University of Applied Sciences and Arts Northwestern Switzerland
School of Engineering

First Demonstration of a Post-Quantum Key-Exchange with a Nanosatellite

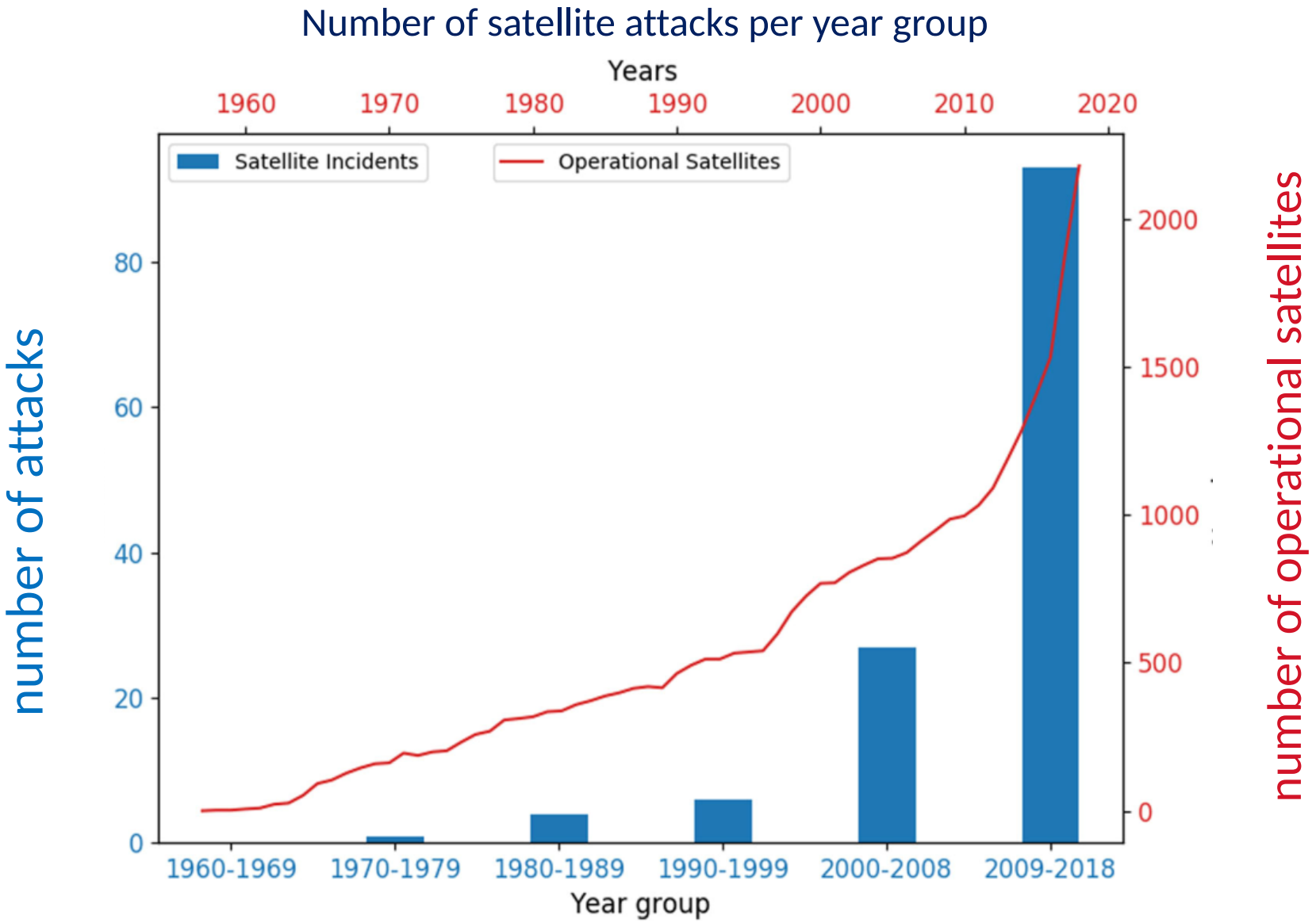
FHNW University of Applied Sciences and Arts Northwestern Switzerland

