



Network Traffic Encryptor on Linux Platform

R&D in Quantum Technologies

Bc. Jan Havlín
Oct. 9, 2025



R&D IN CYBERSECURITY

- **Department of Telecommunications, Brno University of Technology**

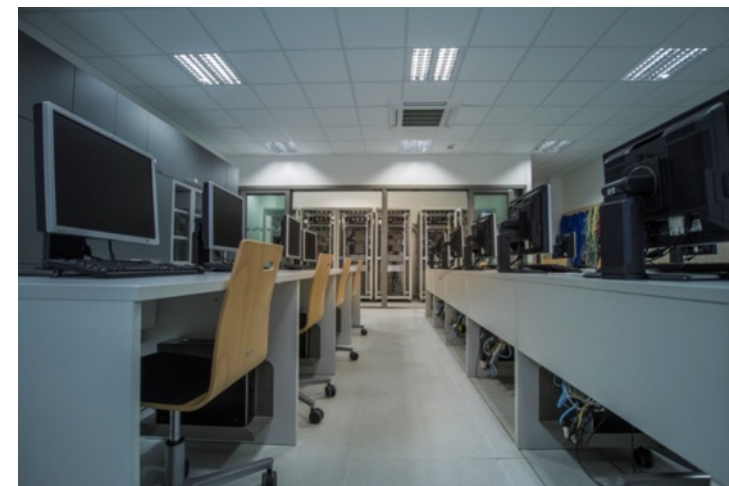
- Applied Cryptography & Security Engineering
- <https://www.utko.fekt.vut.cz/en>
- <https://axe.utko.feec.vutbr.cz>

- **R&D activities**

- (Post)Quantum Cryptography
- Industrial Networks
- Privacy-enhancing Technologies
- H2020, TAČR, GAČR, MVČR, MPO Projects

- **Services in ICT Security**

- Stress Testing, DDoS Testing





HW NETWORK TRAFFIC ENCRYPTOR

- **Postquantum Algorithms on FPGA**
 - Related to the NESPOQ project, part of solution: QKD + PQC
 - First implementations of NIST STANDARDS
 - CRYSTALS-Dilithium
 - CRYSTAL-KYBER
- Practical “down-to-earth” engineering, but first worldwide.
- Parts already done: PQC Signature, Quantum-Safe Cipher, PQC key-agreement.
- Final output: encryption device capable of quantum-safe key agreement and quantum-safe 100G+ high-speed encryption
- **Collaboration:** hardware protection, side-channel analysis, ...





