

Univerzitet u Kragujevcu
Fakultet inženjerskih nauka



Predmet: Kriptografija

Tema: Post-Quantum kriptografija - poređenje performansi
algoritama baziranih na rešetkama

Student:

Marijana Jeremić 620/2021

Predmetni profesor:

Dr Milan Čabarkapa

Sadržaj

1	Uvod	3
1.1	Motivacija za postkvantnu kriptografiju	3
1.2	Kvantni računari i pretnje klasičnoj kriptografiji	7
➤	Shorov algoritam - kvantna pretnja savremenoj kriptografiji	8
➤	Groverov algoritam - kvadratno ubrzanje za probleme pretrage	9
2	Opis kvantnog računarstva i kriptografskih pretnji	11
2.1	Kako kvantni računari ugrožavaju postojeće algoritme	11
2.1.2	Kvantni resursni zahtevi	12
	Performanse i implikacije	12
2.2	Koncept „prikupljanja sada, dešifrovanja kasnije“ (Store Now, Decrypt Later)	12
2.2.1	„Overview of a Merkle Tree certificate deployment“	13
2.2.2	„KEMTLS“	14
2.2.3	Grafovi: TLS handshake time vs. „Dummy data added (kB)” i TLS handshake slowdown (%)	14
2.2.4	Grafovi: Missing requests vs. „Dummy data added (kB)”	15
2.2.5	Graf: Client support for post-quantum key agreement in TLS 1.3 (% kroz vreme)	15
2.2.6	Serijski histogram: TLS handshake latency - CONTROL vs. CECQP2 (X25519+NTRU-HRSS) vs. CECQP2b (X25519+SIKE) po OS-ovima	16
3	Postkvantna kriptografija (PQC)	17
3.1	Trenutne aktivnosti i standardizacija (NIST proces)	17
3.2	Strategije zaštite sistema	18
4	Kategorije PQC algoritama	18
4.1	Rešetkasti (Lattice-based)	18
4.1.1	Osnovni problemi: SIS, LWE i Ring-LWE	19
4.1.2	Prednosti i nedostaci	20
4.1.3	Primeri: Kyber, Dilithium, ML-KEM	20
4.2	Kodna kriptografija (Code-based)	21
4.2.1	Primeri algoritama	21
4.3	Heš-bazirana (Hash-based) kriptografija	21
4.3.1	Primeri i koncepti	21
4.4	Multivarijantna (Multivariate) kriptografija	22
4.4.1	Rainbow, UOV	22
4.5	Izogenijska (Isogeny-based) kriptografija	23
4.5.1	SIKE, SIDH	23
5	Rešetkasta kriptografija u praksi - TLS protokol i Ring-LWE	23
5.1	Uvod u TLS i njegove sigurnosne komponente	23
5.2	Ring-LWE za razmenu ključeva	24
5.3	Mehanizam funkcionisanja Ring-LWE	25
5.4	Integracija u TLS protokol	25

5.5 Performanse u odnosu na ECDH	26
5.6 Hibridna šema (klasična + PQC)	26
6 Uporedna analiza performansi PQ algoritama	27
6.1 Brzina (latencija i throughput)	27
6.2 Veličina ključeva i memorijski zahtevi	29
6.3 Sigurnost i otpornost na kvantne napade	30
6.4 Efikasnost u aplikacijama (e-mail, TLS, kriptovalute)	31
Primer sertifikata	36
7 Zaključak	37
7.1 Prednosti PQC algoritama	37
7.2 Preporuke za buduću migraciju	37
7.3 Važnost pravovremene pripreme	37
8 Literatura	39

1 Uvod

Tema ovog semestralnog rada na izbornom predmetu Kriptografija u osmom semestru smera Računarska tehnika i softversko inženjerstvo Fakulteta inženjerskih nauka u Kragujevcu jeste Post-Quantum kriptografija: poređenje performansi algoritama baziranih na rešetkama. Ona treba odgovoriti na sledeći zahtev: Uporediti performanse post-kvantnih algoritama (npr. Kyber, Dilithium) u aplikacijama kao što su sigurni mejlovi i TLS konekcije.

1.1 Motivacija za postkvantnu kriptografiju

Nauka nudi najhrabriju metafiziku današnjice. Ona je u potpunosti ljudska tvorevina, vođena verom da ako sanjamo, otkrivamo, objašnjavamo i ponovo sanjamo, svet će nam postati jasniji i shvatićemo njegovu pravu čudnovatost - koja će, iznenađujuće, biti povezana i imati smisla. - **Edward O. Wilson**

Informacija je fizička. – Rolf Landauer

Pitanja poput: *Koji su fundamentalni koncepti kvantne informatike? Kako su se razvijali? Kako ih možemo primeniti?* – čine osnovu ove oblasti. Ova uvodna diskusija opisuje istorijsku pozadinu, razvoj osnovnih ideja, i daje širok pregled kvantne informatike i računanja. Na početku 20. veka, fizika je prolazila kroz krizu – klasična fizika nije mogla objasniti pojave kao što su "ultravioletna katastrofa". Rešenje je došlo kroz razvoj **kvantne mehanike**. Uprkos svojoj preciznosti, kvantna mehanika je dugo bila kontraintuitivna. Jedan od motiva kvantnog računanja je upravo pokušaj da se shvati i intuitivnije predstavi kvantni svet. Jedan od ključnih momenata bio je "no-cloning teorem" (nemogućnost kloniranja nepoznatih kvantnih stanja), otkriven 1980-ih. Ova ideja je bila revolucionarna i pokazala je da kvantna informacija funkcioniše drugačije od klasične. Dalji napredak se desio sa razvojem metoda za kontrolu pojedinačnih kvantnih sistema, kao što su atomi uhvaćeni u "atomskim zamkama", što je otvorilo vrata za **izgradnju kvantnih računara**.

Do danas su ovi napori rezultirali skromnim uspesima. Mali kvantni računari, sposobni da izvrše nekoliko desetina operacija nad nekoliko kvantnih bita (ili kubita) predstavljaju trenutno dostignuće kvantnog računanja. Eksperimentalni prototipovi za kvantnu kriptografiju – način tajne komunikacije na velikim udaljenostima – već su demonstrirani i nalaze se na nivou gde mogu biti korisni za neke primene u stvarnom svetu. Ipak, ostaje veliki izazov za buduće fizičare i inženjere da razviju tehnike koje bi omogućile realizaciju kvantnog procesiranja informacija u velikim razmerama.

Sada se pažnja sa kvantne mehanike usmerava na još jedno veliko intelektualno dostignuće dvadesetog veka – računarske nauke. Poreklo računarske nauke izgubljeno je u dubinama istorije. Na primer, klinasti zapisi pokazuju da su do vremena vladavine Hamurabija (oko 1750. godine pre nove ere) Vavilonci razvili prilično sofisticirane algoritamske ideje, i verovatno je da mnoge od tih ideja datiraju i iz ranijih perioda.

Moderna inkarnacija računarske nauke objavljena je od strane velikog matematičara **Alana Tjuringa** u izuzetnom radu iz 1936. godine. Tjuring je detaljno razvio

apstraktnu predstavu onoga što bismo danas nazvali programabilnim računarom – model računanja poznat kao **Tjuringova mašina**, u njegovu čast. Tjuring je pokazao da postoji Univerzalna Tjuringova Mašina koja može da simulira bilo koju drugu Tjuringovu mašinu. On je takođe tvrdio da ta univerzalna mašina u potpunosti obuhvata pojam algoritamskog rešavanja zadataka. Drugim rečima, ako se neki algoritam može izvršiti na bilo kom hardverskom sistemu (npr. savremenom personalnom računaru), tada postoji ekvivalentni algoritam za univerzalnu Tjuringovu mašinu koji obavlja isti zadatak. Ova tvrdnja poznata je kao Teza Church–Turing, nazvana po Tjuringu i još jednom pioniru računarskih nauka, Alonzu Čerču. Ona uspostavlja ekvivalentnost između fizičkog koncepta računanja i matematičkog modela univerzalne Tjuringove mašine. Opšte prihvatanje ove teze postavilo je temelje za razvoj bogate teorije računarskih nauka. Nedugo nakon Tjuringovog rada, konstruisani su prvi računari na osnovu elektronskih komponenti. **Džon fon Nojman** razvio je **jednostavan teorijski model** kako da se praktično sklope sve komponente potrebne da bi računar bio **potpuno sposoban kao univerzalna Tjuringova mašina**. Hardver je zaista počeo ubrzano da se razvija 1947. godine, kada su **Džon Bardeen**, **Volter Bratejn** i **Vilijam Šokli** razvili **tranzistor**.

Snaga računarskog hardvera od tada je rasla **zapanjujućim tempom**, do te mere da je taj rast 1965. godine formalizovao **Gordon Mur** u zakonu koji danas poznajemo kao **Muurov zakon: računarska snaga će se udvostručavati po fiksnoj ceni otprilike svakih dve godine**. Neverovatno je da se Muurov zakon otprilike održao tokom decenija od 1960-ih. Ipak, većina posmatrača očekuje da će se taj „zlatni niz“ završiti negde tokom prve dve decenije dvadeset prvog veka. Klasične metode izrade računarske tehnologije sve više nailaze na fundamentalna ograničenja veličine. **Kvantni efekti** počinju da ometaju rad elektronskih uređaja koji su sve manji i manji.

Jedno moguće rešenje problema koji nastaje **zbog kraja važenja Murovog zakona** jeste prelazak na **drugu paradigmu računanja**. Jedna takva paradigma zasniva se na **teoriji kvantnog računanja**, tj. ideji da se koristi **kvantna mehanika** umesto klasične fizike za izvođenje računskih operacija. Ispostavilo se da, **dok običan računar može simulirati kvantni računar, nemoguće je to učiniti efikasno**. Stoga **kvantni računari nude suštinsku brzinsku prednost** u odnosu na klasične računare.

Ta **brzinska prednost** je toliko značajna da mnogi istraživači veruju da **ni jedan zamislivi napredak u klasičnom računarstvu** ne bi mogao da **nadoknadi jaz između snage kvantnog i klasičnog računara**.

Još jedna linija misli koja je doprinela razvoju kvantnog računanja i kvantne informacije je **teorija informacija**. U isto vreme kada je računarska nauka doživljavala ekspanziju tokom 1940-ih, **druga revolucija** se dešavala u našem razumevanju komunikacije. **1948. godine**, Klod Šenon (Claude Shannon) je objavio izuzetna dva rada koja su postavila temelje savremene teorije informacija i komunikacije. Možda je najvažniji korak koji je Šenon napravio bio taj što je **matematički definisao pojam informacije**. U mnogim matematičkim naukama postoji velika fleksibilnost u izboru osnovnih definicija. Pokušajte, na primer, da naivno razmislite o sledećem pitanju: kako biste matematički definisali pojam izvora informacija? Postoji više odgovora koji su naišli na široku upotrebu, ali Šenonova definicija je daleko **najplodotvornija** jer je rezultirala brojnim dubokim rezultatima i teorijom bogate strukture koja vrlo dobro oslikava mnoge (iako ne sve) probleme

stvarnog sveta u vezi sa komunikacijom. Šenon se bavio sa dva ključna pitanja u vezi sa prenosom informacija preko komunikacionog kanala:

- **Koji resursi su potrebni da se informacija prenese kroz kanal?** Npr. telefonske kompanije moraju da znaju koliko informacija mogu pouzdano da prenesu kroz telefonski kabl.
- **Može li se informacija preneti tako da bude zaštićena od šuma u komunikacionom kanalu?**

Šenon je odgovorio na ova pitanja kroz svoje dve fundamentalne teoreme teorije informacija:

- **Teorema o kodiranju bez šuma (noiseless channel coding theorem):** Kvantifikuje fizičke resurse potrebne za skladištenje izlaza iz izvora informacija.
- **Teorem o kodiranju sa šumom (noisy channel coding theorem):** Kvantifikuje koliko informacija je moguće pouzdano preneti kroz šumni kanal. Šenon je pokazao da **korišćenjem kodova za ispravljanje grešaka** informacija može biti uspešno zaštićena.

Međutim, Šenonova teorema **ne daje eksplicitno upotrebljiv skup kodova**, pa su istraživači decenijama razvijali različite klase kodova koje se sve više približavaju Šenonovoj gornjoj granici. Danas imamo razvijenu i sofisticiranu teoriju kodova za ispravljanje grešaka, koji se koriste širom tehnike (CD plejeri, modemi, satelitske komunikacije).

Kvantna teorija informacija je sledila sličan razvoj. **1995. godine**, Ben Šumaher (Ben Schumacher) je obezbedio analog Šenonovom teoremu o kodiranju bez šuma i tom prilikom definisao pojam **kvantnog bita (qubit)** kao opipljivog fizičkog resursa.

Međutim, **ne postoji poznati analog Šenonovog teorema o kodiranju sa šumom** za kvantne informacije. Ipak, analogno klasičnim sistemima, razvijena je **teorija kvantnog ispravljanja grešaka**, koja dozvoljava:

- efikasno računanje kvantnim računarima i
- pouzdanu komunikaciju preko šumovitih kvantnih kanala.

