# PROGRESE ÎN COMUNICAȚIILE CUANTICE

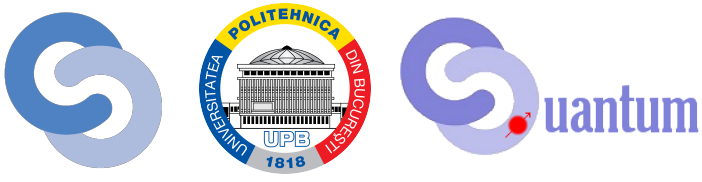
*Securitate, Utilitate, Performanță și Adoptare*

*Teză de Doctorat - Rezumat*

**Alin-Bogdan Popa**

*Coordonator*

Prof. Dr. Ing. **Răzvan Rughiniș**




Departamentul de Calculatoare
Facultatea de Automatică și Calculatoare
Universitatea Națională de Știință și Tehnologie **POLITEHNICA București**

*2024*

# Cuprins

# Contribuțiile mele

## Publicații de jurnal

1. **Alin-Bogdan Popa**, and Pantelimon George Popescu. "Optimal key forwarding strategy in QKD behaviours." Nature Sci. Rep. 14 (2024) - MULTIDISCIPLINARY SCIENCES Q1 (see [1]).
   https://doi.org/10.1038/s41598-024-64994-6

2. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu, Voichiţa Iancu, Florin Pop, and Pantelimon George Popescu. "SkySwapping: Entanglement resupply by separating quantum swapping and photon exchange." Future Generation Computer Systems 158 (2024): 89-97 - COMPUTER SCIENCE, THEORY & METHODS Q1 (see [4]).
   https://doi.org/10.1016/j.future.2024.04.031

3. **Alin-Bogdan Popa**, and Pantelimon George Popescu. "The Future of QKD Networks." Submitted for publication at IEEE Communications Magazine (2024) - ENGINEERING, ELECTRICAL & ELECTRONIC Q1 (see [2]). arXiv preprint (2024). https://doi.org/10.48550/arXiv.2407.00877

4. **Alin-Bogdan Popa** et al. "Optimal QKD Network Design". Submitted for publication at Nature Sci. Rep. (2024) - MULTIDISCIPLINARY SCIENCES Q1 (see [3]).

## Conferințe și workshopuri

5. **Alin-Bogdan Popa**, "Perspectives on Interconnecting National QKD Networks", HellasQCI 3rd Training Event on Quantum Key Distribution and Cyber Security in Heraklion, Crete (Greece). September 4-5, 2024.

6. **Alin-Bogdan Popa**, "Software Primitives for EuroQCI Use-cases" and "Preparing the CEF call. The Future of QKD Networks", IrelandQCI Workshop in Dublin, Ireland. July 1-3, 2024.

7. **Alin-Bogdan Popa**, "Unconditionally Secure File Transfer and Videoconference over a Postquantum VPN enhanced by QKD" and "QKD Simulator", RoNaQCI Workshp in Iași, Romania. June 20-21, 2024.

8. **Alin-Bogdan Popa**, "Quantum Key Distribution (QKD) - What it is, how it is done and why the unique opportunity is now", World Quantum Days at IFIN-HH in Măgurele, Romania. April 15-18, 2024

9. **Alin-Bogdan Popa**, "Quantum @ UPB - Quantum Comm. Networks Workshop", PTQCI Workshop in Aveiro, Portugal. February 26-27, 2024

10. **Alin-Bogdan Popa**, "HURRICANE: High Throughput Unconditional Secure Key Resupply for Real Time Crisis Management", RoNaQCI Workshop in Timișoara, Romania. October 12-13, 2023.

11. **Alin-Bogdan Popa**. "QGP-VPN: QKD enhanced VPN solution for general-purpose encrypted communications." In 2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2023 (see [8]).
https://doi.org/10.1109/RoEduNet60162.2023.10274931

12. **Alin-Bogdan Popa**, Iulia Maria Florea, and Răzvan Rughiniş. "Convolutional Neural Network Portfolio Management System with Heterogeneous Input." 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2020 (see [10]).
https://doi.org/10.1109/RoEduNet51892.2020.9324859

13. **Alin-Bogdan Popa**, Ioan Mihail Stan, and Răzvan Rughiniş. "Instant payment and latent transactions on the Ethereum Blockchain." 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet). IEEE, 2018 (see [5]).
https://doi.org/10.1109/ROEDUNET.2018.8514139.

## Implementări

14. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "QKDGKT - QKD Get Key Tool." Open-source software. Github, 2024 (see [6]).
https://github.com/QuantumUPB/QKD-Infra-GetKey [Online]

15. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "Q-BITS: Quantum-Based Information Transfer System - Unconditionally-Secure File Transfer." Open-source software. Github, 2024 (see [7]).
https://github.com/QuantumUPB/QKD-App-FileTransfer [Online]

16. **Alin-Bogdan Popa**, Bogdan-Călin Ciobanu and Pantelimon George Popescu, "Quantum VPN: Post Quantum VPN and Videocall enhanced by QKD" Open-source software. Github, 2024 (see [9]).
https://github.com/QuantumUPB/QKD-App-VPN [Online]

## Propuneri de proiect

17. Co-authored project proposal: "**HURRICANE**: High Throughput Unconditionally Secure Key Resupply for Real Time Crisis Management", UEFISCDI Proiecte de Cercetare Exploratorie, under review 2024.

18. Co-authored project proposal: "**RExQTCS**: Romanian Excellence in Quantum Technologies enhancing Cybersecurity", UEFISCDI Centre de Excelență (CoEx), under review 2024.

## Cursuri

19. Designed and created course materials for the **Quantum Communication and Cryptography** lecture within the MSc program on Quantum Computing at CS department, POLITEHNICA Bucharest. 2023-Present.

# Peisajul Comunicațiilor Cuantice

## Motivația pentru Comunicațiile Cuantice

În peisajul tehnologic modern, există mai multe tehnologii emergente care primesc o atenție puternică, deoarece potențialul lor disruptiv a fost recunoscut de cercetători, actori din industrie și guverne deopotrivă. De exemplu, în cadrul Casei Albe din Statele Unite, Consiliul Național pentru Știință și Tehnologie (NSTC) a stabilit în 2020 Subcomitetul de Acțiune Rapidă (FTAS) pentru a identifica tehnologiile critice și emergente care pot fi relevante pentru activitățile de securitate națională ale SUA, în scopul de a informa guvernul pentru a ajuta la stabilirea priorităților pentru politicile tehnologice naționale și finanțare. În "Lista Actualizată a Tehnologiilor Critice și Emergente" realizată de FTAS în 2024, a fost identificată o listă de 18 domenii tehnologice (împărțite în 122 de subdomenii) ca fiind de o importanță deosebită pentru securitatea națională a Statelor Unite. Lista include domenii precum semiconductori și știința materialelor, propulsie spațială, realitate augmentată și virtuală, blockchain (ca tehnologii de registru distribuit și active digitale, plăți și identitate), mai multe direcții în inteligența artificială (machine learning, deep learning, reinforcement learning, generative AI, large language models, AI safety), supercomputing avansat, energie regenerabilă și multe altele. Poate nu este surprinzător faptul că unul dintre principalele domenii identificate este "Quantum Information and Enabling Technologies", cu subdomenii ce includ quantum computing, tehnologii materiale pentru dispozitive cuantice, quantum sensing, quantum communications and networking, și sisteme de suport pentru tehnologiile cuantice.

Tehnologiile cuantice (QT) sunt considerate pe scară largă ca având potențialul de a avea un impact imens la nivel internațional. În raportul Quantum Technology Monitor din 2024, publicat de McKinsey & Company, se oferă o estimare pentru o dimensiune totală a pieței pentru anul 2040 de 45 până la 131 de miliarde de dolari pentru quantum computing, 24-36 miliarde de dolari pentru quantum communications și 1-6 miliarde de dolari pentru quantum sensing, cu o valoare economică adăugată potențială de până la 2 trilioane de dolari în doar 4 industrii până în 2035: chimicale, științele vieții, finanțe și mobilitate. În 2024, investițiile cumulate totale în start-up-uri QT la nivel global (estimate la aproximativ 360) au ajuns la 8,5 miliarde de dolari; finanțarea publică totală anunțată de guverne a ajuns la 42 de miliarde de dolari.

Modurile în care se așteaptă ca tehnologiile cuantice să impacteze ecosistemul sunt variate: putere de calcul crescută pentru probleme specifice care sunt greu de abordat de calculatoarele clasice; logistică sau operațiuni financiare îmbunătățite în termeni de eficiență, profit sau timp de calcul; modelarea mai bună a fenomenelor cuantice cu impact în sănătate, chimicale și înțelegerea științifică; capacitatea de a oferi vectori de atac severi

împotriva securității cibernetice clasice, dar și capacitatea de a oferi o soluție parțială sub forma schimbului securizat de chei prin distribuție cuantică de chei; și așa mai departe.

În 1980, Robert Metcalfe a postulat că valoarea financiară sau influența unei rețele este proporțională cu pătratul numărului de dispozitive conectate la rețea (ceea ce este o aproximație asimptotică pentru numărul total de conexiuni posibile, presupunând un graf complet conectat). Deși legea lui Metcalfe, așa cum este cunoscută astăzi, a fost inițial formulată pentru rețelele telefonice și de fax, ea a fost aplicată cu un anumit grad de succes la alte tehnologii de tip rețea, cum ar fi Internetul sau rețelele sociale. Aceeași creștere a valorii este așteptată și într-o rețea cuantică, așa cum va fi viitorul internet cuantic; astfel, nevoia pentru comunicații cuantice eficiente (QComms), care este subiectul acestei teze.

# Distribuția Cuantică de Chei

Având un rol important în Comunicațiile Cuantice și reprezentând o parte semnificativă a acestei teze, Distribuția Cuantică de Chei (Quantum Key Distribution - QKD) este o schemă de comunicație securizată bazată pe mecanica cuantică. În rețelele de comunicații, schimbul de chei (sau stabilirea cheilor) se referă la metodele criptografice prin care două părți (pe care le vom numi Alice și Bob) pot stabili o cheie secretă comună care poate fi utilizată pentru criptarea comunicației lor. De o importanță deosebită este schimbul de chei printr-un canal public, ceea ce înseamnă că comunicația dintre cele două părți poate fi interceptată de public (inclusiv de un potențial atacator, pe care îl vom numi Eve). Motivul pentru cerința unui canal public este scalabilitatea: un canal privat (de exemplu, o valiză fizică care conține chei și este transportată de la Alice la Bob de către gărzi înarmate) nu ar scala corespunzător pentru oricare două părți care doresc să comunice securizat prin Internet, astfel încât este necesar un schimb de chei securizat prin canale publice. O altă presupunere este că canalul public este și autentic (de obicei, prin utilizarea certificatelor de chei publice), adică Alice și Bob știu cu siguranță că vorbesc unul cu celălalt și nu cu un atacator de tip man-in-the-middle.

În practică, configurarea este următoarea: Alice și Bob împart un canal clasic public care poate transmite informații clasice (biți), care este de asemenea citit de un interceptator, Eve. Alice și Bob doresc să stabilească o cheie comună care să fie corectă (adică, cheia pe care o stabilesc la finalul protocolului să fie identică între Alice și Bob cu o probabilitate arbitrar de mare) și securizată (adică, cantitatea de informații pe care Eve o învață despre cheie citind canalul public să fie arbitrar aproape de 0).

