A Survey and Refinement of Repairable Threshold Schemes

Thalia M. Laing and Douglas R. Stinson

Presented by Chelsea H. Komlo

Motivation

- Survey of existing repairable threshold schemes (RTSs)
- Introduce computational and efficiency improvements to several RTSs

Focus on Enrolment protocol

- The paper presents multiple schemes
- Here, we'll focus mainly on the Enrolment scheme

Overview

1. Background
2. Introduction to Repairable Threshold Schemes
3. Naive Repairable Threshold Scheme solution
4. Enrolment Scheme and analysis
5. Reduced Enrolment Scheme and analysis

Threshold schemes

Definition

Suppose t and n are positive integers such that $2 \leq t \leq n$. A (t, n)-threshold scheme is a method in which a dealer chooses a secret s and distributes a share to each of the n players such that the following properties are satisfied:

- Recoverability: any subset of t players can compute the secret from the shares they collectively hold, and
- Secrecy: no subset of fewer than t players can determine any information about the secret

Threshold schemes algorithms

Consists of two algorithms:

- A **Share** algorithm run by the dealer that receives as input the secret s and parameters t, n and outputs n shares, and
- A **Recover** algorithm, which receives as input at least t distinct, valid shares and outputs the secret.

Shamir secret sharing

For a given secret $s \in \mathbb{Z}_p$, the Share and Recover algorithms are as follows:

- **Share**: Select $t - 1$ values $r_1, r_2, \ldots, r_{t-1} \in \mathbb{Z}_p$ uniformly at random, and let f be the polynomial of degree at most $t - 1$ defined by:

  $$f(x) = r_{t-1}x^{t-1} + r_{t-2}x^{t-2} + \cdots + r_1 x + s$$

  The dealer gives each player P_i the share $v_i = f(i)$

- **Recover**: A collection of t or more players perform polynomial interpolation on their shares to recover the polynomial f and determine the secret corresponding to the constant term $s = f(0)$.

Background: Lagrange Interpolation

Shares in Shamir secret sharing $f(x_0), \ldots, f(n)$ can be characterized as follows:

$$f(x_k) = \sum_{i=1}^{t} (\prod_{1 \leq j \leq t, i \neq j} \frac{x_k - x_i}{x_i - x_j} \cdot f(x_i))$$

Where x_k is the target value to find the corresponding $f(x_i)$, and $\frac{x_k - x_i}{x_i - x_j}$ is the Lagrange interpolation constant.

For Shamir secret sharing, this can be used to recover the secret, which is the constant term $(0, f(0))$.

Repairable Threshold Schemes (RTSs)

- RTSs are threshold schemes that enable a player to securely reconstruct a lost share.
- Repairability is a useful attribute when a player in a (t, n)-threshold scheme loses or corrupts their share and wishes to repair it.
- Not bound to the dealer to perform a repair- the repairing participant P_r can enlist their peers.
- Universal versus Restricted Repairability
  - Universal: Any participant can help in the repair for any other participant
  - Restricted: Only a subset of all participants can help

Security for RTSs

1. Assume a passive adversary that is honest-but-curious
2. Want P_r to be able to repair their share, but not reveal any information about the secret s.

(t, n, d)-Repairability Threshold Scheme

- Let $d \in \mathbb{N}, t \leq d \leq n - 1$, where d is the repairing degree.
- A (t, n, d)*-threshold scheme* is defined by a **Repair** algorithm, as well as **Share** and **Recover** algorithms.
- The Repair algorithm allows a repairing player P_r to securely reconstruct their share with help from a set of d helping players.
- Additionally, the Repair algorithm could allow for adding *new* players, by extending the set to $n + 1$ players.

Bounds on RTSs

Bounds for the number of required helping players d

- **Lower Bound.** $t \leq d$

  If fewer than t players could reconstruct a share, they could iterative mint t shares and recover secret without performing the Recover algorithm.

- **Upper Bound.** $d \leq n - 1$

  If one player lost their share, then there would be $n - 1$ remaining players who could help recover the share.

Efficiency metrics to Evaluate RTSs

1. **Information rate**. The amount of information each player is required to store compared to the size of the secret.

2. **Communication complexity** The amount of bandwidth required for each execution of the repair algorithm.

3. **Repairability**. The ratio of d-subsets from the $n-1$ players that can help a repairing player P_r repair their share compared to all possible d-subsets.

4. **Computational complexity**. The computational complexity of the share, recover, and repair algorithms.

Naive RTS solution

- Split each share using a (d, n)-threshold scheme, and distribute the "shares of shares" to all other players.
- Each player stores one share for the secret s protected by the threshold scheme, and also $n - 1$ "shares of shares" for other players.
- To recover a share, a player performs the Recover algorithm, requesting their corresponding sub-share from at least d other players.