2022-08-12

Simon Burkhardt, Willi Meier, Christoph Wildfeuer

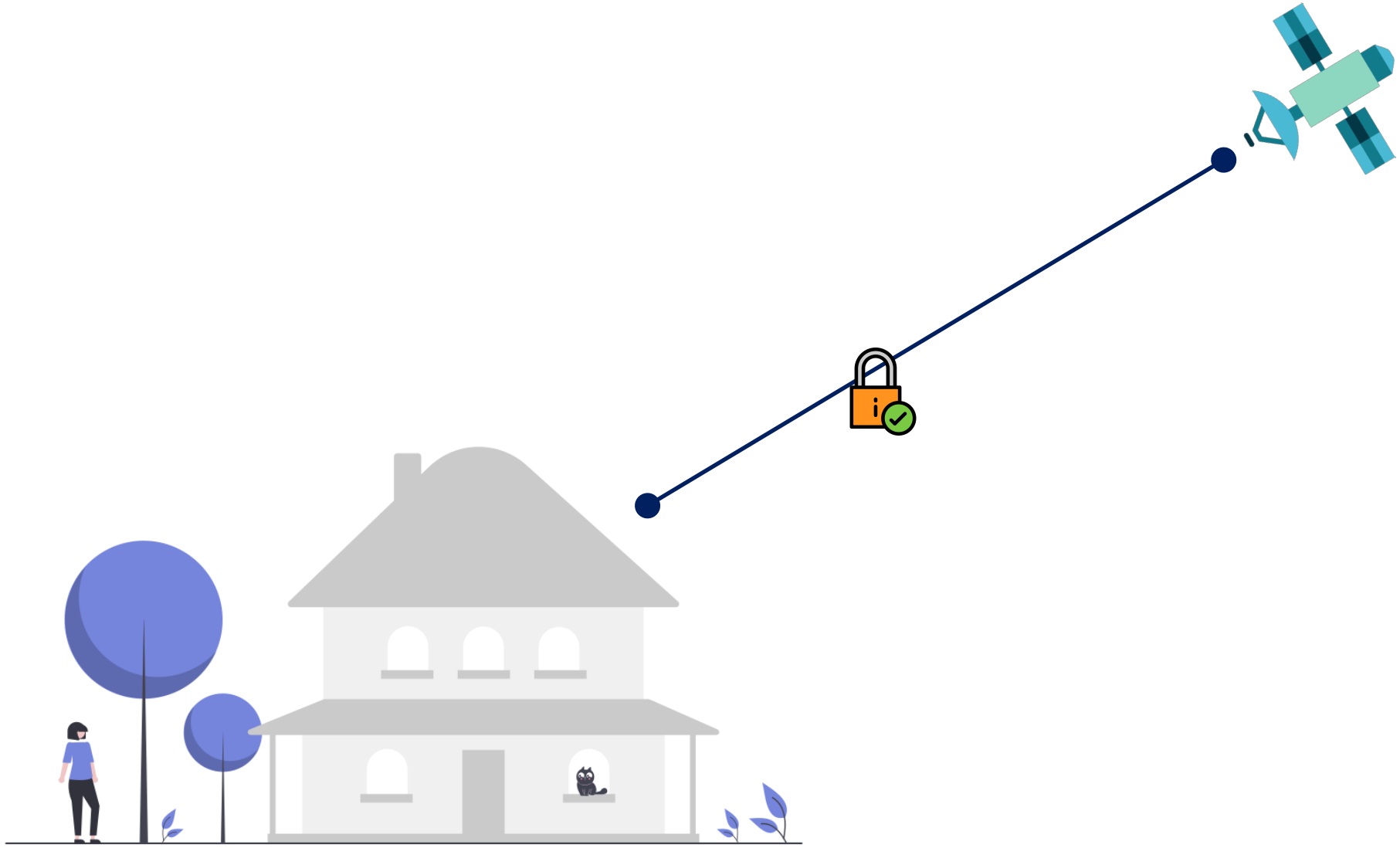
[SSC22-XII-04]
arxiv.org/abs/2206.00978

Cyber attacks on satellites

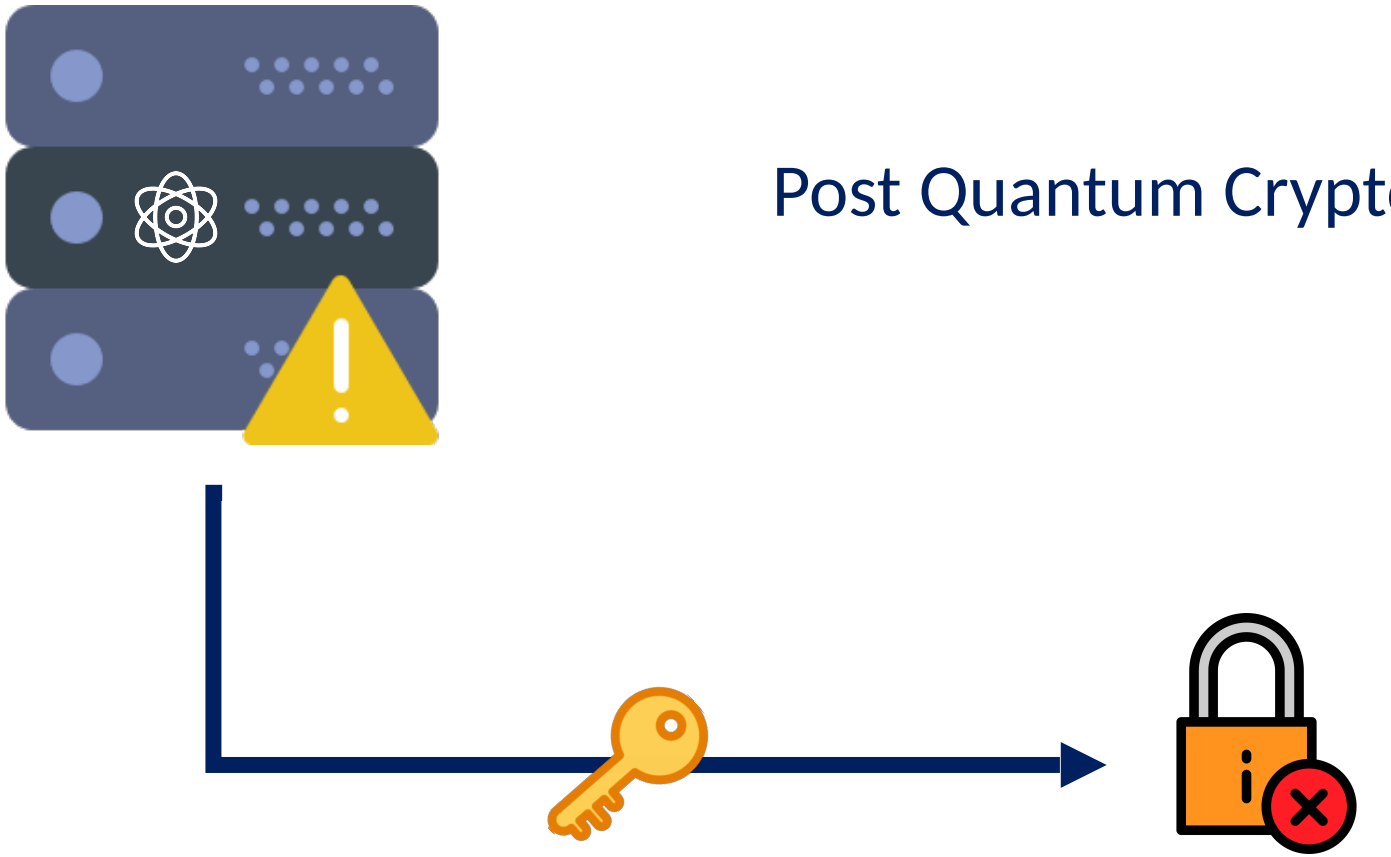


Manulis et. al. “Cyber security in New Space” (2021)

