



# Introduction to Scientific Working (ISW)

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

- 💡 **Lattice attacks:** Look into a lattice attack (Primal, Dual, BDD) and describe it.  
[lena.heimberger@tugraz.at](mailto:lena.heimberger@tugraz.at)
- 💡 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@tugraz.at](mailto:maria.eichlseder@tugraz.at)
- 💡 What are cryptographic **nonces** and what happens if they are misused. Explain how nonce-misuse-resistant encryption can help.  
[marcel.nageler@tugraz.at](mailto:marcel.nageler@tugraz.at)
- 💡 **Differential privacy:** How is differential privacy defined? Why is it a meaningful and usable definition of privacy?  
[fredrik.meisingseth@tugraz.at](mailto:fredrik.meisingseth@tugraz.at)
- 💡 Arithmetization-oriented **Hash** functions and how they relate to Zero-Knowledge Proofs.  
[fabian.schmid@tugraz.at](mailto:fabian.schmid@tugraz.at)
- 💡 Explain the concept of **secret sharing** using the examples of additive secret sharing and Shamir's secret sharing.  
[florian.lugstein@tugraz.at](mailto:florian.lugstein@tugraz.at)

## Literature

- > [Maria Eichlseder](#)
- > [Lena Heimberger](#)
- > [Marcel Nageler](#)
- > [Fabian Schmid](#)
- > [Shibam Mukherjee](#)
- > [Katharina Koschatko](#)
- > [Fredrik Meisingseth](#)
- > [Simon Gerhalter](#)
- > [Florian Lugstein](#)

## Courses & Deliverables

- |   |
|---|
| <input checked="" type="checkbox"/> <b>Introduction to Scientific Working</b><br>Short report on background<br>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 ISEC (highly recommended), check the full list of topics:  
<https://www.isec.tugraz.at/bachelor-thesis>

## Recommended if you're studying

- CS    ICE    SEM

## Prerequisites

- > Interest in **cryptology** or **privacy**
- > (Optional) *Information Security*

## Advisor Contact

[your.supervisor@tugraz.at](mailto:your.supervisor@tugraz.at)