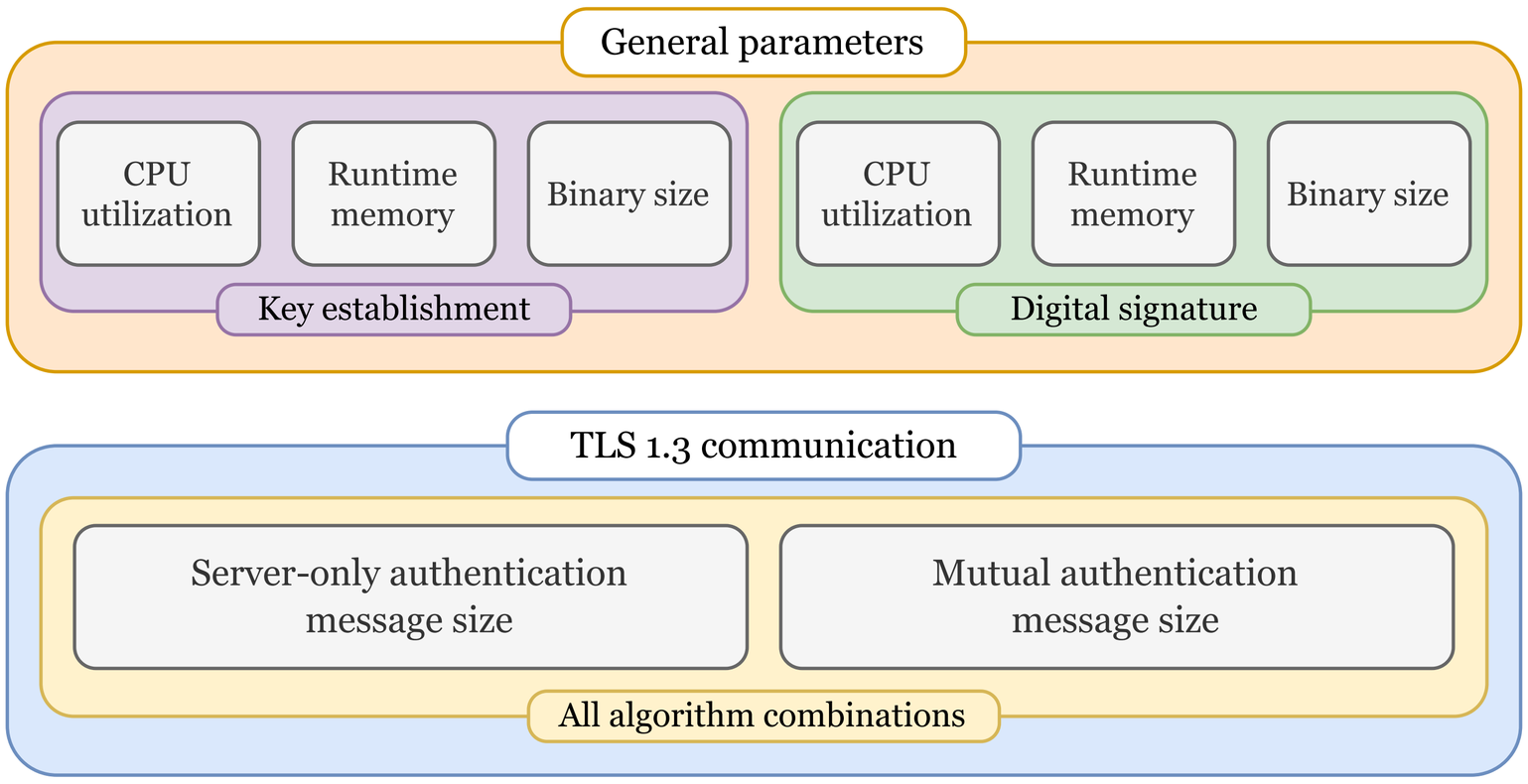
BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024

