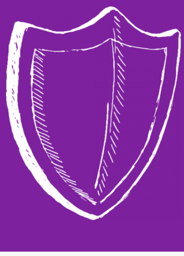
IAIK | Institute of Applied Information Processing and Communications



Computation on Encrypted Education Data

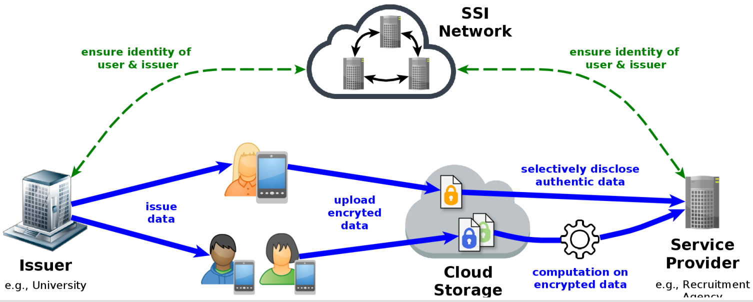
Advisor: **Felix Hörandner**

Motivation

Encryption protects the confidentiality of data, before handing them to a less trusted service (e.g., cloud storage). To perform further business logic on the data, a service/recipient usually first has to decrypt the ciphertext, and then operate on the plaintext – an all or nothing approach. However, if the recipient is only trusted to some degree, the user might not want to reveal her full plaintext, but would be open to reveal a function on her data, e.g., let her data participate in statistics. With functional encryption (FE), the recipient holds a decryption key, which decrypts the ciphertext to a pre-defined function of the plaintext $f(p)$, rather than the whole plaintext. Multi-input functional encryption extends this concept, and allows to decrypt a function on multiple encrypted inputs.

We aim to develop a system to not only securely outsource and share (education) data, but also to perform privacy-preserving computation on them. In more detail: Our proposed system is based on the self-sovereign identity paradigm, where users and issuers of data establish their identities and public keys in a decentralized ledger system. We integrate two cryptographic mechanisms: functional encryption (FE) to enable computation on encrypted data and proxy re-encryption (PRE) to keep users in control over who obtains access to their data to perform the computations.

To illustrate the application of our concept, we elaborate on a job application process: Alice obtains a verifiable credential from her university, which contains a transcript of her grades, and securely shares this credential with a recruitment agency. This agency obtains/buys the computation rights to evaluate the average of other students' grades, which allows to compare Alice's performance and make a more informed decision.



Literature

- M. Abdalla et al.
  Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions Without Pairings
  CRYPTO (1)
  https://doi.org/10.1007/978-3-319-96884-1_20
  https://eprint.iacr.org/2017/972
- G. Ateniese et al.
  Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage
  Proceedings of the Network and Distributed System Security Symposium, NDSS 2005
  https://doi.org/10.1145/1127345.1127346

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: Java
- Interest in public key crypto

Advisor / Contact

felix.hoerandner@iaik.tugraz.at

MASTER PROJECT / THESIS

SECURE APPLICATIONS