

Introduction to Scientific Working (ISW): Crypto

Advisor: **Secure Applications area**

Motivation

ISEC's "Secure Applications Area" consists of multiple teams, working in the areas of web security, identity and trust management, access control, mobile security, computation on encrypted data, and other fields of applied security and privacy.

A strong focus is **identity management** in the context of eGovernment, e.g., identity wallets and federated identity systems (i.e., ID Austria and eIDAS). Our interest is in how to build these systems in a way that maximizes user **privacy**.

Additionally, we look into techniques to increase user's trust in cryptographic systems (e.g., **key transparency**).

Another focus is **mobile security**. We are interested in innovations that assist application developers in creating secure services, even if they are not security experts themselves.

Example Topics

- Become familiar with the modern zero-knowledge frameworks for anonymous credentials (ACs) and provide a systematic overview of them.
  dmytro.shvets@tugraz.at
- Identify and outline applications of recent zero-knowledge proof techniques .
  dmytro.shvets@tugraz.at
- Quantum computers can probably break modern cryptography. Thus, we need to migrate various protocols to novel post-quantum algorithms and understand deployment challenges.
  jakob.heher@tugraz.at

Literature

- Jakob Heher
- Edona Fasllija
- Florian Draschbacher
- Stefan More
- Simon Gutschlhofer
- Dmytro Shvets
- Lukas Treffner
- research@a-sit.at

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 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 our topics, motivation, communication skills, and some experence with involved techniques.

Advisor Contact

your.supervisor@tugraz.at