom kvantnog računara.

Uspešan napad na današnje sisteme sa javnim ključem koji bi bio realizovan u realnom vremenu korišćenjem relativno skromnih računarskih resursa bi diskvalifikovao sve navedene sigurnosne internet protokole i izazvao ogromne gubitke u privredi, potpun zastoј u poslovanju putem interneta, neautorizovano prebacivanje novca sa bankarskih računa, gubitak poverenja u finansijske institucije i mnoge izazove u socijalnoj sferi koji bi usledili nakon ovog događaja. Usled navedenih izazova neophodno je pronaći nove načine sigurnog i efikasnog generisanja i razmene ključeva između dve strane koji bi bio otporan na napad primenom kvantnih računara.

Jedan od pravaca razvoja su istraživanja u domenu takozvane kvantne kriptografije ili preciznije, kvantne distribucije ključeva (QKD). Istraživanja na ovom polju se odvijaju zadnjih 30 godina i danas već postoje komercijalni uređaji kao i desetine implementacija državnih i korporativnih sigurnih komunikacionih mreža koje primenjuju QKD tehnologije. Prednosti QKD tehnologija su bezuslovna sigurnost koja se zasniva na fenomenima kvantne mehanike. Danas je praktično moguće, uz bezuslovnu sigurnost, generisati i distribuirati tajni ključ između dve strane povezane optičkim vlaknom na udaljenostima do 150 kilometara za nekoliko sekundi. Prisluškivanje komunikacije od treće strane ne dovodi do otkrića tajne nego isključivo do smanjenja brzine generisanja ključeva, s tim da obe strane odmah znaju da je linija aktivno prisluškivana. Glavni nedostaci QKD sistema su ograničenje brzine generisanja ključa koja direktno zavisi od udaljenosti učesnika, nemogućnost pojačavanja signala odnosno prenošenja putem neke vrste releja, praktično ograničenje isključivo na komunikacije putem optičkih vlakana, kao i cena implementacija sistema.

QKD sistemi stoga ostaju ograničene primene na "lokalne" sigurnosne sisteme velikih korporacija, finansijskih organizacija, vojne i državne komunikacije unutar ograničenog kopnenog regiona. U ovom trenutku arbitrarna primena QKD sistema između bilo koje dve tačke na internetu nije realna. Smatra se da će QKD tehnologija verovatno imati masovnu ulogu u komunikacijama putem (kvantnog) interneta u bliskoj budućnosti, u trenutku kad realistično prihvatljivi kvantni računari postanu dostupni.

U kontekstu ovih pretnji razvijeni su takozvani post-kvantnih šifarskih sistema za koje se tvrdi da su otporni na napade primenom Šorovog algoritma na kvantnom računaru. Dve najznačajnije pod-klase post-kvantnih sistema zasnivaju se na problemima na celobrojnoj rešetci (CVP i SVP problem), i sistemima na bazi linearnih kodova.

Najpoznatiji post-kvantni šifarski sistem koji se zasniva na problemima rešetke je NTRU šifarski sistem koji omogućuje šifrovanje podataka i digitalno potpisivanje (NTRUEncrypt i NTRUSign algoritmi). Smatra se da je NTRU najpraktičniji sistem za primenu od svih post-kvantnih šema koje su poznate danas. Drugi sistem iz ove klase je GGH koji se zasniva na CVP problem danas se ne koristi. Očekuje se da će i drugi, novi, šifarski sistemi koji se zasnivaju na SVP i CVP problemima na rešetci, biti objavljeni u budućnosti, a veliki broj istraživača se bavi ovim poljem matematike.

