CSE 539: Applied Cryptography
Lec 3: Secret Sharing

Ni Trieu (ASU)

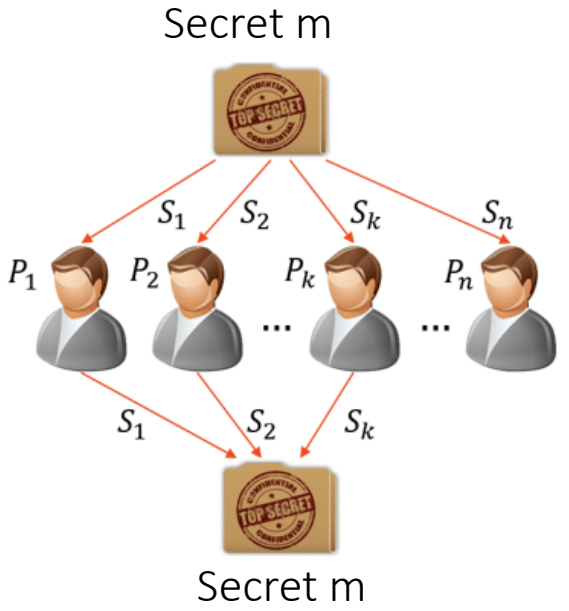
Outline

- General Secret Sharing and Examples
- Applications of Secret Sharing
- Constructions
  - “One-time Pad”?
  - Threshold Secret Sharing (Shamir, Blakely 1979)
- Issues

General Secret Sharing

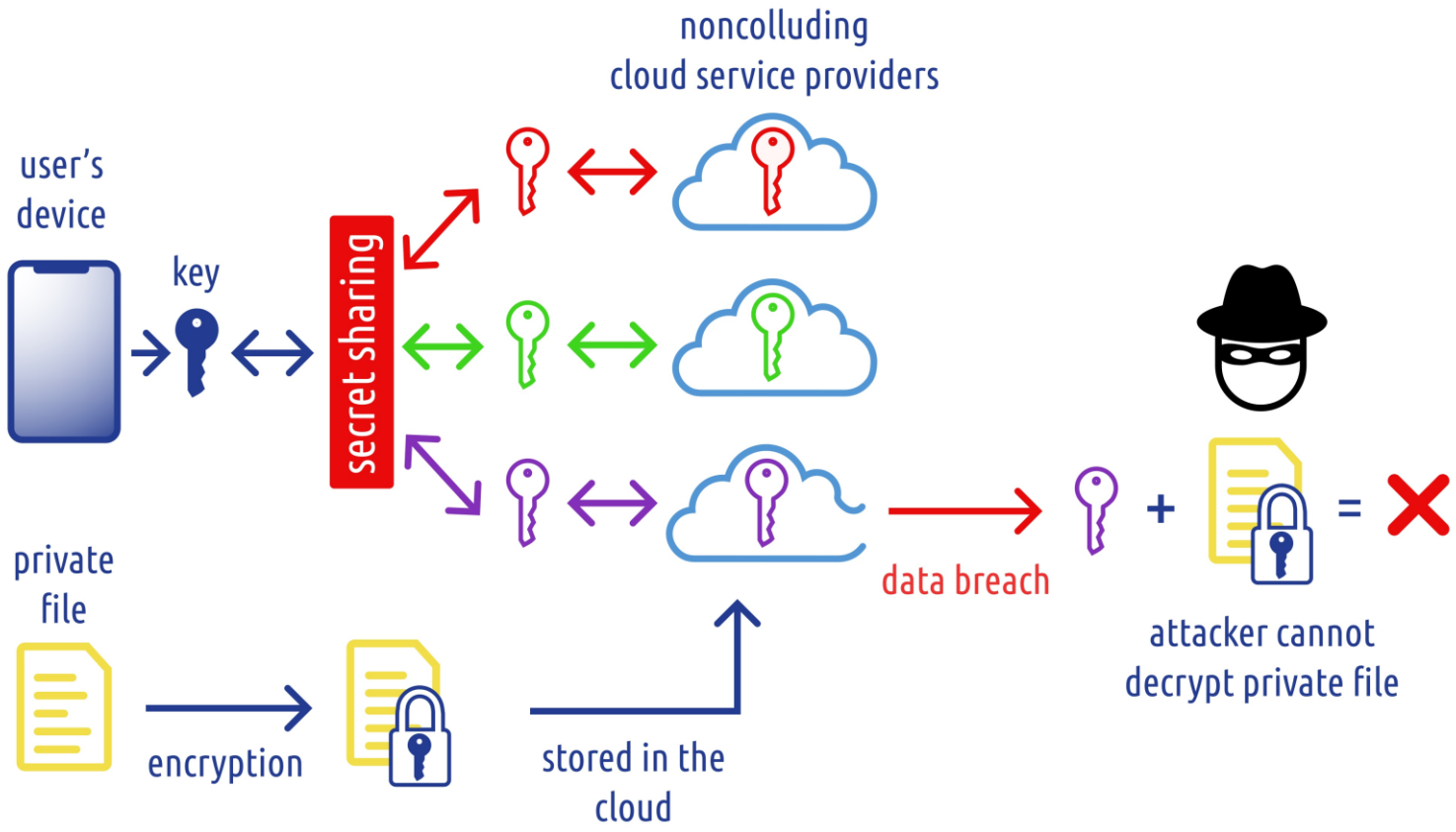
- m – Secret to be shared
- P – Set of participants

