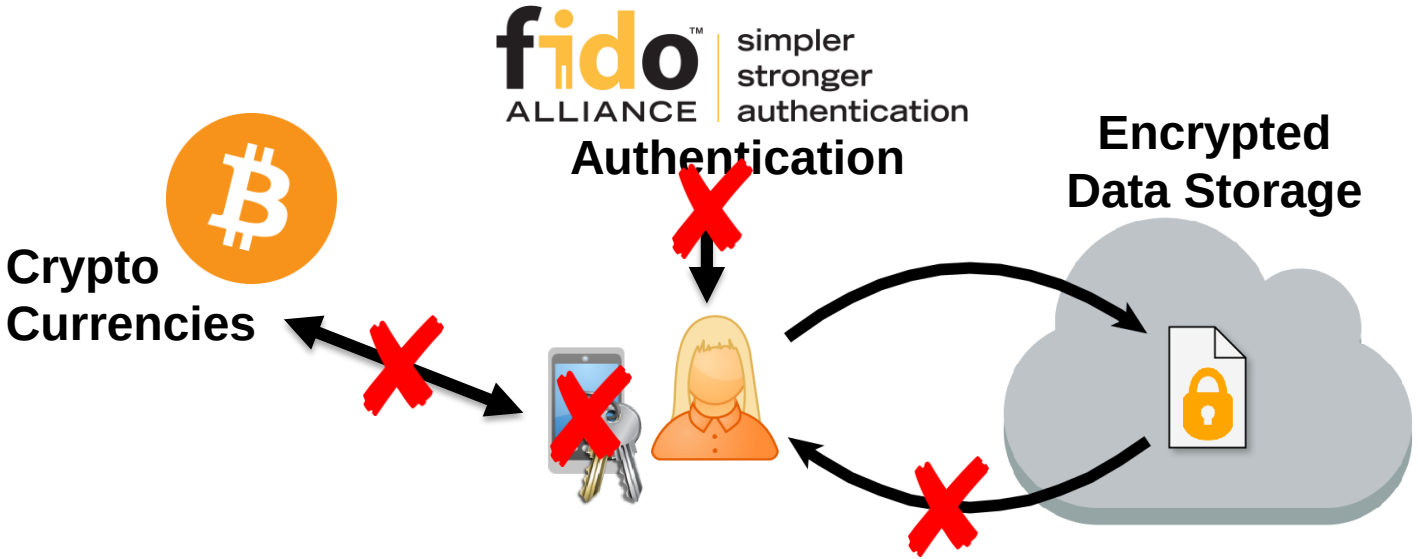
Horcruxes for Everyone –
A Framework for Key-Loss Recovery by Splitting Trust

Felix Hörandner
Graz University of Technology

Christof Rabensteiner
Graz University of Technology

17.01.2020

Introduction



What if device is lost or stolen?