Classical Encryption

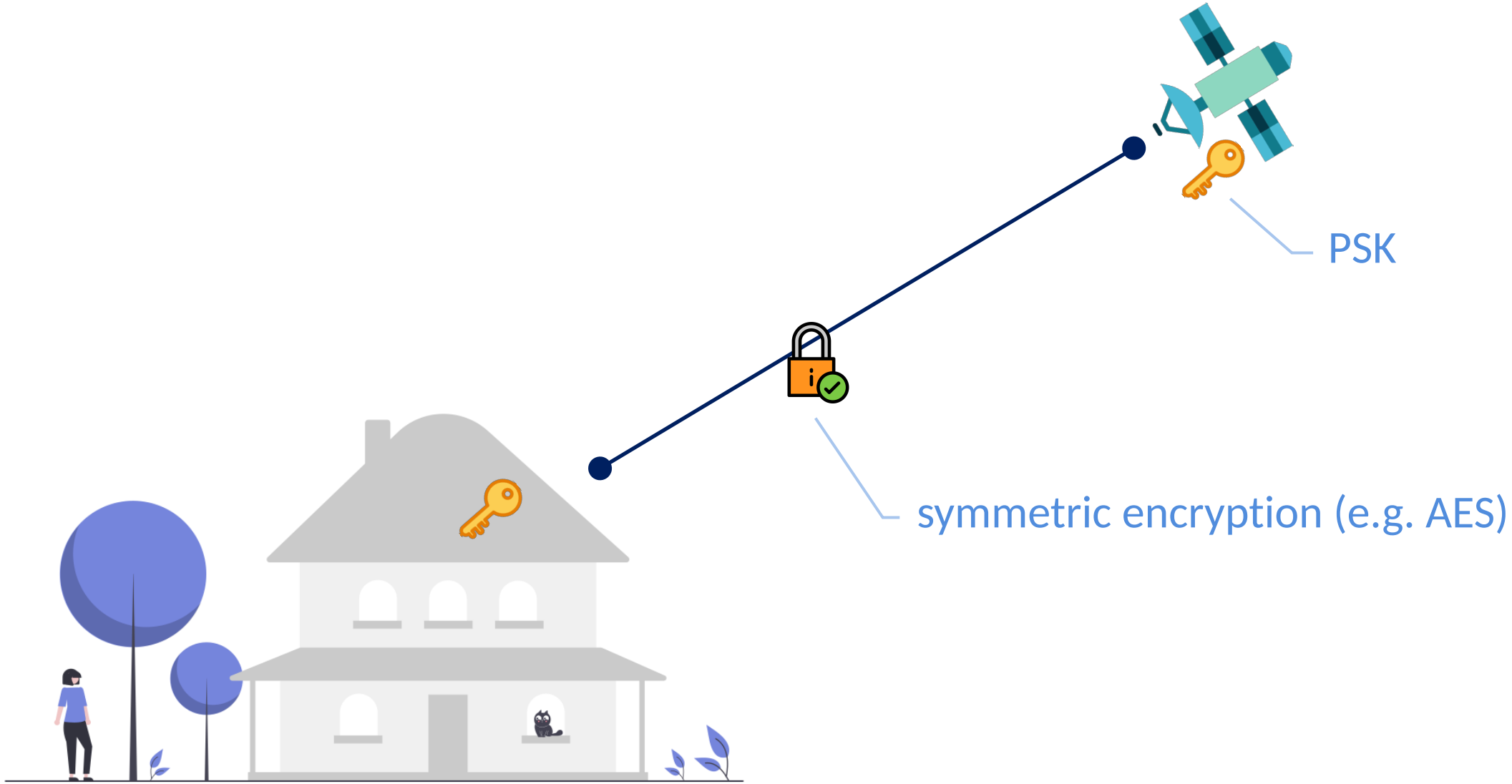


Quantum computers break classical encryption

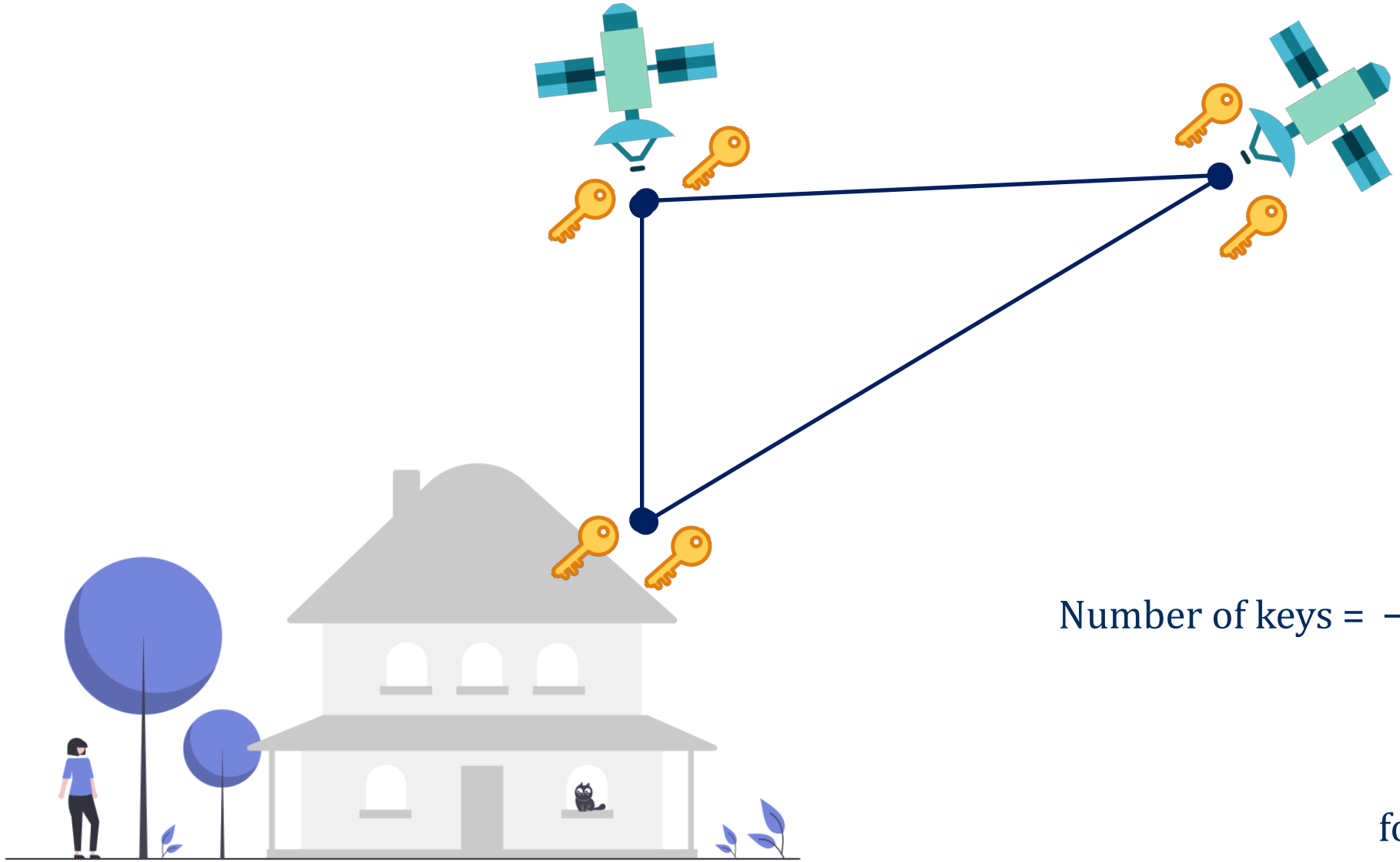


Post Quantum Cryptography

Encryption using a Pre-shared Secret (PSK)



