University of Rijeka
Faculty of Informatics and Digital Technologies
UNIRI

Key Management System in Quantum Key Distribution Networks

Sustavni pregled literature

Javno kvalifikacijsko izlaganje, 21.11.2025.

MSc Žaklina Šupica
zaklina.supica@uniri.hr
zaklina.supica@carnet.hr

University of Rijeka
Faculty of Informatics and Digital Technologies
UNIRI

Sažetak

- Uvod
- Quantum Key Distribution Network (QKDN)
- Key Management System (KMS)
- Sustavni pregled literature:
  - Metodologija
  - Dosadašnja istraživačka postignuća i izazovi
  - Budući pravci razvoja
- Prijedlozi za daljnje istraživanje

Uvod

- Kvantna prijetnja s razvojem kvantnih računala
- Posljednja dva desetljeća uloženi značajni napori u razvoj novih kvantno sigurnih kriptografskih mehanizama
- Rezultat je sigurna komunikacija u postkvantnom razdoblju:
  - Postkvantna kriptografija (Post Quantum Cryptography – PQC)
  - Kvantna distribucija ključeva (Quantum Key Distribution – QKD)

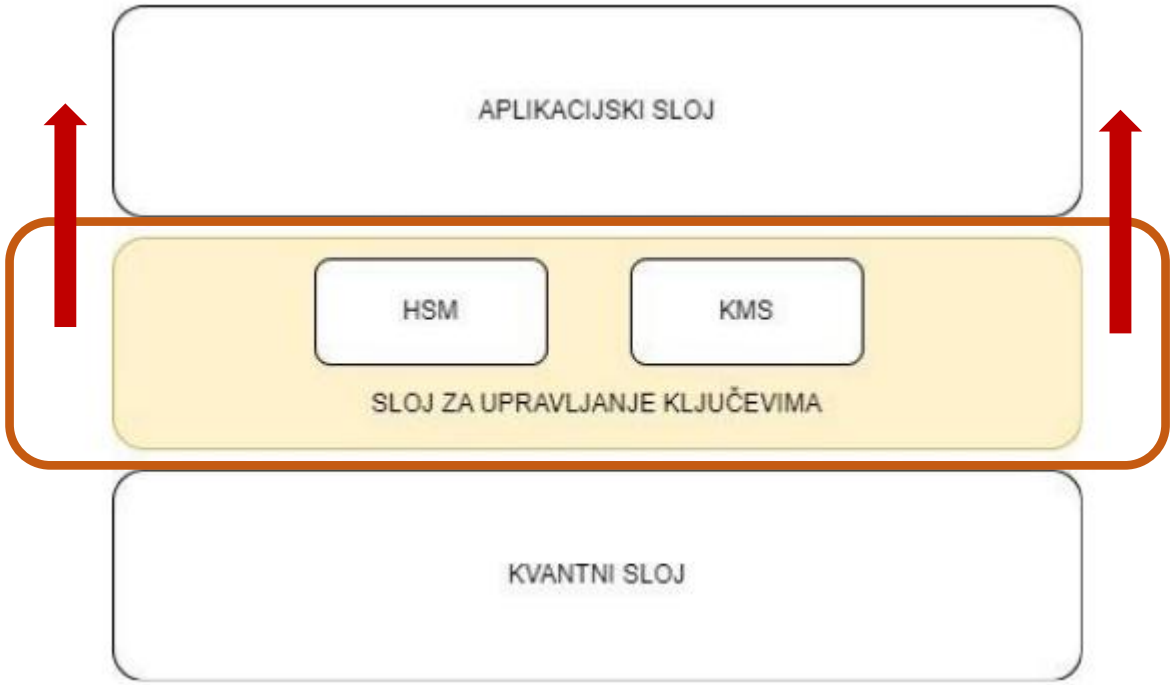
Kvantna distribucija ključeva - QKD

- Tehnologija koja omogućuje informacijsko-teorijski sigurnu razmjenu tajnog ključa između dviju udaljenih strana
- Nadopuna postojećih kriptografskih sustava generiranjem kvantno sigurnih ključeva za aplikacije i servise na višim slojevima
- Glavna svrha mreže: distribucija bezuvjetno sigurnih simetričnih ključeva između bilo kojih korisnika u mreži*
- Potreba mreže: sustav za upravljanje ključevima kao podrška glavnoj svrsi mreže

*R. Alleaume at al., „Using quantum key distribution for cryptographic purposes: a survey”, Dec 2014.
ITU-T, „Quantum key distribution networks – Key Management Recommendation”, Dec 2020.