- Without key: Can't access data, spend money, authenticate, …

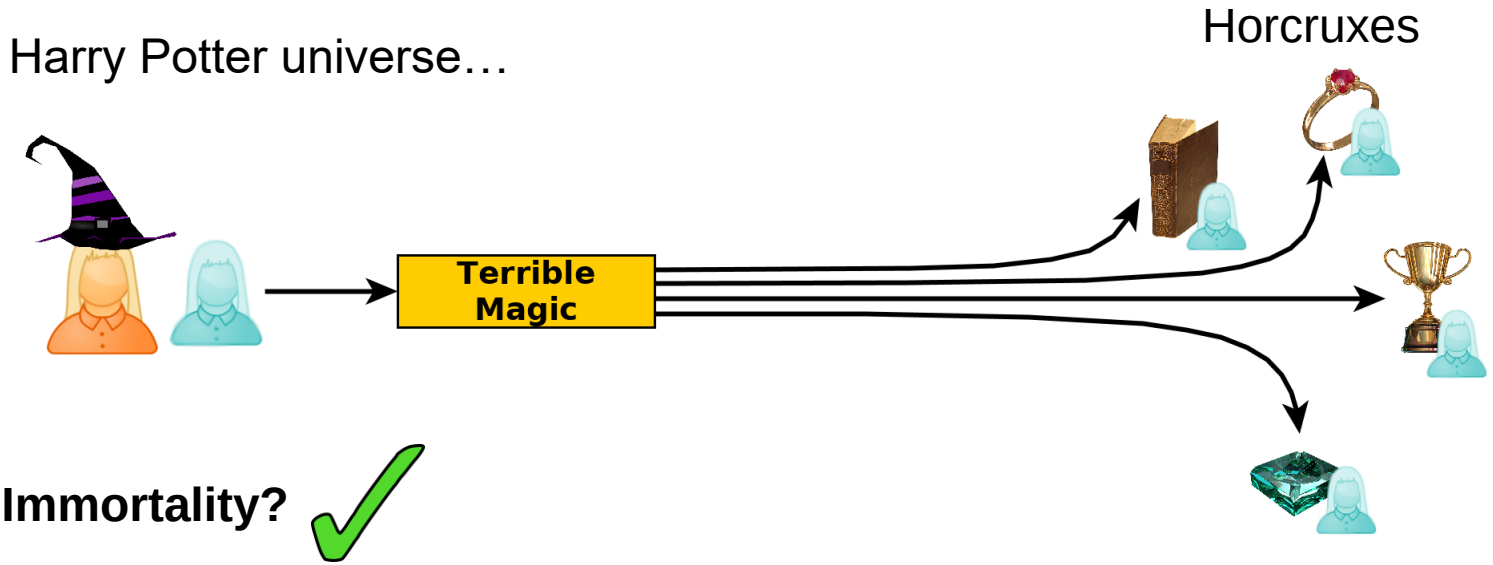
➢ Need to recover from key loss

Traditional approaches

- Backup on flash drive?
- Sheet with QR code?
- Password-encrypted key at cloud storage?

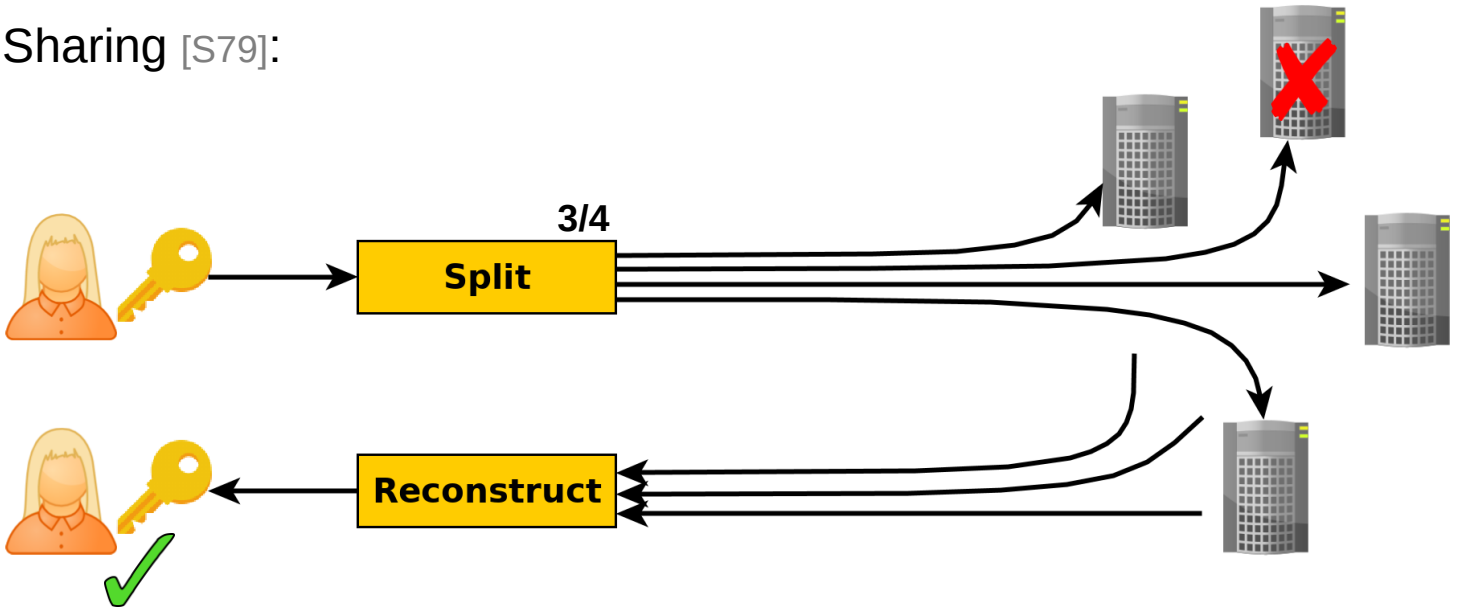
Horcurxes for Immortality

In the Harry Potter universe…



Horcurxes and Secret Sharing

Secret Sharing [S79]:



Users:

