Opis finalista NIST-ovog natjecanja post-kvantne standardizacije kriptografije

Novak, Lena

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka, Faculty of Engineering / Sveučilište u Rijeci, Tehnički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:190:953057

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Diplomski sveučilišni studij računarstva

Diplomski rad

Opis finalista NIST-ovog natjecanja post-kvantne standardizacije kriptografije

Rijeka, rujan 2022.

Lena Novak
0069078206

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Diplomski sveučilišni studij računarstva

Diplomski rad

Opis finalista NIST-ovog natjecanja post-kvantne standardizacije kriptografije

Mentor: izv.prof.dr.sc. Jonatan Lerga

Rijeka, rujan 2022.

Lena Novak
0069078206

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA DIPLOMSKE ISPITE

Rijeka, 21. ožujka 2022.

Zavod: **Zavod za računarstvo**
Predmet: **Teorija informacija i kodiranje**

ZADATAK ZA DIPLOMSKI RAD

Pristupnik: **Lena Novak (0069078206)**
Studij: Diplomski sveučilišni studij računarstva
Modul: Računalni sustavi

Zadatak: **Opis finalista NIST-ovog natjecanja post-kvantne standardizacije kriptografije / Description of Finalists of NITS Competition For Post-Quantum Cryptography Standardization**

Opis zadatka:

Potrebno je opisati, analizirati i usporediti finaliste NIST-ovog natjecanja za standardizaciju postkvantne kriptografije iz srpnja 2020. godine.

Rad mora biti napisan prema Uputama za pisanje diplomskih / završnih radova koje su objavljene na mrežnim stranicama studija.

Zadatak uručen pristupniku: 21. ožujka 2022.

Mentor:

Izv. prof. dr. sc. Jonatan Lerga

Predsjednik povjerenstva za diplomski ispit:

Prof. dr. sc. Kristijan Lenac

Izjava o samostalnoj izradi rada

Izjavljujem da sam samostalno izradila diplomski rad "Opis finalista NIST-ovog natjecanja post-kvantne standardizacije kriptografije" iz kolegija "Teorija informacija i kodiranje" uz vodstvo i stručnu pomoć mentora izv.prof.dr.sc. Jonatana Lerge.

Rijeka, rujan 2022.

Lena Novak

Zahvala

Zahvaljujem se mentoru izv.prof.dr.sc. Jonatanu Lergi na trudu, pomoći i vodstvu tijekom izrade ovog rada. Zahvaljujem svojim roditeljima što su mi omogućili studiranje u dalekom gradu, što su imali razumijevanja i strpljenja te mi bili podrška tijekom cijelog studiranja. Hvala braći Roku i Emeriku, sestričnama, bratićima i ostaloj rodbini i prijateljima na svim savjetima, druženjima i bezuvjetnoj potpori.

Sadržaj

Popis slika

Popis tablica

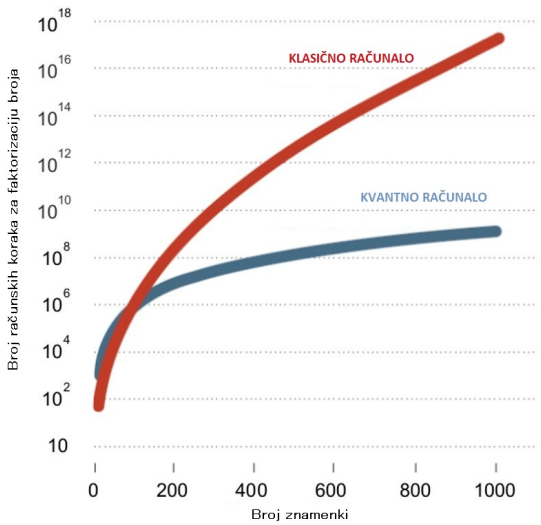
Poglavlje 1

Uvod

Google-ovo kvantno računalo *Sycamore* je krajem desetog mjeseca 2019. godine demonstriralo kvantnu nadmoć (engl. *quantum supremacy*) tako što je u 200 sekundi izmjerilo jednu instancu kvantnog sklopa milijun puta, za što bi klasičnom superračunalu bilo potrebno više od 10 000 godina [1]. Pojam kvantne nadmoći predstavlja kvantna računala koja mogu obavljati razne zadatke ne samo brže od klasičnih računala, nego bi se mogla uhvatiti u koštac s problemima koji su klasičnim računalima nedostižni [2]. Zbog razlike u brzini koju je Google objavio u znanstvenom radu, može se reći kako je to bio vrlo važan trenutak u četrdesetogodišnjoj povijesti područja kvantnog računarstva. Svjetski znanstvenici i stručnjaci mogli su se uvjeriti kako teorijski koncept kvantnog računala funkcionira te kako se u skoroj budućnosti mogu očekivati veliki tehnološki uspjesi unutar tog područja.

Računanje bazirano na zakonima kvantne mehanike pojavilo se u sedamdesetim godinama dvadesetog stoljeća, a popularizirali su ga fizičari poput Benioffa, Feynmana i Deutscha koji su krenuli u ozbiljnije proučavanje istog. Deutsch je 1985. godine definirao univerzalno kvantno računalo i time formalizirao koncept kvantnog računanja [3]. Devet godina kasnije, američki znanstvenik Peter Shor dokazao je kako se dva problema na kojima se temelji sigurnost moderne kriptografije (problem faktorizacije prirodnih brojeva i problem diskretnog algoritma) mogu efikasno riješiti na kvantnom računalu. Shor je time doveo u pitanje sigurnost trenutno postojećih kriptografskih algoritama koji se temelje na teškim matematičkim problemima, a samim time i sigurnost rasprostranjene asimetrične enkripcije [4] .

Na slici 1.1 grafički je prikazan rast kompleksnosti izračunavanja prostih faktora brojeva za tradicionalna i kvantna računala, gdje se na osi apscisa nalazi broj znamenki broja za koji se izračunavaju prosti faktori, a na osi ordinata broj računskih koraka potrebnih za faktorizaciju. Crvenom linijom označena su klasična, a plavom kvantna računala. Kao što se iz grafa može očitati, vrijeme izračunavanja povećava se s većim brojem znamenki. Za klasična računala, vrijeme eksponencijalno raste s porastom znamenki, dok je za kvantna računala porast puno blaži, što se naziva kvantnim ubrzanjem [5]. Do danas, najveći faktorizirani broj na kvantnom računalu je 1 099 551 473 989 [6]. Taj broj je u petom mjesecu 2016. godine iznosio 200 099 [5].



Slika 1.1 Razlike u kompleksnosti tradicionalnih i kvantnih računala [5]

Iako kvantna računala koja bi mogla efikasno i brzo izračunavati teške matematičke probleme na kojima se temelje današnji enkripcijski standardi još uvijek ne postoje, mnogi znanstvenici vjeruju kako će ista postati stvarnost kroz par desetljeća [4]. Postojanje takvih računala dovodi u pitanje sigurnost komunikacije i informacija, zbog čega je 2016. godine američki institut za standarde i tehnologiju, NIST (engl. *National Institute of Standards and Technology*), pokrenuo post-kvantno kriptografsko natjecanje (engl. *the NIST PQC*[1] *Standardization Process*) sa svrhom uvođenja

[1]Postkvantna kriptografija (engl. *Post-Quantum Cryptography*)

post-kvantnog kriptografskog standarda. Cilj natjecanja bilo je uvesti standard za enkripciju javnim ključem (korištenu za enkripciju poruka i stvaranje dijeljenih tajnih ključeva) te standard za digitalno potpisivanje.

Kroz ovaj rad opisat će se osnovni koncepti kriptografije i kvantnog računala. Također će se opisati proces NIST-ovog PQC natjecanja zajedno s principom rada sedam finalista, odabranih u sedmom mjesecu 2020. godine, i njihovom matematičkom pozadinom.

Poglavlje 2

Kriptografija

Kriptografija (grč. *kryptós* - sakriven, *graphein* - pisanje) je znanstvena disciplina koja proučava načine, odnosno metode prijenosa informacija kroz nesigurni komunikacijski kanal (npr. Internet) između pošiljatelja informacije i njenog primatelja. Moderna kriptografija temelji se na prirodnim i tehničkim disciplinama poput matematike, računarstva, elektrotehnike i fizike, a njen je osnovni zadatak zaštititi informaciju od "napadača", odnosno od osobe koja nije pošiljatelj ili primatelj informacije.

Sigurnosni zahtjevi koje kriptografija treba zadovoljiti su [7]:

- Povjerljivost, tajnost (engl. *confidentiality*) - pristup informacijama imaju samo ovlašteni korisnici.
- Integritet (engl. *integrity*) - samo ovlašteni korisnici mogu mijenjati informacije.
- Dostupnost, neporecivost (engl. *confide*) - informacije se ne mogu opovrgnuti i moraju biti dostupne ovlaštenim korisnicima.
- Autentičnost (engl. *authenticity*) - jednoznačno prepoznavanje ovlaštenih korisnika.

Kriptoanaliza (grč. *kryptós* - sakriven, *analýein* - odvezati, olabaviti) je znanstvena disciplina koja se bavi analizom i pronalaženjem propusta u kriptografskim algoritmima, odnosno to je analiza šifrirane poruke s ciljem dešifriranja iste bez

posjedovanja ključa i algoritma kojim je šifrirana [7]. Klasična kriptoanaliza uključuje kombinaciju analitičkog razmišljanja, primjenu matematičkih alata, pronalaženje uzoraka (šablona), strpljenja, odlučnosti i sreće [8]. Kriptoanaliza je jedini način da se zajamči sigurnost kriptosustava, zbog čega je, uz kriptografiju, sastavni dio znanosti kriptologije.

Šifriranje, odnosno enkripcija ili kriptiranje (engl. *encryption*), predstavlja proces konvertiranja izvorne informacije u format kojeg neovlašteni korisnik ne može razumjeti. Neki jednostavniji primjeri enkripcije su: zamjena jedne vrijednosti drugom (zamjena slovom unaprijed ili unazad u abecedi, zamjena parova slova), korištenje šifrarnika (npr. stranice knjiga), logička operacija ekskluzivnog ili (XOR) nad bitovima i tako dalje.

Proces šifriranja sastoji se od četiri dijela:

1. ulaz (jasni, čisti tekst, engl. *clean text*) - izvorni oblik informacije koji je razumljiv korisniku,
2. algoritam - slijed jednoznačno određenih koraka pomoću kojih se čisti tekst pretvara u kriptirani i obratno,
3. ključ - vrijednost koju algoritam koristi kako bi jasni tekst pretvorio u kriptirani,
4. izlaz (šifrat, kriptirani tekst, engl. *chiper text*) - rezultat šifriranja koji predstavlja transformirani oblik čistog teksta pomoću kriptografskog algoritma, gdje se čisti tekst ne može prepoznati bez poznavanja ključa.

Obrnuti postupak kojim se šifrirani tekst pretvara u jasni zove se dešifriranje (dekriptiranje, engl. *decryption*), a oba postupka prikazana su na slici 2.1.

Slika 2.1 Proces šifriranja i dešifriranja

2.1 Simetrični kriptosustavi

Simetrični kriptosustavi, odnosno sustavi enkripcije privatnim ključem (engl. *Private Key Encryption*, PKE) koriste isti ključ za šifriranje i dešifriranje. Takav ključ naziva se još i tajnim ključem. U algoritmima simetričnih kriptosustava najčešće se koristi logička operacija ekskluzivnog ili (XOR) [9].

Prednost ovakvih kriptosustava je brzina, a glavni nedostatak je potreba za velikim brojem ključeva i njihovih razmjena. Kako bi n osoba moglo komunicirati putem simetričnog kriptosustava potrebno je $\frac{n(n-1)}{2}$ ključeva [9]. Drugi nedostatak je to što je dovoljno da se samo jedan ključ kompromitira i sustav postaje nesiguran. Navedeni nedostaci čine simetrični kriptosustav nepraktičnim za internetske protokole [7].

Neki od najpoznatijih simetričnih algoritama su: DES (engl. *Data Encryption Standard*), AES (engl. *Advanced Encryption Standard*), 3DES (engl. *Triple* DES), IDEA, Serpent i Twofish.

Princip komunikacije kroz simetrični kriptosustav je sljedeći: pošiljatelj poruke i njezin primatelj imaju unaprijed dogovoren ključ za šifriranje. Pošiljatelj zatim pomoću tog ključa pretvara razumljiv tekst u šifrat i šalje ga kroz nesigurni komunikacijski kanal do primatelja. U komunikacijskom kanalu može postojati "presretač" koji će vidjeti sadržaj šifrata, no neće moći odgonetnuti tekst poruke. Za razliku od presretača, primatelj zna ključ kojim je poruka šifrirana te će pomoću dešifriranja dobiti razumljiv tekst poruke. Prikaz komunikacije simetričnog kriptosustava

prikazan je na slici 2.2.

Slika 2.2 Slanje poruke pomoću simetričnog kriptosustava

2.2 Asimetrični kriptosustavi

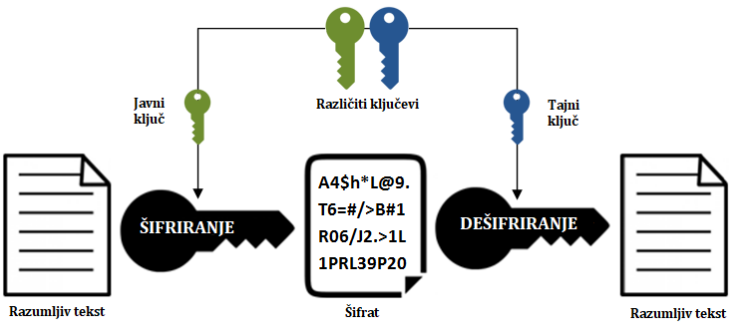
Asimetrični kriptosustavi, odnosno kriptosustavi s javnim ključem (engl. *PKE, Public Key Encryption*), koriste par ključeva, to jest dva različita, ali vezana ključa - privatni i javni ključ. Šifriranje se može odraditi s bilo kojim od ta dva ključa, gdje se drugi onda koristi za dešifriranje. Ideja asimetričnog kriptosustava je da privatni ključ bude dostupan samo vlasniku koji njime dešifrira poruku, a javni ključ korisniku služi za šifriranje poruka. Javni ključ zbog toga može biti dostupan svima jer se s njim ne može izračunati privatni ključ.

Asimetrični algoritmi za šifriranje puno su sporiji od simetričnih te imaju dulje ključeve. Zbog te činjenice, simetrični algoritmi pogodniji su za šifriranje većih količina podataka, a asimetrični algoritmi se onda upotrebljavaju za razmjenu ključeva korištenih u simetričnim kriptosustavima [9].

Proces razmjene informacije pomoću asimetričnog kriptosustava vidljiv je na slici 2.3, a opisan u sljedećih nekoliko koraka:

1. Osoba A generira simetričan ključ K,
2. Osoba A koristi javni ključ Osobe B za šifriranje ključa K,
3. Šifrirani tekst putuje nesigurnim komunikacijskim kanalom,
4. Osoba B dešifrira informaciju pomoću svog privatnog ključa,

5. Osoba B vidi jasni tekst.



Slika 2.3 Asimetrični kriptosustav

2.2.1 Funkcije asimetričnih kriptosustava

Funkcije koje se koriste u asimetričnim kriptosustavima nazivaju se još i jednosmjernim funkcijama s tajnim vratima (engl. *one-way trapdoor functions*) čije je glavno svojstvo jednostavnost računanja u jednom smjeru i izrazita zahtjevnost invertiranja bez dodatnih informacija [9].