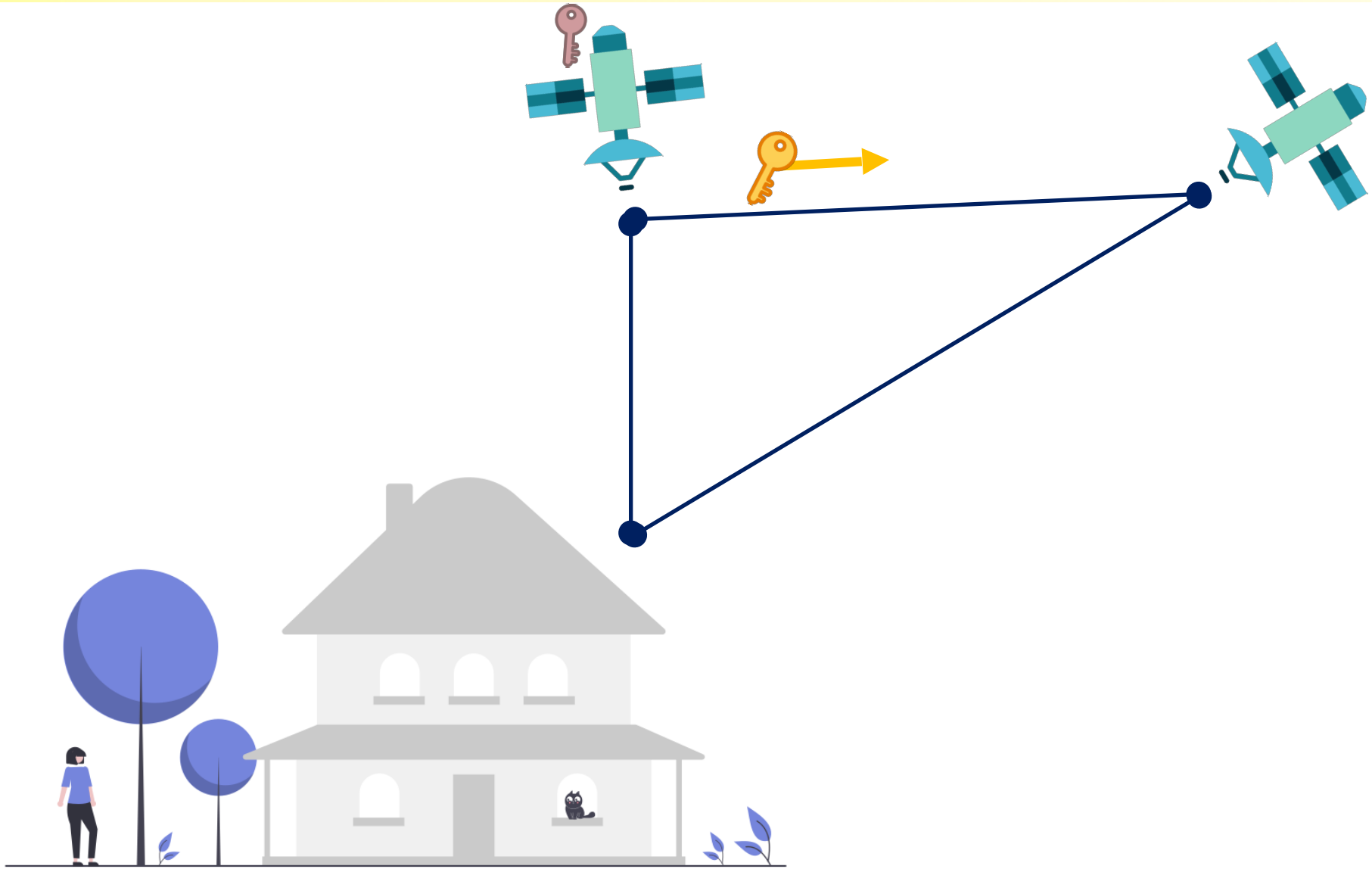
PSK is unpractical with growing number of satellites



$$\text{Number of keys} = \frac{n(n-1)}{2}$$

for n satellites

Public Key Exchange (KEX)