Post-kvantni šifarski sistemi koji se zasnivaju na težini dekodiranja linearnog koda je Mekelis sistem kod koga je dokazana otpornost na napad Šorovim algoritmom. Ovaj sistem nikada nije bio

široko prihvaćen usled nepraktičn velike dužine ključeva i šifrovane poruke. Jedan od razloga neprihvatanja je bio i nedostatak odgovarajuće šeme za potpis, sve do pojave Niderajterove šeme kao varijacije Mekelisa koja podržava potpisivanje i kod koje je proces šifrovanja znanto efikasniji. Postoje i drugi šifarski sistemi za koje se tvrdi da pripadaju ovoj klasi ali je njihova primenljivost veoma ograničena, često isključivo na digitalno potpisivanje. Pored navedenih postoji značajan broj drugih eksperimentalnih šema koje nisu dovoljno poznate i testirane da bi se tvrdilo da su dovoljno zrele za masovnu primenu.

Na osnovu pregledane literature može se reći da je u smislu brzine, primenljivosti i efikasnosti NTRU najbliži kandidat za post-quantni šifarski sistem koji po svojim osobinama može da dopuni i RSA/ECDH u SSL/TLS protokolu. NTRUEncrypt je opisan standardom IEEE 1363.1 iz 2008. godine, a danas postoje i open source softverske biblioteke kao što je CyaSSL koje primenjuju NTRUEncrypt, na osnovu GPL licence. Očekuje se da će NTRU imati značajnu ulogu u budućnosti zbog efikasnosti koji ga preporučuju za upotrebu u mobilnim sistemima kao i zbog potrebe diversifikacije u odnosu na RSA/ECDH za koje se smatra da u idućih nekoliko godina realno mogu biti kompromitovani klasičnim matematičkim metodama.

## 8. Reference

- Knjige

- 1) "The Physics of Quantum Mechanics", 2008, Autori: James Binney, David Skinner
- 2) "Introduction to Quantum Physics", 2007, Autori: A.P. French, Edwin F. Taylor
- 3) "Quantum Physics – Illusion or Reality", 2004, Autor: Alastar I.M. Rae
- 4) "Post-Quantum Cryptography", 2009, Autori: Daniel J. Bernstein, Johannes Buchman, Erik Dahmen

- Radovi

- 1) "Introduction to Quantum Algorithms", 1994, Autor: Peter W. Shor
- 2) "Quantum theory, the Church-Turing principle and the universal quantum computer", 1985, Autor: David Deutsch
- 3) "COVE: A Practical Quantum Computer Programing Framework", 2009, Autor: Matthew Daniel Purkeypile
- 4) "Rosetta Stone for Quantum Mechanics with an Introduction to Quantum Computation", 2010, Autor: Samuel J. Lomonaco
- 5) "Grover's Quantum Search Algorithm", 2008, Autor: Samuel J. Lomonaco
- 6) "Quantum Information Science", 2010, Autor: Seth Lloyd, MIT
- 7) <http://cseweb.ucsd.edu/~daniele/papers/AlgoEncyclopedia.pdf>
- 8) "La Parallelepiped: Cryptanalysis of GGH and NTRU Signatures", 2009, Autor Phong Nguyen

- Veb resursi

- 1) [www.stanford.edu](http://www.stanford.edu)
- 2) <http://www.dwavesys.com>
- 3) <http://qis.mit.edu>
- 4) <http://www.wikipedia.org>
- 5) [http://www.quantiki.org/wiki/Category:Handbook\\_of\\_Quantum\\_Information](http://www.quantiki.org/wiki/Category:Handbook_of_Quantum_Information)
- 6) <http://jqquantum.sourceforge.net>
- 7) <https://pqcrypto2014.uwaterloo.ca>
- 8) <http://research.stevens.edu>
- 9) <https://uwaterloo.ca/institute-for-quantum-computing>
- 10) <http://www.math.ucdenver.edu/~wcherowi/courses/m5410/ctcmcel.html>
- 11) <http://grouper.ieee.org/groups/1363/lattPK/submissions.html#2005-08>
- 12) [http://paper.ijsns.org/07\\_book/200708/20070812.pdf](http://paper.ijsns.org/07_book/200708/20070812.pdf)
- 13) <https://www.securityinnovation.com>
- 14) <https://eprint.iacr.org/2012/533.pdf>