



**WICHITA STATE  
UNIVERSITY**

**UNIVERSITY LIBRARIES**

**Secure message communication via a  
relay using a secret sharing scheme**

Item Type	Thesis
Authors	Dodda, Srilekha
Publisher	Wichita State University
Rights	© Copyright 2023 by Srilekha Dodda All Rights Reserved
Download date	2026-05-17 07:15:27
Link to Item	<a href="https://soar.wichita.edu/handle/10057/25714">https://soar.wichita.edu/handle/10057/25714</a>

SECURE MESSAGE COMMUNICATION VIA A RELAY USING A SECRET SHARING  
SCHEME

A Thesis by

Srilekha Dodda

Bachelor of Science, Jawaharlal Technological University, 2021

Submitted to the Department of Computer Science  
and the faculty of the Graduate School of  
Wichita State University  
in partial fulfillment of  
the requirements for the degree of  
Master of Science

July 2023

© Copyright 2023 by Srilekha Dodda

All Rights Reserved

# SECURE MESSAGE COMMUNICATION VIA A RELAY USING A SECRET SHARING SCHEME

The following faculty members have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Computer Science.

---

Remi Chou, Committee Chair

---

Krishna Krishnan, Committee Member

---

Ed Sawan, Committee Member

## ABSTRACT

Secure message communication between the transmitter and the receiver checks integrity. It involves preserving the message content against unauthorized access. The designed application uses a Shamir secret sharing scheme, where a message can be split into shares. And the transmitter distributes each share to the receiver to reconstruct the message through the relays. In this process, the adversary might attack any of the relays to modify the share information and tries to obtain the original message. Where each share is produced by adding additional information to it also providing the identification protocol at the reconstruction phase to ensure the message integrity. At last, the receiver will perform an identification protocol to identify the authentic shares, if the shares are verified as authentic then the receiver will perform a reconstruction protocol to reconstruct the message.

# TABLE OF CONTENTS

Chapter	Page
1 INTRODUCTION	1
1.1 Organization	2
2 LITERATURE REVIEW	3
2.1 Secret Sharing	3
2.2 Cheaters in Secret Sharing Scheme	3
2.3 Security Guarantee	4
3 METHODOLOGY	5
3.1 Notations	5
3.2 Coding Scheme	6
3.2.1 Distribution and Reconstruction Phase	6
3.2.2 Identification and Reconstruction Protocol	7
4 RESULTS	9
4.1 Case 1: Analysis	9
4.2 Case 2: Analysis	9
5 CONCLUSION	11
BIBLIOGRAPHY	12

# CHAPTER I

## INTRODUCTION

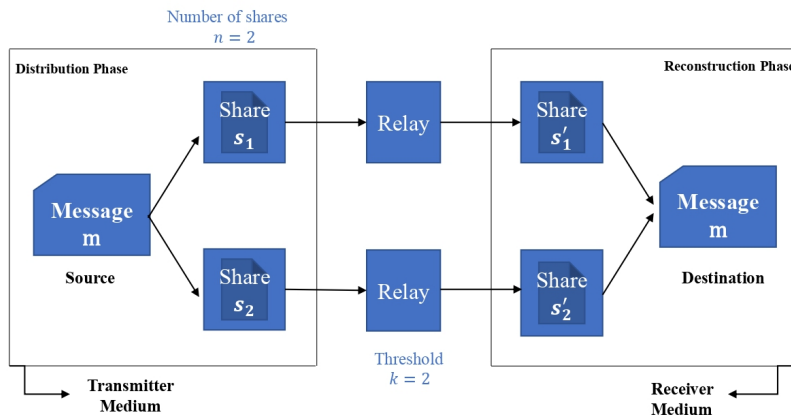


Figure 1: Message Transmission Via Relay

As in 1 Message Transmission Via Relay, we consider a message  $\mathbf{m}$  as a secret. Here, it consists of two phases one is distribution in the transmitter and the reconstruction phase in the receiver also relays. We used the secret sharing scheme in [1].