Klasične ideje o ispravljanju grešaka pokazale su se izuzetno važnim u razumevanju kvantnih kodova. **1996. godine**, dve nezavisne grupe istraživača (Robert Calderbank i Peter Shor, te Andrew Steane) otkrile su klasu kvantnih kodova danas poznatih kao **CSS kodovi** (po njihovim inicijalima).

Ovaj rad je kasnije uopšten kroz **stabilizatorske kodove (stabilizer codes)**, koje su razvili Calderbank, Eric Rains, Peter Shor, Neil Sloane i Daniel Gottesman. Polazeći od ideja klasične linearne teorije kodiranja, omogućeno je brzo razumevanje i primena kvantnih kodova za ispravljanje grešaka.

Kvantni kodovi štite kvantna stanja od šuma. Ali šta je sa slanjem klasičnih informacija preko kvantnog kanala? I tu su otkrivena neka iznenađenja. Na primer, **1992. godine**, Charles Bennett i Stephen Wiesner su pokazali kako da se dva klasična

bita informacija pošalju prenosom samo jednog kvantnog bita (qubita) - ovaj fenomen naziva se super-gusto kodiranje (superdense coding).

Još interesantnije su distribuirane kvantne računске operacije. Zamislamo dve umrežene kvantne mašine koje pokušavaju da reše problem. Pokazano je da kvantni računari mogu zahtevati eksponencijalno manje komunikacije nego što bi to bio slučaj kod klasičnih mreža. Međutim, problemi za koje je ovo pokazano trenutno nisu praktično značajni, što ostavlja otvoren izazov: pronaći realne probleme gde distribuirano kvantno računanje donosi značajnu prednost.

Teorija informacija se tradicionalno bavi **jednim komunikacionim kanalom**, ali u realnim primenama često imamo **mreže kanala**. Takva teorija poznata je kao **networked information theory** i vrlo je razvijena u klasičnom slučaju.

Osnovna jedinica kvantne informacije je kvbit (kvantni bit), koji za razliku od klasičnog bita ne mora biti isključivo u stanju 0 ili 1. Umesto toga, kvbit može istovremeno biti u obe vrednosti, tj. u stanju superpozicije, sve dok se ne izvrši merenje. Na primer, kvbit može biti u stanju:

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

što znači da će merenje dati rezultat **0 ili 1**, sa jednakom verovatnoćom od 50%. Ovo stanje se često označava kao $|+\rangle$ i predstavlja jedan od ključnih gradivnih elemenata kvantnih algoritama.

Fizička realizacija kvbita:

Iako deluju apstraktno, kvbiti su eksperimentalno potvrđeni i mogu se realizovati na više fizičkih načina:

- kroz polarizaciju fotona (horizontalna i vertikalna),
- putem nuklearnog spina u magnetnom polju (NMR kvantni računari),
- korišćenjem dva energetska nivoa elektrona u atomu (osnovno i pobuđeno stanje).

Prelazak kvbita iz stanja $|0\rangle$ u $|1\rangle$ se obično ostvaruje pomoću kontrolisanih interakcija, kao što su svetlosni impulsi koji omogućavaju i prelazak u stanja superpozicije.

Vizualizacija: Blochova sfera

Sva pojedinačna kvbit stanja mogu se prikazati kao tačke na površini Blochove sfere, koristeći izraze:

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

Ovaj model omogućava geometrijsku interpretaciju kvbit stanja i pomaže u razumevanju kvantnih operacija. Ipak, važi samo za jedan kvbit – više kvbita se modeluje u višedimenzionim Hilbertovim prostorima.

Koliko informacija nosi kvbit? Naizgled, kvbit može da „zadrži” beskonačnu količinu informacija, jer se njegove amplitude mogu precizno parametrisati pomoću realnih brojeva (uglove θ i ϕ). Međutim, pri merenju dobijamo samo jedan bit – 0 ili 1. Štaviše, merenje ne samo da ne otkriva sve informacije, već i nepovratno menja kvantno stanje (tzv. kolaps talasne funkcije). Iako kvbit skriva informacije koje ne možemo direktno očitati, one ipak učestvuju u kvantnim operacijama i omogućavaju kvantne interferencije.

Više kvbita i superpozicije

U kvantnim sistemima sa više kvbita, kombinatorika stanja eksponencijalno raste. Dva kvbita ne predstavljaju samo četiri odvojena stanja kao u klasičnom računarstvu (00, 01, 10, 11), već mogu biti u **superpoziciji svih tih stanja istovremeno**:

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle,$$

gde su α_{ij} kompleksne amplitude koje zadovoljavaju uslov normalizacije.

Zanimljivo je da merenje jednog kvbita u takvom sistemu utiče na stanje celog sistema, jer kvantno stanje zavisi od svih amplituda istovremeno.

Entanglement: Kvantna sprega

Jedan od najneobičnijih fenomena kvantne mehanike je **entanglement**, tj. kvantna sprega. U entanglovanim stanjima, kvbiti su povezani na način koji nema paralelu u klasičnom svetu. Primer entanglovanog stanja je tzv. Belovo stanje:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle).$$

U ovom slučaju, ako izmerimo prvi kvbit i dobijemo 0, drugi će sigurno biti 0, bez obzira na udaljenost među njima – što je bio povod za čuvenu debatu o "sablasnom dejstvu na daljinu" (spooky action at a distance). [1]

1.2 Kvantni računari i pretnje klasičnoj kriptografiji

Razvoj kvantnih računara dovodi u pitanje sigurnost savremene kriptografije, čija se bezbednost zasniva na teškoći rešavanja određenih matematičkih problema. Dva najznačajnija kvantna algoritma koja direktno ugrožavaju postojeće sisteme su:

- **Šorov algoritam (Shor, 1994)** – omogućava efikasnu faktORIZACIJU velikih brojeva i rešavanje problema diskretnih logaritama, što direktno ugrožava **RSA**, **DSA**, **ECDSA** i **Diffie-Hellman** algoritme.
- **Groverov algoritam (Grover, 1996)** – omogućava kvadratno ubrzanje pretrage u nestrukturisanim prostorima, pa umanjuje bezbednost simetričnih algoritama poput **AES** (efektivno prepolovljuje bezbednost).

Upravo zato se javlja potreba za **postkvantnom kriptografijom**, koja je otporna na kvantne napade.

Takođe, postoji i koncept „kupi sada, dešifruj kasnije“ (harvest now, decrypt later), gde napadač može da sačuva enkriptovanu komunikaciju i sačeka budući kvantni računar koji bi je mogao razbiti. Zbog ovih pretnji, organizacije kao što je **NIST** pokrenule su proces standardizacije kvantno otpornih algoritama (Kyber, Dilithium, itd.) u okviru postkvantne kriptografije (PQC).

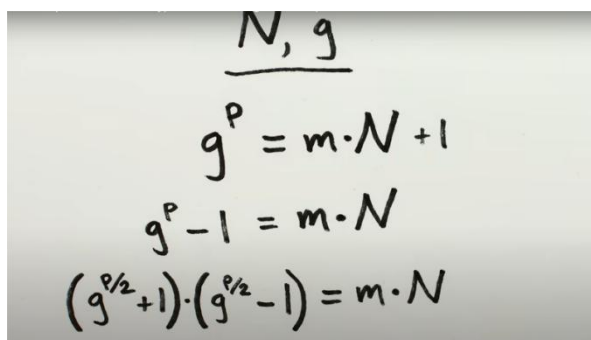
1.3 Osnovni kvantni algoritmi (Shor, Grover)

➤ Shorov algoritam - kvantna pretnja savremenoj kriptografiji

Savremeni sistemi enkripcije, poput RSA algoritma, svoju sigurnost zasnivaju na jednom fundamentalno teškom matematičkom problemu – faktorizaciji velikih brojeva. Dok je množenje dva velika prosta broja računski jednostavno i brzo, njihovo razlaganje (faktorizacija) u proste činioce predstavlja izuzetno zahtevan zadatak za klasične računare. U najefikasnijim postojećim metodama, faktorizacija zahteva eksponencijalno vreme i ogromne računarske resurse, što čini ovakve metode praktično neprobojnim. Međutim, kvantna računarska paradigma ovaj problem transformiše iz temelja. Shorov algoritam, koji je razvio matematičar Piter Šor (Peter Shor), predstavlja kvantni algoritam sposoban da faktorise velike brojeve u **polinomijalnom vremenu**, čime direktno ugrožava bezbednost većine trenutno korišćenih javnih ključeva.

➤ Osnovna ideja algoritma

Shorov algoritam koristi kvantnu mehaniku da identifikuje **period funkcije** definisane u modularnoj aritmetici. Ključni matematički zadatak se svodi na sledeće:


$$\begin{aligned} & \underline{N, g} \\ & g^p = m \cdot N + 1 \\ & g^p - 1 = m \cdot N \\ & (g^{p/2} + 1) \cdot (g^{p/2} - 1) = m \cdot N \end{aligned}$$

Slika 1: Definicija ključnog matematičnog zadatka

Ovaj broj p naziva se period, i on omogućava konstrukciju ova dva izraza čiji najveći zajednički delilac (GCD) sa NN daje jedan od faktora broja NN .

Klasični računar može izračunati takav period samo kroz iscrpljujuće ispitivanje svih mogućih vrednosti, što je računski neefikasno. Suprotno tome, kvantni računar koristi kvantnu superpoziciju i kvantnu Fourierovu transformaciju da simultano obradi sve moguće eksponente i izdvoji upravo vrednost perioda p , sa velikom verovatnoćom tačnosti.[6]

➤ Kvantna komponenta algoritma

Kvantna prednost se ogleda u sledećem:

Superpozicija ulaza: Kvantni računar obrađuje više vrednosti istovremeno, tj. sve moguće eksponente x u izrazu $g^x \bmod N$.

Uvođenje interferencije: Rezultati koji nisu tačni međusobno se poništavaju (destruktivna interferencija), dok se tačne vrednosti pojačavaju.

Kvantna Fourierova transformacija: Koristi se za identifikaciju frekvencije (tj. perioda) iz periodične superpozicije, što omogućava efikasno izdvajanje perioda p .

Nakon određivanja p , faktori broja N se pronalaze upotrebom **Euklidovog algoritma** na izraze $\gcd(g^{p/2 \pm 1}, N)$.

➤ Implikacije po bezbednost

Uspešno izvršavanje Shorovog algoritma na dovoljno snažnom kvantnom računaru omogućilo bi razbijanje većine današnjih kriptosistema zasnovanih na RSA, DSA i ECC algoritmima. Iako trenutni kvantni računari nemaju dovoljno kvantne memorije (qubita) za faktorisanje brojeva korišćenih u praksi (npr. 2048-bitni RSA ključevi), razvoj u ovom pravcu napreduje, i potencijalna pretnja postaje sve realnija. Zato je Shorov algoritam prepoznat kao ključni motivacioni faktor za razvoj postkvantne kriptografije (PQC) – novih metoda otpornih na napade kvantnih računara.

➤ Groverov algoritam - kvadratno ubrzanje za probleme pretrage

Groverov algoritam, koji je 1996. godine razvio Lov Grover, predstavlja kvantni algoritam koji omogućava **kvadratno ubrzanje** u rešavanju problema pretrage u neuređenim skupovima podataka. Iako nije toliko razoran po savremenu kriptografiju kao Shorov algoritam, Groverov algoritam ima široku primenu u mnogim problemima koji pripadaju klasi tzv. **NP problema**, odnosno problema za koje se rešenje lako proverava, ali ga je teško pronaći. [2]

➤ Problem koji Grover rešava

Zamislamo da postoji neka funkcija (tzv. „orakul“) koja prima broj iz skupa od 0 do $N-1$ i vraća tačno jedan rezultat „tačno“ (true), dok za sve ostale brojeve vraća „netačno“ (false). Cilj je pronaći upravo taj broj – „ključ“ – koji zadovoljava funkciju.

Na klasičnim računarima, jedina mogućnost je nasumično ispitivanje vrednosti (brute force), što u proseku zahteva $N/2$ pokušaja. Ovo znači da je vreme izvršavanja algoritma proporcionalno veličini ulaznog skupa – oznakom $O(N)$. Međutim, Groverov algoritam omogućava rešavanje tog problema za $O(\sqrt{N})$ koraka, što predstavlja značajno ubrzanje. Na primer, ako imamo milion mogućih ključeva, klasičnom metodom bi bilo potrebno oko 500.000 provera u proseku, dok bi kvantni računar uz Groverov algoritam taj broj smanjio na samo oko 1.000. [2]

➤ Kvantna osnova algoritma

Za razliku od klasičnih računara koji u svakom trenutku obrađuju jedan mogući ulaz, kvantni računari koriste **superpoziciju**, što znači da mogu obraditi sve moguće ulaze istovremeno. Ipak, ovo ne znači da kvantni računar „vidi“ sve rezultate paralelno-umesto toga, koristi kvantne operacije (kvantne kapije) da pojača verovatnoću tačnog rešenja, a umanju verovatnoću ostalih.

Groverov algoritam koristi dve osnovne operacije:

- ✧ **Inverzija faze (Phase inversion):** menja znak komponente stanja koje predstavlja tačno rešenje (npr. iz +1 u -1). Ova operacija je ključna jer, iako ne menja verovatnoće direktno, omogućava da kasnija interferencija naglasi to rešenje.
- ✧ **Difuziona transformacija (Amplitude amplification):** "rotira" stanje kvantnog sistema oko srednje vrednosti svih stanja, čime pojačava amplitudu verovatnoće željenog rešenja.