U nastavku su nabrojani problemi, odnosno jednosmjerne funkcije s tajnim vratima. Problemi mogu biti NP-teški ako za njih ne postoje algoritmi polinomne složenosti kojima bi se riješili.

- Problem diskretnog logaritma - za dani N i neki broj x, potrebno je pronaći najmanji broj r takav da vrijedi $x^r = 1(modN)$. Problem se smatra NP-teškim.
- Problem faktorizacije - za dani N za koji vrijedi $N = pq$, gdje su p i q prosti brojevi, potrebno je pronaći p i q. Problem se smatra NP-teškim za velike p i q.
- Problem naprtnjače (engl. *knapsack problem*) - kombinatorni problem optimizacije, gdje je za zadani skup elemenata s težinama i vrijednostima potrebno odrediti broj elemenata od svakog tipa elemenata koji se treba uključiti u traženi skup kako bi ukupna težina bila manja od unaprijed određenog limita, a

suma što je moguće veća. Problem naprtnjače je NP-potpun problem, što znači da je teži od problema diskretnog logaritma i faktorizacije.

- Problemi rešetke - algoritmi za rješavanje problema rešetki zovu se algoritmi redukcije rešetke, gdje je formalna definicija redukcije rešetke pronalazak najkraće baze rešetke, a najbolji algoritmi koji rješavaju problem su ili eksponencijalne složenosti ili daju loše aproksimacijske rezultate [9].

  – Problem najkraćeg vektora (engl. *Shortest Vector Problem*, SVP) je traženje vektora rešetke koji će prvi postići periodični minimum.

  Definicija problema najkraćeg vektora glasi da za danu bazu rešetke $B \in \mathbb{Z}^{m \times n}$ treba pronaći ne-nul vektor rešetke Bx (uz $x \in \mathbb{Z}^n \setminus \{0\}$) takav da je $||Bx|| \leq ||By||$ za svaki $y \in \mathbb{Z}^n \setminus \{0\}$.

  Aproksimacijski algoritam (LLL algoritam[1]) u polinomnom vremenu pronalazi vektor rešetke čija duljina može biti maksimalno y puta veća od duljine najkraćeg vektora rešetke. Faktor γ je aproksimacijski faktor, a najboljim se smatra $\gamma = (\frac{2}{\sqrt{3}})^n$.

  Duljina najkraćeg ne-nul vektora prema Gaussovoj heuristici je približno jednaka:

$$\lambda_1(L) \approx \sqrt{\frac{dim(L)}{2\pi e}} det(L)^{\frac{1}{dim(L)}}, \tag{2.1}$$

  gdje $dim(L)$ predstavlja dimenziju rešetke L.

  – Problem najbližeg vektora (engl. *Closest Vector Problem*, CVP) ima sljedeću definiciju: uz danu bazu rešetke $B \in \mathbb{Z}^{m \times n}$ i vektor $t \in \mathbb{Z}^m$, potrebno je pronaći vektor rešetke Bx koji je najbliži vektoru t.

  Aproksimacijski algoritam polinomne složenosti za CVP problem postoji, a njegov aproksimacijski faktor γ je jednak $2(\frac{2}{\sqrt{3}})^n$.

[1] Lenstra–Lenstra–Lovász algoritam redukcije baze rešetke je algoritam redukcije rešetke u polinomnom vremenu koji su izumili Arjen Lenstra, Hendrik Lenstra i László Lovász 1982. godine.

2.2.2 Pregled asimetričnih kriptosustava

U tablici 2.1 nalazi se popis najpoznatijih asimetričnih algoritama i problema na kojima su temeljeni. Od navedenih u tablici, u najširoj su primjeni asimetrični algoritmi RSA i ECC[2] [9].

Tablica 2.1 Popis asimetričnih kriptosustava

Naziv asimetričnog algoritma	Problem na kojem se temelji
Blum-Goldwasser	problem faktoriziranja
DSS	diskretni logaritam
Diffie-Hellman	diskretni logaritam
ECC	diskretni logaritam
ElGamal	diskretni logaritam
LUC	diskretni logaritam
McEliece	dekodiranje linearnog koda
Merkle-Hellman	problem naprtnjače
RSA	problem faktoriziranja
Rabin	problem faktoriziranja
Rivest-Chor	problem naprtnjače

2.3 Sažetak poruke

Sažetak poruke (engl. *hash*) niz je bitova određene duljine koji nastaje uz pomoć hash funkcija koje moraju imati sljedeća svojstva:

1. Funkcija mora biti jednosmjerna - iz sažetka se ne može dobiti izvorna poruka,
2. Ako se kroz jednu hash funkciju provede ista poruka, dobiveni rezultati će biti identični,

[2]Kriptografija temeljena na eliptičkim krivuljama, engl. *Eliptic Curve Cryptography*

3. Parovi različitih poruka moraju se preslikavati u različite sažetke, čak i ako je razlika u samo jednom bitu poruke,
4. Hash funkcija određuje duljinu sažetka i ista duljina se ne mijenja s duljinom poruke.

Kako bi se osigurao integritet poruke koriste se hash funkcije, a zajedno s asimetričnim algoritmima služe za osiguravanje podrijetla poruke [9].

2.4 Digitalni potpis

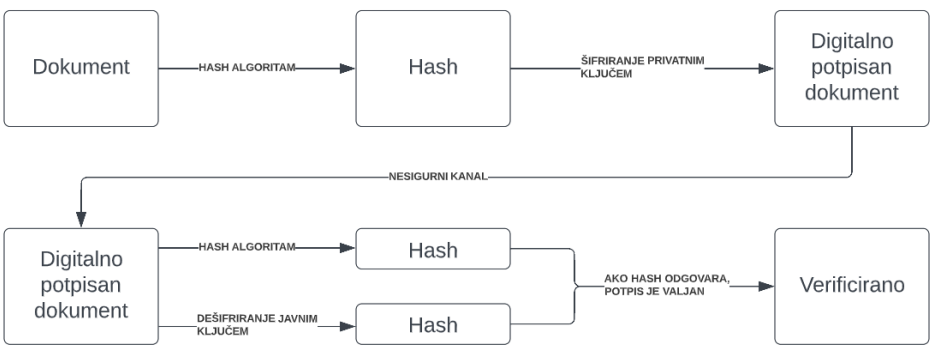
Digitalnim potpisom omogućuje se utvrđivanje autentičnosti poruke, a poruka je autentična ako je poznat identitet njenog autora. Digitalni potpis osigurava autentičnost, integritet i neporecivost.

Formalna definicija digitalnog potpisa je:

$$Potpis = E(H(m), S_A), \tag{2.2}$$

gdje je m poruka, $H(m)$ hash poruke m, S_A potpisnikov tajni (privatni) ključ i E asimetrični algoritam šifriranja.

Proces potpisivanja dokumenta započinje korisnikom A koji potpisuje dokument privatnim ključem, gdje potpis nastaje tako što se prvotno napravi sažetak dokumenta, a onda se taj sažetak šifrira privatnim ključem korisnika A. Korisnik A šalje dokument i potpis korisniku B preko nesigurnog kanala. Korisnik B po primitku dokumenta i potpisa radi sljedeće: izrađuje sažetak dokumenta, dešifrira potpis javnim ključem korisnika A i uspoređuje dobiveni sažetak s dobivenim potpisom [7]. Proces digitalnog potpisivanja vidljiv je na slici 2.4.



Slika 2.4 Proces digitalnog potpisivanja [2]

Poglavlje 3

Kvantno računalo

Iako se u posljednjih nekoliko godina pojavilo mnoštvo novih računalnih tehnologija, kvantna računala su nedvojbeno tehnologija koja zahtjeva najveću promjenu paradigme od strane programera [10].

Ideju o kvantnim računalima pokrenuo je 1980. godine Jurij Ivanovič Manin, koji ih je opisao kroz znanstveni rad "Izračunljivo i neizračunljivo". Godinu dana nakon, Richard Feynman predložio je model za izradu kvantnog računala koje se temelji na zakonima kvantne fizike kao što su superpozicija i sprezanje.

Osnovno načelo kvantnoga računanja je upotreba kvantnih svojstava čestica za predstavljanje i strukturiranje podataka te primjena kvantnih mehanizama kod izvođenja operacija nad tim podacima [2].

Kvantno računalo predstavlja kvantno-mehanički uređaj koji koristi zakone kvantne fizike za obavljanje operacija nad podacima. Kvantna računala koriste se za optimiziranje postojećih rješenja, pretraživanje velikih baza, faktoriziranje velikih brojeva, strojno učenje, uspoređivanje molekula u kemiji, za analizu, pretraživanje i uspoređivanje slika i tako dalje [11].

3.1 Qubit

Kvantni bit ili *qubit* (engl. *quantum bit*) osnovna je jedinica za prijenos informacija u kvantnom računarstvu. Kod klasičnih računala, osnovna jedinica za prijenos informacija je bit koja može biti u jednom od dva stanja, nula ili jedan, a predstavljena je kroz binarni brojevni sustav. Qubit je također temeljen na binarnom brojevnom sustavu i u trenutku njegovog mjerenja može poprimiti vrijednost nule ili jedinice. Kvantno logičko stanje 0 u qubitu odgovara vektoru $\binom{1}{0}$, a kvantno logičko stanje 1 odgovara vektoru $\binom{0}{1}$. Standardno qubitovo stanje može se zapisati pomoću Diracove notacije:

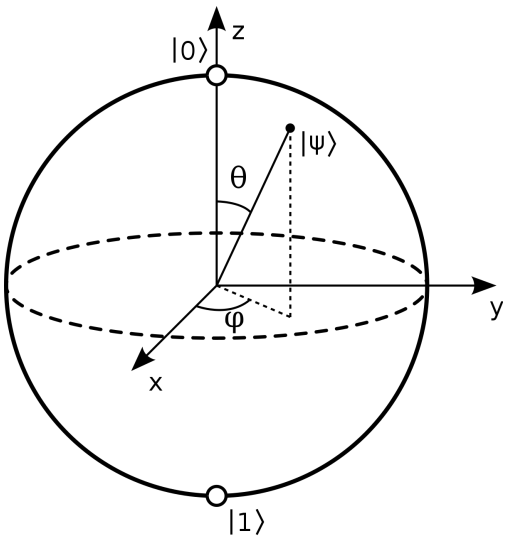
$$|0\rangle = \binom{1}{0}, |1\rangle = \binom{0}{1}, \tag{3.1}$$

gdje vektori $|0\rangle$ i $|1\rangle$ čine bazu Hilbertovog prostora [9]. Hilbertov prostor je vektorski prostor konačne dimenzije unutar kojeg je definiran skalarni produkt. Vektori u tom prostoru predstavljaju stanje čestica nad kojima mogu djelovati unitarni[1] i hermitski[2] linearni operatori [9].

Qubit se najčešće reprezentira pomoću Blochove sfere, geometrijskog prikaza čistog prostora stanja dvorazinskog kvantno-mehaničkog sustava. Sfera je vidljiva na slici 3.1.

[1]Operator U je unitarni ako vrijedi $UU* = U * U = I$

[2]Operator A je hermitski ako vrijedi $A = A*$, gdje je $A* = (A^T)*$



Slika 3.1 Blochova sfera [12]

3.2 Svojstva kvantnog računala

3.2.1 Superpozicija

Kvantna superpozicija je svojstvo koje omogućuje kvantnom bitu (qubitu) da bude u jednom od tri stanja - stanju nule, stanju jedinice ili stanju nule i jedinice istovremeno. Ovo svojstvo uz niz drugih kvantnih učinaka omogućuje kvantnim računalima znatno brže izvođenje određenih operacija u odnosu na standardna računala.

Umjesto da postoji u jednom određenom stanju, kvantni sustav je zapravo u svim svojim mogućim stanjima istovremeno. To znači da kvantni registar postoji u superpoziciji svih svojih mogućih konfiguracija nula i jedinica u isto vrijeme, za razliku od klasičnog sustava čiji registar sadrži samo jednu određenu vrijednost u bilo kojem trenutku. Tek kad se kvantni sustav krene mjeriti, odnosno promatrati, on poprima definitivno stanje [2].

Matematički prikaz stanja qubita u bilo kojem trenutku je kao dvodimenzionalni prostor stanja sa ortonormalanim[3] baznim vektorima $|0\rangle$ i $|1\rangle$. Superpozicija $|\psi\rangle$

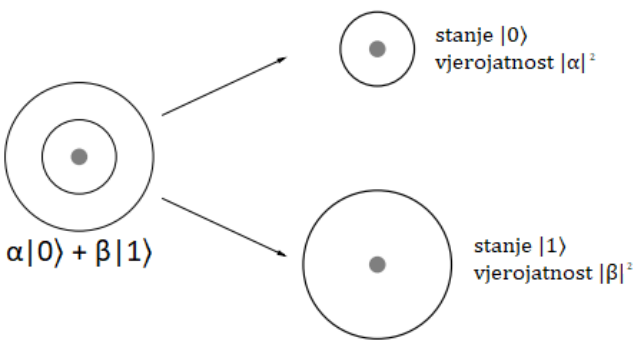
[3]Bazni vektori su ortogonalni i normalizirani vektori.

qubita može se prikazati kao linearna kombinacija ta dva bazna vektora:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{uz } \alpha, \beta \in \mathbb{C} \text{ gdje, } |\alpha|^2 + |\beta|^2 = 1, \tag{3.2}$$

gdje vrijednosti α i β predstavljaju amplitude pojedinog stanja superpozicije $|\psi\rangle$, a kvadrati njihovih apsolutnih vrijednosti označavaju vjerojatnosti pojavljivanja određenih stanja uslijed mjerenja qubita. Vjerojatnost da je izmjerena vrijednost $|\psi\rangle$ jednaka nuli iznosi $|\alpha|^2$, a vjerojatnost da je jednaka jedinici iznosi $|\beta|^2$. Kad se sustav izmjeri, on ostaje u tom izmjerenom stanju te se prethodno stanje sustava briše, odnosno uništava.

Mjerenje superpozicije ima učinak prisiljavanja sustava da odluči o određenom stanju, s vjerojatnostima koje su određene preko amplituda što je grafički prikazano na slici 3.2.



Slika 3.2 Mjerenje superpozicije

3.2.2 Kvantno sprezanje

Kvantna spregnutost (engl. *quantum entanglement*) se odnosi na stanja u kojima kombinirano stanje qubita sadrži više informacija nego što jedan qubit ima zasebno. Ogromna većina *multi-qubit* kvantnih stanja je spregnuta i predstavlja vrijedan resurs. Na primjer, spregnuta stanja između qubita mogu se koristiti za kvantnu teleportaciju, gdje se zajedničko spregnuto stanje dva qubita može koristiti za prijenos informacija s jednog qubita na drugi, bez obzira na njihovu fizičku

udaljenost. Spregnuta stanja, kao prirodna stanja kvantnih sustava, važna su u područjima poput kvantne kemije i kvantnih simulacija, gdje rješenja često budu u obliku spregnutih multi-qubit stanja [13].

3.2.3 Kvantni paralelizam

Početno stanje kvantnog računala ne mora biti neko od stanja računalne baze, već može biti bilo koja superpozicija tih stanja. Konačno stanje kvantnog računala tada postaje superpozicija stanja koja bi se dobila uz početna stanja jednaka stanjima računalne baze. Konačno stanje kvantnog računala, koje može biti jedno i jedino, ovisi o rezultatu koji se dobije uz sva moguća početna stanja. Sposobnost kvantnih algoritama da u jednom koraku obave operacije nad više različitih vrijednosti argumenta zove se kvantni paralelizam [14].