Naive RTS solution analysis

- **Communication Complexity:** To perform a repair, d messages must be sent from each helping participant to P_r.
- **Information rate**: Each player is required to store n shares. One share to use when performing the Recover algorithm for s, and $n-1$ "shares of shares" to help other players recover lost shares.

Enrolment scheme

- Share and Recover algorithms are the same as Shamir secret sharing
- Within the Repair algorithm, any participant can help a peer recover a lost share without revealing their own share in the process.
- Enrolment RTS is a *oblivious protocol*, meaning the decision for player P_i to send a message to P_j in round h is determined by i, j, k (does not depend on input or random coins).

Enrolment scheme: High level intuition

Assume $d = t$, and $f \in \mathbb{Z}_q[x]$ is a polynomial of degree at most $t-1$ whose constant term is s.

A share ϕ_r can be expressed as:

$$\phi_r = \sum_{i=1}^{t} \zeta_i \phi_i$$

Where ζ_i is the public Lagrange coefficients of P_i,

We can use this to define a Recover mechanism for an individual share.

Enrolment Scheme: Repair Algorithm

1. Every helping player P_i computes t random values $\delta_{j,i}$ for $1 \leq j \leq t$, such that:

   $$\zeta_i, \phi_i = \sum_{j=1}^{t} \delta_{j,i}$$

   This effectively "splits" ϕ_i into t portions.

2. Participants exchanges the $\delta_{j,i}$ values to all other players $1 \geq j \geq t,\ j \neq i$ via a pairwise exchange.

3. All players P_j sum their received values: $\sigma_j = \sum_{i=1}^{t} \delta_{j,i}$

4. P_j transmits σ_j to P_r, the player whose share requires recovery.

5. P_r computes their share by adding the received σ_j values.

   $$\phi_r = \sum_{j=1}^{t} \sigma_j$$

Enrolment Scheme analysis

1. **Information rate.** Optimal, as each player is required to only store their own share.

2. **Communication complexity.** Requires t^2 information to be transmitted relative to the secret size.
   - 2.a Step 2, each player sends one messages to $t - 1$ other players, resulting in $t(t - 1)$ messages
   - 2.b Step 4, t players sends one message to the repairing player P_r

Enrolment Scheme analysis (cont'd)

3. **Repairability.** Universally repairable inheriting from Shamir threshold scheme (any share can be used in combination with any other share)

4. **Computational complexity.** In total, $2t^2 - t - 1$ modular additions are required
   - 4.a Helping players computes $2(t - 1)$ additions.
   - 4.b Repairing players computes $t - 1$ additions.

Reduced Enrolment Scheme

1. Every player computes t random values $\delta_{j,i}$ for $1 \leq j \leq t$, such that:
$$\zeta_i, \phi_i = \sum_{j=i}^{t} \delta_{j,i}$$
2. For all $1 \leq i \leq t, i \leq j \leq t$, player P_i transmits $\delta_{j,i}$ to P_j
3. For all $1 \leq j \leq t$, player P_j computes
$$\sigma_j = \sum_{i=j}^{t} \delta_{j,i}$$
4. For all $1 \leq j \leq t$, player P_j transmits σ_j values to P_r
5. P_r computes their share
$$\phi_r = \sum_{j=1}^{t} \sigma_j$$

Reduced Enrolment Scheme Analysis

1. **Information rate.** Same as for the Enrolment Scheme, each player stores one share.

2. **Communication complexity.** Improvement as requires $\frac{t(t+1)}{2}$ relative to secret size.

3. **Repairability.** Same as for Enrolment Scheme, every share can be used to repair every other share.

4. **Computational complexity.** Improvement as requires $\frac{t(t+1)}{2}$ modular additions.

Optimal communication complexity of the Reduced Enrolment Scheme

- **Communication complexity**: Any scheme where a $t+1$th player computes the sum of t players values is lower-bounded by $\frac{t(t+1)}{2}$ messages sent (relative to size of secret).

- **Obliviousness**: The t-player coalition should not learn the other players' shares or the sum of shares. (cannot learn inputs to the sum and the output).

- **Security**: In the graph where nodes are $\zeta_i\phi_i$ shares and edges are players sending values corresponding to the share to each other, this graph must be a fully-connected clique and every node must have degree t. Knowledge of all inputs/outputs to a vertex will uniquely define the share.

Takeaways

- Repairable secret sharing schemes can be highly beneficial in a real-world setting due to the chance of share loss or damage.
- The Enrolment Scheme provides a Repair algorithm that is compatible with the Share and Recover algorithms in Shamir secret sharing.
- The communication complexity of the Enrolment scheme is high considering the number of exchanges players must perform.