Stručni rad
UDK 621.39:004.8
DOI 10.7251/BLCZR0125085C

RAZVOJ I PRIMJENA KVANTNO-OTPORNOG KRIPTOGRAFSKOG SISTEMA U TELEKOMUNIKACIJAMA UZ PRIMJENU UMJETNE INTELIGENCIJE ZA UNAPREĐENJE SIGURNOSTI I PERFORMANSI

Čelarević Armin[1]

SAŽETAK

Ubrzani razvoj tehnologija poput 5G, Internet stvari (IoT), autonomnih sistema i pametnih gradova donosi značajan napredak u digitalnoj komunikaciji, ali istovremeno povećava zahtjeve za sigurnošću. Kvantni računari, iako još uvijek u razvoju, predstavljaju ozbiljnu prijetnju savremenim kriptografskim algoritmima poput RSA, DSA i ECC, koji čine temelj današnje digitalne sigurnosti. Njihova sposobnost izvođenja složenih kvantnih algoritama, poput Shorevog, omogućava razbijanje postojećih šifrarskih sistema, čime se otvara prostor za kompromitaciju podataka u telekom mrežama. Kao odgovor, razvijaju se kvantno-otporni kriptografski sistemi koji zahtjevaju visoku efikasnost, naročito u distribuiranim i kompleksnim mrežnim okruženjima. U tom kontekstu, umjetna inteligencija (AI) igra ključnu ulogu. Omogućava analizu podataka u realnom vremenu, detekciju prijetnji, upravljanje ključevima i optimizaciju sigurnosnih protokola. Ova tema dobija na važnosti s pojavom 6G mreža, koje donose još veću decentralizaciju, broj povezanih uređaja i potrebu za naprednim sigurnosnim sistemima.

KLJUČNE RIJEČI: *Kvantno-otporna kriptografija, Umjetna inteligencija, Digitalna sigurnost, Enkripcija, Sigurnosni protokoli*

DEVELOPMENT AND APPLICATION OF A QUANTUM-RESISTANT CRYPTOGRAPHIC SYSTEM IN TELECOMMUNICATIONS USING ARTIFICIAL INTELLIGENCE TO IMPROVE SECURITY AND PERFORMANCE

ABSTRACT

The rapid development of technologies such as 5G, the Internet of Things (IoT), autonomous systems and smart cities is bringing significant advances in digital communication, but at the same time increasing security requirements. Quantum computers, although still in development, pose a serious threat to modern cryptographic algorithms such as RSA, DSA and ECC, which

1 Master of Electrical Engineering, celarevicarmin@gmail.com

form the basis of today's digital security. Their ability to execute complex quantum algorithms, such as Shore's, allows for the breaking of existing encryption systems, thus opening up the possibility of compromising data in telecom networks. In response, quantum-resistant cryptographic systems are being developed that require high efficiency, especially in distributed and complex network environments. In this context, artificial intelligence (AI) plays a key role. It enables real-time data analysis, threat detection, key management and optimization of security protocols. This topic gains importance with the advent of 6G networks, which bring even greater decentralization, the number of connected devices and the need for advanced security systems.

KEYWORDS: *Quantum-resistant Cryptography, Artificial Intelligence, Digital Security, Encryption, Security Protocols*

UVOD

U savremenom digitalnom društvu, telekomunikacione mreže čine ključnu infrastrukturu za svakodnevno funkcionisanje privrede, države i građana. Razvoj tehnologija kao što su 5G, IoT, autonomni sistemi i pametni gradovi stvara složene mreže arhitekture koje zahtjevaju visok novo sigurnosti, dostupnosti i otpornosti na napade. Međutim, paralelno sa ovim razvojem, ubrzano napreduje i oblast kvantnog računarstva, koja potencijalno ugrožava temeljne principe današnje digitalne sigurnosti.

Kvantni računari, korištenjem kvantnih bitova (qbita) i algoritama poput Shorevog i Graverovog, mogu efikasno riješiti matematičke probleme na kojima se zasnivaju klasični kriptografski algoritmi kao što su RSA, DSA i ECC. Time dolazi do erozije povjerenja u postojeće sigurnosne protokole koji štite komunikaciju, autentifikaciju i digitalne transakcije. Zbog toga se u posljednjoj deceniji intenzivno razvijaju tzv. kvantno-otporni (post-kvantni) kriptografski algoritmi, koji se temelje na problemima za koje kvantni računari ne prižaju efikasna rješenja kao što su rešetke, hash funkcije i kodna teorija [D. J. Bernstein, J. Buchmann, and E. Dahmen].

