AUSHANG

FREIE UNIVERSITÄT BERLIN

Fachbereich Mathematik und Informatik

Promotionsbüro, Arnimallee 14, 14195 Berlin

DISPUTATION

Dienstag, 28. August 2018, 14:00

Ort: Ehrhard-Schmidt-Hörsaal
(WIAS, Mohrenstr. 39, 10117 Berlin)

Disputation über die Doktorarbeit von

Herrn Clemens Bartsch

Thema der Dissertation:

A Coupled Stochastic-Deterministic Method for the Numerical Solution of Population Balance Systems

Thema der Disputation:

Post-quantum cryptography and the first quantum-safe digital signature scheme

Die Arbeit wurde unter der Betreuung von **Prof. Dr. V. John** durchgeführt.

Abstract:
In May 2018 news spread far beyond the cryptologist community: a group of German, Dutch and American computer scientists had published the first quantum-resilient digital signature scheme as an internet standard (RFC 8391), thus taking a major step towards arming digital signature against future attacks with quantum computers. The proposed XMSS scheme (eXtended Merkle Signature Scheme) makes use of cryptographic hash functions, which are considered quantum-safe.

In this talk we want to lead the audience towards an understanding of the importance and mode of operation of digital signature schemes, the threat that quantum computers might in the near future pose to them, and how the newly standardized scheme offers resilience against quantum computer attacks. We will start with a general introduction of digital signature and an explanation of a basic version of the widespread RSA algorithm and its major weaknesses, focusing on factorization attacks. Then we will introduce the basics of quantum computing, show how Shor‘s algorithm enables them to very efficiently perform factorization attacks, thus breaking RSA, and finally introduce XMSS and give an explanation for why it is supposed to be safe against quantum-aided attacks. Code examples and examples of quantum computations performed with a prototypical 5-qubit processor (IBM Q Experience) will be included in the talk.

Die Disputation besteht aus dem o. g. Vortrag, danach der Vorstellung der Dissertation einschließlich jeweils anschließenden Aussprachen.

Interessierte werden hiermit herzlich eingeladen

Der Vorsitzende der Promotionskommission
Prof. Dr. V. John