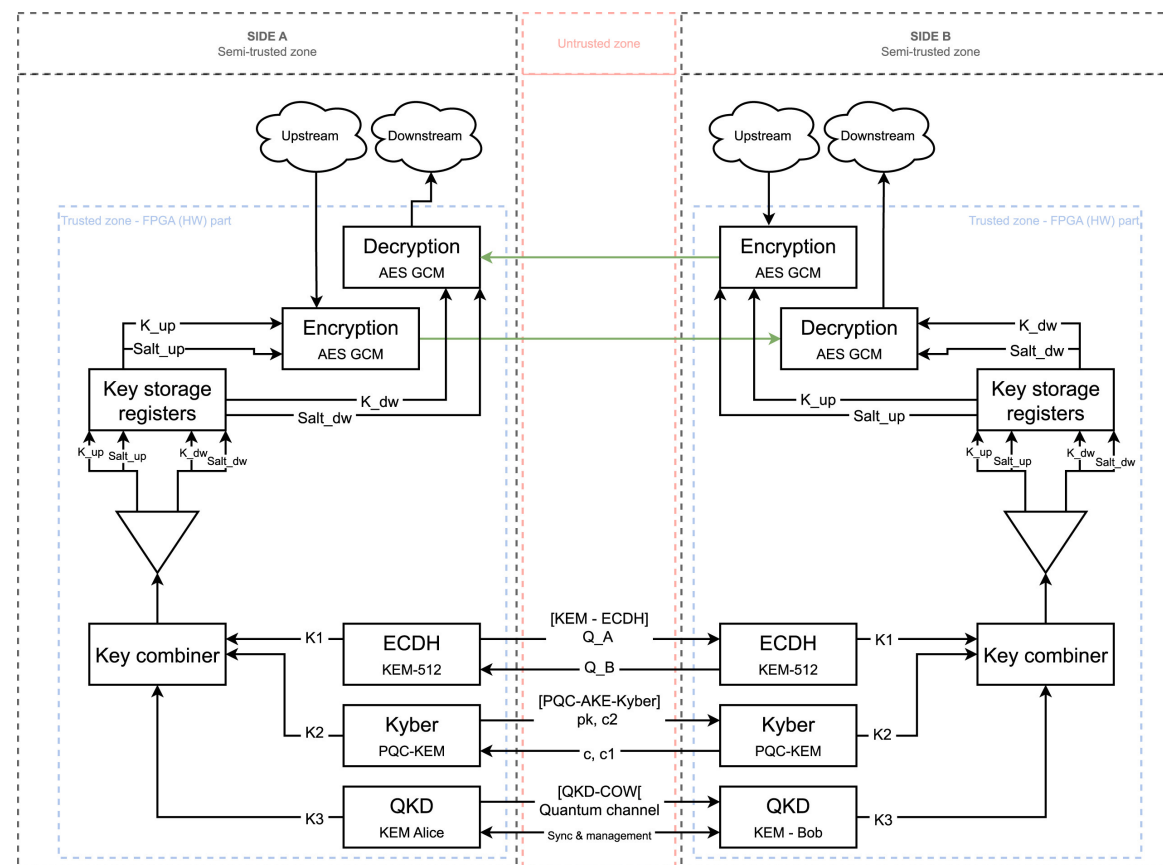
SW NETWORK TRAFFIC ENCRYPTOR

- **Postquantum Algorithms on Linux**

- C++ based project
- Using OpenSSL (3.0.14) and liboqs libraries
- Aims to offer flexibility and ease of deployment
- Suitable for devices with no hardware acceleration

- **Functionality**

- Uses AES-256-GCM for encryption
- Encryption key is derived from 3 separate keys
- Utilization of ECDH, CRYSTALS-Kyber (PQC), QKD
- Offers 2 work modes – with/without QKD
- Allows to use it without costly QKD infrastructure
- Periodical updates of encryption key





