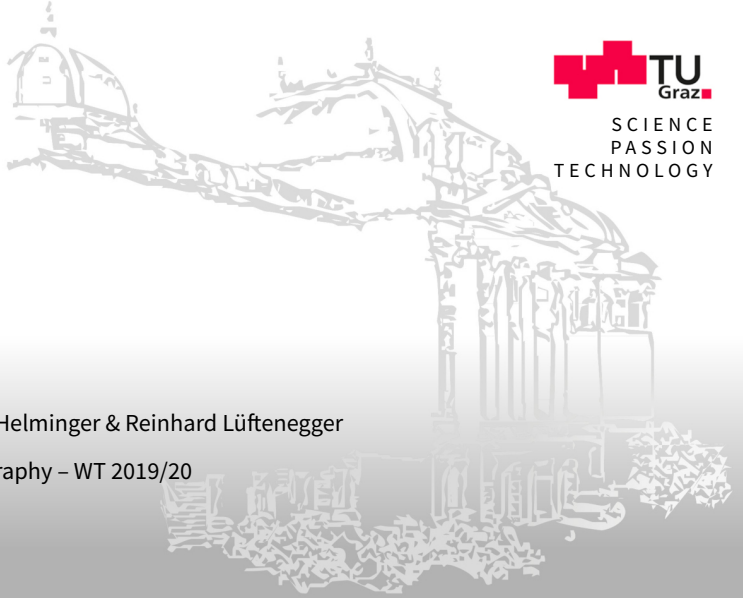
TU Graz

SCIENCE
PASSION
TECHNOLOGY



Introduction

Christian Rechberger featuring Lukas Helminger & Reinhard Lüftenegger

Mathematical Background of Cryptography – WT 2019/20

Motivation

Cryptography is everywhere, goal is to deepening understanding of some of IT

Seminar gives a solid basis, also useful for exciting new areas of applications.
Examples:

- Post-quantum cryptgraphy
- Privacy-preserving data mining and machine learning
- Building blocks for practical zero-knowledge proof systems

How did you get here? Your background?

Course Organisation

- The weekly seminar unit takes place every **Thursday** and starts at **10:15h**.
- On 10 out of overall 15 seminar dates we **lecture** about **selected aspects of mathematics** in cryptography. Each lecture lasts 2 academic hours (which is 1.5 real-time hours).
- During the remaining part of the seminar you **present a talk** on a specified topic (details follow below).
- The seminar is a **continuous assessment course** (“prüfungsimmanent”). We don’t enforce compulsory attendance, but you may receive content-related questions during your seminar presentation.

Content

- L1 – Groups
- L2 – Rings
- L3 – Fields and Finite Fields
- L4 & L5 – Gröbner Bases
- L6 – Elliptic Curves
- L7 – Discrete Logarithm
- L8 – Boolean Functions
- L9 – Codes
- L10 – Lattices

Goals

At the end of this course you know how to ...

- ... **describe** the most important **algebraic structures** used in cryptography.
- ... **represent** (certain) **cryptographic primitives** as polynomials and **conduct algebraic cryptanalysis** with this representation.
- ... **analyse** the **hardness of the discrete logarithm problem** in different groups and the implications for security parameters.
- ... **assess boolean functions** and identify their applications in codes and lattices.

How to Get Your Grade

Seminar papers (50%)

You write **two short papers** about predefined topics. The topics will be announced at latest by the end of October. Submission deadlines are **December 1st** for the first paper and **January 30th** for the second one.

Seminar presentation (50%)

You work on a topic of your own choosing or from a list of given topics and present your results in form of a **seminar talk**. A self chosen topic is related to the content of the seminar. Your talk lasts approximately **20 minutes**. The dates for presentations are

- **October 31st** and **November 28th** (during the seminar),
- **January 16th** and **January 23rd** (end of the seminar).

Further Information

- Course website

  https://www.iaik.tugraz.at/course/selected-topics-it-security-2-705051-wintersemester-2019-20/

- Seminar papers

  Send us your seminar papers in PDF via Email to {christian.rechberger, reinhard.lueftenegger, lukas.helminger}@iaik.tugraz.at.

- Seminar talk
  - Coordinate your topic and the intended content with us **before you start**.
  - Make an appointment and meet us **1 week before your talk** in one of our offices IF01{112, 010} to inform us about your presentation slides.
  - Send us your presentation slides in PDF **22 hours before your talk** via Email.

Questions?