Načela kvantne fizike ne dopuštaju da se mjerenjem konačnih stanja qubitova kvantnog računala pristupi svim informacijama koje se nalaze u konačnom stanju računala.

3.3 Kvantna vrata

Logičkim krugovima mogu se opisati svi izvršeni programi klasičnog računala. Svaki logički krug sastoji se od logičkih vrata - ILI (engl. *OR*), I (engl. *AND*), NE (engl. *NOT*), ekskluzivno ILI (engl. *XOR*) i tako dalje, koja djeluju na bitove [15].

Programi koji se izvršavaju na kvantnim računalima opisuju se pomoću kvantnih krugova u kojima na qubite djeluju kvantna vrata.

Kvantnim vratima smatraju se proizvoljni unitarni operatori u prostoru stanja, a kvantni sklopovi su nizovi proizvoljnih unitarnih operatora. U nastavku slijede najčešće korišteni operatori (kvantna vrata) koji djeluju na jedan qubit:

- Pauli-X (NOT ili X vrata): $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, tj. $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$. Matrično $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
- Pauli-Z (Z vrata): $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$. Matrično $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

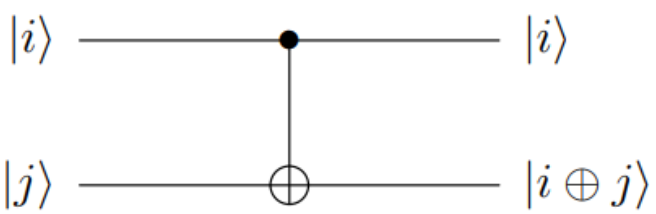
- Hadamardova vrata: $H : H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Matrično $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Uočava se kako je $H^2 = Id$.

Gore navedeni operatori su unitarni što govori da je reverzibilnost operacija omogućena. Pauli-X operator je analogija klasičnog NOT operatora, a operatorom Hadamard stanje qubita prelazi u superpoziciju stanja [9].

Od operatora (kvantnih vrata) koji djeluju na dva qubita potreban je kontrolni NOT ili CNOT operator. On djeluje na dva qubita, na kontrolni qubit $|i\rangle$ i qubit $|j\rangle$. Na qubit $|j\rangle$ primjenjuju se NOT ili X vrata ako je kontrolni qubit jednak $|1\rangle$. Ako je kontrolni qubit različit od $|1\rangle$, ne događa se ništa. Kontrolni qubit se nikad ne mijenja. CNOT operator prikazan je na slici 3.3, gdje $\oplus$ predstavlja operaciju ekskluzivnog ILI (XOR), i vrijedi [15]:

- CNOT vrata: $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |10\rangle$, odnosno: $|a, b\rangle \mapsto |a, a \oplus b\rangle$.

.



Slika 3.3 CNOT vrata (operator)

U klasičnom računarstvu vrlo je jednostavno napraviti logički sklop koji će kopirati neki bit. Potreban je registar od dva bita, gdje će se vrijednost prvog bita kopirati u drugi bez brisanja vrijednosti. U kvantnom računarstvu nije moguće kopirati kvantna stanja što se smatra vrlo važnim svojstvom, a teorem kojim se opisuje zove se *No-cloning* teorem [16].

3.4 Kvantni algoritmi

3.4.1 Shorov algoritam

Vjerojatno najpoznatiji događaj u kvantnom računarstvu bio je objava kvantnog algoritma za izvođenje proste faktorizacije cijelih brojeva u polinomijalnom vremenu kojeg je definirao američki profesor Peter Shor 1997. godine [17]. Shorov algoritam je bio veliko otkriće, ne samo zato što pruža eksponencijalno ubrzanje u odnosu na najbrže klasične algoritme, već zato što brojni algoritmi za kriptografiju s javnim ključem, uključujući uobičajeno korišteni RSA algoritam, ovise o činjenici da ne postoji učinkoviti klasični algoritam koji može rastaviti velike cijele brojeve na proste faktore [18]. Shor je dokazao da bi realizacija dovoljno snažnog kvantnog računala imala potencijal uvelike povećati brzine računanja. Shorovo otkriće potaknulo je na istraživanje kvantnih računala i njihovih algoritama.

Shorov kvantni algoritam je BQP (engl. *Bounded error Quantum Polynomial time*) klase, što označava da je vrijeme njegovog izvršavanja polinomijalno, te da najveća vjerojatnost za pogreškom algoritma iznosi $1/3$. Shorov algoritam je kvantni analogon klasi PP (engl. *Probabilistic Polynomial time*) koja predstavlja probabilističke algoritme u polinomijalnom vremenu [19].

Algoritam se temelji na rješavanju problema diskretnog logaritma, gdje se broj N može faktorizirati kroz sljedeće korake:

1. Odabere se proizvoljni $x < N$.
2. Zatim se određuje $nzd(x, N)$.
   - Ako je $nzd(x, N) \neq 1$, postupak je završen jer je za broj N pronađen jedan od faktora,
   - ako je $nzd(x, N) = 1$, potrebno je pronaći najmanji r gdje vrijedi $x^r \equiv 1(modN)$.
3. Ako je r neparan, bira se novi x i postupak se ponavlja do kad r ne bude paran broj.
4. Kad je pronađen paran r, relacija $x^r \equiv 1(modN)$ se kroz razliku kvadrata može

raspisati kao $(x^{r/2}-1)(x^{r/2}+1) \equiv kN$, za $k \neq 0$.

5. U konačnici, $nzd((x^{r/2}-1), N)$ i $nzd((x^{r/2}-1), N)$ daju netrivijalne faktore broja N

Periodičnost niza ($x^0(modN)$, $x^1(modN)$, $x^2(modN)$, ...) je temelj kvantnog algoritma za rješavanje problema diskretnog logaritma. Niz je periodičan s periodom r ($x^0(modN) = x^r(modN)$) te je r rješenje problema diskretnog logaritma.

Algoritam koristi dva n-qubitna registra i izvodi se na sljedeći način:

1. Odabere se broj n, gdje vrijedi $N^2 < 2^n < 2N^2$.
2. Izvrši se uniformna superpozicija:

$$2^{-n/2} \sum_{k=0}^{2^n-1} |k\rangle|0\rangle \tag{3.3}$$

.

3. Napravi se modularno potenciranje kako bi se dobilo stanje:

$$2^{-n/2} \sum_{k=0}^{2^n-1} |k\rangle|x^k modN\rangle \tag{3.4}$$

4. Na prvi registar stanja iz jednadžbe 3.4 primjenjuje se kvantna Fourierova transformacija (engl. *Quantum Fourier Transform*, QFT) čime se dobije:

$$2^{-n} \sum_{jk=0}^{2^n-1} e^{2\pi ijk/2^n} |j\rangle|xkmodN\rangle. \tag{3.5}$$

.

Pozitivna interferencija se zbog periodičnosti događa kada je $j(k+lr)$ blizu višekratnika od 2^n. Broj j dobiva se mjerenjem prvog registra takav da je $jr/2^n$ blizu nekog cijelog broja, što znači da se broj j pronalazi kada vrijedi $j/2^n = s/r$ za neki cijeli broj s. Razlomci se pronalaze korištenjem kontinuirane aproksimacije razlomka. Za pronalazak broja r dovoljno je par ponavljanja aproksimacije razlomka ($2logN$ puta)[9].

3.4.2 Groverov algoritam

Znanstvenik Lov Grover proučavao je nove efikasnije načine pretraživanja NP prostora stanja, ali najveća brzina koju je postigao sa svojim kvantnim algoritmom bilo je $O(\sqrt{n})$ koraka, gdje je n broj podataka, što je preslabo ubrzanje ako n eksponencijalno raste. Iz tog je razloga utjecaj Groverovog kvantnog algoritma zanemariv za današnje kriptosustave [9].

Problem pretraživanja prostora sastoji se od traženja indeksa x nekog podatka, gdje vrijedi $f(x) = 1$ ako se taj podatak traži, $f(x) = 0$ inače. Indeks se pretražuje pomoću crne kutije koja predstavlja unitarni operator O, gdje je interna struktura tog operatora nebitna. Definicija djelovanja operatora O nad dva qubita je sljedeća:

$$|x\rangle|y\rangle \xrightarrow{O} |x\rangle|y \oplus f(x)\rangle. \tag{3.6}$$

Pod pretpostavkom traženja indeksa x, utjecaj operatora O na $|x\rangle|0\rangle$ rezultira s $|x\rangle|1\rangle$, što se smatra invertiranjem drugog qubita. Postavljanjem drugog qubita u superpoziciju unutar crne kutije dobiva se:

$$|x\rangle|\frac{|0\rangle - |1\rangle}{\sqrt{2}}\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle|\frac{|0\rangle - |1\rangle}{\sqrt{2}}\rangle. \tag{3.7}$$

U zamjenu za invertiranje drugog qubita, prema 3.7, promijenio se predznak amplitudi stanja sustava. Budući da se drugi qubit ne upotrebljava, djelovanje unitarnog operatora prikazuje se kao:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle. \tag{3.8}$$

Groverov kvantni algoritam koristi unitarni operator O, Hadmardov operator H i definira novi unitarni operator U_0 [9]:

$$|0...0\rangle \xrightarrow{U_0} -|0...0\rangle \text{ i } |j\rangle \xrightarrow{U_0} |j\rangle \text{ za } j \neq 0, \tag{3.9}$$

gdje $|j\rangle$ predstavlja različita stanja sustava koja se zapisuju u binarnom formatu.

Rad Groverovog kvantnog algoritma može se opisati kroz tri koraka [9]:

1. Postavljanje svih qubita u stanje $|0\rangle$.

2. Na sve qubite se primjenom Hamardovog operatora H dobiva stanje sustava $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$.
3. Slijedno se primjenjuju operatori O, H i U_0 i ponovno H : $U_G = HU_0HO$ sveukupno $(\pi/4)\sqrt{N}$ puta.

Sustav je nakon primjene Groverovog algoritma s velikom vjerojatnošću u stanju $|w\rangle = |1\rangle$, odnosno $U_G^{\sqrt{N}}|0...0\rangle \approx |w\rangle$. Svaka izmjena operatora U_G predstavlja jedno pozivanje unitarnog operatora O, traženo stanje $|w\rangle$ će se postići nakon $O(\sqrt{N})$ poziva crne kutije.

Groverov algoritam također radi za slučajeve u kojima postoji više elemenata za koje vrijedi $f(x) = 1$. U tim slučajevima algoritmu treba $(\pi/4)\sqrt{N/M}$ poziva crne kutije kako bi pronašao traženi element, gdje M predstavlja broj različitih elemenata za koje vrijedi $f(x) = 1$.

Poglavlje 4

NIST-ovo natjecanje

Nacionalni institut za standarde i tehnologiju, NIST (engl. *National Institute of Standards and Technology*), sa sjedištem u SAD-u, neregulatorna je agencija američkog ministarstva trgovine i laboratorij za STEM[1] područja. Vizija instituta je promicati američke inovacije i industrijsku konkurentnost [20].

Kroz povijest kriptografskih standarda, NIST je zaslužan za razvoj i definiranje AES[2] i SHA [3] algoritama (SHA-1, SHA-2 i, odnedavno, SHA-3). Iako su SHA-1 i SHA-2 algoritmi bili dizajnirani od strane Nacionalne sigurnosne agencije (NSA), algoritmi AES i SHA-3 direktni su rezultat NIST-ovog otvorenijeg procesa. Kako bi se zamijenio tada korišteni DES[4], NIST je 2001. godine proveo otvoreni natječaj i odabrao Rijndael algoritam za AES, a Keccak algoritam 2015. kao SHA-3 algoritam koji je upotpunio SHA-1 i SHA-2 algoritme. [21]

NIST je u drugom mjesecu 2016. godine na *PQCrypto* konferenciji, sedma internacionalna konferencija o post-kvantnoj kriptografiji održana u Japanu 24.-26.02.2016., objavio kako se pokreće proces standardizacije post-kvantnih kriptografskih algoritama, a rok za inicijalne prijave postavili su na 11. mjesec 2017. godine,

[1] Akronim pojmova: znanost, tehnologija, inženjerstvo i matematiku (engl. *science, technology, engineering and mathematics*)

[2] Napredni standard šifriranja, engl. *Advanced Encryption Standard*

[3] Sigurni *hash* algoritam - algoritama koji služi za provjeru autentičnosti datoteka ili poruka prilikom prijenosa između pošiljaoca i primatelja (engl. *Secure Hash Algorithm*)

[4] Standard šifriranja podataka, engl. *Data Encryption Standard*

što je omogućilo znanstvenicima iz cijelog svijeta period od godinu dana i devet mjeseci da osmisle rješenje i isto prijave u program, odnosno natjecanje [22].

Bitno je naglasiti kako su se za natjecanje tražili PQC[5] algoritmi koji predstavljaju rješenja namijenjena za trenutna klasična računala koja će biti otporna na klasičnu i kvantnu kriptoanalizu. Za razliku od PQC-a, kvantna kriptografija označava kriptografska rješenja koja koriste kvantna računala i svojstva kvantne fizike kako bi se ostvarila određeni sigurnosni faktori [23].

U sklopu PQC natjecanja, tražile su se sljedeće vrste algoritama:

- Algoritmi za šifriranje javnim ključem (PKE) - uključuje algoritme za generiranje ključeva, šifriranje i dešifriranje.
- Mehanizmi enkapsulacije ključa (engl. *Key Encapsulation Mechanism), KEM* - uključuje algoritme za generiranje ključeva, enkapsulaciju i dekapsulaciju.
- Algoritmi za digitalno potpisivanje - uključuje algoritme za generiranje ključeva, generiranje potpisa i verifikaciju potpisa.

Prethodno navedeni algoritmi detaljnije su opisani u poglavljima 4.3 i 4.4.

PQC natjecanje razlikuje se od prethodnih (npr. AES/SHA-3) NIST-ovih natjecanja iz više razloga. Prvotno po tome što je postkvantna kriptografija kompliciranija od AES/SHA-3 kriptografije. Svaki kandidat ima nekoliko nedostataka, a zbog manjka istraživanja kvantnih algoritama teško se može garantirati sigurnost i kvaliteta dostavljenih algoritama. Kroz ovo natjecanje očekivao se odabir više kandidata, umjesto jednog. Kandidati su mogli imati potpuno različite atribute dizajna i matematičke temelje, što je otežalo izravnu usporedbu kandidata. NIST je također najavio kako će se zahtjevi i vremenski okviri natjecanja potencijalno mijenjati na temelju kontinuiranog istraživanja područja [24].

4.1 Selekcijski kriteriji

Glavni selekcijski kriteriji naglašeni za NIST-ovo PQC natjecanje su [24]:

[5]Post-kvantna kriptografija, engl. *Post-Quantum Cryptography*

1. Sigurnost - protiv klasičnih i kvantnih napada,
2. Performanse - mjerene na raznim "klasičnim" platformama,
3. Ostala svojstva - kompatibilnost s postojećim protokolima i mrežama, jednostavnost i fleksibilnost, otpornost na zlouporabu i tako dalje.

Sigurnost je NIST-ov najbitniji kriterij podijeljen u pet različitih kategorija prikazanih na tablici 4.1. Svaka kategorija postavlja minimalne potrebne računalne resurse za razbijanje poznatih simetričnih blokovnih šifri ili hash funkcija, gdje razbijanje blokovne šifre označava uspješan *brute-force* napad pretraživanja ključa (engl. *exhaustive key search*), a razbijanje hash funkcije uspješan *brute-force* napad kolizije (engl. *collision search*).