KMS u QKD mreži (1/2)

- Uobičajen konceptualni prikaz QKD mreža je u troslojnom okviru*



Izvor: Ž. Šupica, D. Ivković: „Test Environment Concept Incuding a Key Management System in QKD Newtork", unpublished paper, 2024.

*C.-W. Tsai et al., „Quantum Key Distribution Networks: Challenges nad Future Research Issues in Security", 2021.

KMS u QKD mreži (2/2)

- Osnovne funkcionalnosti:
  - upravljanje životnim ciklusom kriptografskih ključeva i nadzor nad pristupom istima
  - osiguravanje da su ključevi sinkronizirani između dva QKD čvora koja su izravno povezana kvantnim linkom, autentifikacija
  - uspostavljanje sigurne komunikacije između dva čvora koja nisu izravno povezana kvantnim linkom

Upravljanje životnim ciklusom ključeva

- Upravljanje životnim ciklusom ključeva: nastanak, pohrana, uporaba, povlačenje, uništavanje
- Pohrana ključeva:
  - Kratkotrajna memorija
  - Lokalna baza podataka
  - Vanjska baza podataka (HSM)
- Dohvaćanje ključeva:
  - Na zahtjev (on demand)
  - Kontinuirani tijek ključeva (key sream)
- Dostavljanje ključa:
  - Između entiteta (KMS-aplikacija ili KMS-KMS)

Istraživačka pitanja

RQ1: Koja su dosadašnja istraživačka postignuća i izazovi distribucije kvantno generiranih ključeva prema sustavu za upravljanje ključevima (KMS-u) te aplikacijama?

RQ2: Koji su budući pravci razvoja sustava za upravljanje ključevima u QKD mreži?

Metodologija (1/3)

