Fraunhofer AISEC

Fraunhofer Institute for Applied and Integrated Security AISEC

TUM Bachelor / Master Seminar WiSe 22/23

Cryptography vs. Quantum Computing

Analysis of the threats to current cryptography and possible post-quantum-based measures

Vivija Simić and Barbora Hrdá

General Information

Topic suggestion - Current Crypto

General approach:

Current Crypto -> QC Threat -> PQC Measure

General Information

Topic suggestion - Current Crypto

- Private Key Cryptography (2 students)
- Public Key Cryptography: (2-3 students for each topic)
  - Diffie-Hellman (Key Exchange)
  - RSA
  - ElGamal (Dig. Signature)
  - EEC

General Information

Topic suggestion - PQC Measures

- Signature methods using CRYSTAL-Dilithium, Falcon and SPHINCS+
- Lattice-based encryption methods (eg. CRYSTAL-Kyber)
- Classical McEliece, BIKE, HQC, SIKE (runner-up)
- Students are welcome to suggest own topics

General Information

Prerequisites

- Strong mathematical background
- QC knowledge preferred
- Mandatory participation in the preliminary meeting
- Registration via the matching tool

General Information

Objectives

- Group assignment (2-3 students)
- Improving scientific writing skills in Tex (15-20 pages, IEEE template)[1]
- Presenting a scientific topic (in German/English):
  - 30 minutes (per student) + 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 **encrypted** email with your top 3 desired topics until 27th of July.
- You can add a letter of motivation to emphasize your top choice.
- Presentations will take place as a block seminar on **12.12.2022 - 16.12.2022** , attandance is mandatory!

General Information

Time Table

Date	
18.07.22 10:00	Preliminary Meeting (today)
27.07.22	Deadline for registration in matching system and encrypted email with desired topics
09.08.22	Welcome mail with topic distribution
09.09.22	Deadline for deregistration (afterwards 5.0!)
16.09.22 23:59[2]	Deadline for submission of table of content (ToC)
19.09.22 - 30.09.22	Individual team meetings to discuss ToC
30.11.22 23:59[2]	Deadline for submission of paper
12.12.22 - 16.12.22	Presentations, attendance is mandatory!

[2] Central European Time


Fraunhofer
AISEC
Fraunhofer Institute for Applied
and Integrated Security AISEC
Thank you for your attention!

Contact

Vivija Simić
TUM / Fraunhofer AISEC
vivija.simic@in.tum.de

Barbora Hrdá
Fraunhofer AISEC
barbora.hrda@aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC