A LEAKAGE-RESILIENT AUTHENTICATION AND DATA MANAGEMENT SYSTEM

SeongHan Shin

An Extended Protocol of "LR-AKE"

- LR-AKE: Leakage-Resilient Authenticated Key Exchange
- Mutual authentication and session key generation
- Data-key retrieval

Advantages and Functionalities

- Accepts one short password for multiple services
  - Secure against off-line exhaustive search even if stored secrets leak out from any side of client and server
- Automatic revocation of leaked secrets
- "Strong" forward secrecy
- Computational efficiency on client side
- No public-key certificate management

Applications

- Any service with authentication and/or storage
- SSO (Single Sign On) @ client side
- and so on

Demo

- LR-LoginChecker
  - Online data-key recovery