Un protocol de schimb de chei care este utilizat în mod obișnuit în comunicațiile pe Internet este Diffie-Hellman (DH), a cărui securitate se bazează pe dificultatea (percepută) a rezolvării problemei logaritmului discret. Un protocol DH tipic implică următorii pași:

1. Alice și Bob sunt de acord public asupra a două numere prime mari $n$ și $g$;
2. Alice alege un alt număr prim mare aleatoriu $x$ în mod privat și calculează $A = g^x \mod n$, pe care îl trimite public lui Bob;
3. Bob alege un alt număr prim mare aleatoriu $y$ în mod privat și calculează $B = g^y \mod n$, pe care îl trimite public lui Alice;
4. Alice calculează în mod privat $K_A = B^x \mod n$, în timp ce Bob calculează în mod privat $K_B = A^y \mod n$;

5. Datorită proprietății comutative a exponențierii în aritmetica modulară (adică $(g^x)^y = (g^y)^x \mod n$), valorile $K_A$ și $K_B$ vor fi identice.

Securitatea acestui algoritm se bazează pe dificultatea lui Eve de a calcula $x$ cunoscând $A$, $g$ și $n$, lucru care pe un calculator clasic poate fi realizat în prezent doar în timp subexponențial ($O(exp((\log n)^{1/3}(\log\log n)^{2/3}))$) folosind algoritmul General Number Field Sieve (GNFS), făcându-l astfel nepractic pe un calculator clasic. O altă variantă, Elliptic-Curve Diffie-Hellman, care se bazează pe problema logaritmului discret pe curbe eliptice (ECDL) în loc de câmpuri întregi finite, este considerată în general mai greu de spart (cel mai cunoscut algoritm pentru rezolvarea ECDL, algoritmul lui Pollard rho, operează în $O(\sqrt{n})$ unde $n$ este ordinul grupului curbei și este aproximativ egal cu $2^k$ pentru o cheie de $k$ biți). Cu toate acestea, deși sunt implementate pe scară largă în comunicațiile securizate pe Internet în protocoale precum SSH, SSL, HTTPS, TLS, Signal Protocol, Elliptic Curve Digital Signature Algorithm (ECDSA), operațiuni blockchain (generarea de adrese, semnarea tranzacțiilor, semnăturile contractelor inteligente etc.), aceste protocoale bazate pe problema logaritmului discret suferă de mai multe probleme. În primul rând, securitatea lor nu este demonstrată; algoritmii prezentați mai sus (GNFS, Pollard's rho) sunt cei mai eficienți algoritmi de factorizare cunoscuți până în prezent, dar o descoperire teoretică în factorizarea numerelor întregi ar putea face ca aceste protocoale să fie ușor de spart. În al doilea rând, ele nu sunt necondiționat sigure (adică securitatea lor se bazează pe presupunerea unei puteri de calcul limitate a potențialilor atacatori); dacă un atacator ar avea o putere de calcul infinită, ar putea rezolva problema logaritmului discret (și astfel ar compromite securitatea schemelor) instantaneu. În cele din urmă, odată cu apariția tehnologiei cuantice, atunci când computere cuantice suficient de mari (în numărul de qubiți) și suficient de stabile (în numărul de erori) vor deveni disponibile, factorizarea numerelor întregi poate fi rezolvată eficient pe un calculator cuantic folosind algoritmul lui Shor. Astfel, apare necesitatea unor protocoale de schimb de chei mai bune, cum ar fi Quantum Key Distribution (QKD).

Primul (și poate cel mai cunoscut) protocol QKD este protocolul BB84, propus în 1984 de Charles H. Bennett și Gilles Brassard [11]. În BB84, Alice și Bob împart un canal cuantic în plus față de canalul clasic, prin care pot schimba informații cuantice. Într-o configurație simplă, Alice are o sursă de fotoni unică și un polarizator de fotoni, în timp ce Bob are un detector de polarizare a fotonilor. Protocolul funcționează astfel:

1. Alice generează două șiruri de biți aleatori $a_i, b_i$.

2. Pentru fiecare $i$, Alice generează un singur foton $p_i$ care, prin utilizarea polarizatorului de fotoni, codifică informația din $a_i$ și $b_i$ în direcția sa de polarizare. De exemplu, dacă $(a_i, b_i) = (0, 0)$, polarizarea fotonului este verticală; dacă $(a_i, b_i) = (1, 0)$, polarizarea este orizontală; dacă $(a_i, b_i) = (0, 1)$, polarizarea este diagonală pe direcția stânga-jos - dreapta-sus; dacă $(a_i, b_i) = (1, 1)$, polarizarea este diagonală pe direcția stânga-sus - dreapta-jos; se poate spune, de asemenea, că $b_i$ codifică una dintre cele două baze de polarizare reciproc necuplate ($b_i = 0$ pentru polarizare rectangulară; $b_i = 1$ pentru polarizare diagonală), în timp ce $a_i$ codifică unul dintre cele două stări ortogonale în cadrul bazei selectate.

3. Alice trimite fotonii codificați unul câte unul lui Bob prin canalul cuantic.

4. Bob generează o secvență aleatorie $b'_i$.

5. Bob măsoară fiecare foton $p_i$ în baza (rectangulară sau diagonală) definită de $b'_i$, obținând $a'_i$. Dacă baza $b'_i$ a lui Bob se potrivește cu baza în care este codificat fotonul, atunci $a'_i$ va coincide cu valoarea corectă $a'_i$; dacă însă baza $b'_i$ a lui Bob nu se potrivește cu baza fotonului (de exemplu, prin măsurarea unui foton polarizat orizontal în baza diagonală), atunci $a'_i$ va fi o valoare aleatorie 0 sau 1 cu o probabilitate de 50%.

6. După ce toți fotonii au fost trimiși de Alice și măsurați de Bob, atât Alice, cât și Bob dezvăluie bazele pe care le-au folosit $b_i$ și $b'_i$. Ei vor păstra doar măsurătorile asupra $p_i$ unde bazele selectate s-au potrivit ($b_i = b'_i$). Pentru aceste măsurători, $a_i$ și $a'_i$ sunt garantate să se potrivească și pot forma o cheie secretă comună.

7. Un pas de reconciliere a informațiilor este aplicat de Alice și Bob, unde aceștia aplică un cod de detecție a erorilor asupra cheilor obținute pentru a identifica (și, eventual, corecta) biții de cheie eronați, dacă există.

8. Un ultim pas de amplificare a confidențialității este aplicat, pentru a distila cheile finale în chei mai scurte, dar despre care un interceptator să nu poată avea nicio informație.

Securitatea protocolului BB84 se bazează pe teorema imposibilității clonării și pe proprietatea distructivă a măsurării. Chiar dacă canalul cuantic este public, dacă Eve măsoară un foton (distrugându-l astfel) într-o bază aleatorie $b''_i$ obținând $a''_i$ și trimite un foton nounouț lui Bob codificând aceste valori, șansa lui Eve de a nu fi detectată de Bob este de doar 75%. Presupunând că baza $b'_i$ a lui Bob se potrivește cu baza $b_i$ a lui Alice (altfel, fotonul este aruncat, deci în acest caz Eve nu este detectată, dar interceptarea nu îi aduce niciun avantaj), dacă Eve a ghicit corect baza inițială $b_i$ (ceea ce are o probabilitate de 50%), atunci fotonul este citit cu succes și nu apare nicio schimbare vizibilă pentru Alice sau Bob; însă, dacă Eve nu a ghicit baza $b_i$, atunci Bob va obține o măsurătoare incorectă cu o probabilitate de 50%, pe care el și Alice o vor descoperi la sfârșitul protocolului în timpul fazei de reconciliere a informațiilor. Deși se așteaptă un anumit grad de erori din cauza fluctuațiilor aleatorii pe canalul cuantic, un număr semnificativ mai mare de erori indică prezența unui interceptator, caz în care Alice și Bob pot pur și simplu să repete protocolul până când Eve nu mai ascultă. Eve poate încerca o altă abordare, clonând fotonul și stocându-i starea într-o "memorie cuantică" până când Alice și Bob efectuează pasul de dezvăluire a bazei, apoi măsurând fotonul stocat în baza corectă care a fost selectată de Alice și Bob; cu toate acestea, un clon perfect este imposibil, deoarece este interzis de teorema imposibilității clonării (acesta este și motivul pentru care BB84 necesită o sursă perfectă de fotoni unici: dacă pulsul de lumină de la Alice conține mai mult de un foton, Eve poate lăsa un foton să treacă la Bob și să captureze ceilalți, stocându-i până la faza de dezvăluire a bazei). Clonele imperfecte duc la încurcări și limitele de incertitudine arată că, indiferent ce face Eve, va fi detectată. Ultima șansă a lui Eve este de a încerca să intercepteze doar un număr mic de fotoni, obținând câțiva biți din cheia finală, dar cu o mare șansă de a face acest lucru nedetectată; acesta este motivul pentru pasul final de amplificare a confidențialității, unde biții de cheie pe care Eve i-ar putea fi învățat sunt făcuți inutilizabili. Alte protocoale sau variante ale QKD au fost de asemenea propuse: E91, propus în 1991 de Artur Ekert, care se bazează pe corelații bazate pe inseparabilitatea cuantică; B92, propus în 1992 de C. Bennett ca o variantă a BB84 care folosește 2

stări de polarizare în loc de patru; protocolul COW (Coherent One-Way), care se bazează pe impulsuri de lumină coerentă (deși se pare că există puțin consens în literatura de specialitate cu privire la faptul dacă COW este necondiționat sigur).

QKD (în special protocoalele precum BB84, E91, B92) este în prezent singura schemă cunoscută pentru schimbul de chei necondiționat sigur printr-un canal public, ceea ce este de o importanță maximă în comunicațiile de date sensibile (de exemplu, tranzacții bancare, comunicații militare, secrete guvernamentale și așa mai departe). Chiar dacă metodele de spargere a schemelor de schimb de chei clasice care sunt în vigoare în prezent nu sunt încă practice, se așteaptă ca acestea să devină disponibile sau practice în următorii 10 ani, ceea ce reprezintă un pericol imediat datorită strategiei Harvest-Now-Decrypt-Later (HNDL).

Cheile obținute prin QKD pot fi apoi utilizate pentru a stabili o sesiune de comunicație securizată, pentru a forma baza unei sesiuni VPN post-cuantic, sau chiar pentru a cripta direct un fișier sau o bucată de date într-o manieră necondiționat sigură, de exemplu prin utilizarea One-Time Pad (OTP) care criptează un mesaj aplicând o operație XOR între fiecare bit $m_i$ al mesajului și $k_i$ al cheii. Se poate demonstra că pentru orice schemă de criptare (inclusiv OTP), securitatea necondiționată implică necesitatea utilizării unei chei care este cel puțin la fel de lungă ca mesajul care urmează să fie criptat (demonstrația este simplă: dacă cheia este mai mică decât mesajul, atunci setul de cifruri posibile de lungime $L$ care pot fi obținute dintr-un text clar de lungime $L$ este neapărat mai mic decât setul de mesaje posibile de lungime $L$; invers, numărul de texte clare care pot genera un anumit cifru este neapărat mai mic decât numărul total de texte clare de acea dimensiune; astfel, prin cunoașterea unui cifru, se obține informație despre textele clare posibile care l-ar fi putut genera). Cerința unor chei mari pentru volume mari de date este în centrul necesității unor rate ridicate de schimb de chei și a unei transmiteri eficiente a cheilor, care sunt teme centrale în capitolul despre QKD din această teză.