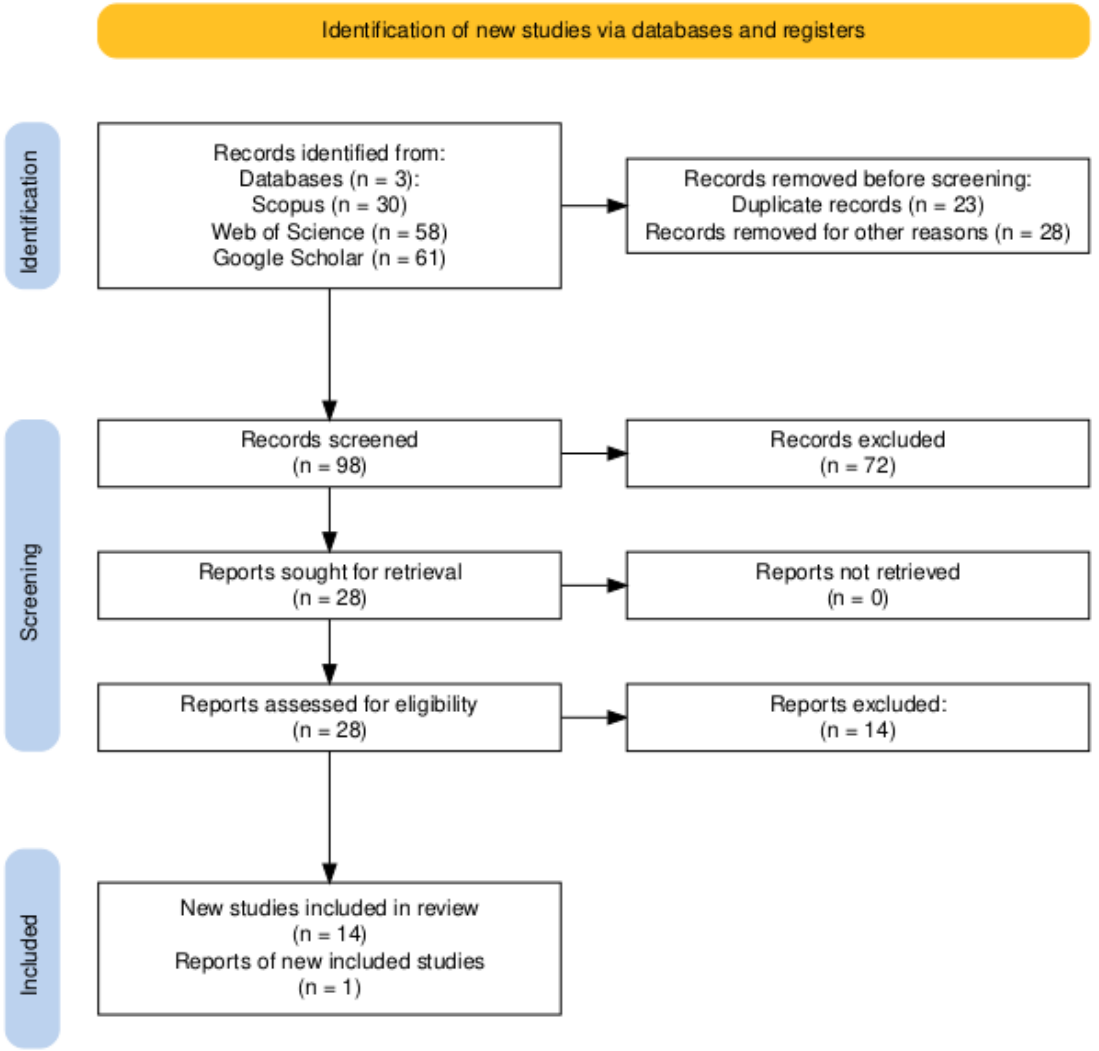
- Baze za pretraživanje: **Scopus, Web of Science** i **Google Scholar**
- Kriteriji uključivanja: radovi u časopisima i zbornicima, standardi, peer review, engleski jezik, vremenski okvir: 2010.–2025.
- Kriteriji isključivanja: patenti, blogovi, znanstveno polje fizika, znanstveno polje matematika
- Boolean string: „quantum key distribution network” **AND** „key management system”
- Pretraživanje po poljima: naslov, sažetak, ključne riječi

Metodologija (2/3)

- Scopus: 30
- WoS: 58
- Google Scholar: 61
- Total: **149** radova
- Mendeley Reference Manager:
  - uklonjena 23 duplikata -> rezultat **126** radova
  - dvostupanjski pregled po naslovu i sažetku -> rezultat **28** radova

Metodologija (3/3)

- Detaljna analiza pune verzije izabranih radova:
  - Kriterij uključivanja: Key management system OR application/entity
  - Kriterij isključivanja: isključivo QKD
- Nakon detaljne analize u sustavni pregled literature uključeno **14+1*** radova



Izvor: Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230
Download citation (.ris)

* uključen autorski neobjavljen rad

Dosadašnja istraživačka postignuća i izazovi– RQ1

Istraživačka postignuća	
✓ Fokus na dugoročnu sigurnost podataka i nadogradnju klasičnih kriptografskih sustava ✓ Opis osnovnih funkcionalnosti KMS-a → generiranje, spremanje, distribucija, autentifikacija, sinkronizacija ključeva ✓ Standardi komunikacijskih sučelja za interoperabilnost uređaja različitih dobavljača ✓ Standardi koji specificiraju ulogu KMS-a kako bi se osigurao životni ciklus ključeva	✓ Primjeri velikih implementacija (npr. KREONET, EQUO) ✓ Usmjerenost na velike mreže i veliki broj QKD čvorova - konceptualni pristup