U isto vrijeme, umjetna inteligencija (AI) postaje neizostavan alat u oblasti mrežne sigurnosti, s posebnim naglaskom na sposobnost prepoznavanja obrazaca, adaptivnog reagovanja i upravljanja kompleksnim sistemima. Uvođenje kvantno-otpornih protokola u distribuirane telekomunikacione mreže stvara izazove u pogledu performansi, upravljanja kriptografskim ključevima, detekcije prijetnji i fleksibilnosti sigurnosnih politika. AI posebno u formi mašinskog i dubokog učenja, omogućava optimizaciju enkripcije, predikciju napada i efikasno upravljanje kriptografskim resursima u realnom vremenu [T. Kim].

Pojava 6G mreža dodatno naglašava potrebu za naprednim sigurnosnim rješenjima. Očekuje se da će 6G donijeti masovno umrežavanje uređaja, ultra nisku latenciju i decentralizovanu obradu podataka na ivici mreže (edge computing), što stvara složenije sigurnosne izazove [W. Saad]. integracija kvantno-otporne kriptografije i umjetne inteligencije u ovu novu mrežnu paradigmu predstavlja neophodan korak prema stvaranju sigurnosnih sistema koji su proaktivni, prilagodljivi i dugoročno održivi.

1. TEORIJSKI I TEHNOLOŠKI TEMELJI KVANTNO-OTPORNE SIGURNOSTI U TELEKOMUNIKACIJAMA

Kvantni računari predstavljaju fundamentalni iskorak u razvoju računarskih sistema, baziran na principu kvantne mehanike, kao što su superpozicija i kvantna spregnutost. Dok

klasični računari koriste bitove koji mogu imati vrijednost 0 ili 1, kvantni računari koriste kvantne bitove, koji mogu istovremeno biti u više stanja. Ova osobina omogućava paralelno izvođenje velikog broja računskih operacija čime se značajno povećava efikasnost u rješavanju određenih klasa problema [M. A. Nielsen]. Uprkos činjenici da su kvantni računari još uvijek u ranoj fazi primjene, njihova potencijalna primjena u oblastima kriptografije, simulacija, optimizacije i biomedicine već izaziva snažan interes naučne zajednice i industrije [F. Arute].

Dva kvantna algoritma imaju posebno značajan uticaj na sigurnost digitalne komunikacije:

- Shorov algoritam
- Groverov algoritam

Shorov algoritam omogućava faktorisanje velikih brojeva u polinomnom vremenu, čime direktno ugrožava sigurnost RSA kriptosistema i drugih šema koje se oslanjaju na teškoću faktorisanja i diskretnog algoritma [P. W. Shor]. Budući da je RSA temelj za mnoge sigurnosne protokole uključujući TLS/SSL, VPN i digitalne potpise njegova ranjivost u kvantnom okruženju izaziva ozbiljnu zabrinutost.

Groverov algoritam, iako manje razoran, omogućava ubrzanje pretrage nestruktuiranih baza podataka kvadratnim faktorom. U kontekstu simetrične kriptografije, kao što je AES, to znači da bi sigurnost 256 – bitnog ključa pala na nivo 128 – bitne sigurnosti, što je i dalje prihvatljivo, ali zahtjeva prilagođavanje dužine ključeva i pojačavanje algoritama [L. K. Grover]. Ovi algoritmi predstavljaju ključne razloge zašto su u fokusu međunarodne zajednice istraživanja kvantno-otpornih alternativa.

Najznačajnije klase kvantno-otpornih algoritama uključuju:

- Rešetkasto zasnovanu kriptografiju (Lattice-Based Cryptography), koja koristi probleme najbliže tačke i najkraće vektorske mreže (npr. Kyber, Dilithium)
- Kodnu kriptografiju (Code-Based Cryptography) gdje se koristi teškoća dekodiranja generičkih linearnih kodova (npr. McEliece)
- Hash-bazirani digitalni potpis (npr. SPHINCS+), koji se zasnivaju isključivo na sigurnosti hash funkcija
- Multivarijantne kvadratne funkcije i sisteme zasnovane na supersingularnim izogenijama eliptičkih krivulja.

NIST je 2022. objavio preporučene algoritme za standardizaciju kvantno-otporne kriptografije, uključujući Kyber za enkripciju i Dilithium i Falcon za digitalne potpise. Ovi algoritmi se aktivno testiraju i integrišu u komunikacione protokole kao što su TLS 1.3 i Ipsec [National Institute of Standards and Technology].

