Combinatorial Repairability for Threshold Schemes

Douglas R. Stinson, Ruizhong Wei

Presented by: Kyle Tilbury
July 3, 2019

Repairability

- ➔ Suppose some person loses their share in a (k, n)-threshold scheme
- ➔ Want a way to securely reconstruct (or repair) that person's lost share without revealing any additional information about the secret
- ➔ This paper presents two repairability schemes:
  1. Enrollment protocol based
  2. Combinatorial

Secret Sharing Threshold Schemes

- (k, n)-threshold scheme
  - k and n are positive integers where $k \leq n$
  - k is the **threshold**
  - n participants, denoted $P_1, \ldots, P_n$
  - There exists a **dealer** who is some trusted authority that splits some secret value K into n **shares**, $s_1, \ldots, s_n$
  - Each share s_i is distributed to participant P_i in a secure manner
- Two properties must hold:
  1. The secret can be reconstructed given any k of the n shares
  2. Any $k-1$ or fewer shares reveal no information about the secret

Ramp Schemes

- ➔ (k_1, k_2, n)-ramp scheme
  - ◆ k_1 is the **lower threshold**
  - ◆ k_2 is the **upper threshold**
  - ◆ When $k_2 = k_1 + 1 = k$, a ramp scheme is equivalent to a (k, n)-threshold scheme

- ➔ Two properties must hold:
  1. Any subset of k_2 players can compute the secret from the shares they collectively hold
  2. No subset of k_1 players can determine any information about the secret

Motivation for Ramp Schemes

- ➔ Efficiency of secret sharing is often measured in **information rate**
  - Where $\mathcal{K}$ is the set of all possible secrets and $\mathcal{S}$ is the set of all possible shares, information rate $\varrho = \log_2 |\mathcal{K}| / \log_2 |\mathcal{S}|$
  - This is the ratio of the size of the secret to the size of the share
- ➔ A fundamental property of a (k, n)-threshold scheme is $|\mathcal{K}| \leq |\mathcal{S}|$, so $\varrho \leq 1$
  - For a Shamir threshold scheme $|\mathcal{K}| = |\mathcal{S}|$, so $\varrho = 1$
  - $\varrho = 1$ is the optimal informate rate for a threshold scheme
- ➔ Ramp schemes permit larger secrets to be shared for a given share size
  - For (k_1, k_2, n)-ramp schemes there are constructions where the optimal information rate $\varrho = k_2 - k_1$
  - $\varrho > 1$ information rate is possible for a non-threshold ramp scheme

Repairable Schemes

- ➔ Share Repairability
  - Repairable Threshold Schemes
  - Types of Repairability
- ➔ Two types of schemes
  1. Enrollment
  2. Combinatorial

Share Repairability

- ➔ A participant P_ℓ has lost their share s_ℓ
- ➔ Goal is to have a secure protocol involving P_ℓ and a subset of other participants that allows s_ℓ to be reconstructed
- ➔ Two assumptions:
  1. the dealer is no longer present in the scheme after the initial setup
  2. there exist secure pairwise channels linking pairs of players

Share Repairability

➔ A (k, n, d)-repairable threshold scheme, or (k, n, d)-RTS, is a protocol that operates in two phases:

1. **Message exchange phase:**
   - A certain subset of d participants (not including P_i) exchange messages among themselves
   - This integer d is called the **repairing degree** ($d \geq k$ is a necessary condition)
   - Only protocols where each participant sends at most one message to any other participant and where every message is sent at the same time are considered
2. **Repairing phase:**
   - The same d participants each send a message to P_i
   - Messages received by P_i allow s_i to be reconstructed

Types of Repairability

1. Universal Repairability
    - Any subset of *d* participants can repair a share of any other player

2. Restricted Repairability
    - There exists a subset of *d* participants who will be able to repair a given share belonging to some other player
    - Potential advantage is that it can lead to more efficient schemes (in terms of info rate and/or communication complexity)
    - Potential disadvantage is that some of the *d* participants may be unavailable, rendering the repair impossible

Enrollment Protocol

- Recall the **enrollment protocol** from an earlier talk in this course
  - Was introduced to create a share for a new participant in a threshold scheme without requiring the dealer who initially set up the scheme
- Enrollment protocol as a (k, n, k)-RTS
  - Suppose we have a scheme defined over a finite field of order Q, denoted $\mathbb{F}_Q$
  - Participants $P_1, \ldots, P_k$ want to reconstruct the share for participant P_ℓ where $\ell > k$
  - The share for P_ℓ is $s_\ell = f(\ell)$
  - The share s_ℓ can be expressed as:

$$s_\ell = \sum_{i=1}^{k} \gamma_i s_i$$

where the γ_i's are public Lagrange coefficients

Enrollment Protocol for Repair

The enrollment protocol repair process would proceed as follows:

Message Exchange Phase

1. For all $1 \le i \le k$, participant P_i computes random value $\delta_{j,i}$ for $1 \le j \le k$ such that

$$\gamma_i s_i = \sum_{j=1}^{k} \delta_{j,i}$$

2. Then, for all i, j, participant P_i transmits $\delta_{j,i}$ to participant P_j

Repairing Phase

3. For all j, participant P_j transmits σ_j to participant P_ℓ, where

$$\sigma_j = \sum_{i=1}^{k} \delta_{j,i}$$

4. Finally, the participant P_ℓ computes their share s_ℓ with

$$s_\ell = \sum_{j=1}^{k} \sigma_j$$

Things to Note - Enrollment Protocol for Repair

➔ This protocol achieves universal repairability

- Any subset of *d* participants can repair a share of any other player

➔ This protocol is secure against coalitions of size *k* - 1

➔ This protocol also works in the case of a ramp scheme

- I.e. protocol works similarly when using a ramp scheme instead of a threshold scheme