Ove dve operacije se ponavljaju više puta, pri čemu se sistem korak po korak približava stanju u kome je verovatnoća za očitavanje tačnog rešenja maksimalna.

➤ Geometrijska intuicija

Groverov algoritam se može intuitivno razumeti kao **rotacija kvantnog stanja** unutar dvodimenzionalne ravni. U početku, kvantno stanje je ravnomerno raspodeljeno – sve vrednosti imaju istu verovatnoću. Međutim, ponovljenom primenom pomenutih operacija, vektor kvantnog stanja se rotira ka stanju koje odgovara tačnom rešenju.

Nakon približno $\pi/4 \cdot \sqrt{N}$ ponavljanja, kvantni sistem će se naći u stanju u kome je verovatnoća za očitavanje tačnog rešenja skoro 100%. Tada se sistem meri, i sa velikom verovatnoćom se dobija tačno rešenje.

➤ Ograničenja i verifikacija

Groverov algoritam ne garantuje apsolutno tačno rešenje nakon jednog pokretanja, već vrlo visoku verovatnoću. Međutim, s obzirom na to da se u većini NP problema rešenje lako proverava (npr. da li je ključ ispravan), algoritam se jednostavno može ponoviti ukoliko prvi pokušaj ne uspe.

Takođe, Groverov algoritam ne donosi **eksponencijalno ubrzanje**, kao što to čini Shorov algoritam, već **kvadratno ubrzanje**, što je i dalje izuzetno značajno u kriptografiji. Na primer, **AES-256**, koji se danas smatra sigurnim, zbog Groverovog algoritma bi efektivno imao sigurnost približno ekvivalentnu **AES-128**, pa se preporučuje korišćenje dužih ključeva kao mera predostrožnosti.

➤ Značaj u postkvantnom okruženju

Groverov algoritam ukazuje da čak i simetrične šeme enkripcije (kao što su AES, SHA-2, itd.), koje se smatraju otpornim na Shorov algoritam, nisu u potpunosti bezbedne pred kvantnim pretnjama. Iako nisu direktno razbijene, njihova bezbednost

je smanjena, pa se zato preporučuju **duži ključevi** i primena **kvantno otpornih heš funkcija**.

➤ *Rezime*

Groverov algoritam je jednostavan, ali izuzetno moćan kvantni algoritam koji demonstrira kako kvantna mehanika može unaprediti klasične metode. Iako ne predstavlja trenutnu opasnost za internet bezbednost, on je snažan argument zašto treba što pre usvojiti i standardizovati postkvantne bezbednosne protokole.

2 Opis kvantnog računarstva i kriptografskih pretnji

2.1 Kako kvantni računari ugrožavaju postojeće algoritme

Kvantni računari direktno ugrožavaju temelje asimetrične (javne) kriptografije. Dva najpoznatija algoritma:

- Shorov algoritam – efikasno faktoriše velike brojeve - razbija RSA, DSA, ElGamal, ECC.
- Groverov algoritam – ubrzava brute-force napade na simetrične šeme - efektivno prepolovljuje sigurnost šema poput AES, SHA-2.

Shorov algoritam faktoriše broj N u polinomijalnom vremenu: oko $O((\log N)^3)$, što je eksponencijalno brže od najboljih klasičnih algoritama koji rade u vremenu ekvivalentnom $O(e^{\{n^{1/3}\}})$. Najefikasniji klasični algoritam (general number field sieve) ima sub-ekspresionalnu složenost $O(\exp(1.9 \cdot (\log N)^{1/3} (\log \log N)^{2/3}))$. Shor je, takođe, pokazao da može efikasno rešiti diskretni logaritam, što direktno ugrožava ECC i Diffie-Hellman šeme.

Groverov algoritam i uticaj na simetrične šeme (AES) - Grover pruža kvadratno ubrzanje za neorganizovanu pretragu: sa $O(N)$ klasičnih provera na $O(\sqrt{N})$ poziva kvantnog orakla. To znači da AES-128 efektivno ima samo 64-bitnu sigurnost protiv kvantnog napada koristeći Grover.

Primeri aplikacija koje su ugrožene:

- Sigurne e-mail komunikacije (PGP, S/MIME)
- TLS konekcije (RSA i ECDH koriste se za razmenu ključeva).

2.1.1 Microsoft Research: kvantna analiza Groverovog napada na AES

Tim iz Microsoft Research-a (Jaques, Naehrig, Roetteler, Virdia) razvio je kompletne kvantne orakl-cirkuirne konstrukcije za AES-128, AES-192 i AES-256, fokusirajući se na minimizaciju dubine orakla, čak po cenu većeg broja kubita. Implementirali su prototip u jeziku Q#, podržan automatskim računima dubine i broja kubita putem Q# kompajlera. Od metričkih modela su korišćeni:

- Gate-count: ukupni broj kvantnih kapija – važan za NIST-ove kategorije sigurnosti.
- Depth \times Width: produkt dubine (redosled paralelnih slojeva) i širine (broj kubita) - realniji model troškova u korekciji grešaka
- Rad cilja na smanjenje dubine uz prihvatljivo povećanje broja kubita. [3]

2.1.2 Kvantni resursni zahtevi

AES-128

- Logički kubiti: između ~3.000 i ~7.000 logičkih kubita potrebnih za implementaciju Grover-ove iteracije (u zavisnosti od trade-off podešavanja).
- Glavni troškovi: najveći deo vremena i složenosti čini key expansion za svaki krug AES unutar orakla zbog serijske strukture Grover-ove aplikacije.

Ključevi i kapije:

- Koristi se Clifford+T logički skup kapija, gde je T-kapija najskuplja zbog korekcije grešaka.
- Tipična razgradnja Toffoli kapije zahteva 7 T-gate (moguće optimizacije smanjuju na 4, uz dodatni pomoćni kubit)

Performanse i implikacije

Prema modelu dobivenom u radu, za AES- 128 napad:

- Neophodno je $\sim \sqrt{2^{128}} = 2^{64}$ Grover-ovih iteracija.
- Svaka iteracija zahteva kvantno izvođenje orakla, što po resursima znači hiljade kubita i dubine koja može biti problematična za praktičnu implementaciju čak i bez korekcije grešaka

Kada se uzme u obzir implementacija zaštićena korekcijom grešaka:

- Potencijalno se prelazi u decine miliona fizičkih kubita i vreme izvođenja meri danima ili satima, u zavisnosti od optimizacije (npr. 'minimize qubit count' ili 'minimize depth').
- Za AES, realne procene variraju od ~5 do 25 miliona fizičkih kubita i trajanja od ~12 sati do ~1 dana za napad, u zavisnosti od tehnologije (npr. obična gate baza).

2.2 Koncept „prikupljanja sada, dešifrovanja kasnije“ (Store Now, Decrypt Later)

Napadači danas mogu presretati i čuvati šifrovanu komunikaciju (npr. e-mail, TLS sesije), iako trenutno ne mogu da je dešifruju. Međutim, kada kvantni računari postanu dostupni, oni će moći da razbiju te zapise unazad, što predstavlja ozbiljnu pretnju za dugoročnu privatnost i bezbednost. Zašto je ovo važno?

- Tajni podaci (npr. vojni, medicinski, obrazovni, finansijski) moraju biti sigurni desetinama godina.

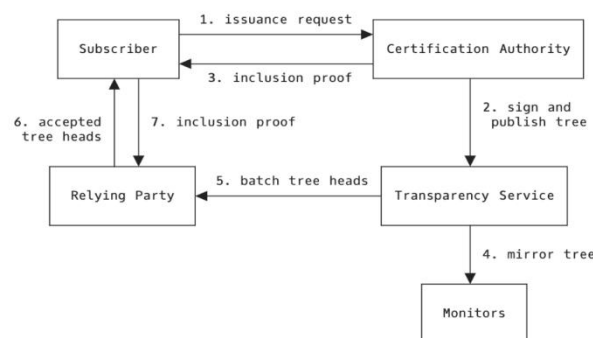
- Ako se šifruju algoritmima poput RSA danas, a kvantni računar se pojavi za 10 godina, kompromitacija je retroaktivna.

Primer:

Cloudflare i Google su testirali TLS 1.3 sa PQC algoritmima (npr. Kyber) kako bi bili otporni na kvantne napade i zaštitili podatke dugoročno.

2.2.1 „Overview of a Merkle Tree certificate deployment“

Šta se posmatra: arhitekturu *Merkle Tree Certificates (MTC)* - način da se drastično smanji veličina sertifikata/lanaca i pritom obezbedi proverljivost preko transparentnog loga.[7]



Slika 2: Overview of a Merkle Tree certificate deployment [7]

Koraci (označeni brojevima na slici):[7]

- Subscriber - CA: issuance request – vlasnik sajta traži sertifikat.
- CA - Transparency Service: sign & publish tree – CA potpisuje i objavljuje „stablo“ (root + grane) u servis transparentnosti.
- Transparency Service - Subscriber: inclusion proof, vlasnik dobija *dokaz uključenja* (Merkle proof) da je tačno njegov list u stablu.
- Transparency Service - Monitors: mirror tree, nezavisni nadzornici (monitori) preuzimaju/mirroruju stablo i otkrivaju zloupotrebe.
- Transparency Service - Relying Party: batch tree heads, posetioci/klijenti (relying parties, npr. pregledači) dobijaju „glave“ stabala (tree heads) u paketu.
- Relying Party - Subscriber: accepted tree heads – klijent potvrđuje da prihvata određene „glave“ stabla.
- Relying Party - Subscriber: inclusion proof, pri konekciji klijent proverava dokaz uključenja za konkretan sertifikat/brz *proof* umesto ogromnog lanca.

Zašto je bitno za SNDL/PQC:

PQC potpisi i lanci su veći. MTC zamenjuje isporuku masivnih lanaca kompaktnim *proof*-om (log-verifikacija preko Merkle stabla). Time se:

- smanjuje „težina“ TLS handshaka,
- ubrzava uspostavljanje sesije,

- čuva kompatibilnost i revizabilnost (monitori otkrivaju zloupotrebe).
Manji handshake = manje šanse da se konekcije lome na slabim linkovima ili u middlebox-ovima, pa je realno moguće široko uvesti kvantno-otporne sertifikate već danas.

Ključna poruka slike: *Transparentnost + kompresija dokaza (Merkle) rešavaju praktične prepreke velikih PQC sertifikata.*

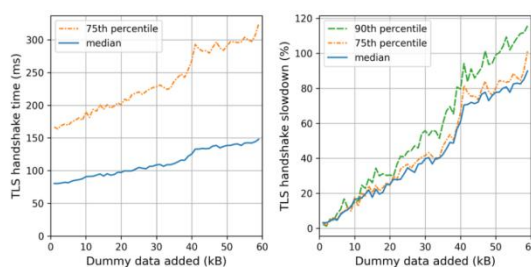
2.2.2 „KEMTLS“

Ideja je da se u TLS-u zamene potpisi u leaf sertifikatu KEM-om (Key Encapsulation Mechanism), pa server dokazuje posjedovanje ključa dešifrovanjem izazova (umesto potpisivanja).[7]

Zašto je bitno:

- Post-kvantni potpisi (npr. ML-DSA-44) su veliki (u tekstu je primer ~2 420 B po handshake potpisu).
- KEMTLS sa ML-KEM-512 može uštedeti ~852 B ukupno po handshaku (a na samom serveru ~1 620 B od oko 17 kB prenosa).
- U mrežnim uslovima gde si blizu granice congestion window-a, ušteda ~1.6 kB može izbeći dodatni RTT i značajno smanjiti latenciju.
- Za embedded/IoT je plus što se smanjuje broj algoritama koje treba implementirati (KEM za autentikaciju i razmenu tajne - „2 u 1“).

2.2.3 Grafovi: TLS handshake time vs. „Dummy data added (kB)” i TLS handshake slowdown (%)



Slika 3:Performanse TLS handshaka pri povećanju veličine sertifikata (simulacija post-kvantnih sertifikata) [7]

Šta se posmatra: Cloudflare je simulirao PQC sertifikate tako što je veštački uvećavao veličinu sertifikacionog lanca i merio posledice.[7]

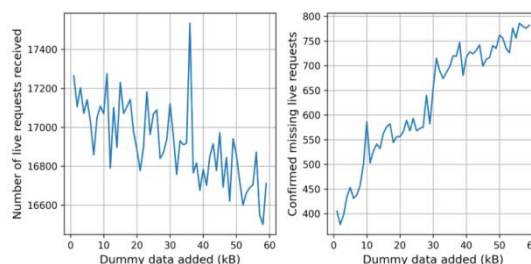
- Levo (ms): median i 75. percentil latencija handshaka linearno rastu sa veličinom „dodatih bajtova“.
- Desno (% usporenja): relativno usporenje eksponencijalno raste; pri većim veličinama usporenje ide i preko 100% (kod viših percentila).

Napomena: oko ~40 kB dolazi do skoka - tipično jer se probija početni congestion window, pa je potreban još jedan RTT.

Veza sa SNDL/PQC: PQC potpisi i lanci mogu lako da „naduvaju“ handshake. Ako handshake postane prevelik → spor + nepouzdan → operativni sistemi, pregledači ili middlebox-ovi počnu da pucaju. Zato su neophodni pristupi kao MTC i KEMTLS.