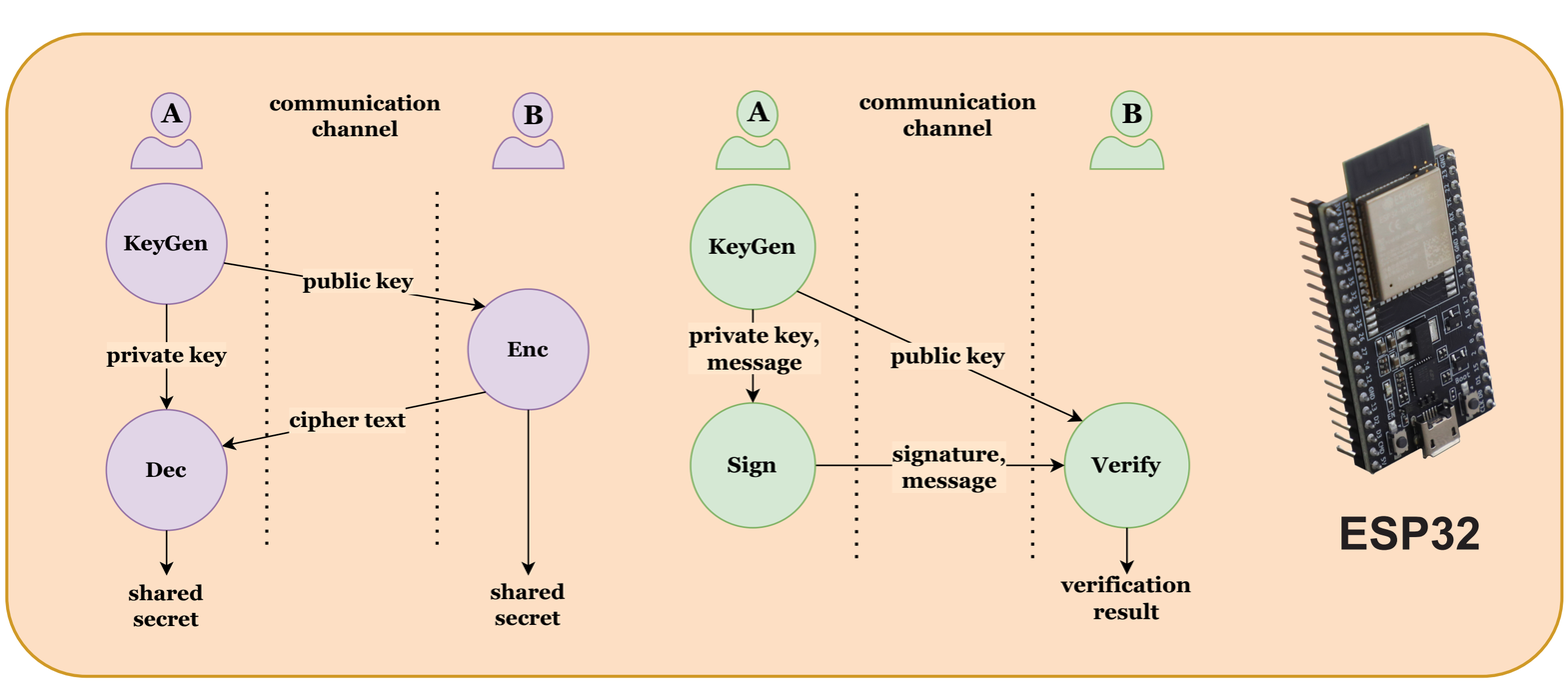
Usability of post-quantum cryptography in IoT