=> A qualified subsets of can reconstruct m



- Formally, secret sharing scheme allows share a secret m among n parties such that for a fixed number t < n, the following conditions are satisfied.
  - If < t parties get together, then they get no additional information about the secret.
  - If > t parties get together, then they can correctly reconstruct the secret

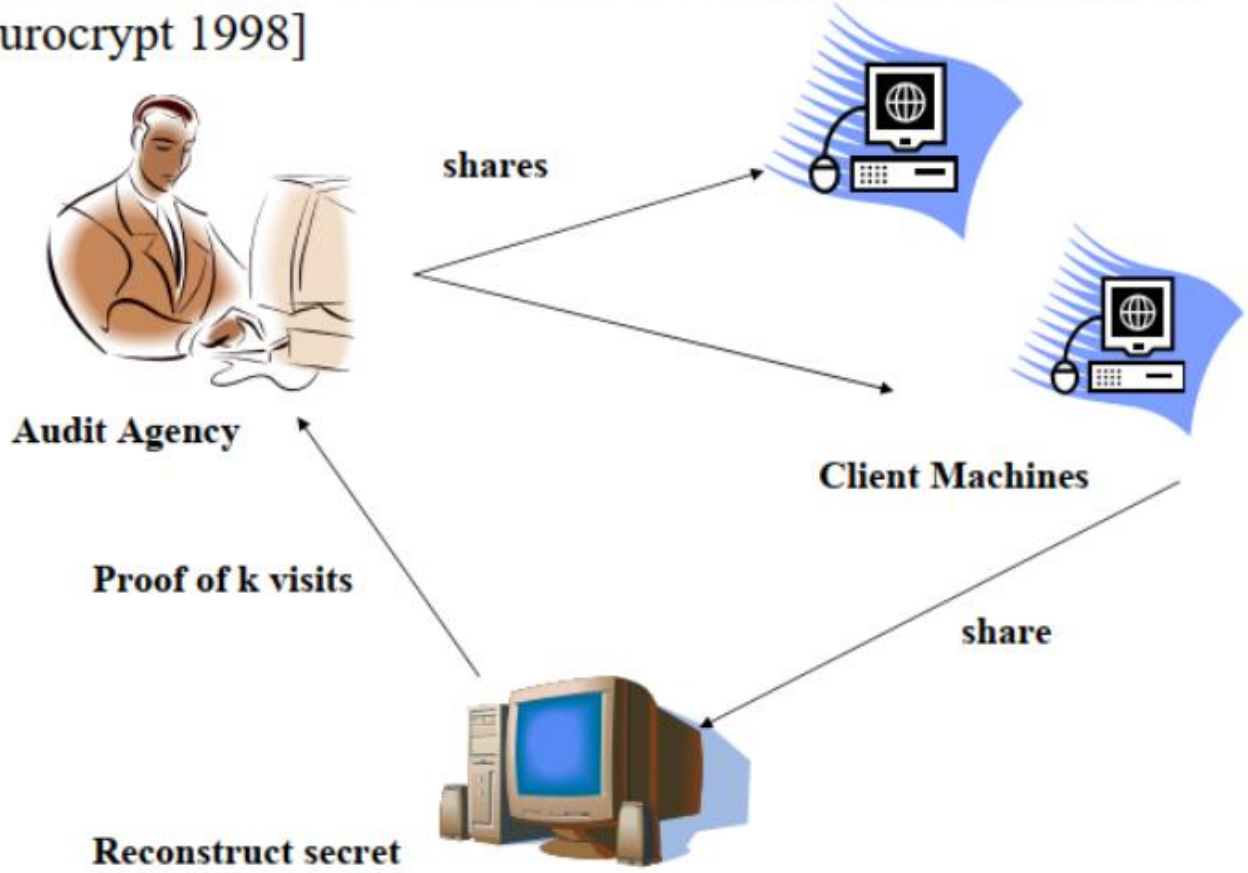
Applications of Secret Sharing



Practical Use of Secret Sharing for Enhancing Privacy in Clouds

Applications of Secret Sharing

Secure and Efficient Metering [Naor and Pinkas, Eurocrypt 1998]



Applications of Secret Sharing

- Threshold Signature Sharing
- RSA Signatures
- …

Outline

- ~~General Secret Sharing and Examples~~
- ~~Applications of Secret Sharing~~
- Constructions
  - “One-time Pad”?
  - Threshold Secret Sharing (Shamir, Blakely 1979)
- Issues

Basic Solution of Secret Sharing

- OTP?