- Reconstruct with threshold of shares

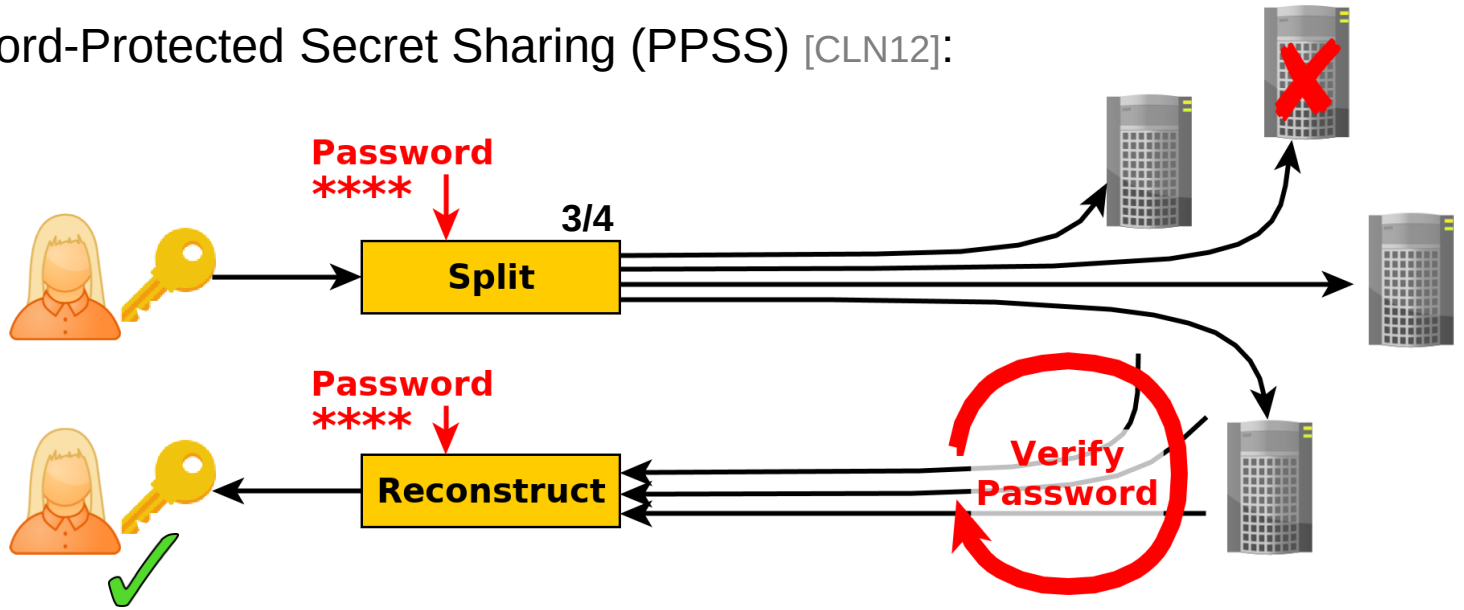
Servers: Split Trust

- Cannot reconstruct alone

[S79] Adi Shamir: How to Share a Secret. Commun. ACM 1979

Password-Protected Secret Sharing (PPSS)

Password-Protected Secret Sharing (PPSS) [CLN12]:



Users:

- Human-memorisable password

Servers:

- Do not learn password

[CLN12] J. Camenisch, A. Lysyanskaya, and G. Neven. ACM CCS 2012.
Practical yet Universally Composable Two-Server Password-Authenticated Secret Sharing

Challenges and Our Contribution

- User-friendly system to recover from device/key-loss
  - Addresses challenges of applying PPSS in practice

Usability
- Reach trust decisions
- Understand impact of future changes
- Repetition vs. Re-Use

Practicability
- Convince trustworthy organizations to operate PPSS servers

Generic framework
- Build and maintain trust hierarchy
- Recommender: support in making trust decisions
- Management app: simplifies integration

Implementation
- Feasibility: introduce hierarchical PPSS
- Minimize effort for server operators
- Evaluate performance, estimate costs

