Workingtitle
Postquantumcryptography

Jannis Priesnitz
University of Applied Sciences
Department of Computer Science
Schöfferstraße 3
64295 Darmstadt
Email: jannis.priesnitz@stud.h-da.de

***Abstract*—ABSTRACT**
***Index Terms*—Message Oriented Middleware, IoT**

I. Introduction

State of the art asymmetric cryptosystems compared with unsage of *hinreichend* long Keys are considered as "'safe"' with a view on current computersystems. This turns immidiatly if quantum computers enter the scene. But why is this the case? In this paper I briefly show up the main differences between normal comuputer systems and quantum computers, show up why state of the art cryptosystems like RSA and ECC not save in the quantum computation world. In addtion to that I give a detailed introduction to the McEliece Cryptosystem explain the strengs and downsides of the algortihm and give some details about the current *erkenntnisse* about codes which can be use for the system.

Outline

In the Section 2 ...

II. Conventional Computer systems vs. quantum computers

On conventional...

III. State of the art cryptography vs. Post quantum cryptography

With the background of Section 1 what do we have to change on our cryptosystems?

IV. The McElice cryptosystem

Back in 1978 Heinz McElies explained a quantum resistent cryptosystem based on linear codes. ...

A. Encryption

Entryption...

B. Signing

Signing

C. Key Agreement

Key Agreement

V. Codes can be used for MCElice

As destribed in the last Section the strength, computation time and keyspace is based on the codes used by the cryptosystem. ...

*A. *enter codes**

...

VI. Conclusion

...