Quantum Computing - Practical and theoretical analysis of selected algorithms

Bachelor/Master Seminar SoSe 2021

Vivija Simić and Barbora Hrdá, February 8th, 2021 **update March 7th, 2021**

Fraunhofer

AISEC

Quantum Computing

Topic Suggestions

- Quantum Teleportation - Explanation of the operation mode using a practical implementation in Qiskit
- Amplitude Amplification using the example of the implementation of a simple Grover search algorithm in Qiskit
- Quantum Fourier Transformation and its significance for Shor's algorithm
- IT Protection Goals in Quantum Computing: Measures to Protect Integrity and Confidentiality

Post-Quantum Cryptology

Topic Suggestions

- Lattice-based encryption methods
- Methods based on mutlivariate polynomials
- Signature methods based on cryptological hash functions
- Encryption methods based on error correcting codes

Students are welcome to suggest own topics.

General Information

Prerequisites

- Strong mathematical background
- Good Python skills
- Mandatory participation in the preliminary meeting
- Registration via the matching tool

General Information

Objectives

- Improving scientific writing skills in Tex (10 Pages, IEEE template)[1]
- Presenting a scientific topic (in German/English):
  40 minutes + 15 minutes discussion.
- Enhancing theoretical and practical security skills

[1] https://www.ieee.org/conferences/publishing/templates.html

General Information

Grading

- Scientific paper: 50% (Content, Style, Effort, Grasp)
- Presentation: 40% (Content, Lecture Style, Understandability)
- Active participation/discussion: 10%

General Information

Registration and Presentations

- Register in the TUM Matching Tool on time!
- Send us an email with your top 3 desired topics until **16th of February**.
- You can add a letter of motivation to emphasize your top choice.
- Presentations will take place as a block **08.06 -10.06**, attandance is mandatory!

General Information

Time Table

08.02	Preliminary meeting (today)
16.02	Deadline for registration in matching system and email with desired topics
25.02-10.03	Welcome mail with topic distribution
16.04	Deadline for deregistration (afterwards: 5.0!)
28.04 23:59[2]	Deadline for submission of table of contents (ToC)
01.05. - 10.05.	Individual meetings to discuss ToC
07.06 23:59[2]	Deadline for submission of paper
08.06.-10.06	Presentations, attandance is mandatory!

[2] Central European Time

Contact Information

Vivija Simić and Barbora Hrdá

Department Secure Operating Systems

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstr. 11
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

E-Mail: vivija.simic@in.tum.de
barbora.hrda@aisec.fraunhofer.de