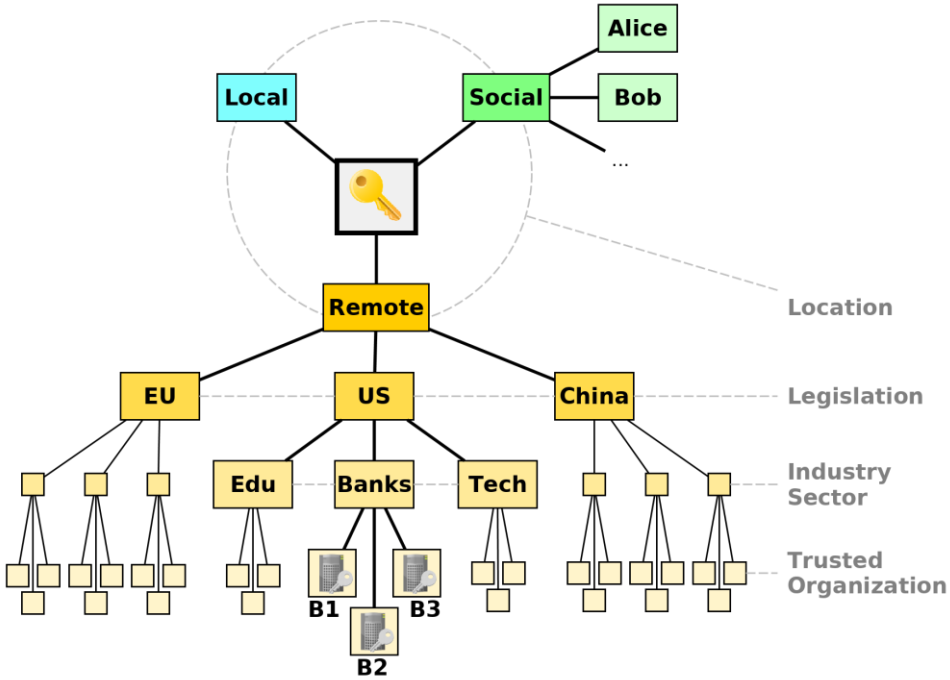
Whom to Trust?

… to keep shares secure and available

- **Own devices**
- **Social circle**
  - Trusted
  - Ability and Availability?

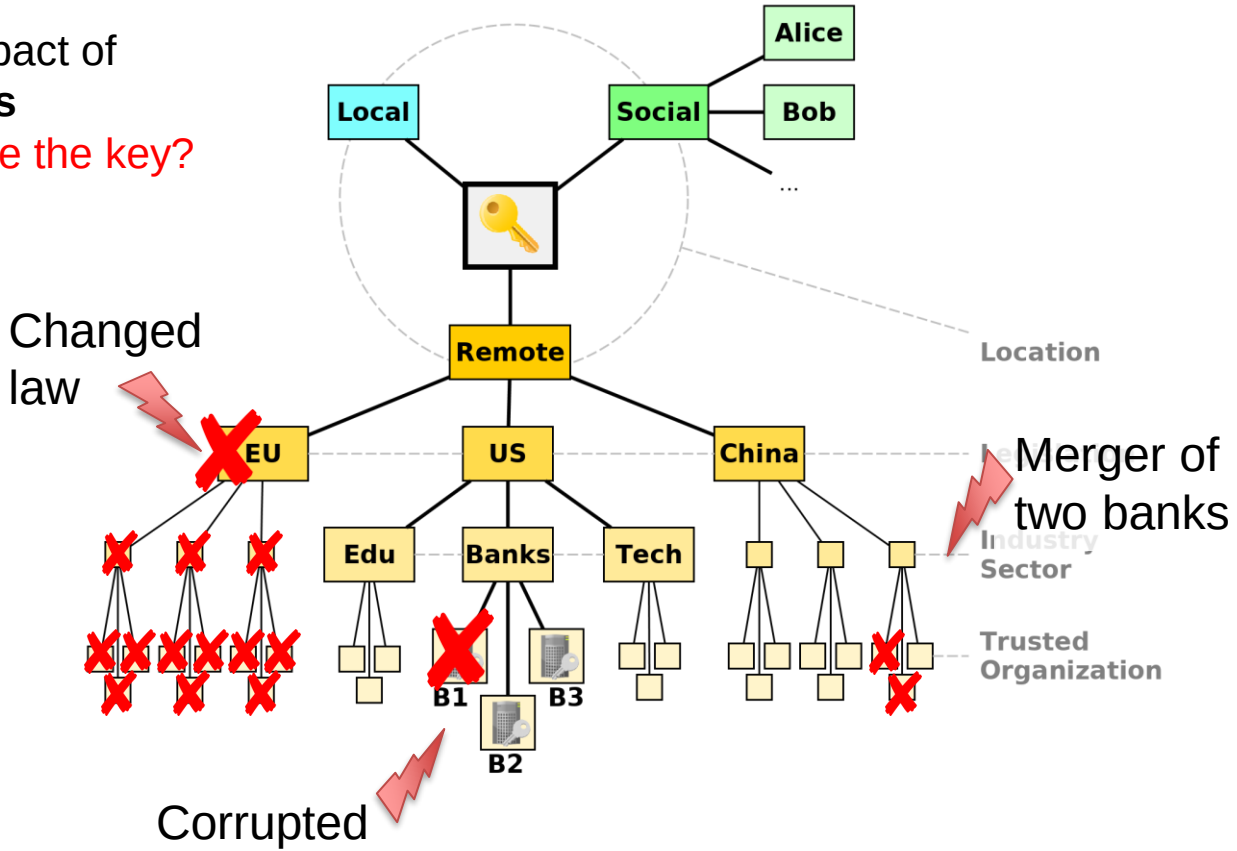
- **Trusted organizations**
  - Trusted for inherent factors
    - Motivation, Competence
  - Impacted by external factors
    - E.g. when laws change