Firstly, the message can divide into two shares  $s_1$  and  $s_2$  using the secret sharing protocol. In addition, the toeplitz matrices were attached to each share along with the generated random numbers. The purpose of this additional information adding to each share is for security, which means if the adversary corrupts the relay, it is still hard to find the original message from the shares  $s_1$  and  $s_2$ . Next, the transmitter is going to send each share to the corresponding relays. Now each relay is going to send the received two shares

from the transmitter to each receive. And before the reconstruction of the message, the receiver will check whether the shares  $s'_1$  and  $s'_2$  are authentic or not using the identification protocol in [1]. The threshold  $k = 2$ , then the receiver going to reconstruct the message from shares  $s'_1$  and  $s'_2$  using the reconstruction protocol.

Then, we need to perform analysis to see the cases where any one share  $s'_1$  or  $s'_2$  is modified by the adversary and no shares are modified, that are going to be detected as modified shares by the receiver or not and also have to see the probability of detecting the modified or authentic shares by the receiver. we assumed at least one share is not modified by the adversary. To know which share is not modified, it has to do several tests.

## 1.1 Organization

The Thesis is as follows: In Chapter II literature review. Next, Chapter III the notation that is used for the coding scheme and description of the application. Then, Chapter IV is the analysis. Finally, Chapter V is conclusion of the thesis.

## CHAPTER II

### LITERATURE REVIEW

#### 2.1 Secret Sharing

[2] In general, two-sub protocols, which are  $sh$  and  $Rc$  combine to create the secret sharing protocol  $(Sh, Rc)$ . The sharing protocol  $Sh$  started by the dealer, who has secrets  $s$  in the secret space  $\mathcal{S}$ . The  $i$ -th participant for each  $i \in [n]$ , where  $[n = 1, 2, 3...]$  receives their share  $v_i$  in the shared space  $\mathcal{V}$  at the end of  $Sh$ . In the common secret sharing schemes,  $Sh$  is just a non-interactive protocol that receives an input of  $s \in \mathcal{S}$  and outputs  $v_1, \dots, v_n$ . The dealer sends  $v_i$  to the  $i$ -th participant for each  $i \in [n]$  after producing  $n$  shares.  $Sh$  could be seen as a probabilistic function from  $\mathcal{S}$  to  $V^n$  and  $Rc$  is an algorithm that attempts to recover the secret  $s$  by using a subset of all the shares with players indices as input.

#### 2.2 Cheaters in Secret Sharing Scheme

As described in [1], for traditional secret-sharing procedures, it is assumed that all participants are entirely or partially honest. However, in a genuine situation, certain individuals might act maliciously when the protocol is being executed. In particular, certain individuals may submit inaccurate shares, which would result in an inaccurate secret being produced during the reconstruction process. To solve the issue, novel schemes like cheater-identifiable secret sharing- CISS and extra qualities to conventional secret sharing have been taken into consideration. Here, a player who submits false shares is referred to as a cheater. Cheater identification protocol to identify the cheaters at the reconstruction phase.

### 2.3 Security Guarantee

In [1], A secret sharing concept  $(t, \varepsilon)$  cheater-identifiable for individual identification is  $(Sh_{cheater}, Rc_{cheater})$ . If the subsequent condition is true. For any adversary  $\mathcal{A}$  that corrupts at most  $t$  players and for any two unique applicants  $i, j$ .  $(n' - 1, q^{-l'})$  cheater-identifiable protocol for individual identification, where  $t = n' - 1$  and  $\varepsilon = q^{-l'}$ . And the probability of successfully detecting the cheaters is  $1 - q^{-l'}$ ,  $l'$  is a security parameter also used universal-2 hash functions based on the toeplitz matrix to calculate the probability of detecting cheaters.