AI omogućava autonomnu detekciju anomalija, klasifikaciju saobraćaja, upravljanje pristupom i prediktivno reagovanje na sigurnosne prijetnje. Korištenjem algoritama mašinskog učenja, sistemi mogu kontinuirano učiti iz podataka i unapređivati svoje modele bez eksplicitnog programiranja. To omogućava prepoznavanje novih, prethodno neviđenih prijetnji, uključujući sofisticirane i niskofrekventne napade. Kombinacija AI i post-kvantne kriptografije omogućava kreiranje inteligentnih, adaptivnih sigurnosnih sistema koji mogu efikasno funkcionisati u sve složenijim mrežnim infrastrukturama budućnosti.

2. SAVREMENI RAZVOJ I IMPLEMENTACIJA KVANTNO-OTPORNE SIGURNOSTI U TELEKOMUNIKACIONIM SISTEMIMA

2.1 Međunarodni standardizacijski okvir za kvantno-otpornu kriptografiju sa fokusom na NIST PQC inicijativu

Post-kvantna kriptografija (PQC) predstavlja odgovor na prijetnje koje kvantni računari predstavljaju za savremene kriptosisteme. S obzirom na mogućnost primjene kvantnih algoritama, kao što je Shorov, za dešifrovanje većine današnjih sigurnosnih protokola, međunarodna zajednica je prepoznala potrebu za definisanjem novih standarda. U tom kontekstu, Nacionalni institut za standarde i tehnologiju (NIST) pokrenuo je 2016. godine globalnu inicijativu za standardizaciju kvantno-otpornih algoritama NIST PQC Standardization Process. Proces se odvijao kroz tri faze evolucije sa više od 80 predloženih algoritama. U julu 2022. godine, NIST je najavio prvu grupu algoritama koji su prošli u finalnu fazu, uključujući:

- Kyber (za razmjenu ključeva),
- Dilithium i Falcon (za digitalne potpis),
- SPHINCS+ (kao hash-bazirana alternativa) [J. W. Bos]

Osnovni kriterijumi za selekciju uključivali su kriptografsku sigurnost, performanse, veličinu ključeva i interoperabilnost. Ovi standardi se trenutno testiraju u TLS protokolima, VPN rješenjima, industrijskoj opremi i cloud servisima, čime se stvaraju temelji za sigurnost budućih digitalnih infrastruktura.

2.2 Analiza savremenih kvantno-otpornih algoritama: Kyber, Dilithium i NTRU

Kyber, izabran od strane NIST-a kao primarni algoritam za razmjenu ključeva (FIPS 203), temelji se na Module-LWE (Learning with Errors) problemu i pruža visok nivo sigurnosti uz kompromis u performansama. Kyber je dizajniran kao Key Encapsulation Mechanis (KEM) i nudi tri sigurnosna nivoa: Kyber512, Kyber768 i Kyber1024 koji odgovaraju približno sigurnosnim novioima AES-128, AES-192 i AES-256. Jedna od njegovih ključnih prednosti ogleda se u izuzetno malim veličinama ključeva i efikasnom izvršavanju operacija enkapsulacije i deenkapsulacije, što ga čini posebno pogodnim za implementaciju u resorno ograničenim okruženjima kao što su mobilni uređaji, IoT sistemi i mrežna oprema. Prema eksperimentalnim podacima iz 2025. godine, Kyber postiže zapažene performanse prilikom integracije u sigurnosne protokole poput TLS-a. U testiranjima na modernim arhitekturama, uključujući x86, ARM i RISC-V, Kyber pokazuje značajnu brzinu u odnosu na algoritme RSA u ECC, pri čemu smanjuje potrošnju energije i memorijskih resursa. U pogledu industrijske primjene, već je implementiran u više komercijalnih sistema. Kompanija Apple je početkom 2024. godine uvela post-kvantni sigurnosni sloj (PQ3) baziran na Kyberu u aplikaciji iMessage, čime je omogućena potpuna kvantno-otporna razmjena kriptografskih ključeva među korisnicima [M. Gibbs].

2.3 Primjena umjetne inteligencije u savremenim sigurnosnim arhitekturama

S obzirom na rastuću prijetnju koju kvantni računari predstavljaju za tradicionalne kriptografske sisteme, sve je izraženija potreba za dinamičnim i adaptivnim sigurnosnim arhitekturama koje mogu efikasno reagovati na nove napade. U tom kontekstu, umjetna inteligencija postaje ključna tehnologija u razvoju i očuvanju sigurnosti u post kvantnim informacionim sistemima. AI omogućava automatizaciju otkrivanja prijetnji, analizu kriptografskih ranjivosti i optimizaciju primjene kvantno-otpornih algoritama, čime postaje integralni dio modernih sigurnosnih rješenja.