# Rețele și infrastructură QKD

Deși rețelele de distribuție a inseparabilității cuantice au puține cazuri de utilizare practică astăzi, un număr de rețele QKD au fost implementate în scopuri de cercetare, guvernamentale și comerciale. Prima rețea QKD lansată a fost DARPA Quantum Network, care a funcționat între 2003 și 2007 și a constat din 10 noduri în Boston și Cambridge, Massachusetts. La scurt timp după, prima rețea europeană a fost implementată la Viena, Austria, ca parte a proiectului SEcure COmmunication based on Quantum Cryptography (SECOQC) între 2004-2008, constând din 6 noduri, și care a fost utilizată pentru a demonstra o comunicație telefonică criptată prin one-time pad și o videoconferință securizată pe baza AES, printre alte experimente. În 2009, rețeaua SwissQuantum a fost lansată, devenind prima rețea transfrontalieră. Aceasta s-a întins pe un total de trei noduri: două în centrul orașului Geneva, Elveția, și unul pe site-ul CERN din Franța. În Asia, Tokyo QKD Network a fost construită în Tokyo, Japonia, în 2010, constând din 6 noduri cu 6 legături, inclusiv o legătură pe distanță mai lungă de 45 km între Koganei și Otemachi. În 2018, UK Quantum Network (UKQN) a operat o rețea QKD cu mai multe noduri între Cambridge și Bristol, care în 2019 a fost extinsă la Adastral Park. În 2016, misiunea spațială chineză QUESS a lansat satelitul Micius, care permite QKD și care a fost ulterior utilizat pentru a stabili primul apel video cuantic securizat intercontinental între Viena, Austria și Beijing, China - o distanță la sol de 7.500 km. În plus, printre

implementatorii de rețele QKD, China conduce în prezent în termeni de scară: Rețeaua de Comunicații Cuantice din China, condusă de cercetătorul chinez Jian-Wei Pan (adesea numit "părintele cuanticului"), a cuprins în 2020 un total de 109 noduri, 57 de relee și 608 legături, împărțite între Beijing, Jinan, Shanghai, Heifei, Xinglong și Nanshan (acesta din urmă, în special, o locație îndepărtată la 2.600 km distanță de celelalte și conectată prin satelit).

La nivelul Uniunii Europene, în 2019 a început cea mai mare inițiativă internațională de până acum prin semnarea Declarației EuroQCI, care a fost ulterior semnată de toate cele 27 de state membre ale UE. Infrastructura Europeană de Comunicații Cuantice (EuroQCI) își propune să construiască o rețea QKD la nivelul UE (cu segmente terestre și spațiale) pentru a proteja datele sensibile și infrastructura critică (protejând instituțiile guvernamentale, centrele de date, rețelele energetice, spitalele și altele). Proiectul este finanțat de UE și este construit de statele membre (în cazul segmentului terestru) și de Agenția Spațială Europeană (ESA) în colaborare cu compania SES, cu sediul în Luxemburg, care furnizează comunicații prin satelit (în cazul segmentului spațial). EuroQCI constă în două faze distincte: prima fază de implementare a început în ianuarie 2023 și a fost finanțată de Programul Digital Europe al Comisiei Europene (cu un buget total de 90 milioane de euro), cofinanțat de cel puțin 50% cu guvernele naționale, pentru a permite statelor membre să proiecteze și să construiască o rețea națională de comunicații cuantice în fiecare țară ca un banc de teste pentru diferite tehnologii, protocoale și echipamente; se așteaptă să se finalizeze în jurul anului 2025. A doua fază a EuroQCI este interconectarea internațională între statele membre, fie prin legături terestre transfrontaliere, fie prin legături segmentate spațial prin intermediul prototipului de satelit Eagle-1, a cărui lansare este așteptată (în prezent) în 2024-2025 și este dezvoltat de SES. A doua fază este așteptată să fie lansată la sfârșitul anului 2024 și începutul anului 2025, și se așteaptă să fie finanțată prin programul Connecting Europe Facility (CEF) al Comisiei, gestionat de Agenția Executivă Europeană pentru Sănătate și Digital (HaDEA), cu un buget total de încă 90 milioane de euro.

În România, proiectul național Romanian National Quantum Communication Infrastructure - RoNaQCI (din care fac parte și eu), parte a EuroQCI, își propune să implementeze cea mai mare rețea QKD din EuroQCI, cu peste 1500 km de legături QKD. Consorțiul RoNaQCI implică 12 universități, 7 institute de cercetare, 3 agenții naționale, 3 companii private și 5 părți interesate relevante, și este condus de POLITEHNICA București, cu prof. M. Carabaș ca director de proiect și prof. P.G. Popescu ca coordonator tehnic. Rețeaua RoNaQCI valorifică conexiunile de fibră întunecată Dense Wavelength-Division Multiplexing (DWDM) existente ale RoEduNet (NREN-ul românesc) și implementează o rețea QKD care acoperă 20 de legături QKD metropolitane, împărțite în 6 rețele metropolitane din orașele București, Iași, Timișoara, Cluj-Napoca, Craiova și Constanța, conectate la coloana vertebrală națională de 16 legături QKD pentru un total de 36 de legături. RoNaQCI are cazuri de utilizare planificate pentru rețea în cercetare, educație, medical, comunicații speciale, activități de centre de date și administrație publică. În plus față de rețeaua națională, POLITEHNICA București a implementat în incinta sa din București o rețea QKD separată cu 3 noduri (două legături) între trei clădiri din campusul universității, care a fost utilizată în iunie 2023 ca banc de testare pentru prima realizare experimentală românească a unei videoconferințe printr-un VPN post-cuantic securizat prin QKD de A.B. Popa și prof. P.G. Popescu și primul transfer de fișiere necondiționat sigur din România prin QKD de B-C. Ciobanu și prof. P.G. Popescu.

# Capitolul 1

# Perspective asupra Quantum Key Distribution

## 1.1 Strategia Optimă de Rutare în Comportamentele QKD - vezi [1]

Modelăm problema distribuirii ratei de cheie într-o rețea QKD complexă ca o problemă de optimizare pentru care oferim o soluție optimă. Abordarea noastră implică următorii pași: definirea problemei de optimizare și a obiectivului acesteia; propunerea unei liste de scenarii de optimizare cu aplicabilitate la rețele QKD din lumea reală; formalizarea problemei și a procesului de transmitere a cheilor; modelarea formalizării ca o problemă de programare liniară (LP) pentru a asigura optimalitatea; analizarea rezultatelor și discutarea perspectivelor colectate pe scenariu de optimizare, topologie de rețea și parametrii QKD. În restul acestei secțiuni vom detalia fiecare dintre punctele de mai sus.

Definim următoarele scenarii principale cu aplicabilitate practică.

Scenariul All-to-All (Echilibrat) ($S_{A2A}$): acest scenariu este aplicabil unei rețele QKD federate în care toți utilizatorii finali sunt egali și nu există un set preferențial de noduri. Fiecare utilizator final dorește să aibă o rată de cheie cât mai mare cu toate celelalte noduri, fără a afecta semnificativ rata generală de generare a cheii în rețea. Este oferit un exemplu de rețea echilibrată, unde comportamentul dorit este maximizarea ratei minime de cheie între orice pereche de două noduri, fie ele conectate direct printr-o legătură fizică sau nu (legăturile logice sunt afișate cu roșu).

Scenariul One-to-All (Broadcast) ($S_{O2A}$): acesta este scenariul în care un nod particular este preferențial și se dorește maximizarea ratei de cheie între nodul preferențial și toate celelalte noduri. De exemplu, în cadrul unei infrastructuri naționale de comunicații cuantice, guvernul ar putea dori ocazional să maximizeze rata de cheie între agenția sa centrală și toate celelalte noduri, chiar dacă acest lucru ar duce la o rată de cheie mai mică între nodurile nepreferențiale. Este oferit un exemplu de rețea broadcast, unde comportamentul dorit este ca nodul B să maximizeze rata sa minimă de cheie cu fiecare alt nod.

Scenariul One-to-One (High-throughput) ($S_{O2O}$): un scenariu în care, într-o rețea complexă, o anumită legătură (fie fizică, fie logică) trebuie să fie prioritară cu orice preț. De exemplu, într-o situație critică (război, dezastru natural etc.) este necesară o comunicație

în timp real și cu un debit ridicat între primii respondenți și zonele afectate, chiar dacă acest lucru ar afecta comunicația dintre orice alte perechi de noduri din rețea. Este oferit un exemplu de conexiune high-throughput, unde nodurile B și F trebuie să atingă cea mai mare rată de cheie posibilă, în detrimentul comunicației dintre orice altă pereche de noduri. După formalizare, distribuția cheilor la nivelul KMS este echivalentă cu problema fluxului multicomoditar fracționat, unde multiple mărfuri (chei între oricare dintre perechile țintă $\tau = (t_1, t_2)$) trebuie să circule într-un graf (mai precis, subgraful rețelei compus doar din legături fizice *negre*) între o sursă (nodul $t_1$) și un recipient (nodul $t_2$) unde fiecare legătură are o capacitate maximă de flux (rata de cheie $w(e)$). Problema fluxului multicomoditar este cunoscută ca fiind NP-completă pentru cazul discret (adică, unde fluxurile de mărfuri într-o anumită legătură sunt întregi), dar cu fluxuri fracționate problema poate fi rezolvată optim în timp polinomial cu programare liniară [12]. Pot fi utilizate scheme de aproximare chiar mai rapide [13, 14]. Abordarea fracționată poate fi utilizată în acest caz deoarece considerăm că rata de cheie este măsurată în biți de cheie pe secundă; semnificația redistribuirii fracționate este că un număr de biți de cheie trebuie să fie rezervați pe o fereastră de timp mai lungă de o secundă.

În această lucrare, introducem conceptele relevante pentru transmiterea securizată a cheilor generate de QKD utilizând OTP și motivăm necesitatea acestei abordări având în vedere cerințele de securitate și rata scăzută de cheie a dispozitivelor QKD disponibile comercial. Introducem formalismul matematic al grafurilor pe care îl folosim pentru a modela rețelele QKD și pentru a extinde graful rețelei la graful complet folosind legături logice între toate nodurile care nu sunt conectate fizic prin infrastructura QKD. Oferim o formulare a problemei de flux multicomoditar și trei scenarii cu aplicabilitate practică în cazuri de utilizare tipice QKD. Oferim o descriere în sintaxa LP pe care o rulăm și analizăm pe 16.250 de rețele simulate în total, cu până la 40 de noduri și 15 legături redundante, oferind o investigație detaliată asupra rezultatelor și performanței algoritmului, precum și asupra impactului dimensiunii și topologiei grafului.

Ca lucrări viitoare, menționăm că prin această abordare putem aborda orice tip de problemă de transmitere a cheilor în rețelele QKD folosind același formalism, inclusiv adăugarea optimă de legături fizice QKD și generarea unui program de transmitere orientat spre obiective, bazat pe timp.

## 1.2 Viitorul Rețelelor QKD - vezi [2]

Necesaritatea legăturilor logice (spre deosebire de cele fizice) apare din existența unor potențiale cazuri de utilizare între noduri care nu sunt conectate direct. De exemplu, în cazul unei rețele cu trei noduri (A, B, C) cu legături fizice între A-B și B-C, dacă există un mecanism de transmitere a cheilor astfel încât A și C să poată obține, de asemenea, chei necondiționat sigure, considerăm legătura A-C ca fiind o legătură logică.

Unitatea fundamentală a QVNets este legătura virtuală QKD (QVLink). La nivel fizic, o legătură QKD tipică constă dintr-un canal fizic care conectează două puncte finale QKD capabile să ruleze un protocol QKD pentru a genera secrete partajate. Secretele partajate pot fi utilizate pe loc sau pot fi agregate într-un depozit de chei pentru utilizare ulterioară. În practică, însă, hardware-ul QKD se bazează pe comunicații bazate pe fotoni, care, din cauza absorbției și zgomotului din canal, au o rază limitată (pentru legăturile terestre, de obicei în jur de 60-120 km [15]); astfel, conectarea nodurilor pe distanțe mari

poate necesita mai mulți repetitori de încredere (sub formă de noduri intermediare) care transmit cheile, de obicei prin One Time Pad (OTP) aplicând o operație XOR.

