Quantum-resistant digital signatures schemes for low-power IoT

H. Hattenbach
Freie Universität Berlin

Seminar Internet of Things, 2021

Outline

Motivation

- Quantum Computing
- Internet of Things

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Outline

Motivation

- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes

- Performance Metrics
- different types

Structure

- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Quantum Computing breaks ordinary Cryptography

Freie Universität Berlin

- sufficiently sized Quantum Computers (explained later) on the horizon
- They can break most of the cryptography in current use
  - RSA
  - ECDSA / ECDH
  - $\rightarrow$ Signal, WhatsApp, PGP, SSH, TLS/HTTPS, ...
- not everything equally effected
  - schemes in standardization to replace current cryptography
  - some are rather computationally intense
  - that is why i have a deeper look on which are feasable for IoT

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Shors algorithm poses threat against asymmetric cryptography

- 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 asymmetric cryptography
    - can derive private key from public key
    - for everything based on Number-Theory (like RSA, ECDSA, ..)
  - Grovers algorithm poses threat against symmetric crypto and hash-functions
    - only quadratic speed-up
    - doubling length restores security (e.g. AES128 $\mapsto$ AES256)

- Quantum Computers operate on Qubits instead of normal Bits

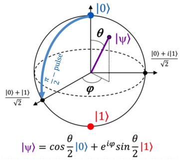

Figure: Model of a Qubit [?]

- Algorithms can leverage those mechanics
  - up to exponential speed up in some cases
  - Shors algorithm completely breaks common asymmetric cryptography
    - can derive private key from public key
    - for everything based on Number-Theory (like RSA, ECDSA, ..)
  - Grovers algorithm poses threat against symmetric crypto and hash-functions
    - only quadratic speed-up
    - doubling length restores security (e.g. AES128 $\mapsto$ AES256)

Shors and Grovers algorithms

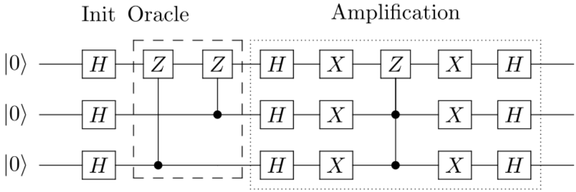

Figure: Grovers Algorithm [?]

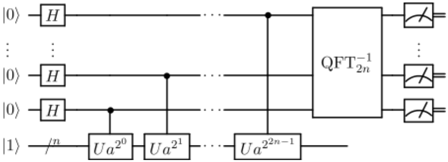

Figure: Shors Algorithm[?]

Outline

Motivation

- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes

- Performance Metrics
- different types

Structure

- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Many ressource constrained devices

- Internet of Things
- Smart-devices that are actually pretty dumb
  - little memory (kilobytes to megabytes)
  - low computing power (slow clock, small cache, etc.)
  - limited energy ressources (battery or solar operated)
- NIST classified into 3 classes:

Table: IETF IoT Classes

Class	RAM	Flash
C0	$<<$ 10 KiB	$<<$ 100 KiB
C1	10 KiB	100 KiB
C2	50 KiB	250 KiB

Outline

Motivation
    Quantum Computing
    Internet of Things

Quantum Resistant Signature Schemes
    Performance Metrics
    different types

Structure
    Skeleton
    Width-Covorage
    Depth-Covorage
    Ressources
    Schedule

What makes a signature scheme better than any other?

Freie Universität Berlin

- length of:
  - signature
  - public key
  - private key
- time and space needed to:
  - generate keys (GEN)
  - sign a message (SIGN)
  - verify a message (VER)
- security against quantum computers and traditional attackers

Table: QR Security classes and their traditional counterparts as classified by the NIST

Class	security comparable to
1	AES-128
2	SHA256
3	AES-192
4	SHA384
5	AES-256

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Multiple types of underlying mathematica problems

Freie Universität Berlin

- Super-singular isogeny based
  - SIKE
  - not well studied
- Multivariate polynomial based
  - Rainbow
  - not well studied
  - involves guessing work $\rightarrow$ not suited for low power devices
- Code based
  - McEliece
  - no finalist
- Hash based
  - SPHINCS+
  - big signatures (see next slide)
  - very well studied
- Lattice based
  - FALCON, Dilithium
  - most promising
  - most NIST finalists
  - most efficient
  - not as proofed as HBS

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Skeleton

- Introduction
- Internet of Things
- Quantum Resistant Security
  - Quantum Computing
  - QR Algorithms
    - Performance Metrics
    - Encryption
    - Signatures
- QR Signatures in IoT
  - Performance Metrics in IoT
  - Failed Signatures
    - WalnutDSA
    - qTESLA
  - FALCON
- Conclusion

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Creating an Overview

- Skimming multiple Quantum Resistant (QR) algorithms [**?**, **?**] that focus on IoT [**?**, **?**, **?**, **?**, **?**]
- Deeper reserach about signature Schemes [**?**]
- and having a slightly more detailed look at two failed sschemes [**?**, **?**, **?**, **?**]

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Diving Deeper

- having a deeper look at a NIST QR finalist with the most compact implementation:
  FALCON [**?**, **?**, **?**]
- maybe having an outlook in the end on a Hardware-Accelerated QR chip [**?**]

Outline

Motivation

Quantum Computing

Internet of Things

Quantum Resistant Signature Schemes

Performance Metrics

different types

Structure

Skeleton

Width-Covorage

Depth-Covorage

Ressources

Schedule

Ressources

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types

Structure
- Skeleton
- Width-Covorage
- Depth-Covorage
- Ressources
- Schedule

Planned Schedule

- 7.5. : skim breadth coverage literature
- 15.5.: write until signatures (at least bullet point comments)
- 30.5.: finish breadth (at least bullet point comments)
- α: skim and bullet point Depth
- 30.6.: finish