Tablica 4.1 Kategorije sigurnosti algoritama PQC natjecanja

Kategorija	Opis
I	Barem jednako teško razbiti kao AES128 (exhaustive key search)
II	Barem jednako teško razbiti kao SHA256 (collision search)
III	Barem jednako teško razbiti kao AES192 (exhaustive key search)
IV	Barem jednako teško razbiti kao SHA384 (collision search)
V	Barem jednako teško razbiti kao AES256 (exhaustive key search)

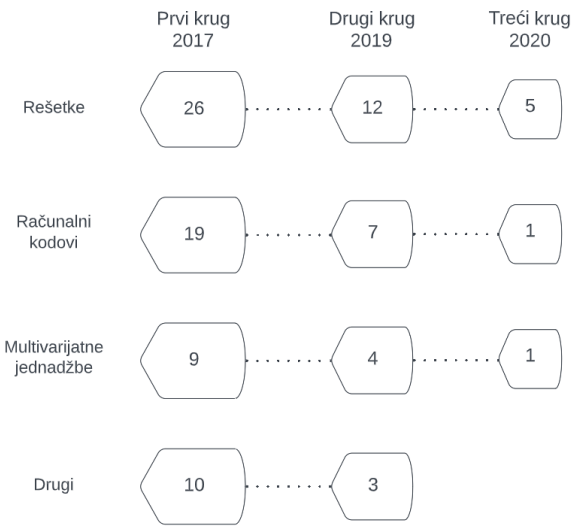
NIST je kod poziva na sudjelovanje preporučio podnositeljima da se prvenstveno usredotoče na parametre koji ispunjavaju zahtjeve iz prve, druge i/ili treće kategorije, jer će takvi algoritmi pružiti dovoljnu sigurnost u bližoj budućnosti. Uz to, podnositelji su trebali osigurati barem jedan skup parametara koji pruža višu razinu sigurnosti, odnosno razinu iznad treće kategorije, kako bi sustavi mogli ostati zaštićeni i od budućih otkrića u kriptoanalizi i računalnoj tehnologiji općenito [25].

4.2 Tijek natjecanja

U prosincu 2017. godine, NIST je objavio kako se na natjecanje prijavilo 82 podnositelja, od kojih njih 13 nije potpuno i pravilno podnijelo svoje rješenje, a

petero njih je naknadno odustalo od natjecanja. Od 64 preostale pravilne i potpune prijave, njih 19 bilo je za digitalno potpisivanje, a ostalih 45 za PKE/KEM rješenja [24]. Sudjelovali su znanstvenici iz 25 različitih zemalja svijeta te su koristili različite tehnike iz brojnih matematičkih područja, uključujući rešetke, kodove za ispravljanje pogrešaka, multivarijatne jednadžbe, hash funkcije, eliptične krivulje i druge [4].

Do siječnja 2019., NIST se odlučio za 26 kandidata koji su prešli u drugi krug natjecanja. U srpnju 2020. godine, više od 18 mjeseci nakon odabra kandidata za drugi krug, NIST je objavio finaliste natjecanja: 4 PKE/KEM algoritma i 3 sheme za digitalno potpisivanje. Prikaz natjecatelja po kategorijama kroz tri kruga natjecanja nalazi se na slici 4.1, a popis finalista i njihovih matematičkih podloga vidljiv je u sklopu tablice 4.2.



Slika 4.1 Rezime natjecatelja po kategorijama kroz tri kruga natjecanja [26]

NIST-u je bilo u cilju odabrati jednog ili više finalista koji će se koristiti za PQC standardizaciju do kraja trećeg kruga natjecanja. Alternative (njih 8) su se izabrale za daljnje promatranje, s pretpostavkom da će neki od tih algoritama biti standardizirani nakon četvrtog kruga evaluacija. Odabrani alternativni algoritmi sadrže kombinacije poželjnih karakteristika i nekih značajnijih nedostataka, na primjer mogu biti vrlo sigurni, ali neučinkoviti ili im nedostaje potrebna razina izloženosti kriptoanalizi [26]. Popis alternativnih algoritama nalazi se u tablici 4.3.

Tablica 4.2 Popis finalista PQC-a

	Naziv kandidata	Vrsta
PKE/ KEM	Classic McEliece	Računalni kodovi
	CRYSTALS-Kyber	Rešetke
	NTRU	Rešetke
	SABER	Rešetke
Digitalni potpis	CRYSTALS-Dilithium	Rešetke
	FALCON	Rešetke
	Rainbow	Multivarijatne jednadžbe

Tablica 4.3 Popis alternativnih finalista PQC-a

	Naziv alternativnog kandidata	Vrsta
PKE/ KEM	FrodoKEM	Rešetke
	NTRU Prime	Rešetke
	BIKE	Računalni kodovi
	HQC	Računalni kodovi
	SIKE	Eliptične krivulje
Digitalni potpis	SPHINCS+	Hash funkcije
	GeMSS	Multivarijatne jednadžbe
	Picnic	Dokaz nultog znanja[6]

4.3 PKE/KEM algoritmi

Postoje tri sigurnosna pojma kojima se opisuju PKE i KEM algoritmi, gdje se prva dva pojma odnose na PKE, a treći na KEM algoritme [23].

- IND-CPA (engl. *ciphertext-indistinguishability under chosen plaintext attacks*) je sigurnosni pojam kojim se osigurava će sve informacije o čistom tekstu poruke (osim duljine) biti skrivene od napadača kojem je šifrat poznat. Ovo je modelirano tako da se napadaču daju na biranje dvije poruke. Nasumično se

jedna od te dvije poruke šifrira, a njen šifrat podijeli s napadačem. Napadač tada mora odlučiti koja je poruka šifrirana. IND-CPA sigurnost postiže se nasumičnim PKE-om gdje algoritam istu poruku nikad ne šifrira u isti šifrat.

- OW-CPA (engl. *one-wayness under chosen plaintext attacks*) je sigurnosni pojam koji govori da se šifriranjem nasumične poruke (koju nije odabrao napadač) ne može dobiti izvorni tekst poruke. Ovo je slabiji sigurnosni pojam od IND-CPA pojma, a postiže se determinističkim PKE-om (dPKE) gdje šifriranje poruke fiksnim javnim ključem uvijek rezultira istim šifratom.
- IND-CCA (engl. *key-indistinguishability under chosen ciphertext attacks*) je sigurnosni pojam kojim sve informacije o enkapsuliranom ključu ostaju skrivene od napadača, i u slučaju da je napadaču poznat šifrat. Ovakva sigurnost postignuta je tako što se napadaču daje šifrat i ključ sesije, gdje ključ sesije može biti onaj vraćen enkapsulacijom nakon generiranja šifrata ili nasumično odabran ključ sesije neovisan o šifratu. Napadač bi trebao znati podrijetlo ključa sesije.

4.4 SIGNATURE algoritmi

PQC sustavi za digitalne potpise (DSS, engl. *digital signature scheme*) sastoje se od tri algoritma [23]:

- algoritam za generiranje ključeva koji generira par ključeva (javni i tajni ključ),
- algoritam za potpisivanje koji izrađuje potpis pomoću poruke i tajnog ključa,
- verifikacijski algoritam koji uz pomoć poruke, potpisa i javnog ključa potvrđuje ispravnost digitalnog potpisa

Uobičajeni pojam sigurnosti za DSS-ove je EUF-CMA (engl. *Existential Unforgeability under Chosen Message Attacks*), a označava sigurnost protiv aktivnih napadača. EUF-CMA označava razinu sigurnosti na kojoj je napadaču teško krivotvoriti potpis bilo koje poruke koju nije potpisao vlasnik tajnog ključa [23].

Poglavlje 5

Algoritmi bazirani na rešetkama

Najveći potencijal od svih kriptografskih sustava koji bi se mogli oduprijeti kvantnom napadu su algoritmi bazirani na rešetkama. Takvi sustavi imaju snažne dokaze sigurnosti te poprilično jednostavnu implementaciju i intuitivnost, što govori i činjenica da još uvijek nije otkriven kvantni algoritam koji bi mogao probiti sustav baziran na rešetkama [19].

Dvadeset i šest od početno prijavljenih 69 algoritama (slika 4.1) su algoritmi bazirani na rešetkama, a od algoritama koji su došli do finalnog kruga, čak njih pet od sedam (tablica 4.2). Svih pet finalista se oslanja na (varijante) SVP[1] ili LWE[2] problema te nude konkurentne performanse gledajući zahtjeve brzine i propusnosti [4].

Kada se uspoređuju algoritmi bazirani na rešetkama s ostalim kandidatima, oni su jedina vrsta koja nudi rješenja za šifriranje i digitalno potpisivanje te su među najbržima u obje kategorije. Iako postoje specijalizirani prijedlozi koji bi mogli pružiti bolje performanse u određenim područjima, algoritmi koji se baziraju na rešetkama imaju konkurentne performanse u zahtjevima propusnosti (engl. *bandwidth requirements*), što ih čini favoritima za opću upotrebu [4].

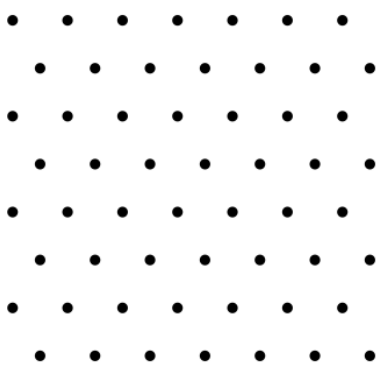
[1]Poznat kao "Problem najkraćeg vektora", opisan u poglavlju 5.1.1
[2]engl. *Learning With Errors*, opisan u poglavlju 5.1.2

5.1 Rešetke

Rešetka je skup svih točaka u n dimenzionalnom prostoru koji se sastoji od n nezavisnih vektora dobiven cjelobrojnim linearnim kombinacijama tih vektora. Na slici 5.1 može se vidjeti struktura takvog skupa točaka koja se definira kao:

$$L(b_1, ..., b_n) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}, \tag{5.1}$$

gdje su $b_1, ..., b_n$ linearno nezavisni vektori iz $\mathbb{R}^n$. Vektori $b_1, ..., b_n$ predstavljaju bazu rešetke L. Baza se može zapisati pomoću matrice vektora $B = (b_1, ..., b_n)$, gdje vrijedi da je rešetka $L(B) = \{Bx : x \in \mathbb{Z}^n\}$ [19].

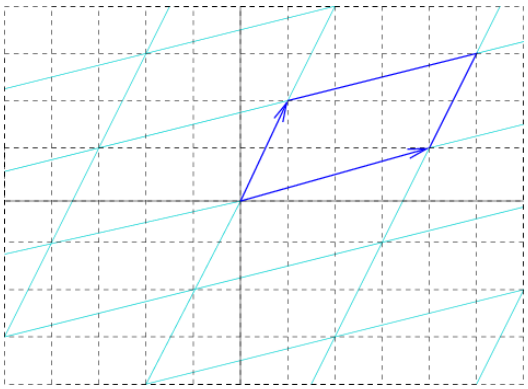


Slika 5.1 Dvodimenzionalna rešetka [19]

Fundamentalno područje rešetke $L \subseteq \mathbb{R}^n$ je n-dimenzionalni paralelopiped definiran pomoću vektora baze L. Područje je vidljivo na slici 5.2.

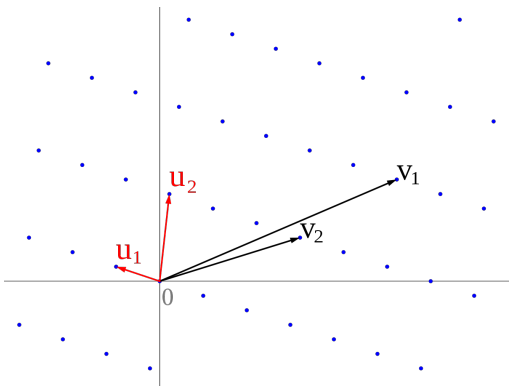
Neka konkretna rešetka $L(B)$ može imati beskonačno baza B (n-dimenzionalnih matrica) za koje vrijedi $L(B) = L(BU)$, gdje je U proizvoljna n-dimenzionalna unimodularna matrica. Različite baze imaju fundamentalno područje jednake površine ako definiraju identičnu rešetku, što se dobije iz činjenice da je $det(U) = 1$. Suština problema rešetki jesu razlike među bazama iste rešetke.

Baze rešetke mogu biti *dobre* ili *loše*, gdje dobre baze predstavljaju one s niskim dualnim ortogonalnim defektom, a loše s velikim defektom. Dobre baze imaju kratke,



Slika 5.2 Fundamentalno područje rešetke [19]

gotovo ortogonalne vektore poput u_1 i u_2 na slici 5.3. Vektori V_1 i V_2 su primjeri loše baze, a rešetke s lošom bazom su izrazito teške za riješiti. Prisustvo kratkih vektora je ključno za rješavanje problema vezanih za rešetke, a kratki vektori $v \in \mathbb{R}^n$ postoje za svaku rešetku L jer vrijedi $||v|| \leq \sqrt{n} \times det(B)^{1/n}$ (Minkowskijev teorem) [19].



Slika 5.3 Jedna rešetka definirana dvjema različitim bazama [19]

5.1.1 Problem najkraćeg vektora

Problem najkraćeg vektora (engl. *Shortest Vector Problem*, SVP) predstavlja problem pronalaska najkraćeg ne-nul vektora rešetke ako je dana loša baza rešetke.

Do danas nije pronađen ni jedan učinkoviti algoritam koji bi mogao riješiti problem, a najbliže su došli znanstvenici Arjen Lenstra, Hendrik Lenstra i László Lovász predstavljanjem LLL algoritma 1982. godine koji u polinomijalnom vremenu (vremenska složenost $2^{O(n)}$) može pronaći aproksimaciju najkraćeg vektora [19].

Javni ključevi koji se temelje na SVP-u mogu biti preveliki za svakodnevnu upotrebu, što je dovelo do realizacije blaže varijante problema koja zahtjeva pronalazak vektora koji je maksimalno γ veći od najkraćeg vektora. Odabir faktora γ utječe na SVP-ovu težinu i zbog toga je izuzetno bitan. Problem je NP-težak za one faktore manje od $n^{O(1/loglog(n))}$. Za faktore veće od $\sqrt{n/log(n)}$ problem nije NP-težak [19].

5.1.2 LWE problem

LWE (engl. *Learning with Errors*) problem, odnosno problem učenja s greškama, se bazira na rješavanju sustava jednadžbi, gdje se namjerno ubaci pogreška kod generiranja sustava, što čini problem izuzetno teškim, čak i za kvantna računala. LWE problem se može svesti na jednadžbu:

$$B = As + e \ mod \ q, \tag{5.2}$$

gdje A i B predstavljaju poznate vrijednosti (javne ključeve), s vrijednost koju je gotovo nemoguće odrediti (tajni ključ), e je namjerno ubačena pogreška, a q veliki prosti broj [27].

Postoje dvije vrste LWE-a koje koriste PQC sustavi, a to su:

- Obični LWE - minimalne je strukture koja omogućava jednostavnu skalabilnost, uz izdatak smanjivanja cjelokupne učinkovitosti.
- Prstenasti LWE (engl. *Ring LWE*, RLWE)- ima veliku učinkovitost u područjima brzine i veličine ključa i šifrata, no nedostatak je što s povećanom algebarskom strukturom algoritma mehanizam postaje ranjiv na napade, zbog čega dolazi do problema skalabilnosti između efikasnosti i sigurnosti.