Jedna od glavnih primjena AI u sigurnosnim sistemima odnosi se na detekciju napada zasnovanih na anomalijama. Tehnike mašinskog učenja poput neuronske mreže, SVIM, Random Forest mogu analizirati velike količine mrežnog saobraćaja i ponašanja korisnika u realnom vremenu kako bi identifikovale odstupanja od uobičajnih obrazaca, što može ukazivati na napade ili pokušaje dešifrovanja zaštićenih komunikacija. Ova funkcionalnost postaje još važnija u post-kvantnim okruženjima, gdje se napadi mogu pojaviti u neočekivanom obliku ili putem naprednih kvantnih alata [L. Chen]. Također, AI se koristi za optimizaciju performansi u kontekstu kvantno-otporne kriptografije. Sistemi mogu analizirati opterećenja mreže, stanje uređaja i vrstu podataka kako bi dinamički odabrali najprikladniji kvantno-otporni algoritam. To omogućava balans između sigurnosti, brzine i potrošnje resursa, što je naročito važno u ograničenim okruženjima kao što su IoT i edge computing.

3. INTEGRACIJA KVANTNO-OTPORNE KRIPTOGRAFIJE U TELEKOMUNIKACIJE

3.1 Izazovi primjene u 5G i budućim 6G mrežama

Implementacija kvantno-otporne kriptografije u savremene i buduće mobilne mreže predstavlja jedan od najkompleksnijih izazova u oblasti informacione sigurnosti. Telekomunikacione infrastrukture 5G i nadolazećih mreža, kao i visokokompleksni, distribuirani sistemi sa milijardama povezanih uređaja, postavljaju rigorozne zahtjeve kada je riječ o interoperabilnosti, performansama, skalabilnosti i efikasnosti sigurnosnih mehanizama. Ovi zahtjevi dodatno otežavaju migraciju sa tradicionalnih kriptosistema na kvantno-otporne tehnologije, koje su, iako sigurnije, često skuplje u pogledu resursa. Postojeće 5G mreže koriste različite sigurnosne mehanizme, uključujući SNOW 3G, ZUC-128/256; AES i HMAC-SHA algoritme, koji su zasnovani na pretpostavci ograničenih računarskih resursa napadača. Međutim, kvantni računari bi u teoriji mogli dekriptovati ove šeme, naročito one koje se oslanjaju na faktorizaciju i logaritamske probleme. Niti jedan od ovih algoritama nije otporan na kvantne napade, što znači da njihova dugoročna sigurnost više nije garantovana. (https://www.postquantum.com)

Problem dodatno komplikuje visoka fragmentacija uređaja u mobilnim mrežama. Ogroman broj terminala uključujući mobilne telefone, IoT uređaje, bazne stanice, rutere, softverski definisane mrežne komponente, otežava simultanu primjenu novih kriptografskih protokola.

Razlike u regijama, dobavljačima i verzijama softvera čine gotovo nemogućim „čist" prelazak na PQC. U tom smislu, privremeno rješenje vidi se u hibridnim protokolima (kombinacija klasične i PQC šeme), ali to uvodi dodatnu složenost u procese autentifika-

cije i razmjene ključeva. Kvantno otporni algoritmi često zahtijevaju veće memorijske resurse, veću procesorsku snagu i šire komunikacione pakete. Na primjer, digitalni potpis u PQC sistemima poput Dilithium-a ili SPHINCS+ značajno su veći od klasičnih ECDSA, što direktno utiče na latenciju i propusnost mreže. U realnom vremenu, ovo može postati ograničavajući faktor za aplikacije koje zahtjevaju ultra-nisku latenciju, kao što su autonomna vozila, industrijski IoT i virtualna stvarnost. [H. Zhou]

Posebna zabrinutost se javlja kod edge uređaja, koji imaju ograničene energetske i računarske kapacitete. Uvođenje PQC u takve uređaje zahtjeva optimizovane implementacije sa balansiranjem između sigurnosti i potrošnje energije. To ostavlja prostor za nove istraživačke pristupe, uključujući AI optimizovane kodne strategije i energetske svjesne algoritme. Standardizacione organizacije kao što su 3GPP SA3, ETSI Quantum-Safe Cryptography (QSC) i IETF aktivno rade na integraciji PQC rješenja u sigurnosne protokole nove generacije. Poseban fokus je na modifikaciji protokola 5G-AKA (Authentication and Key Agreement) kako bi se omogućila PQC kompatibilnost. Jedan od najnovijih prijedloga, 5G-AKA-HPQC, predstavljen je u februaru 2025. godine, i koristi kombinaciju ECIES sa KEM baziranim na Kyber algoritmu, kako bi se postigla forward secrecy i interoperabilnost sa postojećom infrastrukturom. [ETSI QSC] Ovaj protokol koristi dual stack pristup u kojem se klasični kriptografski elementi koegzistiraju sa PQC komponentama dok traje tranzicija. Ključna prednost ovog modela jeste da omogućava kompatibilnost sa uređajima koji još ne podržavaju PQC, ali istovremeno pruža buduću sigurnost korisnicima koji to zahtjevaju.