QVLink este extensia naturală a legăturii logice, considerând fiecare legătură ca o conexiune trunchi care poate susține multiple legături logice independente. Motivația pentru această separare rezidă în problema ratelor de cheie limitate ale dispozitivelor QKD disponibile comercial (care este de obicei în jur de 1-4 kb/s; deși foarte puține rețele au realizat rate de câteva sute de kb/s [15], rata limitează încă sever aplicațiile potențiale - și finanțarea cuantică ar scădea probabil semnificativ dacă investitorii ar vedea imagini securizate cuantic încărcându-se mai lent decât o conexiune dial-up din anii '90). Astfel, dacă mai multe aplicații, cazuri de utilizare sau personal solicitant coexistă între aceleași două puncte finale, atunci ele trebuie neapărat să concureze pentru resursa limitată care este rata de cheie disponibilă. Prin separarea lățimii de bandă a cheii în fluxuri de chei independente, fiecare flux poate fi atribuit diferiților utilizatori sau cazuri de utilizare, după cum necesită administratorii rețelei. În plus, pot fi stabilite reguli programatice pentru a ajusta dinamica cota fiecărui flux, în funcție de condițiile externe sau de cererea de chei.

Cu QVNets, extindem QVLink QKD la nivel de rețea. Un QVNet este graful rețelei compus din toate QVLink-urile cu același ID. Formal, QVNet este un subgraf al grafului rețelei originale, unde greutatea muchiei (adică rata de cheie) este cel mult egală cu greutatea muchiei din graful original.

În această lucrare propunem un protocol de nivel inferior între straturile fizic / Vendor KMS și Network KMS, extinzând conceptele de legături logice și VLAN-uri din rețelele clasice la lumea QKD, sub forma QVLinks și QVNets. Arătăm cum acestea pot atenua mai multe probleme legate de conflictele de cazuri de utilizare și rutarea blackbox transfrontalieră, precum și cum pot crește utilizabilitatea, flexibilitatea și eficiența costurilor rețelei.

Pentru EuroQCI și, în special, pentru conexiunile transfrontaliere care urmează să fie implementate, problema abstractizării infrastructurii pentru control granular (pentru care QVNets reprezintă o soluție) este doar una dintre provocările arzătoare care atrag atenția la nivel mondial. Multe alte probleme vor trebui rezolvate, cum ar fi adresarea nodurilor, descoperirea rețelei, configurarea automată și altele. Sperăm că acesta este un pas necesar către o rețea globală QKD și viitorul internet cuantic, deschizând calea pentru ca aceste tehnologii să fie la fel de omniprezente și integrate precum internetul de astăzi.

## 1.3 Design Optim de rețea QKD - vezi [3]

În această lucrare, abordăm considerentele practice pentru proiectarea optimă a unei rețele QKD. Într-o rețea reală, pot exista mai multe constrângeri în joc: poate exista dorința de a conecta mai multe locații pentru a permite un comportament echilibrat, dar poate exista un buget limitat; pot fi disponibile mai multe dispozitive cu parametri și costuri diferite, și mai multe rute între aceleași locații; în unele cazuri, în funcție de cazurile de utilizare ale rețelei QKD planificate, pot exista cerințe privind multiple comportamente (de exemplu, considerați o rețea care funcționează într-un comportament broadcast de la locația A către toate celelalte locații în zilele lucrătoare și într-un comportament high-throughput între locațiile X și Y în timpul weekendului), iar dorința poate fi să se satisfacă toate constrângerile cazurilor de utilizare, minimizând în același timp

costurile; în alte cazuri, dorința poate fi de a extinde o rețea existentă cu legături suplimentare pentru a conecta o locație nouă sau pentru a crește debitul de cheie pentru un scenariu specific. În contextul viitorului apel CEF și al conexiunilor transfrontaliere care urmează să fie adăugate la EuroQCI, acest aspect este deosebit de important având în vedere bugetul său foarte limitat (doar 90 milioane de dolari din fonduri europene). Aici oferim un formalism matematic pentru nevoile practice de proiectare a unei rețele QKD, prezentăm o abordare Mixed-Integer Linear Programming (MILP) pentru rezolvarea optimă a constrângerilor și oferim o analiză extensivă pentru mai multe scenarii didactice, precum și pentru rețelele practice de fibră optică și QKD din România. Deoarece Infrastructura Națională de Comunicații Cuantice din România (RoNaQCI) este cea mai mare rețea QKD construită ca parte a EuroQCI (cu 6 rețele metropolitane și 20 de legături metropolitane conectate prin coloana vertebrală națională de 16 legături și cu o acoperire de peste 1500 km), credem că abordarea poate fi scalată cu ușurință la alte rețele naționale QKD, precum și la unele chiar mai mari, cum ar fi întreaga EuroQCI conectată.

Deși calcularea rezervării de cheie pentru orice comportament definit mai sus pentru o rețea dată a fost demonstrată în cercetările anterioare ca fiind rezolvabilă optim prin LP pe o formulare MCFP, acum ne preocupă constrângerile practice și cerințele specifice întâlnite la proiectarea unei topologii de rețea QKD.

În primul rând, la proiectarea unei rețele, nu este adesea cazul că o rețea este proiectată pentru un singur comportament. În schimb, părțile interesate ale proiectului QKD doresc să permită mai multe cazuri de utilizare, care pot arăta astfel: 1) Sediul central militar $v_M$ și Forțele Navale $v_N$ trebuie să schimbe continuu 1 b/s de chei pentru a asigura criptarea necondiționat sigură a unor aplicații militare specifice pe parcursul zilei; 2) În fiecare miercuri, Președintele efectuează un broadcast din capitala $v_A$ către toate celelalte orașe $v_X$, care necesită cel puțin 2 kb/s de chei datorită naturii audio a broadcastului; cu toate acestea, broadcastul nu ar trebui să interfereze cu cazul de utilizare 1, care ar trebui să continue neîntrerupt simultan; 3) Capitala ar trebui să fie conectată cel puțin la orașele $v_B, v_C, v_D$; 4) În caz de situații de criză, toate celelalte cazuri de utilizare pot fi suspendate, dar o conexiune high-throughput între cel mai vestic și cel mai estic oraș trebuie să fie disponibilă cu o rată de cheie de cel puțin 5 kb/s pentru gestionarea crizei. Proiectarea rețelei trebuie să ia în considerare toate aceste scenarii diferite după cum este necesar. Rețineți că un scenariu poate consta doar dintr-un comportament așa cum este definit mai sus (echilibrat, broadcast, high-throughput, personalizat), dar poate include și constrângeri specifice (de exemplu, "cazul de utilizare 1 ar trebui să continue neîntrerupt") în plus față de un comportament.

În al doilea rând, deși în proiectarea rețelelor vedem locațiile ca noduri într-un graf, ele sunt departe de a fi astfel: locațiile au poziții geografice și conexiunile QKD pot fi posibile doar între anumite perechi de locații. Mai mult, se poate dori construirea rețelei de la zero sau extinderea unei rețele existente cu legături noi, poate din cauza unei finanțări suplimentare neașteptate care nu era disponibilă atunci când rețeaua a fost proiectată inițial. Astfel, în graful complet al tuturor locațiilor care fac (sau pot face) parte din rețeaua QKD, vedem fiecare muchie ca fiind clasificată într-una dintre următoarele categorii:

- Muchie roșie: o legătură QKD existentă, care are o rată de cheie specifică (măsurată) și care nu implică niciun cost;
- Muchie albastră: o conexiune de fibră optică de calitate unde poate fi instalat un

dispozitiv QKD (și care va implica costul receptorului-transmițător QKD ca un cost);

- Muchie neagră: leagă două locații unde conexiunea de fibră optică de calitate nu este disponibilă, dar instalarea sa este fezabilă; costul implicat va consta în legăturile QKD instalate de-a lungul acestei muchii și costul instalării și întreținerii (sau închirierii) liniei de fibră optică;

- Muchie albă: leagă două locații unde conexiunea nu este disponibilă și nu este fezabilă instalarea.

În al treilea rând, în practică, administratorul rețelei poate avea de ales între diferite modele de dispozitive QKD, iar rețeaua optimă nu este neapărat omogenă în ceea ce privește modelele de dispozitive utilizate (de exemplu, pentru conexiunea transfrontalieră EuroQCI, rețeaua paneuropeană EuroQCI este din necesitate eterogenă, deoarece QCI-urile naționale au achiziționat dispozitive QKD de la mai mulți furnizori). Parametrii relevanți ai unui dispozitiv pot fi rata de cheie estimată, raza de acțiune, atenuarea distanței (care duce la rate de cheie mai mici atunci când se instalează pe distanțe mai lungi) și, evident, costul. În plus, într-o rețea dense wavelength-division multiplexing (DWDM), pot fi instalate mai multe dispozitive QKD de-a lungul aceluiași cablu de fibră optică pentru a crește rata de cheie pentru acel segment.

În cele din urmă, metrica care trebuie maximizată pentru proiectarea optimă a rețelei poate varia în funcție de cerințele specifice și obiectivul rețelei. În unele cazuri, obiectivul poate fi să se implementeze o rețea QKD care să îndeplinească o listă de constrângeri (în termeni de cazuri de utilizare, comportamente etc.) în timp ce se minimizează costul; în alte cazuri, poate exista un buget fix care trebuie cheltuit, cu scopul de a maximiza rata de cheie într-un anumit caz de utilizare, poate în timp ce se satisface și un nou set de constrângeri.

În această lucrare oferim o formalizare a constrângerilor practice, formulăm constrângerile ca ecuații și inegalități liniare și propunem un algoritm MILP pentru a produce proiectul optim al rețelei QKD.

## 1.4 Distribuire de Entanglare Cuantică - vezi [4]

Spre deosebire de BB84, care a fost prezentat anterior, unele protocoale QKD se bazează pe proprietățile particulelor încurcate. De exemplu, E91, propus de Artur Ekert în 1991, utilizează perechi de fotoni încurcați partajați între Alice și Bob; perechile pot fi create de orice sursă, inclusiv chiar de interceptatorul Eve, deschizând astfel calea către QKD independent de dispozitiv, în care utilizatorii nu trebuie neapărat să aibă încredere în producătorii dispozitivelor. Cele două particule dintr-o pereche, una deținută de Alice și una deținută de Bob, sunt perfect corelate (ceea ce înseamnă că dacă atât Alice, cât și Bob decid asupra unei direcții de polarizare pentru măsurare, vor obține același răspuns, deși aleatoriu, cu o probabilitate de 100%). Într-un mod similar cu BB84, Alice și Bob decid aleatoriu asupra unei baze private pentru măsurare dintr-un set de baze posibile; la sfârșitul protocolului, dezvăluie public baza aleasă pentru fiecare pereche. Pentru a detecta interceptarea, nu contează numărul de erori din transmisie unde bazele s-au potrivit, așa cum se face în BB84; în schimb, calculează statistică de test $S$ pe baza coeficienților

de corelație, similar cu testul Bell. Se poate demonstra că, clasic (când nu este implicată nicio încurcare cuantică), atunci $|S| \leq 2$ (cunoscută ca inegalitatea CHSH); în schimb, pentru stările încurcate maximal, inegalitatea este încălcată și limita superioară devine $2\sqrt{2}$ (cunoscută ca limita lui Tsirelson). Având în vedere că încurcarea este monogamă (adică două stări încurcate maximal nu pot fi deloc încurcate cu o a treia stare), orice încercare a lui Eve de a încurca una dintre particulele din pereche cu o particulă de-a sa pentru a obține informații despre cheie va face ca cele două particule deținute de Alice și Bob să nu mai fie încurcate maximal, iar statistica de test se va îndepărta de limita lui Tsirelson. Perechile încurcate sunt consumate ca parte a E91 pentru a obține o cheie QKD; aceasta oferă un stimulent puternic pentru rețelele de distribuție a încurcării cuantice, în contextul QKD practic cu protocoale bazate pe încurcare.

