BRNO UNIVERSITY OF TECHNOLOGY

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

CHESS Brokerage Event at JIC

Post-Quantum Hardware Encryptors

Jan Hajný

CHESS

https://chess-eu.cs.ut.ee

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.

Post-Quantum Hardware Encryptors

- **Motivation**
  - **NIST PQC standards** released in 2024
  - **EU and US authorities** recommend post-quantum transition (and support it by many calls)
  - **NÚKIB recommends** post-quantum transition, part of mandatory requirements.

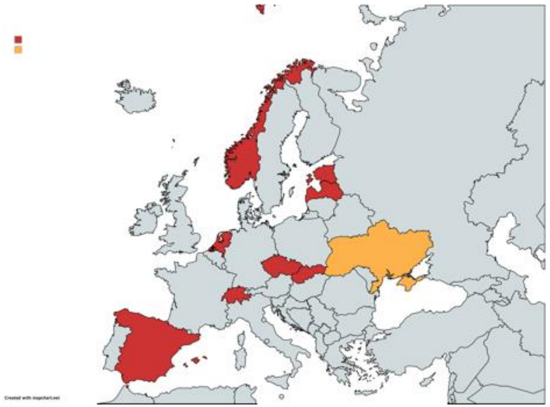
- **Solution**
  - High-speed network **cards based on FPGA** with accelerated encryption and key management, all PQC.
  - Based on **proven primitives** (CRYSTALS-Kyber, AES)
  - Advanced features, such as Quantum Key Distribution (**QKD**)
  - Developed and tested in **BUT Quantum Security Lab**.
  - Available for **purchase** (or distribution) as **IP Cores**.
  - **Functional samples** based on Intel (Altera) and Silicom Denmark available.
  - Free **open-source software** variants available.

Post-Quantum Hardware Encryptors

- **Collaboration Opportunities**
  - Joint research projects (Horizon Europe, MVČR, …)
  - Direct contractual research
  - Technology transfer, licensing
- **Other Relevant Activities**
  - Cryptographic protocol design
  - Implementation on specific platforms
    - FPGAs, constrained devices
  - Verification of secure implementations, testing

European Commission

Horizon Europe
2021-2027



Thank you for your attention!

hajny@vut.cz