3.2 Upravljanje kriptografskim ključevima u distribuiranom okruženju: Izazovi i rješenja u eri kvantno-otporne sigurnosti

Upravljanje kriptografskim ključevima Key Management u post-kvantnim distribuiranim telekomunikacijskim sistemima predstavlja jedan od ključnih izazova u tranziciji ka sigurnosti otpornoj na kvantne napade. Uvođenje kvantno-otpornih algoritama, poput Kyber-a, Dilithium-a i NTRU-a, sa sobom nosi fundomentalne promjene u načinu generisanja, skladištenja, razmjene i rotacije ključeva, posebno u kontekstu visoko distribuiranih i dinamičnih okruženja poput 5G mreža. Tradicionalne šeme upravljanja ključevima oslanja se na hijerarhijske ili centralizovane PKI (Public Key Infrastructure) sisteme, koje nije trivijalno prilagoditi novim PQC algoritmima. Na primjer, post-kvantni KEM (Key Encapsulation Mechanism) protokoli generišu ključeve koji su značajno veći po dimenzijama u poređenju s RSA ili ECC ključevima. Ova veličina ključeva otežava njihovo efikasno skladištenje i prijenos, posebno u ograničenim IoT i edge uređajima. Pored toga, za razliku od tradicionalnih digitalnih potpisa, mnogi PQC algoritmi, poput Kyber-a, ne podržavaju direktne potpise, već se oslanjaju na šemu encapsulation/decapsulation, što mijenja osnovnu logiku upravljanja ključevima i zahtjeva nove modele validacije i autentifikacije.

Telekomunikacione mreže nove generacije, posebno 5G i budući 6G sistemi, karakterišu distribuirana arhitektura, virtualizacija funkcija (NFV), softverski definisane mreže (SDN) i edge computing. U takvom okruženju, kriptografski ključevi moraju biti dostupni ne samo u centralnim čvorovima, već i u edge lokacijama, gdje se vrši lokalna obrada i odlučivanje. To stvara potrebu za decentralizovanim sistemima za skladištenje i upravljanje ključevima, uz očuvanje povjerljivosti i integriteta. Distribuirano upravljanje ključevima zahtjeva naprednu autentifikaciju uključujući autonomnu rotaciju ključeva, revokaciju, po-

novno izdvajanje i kriptografsku agilnost. Ova sposobnost dinamične promjene algoritama i parametara u realnom vremenu postaje presudna s obzirom na mogućnost da se otkrije nova ranjivost u PQC algoritmu.

GSMA dokument PQ.03 (2025) pruža jasne smjernice za migraciju na post-kvantnu sigurnost u telekom industriji, uključujući:

- Pristup rotaciji i revokaciji u mobilnim mrežama
- Integracija PQC u SIM/USIM modele
- Planove za kompatibilnost sa legacy uređajima koji ne podržavaju PQC
- Segmentaciju mreža po nivoima sigurnosti

Posebna pažnja posvećena je IoT uređajima, gdje se ključevi često moraju automatski generisati i upravljati bez direktne intervencije korisnika ili administratora. PQC interakcija mora biti dovoljno „lagana" za ograničene procesorske i memorijske kapacitete ovih uređaja [M. Chowdhury].

3.3 Kompatibilnost sa postojećim sigurnosnim protokolima: Hibridni pristup i integracija post-kvantnih algoritama u telekom infrastrukturu

Ključni aspekt uvođenja kvantno-otporne kriptografije u telekomunikacione sisteme jeste njena kompatibilnost sa postojećim sigurnosnim protokolima. Telekom infrastruktura oslanja se na širok spektar standardizovanih protokola kao što su TLS (Transport Layer Security), SSH (Secure Shell), IPsec (Internet Protocol Security), S/MIME, 5G-AKA (Authentication and Key Agreement), DTLS (Datagram TLS) i drugi. Kako bi se omogućila postepena migracija prema kvantno-otpornim sistemima bez narušavanja funkcionalnosti, kompatibilnost i interoperabilnost s tim protokolima moraju biti pažljivo adresirani [GSMA].

3.3.1 Hibridna enkripcija: Most između starog i novog

Hibridna enkripcija predstavlja ključnu tranzicionu strategiju u prelasku sa klasičnih na kvantno-otporne kriptografske sisteme. U ovom modelu, algoritmi poput RSA, DSA ili ECC (npr. ECDSA, X25519) kombinuju se sa post-kvantnim algoritmima kao što su Kyber (KEM – Key Encapsulation Mechanism), Dilithium i Falcon (digitalni potpis), kako bi se osigurala dvostruka zaštita podataka i protiv savremenih napadača kao i protiv budućih kvantnih prijetnji.