Post Quantum Cryptography

National Institute of Standards and Technology

- 6 year competition by NIST to find new PQC encryption algorithms

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Kyber key encapsulation mechanism (KEM)

- IND-CCA2-secure KEM
- Recommended for general use
  at NIST PQC competition on July 5th 2022
- Well tested on x86

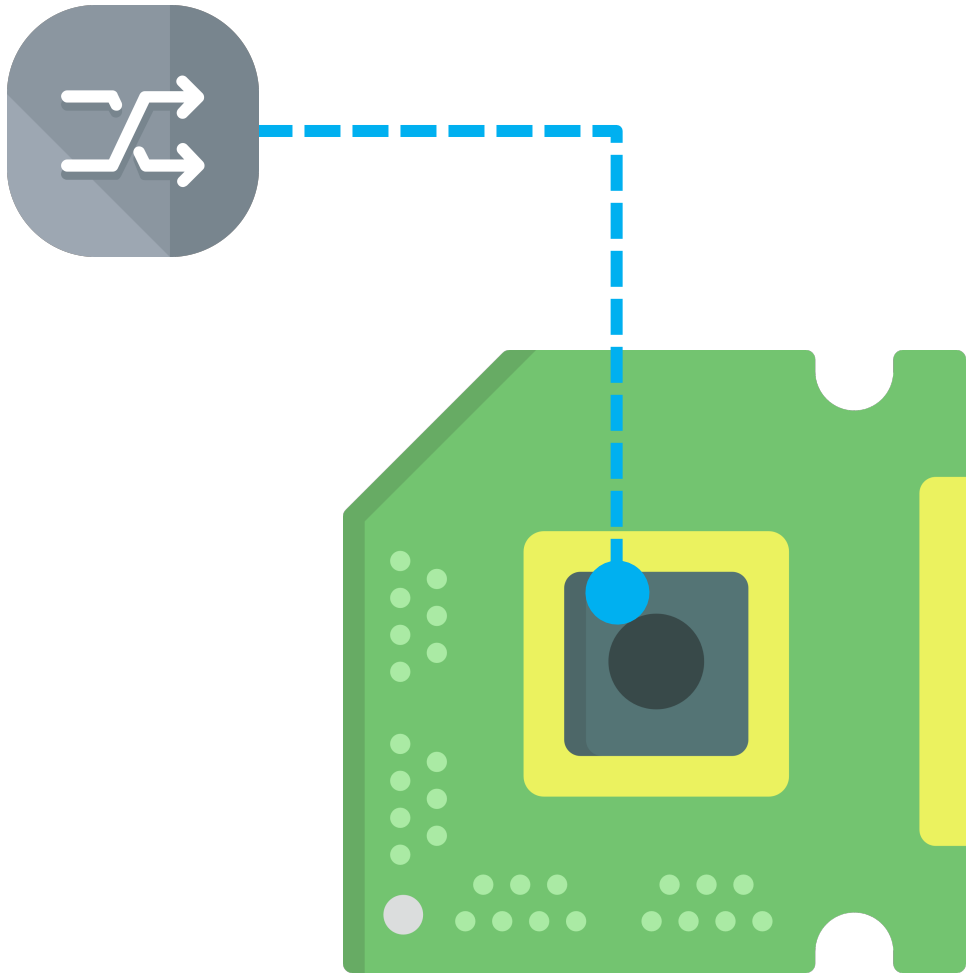
SpooQy-1 nano satellite

- Embedded System
- AVR32 microcontroller @ 64 MHz
- FreeRTOS
- CubeSat Space Protocol CSP