Ključna poruka slike: Veći sertifikati = veći RTT i latencija; prelazak na PQC bez optimizacija je bolan.[7]

2.2.4 Grafovi: Missing requests vs. „Dummy data added (kB)“



Slika 4: Uticaj povećanja veličine sertifikata na gubitak TLS konekcija [7]

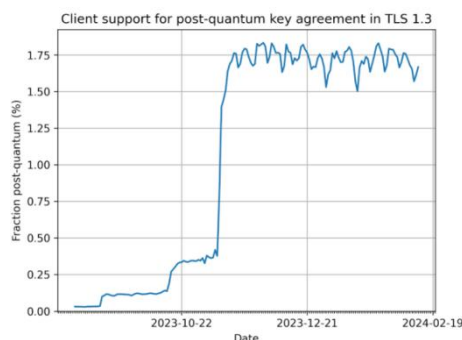
Šta se posmatra: dve metrike koje detektuju „ispadanje“ konekcija kad su lanci „naduvani“.[7]

- Levo: broj primljenih „live“ zahteva opada kako raste veličina lanca.
- Desno: broj sigurno propuštenih zahteva raste sa veličinom (primetni „skokovi“ oko 10 kB i 30 kB), što upućuje na klijente ili middlebox-ove koji ne trpe velike lance.

Veza sa SNDL/PQC: Ako zbog PQC-a lanci porastu, kompatibilnost strada, baš ono što sprečava masovno uvođenje PQC i ostavlja otvorenu SNDL pretnju. Rešenja: Merkle-dokazi umesto lanaca (MTC) i/ili KEMTLS.[7]

Ključna poruka slike: *Preveliki lanci ne samo da usporavaju — oni realno lome konekcije.*

2.2.5 Graf: Client support for post-quantum key agreement in TLS 1.3 (% kroz vreme)



Slika 5: Rast podrške klijenata za post-quantnu razmenu ključeva u TLS 1.3 [7]

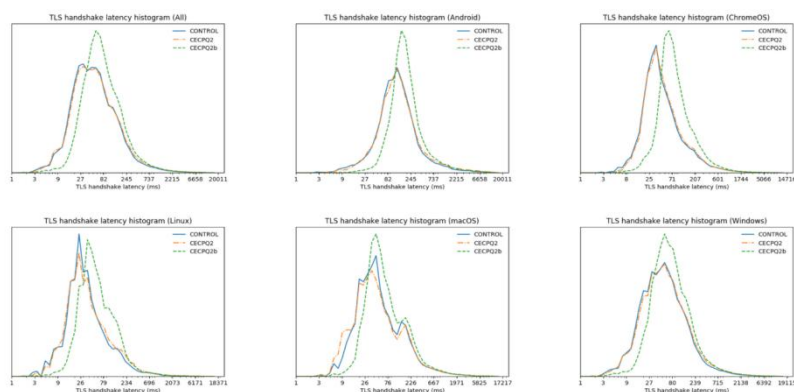
Šta se posmatra: udeo klijenata (pregledača) koji podržavaju PQC razmenu ključa (npr. hibrid X25519+Kyber) u TLS 1.3.[7]

- Kriva pravi veliki skok krajem oktobra 2023. (kada je Chrome/Chromium uključio hibridnu podršku), pa se stabilizuje oko ~1.6–1.8%.
- Zaključak: još je rano, ali trend postoji, ključni korak da se današnji saobraćaj štiti od sutrašnjih kvantnih napada.

Veza sa SNDL/PQC: Što pre klijenti podrže PQC, to pre prekidamo „prikupljaj sada, dešifruj kasnije“ strategiju napadača za novi saobraćaj.

Ključna poruka slike: *PQC podrška na klijentima raste — ali smo tek na početku.*

2.2.6 Serija histograma: TLS handshake latency - *CONTROL* vs. *CECPQ2* (*X25519+NTRU-HRSS*) vs. *CECPQ2b* (*X25519+SIKE*) po OS-ovima



Slika 6: Poređenje latencije TLS handshaka sa klasičnim i post-quantnim hibridnim algoritmima na različitim operativnim sistemima [7]

Šta se posmatra: rezultate Cloudflare-Google eksperimenata (2016/2018) sa hibridnim PQC šemama na realnim klijentima i OS-ovima. [7]

- Oblik krivih je vrlo sličan kontroli (klasični X25519), tj. overhead je mali i najčešće jedva vidljiv „golim okom“.
- CECPQ2 (NTRU-HRSS) se pokazao stabilno po latenciji.
- CECPQ2b (SIKE) je bio koristan za testiranje *performansi*, ali je algoritam krypto-napadom razbijen 2022.- što je i poenta eksperimenata: naći praktično brze i krypto-robuste kombinacije (danas: ML-KEM/Kyber).

Veza sa SNDL/PQC: Ovi eksperimenti su dokazali da PQC može da bude brz i transparentan za korisnika - pa nema izgovora da se ne pređe na hibridne key-agreement-e već sada.

Ključna poruka slika: *Rani eksperimenti su pokazali da je PQC handshake praktično izvodljiv bez „kazne“ po korisničko iskustvo.*

3 Postkvantna kriptografija (PQC)

3.1 Trenutne aktivnosti i standardizacija (NIST proces)

S obzirom na pretnju koju kvantni računari predstavljaju za tradicionalne asimetrične kriptografske algoritme poput RSA, DSA i ECC (Elliptic Curve Cryptography), američki Nacionalni institut za standarde i tehnologiju (NIST) pokrenuo je 2016. godine sveobuhvatan proces standardizacije postkvantnih kriptografskih algoritama. Ovaj proces ima za cilj definisanje novih kriptografskih standarda koji će biti bezbedni i u postkvantnoj eri, tj. otpornim na napade pomoću kvantnih računara. Faze NIST PQC standardizacije - NIST proces se odvija u više faza:[8]

- Prva faza (2016–2019) - Tokom prve faze, NIST je primio 82 prijave algoritama iz celog sveta. Nakon inicijalne evaluacije na osnovu bezbednosti, performansi i implementacione efikasnosti, 26 algoritama je prošlo u drugu fazu.
- Druga faza (2019–2022) - Ova faza je uključivala detaljnije analize preostalih kandidata. NIST je pratio performanse algoritama u različitim okruženjima (hardver, softver, embedded sistemi) i analizirao kriptografske otpornosti na poznate (klasične i kvantne) napade. Na kraju ove faze, 7 algoritama je ušlo u završnu fazu razmatranja.
- Treća faza (od 2022) - U julu 2022. godine, NIST je najavio prvi skup postkvantnih algoritama koji će biti standardizovani. To su:
 - ✧ CRYSTALS-Kyber – za postkvantnu enkripciju i razmenu ključeva.
 - ✧ CRYSTALS-Dilithium, FALCON i SPHINCS+ - za postkvantne digitalne potpise.

Ovi algoritmi zasnovani su na različitim matematičkim problemima koji se smatraju otpornim na kvantne napade, kao što su problemi rešetki (lattice-based cryptography), hash-based konstrukcije i strukture koda (code-based cryptography).[8]

Uloga industrije i međunarodna saradnja:

Pored NIST-a, i druge institucije i organizacije kao što su ETSI (European Telecommunications Standards Institute) i ISO (International Organization for Standardization) sprovode sopstvene evaluacije i predlažu standarde koji se uklapaju u globalnu sigurnosnu strategiju prelaska ka PQC.

Neke multinacionalne kompanije kao što su Google, IBM, Microsoft i Cloudflare već sprovode testiranja u realnim mrežnim uslovima koristeći hibridne pristupe - kombinovanje klasičnih i PQC algoritama kako bi se omogućila postepena tranzicija bez prekida kompatibilnosti. Prelazni period i implementacione preporuke:

- NIST preporučuje hibridne implementacije kao prelazno rešenje: da se istovremeno koriste klasični i postkvantni algoritmi dok kvantna infrastruktura ne postane dovoljno pouzdana. Takođe se razvijaju specijalizovani alati, kao što je NIST's Migration to PQC Toolkit, koji pomažu organizacijama da identifikuju kritične komponente sistema i planiraju tranziciju.

- Naredni koraci uključuju objavljivanje zvaničnih specifikacija i interop testove, kao i definisanje potrebnih bezbednosnih nivoa za različite primene (npr. IoT, vladine komunikacije, finansijski sistemi).[8]

3.2. Strategije zaštite sistema

Strategije zaštite sistema - NIST proces i standardizacija

U eri ubrzanog razvoja kvantnih računara, tradicionalni kriptografski algoritmi, kao što su RSA i ECC, postaju ranjivi. Nacionalni institut za standarde i tehnologiju (NIST) pokrenuo je proces standardizacije postkvantnih kriptografskih (PQC) algoritama kako bi omogućio bezbednu komunikaciju čak i u prisustvu kvantnih napada. Ovaj proces uključivao je višegodišnje istraživanje, takmičenje i rigoroznu analizu sigurnosti i performansi predloženih algoritama. Kao rezultat, NIST je u **avgustu 2024. godine** objavio tri zvanična postkvantna standarda:

- ML-KEM (FIPS 203) – Mehanizam za enkapsulaciju ključeva, baziran na algoritmu CRYSTALS-Kyber. Namenjen je za opštu enkripciju, kao što je obezbeđivanje sigurnih veza na internetu (npr. TLS/SSL konekcije).
- ML-DSA (FIPS 204) – Lattice-bazirani algoritam za digitalne potpise, zasnovan na CRYSTALS-Dilithium. Predstavlja efikasno rešenje za autentifikaciju korisnika i verifikaciju integriteta podataka.
- SLH-DSA (FIPS 205) – Hash-bazirani algoritam za digitalne potpise, izveden iz SPHINCS+. Ovaj algoritam koristi stateless pristup, što ga čini otpornim na veliki broj napada, ali dolazi uz veće veličine potpisa.

Pored ovih standarda, NIST je privremeno odložio standardizaciju algoritma FALCON, takođe baziranog na rešetkama, zbog izazova u implementaciji. Dodatno, algoritam HQC (Hamming Quasi-Cyclic) je odabran kao deo narednog koraka u proširenju portfolija PQC algoritama.[8]

4 Kategorije PQC algoritama

Post-kvantni kriptografski (PQC) algoritmi klasifikuju se prema matematičkim problemima na kojima se zasnivaju. S obzirom na to da kvantni računari predstavljaju pretnju za klasične asimetrične algoritme kao što su RSA, DSA i ECC, neophodno je razviti algoritme koji ostaju bezbedni i u post-kvantnom okruženju. U nastavku su prikazane glavne kategorije PQC algoritama.

4.1 Rešetkasti (Lattice-based)

Rešetkasti algoritmi predstavljaju jednu od najperspektivnijih grana postkvantne kriptografije. Njihova sigurnost se zasniva na teškim matematičkim problemima u rešetkama, kao što su SIS (Short Integer Solution), LWE (Learning With Errors), i Ring-LWE. Osim što nude visok nivo sigurnosti protiv kvantnih napada, ovi algoritmi su poznati po svojoj efikasnosti i mogućnosti implementacije na uređajima sa ograničenim resursima.

4.1.1 Osnovni problemi: SIS, LWE i Ring-LWE

Problem SIS:

Problem SIS predstavlja jedan od centralnih problema u oblasti lattice-based kriptografije. On formalizuje zadatak nalaženja „kratkog“ (tj. vektora male norme) nenultog celobrojnog vektora koji poništava unapred datu matricu kada se množenje posmatra po modulu q .

Za date parametre:

- ✧ prost broj $q \in \mathbb{Z}_q$
- ✧ dimenzije $n, m \in \mathbb{N}$, $m \in \mathbb{N}$
- ✧ matricu

Traži se vektor x .

$$A \cdot x \equiv 0 \pmod{q}, \quad x \neq 0, \quad \|x\| \text{ je mala}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod{q}$$

LWE (Learning With Errors):

LWE je sličan problem, ali uključuje dodatnu komponentu "šuma" (greške).

Za poznatu matricu:

$$A \in \mathbb{Z}_q^{n \times m},$$

tajni vektor:

$$s \in \mathbb{Z}_q^m,$$

i vektor greške:

$$e \in \mathbb{Z}_q^n,$$

dobija se:

$$b = A \cdot s + e \pmod{q}.$$

Cilj: Na osnovu para (A, b) pronaći tajni vektor s .

Ring-LWE:

Ring-LWE je optimizovana verzija LWE problema, koja koristi strukturu polinoma i aritmetiku nad prstenovima (ringovima). Predstavlja kompromis između sigurnosti i efikasnosti, omogućavajući kraće ključeve i bržu obradu. U praksi se koristi u naprednim sistemima kao što su Kyber i Dilithium, kandidati za postkvantne standarde.

4.1.2 Prednosti i nedostaci

Prednosti:

- Otpornost na kvantne napade: Bazira se na problemima za koje ne postoje kvantni algoritmi koji ih efikasno rešavaju.
- Efikasnost: Brza enkripcija i dekripcija; efikasni potpisni algoritmi.
- Fleksibilnost: Lako prilagodljivi različitim bezbednosnim parametrima i potrebama.
- Teorijska snaga: Problemi kao što su SIS i LWE su dokazano teško rešivi čak i uz kvantne resurse.

