Unconditionally-Secure Robust Secret Sharing with Minimum Share Size

Rei Safavi-Naini and Mahabir P. Jhanwar
University of Calgary, Canada

Financial Cryptography 2013

Outline of the talk

- Secret Sharing
- Robust Secret Sharing
- Proposed Scheme
- Comparing with Existing Constructions
- Concluding Remarks

(t, n)-threshold Secret Sharing

- **Secret Sharing:**

$$s \xrightarrow{\text{Share Distribution}} s_1, s_2, \dots, s_n \xrightarrow[\text{any } t+1 \text{ shares}]{\text{Reconstruction}} s$$

- **Privacy (Perfect) :** t shares gives no information about s

$$s_{i_1}, \dots, s_{i_t} \xrightarrow{\text{unlimited adversary}} ?$$

Example (Shamir Secret Sharing)

- **Secret:** $s \in \mathbb{F}$.
- $f(x) = s + a_1x + a_2x^2 + \cdots + a_tx^t \in \mathbb{F}[x]$.
  Shares: $s_1 = f(1), s_2 = f(2), \dots, s_n = f(n)$
- **Privacy** and **Reconstructability**: use Lagrange Interpolation.

Efficiency Parameters

- **Information Rate:** $\rho = \min\left\{\frac{\log_2 s}{\log_2 s_i} : 1 \leq i \leq n\right\}$.
- Perfect secret sharing, $\rho \leq 1$
  - share size $\geq$ secret size
- **Ideal Secret Sharing:** $\rho = 1$
- Shamir secret sharing scheme is ideal.

Robust Secret Sharing

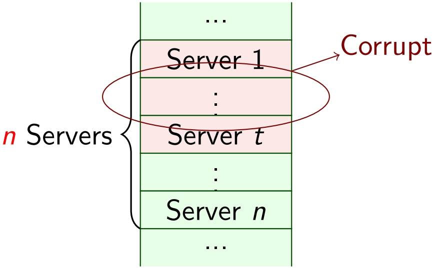
Active corruption: participants modify submitted shares.

- **Robust Reconstruction:** up to t shares are faulty

$$s'_{i_1}, \ldots, s'_{i_t}, s_{t+1} \longrightarrow s'$$
$$s'_{i_1}, \ldots, s'_{i_t}, s_{t+1}, \ldots, s_n \longrightarrow s$$

Application: Secure Data Storage

- Data file $\longrightarrow$



- Robust Reconstruction $\longrightarrow$ Data file

Application: Constructing Robust Primitives

- Building block of other robust crypto primitives:
  Secure Message Transmission
  Secret Sharing with Cheater Detection/Identification
  Verfiable Secret Sharing
  Multiparty Computation

Robust Secret Sharing

Algorithms

- Share: Dealer $\mathcal{D}$: For a secret $s \in \mathcal{S}$,
  - Generates $\sigma_1, \ldots, \sigma_n$
  - Privately gives σ_i to P_i.
- Rec: Reconstructor $\mathcal{R}$
  - Receives σ_i from P_i, $\forall i$
    (possibly several communication rounds),
  - Produces an output s'.

Security

- Privacy: No information about s is leaked during Share.
- δ – Reliability: $\Pr(s' = s) \geq 1 - \delta$.

Rushing vs Non-Rushing

- Rushing adversary sees other shares before choosing the wrong shares:
  Rushing adversary can know the secret.

Cost of Robustness

- Depends on t and n:

$$1 \underbrace{\qquad\qquad\qquad\qquad}_{t<n/3} \Big| \underbrace{\qquad\qquad}_{n/3 \leq t < n/2} \Big| \underbrace{\qquad\qquad\qquad\qquad\qquad}_{t \geq n/2} n$$

  - $t < n/3$: Robustness is for free!
    - Shamir secret sharing is robust: reconstruction is Reed-Solomon decoding.
  - $t \geq n/2$: Robust secret sharing is not possible.
  - $n/3 \leq t < n/2$:
    - $\delta > 0$.
    - Existing constructions have increased share size .

Approaches to Providing Robustness

- Known approaches:
  1. $\sigma_i = \{\text{share of } s, \text{additional info}\}$
     Additional info is used for verifying others' shares.
  2. $s.r = \rho$
     Share three elements satisfying a relation.
- Our approach: Use the share of one extra honest participant.
  $\rightarrow n = 2t + 2$.
  - For n even, this is the minimum.
    For n odd, one extra participants.

