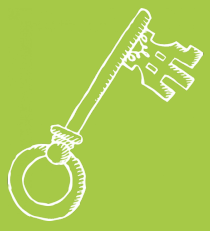

Is $P \neq NP$ enough for one-way functions to exist?

Advisor: **Fredrik Meisingseth**

Motivation

A common theme in cryptography is that one needs to make some assumption relating to complexity theory in order to ascertain that a given cryptographic object exists. One of the most basic cryptographic objects is that of one-way functions (OWFs), meaning functions that can be evaluated efficiently but for which it is hard to find an input that gives a specific output. At first glance, the existence of such functions seems quite similar to the assumption that the complexity classes *P* and *NP* are not equal, essentially saying that there are problems where a solution can be verified (or falsified) efficiently but where no efficient algorithm can find a solution. This similarity makes us ask; *If it turns out that $P \neq NP$, does that mean that OWFs exist?* (Spoiler, the answer is 'no').[1]

In your ISW project, you will:

- Study the definition of OWFs and the complexity classes *P*, *NP*, *BPP*.
- Discuss why $P \neq NP$ is not enough to guarantee that OWFs exist.
- Discuss what complexity assumptions are needed to make sure OWFs do exist.

Goals and Tasks

- Understand the definition of OWFs and why it is crucial to the field of cryptography.
- Understand OWFs relate to the complexity classes *P*, *NP*, *BPP* and their use in cryptography.

The fundamental nature of these questions mean that they can serve as preparation a broad range of thesis topics, if you are interested in following the ISW project up with a thesis just let us know and we can together formulate a topic to fit your interests.

Literature

- S. Goldwasser and M. Bellare
  Lecture Notes on Cryptography, Section B
  https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Strong interest in mathematics and cryptography

Advisor Contact

fredrik.meisingseth@iaik.tugraz.at