5.2 PKE/KEM finalisti

5.2.1 CRYSTALS-Kyber

CRYSTALS-Kyber je skup algoritama za razmjenu ključeva, a sigurnost postiže korištenjem LWE problema. Kyber se koristi jednadžbom 5.2, gdje za A koristi matricu, a preostale varijable su vektori. Budući da obje vrste LWE-a (obična i prstenasta) imaju svojih prednosti i nedostataka, Kyber koristi modularni LWE (MLWE), čija je struktura smanjena u odnosu na LWE, ali je skalabilnost puno bolja.

Kyber je također IND-CCA2 siguran sustav, a takvi sustavi se još nazivaju i aktivno sigurnim sustavima, što podrazumijeva otpornost na aktivne napadače koji se nalaze u komunikacijskom kanalu te na pasivne koji samo prisluškuju. IND-CCA2 osigurava da promjena šifrata ne vodi predvidljivoj izmjeni dešifriranog teksta [27].

Svojstva

Budući da algoritam u većini koraka koristi brze varijante diskretne Fourierove transformacije (DFT), performanse ovise o korištenim kriptografskim primitivima. Kriptografski primitivi CRYSTALS-Kybera dolaze iz Keccak porodice algoritama, što označava velike brzine izvršavanja na računalima čija sklopovska podrška podržava takve kriptografske funkcije [27].

Sigurnost

CRYSTALS-Kyber dolazi u tri varijante, gdje svaka predstavlja određenu razinu sigurnosti. To su po jačini redom: Kyber512, Kyber768 i Kyber1024, a prikazane su u tablici 5.1 zajedno s *core-SVP*[3] vrijednostima. Postoje dva načina za "slomiti" Kyber: pronalazak i iskorištavanje grešaka u kriptografskim primitivima Kybera ili rješavanjem modularnog LWE problema. Izvedba oba slučaja je vrlo teška.

[3]Jedna od procjena NIST-ovog PQC natjecanja za algoritme bazirane na rešetkama

Tablica 5.1 Sigurnosne značajke CRYSTALS-Kyber sustava

	core-SVP (klasično)	core-SVP (kvantno)	Razina sigurnosti
Kyber512	111	100	1 (AES-128)
Kyber768	181	164	3 (AES-192)
Kyber1024	254	230	5 (AES-256)

Prednosti i nedostaci

Kyberov sustav postiže zadovoljavajuće brzine uz pomoć brzih Fourierovih transformacija i Keccakovih algoritama, te su performanse izvrsne pri svakom nivou implementacije. Sigurnosno svojstvo IND-CCA2 donosi dodatnu razinu sigurnosti sustava. Kyber algoritam je izrazito skalabilan radi činjenice da je dovoljna samo promjena dimenzije matrice kako bi se povećala razina sigurnosti.

5.2.2 NTRU

NTRU[4] je strukturirani PKE kriptosustav baziran na rešetkama, a osmislili su ga znanstvenici Hoffstein, Piper i Silverman 1996. godine. Sustav se temelji na SVP-u, a radi pomoću prstena polinoma. NTRU je IND-CCA2 siguran kriptosustav koji se temelji na teškom problemu rješavanja prstenastog LWE-a. Nekoliko kandidata temeljenih na originalnom NTRU kriptosustavu se prijavilo u prvi krug NIST-ovog natjecanja, a kandidat koji je došao do trećeg kruga i kojeg se opisuje ovim poglavljem zapravo je rezultat spajanja dva kandidata: NTRUEncrypt i NTRUHRSS-KEM [28].

Svojstva

Osnovna verzija NTRU šifriranja implementira se pomoću polinoma iz prstena $R = \mathbb{Z}_q[x]/(x^n - 1)$, gdje je q potencija broja dva. Dva polinoma f i g generirana su privatnim koeficijentima iz skupa $\{-1, 0, 1\}$ te javnim ključem $h = g \cdot f^{-1}$ iz R. Za šifriranje poruke m, predstavljene polinomom iz R s $\{-1, 0, 1\}$-koeficijentima, pošiljatelj izračunava $c = 3hr + m$, gdje je $r \in R$ polinom nasumično odabranih

[4]engl. *N-th degree TRUncated polynomial ring*

koeficijenata iz skupa $\{-1, 0, 1\}$. Kako bi se poruka m dešifrirala, vlasnik tajnog ključa izračunava $e = cf \ mod \ q$ pomoću kojeg dobiva poruku $m = e \cdot f^{-1} \ mod \ 3$ [29].

NTRU verzija NTRU-HPS koristi fiksne težinske prostore uzoraka za generiranje polinoma, gdje fiksna težina znači da kad se gledaju koeficijenti (koji su svi izvučeni iz skupa $\{-1, 0, 1\}$), broj ukupnih jedinica (1) i negativnih jedinica (-1) je fiksna vrijednost. S druge strane, NTRU-HRSS verzija koristi proizvoljne nasumične težinske prostore uzoraka, što znači da je svaki koeficijent ravnomjerno i nasumično odabran iz skupa $\{-1, 0, 1\}$.

Sigurnost

NTRU PKE kriptosustav nije IND-CCA siguran, ali zato kao i drugi KEM kandidati NIST-ovog PQC natjecanja koristi varijaciju Fujisaka-Okamoto transformacije za pretvaranje PKE-ova u IND-CCA2 sigurne KEM-ove [29]. NTRU koristi SXY transformaciju, koja predstavlja ponovno šifriranje podataka kako bi se provjerio izlaz dešifriranja i ispis slučajne vrijednosti kad provjera ne uspije. Rezultat korištenja transformacije je taj što napadač ne bi dobio nikakve korisne informacije gledajući rezultat kad je krivi šifrirani tekst unesen u funkciju dekapsulacije.

Tablica 5.2 Veličina ključeva i šifrata (u bitovima) NTRU varijacija [29]

	Javni ključ	Tajni ključ	Šifrat	Razina sigurnosti
NTRU-HPS2048677	930	1234	930	1. razina
NTRU-HRSS701	1138	1450	1138	1. razina
NTRU-HPS4096821	1230	1590	1230	3. razina
NTRU-HPS40961229	1842	2366	1842	5. razina
NTRU-HRSS1373	2401	2983	2401	5. razina

NTRU je uspješno preživio posljednjih dvadesetak godina kriptoanalize, što daje veliko povjerenje u njegovu sigurnost. Složenost najboljih napada na NTRU određena je složenošću algoritma redukcije rešetke, a složenost algoritama ovisi o složenosti SVP-a [23].

Prednosti i nedostaci

KEM NTRU-a je savršeno ispravan, što znači da je garantirana sto postotna ispravnost kod dešifriranja. Šifriranje i dešifriranje su također zadovoljavajućih brzina zato što su glavne operacije korištene u NTRU kriptosustavu efikasna množenja polinoma[30]. Generiranje ključeva je sporije od sustava koji se koriste RLWE i MLWE shemama jer je za generiranje potrebna polinomska podjela (engl. *polynomial division*).

5.2.3 SABER

SABER je skupina kriptografskih algoritama koji se baziraju na *Module Learning With Rounding* problemu (M-LWR). Taj problem razlikuje se od LWE problema prema načinu na koji su jednadžbe aproksimirane. U LWE-u dodaje se mala pogreška, a u LWR-u pogreške se zaokružuju na manji modulo. LWR i LWE problemi su iste sigurnosne razine no LWR ipak ima dvije prednosti: robusniji je jer se zaokruživanjem smanjuje veličina ključeva i veličina šifrata te je jednostavniji i učinkovitiji jer ne treba uzorkovati pogreške iz distribucije [30].

SABER je strukturirani KEM algoritam baziran na rešetkama, a razvila ga je istraživačka skupina u sklopu COSIC-a[5] u Belgiji: D'Anvers, Karkmakar, Sinha Roy i Vercautren. Postoje tri varijante SABER-a: LightSABER (prva NIST-ova sigurnosna razina), SABER (treća sigurnosna razina) i FireSABER (peta sigurnosna razina).

Svojstva

Cjelobrojni moduli SABER-a potencije su broja 2 što omogućuje ostvarenje glavnih ciljeva sustava: jednostavnost, djelotvornost i fleksibilnost. Upotrebom LWR problema, broj nužnih generiranja slučajnih varijabli je prepolovljen u odnosu na LWE sheme, čime se smanjuje propusnost, a struktura sustava pruža fleksibilnost ponovnom upotrebom temeljene komponente.

[5]Grupa za računalnu sigurnost i industrijsku kriptografiju, engl. *Computer Security and Industrial Cryptography group*

SABER-ov PKE sustav, odnosno način šifriranja javnim ključem, sastoji se od tri algoritma: Saber.PKE.KeyGen (algoritam za generiranje javnog ključa), Saber.PKE.Enc (algoritam za šifriranje javnim ključem pri čemu se koristi zadani argument r) i Saber.PKE.Dec (algoritam za dešifriranje javnim ključem).

KEM sustav za enkapsulaciju ključem također sadrži tri algoritma: Saber.KEM.KeyGen (algoritam za generiranje ključa), Saber.KEM.Enc (algoritam za enkapsulaciju ključa pomoću Saber.PKE.Enc algoritma) i Saber.KEM.Dec (algoritam za dešifriranje ključa pomoću Saber.PKE.Dec algoritma).

Sigurnost

PKE sustav SABER-a je IND-CPA siguran način šifriranja koji se kasnije pretvara u KEM, čija je sigurnost enkapsulacije označena IND-CCA razinom, koja se postiže uz pomoć Fujisaki-Okamoto transformacija.

Pretvorba sažetka javnog ključa u vektor jamči ovisnost ključa o unosu obje strane čime se nudi višestruka zaštita. Pretvorba se događa u stalnom vremenu što označava dobru obranu protiv napadača koji se koriste podacima o vremenu zadanih izračuna pomoću kojih bi dobili podatke o dugotrajnom tajnom ključu [27]. U tablici 5.3 prikazane su vrijednosti sigurnosti za PKE i KEM varijante SABER sustava.

Tablica 5.3 Sigurnosne značajke SABER sustava

	core-SVP (klasično)	core-SVP (kvantno)	Razina sigurnosti
LightSaber-PKE	2^{118}	2^{107}	1 (AES-128)
Saber-PKE	2^{189}	2^{172}	3 (AES-192)
FireSaber-PKE	2^{260}	2^{236}	5 (AES-256)
LightSaber-KEM	2^{118}	2^{107}	1 (AES-128)
Saber-KEM	2^{189}	2^{172}	3 (AES-192)
FireSaber-KEM	2^{260}	2^{236}	5 (AES-256)

Prednosti i nedostaci

Iako povećanje dimenzija problema rešetke povećava sigurnost, istovremeno se smanjuje i točnost sustava. Prednost SABER sustava je što osigurava da napadač ne može unaprijed izračunati slabe vrijednosti za vrijeme traženja grešaka u dešifriranju. Velika prednost je što sustav također ne koristi kodove za ispravljanje pogrešaka, čime izbjegava napade koji su povezani s maskiranjem bloka za ispravljanje pogrešaka [27].

5.3 SIGNATURE finalisti

5.3.1 CRYSTALS-Dilithium

CRYSTALS-Dilithium je jedan od dva finalista za digitalno potpisivanje koji se bazira na rešetkama. Dilithium koristi Fiat-Shamir i Aborts radne okvire te SVP. Varijante Dilithiuma su: Dilithium , Dilithium 3 i Dilithium 4, gdje redom odgovaraju prvoj, drugoj i trećoj sigurnosnoj kategoriji NIST-ovog natjecanja [31].

Svojstva

Dilithium koristi prsten $R_q := \mathbb{Z}_q[X]/(X^{256} + 1)$, gdje je q prosti broj jednak $2^{23} - 213 + 1$. Javni ključ Dilithiuma je modularni LWE oblika $(A, t := As_1 + s_2)$, gdje A predstavlja matricu nad R_q, a s_1 i s_2 vektore grešaka nad R_q.

Posebna značajka Dilithiuma je njegova distribucija pogrešaka. Dok algoritmi za digitalno potpisivanje bazirani na rešetkama koriste skraćenu Gaussovu distribuciju za izračun koeficijenata svojih vektora pogrešaka, Dilithium koristi uniformnu distribuciju preko $\{\eta, -\eta + 1, ..., \eta\}$, gdje je η mali pozitivni cijeli broj.

Algoritam je temeljen na "Fiat-Shamir s prekidima" (engl. *Fiat-Shamir with aborts*) pristupu IMB-ovog znanstvenika Vadima Lyubashevskyog. Središte ovog pristupa je identifikacijska shema zasnovana na tri poruke temeljene na rešetkama koje omogućuju provjeru nositelja tajnog ključa (s_1, s_2) bez otkrivanja ključa. Nositelj tajnog ključa izračunava vektor w koji se sastoji od bitova visokog reda od Ay (za slučajni y) i šalje ga na verifikaciju. Algoritam verifikacije odgovara s polinomom

slučajnog izazova (engl. *random challange polynomial*) $c \in \mathbb{R}$ koji se sastoji od malih koeficijenata. Nositelj tajnog ključa povratno šalje vektor $z := y + cs_1$, gdje z može slučajno odati informacije o s_1. Zbog toga, dodaje se korak odbijanja uzorkovanja kako bi se osiguralo da su koeficijenti od z ispravne veličine. Verifikacija vektora je valjana ako se može dokazati da je $Az \approx w + ct$.

Kao što je prethodno navedeno, da bi se dobila shema potpisa potrebno je primijeniti Fiat-Shamirovu transformaciju, gdje nositelj tajnog ključa generira s hashiranjem vektora w zajedno s porukom μ. Dilithiumova shema uključuje i nekoliko dodatnih optimizacija: javni ključ je komprimiran korištenjem pseudoslučajnosti i izostavljanjem više od polovice bitova nižeg reda t. Kako bi se nadoknadili bitovi koje je potpisnik "ispustio", kao dio svakog potpisa, šalju se i "savjeti" (engl. *hints*) koji omogućuju algoritmu verifikacije ispravnu provjeru potpisa [29].

Sigurnost

Sigurnosti Dilithiuma temeljena je na MLWE-u, koji osigurava da se nikakve informacije o tajnom ključu ne mogu dobiti kroz javni ključ. Kao i kod drugih algoritama koji se baziraju na rešetkama, najpoznatiji napadi na Dilithium se svode na korištenje generičkih algoritama za pronalazak najkraćih vektora (SVP) u rešetkama. Na tablici 5.4 vidljive su duljine ključeva. Dilithium nudi niz opcija za različite parametre kako bi se povećala sigurnost po cijenu povećanja veličine ključeva i/ili sporijeg izvršavanja [29].

Tablica 5.4 Veličina ključeva i potpisa (u bitovima) Dilithium kriptosustava [29]

	Javni ključ	Tajni ključ	Šifrat	Razina sigurnosti
Dilithium	1312	2528	2420	1. razina
	1952	4000	3293	3. razina
	2592	4864	4595	3. razina

Prednosti i nedostaci

CRYSTALS-Dilithium je algoritam za digitalno potpisivanje koji je jako siguran pod odabranim napadima poruka na temelju teškoće rješavanja problema rešetki [28]. Za razliku od drugih prijedloga aglgoritama za digitalno potpisivanje, Dilitihium upotrebljava uniformnu distribuciju, izbjegavajući složeno i neučinkovito uzorkovanje iz diskretne Gaussove distribucije. Modularna struktura Dilithiuma osigurava da se množenje polinoma uvijek izvodi u istom prstenu bez obzira na razinu sigurnosti, što olakšava prebacivanje između njih. Množenje se može izvesti učinkovito zahvaljujući NTT[6] prijateljskim parametrima. Primjenjujući trik za komprimiranje javnog ključa s faktorom dva, Dilithium ima najmanji javni ključ i veličinu potpisa među shemama temeljenim na rešetkama koje koriste uniformno uzorkovanje [23].