SW NETWORK TRAFFIC ENCRYPTOR

- **Testing and Deployment**

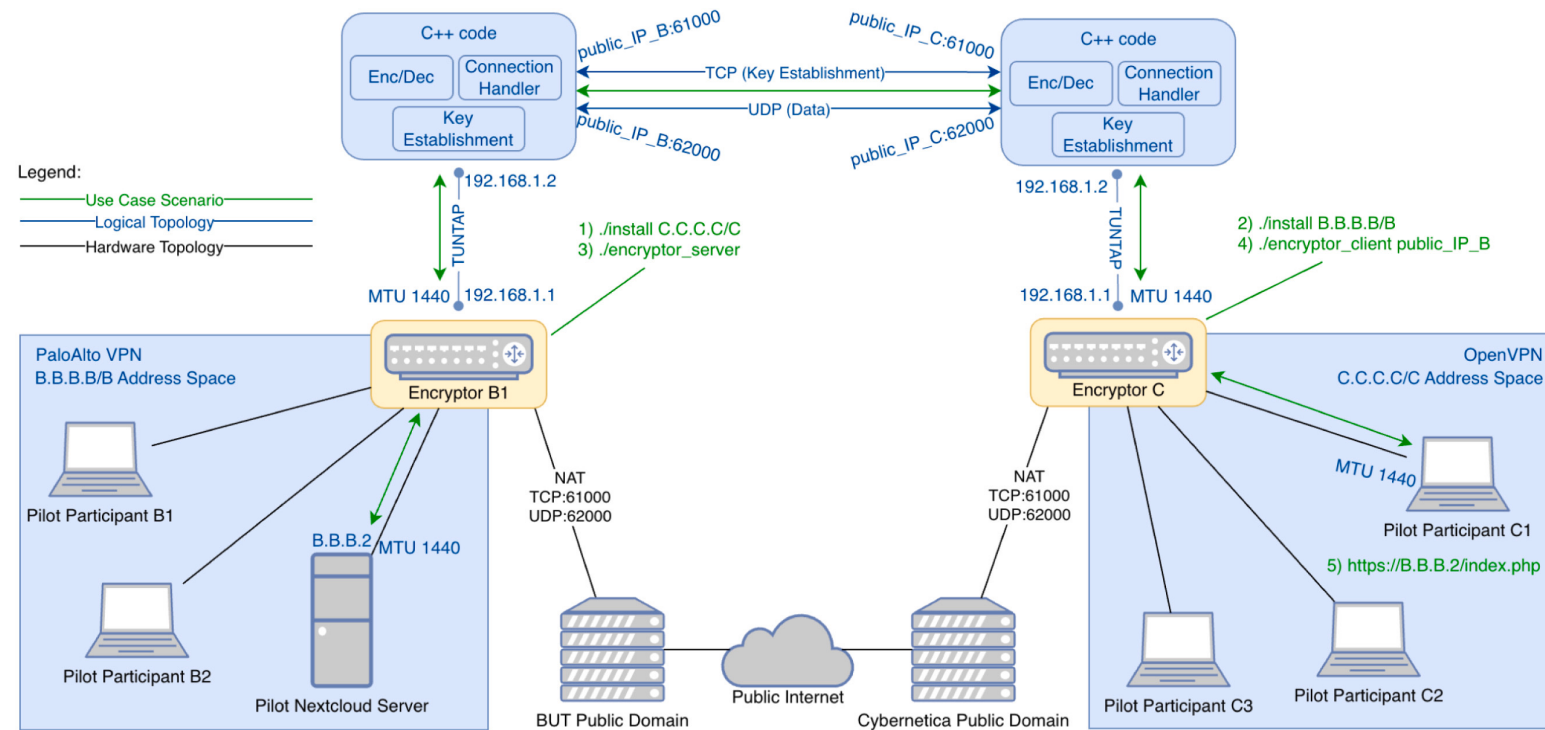
- Performance testing
- Virtual machines
- Low-end IoT devices

