Freie Universität Berlin

Quantum-resistant digital signatures schemes for low-power IoT

H. Hattenbach
Freie Universität Berlin

Seminar Internet of Things, 2021

Outline

Quantum Computing breaks ordinary Encryption

- Quantum Computers operate on Qubits instead of normal Bits
- Qubits are Quantum-Mechanical
  - using spin of an electrons
  - Entanglement and Superposition
- Algorithms can leverage those mechanics
  - up to exponential speed up in some cases
  - Shors algorithm completely breaks common Encryption (like RSA, ECDSA, ..)
    - (Qubits are currently rather unstable $\rightarrow$ not broken yet)

- There are a few proposed solutions
- mostly based on Lattice-Based hard Problems
  - Frodo-Kem (Encryption)
  - FALCON (Signature)

Planned Structure

Outline

Creating an Overview

Outline

Diving Deeper

Outline

Planned Schedule