5.3.2 FALCON

FALCON (engl. *Fast Fourier Lattice-based Compact Signatures over NTRU*) je algoritam za digitalno potpisivanje baziran na rešetkama koje koriste *"hash-and-sign"* paradigmu [29].

Svojstva

FALCON se temelji na GPV okviru, kojeg su 2007. godine predstavili Gentry, Peikert i Vaikuntanathan, a služi za konstruiranje *hash-and-sign* shema za digitalno potpisivanje pomoću *trapdoor* funkcija baziranih na rešetkama s uzorkovanjem preslike. FALCON se temelji na nizu funkcija čiji je cilj učinkovito instancirati GPV pristup u NTRU rešetkama, s fokusom na kompaktnost javnog ključa i potpisa. Instanciranje NTRU rešetki u FALCON shemi je poprilično jednostavno, sa setom polinoma $f, g, F, G \in \mathbb{Z}[x]/(x^n+1)$, gdje je $fG-gF = q$ i javnim ključem $h = g \cdot f^{-1}$. Konkretno, tajna je skup polinoma f,g,F,G Z[x]/(x n + 1) tako da je $fGgFq$, a javni ključ je $hg \cdot f$. Za ispravno generirane tajne, h je nasumičan, a baze koje generiraju

[6]Generalizacija klasičnog DFT-a nad konačnim poljima, engl. *Number Theoretic Transform*

rešetku su sljedeće:

$$\begin{bmatrix} 1 & h \\ 0 & q \end{bmatrix} \text{ i } \begin{bmatrix} f & g \\ F & G \end{bmatrix}. \tag{5.3}$$

FALCON koristi složene strukture podataka poput FALCON stabala, što ga čini znatno zahtjevnijim za implementirati od drugih algoritama baziranih na rešetkama.

Sigurnost

Tablica 5.5 Veličina ključeva i potpisa (u bitovima) FALCON kriptosustava [29]

	Javni ključ	Tajni ključ	Šifrat	Razina sigurnosti
FALCON-512	897	7553	666	1. razina
FALCON-1024	1793	13 953	1280	5. razina

Prednosti i nedostaci

Jedna od prednosti FALCON-a je što nudi najmanji *bandwidth* (veličina javnog ključa i potpisa) od svih shema iz trećeg kruga algoritama za digitalno potpisavanje. FALCON je također učinkovit u potpisivanju i verifikaciji, iako je generiranje ključeva sporije. FALCON se lako može implementirati u postojeće protokole i aplikacije te nudi vrlo dobre globalne performanse. [32]

Poglavlje 6

Algoritmi bazirani na računalnim kodovima

Kriptografija bazirana na računalnim kodovima temelji se na teoriji kodova za ispravljanje pogrešaka (engl. *error-correcting codes*). Kodovi za ispravljanje pogrešaka koriste se kako bi se postigla kontrola pogrešaka u podacima koji putuju kroz nepouzdane komunikacijske kanale. Cilj ovakve kriptografije je namjerno ubacivanje grešaka među podatke, kako bi samo nositelju tajnog ključa bilo omogućeno iste identificirati i/ili ukloniti [4].

Kriptografija bazirana na računalnim kodovima je prvi put bila predložena prije više od 40 godina (1978. godine) kao shema za šifriranje od strane američkog znanstvenika Roberta McEliecea.

Svi algoritmi za digitalno potpisivanje bazirani na računalnim kodovima koji su se prijavili na NIST-ovo PQC natjecanje bili su "slomljeni". Šest PKE/KEM algoritama dospjelo je u drugi krug natjecanja, ali njih četiri (Rollo i RQC[1] te LEDAkem i LEDAcrypt[2]) nije došlo do trećeg kruga. Preostali kandidati temeljeni na računalnim kodovima su klasični McEliece (engl. *classic* McEliece), BIKE i HQC. Klasični McEliece je postao jedan od četiri PKE/KEM finalista, dok su BIKE i HQC ušli u treći krug kao alternativni kandidati. BIKE i HQC koriste specifične kodove po-

[1]engl. *Rank-metric codes*
[2]engl. emphLow-denisity paritycheck codes

moću kojih se smanjuje dužina javnog ključa, što se smatra glavnim nedostatkom algoritama baziranih na računalnim kodovima [23].

6.1 Linearni kodovi

$[n, k]$-linearni kod C je k-dimenzionalni linearni potprostor konačnog polja $\mathbb{F}^n$ veličine n. Kod C je duljine n i dimenzije k, gdje se u slučaju McElieceovog sustava govori o binarnim linearnim kodovima nad poljem $\mathbb{F}_2$. Kodne riječi se prikazuju kao bit-vektori[3] [33].

Hammingova težina kodne riječi $x \in \mathbb{F}_2^n$, označena kao $wt(x)$ predstavlja konačan broj koordinata koje su različite od nule. Broj koordinata je jednak udaljenosti od nultog vektora: $wt(x) = d(x, 0)$.

Hammingova udaljenost između dvije kodne riječi $x = x1_{,}..., x_n$ i $y = y_1, ..., y_n$ definirana je kao:

$$d(x, y) = \sum_{i=1}^{n} d(x_i, y_i), \text{ gdje vrijedi } (x_i, y_i) = \begin{cases} 1 & x_i \neq y_i \\ 0 & x_i = y_i \end{cases} . \tag{6.1}$$

Udaljenost koda C se označava kao minimalna Hammingova udaljenost bilo koje dvije različite kodne riječi od C:

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y). \tag{6.2}$$

Ako je C $[n, k]$-linearni kod s udaljenošću d, onda se C naziva $[n, k, d]$-linearnim kodom.

Generator matrice (engl. *generator matrix*) G $[n, k]$-linearnog koda C je $k \times n$ matrica čiji redci čine osnovu koda C. Generator matrice za linearni kod općenito nije jedinstvena, zato što svaka osnova koda C daje drugačiji, ali ekvivalentni generator matrice za C.

Vrijedi da $[n, k, d]$-linearni kod C s generatorom matrice G može ispraviti do t različitih pogrešaka, ako postoji algoritam za dešifriranje $Dec : \mathbb{F}^n \to C$ takav da za

[3]Jednodimenzionalni nizovi Booleovih vrijednosti

svaki $u \in \mathbb{F}^k$ i svaki vektor $e \in \mathbb{F}^n$ težine $wt(e) \leq t$, riječ $y = uG + e$ bude uvijek ispravno dešifrirana kao $Dec(y) = u$. Kod C se tada smatra kodom za ispravljanje pogrešaka [33].

Matrica permutacije (engl. *permutation matrix*) P je binarna matrica unutar koje svaki stupac i redak sadrži jednu jedinicu, a ostale ćelije su prazne (sadrže nulu). Rezultat množenja matrice permutacije s bilo kojom drugom matricom daje matricu koja sadrži iste stupce kao i izvorna, ali s permutiranim redoslijedom.

6.2 PKE/KEM finalisti

6.2.1 Klasični McEliece

Klasični McEliece je kriptosustav temeljen na računalnim kodovima koji koristi binarne Goppa kodove koji su bili inicijalno predloženi u radu američkog znanstvenika Roberta McEliecea 1978. godine. Ni 40 godina nakon objave McElieceovog algoritma, ne postoje učinkoviti napadi na taj sustav, kako klasični, tako ni kvantni. Klasični McEliece sustav obilježava javni ključ koji je definiran kao velika matrica.

Svojstva

Generiranje ključeva kod klasičnog McEliece kriptosustava započinje odabirom Goppa koda Γ s generatorom matrice G koji može ispraviti t pogrešaka. Odabiru se ne-singularna matrica S i nasumična matrica permutacije P te se izračuna $G' = SGP$. Javni ključ (G', t) se šalje kroz nesigurni kanal, a tajni ključ se čuva kao skup (S, G, P).

Enkripcija, odnosno šifriranje, se izvršava tako što se šifriranoj poruci u dodaje vektor pogreške e s težinom t. Poruka $y = uG' + e$ nastaje kao zbroj šifrirane poruke i vektora pogreške.

Dekripcija se vrši množenjem poruke y s P^{-1}, gdje P^{-1} predstavlja inverz matrice permutacije P. Vrijedi da je:

$$yP^{-1} = uSG + eP^{-1}, \text{ gdje vrijedi } ht(eP^{-1}) = ht(e) = t, \tag{6.3}$$

gdje uSG predstavlja kodnu riječ Goppa koda Γ, koja se može dešifrirati i dati poruku uS. Budući da je S invertibilna matrica, ista se pomnoži sa svojim inverzom i rezultat je poruka (čisti tekst) u [19].

Sigurnost

Klasični McEliece kriptosustav je jednosmjerni kriptosustav, što znači da napadač bez ikakvog znanja o jasnom tekstu (informaciji) ne može rekonstruirati nasumično odabranu kodnu riječ pomoću šifrata i javnog ključa. To svojstvo naziva se još i OW-CPA sigurnost. Kako bi postigao IND-CCA sigurnost, klasični McEliece koristi implicitnu verziju Fujisaki-Okamoto (FO) transformacije.

Ako napadač posjeduje šifriranu poruku c, mogao bi saznati jasni tekst (izvornu poruku) m na dva načina: [33]

1. Saznati G uz pomoć G'.
2. Dešifrirati c bez pomoći efikasnog algoritma za dešifriranje.

Napad opisan prvim načinom naziva se još i strukturalnim napadom, a drugi način znan je kao napad dešifriranja (engl. *decoding attack*). Sigurnost klasičnog McEliece kriptosustava je predložena pomoću NP-teških problema dešifriranja.

Opći problem dešifriranja linearnih kodova govori da je za dani $[n, k]$-linearni kod C i kodnu riječ $y \in \mathbb{F}^n$, potrebno pronaći kodnu riječ $c \in C$, gdje je udaljenost $d(y, c)$ minimalna.

Prednosti i nedostaci

Klasični McEliece ima vrlo velike javne i privatne ključeve, gdje se privatni ključ sastoji od tri velike matrice, te je poprilično sporo generiranje istih, zbog čega je nepoželjan za većinu okruženja. Poželjan odabir bi mogao biti u sustavima gdje se javni ključ može iskoristiti više puta i ne mora slati kod svake nove komunikacije. Od svih PQC kandidata, klasični McEliece ima najmanju veličinu šifrata [29]. McEliecevo šifriranje i dešifriranje je brže od tradicionalnog RSA, no veličina ključeva se kreće od 250 KB za varijantu prve kategorije sigurnosti NIST-ovog natjecanja do 1.3

MB za varijantu pete kategorije sigurnosti.

Poglavlje 7

Algoritmi bazirani na multivarijatnim kvadratnim polinomima

Kriptosustavi bazirani na multivarijatnim kvadratnim polinomima MVQ[1], svode se na rješavanje sustava jednadžbi drugog stupnja s dvije ili više nepoznatih varijabli nad konačnim poljima. Sustav baziran na MVQ shemi je takav da samo osoba s tajnim ključem može pronaći rješenje, što se postiže gradnjom jednadžbi posebne strukture i maskiranjem istih tako da napadaču izgledaju nasumično generirane [4].

U prvi krug NIST-ovog natjecanja, prijavljeno je bilo sedam MVQ shema za digitalno potpisivanje, od ukupno njih 19, te dva MVQ algoritma za šifriranje (slika 4.1). Do trećeg kruga uspješno su došla dva MVQ kandidata za digitalno potpisivanje, gdje je Rainbow ušao u treći krug kao finalist, a drugi kandidat, GeMSS, kao alternativno rješenje.

Bitna prednost MVQ shema za digitalno potpisivanje je generiranje malih potpisa. U nekim slučajevima te veličine su manje od RSA potpisa koji se koriste danas. MVQ sheme također pružaju brza potpisivanja. Jedan od nedostataka MVQ shema su veliki javni (a ponekad i privatni) ključevi, zbog čega nisu prikladne za opću upotrebu [4]. Drugi nedostatak je njihova novost. Većina početnih istraživanja multivarijatne kriptografije provedena je u Japanu pa je stoga i većina publikacija dostupna samo na japanskom. Istraživanje multivarijatne kriptografije od tada je u stalnom porastu i u

[1]engl. *Mutlivariate Quadratic*

ostalim krajevima svijeta, ali potrebno je puno više vremena da se dokaže sigurnost kriptosustava baziranih na multivarijatnoj kriptografiji [33].

7.1 Multivarijatni kvadratni polinomi

Multivarijatna polinomska kriptografija bazira se na poteškoćama rješavanja sustava multivarijatnih polinoma nad konačnim poljima. Većina multivarijatnih kriptosustava koristi kvadratne polinome i oslanja se na NP-teški MVQ problem. MVQ problem sastoji se od rješavanja multivarijatnog sustava kvadratnih jednadžbi nad konačnim poljem, uz dane koeficijente y_k, $a_i j^k$, b_i^k i c^k kako bi se pronašlo rješenje $(x_1, ..., x_n)$ za:

$$\begin{aligned} f_1(x_1, ..., x_n) = y_1 &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{(1)} x_i y_j + \sum_{i=1}^{n} b_i^{(1)} x_i + c^{(1)} \\ &\vdots \\ f_1(x_1, ..., x_n) = y_m &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{(m)} x_i y_j + \sum_{i=1}^{n} b_i^{(m)} x_i + c^{(m)} \end{aligned} \tag{7.1}$$

gdje je n broj varijabli, m broj jednadžbi, a k broj u rasponu od 1 do m. Svi koeficijenti su elementi konačnog polja $\mathbb{F}$ [33].

7.2 SIGNATURE finalisti

7.2.1 Rainbow

Rainbow je multivarijatna shema za digitalno potpisivanje koja koristi *hash-and-sign* paradigmu s HFE[2] modifikacijom. Rainbow je slojevita generalizacija neuravnotežene sheme ulje-ocat (engl. *oil-vinegar*, UOV) [29].

Rainbow kriptosustav predložili su znanstvenici Jintai Ding i Dieter Schmidt 2005. godine, a temelji se na UOV shemi znanstvenika Patarina [34]. UOV sheme

[2]engl. *Hidden Field Equations*

koriste dvije vrste varijabli, varijable ulja i varijable octa, kako bi se generirala multivarijatna kvadratna funkcija za koju se lako izračunaju preslike. Multivarijatna kvadratna funkcija Rainbow kriptosustava sadrži članove koji su kvadratni za varijable octa i članove koji su bilinearni za varijable ulja i octa. Funkcija ne sadrži članove koji su kvadratni isključivo u varijablama ulja, čime se postiže da vlasnik privatnog ključa može nasumično dodijeliti vrijednosti varijablama octa i linearno riješiti vrijednosti varijabli ulja [29].

Rainbow u osnovnoj konstrukciji definira slojeve različitih skupova varijabli ulja koje se mogu sekvencijalno rješavati, sloj po sloj. Multivarijatna kvadratna funkcija se izrađuje pomoću linearnih mapa kako bi se sakrila interna struktura. Korištenje slojeva u konfiguraciji Rainbow kriptosustava omogućava manje potpise i bržu verifikaciju od tradicionalnih UOV shema, no komplicira se struktura kriptosustava.