## CHAPTER III

### METHODOLOGY

#### 3.1 Notations

- The access structure  $\mathbb{A}$  expresses the condition for a subset of  $[n]$  to recover the secret  $S \in \mathcal{S}$ , where  $n$  is the number of shares.
- An  $(Sh, Rc)$  be a secret sharing protocol realizing access structure  $\mathbb{A}$  with sharing function  $Sh : \mathcal{S} \rightarrow \mathcal{V}^n$ , where  $\mathcal{V}$  is  $m$ -dimensional vector space  $\mathbb{F}_q^m$  over a finite field  $\mathbb{F}_q$ , where  $q$  is the order of the finite field and reconstruction function  $Rc$ .
- Cheater identifiable secret sharing uses message authentication protocols [3], [4] in which universal hash functions are used. A family  $\mathcal{H}$  of hash functions  $h_i : A \rightarrow B$ ,  $i \in [n]$  is a universal-2 if for any  $a \in A$  and  $b \in B$

$$Pr_{h_i \leftarrow \mathcal{H}}[h_i(a) = b] = \frac{1}{|B|}$$

holds, where the probability is over the uniformly random choice of  $h_i$  from  $\mathcal{H}$ .

- An  $(l' \times m)$ , where  $l'$  is a security parameter, Toeplitz matrix  $T_j = (T_{c,d})$ ,  $j \in [n]$ , over  $\mathbb{F}_q$  can be determined by  $\mathbf{a}_j = a_1 a_2 \dots a_{l'+m-1} \in \mathbb{F}_q^{l'+m-1} \setminus \{0^{l'+m-1}\}$  as follows: Set  $T_{l',1} = a_1, \dots, T_{1,1} = a_{l'}$  (for the first column) and  $T_{1,2} = a_{l'+1}, \dots, T_{1,m} = a_{l'+m-1}$  (for the first row). The remaining entries can be set to satisfy that  $T_{c,d} = T_{c-1,d-1}$  for any  $c$

and  $d$  with  $2 \leq c \leq l'$  and  $2 \leq d \leq m$ . That is,  $T_j$  written as

$$T_j = \begin{pmatrix} a_{l'} & a_{l'+1} & a_{l'+2} & \cdots & a_{l'+m-1} \\ a_{l'-1} & a_{l'} & a_{l'+1} & \cdots & a_{l'+m-2} \\ a_{l'-2} & a_{l'-1} & a_{l'} & \cdots & a_{l'+m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_m \end{pmatrix}.$$

The matrix  $T_j$  represents a linear map from  $\mathbb{F}_q^m$  to  $\mathbb{F}_q^{l'}$ . Let  $\mathcal{H}_{m,l'} = (m \times l')$ - Toeplitz matrix  $T_j$  determined by  $a_j | a_j \in \mathbb{F}_q^{l'+m-1} \setminus \{0^{l'+m-1}\}$  where  $l' < m$ ,  $T_j$  regarded as a hash function indexed by  $\mathbf{a}_j$ . Then  $\mathcal{H}_{m,l'}$  is a family of universal-2 hash functions from  $\mathbb{F}_q^m \setminus \{0^m\}$  to  $\mathbb{F}_q^{l'}$ .

## 3.2 Coding Scheme

The distribution phase follows the secret sharing protocol *Sh*. Also, the reconstruction phase follows with identification and reconstruction protocol *Rc*. We consider a message  $m$  into the shares  $s_1$  and  $s_2$ , where  $n = 2$  using shamir secret protocol. And the threshold  $k = 2$ , where shares  $s'_1$  and  $s'_2$  needed to reconstruct the secret. If any of one shares is modified, the receiver can not reconstruct message  $m$ . At the reconstruction phase, the receiver will execute identification protocol then reconstruction of the original message  $\mathbf{m}$ .

### 3.2.1 Distribution and Reconstruction Phase

- For a secret  $S \in \mathcal{S}$ , the transmitter computes  $X_i := Sh_i(S)$ ,  $i \in [n]$ ,  $n = 2$  then independently generates Toeplitz matrix  $T_j$ ,  $j \in [n]$ , with dimension  $l' \times m$  as well. Also for  $i \neq j$ , generates  $n(n-1)$  random numbers  $Z_{j,i}$ ,  $(i, j) \in [n]$ , by taking the values in  $\mathbb{F}_q^{l'}$ . And we have the following combinations,
- $j = 1, i = 2, Y_{1,2} := T_1 X_2 + Z_{1,2}$ ,
- $j = 2, i = 1, Y_{2,1} := T_2 X_1 + Z_{2,1}$ .