Example: Trust Hierarchy

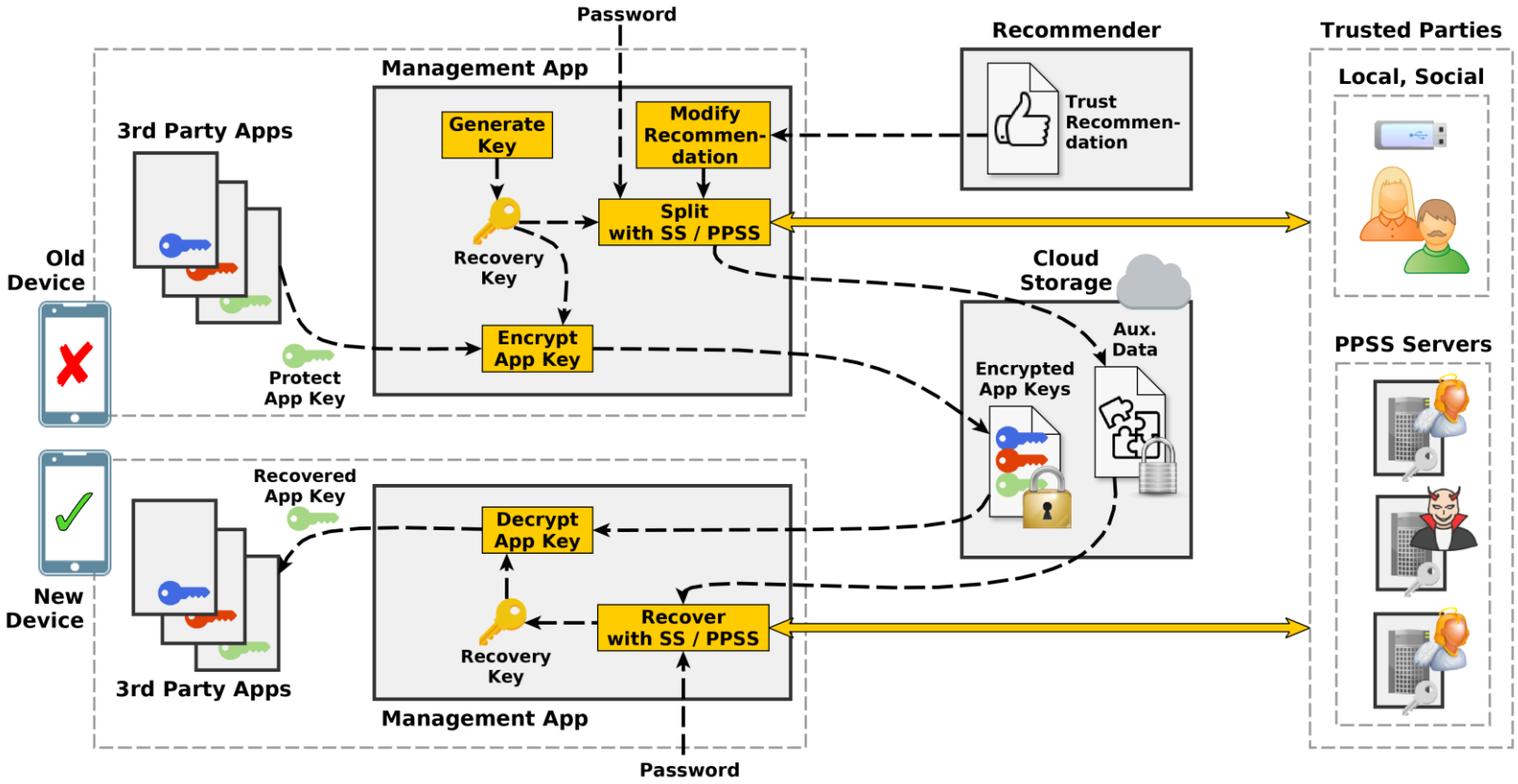


Trust Hierarchy

- Understand impact of **future changes**
- ➢ When to change the key?