Struktura Rainbow kriptosustava nad konačnim poljem $\mathbb{F}_q$ je sljedeća. Definira se sustav $P = (P^{(1)}, ..., P^{(m)})$ multivarijatnih kvadratnih polinoma koji se sastoje od m jednadžbi i n varijabli:

$$P^{(k)}(x_1, ..., x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(k)} x_i y_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)}, \tag{7.2}$$

gdje je $k = 1, ..., m$, a koeficijenti $p_{ij}^{(k)}, p_i^{(k)}, p_0^{(k)} \in_R \mathbb{F}_q$. [33]

Glavna ideja generiranja ključa u MVQ shemi za digitalno potpisivanje je odabrati središnju funkciju multivarijatnih kvadratnih polinoma $F = (F^{(1)}, ..., F^{(m)}) : F_q^n \to F_q^m$, koji se mogu jednostavno invertirati. Nakon odabira središnje funkcije, biraju se dvije afinitetne ili linearne invertibilne funkcije $S : F_q^m \to F_q^m$ i $T : F_q^n \to F_q^n$ pomoću kojih se skriva struktura središnje funkcije F u javnom ključu. Kvadratna funkcija $P = S \times F \times T$ je sastavni dio javnog ključa koju je teško razlikovati od slučajnog sustava, a samim time i invertirati. Tajni ključ se sastoji od 3 funkcije (S, F, T) što omogućuje invertiranje javnog ključa P.

Svojstva

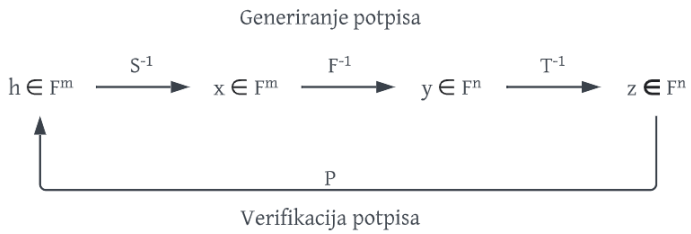
Kako bi se dokument d uspješno potpisao, hash funkcija $H : 0, 1 \to \mathbb{F}^m$ je korištena za izračun hasha $h = H(d) \in \mathbb{F}^m$. Potpis z generira se kroz sljedeća tri koraka

[33]:

1. Računa se $x = S^{-1}(h) \in \mathbb{F}^m$.
2. Preslika vrijednosti x izračunala se kroz središnju funkciju F kako bi nastao y. Preslika od x se izračunava posebnim algoritmom koji uzima vrijednost x i središnju funkciju F kao argumente, a vraća vektor $y \in \mathbb{F}^n$, gdje je $F(y) = x$.
3. Potpis $z \in \mathbb{F}^n$ se izračunava kao $z = T^{-1}(y)$

Za verifikaciju potpisa potrebni su dokument d i potpis z. Prvotno se izračunava hash vrijednost dokumenta: $h = H(d) \in \mathbb{F}^m$, a zatim $h' = P(z) \in \mathbb{F}^m$. Ako vrijedi $h = h'$, potpis z je valjan, odnosno verificiran.

Kroz sliku 7.1 prikazan je proces generiranja i verificiranja potpisa koristeći MVQ shemu za digitalno potpisivanje.



Slika 7.1 Proces generiranja i verificiranja potpisa koristeći MVQ shemu *[33]*

Rainbow kriptosustav dodaje poboljšanja prethodno opisanim osnovnim algoritmima za generiranje potpisa i verifikaciju kako bi se povećala sigurnost i brzina sustava. Na primjer, kako bi se olakšalo računanje, neki od nasumično odabranih $p_{ij}^{(k)}$ koeficijenata se mogu postaviti na nulu.

Sigurnost

Rainbow kriptosustav je kod prijave na NIST-ovo natjecanje predstavio tri varijante: Rainbow Ia, kriptosustav prve kategorije sigurnosti; Rainbow IIIc, kriptosustav treće kategorije sigurnosti i Rainbow Vc, kriptosustav pete kategorije sigurnosti.

U tablici 7.1 prikazane su veličine ključeva i potpisa u bitovima za sve tri prethodno spomenute varijante.

Tablica 7.1 Veličina ključeva i potpisa (u bitovima) Rainbow varijanti [29]

	Javni ključ	Tajni ključ	Potpis	Razina sigurnosti
Rainbow Ia	161 600	103 616	66	1. i 2. razina
Rainbow IIIc	882 080	626 016	164	3. i 4. razina
Rainbow IVc	1 930 600	1 408 704	212	3. razina

Kao i većina multivarijatnih shema za digitalno potpisivanje, Rainbow nema sigurnosni dokaz koji reducira težak računalni (NP-težak) problem na sigurnost sheme. Pretpostavke sheme nisu pouzdane, zbog čega su se izvodile razne kriptoanalize isključivo namijenjene za Rainbow. Kriptoanaliza Rainbowa je u prvih nekoliko godina bila relativno stabilna, no ulaskom u NIST-ovo PQC natjecanje, postigli su se rezultati koji su poboljšali postojeće napade. Za vrijeme trećeg kruga NIST-ovog natjecanja, objavljena su dva nova napada koja su slomila sigurnosnu podlogu Rainbowa. Tim koji se bavi razvojem Rainbow kriptosustava, najavio je novi set parametara koji će biti otporni na novootkrivene napade [23].

U 2022. godini, IBM-ov znanstvenik Beullens objavio je članak "Breaking Rainbow Takes a Weekend on a Laptop" kojim predstavlja novi napad oporavka privatnog ključa (engl. *key recovery attack*) Rainbow Ia varijante, gdje je za napad potreban javni ključ, klasično računalo i otprilike 50 sati [35].

Prednosti i nedostaci

Rainbow potpisi su mali, a algoritmi za potpisivanje i verifikaciju potpisa brzi. Rainbow koristi isključivo linearnu algebru nad vrlo malim konačnim poljima, što ga čini prikladnim za implementaciju sheme na jeftinijim uređajima, bez potrebe za kriptografskim koprocesorom.

S druge strane, javni ključevi su veliki (npr. 158 KB za Rainbow Ia), no taj problem je moguće riješiti kompresijom javnog ključa čija se veličina može smanjiti tri puta na račun sporijeg vremena potpisivanja [23]. Novi velik nedostatak Rainbowa

je slamanje varijante prve sigurnosne kategorije pomoću prethodno opisanog napada.

Poglavlje 8

Usporedba PKE/KEM finalista

U ovom poglavlju prikazuje se usporedba PKE/KEM finalista po različitim svojstvima kao što su performanse i sigurnost. Svaki finalist ima više varijacija s različitim razinama sigurnosti i optimizacijom. Kako bi usporedba bila što vjerodostojnija, za finaliste se koristila neoptimizirana verzija pete sigurnosne kategorije NIST-a.

8.1 Performanse

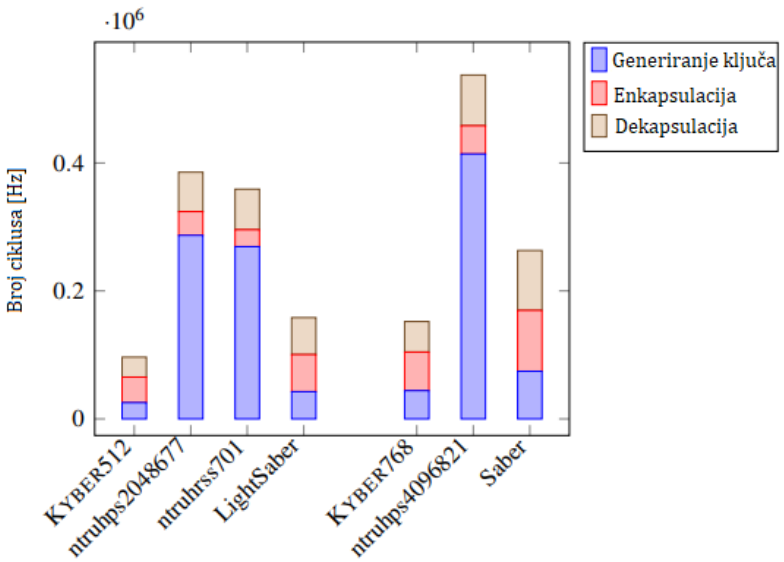
U tablici 8.1 prikazane su veličine javnih i tajnih ključeva te šifrata svakog finalista. Kao što se spominjalo i u prethodnim poglavljima, klasični McEliece ima problem velikih tajnih i javnih ključeva što ga čini neprikladnim za široku upotrebu u internetskim protokolima, ali zato ima i najmanji šifrat koji je rezultat operacija jednostavnih objekata kao što su binarni vektori i matrice.

Tablica 8.1 Veličine ključeva i šifrata PKE/KEM finalista u bitovima [30][36]

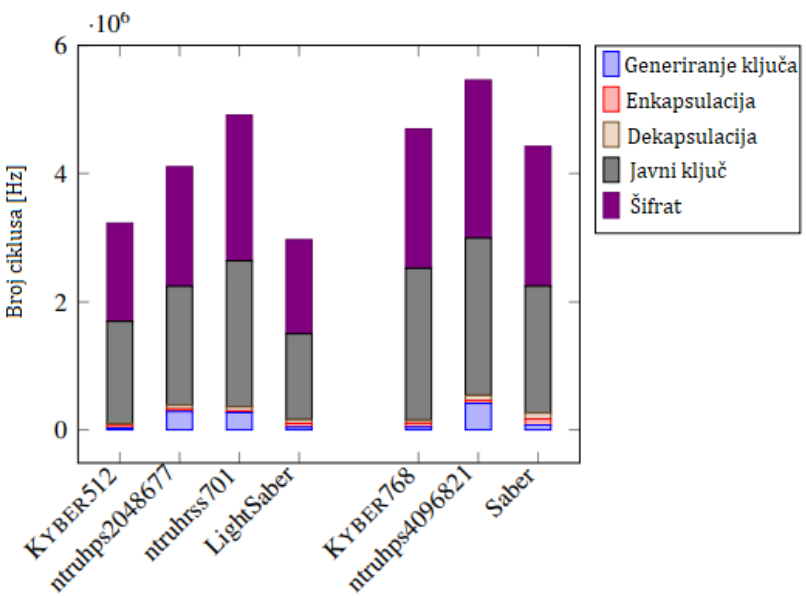
	Javni ključ	Privatni ključ	Šifrat
Crystals-KYBER	12 544	25 344	12 544
Classic McEliece	10 862 592	112 960	1920
NTRU	9840	12 736	9840
Saber	10 496	13 312	11 776

Što se tiče vremena izvođenja generiranja ključeva, šifriranja i dešifriranja, algoritmi koji koriste varijacije LWE-a postižu bolje performanse od osnovne LWE verzije. NTRU koristi MLWR i postiže konkurentne performanse za šifriranje i dešifriranje, ali je znatno sporiji za generiranje ključeva od strukturiranih LWE shema [30]. Najsporije generiranje ključeva ima finalist McEliece zbog veličine ključeva, ali su mu vremena izvođenja procesa enkapsuliranja i dekapsuliranja brža od ostalih PKE/KEM finalista [37]. Vidljivo je kako su vremena izrade ključeva i šifrata proporcionalna njihovim veličinama.

Na slici 8.1 se nalazi usporedba računalnih performansi PKE/KEM finalista koji su bazirani na rešetkama prema [38]. Usporedba se radila za procesor x86-64 s AVX2 ekstenzijama za varijante finalista iz prve i druge kategorije sigurnosti. Iz slike se zaključuje kako su enkapsulacija i dekapsulacija vrlo brze za sve prikazane finaliste. Saber ima najniži ukupni trošak zbog manjih javnih ključeva i šifrata, ali trošak između KYBER-a i Sabera nije dovoljno velik da bi se smatrao značajnim. Slikom 8.2 prikazan je ukupni trošak za korištenje PKE/KEM shema, gdje je procijenjeni trošak 2000 ciklusa po bajtu. NTRU ima veće javne ključeve i šifrate pa je zbog toga ukupni trošak njegovih varijacija za 30% veći od varijacija KYBER-a i Sabera.



Slika 8.1 Računalne performanse PKE/KEM finalista [29]



Slika 8.2 Računalne performanse PKE/KEM finalista uz trošak izrade ključa i šifrata [29]

8.2 Sigurnost

Tablica 8.2 prikazuje stupnjeve pogreške (engl. *failure rate*). Može se primijetiti kako su klasični McEliece i NTRU finalisti bez stupnja pogreške, odnosno u potpunosti su ispravni. Ostali finalisti se također mogu smatrati ispravnima zbog vrlo niskih stupnjeva pogreške što im omogućuje primjenu FO transformacije, a samim time i IND-CCA-siguran kriptosustav.

Tablica 8.2 Stupnjevi pogreške PKE/KEM finalista [30][36]

	Stupanj pogreške
Crystals-KYBER	2^{-228}
Classic McEliece	0
NTRU	0
Saber	2^{-165}

Svi finalisti su IND-CPA sigurni zbog korištenja neke varijante LWE problema (finalisti bazirani na rešetkama) ili sindroma problema dešifriranja (klasični McEliece).

Poglavlje 9

Usporedba SIGNATURE finalista

Svaki od finalista za digitalno potpisivanje ima više varijacija ovisno o izboru parametara čime se kontrolira razina sigurnosti algoritma. Parametri utječu na duljinu javnog i privatnog ključa, kao i na duljinu potpisa. Sigurnost algoritma raste kako se duljina potpisa povećava.

Dilithium i FALCON su finalisti za opću namjenu, a NIST je najavio kako će se izabrati samo jedan od njih [29]. Treći finalist, Rainbow, je imao zadovoljavajuće rezultate te bi bio odličan odabir za aplikacije koje zahtijevaju male potpise ili brzu provjeru, ali je zbog sigurnosnih incidenata opisanih u potpoglavlju 7.2.1 bio izostavljen iz daljnjeg natjecanja.

9.1 Performanse

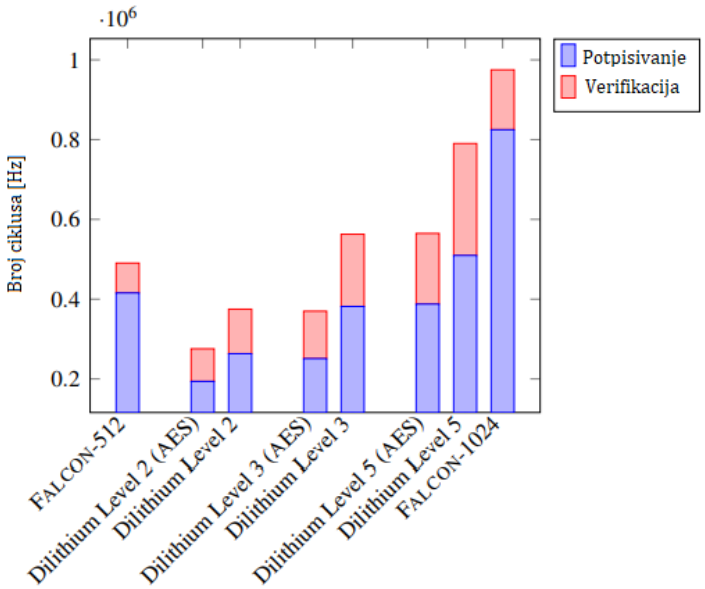
U tablici 9.1 vidljive su duljine javnog i privatnog ključa te duljina potpisa za finaliste s parametrima koji odgovaraju prvoj razini sigurnosti. Rainbow ima najveće duljine ključeva, ali zato i najmanji potpis, što se spominjalo u uvodu ovog poglavlja. Dilithiumovi ključevi i šifrat su veći od FALCON-ovih, a njihova detaljnija usporedba slijedi u nastavku.