Combinatorial Scheme for Repair

➔ Combinatorial repairability method has two components:

1. Base Scheme
   - An underlying scheme used to give each participant multiple sub shares
   - Can use threshold schemes or ramp schemes
2. Distribution design
   - A combinatorial design which specifies what sub shares are given to a participant
   - Can use:
     - Steiner Triple Systems
     - BIBD with $\lambda = 1$
     - Projective Planes

Combinatorial Repair Example - (2, 7, 3)-RTS

Example of a **(2, 7, 3)-RTS**

➔ Distribution design

- Start with a (7, 3, 1)-BIBD which has seven blocks
- This design is public
- Associate a block with each participant:

$P_1 \leftrightarrow 123$ $P_3 \leftrightarrow 167$ $P_5 \leftrightarrow 257$ $P_7 \leftrightarrow 356$
$P_2 \leftrightarrow 145$ $P_4 \leftrightarrow 246$ $P_6 \leftrightarrow 347$

➔ Base scheme

- Construct a (5,7)-threshold scheme
- The shares from the base scheme are $s_1, s_2, \ldots, s_7$

Combinatorial Repair Example - (2, 7, 3)-RTS

- Distribution design:

$P_1 \leftrightarrow 123$ $P_3 \leftrightarrow 167$ $P_5 \leftrightarrow 257$ $P_7 \leftrightarrow 356$

$P_2 \leftrightarrow 145$ $P_4 \leftrightarrow 246$ $P_6 \leftrightarrow 347$

- Base scheme:
  - The shares from a (5,7)-threshold scheme are $s_1, s_2, \ldots, s_7$
- Each participant gets 3 shares from the base scheme
- The blocks in the distribution design list the indices of the sub shares from the base scheme held by each participant
- Expanded Scheme:

P_1's expanded shares are s_1, s_2, s_3

P_2's expanded shares are s_1, s_4, s_5

P_3's expanded shares are s_1, s_6, s_7

P_4's expanded shares are s_2, s_4, s_6

P_5's expanded shares are s_2, s_5, s_7

P_6's expanded shares are s_3, s_4, s_7

P_7's expanded shares are s_3, s_5, s_6

Combinatorial Repair Example - (2, 7, 3)-RTS

- Expanded Scheme:

  P_1's expanded shares are s_1, s_2, s_3

  P_2's expanded shares are s_1, s_4, s_5

  P_3's expanded shares are s_1, s_6, s_7

  P_4's expanded shares are s_2, s_4, s_6

  P_5's expanded shares are s_2, s_5, s_7

  P_6's expanded shares are s_3, s_4, s_7

  P_7's expanded shares are s_3, s_5, s_6

- The base scheme has a threshold of 5 and the resulting RTS has a threshold of 2

- Any two blocks contain at least 5 different sub shares
  - So any 2 users can reconstruct the secret since they have at least the threshold number of shares
  - Any 1 user has less than the threshold number of sub shares so they can learn nothing about the secret

Combinatorial Repair Example - (2, 7, 3)-RTS

P_1's shares are s_1, s_2, s_3

P_2's shares are s_1, s_4, s_5

P_3's shares are s_1, s_6, s_7

P_4's shares are s_2, s_4, s_6

P_5's shares are s_2, s_5, s_7

P_6's shares are s_3, s_4, s_7

P_7's shares are s_3, s_5, s_6

➔ Repairing process:

- When a participant wants to repair their share they would contact d=3 other participants
- If P_1 loses their share $\{s_1, s_2, s_3\}$
  - Can contact P_2 to recover their first sub share s_1
  - Can contact P_4 to recover their second sub share s_2
  - Can contact P_6 to recover their third sub share s_3
  - Then their share is recovered

Things to Note - Combinatorial Repairability

- ➔ This protocol achieves restricted repairability
  - I.e. There exists a subset of *d* participants who will be able to repair a given share belonging to some other player
  - Paper considers ways to achieve universal repairability
- ➔ Not every threshold (k, n) is possible
  - Reliant on the existence of combinatorial designs that support the threshold
  - Some tricks are possible (Ex. use a subset of blocks)
- ➔ Compared to a past scheme (GLF), the combinatorial construction presented improves in terms of information rate and communication complexity

Conclusion

- ➔ Presented two methods for repairing secrets in threshold schemes
- ➔ Identified constructions for combinatorial repairable threshold schemes
  - ◆ Suitable base schemes
  - ◆ Combinatorial designs for distribution designs
- ➔ Improved information rate and/or communication complexity over previous work in the area (in exchange for restricted repairability)
- ➔ Proposed possible ways to achieve universal repairability in the combinatorial repairable threshold schemes they introduced

References

- Stinson, Douglas R., and Ruizhong Wei. “Combinatorial repairability for threshold schemes.” Designs, Codes and Cryptography 86.1 (2018): 195-210.

- See also the talks from Douglas R. Stinson:
  - “Combinatorial techniques for repairing shares in threshold schemes” from Combinatorics 2018 in Arco, Italy, June 4, 2018
  - “A Combinatorial Design Method for Repairing Shares in Threshold Schemes” from Conference on Combinatorics and its Applications In Celebration of Charlie Colbourn’s 65th Birthday in Singapore, July 16, 2018