Nedostaci:

- Veličina ključeva: Veća u poređenju sa klasičnim algoritmima poput RSA ili ECC.
- Parametarski izazovi: Pogrešan odabir parametara može narušiti sigurnost.
- Implementacione ranjivosti: Kao i kod svih šema, važno je implementirati algoritme uz pažnju na napade kanalom sporednih informacija (side-channel attacks).

4.1.3 Primeri: Kyber, Dilithium, ML-KEM

Kyber:

Kyber je rešetkasta kriptografska šema za razmenu ključeva (KEM - Key Encapsulation Mechanism) koja koristi Module-LWE problem. Jedna je od najefikasnijih postkvantnih šema, sa odličnim balansom između sigurnosti, brzine i veličine ključeva. Uključena je u finalnu selekciju NIST PQC standardizacije pod nazivom ML-KEM (Module Lattice KEM).[10]

Dilithium:

Dilithium je digitalni potpis baziran na Module-LWE i Module-SIS problemima. Koristi jednostavnu i sigurnu strukturu sa fiksnom veličinom potpisa i ključeva. Odlikuje se jednostavnom implementacijom i jakim sigurnošću. U okviru NIST PQC standarda, poznat je kao ML-DSA (Module Lattice Digital Signature Algorithm).[10]

ML-KEM (Module-Lattice KEM):

Naziv koji koristi NIST u finalnoj verziji standardizacije za Kyber šemu. Bazira se na Module-LWE problemu, a cilj je zamena trenutnih algoritama za razmenu ključeva kao što su RSA i ECC.

Bez poznavanja trapdoora, pronalaženje validnog potpisa implicira rešavanje (in)homogenog SIS problema, što je teško.

Zaključak ovoga dela

Rešetkasti kript algoritmi su bazirani na dubokim teorijskim osnovama, nude visoku sigurnost i otpornost na kvantne napade. Njihova praktična vrednost je potvrđena kroz brojne NIST finalist algoritme (Kyber, Dilithium, Falcon), a teorijska osnova leži u matematički rigoroznim pretpostavkama vezanim za rešetke i njihovu teškoću.

4.2 Kodna kriptografija (Code-based)

Kodna kriptografija zasniva se na teoriji kodova za detekciju i ispravljanje grešaka. Smatra se jednom od najstarijih i najotpornijih kategorija kriptografije.

4.2.1 Primeri algoritama

- **McEliece:** Jedan od najstarijih kriptosistema, poznat po otpornosti na kvantne napade. Bazira se na skrivenim Goppa kodovima. Iako su ključevi veoma veliki, algoritam je izuzetno brz.[11]
- **BIKE (Bit Flipping Key Encapsulation):** KEM algoritam zasnovan na QC-MDPC (Quasi-Cyclic Moderate Density Parity Check) kodovima.
- **HQC (Hamming Quasi-Cyclic):** Takođe koristi kvazi-ciklične kodove i predstavlja kompromis između veličine ključeva i performansi.[10]

Prednosti:

- Dugo se smatraju sigurnim protiv kvantnih napada.
- Brze operacije dešifrovanja.

Nedostaci:

- Veoma velike veličine javnih ključeva (posebno kod McEliece algoritma).
- Ograničena primenljivost u uređajima sa malim resursima.

4.3 Heš-bazirana (Hash-based) kriptografija

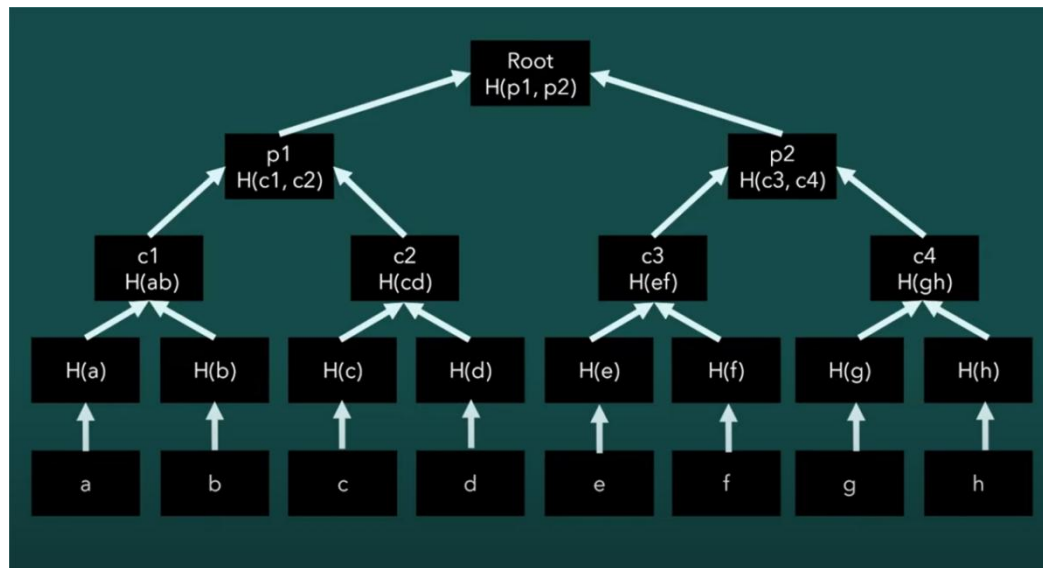
Ova kategorija koristi kriptografske heš funkcije kao osnovu za potpisne šeme. Predstavlja veoma sigurnu, ali specijalizovanu vrstu PQC algoritama.

4.3.1 Primeri i koncepti

- **Merkleovo stablo:** Struktura koja omogućava da se veliki broj jednokratnih potpisa efikasno objedini i validira putem heš stabla. [9]

Merkleovo stablo izgleda kao obrnuto stablo - koren je na vrhu, a listovi na dnu. Svaka poruka se hešira i postaje list. Dva lista se kombinuju i heširaju u **roditeljski čvor**, i tako sve dok se ne dođe do jednog - **korenog heša**.

Ako želimo dokazati da je neka poruka deo tog stabla, dovoljno je da se zna heš njenog para. Na primer, za poruku C, potreban je heš njenog para D, heš sledećeg roditelja, itd. Ako se dobije isti korenski heš, poruka nije izmenjena.



Slika 7: Merkle stablo

- **LMS (Leighton-Micali Signatures):** Efikasna i jednostavna potpisa šema, pogodna za uređaje sa ograničenim resursima.
- **SPHINCS+:** Stateles potpisna šema bazirana na hash funkcijama. Ima male ključeve, ali duže potpise.

Prednosti:

- Visoka sigurnost zasnovana na dokazima sigurnosti heš funkcija.
- Pogodne za verifikaciju potpisa u okruženjima sa niskim kapacitetima.

Nedostaci:

- Neke šeme zahtevaju "stateful" pristup - isti ključ se može koristiti samo jednom.
- Veća dužina potpisa (posebno kod SPHINCS+).

4.4. Multivarijantna (Multivariate) kriptografija

Zasniva se na teškoći rešavanja sistema multivarijantnih polinoma nad konačnim poljima.

4.4.1 Rainbow, UOV

- **Rainbow:** Digitalna potpisna šema koja koristi višeslojne strukture kvadratnih polinoma. Bila jedan od finalista NIST PQC takmičenja, ali je povučena zbog otkrivenih ranjivosti.
- **UOV (Unbalanced Oil and Vinegar):** Osnovna konstrukcija za multivarijantne potpise. Fokusira se na sigurnost u odnosu između ulaznih varijabli i tajnih parametara.

Prednosti:

- Brzo potpisivanje i verifikacija.
- Teorijski otporna na kvantne napade.

Nedostaci:

- Ranije verzije su bile ranjive na različite napade.
- Veće veličine ključeva i potpisa kod pojedinih implementacija.

4.5 Izogenijska (Isogeny-based) kriptografija

Ova kategorija koristi kompleksnu strukturu eliptičkih krivih i izogenija između njih. Smatra se jednom od najnovijih i najsloženijih oblasti u PQC istraživanju.

4.5.1 SIKE, SIDH

- **SIKE (Supersingular Isogeny Key Encapsulation):** Baziran na isogenijama supersingularnih eliptičkih krivih. Bio je jedan od kandidata u NIST PQC procesu, ali je povučen nakon otkrića kvadratnog napada.
- **SIDH (Supersingular Isogeny Diffie-Hellman):** Ključni predak SIKE algoritma, koristi slične principe za razmenu ključeva.

Prednosti:

- Veoma male veličine ključeva i tajnosti komunikacije.
- Zanimljiv zbog jedinstvene strukture i inovativnosti.

Nedostaci:

- Veoma spori algoritmi u poređenju sa drugim PQC rešenjima.
- Ranjivosti pronađene 2022. godine dovele su do povlačenja SIKE iz NIST konkurencije.

5 Rešetkasta kriptografija u praksi - TLS protokol i Ring- LWE

5.1 Uvod u TLS i njegove sigurnosne komponente

- **TLS 1.3** je aktuelni standard za enkriptovanu komunikaciju na Internetu, pružajući poverljivost, integritet podataka i autentifikaciju klijenata/servera.
- Tradicionalne komponente:
- **Key exchange:** ECDH (Elliptic Curve Diffie-Hellman)
- **Autentifikacija:** RSA ili ECDSA potpisi
- Ključni problem: ovi sistemi su **ranjivi na kvantne napade** preko Shorovog algoritma [11]

5.2 Ring- LWE za razmenu ključeva

Razvoj postkvantne kriptografije zasniva se na traženju matematičkih problema za koje se veruje da ih čak ni kvantni računari ne mogu rešiti u razumnom vremenu. Jedan od najznačajnijih takvih problema jeste takozvani *Ring-Learning With Errors* (Ring-LWE). Ovaj problem potiče iz opšteg problema *Learning With Errors* (LWE), ali je prilagođen za rad u prstenovima polinoma. Ideja je da se koriste polinomi sa koeficijentima moduo velikog celog broja q , dok se u račun unosi i mali „šum“ (error) koji onemogućava napadaču da rekonstruše tajnu. Na taj način sigurnost se ne zasniva na klasičnim problemima poput faktORIZACIJE ili diskretnog logaritma, koje kvantni računari mogu lako rešiti pomoću Šorovog algoritma, već na problemima vezanim za rešetke (lattices) i njihove strukture. Posebno je važno što je dokazano da rešavanje Ring-LWE problema nije ništa lakše nego rešavanje najtežih problema na idealnim rešetkama u najgorem slučaju, pa se sigurnost ovakvih šema smatra veoma pouzdanom.

U kontekstu razmene kriptoključeva, Ring-LWE se koristi kao osnova za izgradnju protokola koji omogućavaju dvema stranama da, preko nesigurnog kanala, izgrade zajedničku tajnu. Sama procedura ima određene sličnosti sa poznatim Diffie-Hellman algoritmom, ali umesto multiplikacija u grupi koristi operacije nad polinomima u prstenu. Strane u komunikaciji generišu svoje tajne polinome i dodaju im mali šum, a zatim razmenjuju polinome dobijene množenjem sa javnim parametrima. Iako se zbog šuma rezultati na dve strane ne poklapaju u potpunosti, uvodi se dodatna faza koja se naziva *reconciliation*. Ova faza omogućava da se nesavršenosti usled šuma uklone i da se na obe strane dobije identičan zajednički ključ. Na taj način, iako je razmena javna, treća strana koja prisluškuje ne može da izračuna tajnu, jer bi za to morala da reši Ring-LWE problem, što je računski neizvodljivo.

Prednost Ring-LWE razmene ključeva ogleda se u efikasnosti i veličini ključeva. U poređenju sa klasičnim LWE pristupom, veličine ključeva i parametara su značajno smanjene, što omogućava bržu implementaciju i manje zahteve za memorijom. Ipak, u poređenju sa tradicionalnim sistemima kao što su RSA ili eliptičke krive, veličine ključeva su i dalje veće, ali se taj kompromis prihvata jer je sigurnost protiv kvantnih napada daleko viša. U praksi su razvijeni i testirani različiti protokoli zasnovani na Ring-LWE, kao što je *NewHope*, koji je korišćen i u eksperimentalnim verzijama TLS protokola od strane kompanija poput Google-a i Cloudflare-a. Parametri koji se koriste u ovim protokolima pažljivo su birani: na primer, za nivo sigurnosti od 128 bita tipično se bira polinom stepena 512 i moduli reda desetina hiljada, dok se za 256 bita koristi polinom stepena 1024 i još veći moduli. Time se postiže ekstremno mala verovatnoća neuspeha u procesu usklađivanja ključeva, što praktično znači da sistem radi pouzdano.

Dalji razvoj ovih ideja doveo je i do formiranja standarda. Najpoznatiji predstavnik je algoritam **CRYSTALS-Kyber**, koji se ne oslanja direktno na čisti Ring-LWE problem, već na njegovu varijantu poznatu kao Module-LWE (MLWE). Razlika je u tome što se umesto jednog prstena koristi struktura modula koja obezbeđuje još bolju efikasnost i fleksibilnost. Kyber je nakon višegodišnjeg procesa evaluacije izabran od strane američkog instituta NIST kao zvanični standard za postkvantnu razmenu ključeva i objavljen pod imenom **ML-KEM (FIPS 203)**. Ovaj standard definiše tri sigurnosna nivoa (ML-KEM-512, ML-KEM-768 i ML-KEM-1024), pri čemu svaki

nudi različit odnos između brzine, memorijskih zahteva i nivoa sigurnosti. Bitna odlika Kyber algoritma jeste to što generiše tajni ključ fiksne dužine od 256 bita, što ga čini kompatibilnim i lako primenljivim u postojećim bezbednosnim protokolima.

