# Quantum-resistant digital signatures schemes for low-power IoT

1st Hannes Hattenbach
*Computational Science*
*Freie Universität*
Berlin, DE
hannes.hattenbach@fu-berlin.de

***Abstract*—**
***Index Terms*—Internet of Things, Quantum Resistance, Secure Signatures, Power Constraint Devices**

## I. Introduction

The quantum revolution is coming. With quantum computers[1] on the way to get more and more functional, people are fearing a loss of their security and privacy. That is because there are algorithms based on Shors algorithm that can forge signatures and decrypt encrypted messages whos security is based on number theory problems. The quantum computer only needs access to the public keys of these asymetric schemes. The expenditure to forge a signature[2] with classic[3] computers rises exponentially with increased key length, therefor beeing essentially unbreakable by classic computers. A sufficient quantum computer on the other hand can derive a private key from a public key in polynomial time, therefor rendering these schemes broken.

That is why there are currently schemes under standarization [**?**] that are based on other hard problems (not number theory) like so called lattice problems that cannot be that easily forged by quantum computers to save our privacy and security.

One of the use cases not directly comming to mind for the end user, but beeing as important non the less is signing sensitive sensor data in the Internet of Things (IoT). Another problem coming up in the IoT compared to end-user-devices like Laptops and Smartphones though is the severe ressource contraintness. The IoT consist of low power devices with wery few storage and computing power.

In this paper i am going to evaluate existing signature schemes and their usage possibilities for the IoT regarding their performance metrics.

Therefor i am going to give a small introduction and background to quantum computing, beeing a little more detailed about their ability to break current encryption and signature standards. In the next section i will give an overview over current candidates for Quantum Resistant (QR) Algorithms and giving performance metrics for those. The following chapter will then focus on signature schemes in the IoT, starting with additional performance metrics relevant in the IoT. With a little more details about two failed signature schmemes to highlight potetial pitfalls. And finally focussing on the best signature contenter for the IoT so far: FALCON.

[1] compare section III-A

[2] that is considered secure under normal circumstances

[3] we refer to classic if something is not directly leveraging entanglement or superposition

## II. Internet of Things

## III. Quantum Resistant Security

### A. Quantum Computing

### B. QR Algorithms

#### 1) Encryption:

#### 2) Signatures:

#### 3) Performance Metrics:

## IV. QR Signatures in IoT

#### 1) Performance Metrics in IoT:

### A. Failed Signatures

#### 1) WalnutDSA:

#### 2) qTESLA:

### B. FALCON

## V. Conclusion