- **3 Priorities**

- Throughput
- Delay
- Rekeying and its influence on continuity of communication

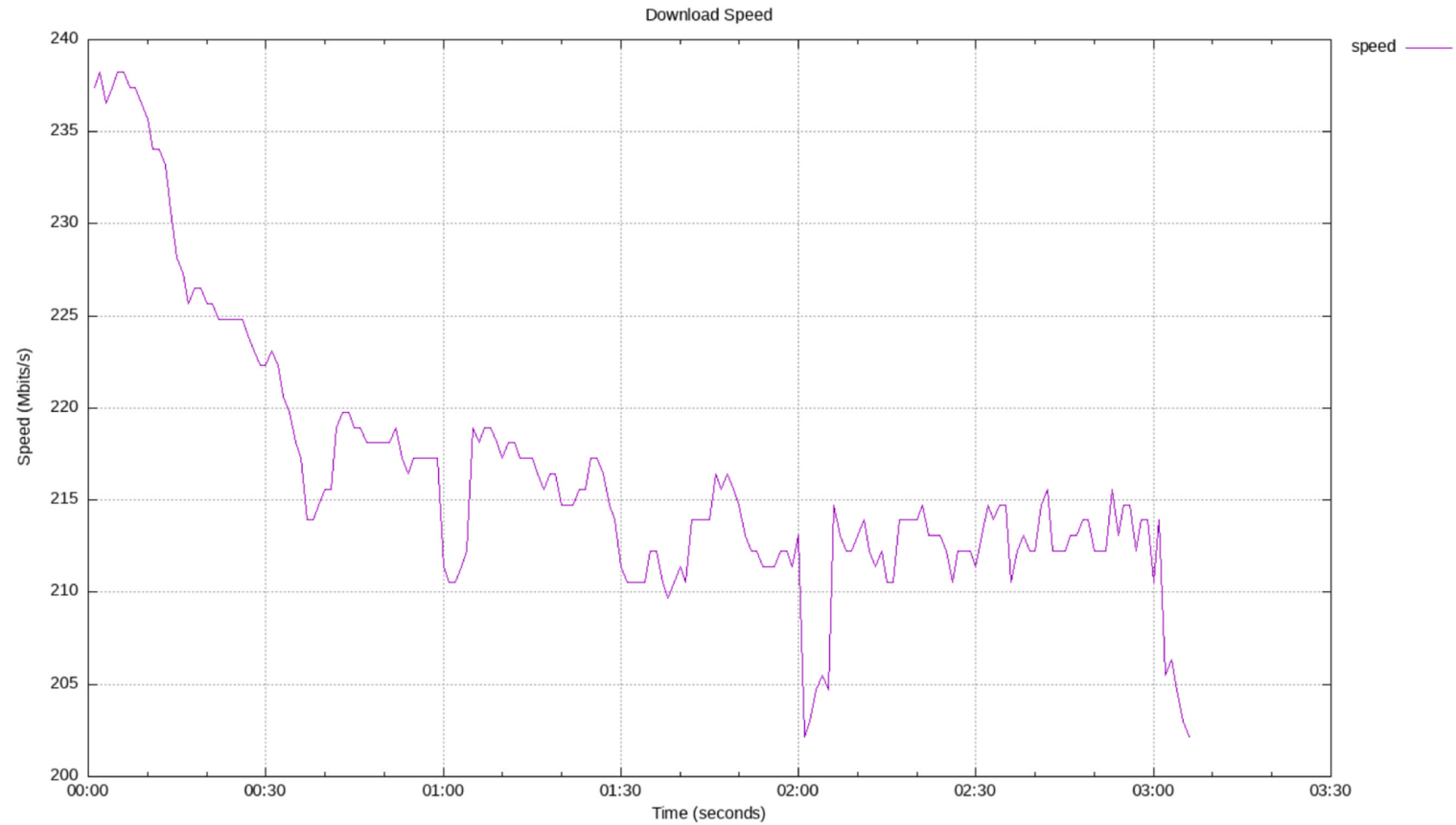
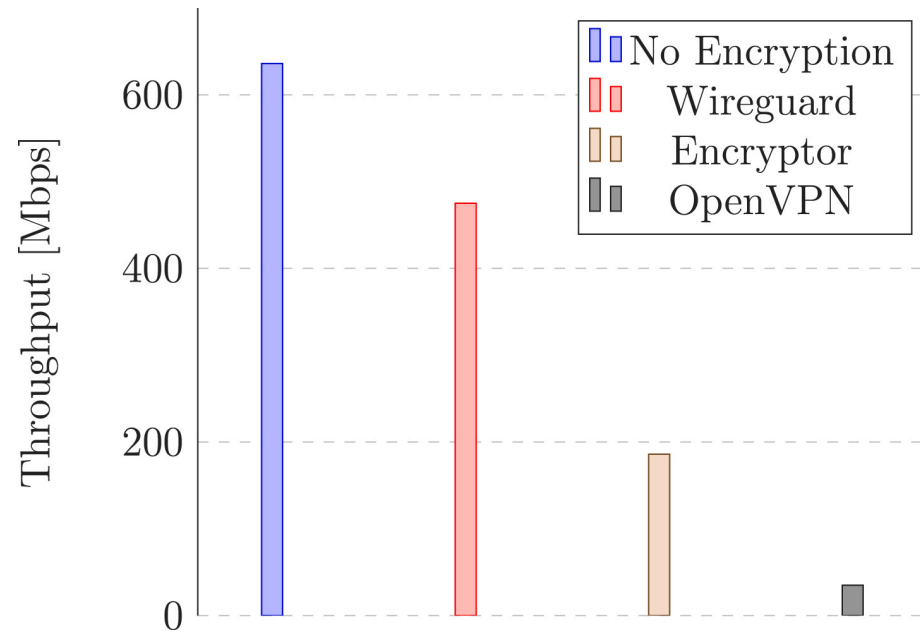
- **Czechia and Estonia pilot**