Kada se uporede Ring-LWE i Kyber, može se uočiti da oba pristupa počivaju na istoj ideji, korišćenju rešetkastih problema i unošenju šuma kako bi se sprečila rekonstrukcija tajne. Razlika je u formalizaciji: dok je Ring-LWE više matematički čist problem koji služi kao teorijska osnova, Kyber predstavlja praktičnu, optimizovanu implementaciju namenjenu standardizaciji i širokoj upotrebi. Upravo zato se u praksi danas, u realnim komunikacionim protokolima poput TLS-a ili VPN sistema, koristi Kyber odnosno ML-KEM, dok je Ring-LWE ostao ključni teorijski temelj koji obezbeđuje matematičku garanciju bezbednosti.

Na taj način, Ring-LWE za razmenu ključeva predstavlja most između teorijske osnove postkvantne kriptografije i njene praktične primene. On pokazuje kako je moguće izgraditi protokole koji su otporni na kvantne napade, efikasni u implementaciji i dovoljno sigurni za standardizaciju na globalnom nivou. CRYSTALS-Kyber, kao naslednik i praktična realizacija ideja Ring-LWE-a, danas predstavlja stub postkvantne sigurnosti i već se ugrađuje u infrastrukturu velikih kompanija kao što su Microsoft, Google i Cloudflare. Ovaj razvoj jasno pokazuje da se postkvantna kriptografija iz sfere istraživanja preselila u realnost i da će Ring-LWE i njegovi derivati biti osnova bezbedne komunikacije u decenijama koje dolaze. [12]

5.3 Mehanizam funkcionisanja Ring- LWE

- Generišu se mali nasumični polinomi i javni/privatni ključevi s dodatkom grešaka (error polinomi).
- Klijent enkapsulira zajednički ključ: šalje ciphertext baziran na javnom ključu servera i šumu.
- Server dekapulira korišćenjem svog privatnog ključa kako bi izvukao isti zajednički ključ.
- Greška se zaokružuje ("reconciliation") kako bi oba entiteta dobila isti ključ čak i uz minimalnu razliku [4]

5.4 Integracija u TLS protokol

Integracija postkvantnih algoritama u moderne sigurnosne protokole poput TLS-a 1.3 predstavlja ključni korak u prelasku ka bezbednoj komunikaciji u eri kvantnih računara. Jedan od najvažnijih alata za istraživanje i implementaciju ovih algoritama jeste **liboqs**, otvorena biblioteka koju razvija Open Quantum Safe projekat. Ona pruža implementacije različitih PQC algoritama i može se povezati sa bibliotekama kao što je OpenSSL 3, koristeći tzv. OQS provider. Na taj način, postkvantni algoritmi se mogu bez većih prepreka uključiti u TLS 1.3 suite-ove i koristiti zajedno sa već postojećim šemama.

Kompanija Cloudflare bila je među pionirima u ovim integracijama. Oni su među prvim testirali i implementirali tzv. **hibridni pristup**, u kojem se spajaju klasični algoritam X25519 (poznat i kao Curve25519 Diffie-Hellman) i postkvantni algoritam Kyber (ML-KEM). Ovakva kombinacija osigurava otpornost na buduće kvantne napade, dok istovremeno obezbeđuje povratnu kompatibilnost sa postojećim

sistemima. Drugim rečima, čak i ako PQC algoritam u budućnosti bude kompromitovan, sigurnost ostaje zaštićena zahvaljujući X25519; a ako kvantni računari razbiju klasične algoritme, sigurnost obezbeđuje Kyber. Time se dobija dvostruki sloj zaštite u TLS sesijama.

Pored same integracije, značajna pažnja posvećena je i performansama. Studije i eksperimenti pokazuju da su korišćenjem AVX-512 optimizacija u radu "*Faster Post-Quantum TLS 1.3 Based on ML-KEM*" postignuta značajna ubrzanja. Naime, generisanje ključeva ubrzano je za oko **1.64 puta**, dok je u *batch* režimu (istovremena obrada više TLS handshakes) postignuto ubrzanje od **3.5 do čak 4.9 puta**. Ovi rezultati potvrđuju da postkvantni TLS protokoli ne predstavljaju samo teorijski koncept, već i praktično izvodljivu opciju koja može da podrži performanse potrebne u današnjim velikim mrežnim sistemima, uključujući web servise sa milionima korisnika.

5.5 Performanse u odnosu na ECDH

Prirodno pitanje koje se postavlja jeste kako se postkvantni algoritmi ponašaju u poređenju sa klasičnim šemama za razmenu ključeva, pre svega sa eliptičko-krivnim Diffie-Hellmanom (ECDH). Rezultati testiranja i simulacija pokazuju da algoritmi poput **Kyber-a** i **Saber-a** ostvaruju performanse koje su ne samo konkurentne ECDH-u, već ga u mnogim slučajevima i nadmašuju.

Na primer, na platformi ARM Cortex-M4, koja se često koristi u ugrađenim sistemima i IoT uređajima, algoritam **Kyber512** ostvaruje vreme od približno **15 ms** za razmenu ključeva, dok za istu operaciju ECDH SECP256R1 troši oko **27 ms**. Ovakvi rezultati su od izuzetnog značaja, jer pokazuju da postkvantni algoritmi nisu samo sigurniji već mogu biti i brži na realnim hardverskim platformama.

Simulacije sprovedene u okviru konferencije NDSS i drugih istraživačkih radova potvrđuju da su u TLS handshake protokolu Kyber i Saber često podjednako brzi ili brži od ECDH-a, posebno u mrežnim okruženjima sa niskom latencijom i gubicima paketa manjim od 3–5%. Kada se posmatra primena u velikim cloud okruženjima, dodatna istraživanja kao što su ona sprovedena od strane AWS-a pokazuju da je overhead hibridnih šema zanemarljiv. U proseku, korišćenje kombinacije ECDHE + Kyber u handshake fazi povećava latenciju za svega **0.25 ms na strani klijenta** i **0.23 ms na strani servera**, dok je povećanje propusnog opsega oko **2.3 KiB** po sesiji. U poređenju sa ukupnim zahtevima modernih aplikacija i protokola, ovo je praktično neprimetno, a donosi ogromnu sigurnosnu prednost.

Ovi podaci jasno pokazuju da prelazak na postkvantne algoritme u TLS-u ne znači žrtvovanje performansi. Naprotiv, uz pažljivo odabrane parametre i optimizacije, PQC algoritmi mogu da obezbede i veću brzinu i efikasnost u poređenju sa današnjim standardnim rešenjima.

5.6 Hibridna šema (klasična + PQC)

Kako bi se obezbedio što viši nivo sigurnosti i istovremeno očuvala kompatibilnost sa postojećim sistemima, međunarodna zajednica, pre svega kroz rad IETF-a, predložila je koncept **hibridnih šema**. Suština ovog pristupa jeste kombinovanje klasičnih i

postkvantnih algoritama u istom protokolu. Najčešće korišćen primer jeste kombinacija **ECDH (X25519)** sa postkvantnim algoritmom **ML-KEM (Kyber)**.

Prednost ovakvog pristupa je očigledna: čak i ako jedna od šema bude kompromitovana u budućnosti, sigurnost i dalje ostaje očuvana. Ako kvantni računar uspe da razbije ECDH, sigurnost i dalje osigurava Kyber. Ako pak, u nekom neočekivanom scenariju, Kyber bude matematički oslabio, sigurnost ostaje zahvaljujući ECDH-u. Na taj način dobijamo mehanizam dvostruke zaštite, koji praktično eliminiše rizik od pojedinačnog kompromitovanja.

Studije sprovedene od strane Cloudflare-a i drugih istraživačkih centara potvrđuju da hibridni pristup ne uvodi značajne performansne probleme. Tipično, handshake u hibridnoj varijanti traje samo neznatno duže u odnosu na klasični, dok se u mrežnom saobraćaju javlja umereno povećanje veličine paketa (dodatni podaci u klijentskom Hello segmentu). Međutim, to povećanje je zanemarljivo u poređenju sa koristima koje donosi sigurnost otporna na kvantne napade.

Zbog toga se upravo hibridne šeme smatraju realnim rešenjem za prelazni period – sve dok postkvantni algoritmi ne budu u potpunosti standardizovani, testirani i usvojeni globalno. One omogućavaju da se današnji sistemi već sada zaštite od napada „snimi sada, razbij kasnije“, dok se istovremeno zadržava sigurnost i kompatibilnost u odnosu na postojeće infrastrukture.

6 Uporedna analiza performansi PQ algoritama

6.1 Brzina (latencija i throughput)

Benchmark analiza (Arif Dicle Demir et al., 2025)

U poslednjim godinama jedan od ključnih pravaca istraživanja u oblasti postkvantne kriptografije jeste detaljno testiranje performansi novih algoritama u realnim i kontrolisanim uslovima. Posebno značajna studija je rad Arif Dicle Demir i saradnika iz 2025. godine, u kojem su analizirani najvažniji predstavnici postkvantnih algoritama, Kyber kao predstavnik KEM (Key Encapsulation Mechanism) porodice i Dilithium kao predstavnik DSA (Digital Signature Algorithm) porodice. Ovi algoritmi su testirani kroz ključne operacije koje se koriste u realnim protokolima: generisanje ključeva (keygen), enkapsulacija i dekapulacija tajne (encap/decap), potpisivanje i verifikacija (sign/verify). Svaka operacija izvršena je čak 1000 puta kako bi se dobila što pouzdanija statistika, a rezultati su predstavljeni kroz medianu i prosek vremena izvršavanja. Hardverska platforma bila je standardni procesor od 3.3 GHz, što omogućava poređenje sa performansama tradicionalnih algoritama kao što su ECDH (za razmenu ključeva) i ECDSA (za digitalne potpise). Rezultati ovih eksperimenata jasno pokazuju da su postkvantni algoritmi spremni za praktičnu primenu. Naime, i Kyber i Dilithium u velikom broju slučajeva nadmašuju performanse ECDH i ECDSA pri uporedivim nivoima sigurnosti. Na primer, vreme potrebno za generisanje ključeva kod Kybera pokazalo se kraćim od ekvivalentnog ECDH procesa, dok je verifikacija potpisa kod Dilithiuma u mnogim slučajevima bila brža nego kod ECDSA

algoritma. Posebno je interesantno to što su performanse PQC algoritama stabilne i u većim opterećenjima - u batch scenarijima gde se izvršava veliki broj istovremenih TLS handshakes ili verifikacija potpisa, prednosti u brzini postaju još uočljivije. Ovo jasno pokazuje da prelazak na postkvantnu kriptografiju ne znači kompromis u performansama, već da se u pojedinim operacijama može dobiti i značajno ubrzanje u odnosu na klasične algoritme.

AVX optimizacije za Dilithium (Jieyu Zheng et al., 2023)

Pored teorijskih prednosti i osnovnih implementacija, veliki napredak u performansama postignut je korišćenjem optimizacija na nivou procesorskih instrukcija. Posebno značajan doprinos u tom pravcu dali su Jieyu Zheng i saradnici 2023. godine, u svom radu posvećenom optimizaciji Dilithium algoritma korišćenjem AVX2 i AVX-512 instrukcionih setova. Ove optimizacije ciljaju na iskorišćavanje sposobnosti modernih procesora da paralelno obrađuju više podataka, čime se značajno ubrzavaju osnovne aritmetičke operacije nad polinomima i matricama koje su u srecu Dilithium algoritma.

Rezultati ovih optimizacija bili su impresivni. Prema izveštajima autora, generisanje ključeva (key generation) ubrzano je za 43–46%, dok je operacija potpisivanja (signing) ubrzana za 36–44% u zavisnosti od bezbednosnog nivoa (Dilithium2, Dilithium3 ili Dilithium5). Još značajnije, operacija verifikacije potpisa postigla je ubrzanje od čak 45–47% zahvaljujući optimizacijama na nivou AVX instrukcija. Ovakvi rezultati potvrđuju da se PQC algoritmi ne samo oslanjaju na teoretsku otpornost na kvantne napade, već i da mogu biti implementirani na način da zadovolje visoke performanske zahteve modernih informacionih sistema.

Ove optimizacije su od suštinske važnosti za realnu primenu. Digitalni potpisi se koriste u ogromnom broju transakcija i komunikacija na internetu, od TLS handshakes do potpisivanja softverskih paketa i dokumenata. Ako bi ovi algoritmi bili prespori, njihova integracija u globalne sisteme bila bi gotovo neizvodljiva. Međutim, zahvaljujući ovakvim radovima jasno se pokazuje da postkvantni potpisi poput Dilithiuma mogu biti čak i brži od današnjih ECDSA rešenja, posebno na modernim procesorima sa AVX podrškom. Time se otklanja jedna od najvećih prepreka šire implementacije PQC algoritama i omogućava njihova upotreba u sistemima koji obrađuju milione korisničkih zahteva dnevno.

