

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

II. INTERNET OF THINGS

III. QUANTUM RESISTANT SECURITY

A. Quantum Computing

B. QR Algorithms

1) Encryption:

2) Signatures:

IV. QR SIGNATURES IN IOT

A. Failed Signatures

1) WalnutDSA:

2) qTESLA:

B. FALCON

V. CONCLUSION