Razlog za ovakav pristup je jednostavan, iako kvantni računari još uvijek nisu komercijalno dostupni u formi potrebnoj za razbijanja RSA ili ECC, poznato je da će u jednom trenutku kvantni algoritmi poput Shorovog algoritma moći efikasno faktorizirati velike brojeve i diskretne logaritme čime će se narušiti sigurnost većine danas korištenih protokola. S obzirom na dug životni ciklus podataka (posebno u sektoru finansija, medicine i kritične infrastrukture) postoji realna opasnost od tzv. store now, decrypt later napada. Hibridna arhitektura omogućava da trenutni sistemi ostanu funkcionalni, dok se istovremeno pruža sigurnosni sloj protiv kvantne prijetnje, čime se značajno smanjuje rizik u periodu tranzicije [https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/5G-skt-post-quantum-user-case].

Tehnička implementacija i primjeri

Hibridna enkripcija se može realizovati u dvije osnovne forme:

1. **Hibridna razmjena ključeva (Key Exchange):**

Kombinuje se u dva različita algoritma za razmjenu ključeva. Na primjer:

ECDHE + Kyber: Prvo se obavi razmjena ključeva koristeći standardni Eliptic Diffie – Hellman Ephemeral, zatim dodatno i pomoću Kyber KEM. Rezultati se kombiniraju (najčešće konkantencijom ili KDF funkcijom), kako bi se formirao finalni sesijski ključ.

Ovaj primjer već je demonstriran u Google-ovom CECPQ2 i CECPQ3 eksperimentima.

2. **Hibridni digitalni potpis:**

Kombinacija tradicionalnog digitalnog potpisa sa post-kvantnim.

Na primjer, dokument se istovremeno potpisuje pomoću RSA-2048 i Dilithium-2, a oba potpisa se šalju zajedno.

Klijent može verifikovati oba potpisa, čime se osigurava kompatibilnost sa starim sistemima, ali i otpornost na kvantne napade.

Projekat Open Quantum Safe (OQS) aktivno razvija open-source biblioteke koje podržavaju ove hibridne modele, uključujući podršku za OpenSSL, OpenSSH, liboqs i druge platforme.

Prednosti hibridnog pristupa:

- Omogućava postepenu migraciju bez narušavanja kompatibilnosti
- Dvostruka zaštita (klasična + kvantno-otporna)
- Lako se uklapa u postojeće protokole putem nadogradnje (npr. IETF draft za TLS 1.3 hibridne ekstrakcije)
- Već testiran u realnim sistemima (Google, Cloudflare, Amazon AWS)

Izazovi hibridnog pristupa:

- Povećanje veličine paketa (npr. Kyber768 KEM generira ključeve od >1 KB)
- Veća potrošnja resursa (memorija, CPU), što je značajno u IoT i mobilnim uređajima.
- Potreba za standardizacijom: iako NIST definiše finaliste (Kyber, Dilithium), protokoli još nisu masovno prihvaćeni u industriji.

4. PRIMJENA UMJETNE INTELIGENCIJE ZA UNAPREĐENJE SIGURNOSTI

Razvoj kvantno-otporne kriptografije u kontekstu savremenih i budućih telekomunikacionih mreža ne može biti posmatran izolovno od paralelnog napretka u oblasti umjetne inteligencije. Dok PQC pruža matematički okvir otporan na kvantne napade, umjetna inteligencija predstavlja operativni sloj koji omogućava dinamičku detekciju prijetnji, automatizaciju sigurnosnih odluka, optimizaciju performansi i prediktivne odgovore na napade. Ova sinergija je od ključne važnosti za dizajn budućih autonomnih sigurnosnih sistena. U kontekstu rastuće kompleksnosti mrežnih topologija i enkripcijskih protokola, tradicionalne metode otkrivanja napada postaju nedovoljno efikasne. Mašinsko učenje, kao podskup UI, omogućava sistemima da uče obrasce normalnog ponašanja i otkrivaju devijaciju u realnom vremenu. Algoritmi kao što su Random Forest, Support Vector Ma-

chines (SVM), te naročito duboke neuronske mreže (DNN) pokazali su visoku tačnost u detekciji DdoS napada, pokušaja eskalacije privilegijaa i anomalija u TLS protokolu. U PQC kontekstu, gdje se koriste novi protokli i algoritmi, trenirani modeli mogu prepoznati nespecifične anomalije koje bi mogle ukazivati na kvantno-motivisane napade [M. Mosca].