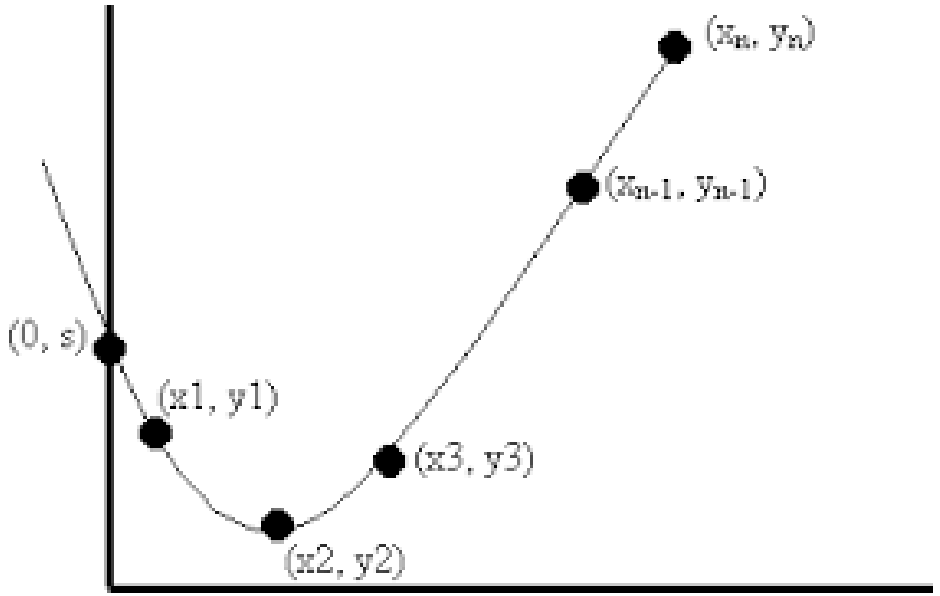
Shamir's Secret Sharing

t-out-of-n secret sharing

$\mathcal{M} = \mathbb{Z}_p$
$p : prime$
$n < p$
$t \leqslant n$

Share(m):
$f_1, \ldots, f_{t-1} \leftarrow \mathbb{Z}_p$
$f(\boldsymbol{x}) := m + \sum_{j=1}^{t-1} f_j \boldsymbol{x}^j$
for $i = 1$ to n:
$s_i := (i, f(i) \,\%\, p)$
return $\boldsymbol{s} = (s_1, \ldots, s_n)$

Reconstruct($\{s_i \mid i \in U\}$):
$f(\boldsymbol{x})$:= unique degree-$(t-1)$ polynomial mod p passing through points $\{s_i \mid i \in U\}$
return $f(0)$



https://joyofcryptography.com/pdf/chap3.pdf

Shamir's Secret Sharing

- Example: Suppose the secret being shared is m = 7, construct 3-out-of-5 secret sharing over Z_{11}.

Shamir’s Secret Sharing

- Sample quiz: Suppose that the secret is m = 7. Which of the following shares are valid in 3-out-of-5 secret sharing scheme

❑(1,1), (2,8), (5,8)

❑(1,1), (2,8), (3,5)

❑(1,1), (2,8), (6,9)

❑(2,8), (3,6), (4,6)

Shamir's Secret Sharing

- n users have shared two secrets using Shamir secret sharing.
  - User i has a share $s_i = (i, y_i)$ of the secret m, and a share $s_i{}' = (i, y_i{}')$ of the secret m'. Both sets of shares use the same prime modulus p, and have the same threshold
- Suppose each user i locally computes $z_i = (y_i + y_i')\%p$
- Are the resulting $\{(i, z_i), i \leq n\}$ a valid secret-sharing of the secret m+m'?

Outline

- ~~General Secret Sharing and Examples~~
- ~~Applications of Secret Sharing~~
- ~~Constructions~~
  - ~~"One-time Pad"?~~
  - ~~Threshold Secret Sharing (Shamir, Blakely 1979)~~
- Issues

Issues

- Honest dealer assumed
- Verifiable Secret Sharing schemes tolerate a faulty dealer
  - Security is computational