Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

*Type of work: Master's thesis*

# Search over encrypted data using Attribute-Based Encryption

## Motivation

The search over encrypted data is an important technique in the area of cloud computing. Fully homomorphic encryption (FHE) is able to provide full computation over encrypted data, but lacks in efficiency and is not applicable for very large data sets until now. Searchable encryption (SE) on the other hand aims at finding the best tradeoff between efficiency and data privacy. Various searchable encryption schemes exist, but a lot of them are restricted to conjunctive queries. In order to raise the query expressiveness, a new approach will be taken (and tested for efficiency) in this master thesis, by applying a key-policy attribute based encryption scheme (KP-ABE) to an encrypted search protocol. In a KP-ABE scheme a ciphertext is created using a set of attributes and a user key contains an access policy. It is possible to decrypt, if the access policy in a user key matches the attributes of a ciphertext.

## Topic

The goal of this thesis is to develop an encrypted search protocol, based on a given KP-ABE scheme. In order to apply a KP-ABE scheme to an encrypted search protocol, various steps have to be completed. The scheme has to be adopted to the requirements of the encrypted search protocol. After adopting the scheme, an index structure has to be created and encrypted. After the creation of the index, a user should be able to search through the data, based on the desired queries. If a query matches an entry in the index, it will be returned to the user. The user should now able to decrypt the result, if the attributes in the ciphertext and the attributes in the query match. Finally we will test the efficiency of the scheme.

## Topic Description

- adopt a KP-ABE scheme to the encrypted search setting (implementations for KP-ABE can be provided in Java or Python)
- implement a searchable index structure (for example an inverted index or a tree)
- implement the encrypted search protocol
- evaluate the result regarding efficiency

## Requirements

- Good general programming skills (Java or Python)
- Interest in Cryptography
- Ability to work self-directed and systematically

The thesis can be written in English or German.

## Contact

**Georg Räß**
Telefon: +49 89 322-9986-147
E-Mail: georg.raess@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Service & Application Security
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de Ausschreibungsdatum: 8. August 2017