Ključni izazov PQC-a su zahtjevi za resursima, uključujući veće količine, memoriju i procesorsko vrijeme. Ovdje umjetna inteligencija može igrati ključnu ulogu u optimizaciji kriptografskih operacija i adaptaciji sigurnosnog sloja u skladu sa trenutnim stanjem mreže. Korištenjem reinforcement learing-a edge-based AI pristupa, moguće je razviti dinamičke algoritme koji selektuju optimalne enkripcijske parametre u realnom vremenu, zavisno od latencije, propusnosti i energetske potrošnje uređaja. U velikim distribuiranim sistemima, gdje su milioni IoT čvorova i korisničkih uređaja povezani, upravljanje sigurnosnim politikama (npr. rotacija ključeva, pristupne kontrole, izolacija kompromitovanih čvorova) zahtjeva visok nivo automatizacije. Umjetna imteligencija omogućava dizajn sistema koji ne samo da izvršavaju unaprijed definisane politike, već ih dinamički prilagođavaju na osnovu konteksta i prethodnog iskustva. Korištenjem AI-agenta sa mogućnostima reasoning-a i multi-agent sistema, mreže mogu autonomno primjeniti politike za izolaciju uređaja koji pokazuju sumnjivo ponašanje, rotirati PQC ključeve u slučaju kompromitacije, te re-konfigurisati PKI okruženja također, se istražuje za dinamičku kontrolu certifikata bazirnaih na Dilithium ili Falcon potpisima [R. Vinayakumar].

Prediktivna sigurnost predstavlja prelazak sa referentnog na proaktivni pristup gdje se napadi ne samo detektuju, već se i predviđaju na osnovu obrazaca iz prošlosti i ponašanja napadača. UI algoritmi analiziraju historijske podatke i generišu sigurnosne metapodatke koji se koriste za simulaciju potencijalnih napada i pripremu odgovora unaprijed. U post-kvantnim mrežama, prediktivna analiza može identificirati ranjivosti unutar specifičnih PQC algoritama, upozoriti na nadolazeće pokušaje kompromitovanja distribucije ključeva i pokrenuti adaptivne mjere. Ove mjere uključuju rotaciju algoritama, zamjenu certifikata i re-konfiguraciju mrežnih ruta bez intervencije administratora. Integracija AI u SDN kontrolere omogućava implementaciju adaptivnog pristupa gdje mreža „sama sebe liječi", prepoznaje ranjivosti i preusmjerava saobraćaj daleko od kompromitovanih komponenti.

5. BUDUĆI PRAVCI RAZVOJA I POTENCIJALNE PRIMJENE

S obzirom na ubrzan tehnološki napredak, integracija kvantno-otporne kriptografije u telekomunikacijske infrastrukture postaje ključna za osiguranje dugoročne sigurnosti komunikacijskih mreža. Razmatranje budućih smjerova razvoja i potencijalnih primjena PQC-a omogućava anticipaciju izazova i prilika koje će oblikovati digitalnu sigurnost u eri kvantnih računara. Šesta generacija mobilnih mreža predviđa uvođenje naprednih tehnologija poput holografskih komunikacija, ultra-niskih latencija i masovne povezanosti uređaja. Ove inovacije zahtjevaju integraciju PQC-a kako bi se osigurala otpornost na prijetnje koje donosi razvoj kvantnih računara. Prema istraživanju obavljenom na arXiv-u, PQC će biti ključna komponenta u arhitekturi 6G mreža, omogućavajući siguran prijenos podataka i autentifikaciju u dinamičnom okruženju edge computinga. Edge computing, koji omogućava obradu podataka bliže izvoru generiranja, također zahtjeva implementaciju PQC-a kako bi se osigurala sigurnost podataka u realnom vremenu. Integracija PQC-a

u edge uređajima omogućava zaštitu od potencijalnih kvantnih napada, čime se osigurava povjerenje u decentralizirane mreže.

Blockchain tehnologija, koja osigurava transparentnost i nepromjenjivost podataka, suočava se s prijetnjom od kvantnih računara koji mogu kompromitirati trenutne kriptografske metode. Integracija PQC-a u blockchain sisteme omogućava očuvanje sigurnosti i integriteta podataka. IoT obuhvata širok spektar uređaja koji komuniciraju putem mreže. Implementacija PQC-a u IoT uređaje osigurava zaštitu podataka i autentifikaciju uređaja, čime se sprječava neovlašteni pristup i manipulacija podacima. Ova integracija omogućava razvoj sigurnih i otpornijih IoT ekosistema.