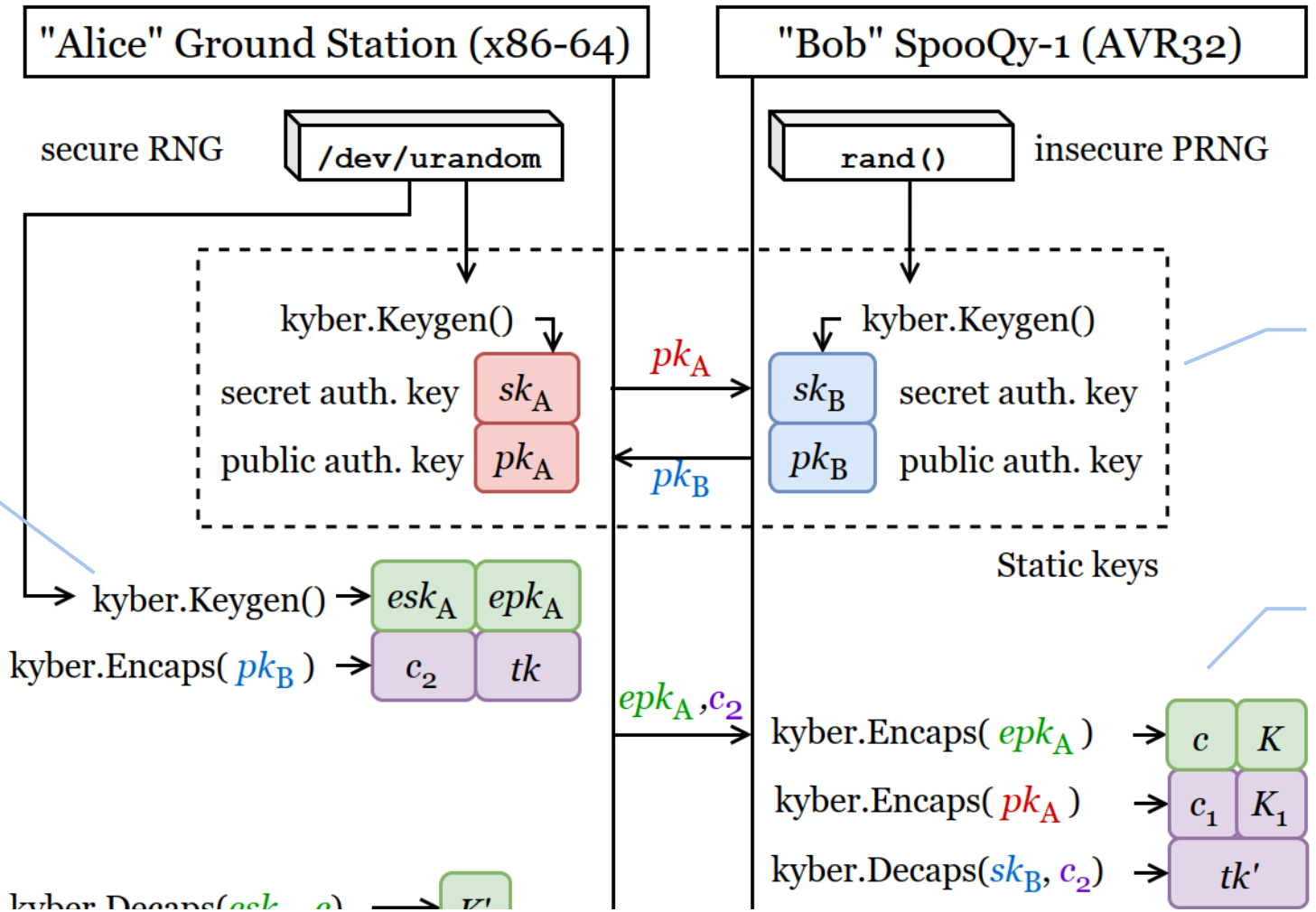
Random number generators (RNG)