În această lucrare, se propune o nouă metodă de distribuire a încurcării cuantice printr-o rețea hibridă sol-satelit, care valorifică quantum swapping pentru a genera perechi încurcate pe sateliți și a distribui preventiv jumătate din pereche către stațiile de sol, apoi realizând swapping-ul la nivel de satelit doar atunci când este creată o cerere de încurcare din partea solului. O comparăm cu alte abordări fără distribuție preventivă și arătăm că există o pierdere de fidelitate mai mică [16, 17] pe distanța parcursă.

Motivația din spatele distribuirii fiabile a încurcării cuantice este multi-fațetată. Încurcarea cu o precizie ridicată îmbunătățește succesul mai multor protocoale sau scheme pentru care poate fi utilizată încurcarea: teleportare, QKD [18, 19, 20, 21], algoritmi cuantici distribuiți [22, 23, 24] și altele. Considerăm că fidelitatea încurcării este pierdută în trei etape diferite: la crearea perechii încurcate [25, 26], în timpul transmisiei acesteia și la pasul de măsurare [27, 28, 29]. În această lucrare abordăm a doua etapă, prin reducerea pierderii de fidelitate în timpul transmisiei particulelor. Rezultatul principal al SkySwapping este demonstrarea faptului că distribuirea preventivă a particulelor încurcate reduce semnificativ distanța pe care particulele trebuie să o parcurgă prin aer, minimizând astfel pierderea de fidelitate în atmosferă (deoarece în afara atmosferei Pământului, inclusiv în orbitele LEO, pierderea de fidelitate este neglijabilă). Distribuția preventivă implică următorii pași:

1. Pe măsură ce sateliții LEO trec peste OGS-uri (într-un unghi de 1 deg [30] față de zenitul local al OGS-ului), satelitul generează perechi încurcate [31, 32], păstrează o particulă din fiecare pereche și trimite cealaltă particulă către OGS. Pe măsură ce acest lucru se întâmplă continuu în timp, fiecare OGS acumulează un număr de particule pereche cu unul sau mai mulți sateliți.

2. Când două OGS-uri, Alice și Bob, au nevoie de încurcare, acestea generează o cerere de încurcare. Atât Alice, cât și Bob partajează perechi încurcate cu unul sau mai mulți sateliți fiecare (de asemenea, poate exista un satelit care partajează încurcarea cu ambele OGS-uri simultan).

3. Definim o metrică de fidelitate compozită care ia în considerare fidelitatea estimată a fiecărei perechi pe care Alice o deține cu sateliții $fid_{S_A}$, fidelitatea fiecărei perechi pe care Bob o deține cu sateliții $fid_{S_B}$ și fidelitatea estimată $flf(S_A, S_B)$ a transmisiei celor două jumătăți de pereche la nivel de satelit către aceeași locație (care ar putea fi unul dintre cei doi sateliți care dețin jumătățile de pereche sau poate un satelit situat la jumătatea distanței între cei doi; dacă un singur satelit este încurcat cu ambele OGS-uri, atunci fidelitatea transmisiei este considerată 1).

4. Algoritmul identifică o pereche de particule $(S_A, S_B)$ pe partea lui Alice și Bob care maximizează metrica de fidelitate compozită.

5. Jumătățile de pereche la nivel de satelit sunt trimise către aceeași locație (dacă este necesar) și se realizează un swapping de încurcare [33, 34, 35], așa cum este descris în [36]. Alice și Bob partajează acum o particulă încurcată.

Pentru a măsura amploarea îmbunătățirii produse de distribuția preventivă, am creat o simulare a unei constelații de sateliți LEO cu un număr de orbite între 1 și 200 și un număr de sateliți pe orbită între 1 și 200 (ambele parametrizate la nivel de simulare cu un factor de densitate a rețelei $\alpha$). Propunem o metrică pentru fidelitatea transmisiei care scade odată cu distanța și care este parametrizată la nivel de simulare cu un factor de pierdere $\beta$ care cuprinde pierderile datorate tuturor tipurilor de factori de mediu pentru care nu avem valori experimentale. Testăm pentru două OGS-uri fixe în două scenarii diferite: scenariul A în care protocolul a fost rulant timp de 2 ore; și scenariul B în care protocolul a fost rulant timp de 24 de ore. Considerăm ca variabile pentru simulări valoarea $\alpha$, rata de transmisie a perechilor încurcate de la sateliți către OGS-uri și rata de consum a încurcărilor la nivel terestru. Plotăm mai multe metrici de performanță: diferența în stocul de particule încurcate la OGS-uri la sfârșitul scenariului (mai mare este mai bine, deoarece înseamnă că OGS-urile au reușit să acumuleze mai multe perechi), numărul mediu de salturi pe care particulele le parcurg între sateliți (mai mic este mai bine, deoarece există mai puțină pierdere de fidelitate din cauza swapping-ului), distanța medie parcursă de particule între sateliți (mai mică este mai bine, deoarece există mai puțină pierdere de fidelitate din cauza transmisiei). Comparăm rezultatele cu protocoalele non-preventive similare cu cele prezentate mai sus și arătăm că distribuția preventivă duce la valori îmbunătățite pe toate metricile de performanță pe care le-am simulat.

## 1.5 Împrumuturi QKD Descentralizate prin Blockchain - vezi [5]

O problemă semnificativă care împiedică adoptarea pe scară largă a infrastructurii QKD pentru comunicații securizate este costul ridicat al dispozitivelor și legăturilor QKD. Un singur dispozitiv QKD comercial are un cost estimat între 200.000 și 700.000 de dolari și o rază de acțiune de doar 90-150 km. În consecință, chiar și pentru entități cu mare putere financiară și interes ridicat pentru securitate (cum ar fi: bănci, firme de investiții, guverne naționale și altele), operarea QKD pe distanțe lungi poate fi încă prohibitivă din punct de vedere financiar.

Pentru a facilita adoptarea, este necesar un sistem care să abstractizeze proprietatea infrastructurii QKD, permițând deținătorilor de infrastructură să împrumute o parte din rata de cheie de-a lungul legăturilor într-un mod descentralizat. Descentralizarea este utilă pentru a produce o rețea democratizată, unde orice entitate poate contribui cu legături suplimentare. De exemplu, o bancă poate fi interesată să securizeze conexiunea dintre un oraș mare C și un oraș mic T. Să presupunem că conexiunea C-T nu este de interes semnificativ pentru alți deținători mari de infrastructură (cum ar fi guvernul național) și, prin urmare, nu este niciodată construită decât dacă banca ia această inițiativă. Pentru bancă, costul este prohibitiv de mare; cu toate acestea, dacă împrumutul unei părți din

rata de cheie de-a lungul acelei legături este o opțiune, profiturile din împrumut ar putea compensa impactul financiar al costului inițial.

Calitățile sistemelor blockchain ca registre descentralizate și imuabile le fac potrivite pentru un astfel de sistem. Cu toate acestea, descentralizarea și imuabilitatea vin cu un cost: sistemele blockchain au dezavantaje puternice de performanță. Nu numai că tranzacțiile au o taxă dinamică pentru execuție (care, în funcție de blockchain și de încărcarea rețelei, poate ajunge chiar la zeci sau sute de dolari, chiar și pentru un simplu transfer de criptomonedă), dar tranzacțiile necesită un timp semnificativ pentru a fi confirmate (deși timpul mediu de bloc este de 10 minute pentru Bitcoin și 12 secunde pentru Ethereum, timpul în care o tranzacție rămâne în așteptare în mempool poate depăși câteva ore dacă congestia rețelei este mare).

Astfel, în această lucrare, proiectăm un protocol de smart contract pe blockchain-ul Ethereum pentru plăți instantanee și tranzacții latente. Acest protocol poate fi utilizat pentru o infrastructură descentralizată pentru a permite accesul instantaneu la servicii, cum ar fi închirierea unei legături QKD.

Cu tranzacțiile latente, ne propunem să rezolvăm una dintre problemele dificile în blockchain-uri - cea a timpilor lungi de consens (adică timpul care trece de la momentul în care o tranzacție este trimisă în blockchain până la momentul în care este inclusă într-un bloc de către un miner și este considerată confirmată) și a taxelor ridicate (adică taxele în criptomonedă care sunt plătite de persoana care trimite o tranzacție către minerul care o include într-un bloc). Scopul este de a permite unui furnizor de servicii să accepte plăți instantanee pentru serviciile lor off-chain și să deconteze plata în criptomonedă reală on-chain atunci când este posibil (și, poate, când rețeaua este mai puțin congestionată și taxele sunt mai mici).

Algoritmul de tranzacții latente constă în următorii pași cheie:

1. Furnizarea serviciului și plicurile latente. În momentul în care furnizorul de servicii $S$ furnizează un serviciu clientului $C$ pentru o sumă de criptomonedă de $P$, clientul $C$ va produce un plic semnat care, dacă ar fi înregistrat în blockchain, ar transfera $P$ din soldul său în cel al lui $S$. Clientul trimite apoi acest plic (off-chain, prin orice metodă de comunicare) către furnizorul de servicii.

2. Faza de inițializare. Ori de câte ori este convenabil, furnizorii de servicii pot înregistra plicurile pe care le-au primit în smart contract. Smart contract-ul va construi un model intern sub forma unui graf orientat, unde nodurile reprezintă utilizatorii sistemului, iar muchiile reprezintă datoria fiecărui utilizator față de un alt utilizator (conform plicurilor înregistrate).

3. Faza de redistribuire. În această fază, muchiile de intrare și de ieșire se anulează reciproc pentru a redistribui datoria în scopul de a minimiza numărul de transferuri care trebuie efectuate între utilizatori, pentru a reduce costul taxei de tranzacție.

4. Faza de execuție. În această fază, datoriile rămase sunt procesate și tranzacțiile latente sunt executate. Un caz special implică un utilizator care încearcă să "cheltuiască dublu" - adică utilizatorul poate trimite plicuri semnate către mai mulți furnizori de servicii astfel încât suma totală a plicurilor să depășească soldul utilizatorului; în acest caz, este necesar un mecanism de soluționare a datoriei. În algoritmul nostru, datoria este soluționată prin împărțirea soldului disponibil al debitorului către toți creditorii săi, proporțional cu datoria datorată fiecăruia.

5. Sistem de revizuire a clienților. Pentru a permite furnizorilor de servicii să aibă o imagine precisă a clienților și să ia decizii informate atunci când își oferă serviciile, fiecare utilizator are o intrare pe un server centralizat care urmărește tranzacțiile lor latente istorice și probabilitatea de a-și plăti datoria.

În contextul închirierii de legături QKD, și având în vedere ratele de cheie de obicei scăzute ale dispozitivelor QKD, acest protocol permite decontarea rapidă a cererilor de închiriere a legăturilor QKD, ceea ce reprezintă un pas important către adoptarea pe scară largă a comunicațiilor securizate prin QKD pe distanțe terestre lungi.