Architecture

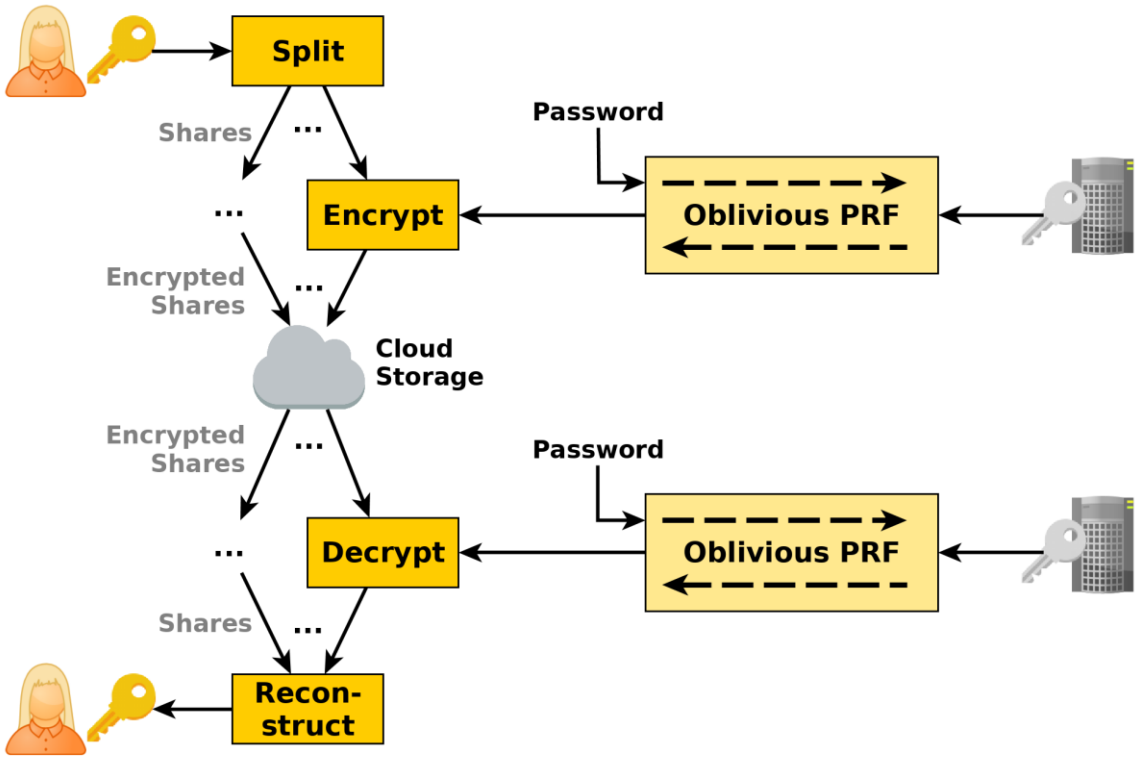


Implementation

- **Convincing organisations to operate servers**
  - **Incentives**
    - National or non-profit organizations: for the common good
    - Companies: grateful for their help in recovery
  - Minimize **effort** for server operators
    - Little storage and computation costs
  - ➢ Select suitable PPSS scheme

- **Support hierarchy in PPSS**
  - ➢ Extend scheme to introduce hierarchical PPSS

Selected PPSS Scheme: Abdalla et al. [ACNP16]

