

---

## - Bachelor/Master Thesis -

### **Aspects of Fuzzy-Hashing**

---

#### **CASED**

In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. For more information visit our webpage [www.cased.de](http://www.cased.de).

#### **Motivation**

Traditional / cryptographic hash functions are widely spread and used for different cases (e.g. file identification, hash tables in databases, ...). Due to their security properties (e.g. the avalanche effect) they have one main drawback: one changing bit in the input changes approximately 50% of the hash value. Therefore these hash functions cannot be used to identify similar files.

A similarity preserving hash function aka *fuzzy hash function* should overcome this drawback and map similar inputs to similar hash values. In general we distinguish between the byte level and the semantic level whereas at the moment the focus is the byte level.

#### **Task**

The choice of topic is depending on the current state of research and needs to be discussed. Depending on your interests, there are normally different possibilities, e.g. do a security analysis of an existing approach, develop an own approach based on your own idea and improve existing approaches.

The exact topic will be defined within a meeting / phone session.

#### **Requirements**

- High motivation, creativity and ability to work independently
- Good communication skills
- Good programming skills (favored C/C++)
- Knowledge of hash functions is a plus
- Very good knowledge of German or English

#### **Start date**

Immediately

#### **Contact**

**Frank Breitinger**  
[frank.breitinger@cased.de](mailto:frank.breitinger@cased.de)

CASED - Center for Advanced  
Security Research Darmstadt  
Mornwegstraße 32  
64293 Darmstadt