Quantum Computing - Practical and theoretical analysis of selected algorithms

Bachelor/Master Seminar SoSe 2021
Vivija Simić and Barbora Hrdá, February 8th, 2021
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 multivariate 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, LNCS)\(^1\)
- Presenting a scientific topic (in German/English):
  40 minutes + 15 minutes discussion.
- Enhancing theoretical and practical security skills

\(^1\)LaTeX-Template e.g. ftp://ftp.springernature.com/cs-proceeding/lncs/lncs2e.zip
General Information

Grading

- Scientific paper: 40% (Content, Style, Effort, Grasp)
- Presentation: 40% (Content, Lecture Style, Understandability)
- Presentation Slides: 10% (Content, Style)
- Active participation: 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**, attendance is mandatory!
### General Information

#### Time Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>08.02</td>
<td>Preliminary meeting (today)</td>
</tr>
<tr>
<td>16.02</td>
<td>Deadline for registration in matching system and email with desired topics</td>
</tr>
<tr>
<td>25.02-10.03</td>
<td>Welcome mail with topic distribution</td>
</tr>
<tr>
<td>12.04</td>
<td>Deadline for deregistration (afterwards: 5.0!)</td>
</tr>
<tr>
<td>28.04 23:59²</td>
<td>Deadline for submission of table of contents (ToC)</td>
</tr>
<tr>
<td>01.05. - 10.05.</td>
<td>Individual meetings to discuss ToC</td>
</tr>
<tr>
<td>07.06 23:59²</td>
<td>Deadline for submission of paper</td>
</tr>
<tr>
<td>08.06.-10.06</td>
<td>Presentations, attendance is mandatory!</td>
</tr>
</tbody>
</table>

²Central 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