Autor: Jakub Kratochvíl
Vedoucí: Mgr. Kamil Malinka Ph.D.
Rok: 2024

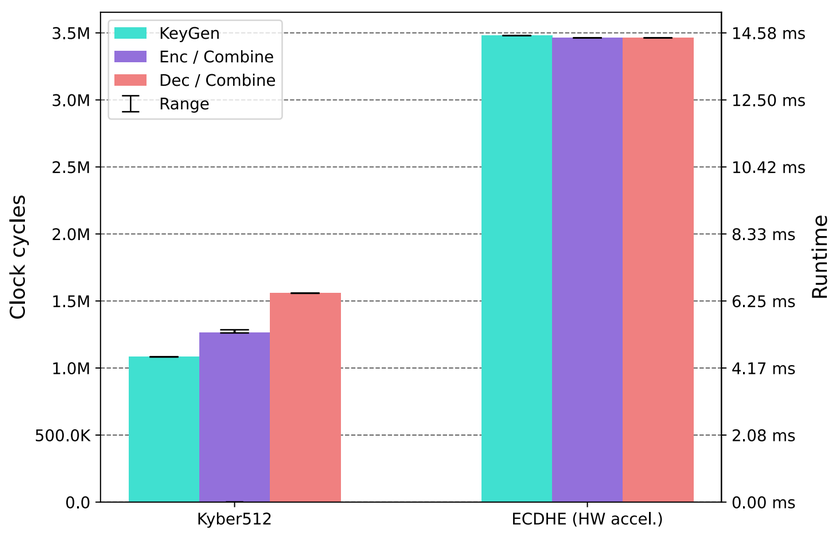
Overview of the measurements

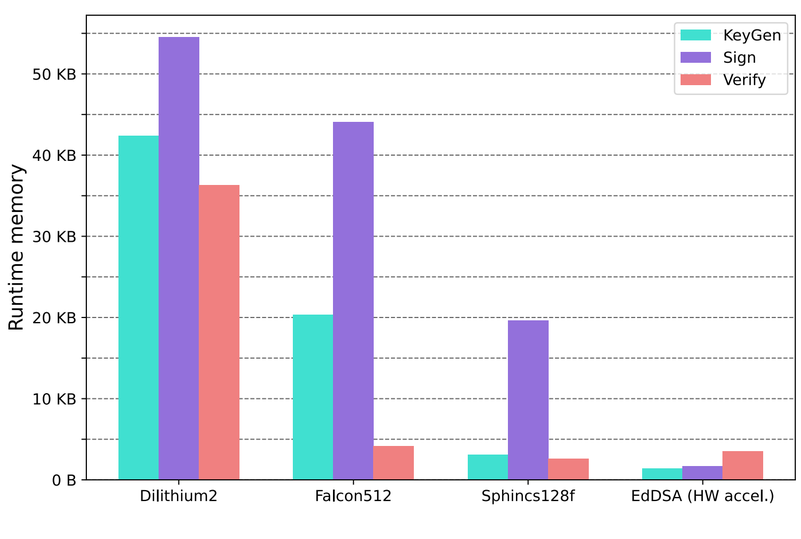


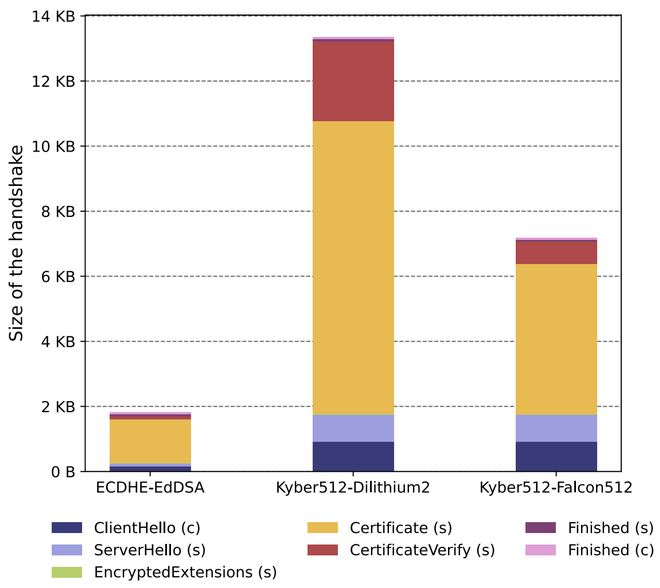
General measurements

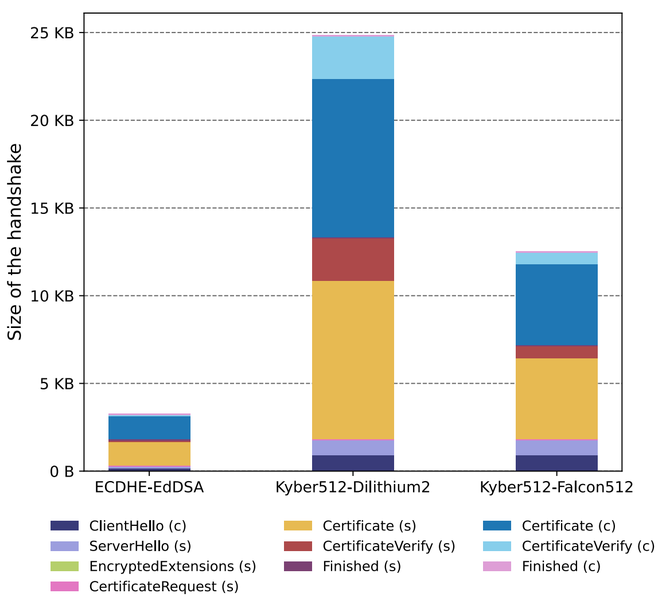


Sample of the results









Introduction

- In 20 years, there is high possibility that quantum computers are powerful enough to break current public-key cryptography
- With post-quantum cryptography in standardization process, it is important to test it, especially on resource constrained devices
- This thesis proposes a measurements for evaluating post-quantum algorithms, divided into two parts, general and real-world

Measured post-quantum algorithms

Kyber
Lattice-based
NIST level 1

SPHINCS+
Hash-based
NIST level 1

Falcon
Lattice-based
NIST level 1

Dilithium
Lattice-based
NIST level 2

PQ TLS 1.3 communication size