Quantum Key Distribution: Infrastructure Security Integration and Practical Deployment for Internet Service Providers and Network Operators

RoNaQCI Training @ Cluj-Napoca

Quantum Computing și Quantum Communications sunt două domenii de frontieră care vor avea un impact covârșitor în cybersecurity și modul în care schimbăm sau stocăm date în mediul online. La nivel global, până în aprilie 2024 în aceste tehnologii se investiseră $8.5 miliarde în mediul privat (start-up-uri), cu peste $40 miliarde anunțați în investiții publice. Folosirea tehnologiilor computaționale bazate pe principii din mecanica cuantică promite optimizări massive cu impact în industria financiară, energie, transport, logistică, farmaceutică și produse medicale, dar și telecomunicații și media, cu o valoare totală adăugată în economie estimată la peste $1 bilion (1000 de miliarde)[i]. În particular, Quantum Key Distribution (QKD), fiind singura tehnologie de schimb de chei criptografice cunoscută în prezent ca fiind sigură necondiționat, este la momentul actual unica variantă de protecție împotriva calculatoarelor cuantice și progreselor în criptanaliză.

La nivel european, proiectul EuroQCI în care s-au investit peste 180 de milioane de euro, își propune crearea unei infrastructuri europene de QKD care să securizeze instituțiile publice, universități, spitale, agenții de stat ș.a.m.d. Proiectul Romanian National Quantum Communication Infrastructure[ii] (RoNaQCI, parte a EuroQCI), condus de POLITEHNICA București, dezvoltă în România cea mai mare infrastructură terestră de QKD din EuroQCI, în 6 orașe (București, Craiova, Timișoara, Iași, Cluj-Napoca, Constanța), conectate la un backbone național, cu 36 de linkuri QKD în total.

La trainingul efectuat la Cluj-Napoca se vor atinge atât fundamentele teoretice pentru quantum computing și quantum key distribution, dar și aspecte practice precum integrarea tehnologiei QKD pentru operatorii de rețele și providerii de Internet pentru crearea unei infrastructuri sigure de comunicație.

- **Training Session 1** – Basic Quantum Knowledge: resources on quantum computing, brief history of quantum, about Sandu Popescu, quantum bit (qubit), superposition and mathematical formalism, quantum measurement, single qubit gates, multiple qubit systems and gates, examples (CNOT, Hadamard, Swap, general n-qubit gates), Walsh-Hadamard transformation, no-cloning theorem, entanglement and Bell states, teleportation protocol
- **Training Session 2** – Basic QKD Knowledge: basics of encryption, classical encryption and key exchange, RSA, Discrete Log Diffie-Hellman, Elliptic Curve Diffie Hellman, security of classical key exchange, quantum key distribution, QKD devices, QKD networks, RoNaQCI, history of QKD, wave nature of light, photon polarization, BB84 protocol with and without eavesdropper, One-Time Pad encryption
- **Training Session 3** – QKD Networks: specifics of QKD infrastructure, QKD hardware requirements and overview, QKD networks examples, QKD network design
- **Training Session 4** – Interacting with a QKD Device and QKD Applications: QKD standards (ETSI GS QKD 014), SAE/KME architecture, ETSI-014 REST API (status, enc_keys, dec_keys), format and optional values of request and response, interacting with a QKD device via curl/postman, OTP with real QKD keys (practical example), using a QKD SDK, live demos of QKD applications.

[i] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

[ii] https://www.ronaqci.eu/