$Y_{1,2}, Y_{2,1}$  is defined by multiplying message  $\mathbf{m}$  in  $X_2, X_1$  with the toeplitz matrix  $T_1, T_2$  and added with additional information, which is the random number  $Z_{1,2}, Z_{2,1}$ . For each  $j \in [n]$ , the transmitter gives information  $(X_j, Z_{1,j}, \dots, Z_{j-1,j}, Z_{j+1,j}, \dots, Z_{n,j})$  and  $(T_j, Y_{j,1}, \dots, Y_{j,j-1}, Y_{j,j+1}, \dots, Y_{j,n})$  to each of the share  $s_1, s_2$ . Share  $s_1, s_2$ :

$$(X_1, Z_{1,2}, Z_{2,1}), (T_1, T_2, Y_{1,2}, Y_{2,1}).$$

$(X_2, Z_{1,2}, Z_{2,1}), (T_1, T_2, Y_{2,1}, Y_{1,2})$ . Next, the transmitter sends share  $s_1$  and  $s_2$  to each relay.

- Here we assumed at least one share is not modified by adversary, to know that one share we need perform the below tests.

- Firstly, each relay sends the shares  $s'_1$  and  $s'_2$  to the receiver.

$$(X'_1, Z'_{1,2}, Z'_{2,1}), (T'_1, T'_2, Y'_{1,2}, Y'_{2,1}).$$

$$(X'_2, Z''_{1,2}, Z''_{2,1}), (T''_1, T''_2, Y''_{1,2}, Y''_{2,1}).$$

- The tests followed as below:

If  $Z'_{1,2} \neq Z''_{1,2}$  or  $Z'_{2,1} \neq Z''_{2,1}$  or  $T'_1 \neq T''_1$  or  $T'_2 \neq T''_2$  or  $Y'_{1,2} \neq Y''_{1,2}$  or  $Y'_{2,1} \neq Y''_{2,1}$ . Then, the receiver will not perform identification and reconstruction protocol. If  $Z'_{1,2} = Z''_{1,2}$ ,  $Z'_{2,1} = Z''_{2,1}$ ,  $T'_1 = T''_1$ ,  $T'_2 = T''_2$ ,  $Y'_{1,2} = Y''_{1,2}$  and  $Y'_{2,1} = Y''_{2,1}$ . Then, the receiver will perform identification and reconstruction protocol.

- Later the above tests we have an identification protocol before executing the reconstruction of the message  $m$ .

### 3.2.2 Identification and Reconstruction Protocol

The identification of shares  $s'_1$  and  $s'_2$  is done by the receiver.

- The receiver computes the following,

$$T'_1 X'_2 + Z'_{1,2}, T'_2 X'_1 + Z'_{2,1}.$$

Now, there are below possibilities that will happen while execution of identification protocol.

- Next, the receiver checks the relations,

If  $Y'_{1,2} = T'_1 X'_2 + Z'_{1,2}$ ,  $Y'_{2,1} = T'_2 X'_1 + Z'_{2,1}$ .

Then the receiver detects the share  $s'_1$  and  $s'_2$  are not modified.

Therefore, the receiver accepts share  $s'_1$  and  $s'_2$  and performs reconstruction protocol.

- If  $Y'_{1,2} \neq T'_1 X'_2 + Z'_{1,2}$ ,  $Y'_{2,1} = T'_2 X'_1 + Z'_{2,1}$ .

Then the receiver detects that share  $s'_2$  is modified and share  $s'_1$  is not modified.

Therefore, the receiver rejects share  $s'_2$  and could not be able to perform reconstruction protocol.

- If  $Y'_{1,2} = T'_1 X'_2 + Z'_{1,2}$ ,  $Y'_{2,1} \neq T'_2 X'_1 + Z'_{2,1}$ ,

Then the receiver detects that share  $s'_1$  is modified and share  $s'_2$  is not modified.

Therefore, the receiver rejects share  $s'_1$  and could not be able to perform reconstruction protocol.

## CHAPTER IV

### RESULTS

#### 4.1 Case 1: Analysis

- Let event  $\mathbf{B}_1$  be the receiver detects that share  $s'_2$  is modified when the adversary modifies share  $s_2$ . Event  $\mathbf{B}'_1$  is the receiver does not detect that share  $s'_2$  is modified when the adversary modifies share  $s_2$ .