# Capitolul 2

# Implementări folosind Quantum Key Distribution

## 2.1 QKD Get Key Tool - vezi [6]

Un standard important și răspândit printre furnizorii de dispozitive QKD este standardul ETSI GS QKD 014 (în prezent la versiunea V1.1.1), publicat de ETSI (European Telecommunications Standards Institute) în februarie 2019, care definește protocolul de comunicație și interfața REST API între un KMS (în ETSI 014, KME - Key Management Entity) și o aplicație (în ETSI 014, SAE - Secure Application Entity). Acest standard oferă o modalitate standardizată pentru aplicații de a solicita chei printr-o legătură QKD, abstractizând astfel detaliile specifice ale implementării acelui dispozitiv particular. Este susținut de mai mulți dintre principalii furnizori care oferă astăzi dispozitive QKD disponibile comercial.

ETSI 014 definește următoarea structură a endpoint-urilor în REST API:

`https://{KME_hostname}/api/v1/keys/{SAE_ID}/{endpoint}`

Sunt definite trei endpoint-uri: Get status (status), Get key (enc_keys) și Get key with key IDs (dec_keys). Endpoint-ul "Get status" returnează diverse informații de status despre dispozitivul qkd, cum ar fi ID-ul acestuia, dimensiunea cheii, numărul de chei stocate, numărul maxim de chei per cerere, dimensiunea minimă și maximă a cheii etc. Endpoint-ul "Get key" preia o cheie între nodul care rulează KME și nodul identificat de parametru SAE id, și returnează cheia și ID-ul acesteia (sau un array de astfel de elemente, dacă sunt solicitate mai multe chei), cu biții cheii codificați în Base64. Același ID trebuie trimis către celălalt nod prin orice canal de comunicație clasic (modul în care este trimis nu face parte din acest standard), care poate obține apoi aceeași cheie utilizând endpoint-ul "Get key with key IDs" prin atașarea ID-ului cheii la cerere; nodul va răspunde cu aceeași cheie ca și KME original.

QKD GKT este disponibil pe Github și a fost lansat public pe 1 iulie 2024 sub licența Apache 2.0.

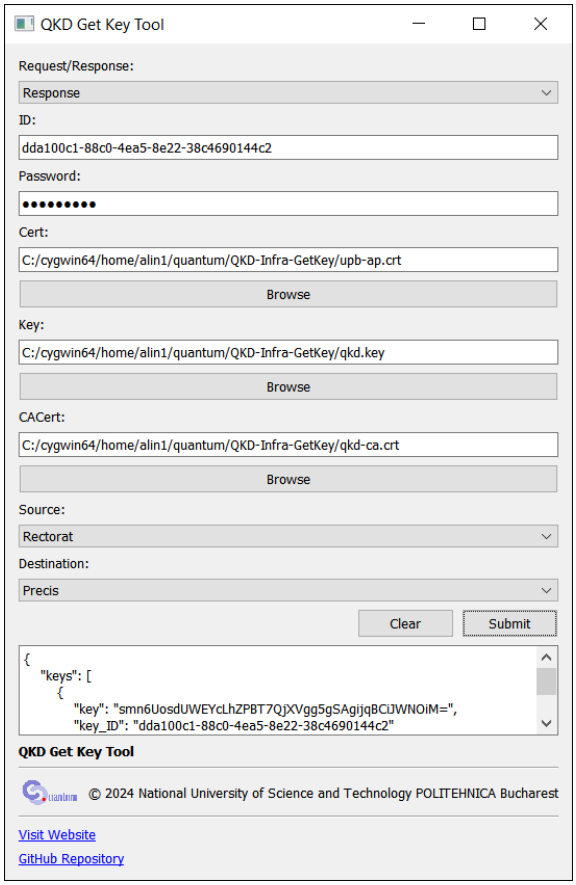



Figura 2.1: Interfața Utilizator pentru QKD Get Key Tool

## 2.2 Transfer de Fișiere Sigur Necondiționat - vezi [7]

Una dintre aplicațiile imediate ale QKD este transferul de fișiere necondiționat sigur. În acest scop, am construit aplicația Quantum File Transfer (QFT) ca un software ușor de utilizat, prietenos cu utilizatorul, pentru valorificarea cheilor QKD pentru transmisii de date necondiționat sigure.

Există câteva elemente importante de remarcat despre broker. În primul rând, acesta nu prezintă un risc pentru securitatea necondiționată: cheile nu părăsesc niciodată locațiile lui Alice și Bob; brokerul doar retransmite fișierul (după ce a fost criptat de Alice) către Bob (care apoi îl decriptează folosindu-și cheia). În al doilea rând, brokerul nu trebuie neapărat să fie accesibil public de oricine prin Internet: brokerul trebuie să fie accesibil doar pentru Alice și Bob. Motivația pentru existența unui broker central care retransmite mesajele între Alice și Bob provine din obiectivul de a face QFT un instrument scalabil și de uz general. În cazul unei rețele mari, Alice sau Bob pot fi în spatele unui punct de Network Address Translation (NAT); dacă nu au un IP public și static, atunci singura modalitate de a se putea conecta unul cu celălalt ar fi să configureze un port forwarding în rețelele lor respective. În funcție de administrarea rețelei, acest lucru poate fi dificil; existența unui broker central, accesibil public, cu un IP static cunoscut atât de Alice, cât

și de Bob, elimină necesitatea acestei configurații.

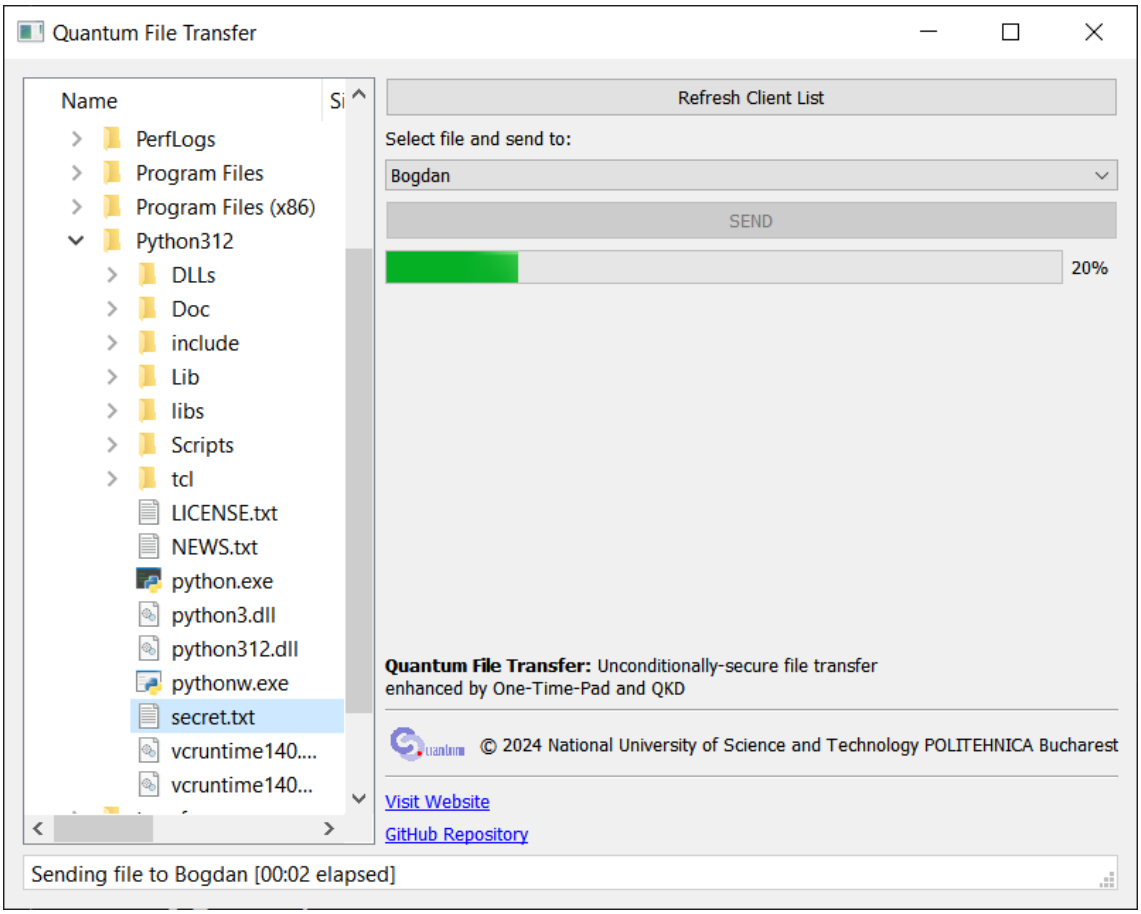



Figura 2.2: Interfața utilizatorului pentru ecranul principal al QFT

Quantum File Transfer este disponibil pe Github și a fost lansat public pe 1 iulie 2024 sub licența Apache 2.0.

## 2.3 Arhitectură de VPN Rezistentă la Atacuri Cuantice - vezi [8]

În această lucrare, ne concentrăm pe dezvoltarea unui sistem de comunicație sigur, eficient și versatil între două puncte finale. Definim următoarele obiective: O1 - ne propunem să proiectăm sistemul pentru utilizare generală și să acomodăm o gamă largă de aplicații; O2 - ne propunem să incorporăm criptarea sigură cuantic pentru a ne apăra preventiv împotriva amenințărilor pe care calculul cuantic le prezintă pentru criptarea clasică; O3 - sistemul ar trebui să fie implementabil practic folosind dispozitivele QKD disponibile astăzi.

Din câte știm, acesta este primul experiment românesc cu un VPN securizat prin chei generate de QKD, utilizând chei furnizate de prima rețea integrată QKD disponibilă în

România, parte a infrastructurii Universității Politehnica din București [37]. Pe parcursul acestor experimente, universitatea noastră pune bazele Infrastructurii Naționale de Comunicații Cuantice din România (RoNaQCI)[38], parte a Infrastructurii Europene de Comunicații Cuantice (EuroQCI)[39], un proiect coordonat de UPB.

Scopul Quantum General-Purpose VPN (QGP-VPN) este de a stabili o soluție VPN quantum-resistant, cu scop general, între două părți, astfel încât orice aplicație sau caz de utilizare să poată fi implementat deasupra acestuia cu ușurință.

Rezistența cuantică este realizată prin efectuarea unui pas QKD ori de câte ori este inițiată o sesiune VPN și utilizarea cheii generate ca secret pre-partajat pentru criptarea sesiunii de schimb de chei ca parte a stabilirii conexiunii VPN. Această abordare va fi implementabilă practic folosind dispozitivele QKD disponibile astăzi, deoarece este necesară o cheie doar la începutul unei sesiuni VPN, ceea ce este realizabil chiar și cu rate de generare a cheilor scăzute.

Arhitectura software este următoarea. Există trei centre de date capabile de QKD: Campus@UPB (Alice), Rectorat@UPB (Bob) și Precis@UPB (Server Central). Serverul Central are o legătură QKD cu Alice (QKD1-A și QKD1-B) și o altă legătură QKD cu Bob (QKD2-A și QKD2-B). În proximitatea fizică a fiecărui dispozitiv QKD (de exemplu, într-o cameră securizată din Campus și Rectorat) există doi clienți VPN (Alice și Bob) și un server VPN accesibil public în Precis. Toate cele trei componente VPN pot solicita chei cuantice de la dispozitivele QKD respective.

Fluxul de date și algoritmul efectuat de componentele VPN ale sistemului pot fi împărțite în două faze separate: faza de pregătire (efectuată o singură dată pentru fiecare dispozitiv) și faza de rulare (efectuată la începutul fiecărei sesiuni de comunicație).

Faza de pregătire implică configurarea Serverului VPN pentru rutarea TCP și schimbul de chei de autentificare între Serverul VPN și fiecare client VPN.