Slika 9.1 prikazuje računalne performanse iz [38] za x86-64 procesor s AVX2 ekstenzijama za finaliste. Za razliku od slike 8.1 na kojoj se prikazala usporedba PKE/KEM finalista, ovdje se ne spominje trošak generiranja ključeva jer se ključevi

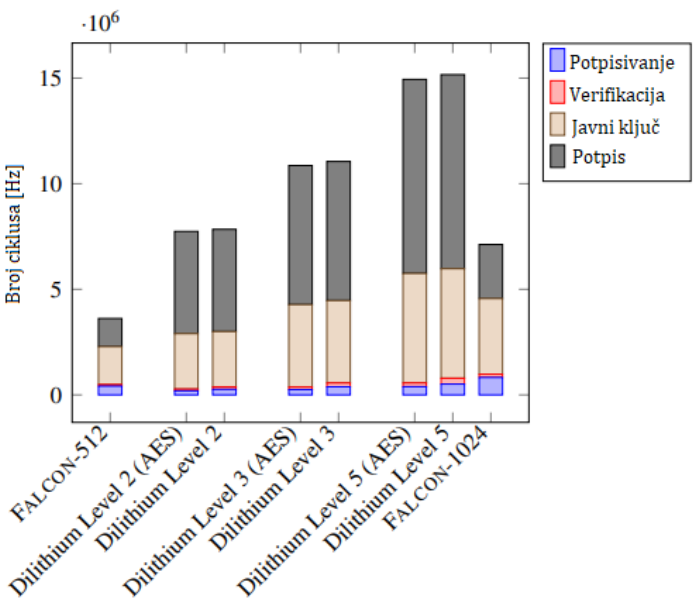
Tablica 9.1 Veličine ključeva i šifrata finalista u bitovima [38]

	Javni ključ	Privatni ključ	Potpis
Dilithium	1312	2528	2420
FALCON-512	897	7553	666
Rainbow Ia	161 600	103 616	66

za potpisivanje ne generiraju kod svake transakcije. Na slici 9.2 prikazani su ukupni troškovi za Dilithium i FALCON s uključenim troškom prijenosa javnog ključa i potpisa. Kao i na slikama iz prethodnog poglavlja, koristi se procijenjeni trošak od 2000 ciklusa po bajtu. Iz slika se vidi da je generiranje potpisa Dilithiumom brže od onog s FALCON-om. Budući da prijenos podataka uvelike doprinosi povećanju ukupnih troškova, zaključuje se da je FALCON-ov trošak manji zbog manjeg javnog ključa i potpisa. Za većinu aplikacija koje koriste x86-64 ili sličan procesor, performanse bi trebale biti prihvatljive i za Dilithium i za FALCON. Dilithiumovi potpisi ne stanu u jedan internetski paket, što bi moglo otežati prilagodbu nekih aplikacija na korištenje Dilithiuma.



Slika 9.1 Računalne performanse finalista za digitalno potpisivanje[29]



Slika 9.2 Računalne performanse finalista za digitalno potpisivanje uz trošak izrade ključa i potpisa [29]

9.2 Sigurnost

Sigurnost finalista baziranih na rešetkama, Dilithiuma i Falcona, temelji se na matematičkom problemu pronalaženja najkraćih vektora na rešetki, a sigurnost Rainbowa se temelji na težini rješavanja multivarijatnih polinoma nad konačnim poljem.

Pronalaženje najkraćeg vektora se može preoblikovati u problem pronalaženja minimuma, koji se potencijalno može riješiti pomoću kvantnog kaljenja (engl. *quantum annealing*) koje je osmišljeno za pronalaženje minimuma funkcije gubitka, a istovremeno je manje zahtjevno što se tiče kvantne korekcije pogreške. Minimum se također može pronaći pomoću univerzalnih kvantnih vrata, no za tu implementaciju bi bio potreban velik broj vrata i kompleksna arhitektura. Ako se kvantno kaljenje koristi za slamanje Dilithiuma i Falcona pronalaskom minimalne duljine vektora na rešetki, to bi moglo značajno ubrzati njihovu kriptoanalizu [31].

Poglavlje 10

Daljnji razvoj natjecanja i post-kvantne kriptografije

NIST je 05.07.2022., dvije godine nakon odabira četiri PKE/KEM finalista i tri finalista za digitalno potpisivanje, odabrao četiri njih koji će postati temelj budućih kriptosustava otpornih na napade kvantnih računala. NIST je također predložio četiri kandidata (BIKE, Klasični McEliece, HQC i SIKE) za naknadna ispitivanja i pozvao ih da dostave dodatne prijedloge za algoritme za digitalno potpisivanje do početka 10. mjeseca 2022. godine [39]. Dok se rešetke čine najboljima za opću upotrebu, kriptografska zajednica nastavit će proučavati druge obitelji algoritama koje također nude razne prednosti za specifične slučajeve, kao i zbog raznolikosti u slučaju da napadi na rešetke postignu novi napredak. Pretpostavlja se da će se standardizacija odabranih algoritama finalizirati do 2024. godine.

Odabrana su dva primarna algoritma, CRYSTALS-Kyber i CRYSTALS-Dilithium, za upotrebu u većini aplikacija, gdje će se Kyber koristiti kao PKE/KEM algoritam, a Dilithium će biti standardizirani algoritam za digitalno potpisivanje. Uz njih, odabrani su FALCON i SPHINCS+, također algoritmi za digitalno potpisivanje. NIST će kroz idućih nekoliko mjeseci izraditi nacrt standarda za odabrane algoritme i zatražiti povratne informacije javnosti o njima. Moguće da će se neki od odabranih algoritama korigirati tijekom izrade nacrta standarda, no ne očekuju se velike promjene.

U nadolazećim mjesecima mnogim će se jezicima, knjižnicama i protokolima dodati preliminarna podrška za trenutnu verziju Kybera i drugih post-kvantnih algoritama. Cilj je da post-kvantni algoritmi postanu dostupni korisnicima kako bi se migracije i druge tehničke prilagodbe, kad za to dođe vrijeme, mogle odraditi što lakše.

Poglavlje 11

Zaključak

Kvantna računala nude svijetlu budućnost glede rješavanja nekih od najvećih izazova današnjice: očuvanje okoliša, poljoprivreda, zdravstvo, energija, klimatske promjene i drugo. S druge strane, jednom kad kvantna računala krenu sa širom primjenom, ugrozit će komunikaciju putem Interneta, uključujući IoT uređaje. Postupak post-kvantne standardizacije od strane američkog NIST-a je rješenje za taj problem. Svaki od četiri matematička temelja na kojima su izgrađeni algoritmi finalisti ima svoje prednosti i nedostatke. Teško je predvidjeti koja će se vrsta kvantno otpornih algoritama u budućnosti pokazati najučinkovitijom. Većina istraživanja se provela nad kriptosustavima koji se baziraju na rešetkama, no i oni koji se baziraju na kodu ostavljaju dobar izbor za buduće kriptografske standarde. Algoritmi koji se baziraju na multivarijatnim jednadžbama pružaju visoku sigurnost za digitalno potpisivanje, ali zbog toga što su još uvijek relativno novi i zbog manjka istraživanja nisu dobili potrebnu popularnost. Na temelju broja predanih zahtjeva na početku natjecanja, postotak algoritama baziranih na rešetkama je bio daleko viši od ostalih, što se prenijelo i do trećeg kruga, gdje je od sedam finalista njih pet bilo bazirano na rešetkama. NIST-ovo natjecanje za post-kvantnu standardizaciju dalo je dobar pregled različitih matematičkih područja i problema te otvorilo nova vrata za kriptostandarde budućnosti. NIST je obavio zahtjevan posao ispitivanja i testiranja svih prijavljenih algoritama kako bi se pronašli najučinkovitiji i najsigurniji algoritmi.

Bibliografija

[1] Arute, F. i dr., "Quantum supremacy using a programmable superconducting processor", Nature, vol. 574, pp. 505-510, 2019.

[2] Bolf, N., "Kvantna računala – tehnologija 21. stoljeća", Osvježimo znanje, Kem. Ind., Vol. 68, pp. 555-556, 2019.

[3] Deutsch, D., "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, Vol. 400, No. 1818, pp. 97-117, 2019.

[4] Canadian Centre for Cyber Security, "Cyber Centre's summary review of final candidates for NIST Post-Quantum Cryptography standards", s Interneta, https://cyber.gc.ca/en/news-events/cyber-centres-summary-review-final-candidates-nist-post-quantum-cryptography-standards, 10.08.2022.

[5] Amundsen, L. i dr., "Supercomputers for Beginners - Part IV", GEO ExPro, Vol. 13, No. 3, 2016.

[6] Crane, L., "Quantum computer sets new record for finding prime number factors", s Interneta, https://www.newscientist.com/article/2227387-quantum-computer-sets-new-record-for-finding-prime-number-factors/, 12.07.2022.

[7] Lenac, K., "Napredni operacijski sustavi", prezentacije s predavanja dostupne na Merlin 2021/2022 sustavu.

[8] PGP Corporation, "An Introduction to Cryptography", s Interneta, https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf, 05.08.2022.

[9] Malović, I., "Asimetrični kriptosustav NTRU", Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, diplomski rad br. 55, lipanj 2010.

[10] Hundek, T. i dr., "Quantum computing history and background", s Interneta, https://docs.microsoft.com/en-us/azure/quantum/concepts-overview, 11.07.2022.

[11] Magić, S., "Kvantno računarstvo", s Interneta, https://docs.google.com/presentation/d/1bncIbVbI3W8-bjSbMd2K4jDeUMThhYvpTqFl0f-3cWU/htmlpresent, 01.08.2022.

[12] "Bloch sphere", s Interneta, https://en.wikipedia.org/wiki/Bloch_sphere, 23.07.2022.

[13] "Quantum computing in a nutshell", s Interneta, https://qiskit.org/documentation/qc_intro.html, 25.07.2022.

[14] "Kvantno računalo", s Interneta, http://sail.zpf.fer.hr/labs/kvarac/fer2archive/akg1617/06_computer.pdf, 02.07.2022.

[15] Kazalicki, M., "Kvantno računanje", s Interneta, https://web.archive.org/web/20210408065150/https://web.math.pmf.unizg.hr/~mkazal/reprints/skripta_kvantno.pdf, 05.08.2022.

[16] Hrg, D., "Simulator kvantnog računala", Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, diplomski rad br. 1444, travanj 2004. .

[17] Shor, P. W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing, No. 5, pp. 1484, 1997.

[18] Strubell, E., "An Introduction to Quantum Algorithms", s Interneta, http://mmrc.amss.cas.cn/tlb/201702/W020170224608150507023.pdf, 14.08.2022.

[19] Čurla, K., "Pregled post-kvantnih kriptografskih sustava", Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Diplomski rad, 2019.

[20] "NIST - National Institute of Standards and Technology", s Interneta, https://www.nist.gov/, 01.07.2022.

[21] Rijneveld, J., "Practical post-quantum cryptography", s Interneta, https://joostrijneveld.nl/thesis/practical-pqc-joostrijneveld.pdf, 10.07.2022.

[22] NIST, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process", s Interneta, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf, 28.06.2022.

[23] Beullens, W. i dr., "POST-QUANTUM CRYPTOGRAPHY Current state and quantum mitigation", European Union Agency for Cybersecurity (ENISA), 2021.

[24] Moody, D., "Let's Get Ready to Rumble - The NIST PQC "Competition"", s Interneta, https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf, 30.06.2022.

[25] Chen, L. i dr., "Report on Post-Quantum Cryptography", s Interneta, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, 15.07.2022.

[26] "An Introduction to Post-Quantum Cryptography", s Interneta, https://www.cryptoquantique.com/blog/post-quantum-cryptography/, 22.07.2022.

[27] Crnković, B. i dr., "Asimetrični kriptografski algoritmi za razmjenu ključeva otporni na napade kvantnim računalom", s Interneta, http://sigurnost.zemris.fer.hr/algoritmi/asimetricni/2020_21_projekt_PDS/downloads/TehDocProjektR.pdf, 15.07.2022.

[28] "Overview of NIST Round 3 Post-Quantum cryptography Candidates", s Interneta, https://www.pqsecurity.com/wp-content/uploads/2020/07/Round-3.pdf, 11.08.2022.

[29] Alagic, G. i dr., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process", s Interneta, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf, 05.08.2022.

[30] Mazzola, G. i dr., "Investigation on NIST post-quantum lattice-based encryption scheme", s Interneta, https://repository.tudelft.nl/islandora/object/uuid%3A57f7922f-93ad-4411-b6c2-9c5a8a5a845e, 02.08.2022.

[31] Raavi, M. i dr., "Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms", s Interneta, https://cwssp.uccs.edu/sites/g/files/kjihxj2466/files/2021-09/1_Security%20Comparisons%20and%20Performance%20Analyses%20of%20Post-Quantum%20Signature%20Algorithms.pdf, 12.07.2022.

[32] Alagic, G. i dr., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", s Interneta, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf, 07.08.2022.

[33] Tera, H., "Introduction to Post-Quantum Cryptography in scope of NIST's Post-Quantum Competition", s Interneta, https://core.ac.uk/download/pdf/237084813.pdf, 11.08.2022.

[34] Patarin, J., "The oil and vinegar signature scheme", Dagstuhl Workshop on Cryptography September, 1997.

[35] Beullens, W., "Breaking Rainbow Takes a Weekend on a Laptop", s Interneta, https://eprint.iacr.org/2022/214.pdf, 17.08.2022.

[36] Basu, K. i dr., "NIST Post-Quantum CryptographyA Hardware Evaluation Study", s Interneta, https://eprint.iacr.org/2019/047.pdf, 10.07.2022.

[37] Dekhuijzen, L. i dr., "A Comparison of Post-Quantum Code-Based Cryptosytems", Delft University of Technology, Bachelor Seminar of Computer Science and Engineering, 01.07.2021.

[38] "eBACS: ECRYPT Benchmarking of Cryptographic Systems", s Interneta, https://bench.cr.yp.to/supercop.html, 13.08.2022.

[39] NIST, "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates", s Interneta, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4, 22.08.2022.

Sažetak

Razvoj kvantnih računala počeo je prije više od 35 godina, a u posljednjih nekoliko godina dogodili su se značajni koraci u njihovom razvoju. Konstantno povećavanje brzina kvantnih računala potvrđuje njihovu kvantnu nadmoć te nagoviješta dugo-očekivanu promjenu računalne paradigme. Ta promjena je započela 2016. godine kada je američki NIST pokrenuo natjecanje post-kvantne standardizacije za asimetričnu kriptografiju i digitalno potpisivanje. Na natjecanje se prijavilo 82 kandidata iz 25 različitih zemalja, a u ovom radu opisuje se njih sedam koji su dospjeli do trećeg, finalnog kruga natjecanja. Algoritmi se temelje na različitim matematičkim područjima koja su opisana zajedno s osnovnim svojstvima i sigurnosnim značajkama finalista. Uz pojedinačno opisivanje algoritama, napravljena je i njihova usporedba, gdje su se promatrali parametri poput performansi i sigurnosti.

Ključne riječi — **asimetrična kriptografija, digitalno potpisivanje, kriptografija, kvantna otpornost, kvantna računala, NIST standardizacija, post-kvantna kriptografija**

Abstract

The development of quantum computers started more than 35 years ago, and in the last few years, there have been significant steps in their development. The constant increase in the speed of quantum computers confirms their quantum supremacy and announces a long-awaited change in the computing paradigm. That change began in 2016 when the US NIST launched a post-quantum standardization competition for asymmetric cryptography and digital signing. Eighty-two candidates from 25 different countries applied for the competition, and this paper describes seven of them who made it to the third and final round of the competition. Algorithms are based on different mathematical fields that are described along with the basic properties and security features of the finalists. In addition to describing the algorithms individually, their comparison was also made, where parameters such as performance and security were observed.

Keywords **— asymmetric cryptography, digital signing, cryptography, quantum resistance, quantum computers, NIST standardization, post-quantum cryptography**