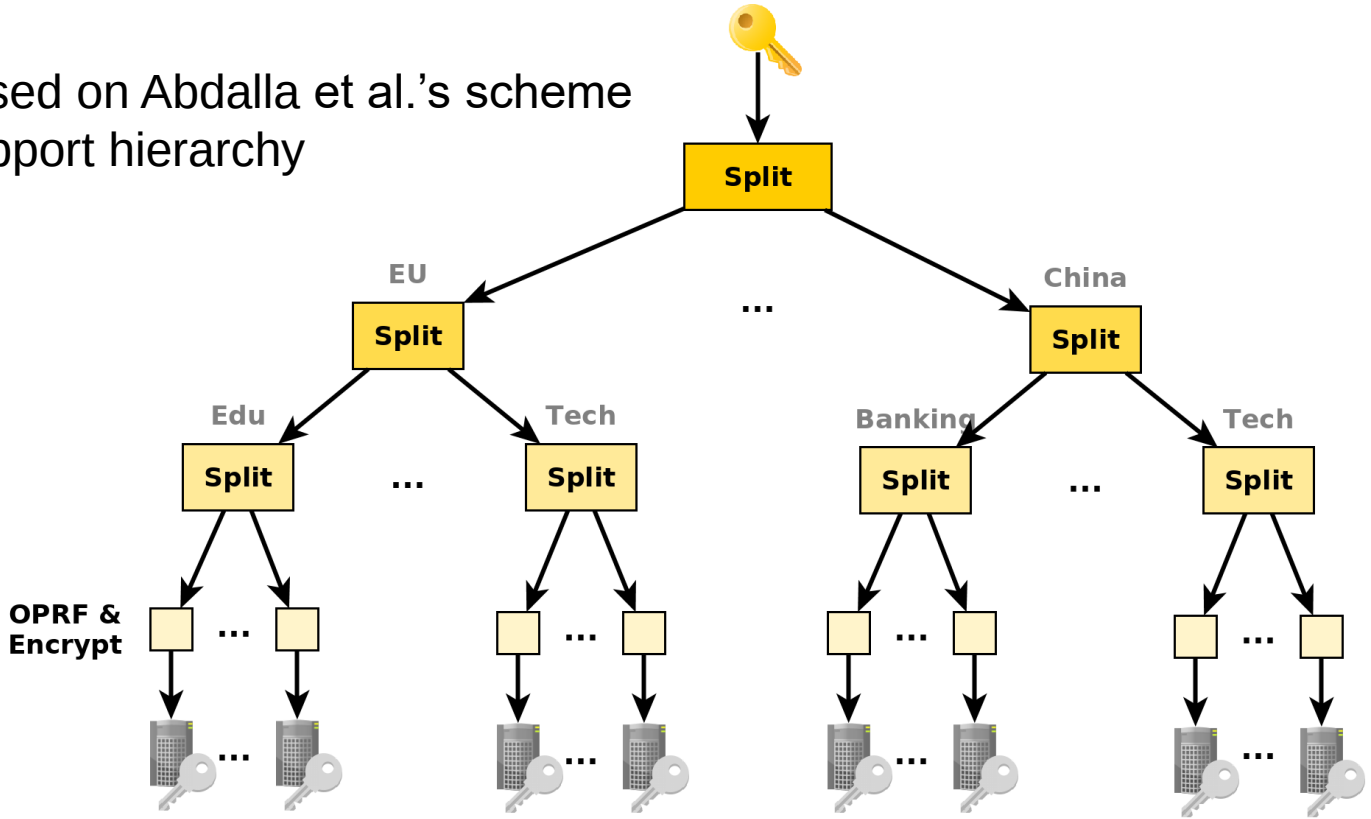


- **User/Cloud**: stores encrypted shares
- **Server**: only stores key

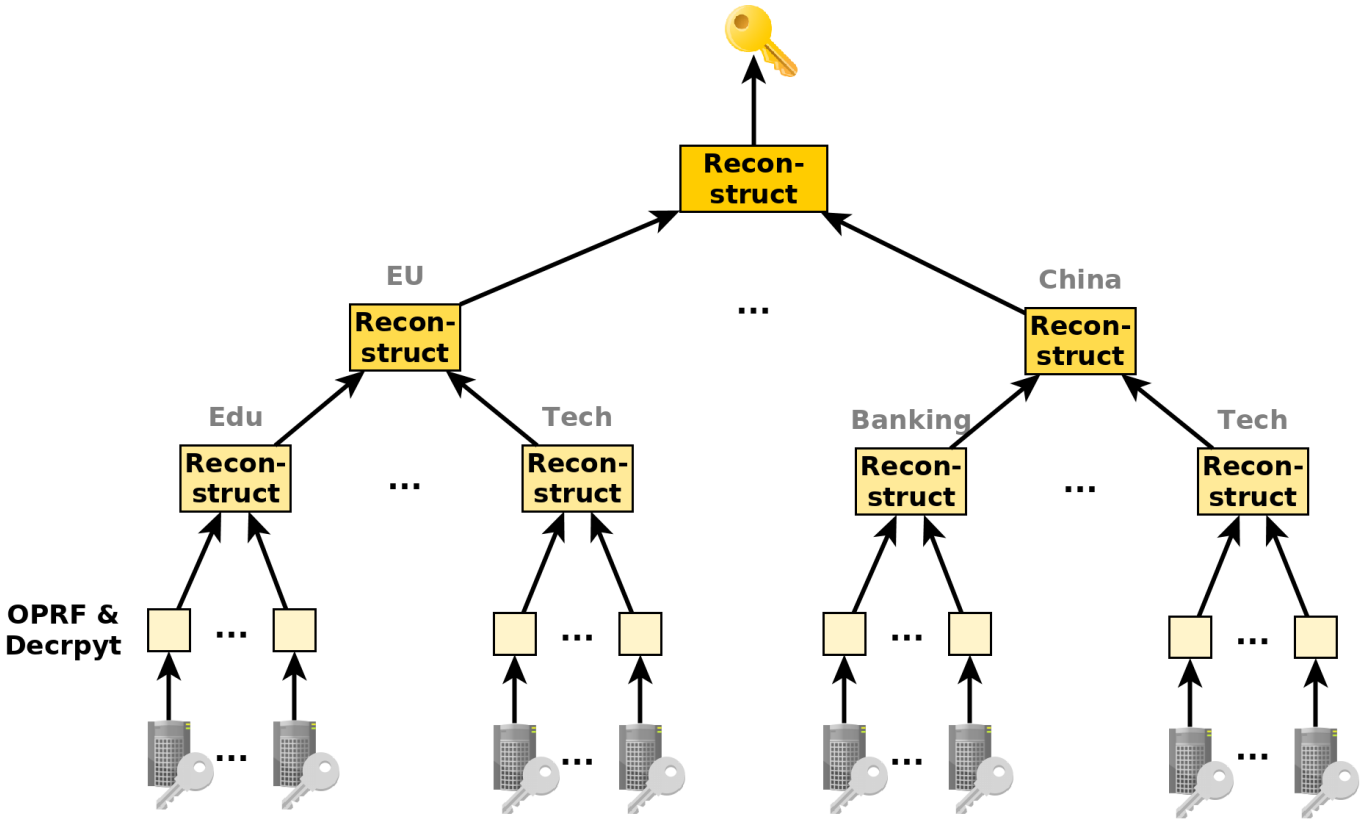
[ACNP16] Michel Abdalla, Mario Cornejo, Anca Nitulescu, David Pointcheval: Robust Password-Protected Secret Sharing. ESORICS 2016

Hierarchical PPSS: Split

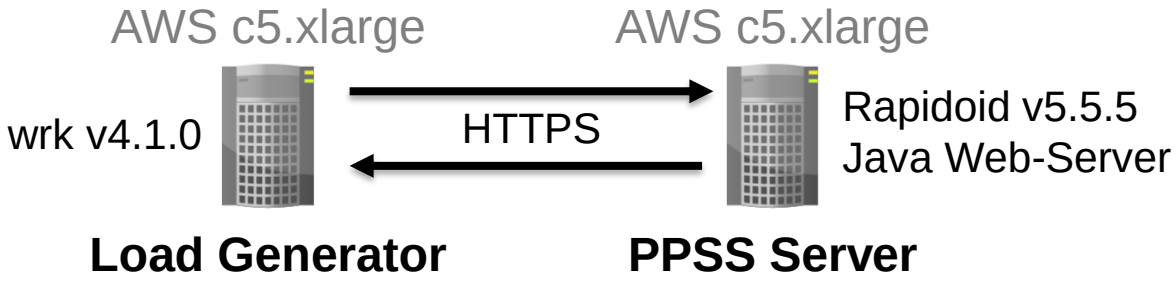
- Based on Abdalla et al.'s scheme
- Support hierarchy



Hierarchical PPSS: Reconstruct



Benchmark



	1 Server Measured	40 Servers Scaled	Price	Total
Operations	5.23 M	100.00 M		
Computation	1.00 h	31.89 days	0.194 $/h	$148.49
Traffic Out	8.55 GB	6.09 TB	0.090 $/GB	$548.47
Table Storage	88.84 MB	63.33 GB	0.100 $/GB	$6.33
Static Storage	1.00 GB	40.00 GB	0.100 $/GB	$4.00
				$707.28

- <20$ per organization

Summary: Key Messages

- **Recovery from key-loss based on PPSS**
  - Memorisable passwords but still resistant to offline guessing
  - Addresses challenges when applying PPSS in practice
- **Framework**
  - Supports users to reach trust decisions and understand impact of changes
  - Trust hierarchy: local, social, and remote organizations
  - App and recommender: create and manage trust hierarchy
- **Implementation**
  - Feasibility: extended Abdalla's PPSS scheme to add trust hierarchies
  - Convincing organizations: evaluated costs for large-scale deployment
    - Consortium of 40 organizations
    - 100 million split or recovery operations ➢ less than $20 per organization

Thank you! Any Questions?