Faza de rulare implică fiecare client VPN care trimite o cerere de cheie către Serverul VPN. Serverul primește cheile generate de dispozitivul QKD asociat acelui client VPN și transmite ID-ul cheii înapoi către clientul VPN. Clientul primește apoi cheia cu același ID de la capătul opus al legăturii QKD. După aceea, atât clientul, cât și serverul folosesc cheia QKD ca secret pre-partajat pentru a cripta parametrii unui schimb de chei Diffie-Hellman, care este utilizat pentru a stabili o cheie de sesiune pentru a cripta comunicațiile în timpul sesiunii de conexiune VPN. Deoarece parametrii Diffie-Hellman înșiși sunt criptați cu cheia generată de QKD, întregul proces este quantum-resistant. Odată ce toți clienții au terminat de efectuat algoritmul, toți sunt în aceeași rețea virtuală și pot rula orice aplicație compatibilă LAN cu securitate quantum-resistant îmbunătățită prin QKD.

Acest lucru a fost realizat folosind dispozitive reale IDQ QKD disponibile la UPB. Codul complet și configurarea sunt disponibile la cerere justificată.

Ca parte a implementării, am utilizat următorul echipament și software: 4x sisteme IDQ Cerberis XG QKD pentru capabilități QKD (Alice, Bob, Charlie) și infrastructura construită la UPB ca parte a proiectului RoNaQCI; o mașină virtuală care rulează Alma Linux 8 în rețeaua internă UPB pentru Serverul VPN; 2x laptopuri Windows 10 care rulează în locații securizate cu acces la dispozitive QKD pentru clienții VPN Alice și Bob; WireGuard – soluție VPN securizată, gratuită, open-source [40], cu configurație personalizată pentru setarea noastră; Linphone – software SIP/VoIP gratuit, open-source, pentru videoconferințe [41].

Ca direcții viitoare de cercetare, sistemul poate fi făcut mai sigur prin actualizarea secretului pre-partajat la fel de des pe cât permite rata de cheie a dispozitivelor QKD,

în loc de a face acest lucru la începutul fiecărei sesiuni de comunicație. O altă direcție de cercetare este analiza comportamentului și a potențialelor optimizări ale sistemului în rețele mai mari. O abordare pentru a crește și mai mult securitatea sistemului ar fi înlocuirea algoritmului de schimb de chei integrat în software-ul VPN cu un algoritm de schimb de chei quantum-resistant mai bun.

## 2.4 Configurator VPN - vezi [9]

Pentru a permite cazuri de utilizare care valorifică cheile QKD mai avansate decât un transfer de fișiere (criptarea traficului arbitrar, cum ar fi o videoconferință peer-to-peer), este necesar un VPN îmbunătățit cu QKD, așa cum a fost prezentat în secțiunea anterioară. Cu toate acestea, configurarea unui astfel de VPN poate fi dificilă pentru persoanele fără cunoștințe tehnice. Scopul Quantum VPN Configurator este de a oferi o interfață grafică prietenoasă pentru utilizator, care să genereze configurațiile necesare.

Configuratorul este conceput pentru a fi rulat de utilizatorii care doresc să stabilească o conexiune VPN după cum urmează: configuratorul este rulat pe un computer care va acționa ca server VPN; în același timp, configuratorul este rulat și pe două (sau mai multe) computere care se vor conecta la serverul VPN ca clienți. Odată rulat cu succes, oricare dintre clienți va putea stabili un tunel VPN către server și va asigura criptarea post-cuantică pentru comunicațiile lor cu oricare alți clienți. Serverul trebuie să fie accesibil public de către toți clienții și să aibă un IP static.

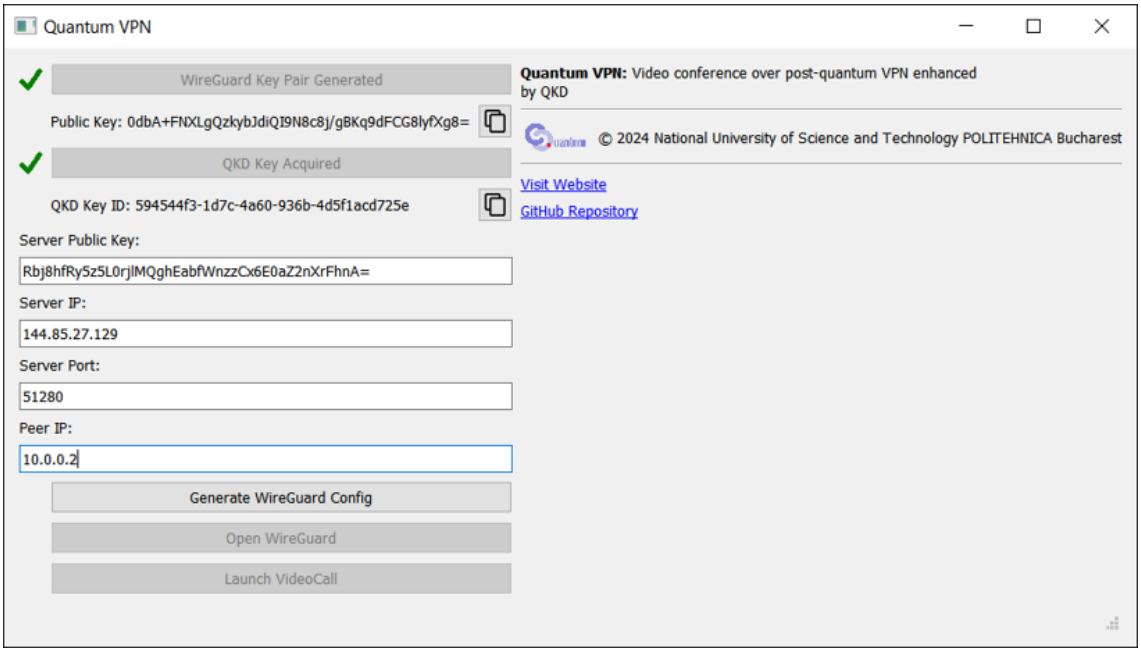



Figura 2.3: Ecranul principal al Quantum VPN Configurator

Pentru a stabili un VPN, se folosește software-ul VPN open-source WireGuard după generarea configurațiilor. În scopuri demonstrative, configuratorul ajută, de asemenea, utilizatorul să efectueze o videoconferință, lansând Linphone (un software open-source VoIP SIP).

VPN Configurator este disponibil pe Github și a fost lansat public pe 1 iulie 2024 sub licența Apache 2.0.

## 2.5 Arhitectură de Monitorizare QKD

Infrastructura RoNaQCI constă într-un ansamblu distribuit la nivel național de dispozitive QKD, legăturile dintre acestea și resursele suport, cum ar fi serverele de acces, depozitele de chei și serviciile de monitorizare. Pentru a monitoriza cu acuratețe starea și statisticile de utilizare ale dispozitivelor și legăturilor și pentru a oferi o metodă ușor accesibilă administratorilor și tehnicienilor RoNaQCI de a actualiza configurațiile dispozitivelor, va fi dezvoltat Dashboard-ul de Monitorizare QKD RoNaQCI (QKD-MonDash). Scopul acestui document este de a defini aspectele tehnice ale QKD-MonDash și de a pune bazele implementării acestuia.

În această lucrare, am identificat o listă de personae relevante pentru proiectarea MonDash (Admin RoNaQCI, Tehnician RoNaQCI, Șef de Partener RoNaQCI, Șef de Caz de Utilizare RoNaQCI, Utilizator QKD RoNaQCI, Auditor RoNaQCI, Public General); am identificat și descris principalele caracteristici țintă ale MonDash (vizualizare și monitorizare, colectare de statistici de utilizare, alerte și notificări personalizabile, actualizarea și configurarea dispozitivelor, acces securizat și roluri de utilizator, API expus pentru integrare ușoară, scalabilitate și autodescoperire, considerații suplimentare), am creat arhitectura software și am conturat componentele și fluxul secvențial al datelor, am dezvoltat un plan de testare și am produs mockup-uri preliminare de design.

## 2.6 Simulator de Rețea QKD

Simulatorul de Rețea QKD este o inițiativă ambițioasă de a crea un simulator complet pentru rețele QKD de scară largă. Interfața simulatorului (afișată în figura 2.4) are trei secțiuni:

- Vederea de proiectare a rețelei, care afișează nodurile și legăturile rețelei. Nodurile pot fi trase în jurul vizualizării, iar informațiile referitoare la noduri și legături sunt afișate conform selecțiilor din planul de control;
- Vederea hărții în timp real, care afișează locațiile geografice ale nodurilor pe o hartă mondială offline;
- Planul de control, unde utilizatorul poate configura diverse setări legate de rețeaua QKD.

Planul de control conține setările rețelei QKD împărțite în următoarele tab-uri:

- File: acest tab conține informații și setări despre fișierul de simulare și permite salvarea și încărcarea configurațiilor;
- Sim: tab-ul Sim controlează parametrii simulării, cum ar fi viteza simulării, avansarea sau întoarcerea în timp, pauzarea simulării;

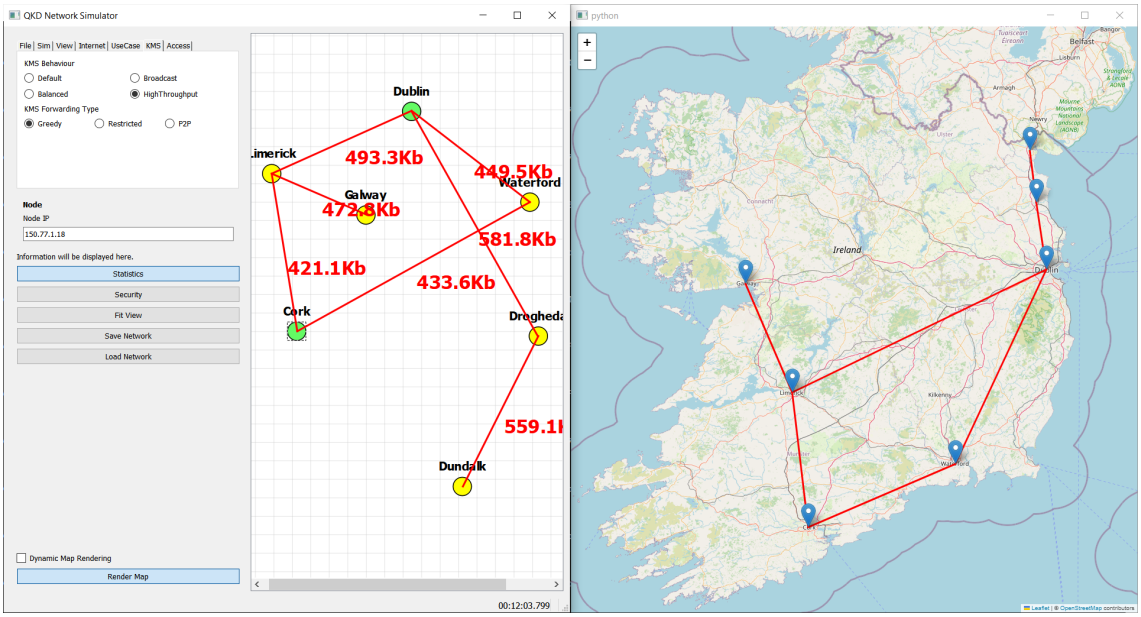



Figura 2.4: Interfața Utilizator pentru Simulatorul de Rețea QKD

- View: tab-ul View poate fi folosit pentru a controla vederea secțiunilor de proiectare a rețelei și a hărții; aici, utilizatorul poate activa sau dezactiva grila, poate edita aspectul nodurilor și poate selecta informațiile care să fie afișate pentru fiecare nod (nume, locație, număr de legături, etc.), legătură (rata de cheie, numărul de chei stocate, utilizarea cheilor, viteza internetului etc.) și stratul rețelei care urmează să fie vizualizat (conexiuni QKD fizice, conexiuni QKD indirecte prin retransmitere, Internet);

- Internet: aici, utilizatorul poate configura parametrii legati de Internet, cum ar fi întârzierea pachetelor pe legătură, pierderea pachetelor, sau poate face nodurile să devină offline sau online. De asemenea, utilizatorul poate configura adresa IP a fiecărui nod;

- UseCase: în tab-ul UseCase, utilizatorul poate seta cazuri de utilizare care consumă chei pentru a simula efectul acestora asupra ratei totale de cheie în rețea. De asemenea, utilizatorul poate programa cazuri de utilizare care se așteaptă să aibă loc periodic;

- KMS: în tab-ul KMS, poate fi configurat comportamentul KMS, precum și metoda de retransmitere a cheilor;

- Access: în tab-ul Access, rolurile utilizatorilor pot fi configurate, iar regulile de acces pot fi setate pentru fiecare nod sau legătură, în funcție de cazul de utilizare.