- In cooperation with Cybernetica AS
- First test in real-world scenario



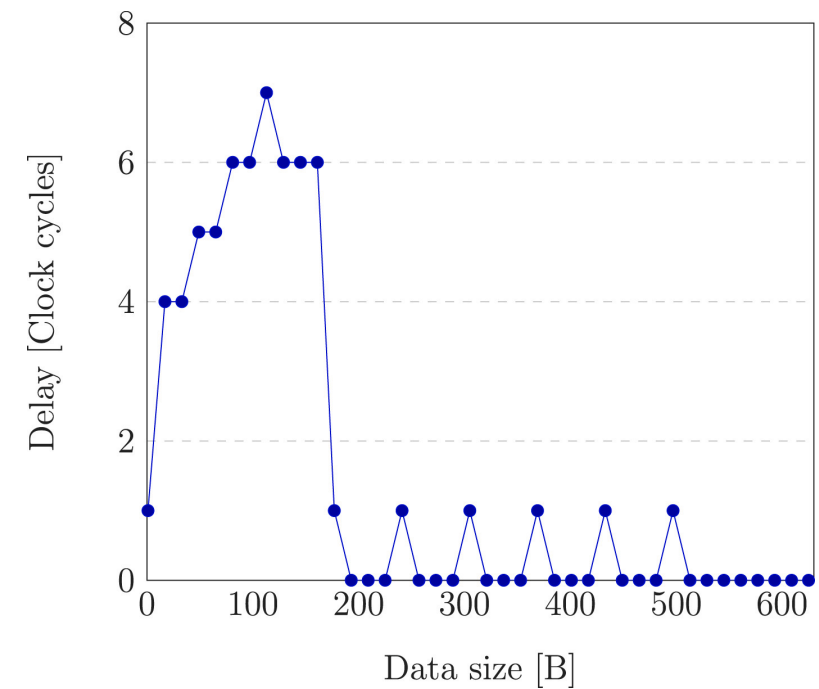
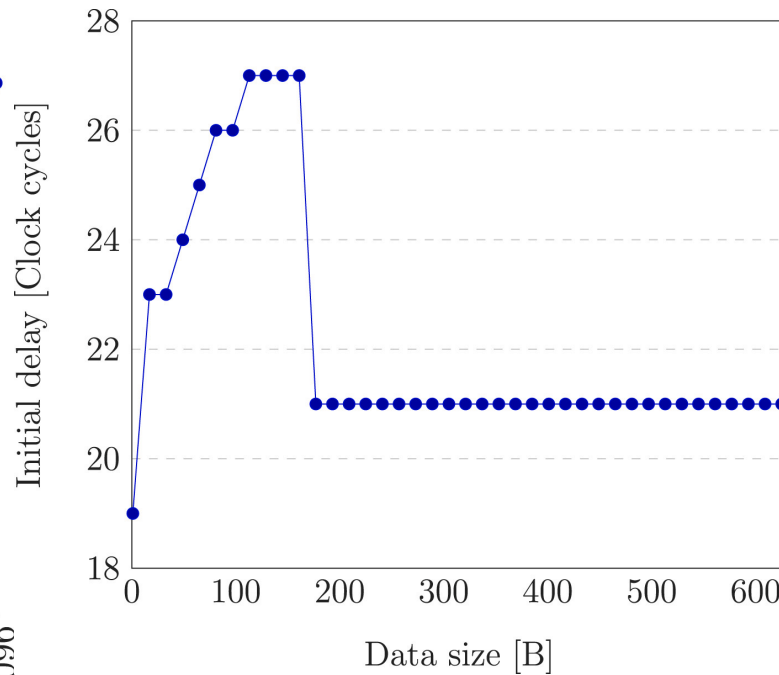
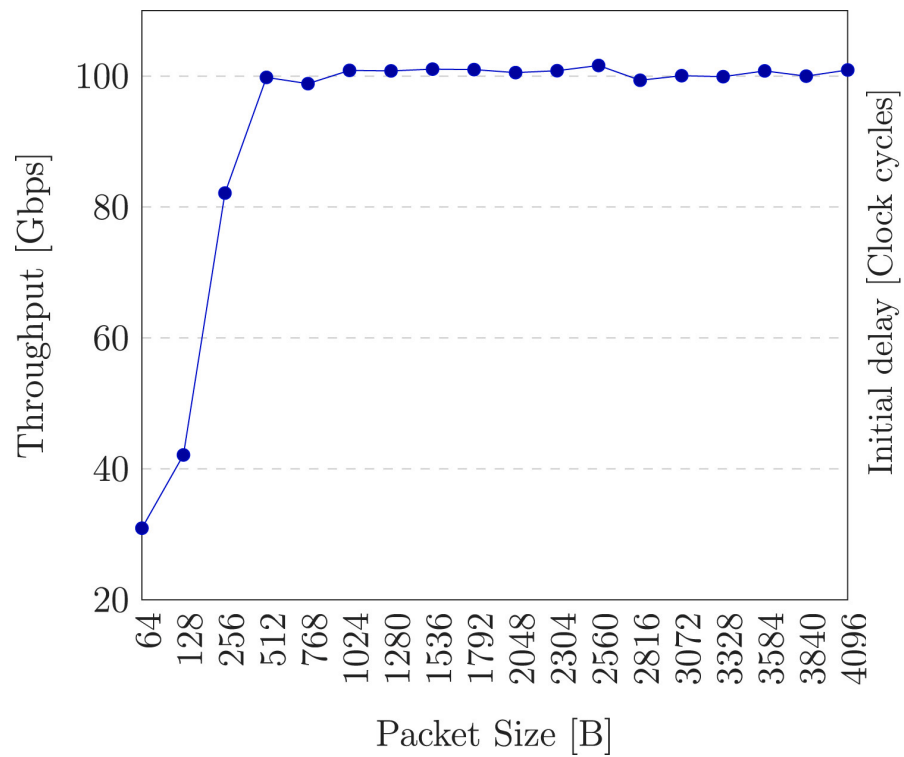


