UnLynx: A Decentralized System for Privacy-Conscious Data Sharing

David Froelicher, Patricia Egger, Joao Sousa, Jean Louis Raisaro, Zhicong Huang, Christian Mouchet, Bryan Ford, Jean-Pierre Hubaux

Motivation

Protect sensitive data and still be able to share them among multiple entities in a privacy-conscious way (medical research, private surveys, ...)

Current solutions depend on a centralized authority that must be trusted (weakest-link) or leverage on decentralized but impractical approaches (e.g., secure multi-party computation)

System Model

- Servers (S), form a collective authority, sum their keys to create the collective public key
- Data providers (DP) store their data encrypted with the collective authority key
- Data are homomorphically encrypted
- All computations are done in the encrypted domain
- Protecting data providers is the main focus of our system

Threat Model

- Queriers (Q) are malicious
- All the servers except 1 are malicious (Anytrust model)
- Data providers are honest-but-curious

Solution

1. Initialisation (step 0)
2. Query (step 1)
3. Response (step 2)
4. Shuffling (step 3)
5. Distributed deterministic tagging (step 4)
6. Collective aggregation (step 5)
7. Distributed results obfuscation (step 6)
8. Key switching (step 7)
9. Decrypt using the querier’s private key (step 8)

Undertaken by
- Querier
- Data provider
- Collective authority

Evaluation

Settings
- 2 Intel Xeon E5-2680 v3 CPUs
- 2.5GHz
- 256GB RAM
- 1Gbps link
- EG (Ed25519)

Future Work

- Explore other crypto systems
  - More functionalities
  - Quantum resistant
  - Better performance
- Distributed ledger (blockchain)
  - Query log
  - Authentication
  - Accountability

Distributed database of hospitals (Switzerland)

- Privacy-preserving sharing of sensitive medical data
- Exchange of crucial information
- Improve data accessibility
- Improve medical research