Dosadašnja istraživačka postignuća i izazovi– RQ1

Izazovi	
🔍 Male QKD mreže nisu analizirane: mreže malih udaljenosti i malog broja čvorova (<10 km i <10 čvorova) 🔍 Nema standardizacije za multi-hop distribuciju ključeva između QKD čvorova koji nisu direktno povezani kvantnim linkom 🔍 Automatizacija i optimizacija rada mreže su minimalno istražene 🔍 Nedostatak i ograničena dostupnost kriptografskih ključeva (key scarcity) → nepoznato koliko ključeva treba pohraniti u danom trenutku	🔍 Nema standardiziranog dizajna sustava za upravljanje ključevima 🔍 Ne analiziraju se niti opisuju zahtjevi za performanse i optimizaciju KMS sustava 🔍 Ne postoji standard integracije KMS-a s aplikacijskim slojem 🔍 Ne postoji definicija ni standard za sučelja za KMS-to-KMS komunikaciju

Budući pravci razvoja KMS-a – RQ2

- Postaviti sloj sustava za upravljanje ključevima te aplikacijski sloj u fokus
- Analizirati prednosti i nedostatke fiksno definirane veličine kvantno generiranog ključa
- Definirati sigurnosna pravila u KMS-u koja se prilagođavaju zahtjevima aplikacije
- Istražiti male mreže i analizirati primjenu koncepata definiranih za velike mreže na male mreže i obrnuto
- Istražiti kako mrežna topologija utječe na generiranje i distribuciju ključeva, latenciju kao i kvalitetu usluge
- Identificirati ključne parametre koji utječu na brzinu, sigurnost i pouzdanost generiranja i distribucije ključeva u različitim aplikacijskim i mrežnim scenarijima
- Identificirati ključne faktore koji utječu na nedostatak i ograničenu dostupnost kriptografskih ključeva

Prijedlozi za daljnje istraživanje (1/2)

Uspostava eksperimentalne mreže:

- Uspostavljanje male QKD mreže prema troslojnoj arhitekturi
- Implementacija KMS-a i definiranje aplikacija unutar QKD mreže
- Testiranje tri scenarija dohvaćanja ključeva: na zahtjev, pozivanje iz lokalne baze KMS-a, pozivanje iz vanjske baze HSM-a
- Integracija KMS i HSM modula u jedinstven sustav za upravljanje ključevima
- Dohvaćanje materijala za generiranje kvantnih ključeva iz dvaju različitih izvora fotona

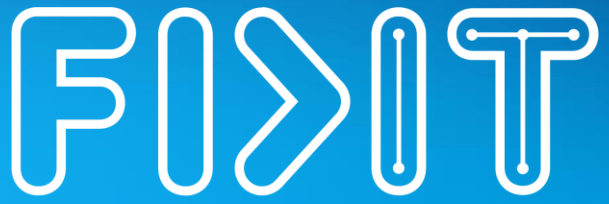
Analiza scenarija dohvaćanja i pohrane kvantnih ključeva:

- Analizirati kako različiti načini pristupa ključevima utječu na dostupnost, latenciju i performanse sustava:
  - Na zahtjev
  - Iz lokalne baze KMS-a
  - Iz vanjske baze (HSM)

Prijedlozi za daljnje istraživanje (2/2)

Sustavno ispitivanje mogućnosti primjene KMS-a u QKDN-u:

- Procijeniti praktičnu iskoristivost kroz stvarne komunikacijske scenarije
- Istražiti razlike u pouzdanosti i propustnosti kod distribucije ključeva između:
  - čvorova izravno povezanih kvantnim linkom
  - čvorova bez izravnog kvantnog linka (multi-hop distribucija)
- Eksperimentalno procijeniti izvedivost integracije aplikacija različite razine složenosti:
  - prijenos digitalnih dokumenata
  - video komunikacija
  - audio komunikacija
- Analizirati utjecaj ograničene dostupnosti ključeva na kvalitetu usluge (QoS)
- Modelirati strategiju pohrane i potrošnje ključeva



University of Rijeka
Faculty of Informatics and Digital Technologies

uniri

Hvala na pažnji!
Pitanja?