# Concluzii

În această lucrare, au fost aduse mai multe contribuții semnificative. Pe partea de distribuție a încurcării, s-a demonstrat că distribuirea preventivă cu swapping la cerere doar la nivelul satelitului crește semnificativ eficiența distribuției încurcării bazate pe spațiu. În ceea ce privește QKD, a fost introdus conceptul de comportamente ale rețelelor QKD și a fost propusă o schemă optimă de retransmitere a cheilor; aceasta a fost extinsă luând în considerare constrângerile rețelelor QKD federate practice (cum ar fi în cazul rețelelor conectate internațional), prin introducerea legăturilor virtuale QKD și a rețelelor virtuale QKD; pentru proiectarea practică a rețelelor QKD, a fost propusă o metodologie și un algoritm de proiectare optimă (în termeni de cost); și a fost sugerată o schemă de plată instantanee a serviciilor bazată pe blockchain cu tranzacții latente. Mai multe contribuții sunt implementări de cod practice (trei dintre ele deja lansate ca software open-source): o interfață grafică de utilizator deasupra celui mai utilizat REST API pentru interacțiunea cu dispozitivele QKD; un instrument software pentru transferul de fișiere necondiționat sigur; o arhitectură propusă și un configurator software pentru un VPN post-cuantic cu QKD, care poate fi utilizat pentru a cripta trafic arbitrar, cum ar fi o videoconferință; un stack de arhitectură pentru monitorizarea stării și performanței rețelelor QKD; și un simulator de rețea QKD foarte necesar pentru a ajuta viitoarele implementări de scară largă.

Obiectivul meu în această teză a fost să avansez comunicațiile cuantice în termeni de securitate, utilitate, performanță și adopție. Mai multe dintre descoperirile mele contribuie la securitate îmbunătățită: rețelele virtuale pot fi utilizate pentru un control mai granular al accesului; stack-ul de arhitectură QKD oferă linii directoare pentru integrarea unui strat de securitate în proiectarea rețelelor QKD; și implementările software oferă utilizatorilor mijloace directe de a beneficia de securitatea necondiționată a cheilor QKD în viața lor de zi cu zi. Alte descoperiri contribuie la creșterea utilității QKD: comportamentele QKD pot face o rețea mai utilă prin asigurarea ratei de cheie necesare pentru cazuri de utilizare specifice; de asemenea, rețelele virtuale pot duce la scenarii de utilizare internaționale mai ușoare. În ceea ce privește performanța: protocolul SkySwapping reprezintă un reper important în ceea ce privește distribuția practică a încurcării pentru viitorul internet cuantic; iar algoritmul de proiectare a rețelei optime asigură că ratele optime de cheie pot fi identificate și atinse în funcție de constrângerile dorite în condițiile unui buget limitat. În cele din urmă, pentru a spori adopția, împrumutul bazat pe blockchain prin tranzacții instantanee deschide calea pentru o rețea QKD globală și descentralizată, accesibilă oricui; rețelele virtuale rezolvă probleme dificile de adopție generate de interconectarea rețelelor cu reguli diferite, poate construite și guvernate de entități cu interese nealiniate sau sub diferite corpuri de reglementare; și în cazurile în care regulile sunt de neschimbat, simulatorul de rețea QKD poate fi utilizat pentru a obține o predicție precisă a interconectării

și, eventual, pentru a găsi o soluție.

Mai multe dintre rezultatele mele pot (și vor) da naștere unor cercetări viitoare. O extindere aprofundată a stack-ului de arhitectură pentru straturi de securitate standardizate; proiectarea optimă a rețelelor QKD în contextul unor constrângeri practice specifice; alte implementări software care valorifică QKD pentru cazuri de utilizare specifice care nu intră în sfera unui transfer de fișiere sau a unui VPN; acestea sunt toate idei care sunt pe masă pentru lucrări viitoare.

Între timp, nu pot să nu mă gândesc că noi, cercetătorii în tehnologii cuantice, ne aflăm într-un moment de cotitură în lumea științifică. Între explorarea limitelor calculului, înțelegerea stării actuale de "Vest Sălbatic" a scenei, cu puțină standardizare și multe teritorii neexplorate, și satisfacerea nevoilor practice ale utilizatorilor actuali și viitori ai acestor tehnologii, avem o oportunitate incredibilă (și o responsabilitate imensă) de a modela viitorul tehnologiei și al societății în ansamblu.

# Bibliografie


[1] A.-B. Popa and P. G. Popescu, "Optimal key forwarding strategy in qkd behaviours," *Scientific Reports*, vol. 14, 2024.

[2] A.-B. Popa and P. G. Popescu, "The future of qkd networks," *arXiv preprint arXiv:2407.00877*, 2024.

[3] A.-B. Popa *et al.*, "Optimal qkd network design," *Submitted for publication at Scientific Reports*, 2024.

[4] A.-B. Popa, B.-C. Ciobanu, V. Iancu, F. Pop, and P. G. Popescu, "Skyswapping: Entanglement resupply by separating quantum swapping and photon exchange," *Future Generation Computer Systems*, vol. 158, pp. 89–97, 2024.

[5] A. B. Popa, I. M. Stan, and R. Rughiniş, "Instant payment and latent transactions on the ethereum blockchain," in *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–4, IEEE, 2018.

[6] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "QKD Get Key Tool," July 2024.

[7] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "Quantum File Transfer," July 2024.

[8] A.-B. Popa, "Qgp-vpn: Qkd enhanced vpn solution for general-purpose encrypted communications," in *2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6, IEEE, 2023.

[9] A.-B. Popa, B.-C. Ciobanu, and P. G. Popescu, "Quantum VPN," July 2024.

[10] A.-B. Popa, I. M. Florea, and R. Rughiniş, "Convolutional neural network portfolio management system with heterogeneous input," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–4, IEEE, 2020.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[12] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2022.

[13] G. Karakostas, "Faster approximation schemes for fractional multicommodity flow problems," *ACM Transactions on Algorithms (TALG)*, vol. 4, no. 1, pp. 1–17, 2008.

[14] L. K. Fleischer, "Approximating fractional multicommodity flow independent of the number of commodities," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 4, pp. 505–520, 2000.

[15] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, *et al.*, "Quantum key distribution: a networking perspective," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[16] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, no. 6, pp. 389–392, 2009.

[17] V. Azimi Mousolou, "Entanglement fidelity and measure of entanglement," *Quantum Information Processing*, vol. 19, no. 9, p. 329, 2020.

[18] S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," *Entropy*, vol. 24, no. 2, 2022.

[19] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, pp. 441–444, Jul 2000.

[20] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[21] R. Terhaar, J. Rödiger, M. Häußler, M. Wahl, H. Gehring, M. A. Wolff, F. Beutel, W. Hartmann, N. Walter, J. Hanke, P. Hanne, N. Walenta, M. Diedrich, N. Perlot, M. Tillmann, T. Röhlicke, M. Ahangarianabhari, C. Schuck, and W. H. P. Pernice, "Ultrafast quantum key distribution using fully parallelized quantum channels," *Optics Express*, vol. 31, pp. 2675–2688, Jan 2023.

[22] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, "Efficient distributed quantum computing," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 469, no. 2153, p. 20120686, 2013.

[23] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Communication*, vol. 1, no. 1, pp. 3–8, 2020.

[24] A. Tănăsescu, D. Constantinescu, and P. G. Popescu, "Distribution of controlled unitary quantum gates towards factoring large numbers on today's small-register devices," *Scientific Reports*, vol. 12, no. 1, p. 21310, 2022.

[25] S. Bose and D. Home, "Generic entanglement generation, quantum statistics, and complementarity," *Physical Review Letters*, vol. 88, p. 050401, Jan 2002.

[26] I. S. Madjarov, J. P. Covey, A. L. Shaw, J. Choi, A. Kale, A. Cooper, H. Pichler, V. Schkolnik, J. R. Williams, and M. Endres, "High-fidelity entanglement and detection of alkaline-earth rydberg atoms," *Nature Physics*, vol. 16, no. 8, pp. 857–861, 2020.

[27] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, "Unambiguous quantum measurement of nonorthogonal states," *Physical Review A*, vol. 54, pp. 3783–3789, Nov 1996.

[28] E. V. H. Doggen, Y. Gefen, I. V. Gornyi, A. D. Mirlin, and D. G. Polyakov, "Generalized quantum measurements with matrix product states: Entanglement phase transition and clusterization," *Physical Review Research*, vol. 4, p. 023146, May 2022.

[29] T.-C. Yen, A. Ganeshram, and A. F. Izmaylov, "Deterministic improvements of quantum measurements with grouping of compatible operators, non-local transformations, and covariance estimates," *npj Quantum Information*, vol. 9, no. 1, p. 14, 2023.

[30] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New Journal of Physics*, vol. 21, no. 9, p. 093055, 2019.

[31] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Review Letters*, vol. 119, p. 200501, Nov 2017.

[32] M. T. Gruneisen, B. A. Sickmiller, M. B. Flanagan, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, "Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver," *Optical Engineering*, vol. 55, no. 2, pp. 026104–026104, 2016.

[33] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Physical Review Letters*, vol. 80, pp. 3891–3894, May 1998.

[34] S. Liu, Y. Lou, Y. Chen, and J. Jing, "All-optical entanglement swapping," *Physical Review Letters*, vol. 128, p. 060503, Feb 2022.

[35] E. Shchukin and P. van Loock, "Optimal entanglement swapping in quantum repeaters," *Physical Review Letters*, vol. 128, p. 150502, Apr 2022.

[36] M.-Z. Mina and P. G. Popescu, "Entanglenet: Theoretical reestablishment of entanglement in quantum networks†," *Applied Sciences*, vol. 8, no. 10, 2018.

[37] "First romanian qkd network." [Online]. Available: `http://quantum.upb.ro/blog.html`. Accessed: 2024.

[38] "Romanian national quantum communication infrastructure," 2023. [Online]. Available: `https://www.ronaqci.eu/`. Accessed: 2024.

[39] "The european quantum communication infrastructure (euroqci) initiative." `https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci`. Online; accessed 12 February 2024.

[40] J. A. Donenfeld, "Wireguard: Fast, modern, secure vpn tunnel." [Online]. Available: `https://www.wireguard.com/`. Accessed: 2024.

[41] "Linphone: open source voip project." [Online]. Available: `https://www.linphone.org/`. Accessed: 2024.