- Toeplitz matrix  $T'_1$  is a hash function with input  $\mathbb{F}_q^m$  and output  $\mathbb{F}_q^{l'}$ ,

$$h_i(T'_1) : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^{l'}$$

$$\Pr_{h_i(T'_1) \leftarrow \mathcal{H}_{m,l'}} [h_i(a) = b] = \frac{1}{|q^{l'}|}, a \neq b, a \in \mathbb{F}_q^m, b \in \mathbb{F}_q^{l'}$$

In the below relations we have toeplitz matrix  $T'_1$  as a hash function, then the output of the hash function definition can be taken as the probability of the event  $\mathbf{B}'_1$ ,

1.  $Y'_{1,2} = T'_1 X'_2 + Z'_{1,2}$

$$\Pr[\mathbf{B}'_1] = q^{-l'}$$

2.  $Y'_{1,2} \neq T'_1 X'_2 + Z'_{1,2}$

$$\Pr[\mathbf{B}_1] = 1 - \Pr[\mathbf{B}'_1]$$

$$\Pr[\mathbf{B}_1] = 1 - q^{-l'}$$

- As we assumed at least one share is not modified, also the test  $Z'_{1,2} \neq Z''_{1,2}$  or or  $T'_1 \neq T''_1$  or  $Y'_{1,2} \neq Y''_{2,1}$ . Then the receiver can not perform reconstruction protocol and able to detect the modified share  $s'_2$  with a high probability.

#### 4.2 Case 2: Analysis

- Let event  $\mathbf{B}_2$  be the receiver detects that share  $s'_1$  is modified when the adversary modifies share  $s_1$ . Event  $\mathbf{B}'_2$  is the receiver does not detect that share  $s'_1$  is modified when the adversary modifies share  $s_1$ .

- Toeplitz matrix  $T_2$  is a hash function with input  $\mathbb{F}_q^m$  and output  $\mathbb{F}_q^{l'}$ ,

$$h_i(T_2) : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^{l'}$$

$$\Pr_{h_i(T_2) \leftarrow \mathcal{H}_{m,l'}} [h_i(a) = b] = \frac{1}{|q^{l'}|}, a \neq b, a \in \mathbb{F}_q^m, b \in \mathbb{F}_q^{l'}$$

In the below relations we have toeplitz matrix  $T_2'$  as a hash function, then the output of the hash function definition can be taken as the probability of the event  $\mathbf{B}'_2$ ,

1.  $Y'_{2,1} = T_2'X_1 + Z'_{2,1}$ ,

$$\Pr[\mathbf{B}'_2] = q^{-l'}$$

2.  $Y'_{2,1} \neq T_2'X_1 + Z'_{2,1}$ ,

$$\Pr[\mathbf{B}_2] = 1 - \Pr[\mathbf{B}'_2]$$

$$\Pr[\mathbf{B}_2] = 1 - q^{-l'}$$

- As we assumed at least one share is not modified, also the test  $Z'_{2,1} \neq Z''_{2,1}$  or  $T_2' \neq T_2''$  or  $Y'_{1,2} \neq Y''_{2,1}$ . Then the receiver can not perform reconstruction protocol and is able to detect the modified share  $s'_1$  with a high probability.

## CHAPTER V

### CONCLUSION

In conclusion, this thesis provided with application that we consider, a message  $m$ , transmitter, and receiver communication through the two relay networks. Focused on dividing the message  $m$  into two shares  $s_1$ ,  $s_2$  and using the share generation, cheater identification and reconstruction protocol scheme in [1].

## BIBLIOGRAPHY

## BIBLIOGRAPHY

- [1] M. Hayashi and T. Koshihara, “Universal construction of cheater-identifiable secret sharing against rushing cheaters based on message authentication,” in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 2614–2618, 2018.
- [2] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, p. 612613, nov 1979.
- [3] H. Krawczyk, “New hash functions for message authentication,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 301–310, Springer, 1995.
- [4] U. M. Maurer, “A unified and generalized treatment of authentication theory,” in *Annual Symposium on Theoretical Aspects of Computer Science*, pp. 387–398, Springer, 1996.