Hybrid Cryptography

Combining Classical, Quantum and Post-Quantum Mechanisms

Jan Hajný

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

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.

Quantum Computing

IBM:

- 2023: IBM Eagle: 127 qubits,
- 2024: IBM Heron: 133 (399) qubits, error mitigation,
- 2025: IBM Flamingo: 156 (1092) qubits, error mitigation.

Google:

- 2019: Sycamore: 53 qubits,
- 2024: $5 mil. prize for actual use.

Anhui Research Center (China):

- 2024: Origin Wukong: 72 qubits,
- was available online (to all).

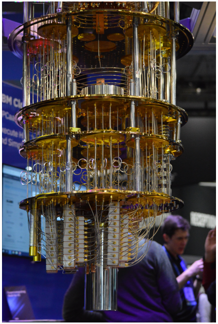


Figure: IBM Quantum Computer.

Quantum Computing - Security Threat I

Schor's Algorithm

- quantum algorithm developed in 1994,
- can be used for fast factorization, i.e. finding p, q for input $n = pq$, and for computing discrete logs,
- runs in polynomial time, i.e. $\log(n)$.

Grover's Algorithm

- quantum algorithm developed in 1996,
- can be used for fast unstructured search, i.e. finding input to blackbox function that produce certain output,
- runs with low complexity of $\sqrt{(}n)$, where n is the size of the function domain.

Quantum Computing - Security Threat II

Asymmetric Cryptography

- Key Agreement Protocols: (EC)**DH** based on discrete logarithm hardness *assumption*,
- Digital Signatures: RSA, (EC)**DSA** based on factoring, discrete logarithm hardness *assumption*,
- Encryption: **ElGamal** based on discrete logarithm hardness *assumption*.

Symmetric Cryptography

- block ciphers based on search complexity.

Advanced Cryptography

- Σ-protocols for ZK proofs: based on discrete logarithm hardness *assumption*,
- ...

Legislation, Recommendations

"As a consequence of quantum vulnerabilities of approved algorithms, it is necessary to replace them with a suitable quantum-resistant cryptography in the not too distant future." NÚKIB

National Authorities

- NUKIB (Czechia): Minimum Requirements for Cryptographic Algorithms
- NSA (US): Commercial National Security Algorithm Suite 2.0
- BSI (Germany): Quantum-safe cryptography – fundamentals, current developments and recommendations
- ANSSI (France): ANSSI views on the PQC transition
- NCSC (UK): Next steps in preparing for PQC

Standardization Bodies

- NIST: Post-Quantum Cryptography Standardization

Solutions: QKD

Quantum Cryptography: Quantum Key Distribution

- known since 1980s, based on quantum physics,
- no hardness assumptions, unconditionally secure (in theory),
- existing solutions: Toshiba, ID Quantique, . . . ,
- massively supported by EU: EuroQCI, CZ-QCI, ...

Problems: expensive (ca. $200K for a link), questionable implementation security, solves only key distribution (expansion), not recommended by security agencies as complete solution[1], difficult integration with existing ICT, only minor standardization

. . .

[1] Position Paper on Quantum Key Distribution

Solutions: PQC

Post-Quantum Cryptography

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

Problems: still based on (QC-safe) hardness assumptions, more complex.

Solutions: Hybrid Cryptography and Agility

Hybrid Cryptography

- combines different approaches: QKD, PQC, Classical cryptography,
- secure if some approach fails,
- recommended by some authorities: BSI, ANSSI, . . . , but not NSA,
- valid at least for the transition period,
- relevant also for combining multiple PQC families.

Cryptographic Agility

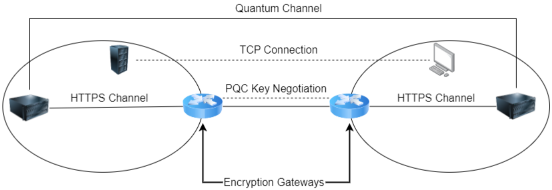
- design that allows simple and quick algorithm replacement.

Problems: slower, larger, easier for KEM, harder for signatures, more space for mistakes.

Experiments: Open-Source Quantum-Safe Encryptor I

CHESS Project Activity: Quantum-Safe Encryptor

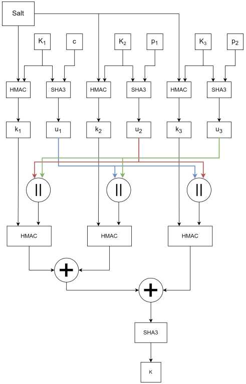
- aim: verify long-distance deployment of a quantum-safe channel,
- based on combination of classical, QKD and PQC,
- deployed between Czechia (Brno - Brno University of Technology) and Estonia (Tartu - Cybernetica),
- based on Linux, publicly available at: https://github.com/gabsssq/Linux-network-traffic-encryptor



Experiments: Open-Source Quantum-Safe Encryptor II

CHESS Project Activity: Quantum-Safe Encryptor

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

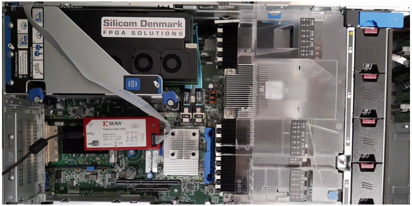


[2]S. Ricci et Al, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 12, 2024.

