Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

**Ephraim Zimmer**, Christian Burkert, Tom Petersen, Hannes Federrath

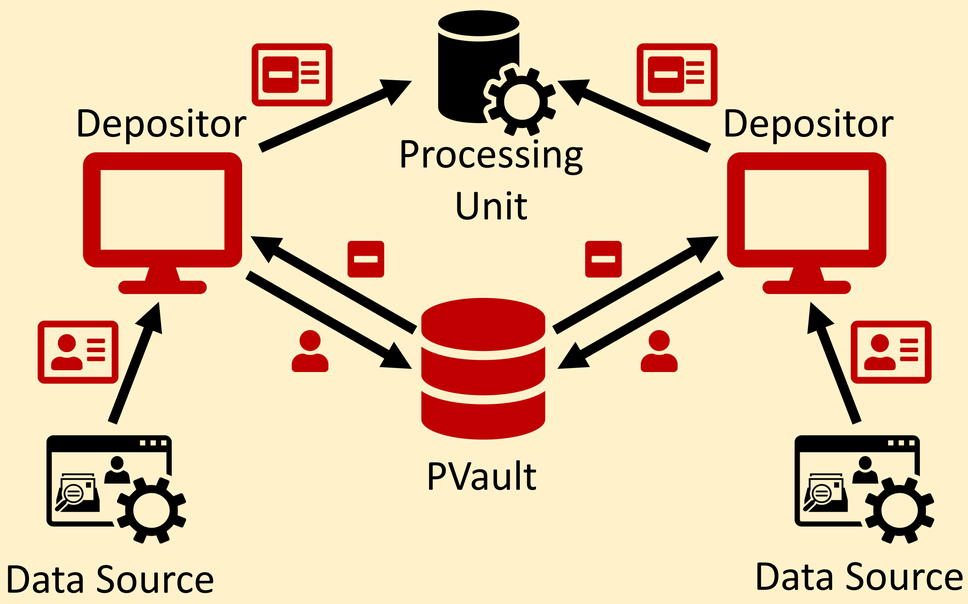
# PEEPLL: Privacy-Enhanced Event Pseudonymisation with Limited Linkability

Pseudonymisation provides the means to **reduce the privacy impact** of data collection and processing on individual subjects. However, its application on data records, especially in an environment with additional constraints, like **re-identification** in the course of incident response, implies assumptions and **privacy issues**, which contradict the achievement of the desirable privacy level. PEEPLL contains technical realisations to achieve **privacy protection goals** by a more rigorous commitment to the concept of personal data minimisation.

## Requirements

- Linkability
- Global Consistency
- No Pseudo-Randomness
- Personal Data Minimisation

## System Model



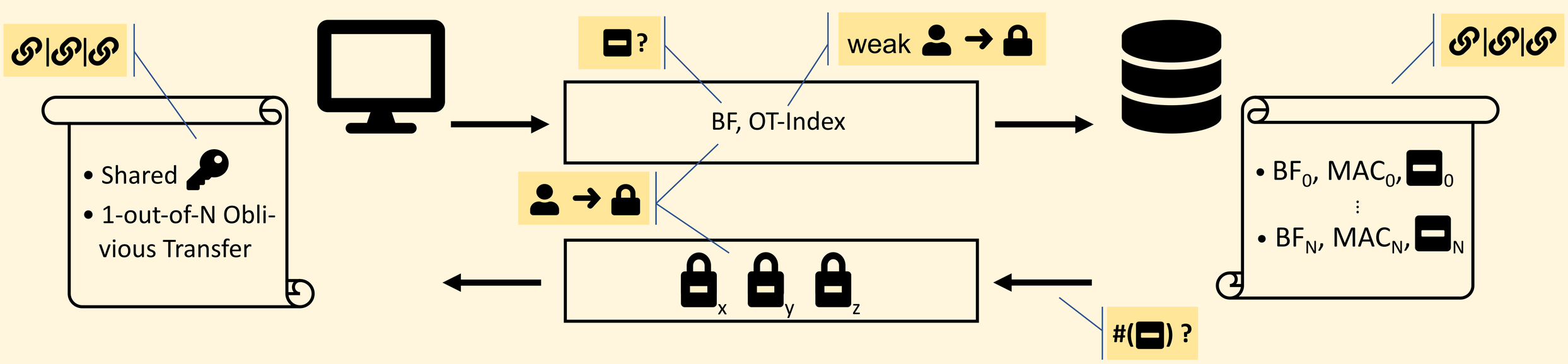

## Privacy Protection Goals

**Re-use Indistinguishability:** The information about whether or how often a pseudonym has been used before by any Depositor is only known to the PVault.

**Deposit Confidentiality:** Neither the PVault nor any other Depositor learn any information about the underlying quasi identifier (QID) of a deposit.

**Matching Pseudonym Unobservability:** The PVault does not learn any information about which entry of the pseudonym lookup table matches a queried deposit.

**Limited Linkability:** The linkability of data records concerning the same QID is only be maintained for a limited period.




## Future Work

1. The integration of a pseudonym re-identification resp. disclosure process and analysis of potential side effects on the privacy protection goals.
2. Enhancements in the realisation of budget limitation in order to achieve anytrust.
3. The full achievement of Re-use Indistinguishability even in the case of not-yet processed pseudonyms.