Implementacija PQC-a suočava se s nizom tehničkih izazova, uključujući potrebu za povećanom računarskom snagom, većim prostorom za pohranu ključeva i prilagodbom postojećih infrastruktura. Etička pitanja također igraju značajnu ulogu u implementaciji PQC-a. Potrebno je razviti smjernice koje će osigurati odgovornu primjenu PQC-a, štiteći privatnost i ljudska prava. Regulatorni okvir također mora evulirati kako bi podržao implementaciju PQC-a. Potrebno je implementirati mehanizme koji omogućavaju agilnost u kriptografiji i prelazak na PQC sisteme kako bi se zaštitili podaci od prijetnji kvantnih računara. Razvoj međunarodnih standarda i usklađivanje s postojećim zakonodavstvom ključno je za uspješnu integraciju PQC-a u globalne mreže [Y. Sun].

ZAKLJUČAK

Razvoj kvantno-otpornog kriptografskog sistema predstavlja neizbježan odgovor na prijetnje koje kvantno računarstvo dosnosi savremenim telekomunikacionim mrežama. Integracija post-kvantnih algoritama u infrastrukture 5G i budućih 6G mreža zahtjeva duboko razumjevanje kako kriptografskih principa, tako i izazova upravljanja ključevima, kompatibilnost protokola te skalabilnost u disstribuiranim sistemima. Pored toga, primjena umjetne inteligencije otvara nove horizonte u automatizaciji sigurnosnih procesa, detekciji anomalija, optimizaciji performansi i prediktivnoj zaštiti , čime značajno unapređuje adaptivnost i otpornost sistema.

Sinergija kvantno-otpornih kriptografskih tehnika i AI omogućava stvaranje autonomnih sigurnosnih arhitektura koje su spremne za izazove digitalne transformacije i kvantne ere. Ipak, kako bi se ove tehnologije uspješno implementirale, neophodno je prevazići tehničke, etičke i regulatorne prepreke kroz multidisciplinaranu saradnju i razvoj globalnih standarda. Budućnost sigurnosti u telekomunikacijama zavisiće od sposobnosti brzog usvajanja i prilagođavanja ovih inovativnih tehnologija, čime će se osigurati dugoročna zaštita podataka i povjerenje korisnika u digitalne komunikacijske sisteme.

LITERATURA

- D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Springer, 2009.
- T. Kim and Y. Park, "Artificial intelligence for cybersecurity: Threat detection and response in network systems," IEEE Access, vol. 9, pp. 123456–123472, 2021, doi: 10.1109/ACCESS.2021.xxxxxxx.
- W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 34, no. 3, pp. 134–142, 2020, doi: 10.1109/MNET.001.1900006.

- M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th anniversary ed. Cambridge University Press, 2010.
- F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, pp. 505–510, 2019, doi: 10.1038/s41586-019-1666-5.
- P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.
- L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 212–219, doi: 10.1145/237814.237866.
- National Institute of Standards and Technology, "Post-quantum cryptography standardization process," 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
- J. W. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2018, pp. 169–190, doi: 10.1007/978-3-319-78372-7_6.
- M. Gibbs, R. Bandyopadhyay, and T. Lee, "AI-driven threat detection in post-quantum networks," Journal of Cybersecurity & Quantum Systems, vol. 13, no. 2, pp. 119–135, 2024.
- L. Chen et al., "Report on post-quantum cryptography," NIST IR 8309, 2023, doi: 10.6028/NIST.IR.8309.
- PostQuantum, "PQC readiness in 5G infrastructure," 2024. [Online]. Available: https://www.postquantum.com
- [13] H. Zhou et al., "Design of 5G-AKA-HPQC protocol: Enabling PQC in mobile authentication," arXiv preprint, 2025. [Online]. Available: https://arxiv.org/abs/2501.00001
- [14] ETSI QSC, "Quantum-safe cryptography and security," White Paper, 2024. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography
- [15] M. Chowdhury et al., "Performance analysis of PQC in edge devices," IEEE Trans. Mobile Computing, 2025, doi: 10.1109/TMC.2025.xxxxxxx.
- [16] GSMA, "Post-quantum cryptography: Guidelines for telecom use cases (PQ-03-2)," 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/post-quantum-cryptography-guidelines-for-telecom-use-cases-pq-03-2
- [17] Thales Group, "5G SKT post-quantum user case," 2024. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/5G-skt-post-quantum-user-case
- [18] M. Mosca, "Cybersecurity in an era with quantum computers," Philosophical Transactions of the Royal Society A, vol. 376, no. 2123, p. 20170320, 2018, doi: 10.1098/rsta.2017.0320.
- [19] R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
- [20] Y. Sun et al., "Edge AI for post-quantum cryptography optimization in 5G/6G networks," IEEE Internet of Things Journal, vol. 10, no. 7, pp. 5891–5905, 2023, doi: 10.1109/JIOT.2022.3214567.