

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

1<sup>st</sup> 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

## 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