KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Complexity-theoretic aspects of the preprocessing model

Bachelor's Thesis

Splitting a task into a preprocessing phase and a computation phase has been considered in many practical applications. An example for this is the creation of a database, where the database layout is optimized (e.g. through sorting), such that subsequent queries can be answered more efficiently (e.g. through binary search). Another example is the creation of rainbow tables, where a table of hash values is created that allows to efficiently invert outputs of a hash function. While the practical aspects of preprocessing are well-studied, there exists little research in the area of complexity-theoretic aspects of the preprocessing model.

In this thesis, the preprocessing model needs to be defined from a complexity-theoretic point of view. It should be shown that this definition captures real-world examples of preprocessing. Based on this model, several variations of complexity classes need to be defined. In a next step, relations between these complexity classes should be shown. Finally, it should be shown how these new complexity classes relate to established classes such as **P** or **NP**.

The goal of this thesis is to get an overview of the complexity-theoretic aspects of preprocessing.

Scope of the work

- Literature research of prior work on complexity-theoretic aspects of preprocessing.
- Formalizing the preprocessing model.
- Showing that this model captures real-world applications of preprocessing.
- Defining complexity classes for this model.
- Showing how these complexity classes relate to each other and how they relate to established classes.

Requirements

Following prior knowledge or skills are useful (or have to be acquired) for the thesis:

- Knowledge of complexity theory and Turing machines.
- Interest in the topic is strongly recommended.

Contact

In case of interest or for further information, please contact Robin Berger, `robin.berger@kit.edu`.