Mathematical Foundations of Cryptography

Lena Heimberger & Reinhard Lüftenegger & Fredrik Meisingseth & Christian Rechberger

Introduction – WT 2022/23

Why this Seminar?

The Universe is written in the language of Mathematics.

We aim to illuminate the mathematics behind cryptographic schemes when

- designing,
- analysing, and
- implementing them.

Your Motivation

Why are you here?

- You had already crypto courses and want to understand them in more depth?
- You are planning to attend crypto courses and want to be prepared?
- Different motivation?

Course Organisation

- Your course contribution consists of a **seminar paper** and a **presentation**.
- Topics for seminar papers are proposed until **13th of October**, self-chosen topics are possible as well.
- Coordinate your topic with us **before you start** working on it.

Course Topics

- **Basics of Algebra**
  Groups, Rings, Fields and Finite Fields
- **Applications to Cryptography**
  (Cryptanalysis of) Boolean Functions, Gröbner Bases, Equation solving
- **Lattices**
  Learning with Errors and Rounding, Constructions and Operations
- **Statistics and Probability Theory**
  Probabilistic inequalities, statistical inference, differential privacy

How to Get Your Grade

Seminar paper

You write a **seminar paper** about a well-defined topic that is coordinated with us. Submission deadline is **January 12th**.

Seminar presentation

- You present your seminar topic in a **seminar talk** that lasts **20 minutes**.
- The dates for presentations are **December 15th**, and **January 12th, 19th**.
- Send us a draft **1 week** before you deliver your presentation.
- Send us your final presentation slides **1 day before your talk**.

Further Information

- **Course website**

  https://www.iaik.tugraz.at/mfc

- **Contact**
  Send us your seminar paper in PDF and other inquiries to

  mfc@iaik.tugraz.at

- **Discussion and Supervision**
  Feel free to write us or meet up if you have any questions!

Mathematical Foundations of Cryptography

Lena Heimberger & Reinhard Lüftenegger & Fredrik Meisingseth & Christian Rechberger

Introduction – WT 2022/23