Mrežna integracija (Sosnowski et al., 2023)

Jedan od ključnih izazova uvođenja postkvantne kriptografije u realne sisteme jeste pitanje kako se novi algoritmi ponašaju u mrežnom okruženju, gde osim samih matematičkih operacija značajnu ulogu imaju i faktori poput latencije, širine propusnog opsega i pouzdanosti veze. U tom kontekstu posebno je važna studija Sosnowski i saradnika iz 2023. godine, koja se fokusirala na integraciju PQC algoritama u TLS 1.3 protokol i analizu njihovih performansi u realističnim mrežnim uslovima. U eksperimentima su testirana dva scenarija: hibridni pristup, u kojem se kombinuju klasični i postkvantni algoritmi, i PQC-only pristup, gde se koriste isključivo postkvantni mehanizmi. Rezultati su pokazali da algoritmi kao što su Kyber i HQC postižu performanse na nivou modernih, široko korišćenih šema, dok su Dilithium i Falcon u nekim slučajevima čak brži od RSA algoritma kada se porede na

višim nivoima sigurnosti. To znači da prelazak na postkvantnu kriptografiju ne mora nužno da znači kompromis u brzini rada protokola, već u određenim uslovima može doneti i dodatna ubrzanja. Ono što je posebno značajno jeste da u studiji nisu uočeni značajni performanski nedostaci prilikom upotrebe PQC algoritama u TLS 1.3. Iako se donekle povećava veličina ključeva i sertifikata, što utiče na širinu propusnog opsega, ove promene nisu bile dovoljno velike da bi predstavljale prepreku za praktičnu primenu. U hibridnom scenariju dodatni overhead bio je minimalan, a ukupno vreme TLS handshaka ostalo je u granicama koje omogućavaju upotrebu u realnim mrežnim sistemima.

Rezultati Sosnowskog i saradnika potvrđuju da je mrežna integracija PQC algoritama tehnički izvodljiva i da može da se sprovede bez ozbiljnih posledica po korisničko iskustvo. Ovo je izuzetno važna poruka za industriju, jer pokazuje da prelazak na postkvantne standarde ne mora da bude težak ni sa aspekta performansi ni sa aspekta interoperabilnosti. Naprotiv, kako su pokazali testovi, algoritmi poput Kybera, HQC-a, Dilithiuma i Falcona već sada mogu uspešno da se uključe u TLS 1.3 i da obezbede sigurnost protiv kvantnih napada, a da se pri tom očuva brzina i pouzdanost moderne internet komunikacije. [5]

6.2 Veličina ključeva i memorijski zahtevi

Jedan od najvažnijih aspekata postkvantnih algoritama, pored njihove sigurnosti i brzine izvršavanja, jesu i veličina kriptografskih ključeva i memorijski zahtevi za njihovu upotrebu. Ovo je od posebne važnosti u realnim sistemima, gde ograničenja hardvera, propusnog opsega i potrošnje energije mogu biti presudna za izbor algoritma. Iako su postkvantni algoritmi projektovani da budu sigurni protiv kvantnih napada, njihova efikasnost u pogledu zauzeća memorije i veličine podataka ima direktan uticaj na mogućnost njihove široke primene, naročito u uređajima sa ograničenim resursima. Prema poređenjima koja se mogu naći u literaturi i tabelama sa Wikipedia stranica i akademskih radova, postkvantni algoritmi imaju značajno različite karakteristike kada je reč o veličini javnih i privatnih ključeva, kao i digitalnih potpisa ili šifrovanih poruka. Na primer, ML-DSA (Dilithium), koji je jedan od standardizovanih algoritama za digitalne potpise, ima javni ključ veličine oko 1 312 bajtova, privatni ključ oko 2 560 bajtova, dok su potpisi relativno veliki i dostižu oko 2 420 bajtova. Drugačiji pristup nudi SPHINCS+, hash-bazirani algoritam, kod kojeg je javni ključ manji, oko 1 000 bajtova, ali su potpisi izrazito veliki i u proseku prelaze 8 000 bajtova. Ovo ga čini nepraktičnim za aplikacije gde se često razmenjuju potpisi, poput TLS handshaka, ali može biti pogodan u situacijama kada je potrebno potpisati retke, ali kritične poruke. Kada se pogleda grupa algoritama za razmenu ključeva, najviše pažnje privlači Kyber512, koji u poređenju sa konkurencijom pokazuje veoma uravnotežen profil. Njegov javni ključ zauzima oko 1 184 bajta, dok je šifrat (ciphertext) oko 1088 bajtova, a privatni ključ zauzima približno 2 400 bajtova. Ove vrednosti predstavljaju značajan kompromis između sigurnosti i praktičnosti, jer omogućavaju da se Kyber uklopi u postojeće mrežne protokole bez velikih izmena i dodatnih troškova u pogledu propusnog opsega. Upravo zato je Kyber i izabran kao standardni KEM algoritam u okviru NIST-ovog procesa standardizacije. Praktični testovi na ograničenim uređajima dodatno osvetljavaju realnu upotrebljivost ovih algoritama. Studija sprovedena na Raspberry Pi platformama pokazala je da Kyber ima najbolji odnos između vremena izvršenja, potrošnje energije, zauzeća memorije i generisane toplote. Drugim rečima, Kyber se

pokazao kao optimalan izbor za male uređaje i IoT okruženja, gde su resursi veoma ograničeni, a energetska efikasnost ključna. Nasuprot tome, algoritmi kao što su BIKE i HQC pokazali su značajno veće zahteve za memorijom, posebno u višim sigurnosnim konfiguracijama. Na primer, HQC-256 je zahtevao čak oko 6 000 KB memorije, što je značajno opterećenje za male uređaje. Pored memorije, ovakvi algoritmi troše i više energije – zabeležena je prosečna potrošnja od oko 4.7 W, što predstavlja ozbiljno ograničenje za upotrebu u prenosnim uređajima ili senzorima na baterije.

Iz ovih podataka jasno se vidi da je prilikom izbora PQC algoritama potrebno voditi računa ne samo o sigurnosnom nivou i matematičkoj otpornosti, već i o praktičnim parametrima kao što su veličina ključeva i potrošnja memorije. Dok algoritmi poput SPHINCS+ mogu biti korisni u specijalizovanim aplikacijama gde se sigurnost stavlja ispred svih drugih faktora, algoritmi poput Kybera nude izuzetno dobar balans i mogu se primeniti u širokom spektru sistema, od serverskih aplikacija do malih IoT uređaja. Upravo ovakva prilagodljivost bila je jedan od ključnih razloga zbog kojih je Kyber izabran kao primarni standard za postkvantnu razmenu ključeva.

6.3 Sigurnost i otpornost na kvantne napade

Jedan od ključnih kriterijuma u odabiru postkvantnih algoritama jeste njihova otpornost na poznate i predvidive napade kvantnih računara. Među kandidatima koje je standardizovao NIST, Kyber (kao KEM) i Dilithium (kao DSA) posebno se izdvajaju jer se zasnivaju na problemima iz oblasti rešetki, pre svega Learning With Errors (LWE) i njegovoj varijanti Ring-LWE. Ovi problemi se smatraju matematički teškim i za klasične i za kvantne računare, jer ne postoji poznat efikasan algoritam koji bi mogao da ih reši u polinomialnom vremenu. Upravo ta matematička čvrstina omogućila je da Kyber i Dilithium budu uvršteni među finaliste NIST-ove standardizacije postkvantne kriptografije i da postanu okosnica buduće sigurnosne infrastrukture. Ono što ih dodatno izdvaja jeste otpornost na najpoznatije kvantne algoritme, uključujući **Šorov algoritam** i **Groverov algoritam**. Šorov algoritam je posebno poguban za klasične šeme kao što su RSA ili ECDH, jer efikasno rešava problem faktORIZACIJE i diskretnog logaritma, čime potpuno narušava njihovu sigurnost. Međutim, za rešetkaste probleme poput LWE i Ring-LWE, Šorov algoritam ne nudi nikakvo ubrzanje. Groverov algoritam, sa druge strane, može teoretski prepoloviti sigurnost brute-force pretrage, ali zbog načina na koji su parametri odabrani u Kyberu i Dilithiumu, ovaj uticaj se ublažava jednostavnim povećanjem dimenzija rešetke i broja bitova. Na taj način, postkvantni algoritmi ostaju dovoljno sigurni i u scenariju gde napadač raspolaže kvantnim računarom. Dodatni sloj analize sigurnosti pružaju tzv. **kvantno-postkvantne (KP) analize**, koje su obuhvaćene i u radovima poput onih koje je objavio Arif Dicle Demir sa saradnicima. Ove analize kvantifikuju sigurnost algoritama u jedinicama resursa koje bi napadaču bile potrebne: meri se broj kvantnih bita (qubits) i broj logičkih operacija (gate-ova) koje bi napad zahtevao. Na osnovu tih metrika može se uporediti realna izvodljivost napada u odnosu na postojeće i buduće tehnologije kvantnih računara. Rezultati ovih analiza pokazuju da lattice-bazirane šeme, poput Kybera i Dilithiuma, pružaju najbolji balans između troška napada i garantovanog nivoa sigurnosti. Na primer, za kompromitovanje Kyber-768 ili Dilithium-3 potrebno bi bilo više miliona stabilnih qubita i ogromna količina kvantnih operacija, što je daleko iznad mogućnosti današnjih ili čak predviđenih kvantnih računara u narednim decenijama. Zbog toga se

Kyber i Dilithium danas posmatraju kao stubovi postkvantne kriptografije: oni kombinuju matematičku čvrstinu sa dokazima o praktičnoj otpornosti na kvantne napade. Dok su drugi kandidati, poput hash-baziranog SPHINCS+ ili kod-baziranih BIKE/HQC šema, takođe sigurni, prednost rešetkastih algoritama jeste u tome što postižu bolji kompromis između sigurnosti, performansi i memorijskih zahteva. Kvantne analize jasno potvrđuju da su lattice-bazirani algoritmi najotporniji izbor i da predstavljaju realno rešenje za buduću digitalnu sigurnost u svetu u kojem kvantni računari postaju sve snažniji.

6.4 Efikasnost u aplikacijama (e-mail, TLS, kriptovalute)

Simulacija TLS i TCP/IP (RQ: Arax PB – Sosnowski et al., 2023)

PQC- TLS vs klasični TLS: nema značajne dodatne latentnosti; pri višim sigurnosnim nivoima PQC čak bolje performira nego ECDSA/RSA u verifikaciji i potpise.[12]

Embedded IoT simulacija (Raspberry Pi)

Korišćenjem liboqs + mbedTLS, testirane su tri KEM opcije: BIKE, HQC, Kyber

Za file prenos (208–2328 B), Kyber zabeležio najniže vreme izvršenja (<0.1–0.2 s), dok BIKE i HQC bili sporiji ~2–3× u višim sigurnosnim nivoima. [13]

Video i aplikacije:

GPU implementacija Dilithium pokazuje 10 000 potpisa/ocena po 32 ms (signing) i 15 ms (verify) - idealna za masovne operacije u blockchain ili serverskim farmama.[13]

Tabelarni prikaz (Tabela 1)

Metrika	Kyber (KEM)	Dilithium (Signature)	SPHINCS+	BIKE / HQC (KEM)
Keygen latency	~1–3 ms	~2–4 ms (AVX opt)	desetine ms	~80–200 ms na Pi
Encapsulation / Signing	~1–2 ms	~2–3 ms (AVX opt)	30–100 ms	BIKE/HQC sporiji
Verification / Decapsulation	~1–2 ms	~1–2 ms (AVX opt)	veća latencija	BIKE/HQC nešto sporiji
Public key size (NIST L1)	~1 KB	~1.3 KB	~8 KB	HQC ~1–3 KB, BIKE varira
Signature / ciphertext size	~1 KB (ciphertext)	~2.4 KB (signature)	>8 KB	BIKE/HQC ~1–2 KB ciphertext
Memory (Raspberry Pi)	~4 KB	malo	veće	HQC visok, BIKE srednji
Throughput (GPU/pdf)	više stotina/s	10 000/s potpis	malo	NIJE optimizovano
Energetska potrošnja	niska	niska	visoka	HQC visoka
OTPP Sigurnost	NIST L1/L3/L5	NIST L1/L3/L5	L1–L5	QEM varira, HQC manje stabilan

Tabela 1: Poređenje performansi post-kvantnih kriptografskih algoritama (Kyber, Dilithium, SPHINCS+, BIKE/HQC)

Primer kod simulacije (Raspberry Pi benchmark) – pseudo-C [14]

```
#include <oqs/oqs.h>

#include <time.h>

// Benchmark KEM on Kyber512

OQS_KEM *kem = OQS_KEM_new(OQS_KEM_alg_kyber_512);

uint8_t *pk = malloc(kem->length_public_key);

uint8_t *sk = malloc(kem->length_secret_key);

uint8_t *ct = malloc(kem->length_ciphertext);

uint8_t *ss = malloc(kem->length_shared_secret);

clock_t t0 = clock();

OQS_KEM_keypair(kem, pk, sk);

clock_t t1 = clock();

OQS_KEM_encaps(kem, ct, ss, pk);

clock_t t2 = clock();

OQS_KEM_decaps(kem, ss, ct, sk);

clock_t t3 = clock();

printf("Keygen: %f ms\nEncap: %f ms\nDecap: %f ms\n",

      (t1 - t0)*1000.0 / CLOCKS_PER_SEC,

      (t2 - t1)*1000.0 / CLOCKS_PER_SEC,

      (t3 - t2)*1000.0 / CLOCKS_PER_SEC);
```

E-mail komunikacija (PGP, S/MIME)

Zahtevi: Brzo generisanje ključeva, mali potpis i šifrat zbog ograničenja veličine poruke.