- Kyber uses `/dev/urandom`
- not available on embedded systems

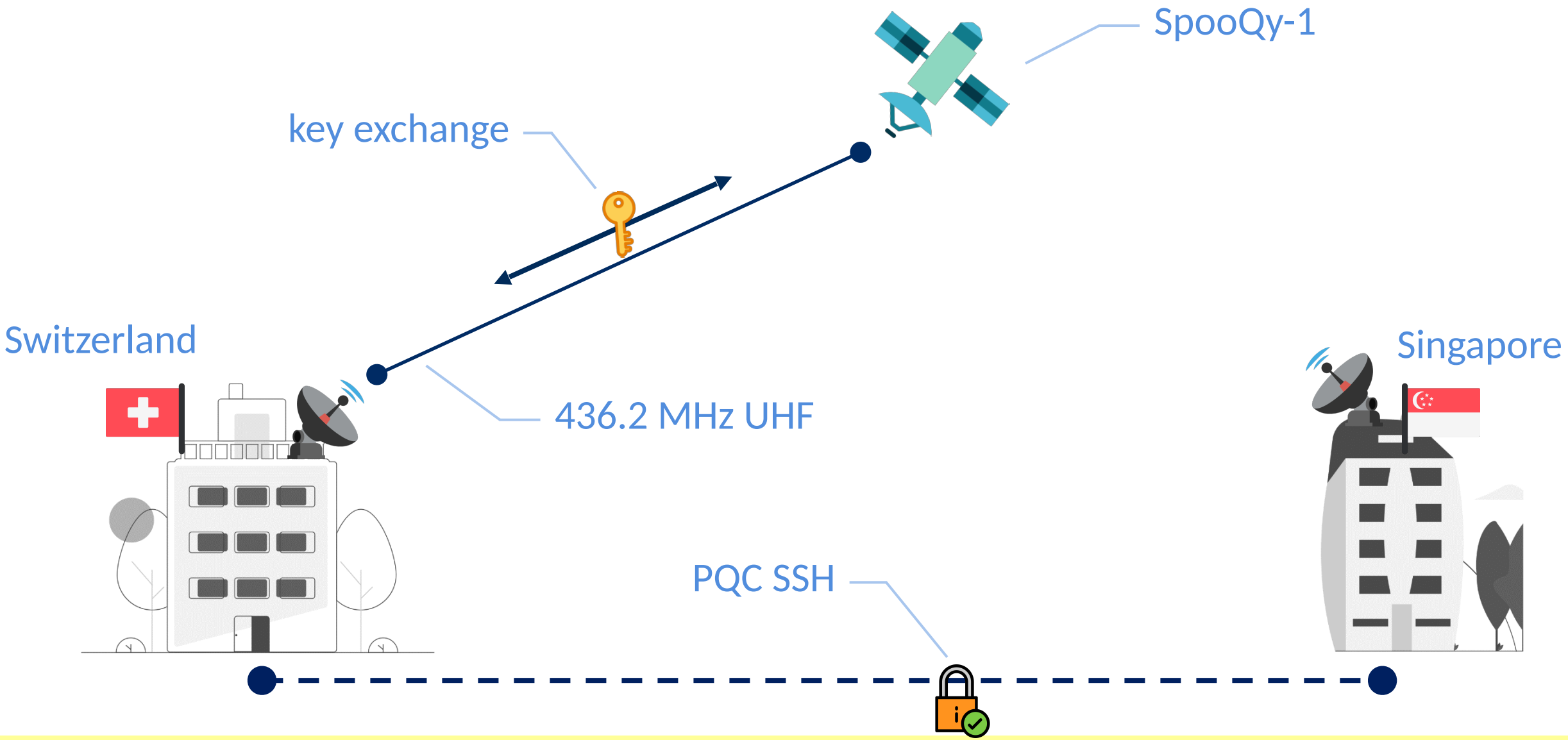
- use pseudo-RNG from AVR `stdlib`



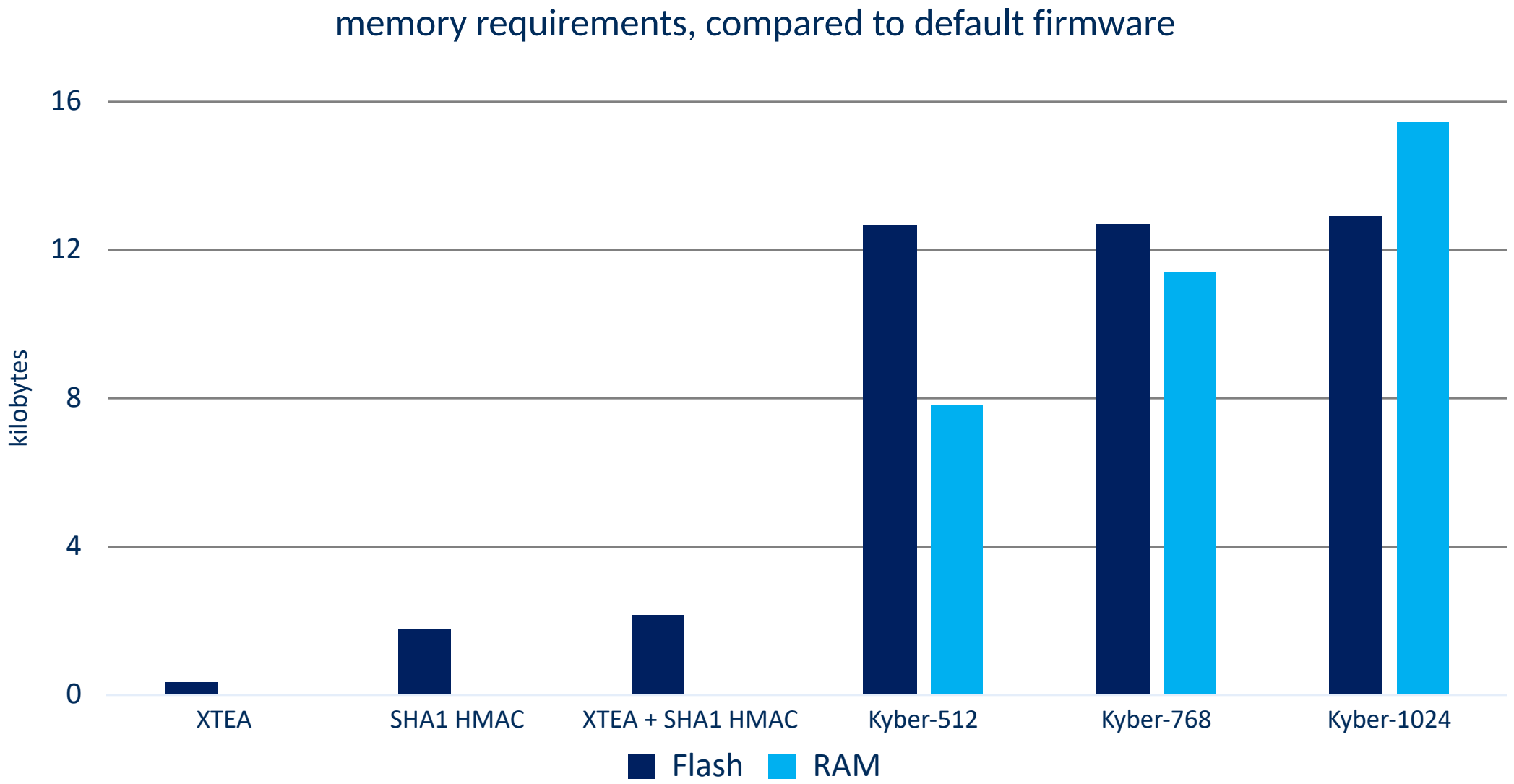
Pseudo RNG during key exchange



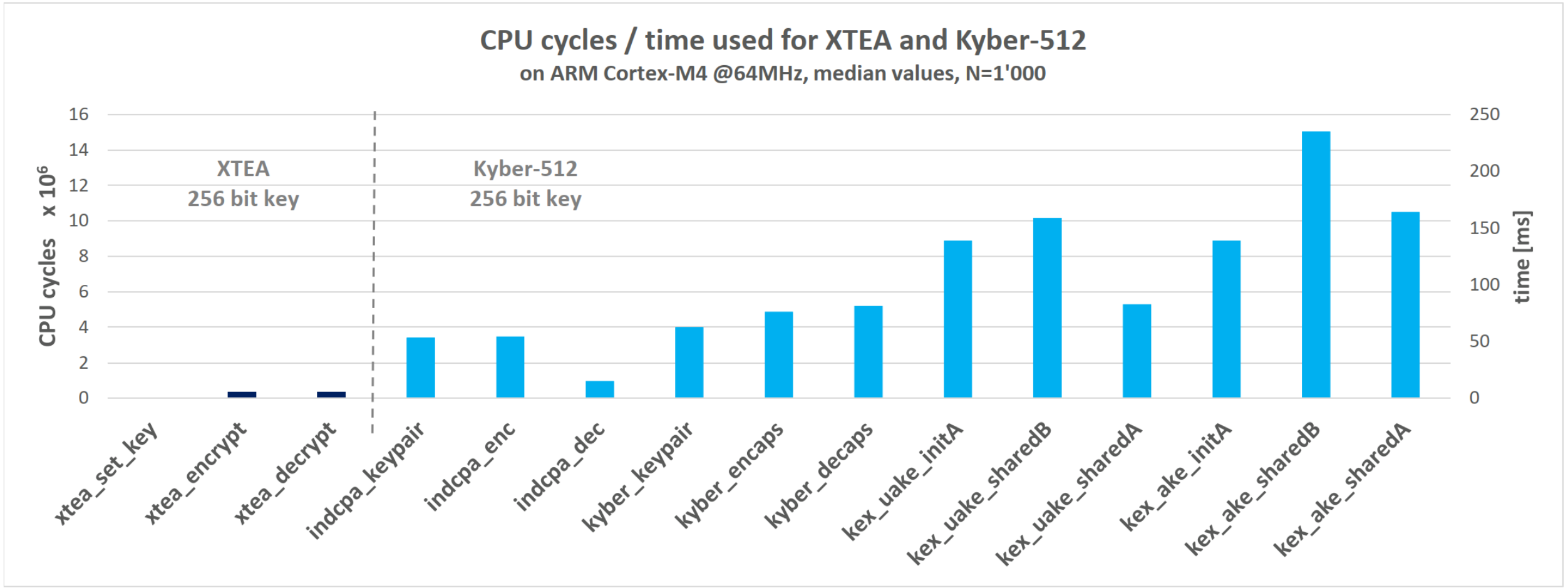
Quantum-safe encryption system for enterprise networks and internet