Proposed Scheme

- Share:
  - $s \in \mathbb{F}_q$, $f(x) \in_R \mathbb{F}_q^{\leq t}[x]$, $f(0) = s$.
  - Find $s_i = f(i), \ \forall i \in [t+1]$.
  - $\forall i \in [n]$, choose $(r_{i1}, \ldots, r_{i(t+1)}) \in (\mathbb{F}_q)^{t+1}$, such that: *any $t+1$ vectors are linearly independent.*
  - $\forall i \in [n], \ \sigma_i = \sum_{j=1}^{t+1} r_{ij} s_j$. $\sigma_i \to P_i$
- Rec:
  - $\forall P_i : \sigma_i \to \mathcal{R}$
  - For every subset of $t+1$ players, $\mathcal{R}$ does the following:
    - Reconstruct $(s_1', s_2', \ldots, s_{t+1}')$ using $t+1$ shares.
    - Accept if $\sum_{j=1}^{t+1} r_{ij} s_j' = \sigma_i$ for at least one more share.
  - Use $t+1$ shares to find $f(x) \in \mathbb{F}_q^{\leq t}[x]$, $s = f(0)$.

Proposed Scheme

- **Share:**

$$s \in \mathbb{F}_q$$

$$\downarrow \text{Shamir Sharing}$$

$$(s_1, \ldots, s_{t+1})$$

$$\downarrow \text{taking linear combinations}$$

$$\begin{bmatrix} r_{11} & \cdots & r_{1(t+1)} \\ r_{21} & \cdots & r_{2(t+1)} \\ \vdots & \vdots & \vdots \\ r_{n1} & \cdots & r_{n(t+1)} \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{t+1} \end{bmatrix} = \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_n \end{bmatrix}$$

- **Rec:** Loop over every $t+1$ shares.

$$(\sigma_1, \ldots, \sigma_t, \sigma_{t+1}, \ldots, \sigma_i, \ldots, \sigma_j, \ldots, \sigma_n)$$

Constructing Shares

- n vectors such that any $t+1$ of them are L.I:
  1. Choose $z_1, \ldots, z_n, w_1, \ldots, w_{t+1} \in \mathbb{F}_q$ with $z_i + w_j \neq 0$. Define
  $$r_i = \left(\frac{1}{z_i + w_1}, \ldots, \frac{1}{z_i + w_{t+1}}\right), \; 1 \leq i \leq n \;\; .$$
  There are $n + t + 1$ random elements.
  2. Use a $n \times (t+1)$ Vandermonde matrix.
  n random elements.
  $\rightarrow$ The scheme has $O(n)$ field elements as public values.
  $n \geq 2t + 2$

Security

- **Privacy**

Theorem

Any t shares gives no information about the secret (information theoretic).

- **Reliability**

Theorem

For $n, t \in \mathbb{N}$ such that $n = 2t + 2$, $\mathbb{F}_q$ with $k = \lceil \log_2 q \rceil$, the pair $(\mathrm{Share}, \mathrm{Rec})$ *forms an n-player (t, δ)-robust secret sharing against non-rushing adversary. Message space is $\mathbb{F}_q$, and*

$$\delta \leq \frac{\sqrt{t+1}}{2^{k-n}} \quad .$$

Comparison with Existing Schemes

Let secret size be k bits.

- Cramer, Damgård and Fehr (01), Cabello et. al. (99)
  - Share size $= 3k$ bits.
  - Reconstruction: exponential in n.
  - $n \geq 2t + 1$.
- Cevallos, Fehr, Ostrovsky and Rabani (12), Rabin et. al. (89)
  - Share size $= k + 3n\frac{k}{\lambda}$ bits.
  - Reconstruction: polynomial in n.
  - $n \geq 2t + 1$.

- Our Construction
  - Share size $= k$ bits. (Ideal)
  - Reconstruction: exponential n.
  - $n \geq 2t + 2$.

Concluding Remarks

- Proposed an ideal RSSS for $n \geq 2t + 2$.
  - Idea: use one extra honest participant share for verification.
  - Reconstruction: exponential.
  - Security against non-rushing adversaries.
- Can be extended to general access structure.

- Open questions:
  - Efficient reconstruction.
  - ideal schemes for $n = 2t + 1$.