TEST RESULTS - SW





TEST RESULTS - HW





ABOUT LAB AND PROJECT NESPOQ

- **Title: Network Cybersecurity in Post-Quantum Era (NESPOQ)**
- Duration: 01/2021 - 12/2025
- Principal investigator: prof. Ing. Jan Hajný, Ph.D. (BUT, hajny@vut.cz)
- Application Guarantee: NÚKIB
- Funding: The Ministry of the Interior of the Czech Republic
- Planned results: (Post-)Quantum Encryptors, Pilot Deployment, Recommendations for Deployment, Scientific Publications



MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

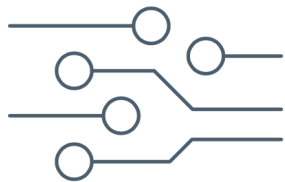
N Ú K I B





ABOUT LAB AND PROJECT QARC

- **Title: Quantum Resistant Cryptography in Practice (QARC)**
- Duration: 01/2026 - 12/2028
- Principal investigator: prof. Ing. Jan Hajný, Ph.D. (BUT, hajny@vut.cz)
- Partners: 18 EU institutions (industry, academia, national authorities)
- Funding: Horizon Europe
- Planned results: Post-quantum Encryptors, Pilots, National Strategies, Roadmaps, Scientific Publications



JOINT POST-QUANTUM INITIATIVE



Funded by
the European Union



Thank you for your attention.