Flash & RAM usage



CPU utilization – embedded system



Outlook

- Hardware implementation on FPGA
- User authentication with Dilithium
- Integrate into CubeSat Space Protocol / X.509

University of Applied Sciences and Arts
Northwestern Switzerland

Institute for Sensors and Electronics

www.fhnw.ch/ise
simon.burkhardt@fhnw.ch

Simon Burkhardt, Willi Meier, Christoph Wildfeuer

Centre for Quantum Technologies

NUS National University of Singapore

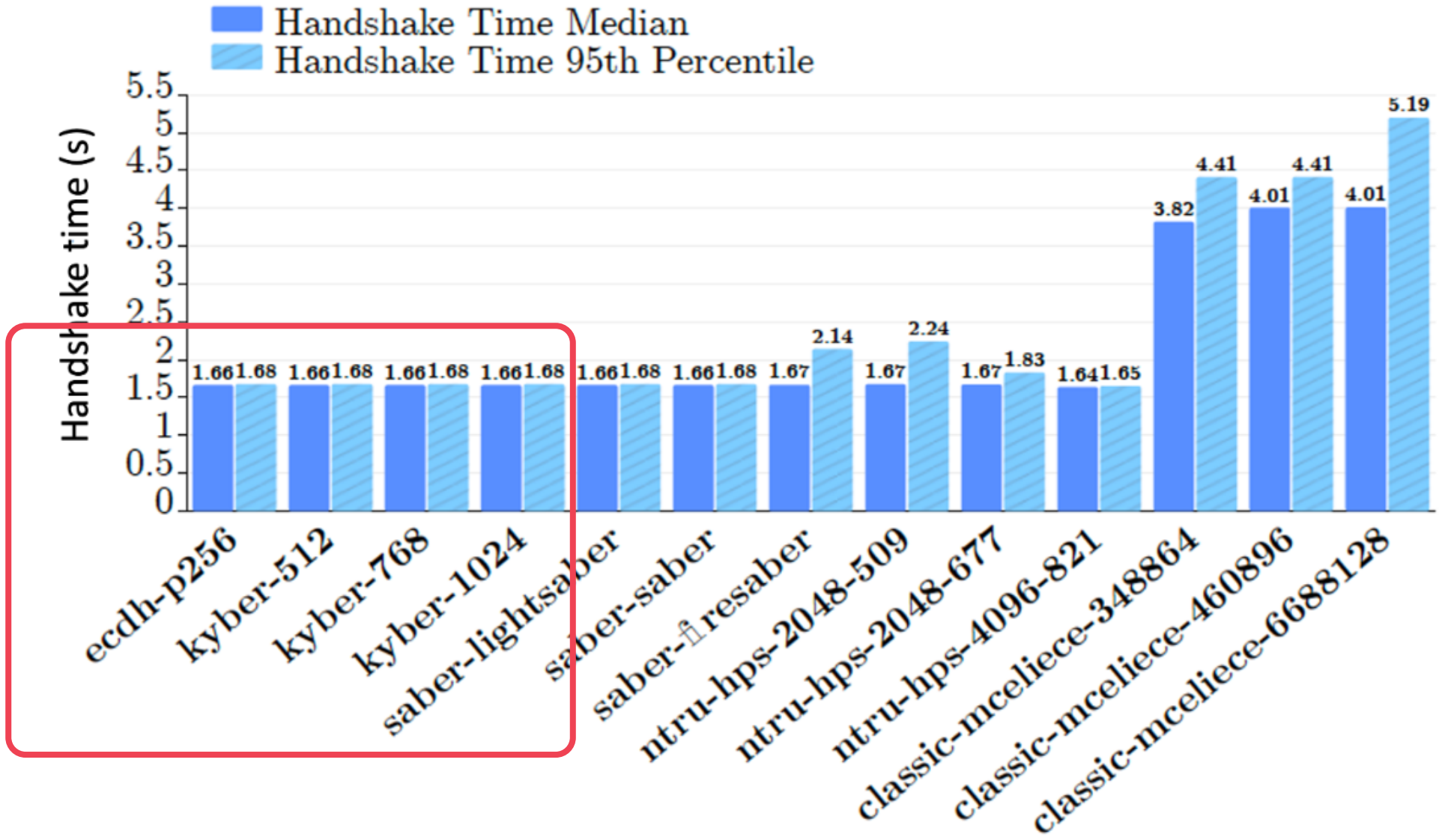
Ayesha Reezwana, Tanvirul Islam, Alexander Ling

proceedings paper

[SSC22-XII-04]

arxiv.org/abs/2206.00978

SSH handshake times



Embedded compilers

- `gcc-avr` uses C99 standard
- Kyber uses C11 standard

Quantum-optical communication