PQ algoritmi u upotrebi:

CRYSTALS-Kyber (šifrovanje) i CRYSTALS-Dilithium (digitalni potpis) su najpogodniji za ovu upotrebu jer su zvanično odabrani od strane NIST-a.

Performanse:

- Potpisi su nešto veći od RSA, ali manji od SPHINCS+.
- Brzina potpisivanja/verifikacije je značajno viša od kod klasičnih algoritama.

Simulacija u Pythonu (Pyca + PQCrypto):

```
from pqcrypto.sign.dilithium2 import generate_keypair, sign, verify

# Generiši ključeve

public_key, secret_key = generate_keypair()

# Potpiši poruku

msg = b"Email content: confidential."

sig = sign(msg, secret_key)

# Verifikuj

try:

    verify(msg, sig, public_key)

    print("Valid signature.")

except:

    print("Signature verification failed.")
```

TLS/HTTPS protokol (sigurnost web komunikacije)

Zahtevi: Mala latencija, podrška za brze handshake mehanizme.

PQTLS: Eksperimentalne implementacije poput OpenQuantumSafe omogućavaju testiranje Kyber i Dilithium unutar TLS protokola.

Implementacije:

Google Chrome + Cloudflare testirali su Kyber512 u hibridnom modusu (Kyber + X25519).

Rezultati:

- Latencija handshake-a povećana za ~1–2 ms.
- Veličina handshake poruka porasla za nekoliko stotina bajtova.
- Bezbednost drastično povećana.

Kriptovalute i blockchain (Ethereum, Bitcoin, itd.)

Zahtevi: Brzo verifikovanje potpisa, minimalan uticaj na veličinu blokova, sigurnost protiv kvantnih napada.

Kandidati:

Dilithium i SPHINCS+ su razmatrani za zamenu ECDSA potpisa.

Analiza:

SPHINCS+ koristi hash funkcije — visok nivo sigurnosti ali **veoma veliki potpisi** (do 40 KB).

Dilithium ima manje potpise (~2.5 KB) i mnogo brže verifikacije.

Stanje u industriji:

Kompanije poput IBM i Zama već testiraju PQ potpise za pametne ugovore. Istražuje se mogućnost “dual signature” pristupa (klasičan + PQ potpis).

```
from pqcrypto.sign.dilithium2 import generate_keypair, sign
```

```
public_key, private_key = generate_keypair()
```

```
transaction = b"user1 -> user2: 1.5 BTC"
```

```
signature = sign(transaction, private_key)
```

Potpis se čuva uz transakciju i verifikuje prilikom obrade bloka.

Aplikacija	Algoritam	Ključ (B)	Latencija	Sigurnost
E-mail (PGP)	Dilithium2	~1,312	Niska	Visoka
TLS 1.3	Kyber512	~1,600	Niska	Visoka
Blockchain	SPHINCS+	32–64	Visoka	Veoma visoka

Tabela 2: Primer primene post-quantum algoritama u različitim aplikacijama

Cilj:

Pokrenuti TLS server koji koristi postkvantnu kriptografiju (tačnije algoritam Kyber) umesto klasičnih algoritama kao što su RSA ili ECDSA, radi testiranja otpornosti na kvantne napade.

Komande - korak po korak:

1. Kloniranje repozitorijuma:

bash

CopyEdit

```
git clone https://github.com/open-quantum-safe/openssl
```

Ova komanda preuzima izvorni kod posebne verzije OpenSSL biblioteke koji je razvijen u okviru projekta Open Quantum Safe (OQS).

Ova verzija sadrži podršku za postkvantne algoritme kao što su Kyber, Dilithium, Falcon itd.

OpenSSL je najčešće korišćena biblioteka za kriptografske operacije u web komunikaciji, uključujući HTTPS i TLS/SSL.

2. Ulasci i kompajliranje:

bash

CopyEdit

```
cd openssl
```

```
./configure
```

```
make
```

Ove komande označavaju sledeće:

cd openssl: ulazi u direktorijum projekta.

./configure: priprema konfiguraciju za kompajlaciju. Ova skripta proverava vaš sistem i priprema Makefile prema vašim bibliotekama, CPU-u i opcijama.

make: kompajlira ceo projekat i pravi izvršne fajlove, uključujući openssl komandnu liniju i biblioteku.

Napomena: ako želimo podršku za OQS, često moramo da imamo i OQS-OpenSSL wrapper i liboqs instaliran. Moguće je da ova verzija već uključuje sve potrebno.

3. Pokretanje TLS servera sa Kyber algoritmom:

Bash

CopyEdit

```
./apps/openssl s_server -cert server.pem -key server.key -tls1_3
```

Objašnjenje:

Ova komanda koristi OpenSSL alatku s_server za pokretanje TLS servera (kao što je HTTPS server), uz sledeće attribute:

Parametar	Objašnjenje
<code>s_server</code>	Pokreće server koji koristi TLS protokol (SSL) za sigurnu komunikaciju
<code>-cert server.pem</code>	Sertifikat servera (X.509), potreban za TLS sesiju
<code>-key server.key</code>	Privatni ključ servera, koji se koristi za potpisivanje i otključavanje podataka
<code>-tls1_3</code>	Forsira upotrebu TLS 1.3 protokola, koji podržava nove algoritme i bolju sigurnost

Tabela 3: Parametri za konfiguraciju TLS servera i njihovo značenje

Gde je ovde Kyber?

Kyber se koristi kao algoritam za uspostavljanje zajedničkog tajnog ključa (key exchange mechanism), umesto klasičnog ECDHE ili RSA. Ako je OQS verzija OpenSSL-a pravilno konfigurisana i linkovana sa liboqs, onda će automatski podržavati Kyber kao algoritam za KEM (Key Encapsulation Mechanism). Mora da se navede koja tačno varijanta KEM se želi (npr. `p256_kyber512`) pri pokretanju ili kroz konfiguraciju.

Kako da testiramo klijenta?

Možemo da koristimo modifikovani openssl klijent iz OQS verzije, ili običan openssl `s_client`, ili još bolje - testiranje kroz Chrome/Firefox Nightly sa PQ podrškom ili cURL:

```
bash
CopyEdit
./apps/openssl s_client -connect localhost:4433 -groups p256_kyber512
```

-groups koristi hybrid KEM: klasični p256 + postkvantni kyber512.

Primer sertifikata

Ako nemamo `server.pem` i `server.key`, možemo da ih generišemo ovako:

```
bash
CopyEdit
openssl req -x509 -newkey rsa:2048 -keyout server.key -out server.pem -days 365 -nodes
Gde je korisno?
```

- Postkvantni TLS server kao ovaj je:
- Osnova za testiranje sigurne web komunikacije u eri kvantnih računara.
- Koristan za aplikacije koje zahtevaju visok stepen sigurnosti (npr. e-mail enkripcija, bankarske aplikacije, kriptovalute, vojna primena).

Simulacija brzine i sigurnosti

U poređenju s klasičnim algoritmima:

Algoritam	Vreme handshake-a (ms)	Veličina ključa (B)	PQ Sigurnost
RSA 2048	3	256	
ECDSA P-256	2	64	
Kyber512	2.5	800	postkvantna otpornost
Kyber1024	3.2	1568	viši nivo otpornosti

Tabela 4: Poređenje performansi klasičnih i postkvantnih algoritama u TLS handshake-u

7 Zaključak

7.1 Prednosti PQC algoritama

Postkvantni kriptografski (PQC) algoritmi predstavljaju ključni korak ka očuvanju poverljivosti i integriteta digitalne komunikacije u eri kvantnih računara. Za razliku od klasičnih algoritama poput RSA i ECC, koji postaju ranjivi pod napadima kvantnih algoritama kao što je Shorov, PQC algoritmi zasnovani su na matematičkim problemima za koje nisu poznati efikasni kvantni algoritmi rešenja. Neke ključne prednosti su:

- Otpornost na kvantne napade: PQC algoritmi obezbeđuju sigurnost i u postkvantnom okruženju.
- Fleksibilnost primene: Mogu se koristiti u već postojećim protokolima poput TLS, VPN, e-mail enkripcije i digitalnog potpisivanja dokumenata.
- Performanse: Odabrani algoritmi poput Kyber i Dilithium pokazali su izuzetnu efikasnost u realnim aplikacijama, čak i na ograničenim sistemima (embedded uređaji).

7.2 Preporuke za buduću migraciju

Da bi prelazak sa klasične na postkvantnu kriptografiju bio uspešan, neophodno je planirati i sprovesti postepenu migraciju uz sledeće preporuke:

- Hibridni pristup: U početnim fazama preporučuje se kombinacija klasičnih i PQC algoritama kako bi se obezbedila kompatibilnost i dodatna sigurnost.
- Pilot-projekti: Uvođenje PQC algoritama u test okruženja omogućava detekciju problema u kompatibilnosti, performansama i skalabilnosti.
- Praćenje standardizacije: Pratiti smernice NIST-a i integrisati samo one algoritme koji su prošli višegodišnju kriptografsku evaluaciju.
- Edukacija kadra: Obezbediti edukaciju programera i sistemskih administratora o karakteristikama PQC algoritama i njihovoj implementaciji.

7.3 Važnost pravovremene pripreme

Kvantni računari još uvek nisu masovno dostupni, ali njihova pojava može momentalno ugroziti sigurnost podataka koji se trenutno čuvaju ili prenose. Zbog toga je:

- Neophodno pravovremeno planirati prelazak, kako bi se izbegla “harvest now, decrypt later” (sakupi sada, dešifruj kasnije) pretnja.
- Institucije i firme koje obrađuju poverljive podatke, poput vlada, banaka, zdravstva, moraju već danas ulagati u PQC infrastrukturu.
- Diverzifikacija algoritama takođe igra ključnu ulogu, korišćenje više različitih PQC šema smanjuje rizik od jednokratnog kvara cele sigurnosne strukture.

Završna napomena

Algoritmi Kyber (ML-KEM) i Dilithium (ML-DSA) pokazali su se kao najsnažniji kandidati za široku upotrebu zahvaljujući balansu između sigurnosti i performansi. Iako SPHINCS+, BIKE i HQC nude dodatne opcije i sigurnosne paradigme, njihova upotreba zavisi od specifičnih potreba i raspoloživih resursa.

Priprema za postkvantnu budućnost nije opcija - to je imperativ.

8 Literatura

Knjige/Naučno-istraživački radovi

- [1] Michael A. Nielsen, 2010, Quantum Computation and Quantum Information, Cambridge University Press
- [2] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
- [3] Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: quantum resource estimates. In Proceedings of PQCrypto 2016 (LNCS). Springer.
- [4] Oded Regev(2009).On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Internet izvori

- [5] <https://www.mdpi.com/2410-387X/9/2/32> (datum pristupa 05.09.2025)
- [6] <https://www.youtube.com/watch?v=lvTqbM5Dq4Q>, (datum pristupa 30.07.2025)
- [7] https://blog.cloudflare.com/pq-2024/?utm_source/, (datum pristupa 05.09.2025)
- [8] <https://blog.cloudflare.com/post-quantum-to-origins/>, (datum pristupa 05.09.2025)
- [9] https://www.google.com/search?sca_esv=256ed5f0640d982f&rlz=1C1ONGR_enRS1116RS1116&sxsrf=AE3TifMutHtFpdwn4CNXpRGiVuQow7TQGw:1757168631494&udm=7&fbs=AIjpxHx_pWn3yifdDwPtDVOaJfQXQUATRgG-vpxTRh7TOSjeeHi3qZ9AwnhrnCn1S7iyoNvfCleH4LuHBMxvrutQ8BJ-tzggq8gD92h4xjNAtaMROAgmpvjNJfwUD8x8akTb86n1O3nhHI_wZ5MbqNOYJa1Y4z8gGHqu9I04KKCfdu1-CW44QohDI-P4Ss3bSlhyXD7mG-gAWlKdombQ2qb0EVmcZ4L5jYquS9Gc2zwY208aOJfD9TdE&q=merkle+tree&sa=X&ved=2ahUKEwjuy9ygg8SPAxU8SvEDHalGJOsQtKgLegQIFRAB&biw=1536&bih=730&dpr=1.25#fpstate=ive&vld=cid:80ef67b6,vid:FaTB91EQGzM,st:0 (datum pristupa 02.08.2025)
- [10] <https://pq-crystals.org/index.shtml>, (datum pristupa 07.08.2025)
- [11] https://tmo.jpl.nasa.gov/progress_report/42-44/44N.PDF, (datum pristupa 07.08.2025)
- [12] <https://net.in.tum.de/homepage/>, (datum pristupa 02.08.2025)
- [13] <https://arxiv.org/>, (datum pristupa 02.08.2025)
- [14] <https://github.com/open-quantum-safe/liboqs> (01.08.2025)