Quantum-Safe Encryptor

CHESS CA5 Activities

Lukas Malina

Brno University of Technology
malina@vut.cz
https://axe.vut.cz

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Brno AXE Applied Cryptography & Security Engineering

CHESS

Funded by the European Union

AXE Group at Brno University of Technology

Applied Cryptography and Security Engineering (AXE):

- based in Brno, Czech Republic,
- focused on PQC, PETs, Lightweight Crypto, SCA,
- delivering implementations for specific platforms: FPGA, smart-cards, constrained devices.

Solutions to Quantum Threat

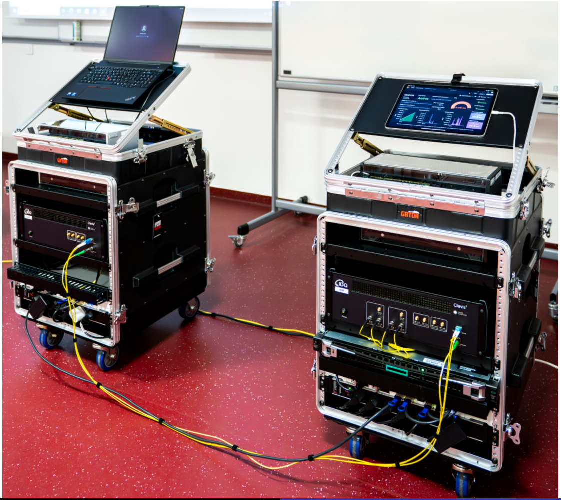
Post-Quantum Cryptography

- *easy* integration with existing ICT, no special HW, cheap,
- existing SW implementations: OpenSSL 3.5, Open Quantum Safe,
- supported by national authorities: UK, US, Germany, France, Sweden, Netherlands, . . . ,
- FIPS standardization: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON (lattice-based) and SPHINCS+ (hash-based)

QKD - Quantum Key Distribution - only key establishment.
Hybrid Solutions - combining PQC, classical cryptography, QKD.

FPGA Quantum-Safe Encryptor I

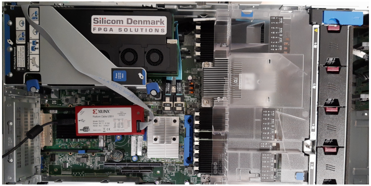
- Demonstrator of FPGA Quantum-Safe Encryptor.



FPGA Quantum-Safe Encryptor II

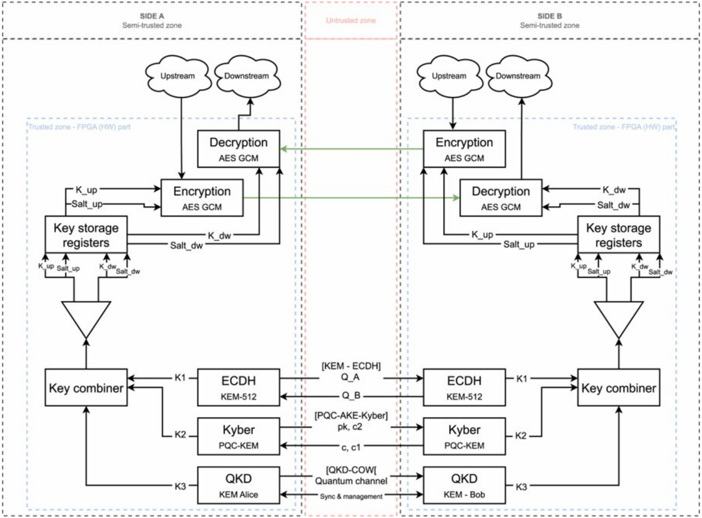
FPGA Quantum-Safe Encryptor

- aim: hardware-accelerate high-speed encryptor for 100 GbE networks using standard TCP/IP protocols,
- hybrid KEM, keys from classical (ECDH), PQC (ML-KEM) and QKD (optional).
- implemented on programmable network interfaces with FPGA,
- supported by the Ministry of Interior (CZ), project NESPOQ #VJ01010008[1], and tested/piloted by CHESS.



[1] https://www.nespoq.cz

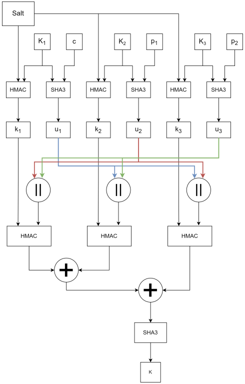
FPGA Quantum-Safe Encryptor III

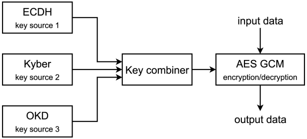


FPGA Quantum-Safe Encryptor IV

Cryptography components:

- Classical cryptography: ECDH-512,
- Quantum Key Distribution: IDQ Clavis 3,
- Post-Quantum: CRYSTALS-Kyber 768,
- Payload Encryption: AES-256-GCM,
- Key Combiner: own[2].

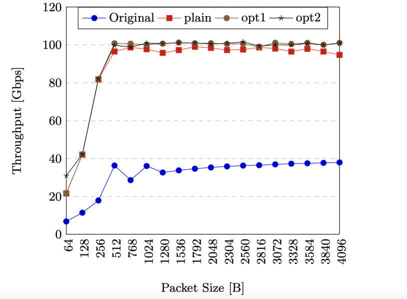


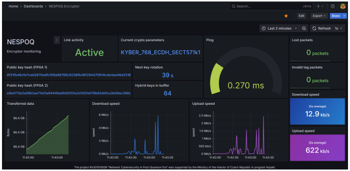

ECDH
key source 1
Kyber
key source 2
OKD
key source 3
Key combiner
input data
AES GCM
encryption/decryption
output data

[2] S. Ricci et Al, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 12, 2024.

FPGA Quantum-Safe Encryptor V

- Throughput: 117,3 Gbps[3], high parallelism (for AES-GCM).
- Generating 1624 hybrid keys per second (without QKD).
- Monitoring via Grafana GUI.





NESPOQ

Encryptor monitoring

Link activity: Active

Current crypto parameters: KYBER_768_ECDH_SECT571k1

Ping: 0.270 ms

Lost packets: 0 packets

Public key hash (FPGA 1): 8f31fb46cfa7ceb5870edfcf09a98768c9238fb46f294470914cde4aa46d2516

Next key rotation: 39 s

Invalid tag packets: 0 packets

Public key hash (FPGA 2): e9a0713e2a09b2ae71e12a94446ad0d5555a2d1d51e078b83dd1ca3b08ac388c

Hybrid keys in buffer: 64

Transferred data

Download speed

Upload speed

Download speed (5s average) 12.9 kb/s

Upload speed (5s average) 622 kb/s

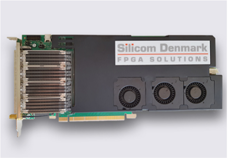
The project #VJ01010008 "Network Cybersecurity in Post-Quantum Era" was supported by the Ministry of the Interior of Czech Republic in program Impakt.

[3] Cibik et al. Quantum-resistant hardware-accelerated IoT traffic encryptor, Internet of Things, 2025.

FPGA Quantum-Safe Encryptor VI

Optimization and Costs:

- originally designed for **Xilinx UltraScale+** FPGA chips,
- implemented and tested on **Silicom Denmark Mango** cards (approx. 10K EUR),
- and adapted for **Intel Agilex** (approx. 4K EUR),
- implemented and tested on **Intel N6010** (approx. 3K EUR),
- since 2025: **IP Cores commercially available**,
- currently: SCA resistance using masking techniques.



Conclusion

- First hybrid encryptor (PQC ML-KEM, ECDH, QKD).
- Extreme performance: up to **100 Gbps**.
- Protected against side channel attacks.
- Piloted between Czechia and Estonia: BUT and CYBERNETICA.
- Supported by CHESS CA5.

Thank you for your attention.

Video: https://www.youtube.com/watch?v=an5DwtZ1BjQ

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Brno AXE Applied Cryptography & Security Engineering

CHESS

Funded by the European Union

Research work is funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.