Experiments: FPGA Quantum-Safe Encryptor I

NESPOQ Project Activity: FPGA Quantum-Safe Encryptor

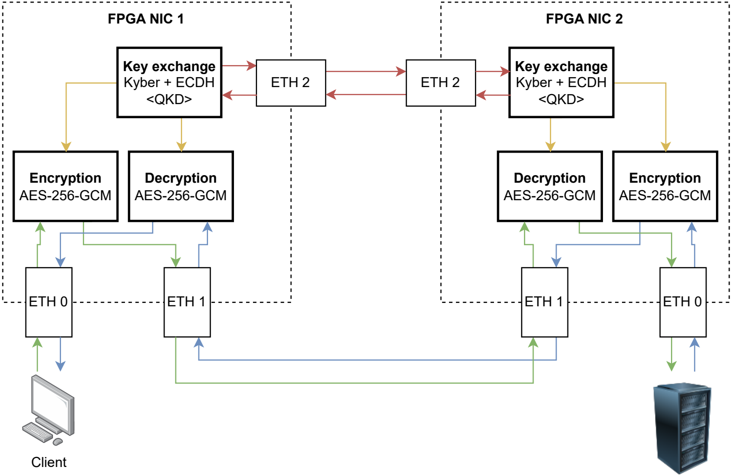
- aim: hardware-accelerate high-speed encryptor for 100 GbE networks using standard TCP/IP protocols,
- based on combination of classical, QKD and PQC - similar to software-based encryptor,
- supported by the Ministry of Interior of Czech Republic, project NESPOQ #VJ01010008 [3],
- implemented on NIC as firmware,
- available also as IP cores.



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

Experiments: FPGA Quantum-Safe Encryptor II

NESPOQ Project Activity: FPGA Quantum-Safe Encryptor

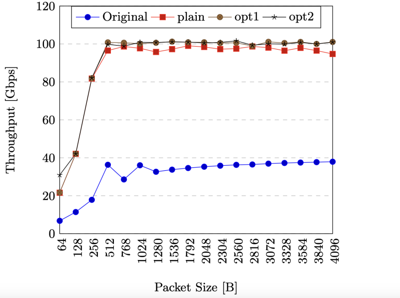


Experiments: FPGA Quantum-Safe Encryptor III

NESPOQ Project Activity: FPGA Quantum-Safe Encryptor

Challenges:

- limmited resources: LUTs, Flip Flops, 200 MHz frequency.
- high throughput: 100 Gbps.
- no existing implementations on FPGAs in VHDL language.
- high parallelism (for AES-GCM).

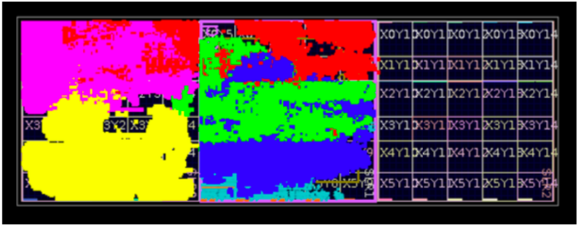


Experiments: FPGA Quantum-Safe Encryptor IV

NESPOQ Project Activity: FPGA Quantum-Safe Encryptor

Components placement after the implementation phase (two out of the three SLRs used):

- yellow - Encryption subcore
- pink - Decryption subcore
- green - Key Exchange
- red - ETH; blue - PCI-E



Conclusions and Provocative Questions

Simple Conclusions:

- Transition to quantum-safe is a must (due to *store and decrypt later* attacks).
- PQC is closer to practical deployment than QKD.
- Concrete algorithms depend on standards and authority recommendations: coming 2024/2025.
- Integration with existing infrastructure is a bigger issue than cryptographic algorithms.
- Agility and hybrid approach is highly advisable.

Provocative questions:

- Will *ever* be quantum computer constructed?
- Are current QCs even close to some *practical use* in cryptography? (noise, stablity, number of logical qubits...)
- Are lattice-based algorithms, i.e. CRYSTALS, *secure*[4]?

[4] Yilei Chen, *Quantum Algorithms for Lattice Problems*, https://eprint.iacr.org/2024/555

Thank you for your attention.

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.