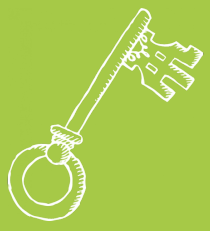


Introduction to Scientific Writing (1/2)

Advisor: **Cryptology & Privacy area**

Motivation

Cryptology is the foundation of everything secure. We **create, analyze, and optimize** modern cryptographic schemes such that they can be broadly used in practice. Our research features a unique combination of deep expertise in the design and **cryptanalysis** of symmetric cryptology with advanced cryptographic approaches such as **multiparty computation**, **homomorphic encryption**, and zero-knowledge proof systems. We design solutions for long-term security and address advanced threat scenarios such as **post-quantum security** and robustness against **implementation attacks**. Applications range from tiny IoT devices and RFID tags to cloud computing and machine learning.

Example Topics, Page 1

- **Privacy-preserving computation** (PPC) enables us to operate on encrypted or otherwise protected data. What are the most prominent representatives, and what are their benefits and shortcomings?
  fabian.schmid@iaik.tugraz.at
- **Multiparty computation (MPC) and differential privacy (DP)** are two privacy enhancing technologies with vastly different goals. What are some challenges to using them together?
  fredrik.meisingseth@iaik.tugraz.at
- **Cryptographic hash functions** are typically built from permutations or block ciphers. Discuss different constructions along with concrete examples where they are used.
  katharina.koschatko@iaik.tugraz.at
- **Algebraic models** are commonly used in cryptography to analyze the security of primitives. Model a concrete primitive and discuss solving strategies.
  katharina.koschatko@iaik.tugraz.at

more topics on the next page!

Literature

- Maria Eichlseder
- Lena Heimberger
- Marcel Nageler
- Fabian Schmid
- Shibam Mukherjee
- Katharina Koschatko
- Fredrik Meisingseth
- Simon Gerhalter

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at IAIK (highly recommended), check the full list of topics:

https://www.iaik.tugraz.at/bachelor-thesis

Recommended if you're studying

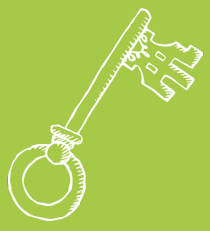
☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **cryptography** or **privacy**
- (Optional) *Information Security*

Advisor Contact

your.supervisor@iaik.tugraz.at



Introduction to Scientific Writing (2/2)

Advisor: **Cryptology & Privacy area**

Example Topics, Page 2

- What is **permutation-based cryptography**, and why has it become so popular in the last years? Explain how generic attacks define the security level of permutation-based sponge and duplex constructions.
  maria.eichlseder@iaik.tugraz.at
- A lot of new **tweakable block ciphers** have been proposed recently. What modes of operation do these ciphers enable compared to traditional block ciphers? Does this type of design present new attack vectors?
  simon.gerhalter@iaik.tugraz.at
- Key-committing and context-committing security are additional properties of authenticated encryption. What advantages does these extended security notions have? What are scenarios where this extra security is necessary?
  marcel.nageler@iaik.tugraz.at

more topics on the previous page!

Literature

- Maria Eichlseder
- Lena Heimberger
- Marcel Nageler
- Fabian Schmid
- Shibam Mukherjee
- Katharina Koschatko
- Fredrik Meisingseth
- Simon Gerhalter

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at IAIK (highly recommended), check the full list of topics:

https://www.iaik.tugraz.at/bachelor-thesis

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **cryptography** or **privacy**
- (Optional) *Information Security*

Advisor Contact

your.supervisor@iaik.tugraz.at