JAMBURA JOURNAL OF MATHEMATICS
Jambura J. Math. Vol. 4, No. 1, pp. 126–134, January 2022
Journal Homepage: http://ejurnal.ung.ac.id/index.php/jjom
DOI: https://doi.org/10.34312/jjom.v4i1.12001

The Application of Recursive Algorithm on Shamir's Scheme Reconstruction for Cheating Detection and Identification

Rafika Husnia Munfa'ati[1*], Sugi Guritman[2], Bib Paruhum Silalahi[3]

[1,2,3]*Department of Mathematics, Faculty of Science and Mathematics, IPB University, Jl. Meranti, Kampus IPB Dramaga, Bogor 16680, Indonesia*
[*]*Corresponding author. Email: rafika_najah@apps.ipb.ac.id*

ABSTRACT

Information data protection is necessary to ward off and overcome various fraud attacks that may be encountered. A secret sharing scheme that implements cryptographic methods intends to maintain the security of confidential data by a group of trusted parties is the answer. In this paper, we choose the application of recursive algorithm on Shamir-based linear scheme as the primary method. In the secret reconstruction stage and since the beginning of the share distribution stage, these algorithms have been integrated by relying on a detection parameter to ensure that the secret value sought is valid. Although the obtained scheme will be much simpler because it utilizes the Vandermonde matrix structure, the security aspect of this scheme is not reduced. Indeed, it is supported by two detection parameters formulated from a recursive algorithm to detect cheating and identify the cheater(s). Therefore, this scheme is guaranteed to be unconditionally secure and has a high time efficiency (polynomial running time).

Keywords:
Cryptography; Recursive Algorithm; Shamir's Linear Scheme

How to Cite:

R. H. Munfa'ati, S. Guritman, and B. P. Silalahi, "The Application of Recursive Algorithm on Shamir's Scheme Reconstruction for Cheating Detection and Identification", *Jambura J. Math.*, vol. 4, No. 1, pp. 126–134, 2022, doi: https://doi.org/10.34312/jjom.v4i1.12001

1. Introduction

Information data owned by individuals, companies, and public agencies are undoubtedly a precious asset. The current flow of digital disruption demands an effective increase of data privacy and security in various digital and internet-based electronic devices. In response, a mathematical study applies cryptographic methods that intend to maintain the security of confidential data by a group of trusted parties. The concept is known as Secret Sharing Scheme (SSS). For more than four decades, it has been proven that SSS remains a solution to numerous possible fraud attack risks. Too few shares will be vulnerable to lose, and contrarily, if too many are duplicated, it can increase the potential for cheating [1].

The concept of SSS was conceived individually by Shamir [2] and Blakley [3], which is more familiarly referred to as (t, n)-Threshold SSS. In principle, encrypted message

e-ISSN: 2656-1344
Received: 12 November 2021 | Accepted: 8 December 2021 | Online: 1 January 2022

(secret) s is distributed by a trusted party (dealer) to n private key-holders (shareholders), and only if there is any subset t or more participants, then the secret can only be read. Shares in this context are secret pieces that the dealer must put together first to decrypt the message.

Although Shamir's scheme is an information-theoretically perfect secure scheme, Tompa & Woll [4] prove that practically it is incompetent in dealing with cheating, so a modified scheme is proposed to detect it. Meanwhile, Rabin & Ben-Or [5] introduced the principle of majority rule $n \geq 2t + 1$ in their scheme, which implicitly implies that a scheme can be said secure if it can resist up to t cheating. The scheme is equipped with an error check vector to detect and identify cheating. Slinko [6] explains that the length of each share in bits should exactly the length of the secret and it cannot be shorter for an ideal scheme. It leads Becerra & Vega [7] and Liu [8] to the idea of a linear (t, n)-scheme that can detect cheating. Both also highlight the discussion of the information rate value and the error probability of cheating detection as parameters for analyzing the scheme's security. Liu *et al*. [9] proposed two cheaters identification algorithms based on symmetric bivariate polynomials at the reconstruction stage, relying on Lagrange interpolation. Unfortunately, its computation is still considered inefficient. Then Ahzan *et al*. [1] proposes a linear approach to improve it but does not include a security analysis of the scheme. So far, it turns out that a more efficient linear scheme can still be modified.

This time, an extended Euclidean algorithm in the recursive technique of a modulo matrix inverse applied to the two main stages of Shamir's linear scheme was chosen as the primary method. In the secret reconstruction stage and since the beginning of the share distribution stage, these algorithms have been integrated by relying on a detection parameter to ensure that the secret value sought is valid (original). Even though the scheme obtained will be much simpler because it utilizes the Vandermonde matrix structure as [1] previously, the security aspect is not reduced. Indeed, it is supported by particular detection parameters formulated from a recursive algorithm to detect cheating and identify the cheater(s). Therefore, it is guaranteed to be unconditionally secure and also has a high time efficiency. The recursive technique can upgrade the computational speed required by calculating the n input size in each algorithm. In other words, this scheme can overcome the shortcomings of previous Shamir's linear scheme studies.

The purposes of this paper were: 1.) to modify Shamir's linear scheme by applying a recursive algorithm, 2.) to construct the scheme with cheating detection and identification capabilities, and 3.) to analyze the security of cheating detection and identification.

This paper is organized as follows. In section 2, we give some preliminaries to describe the fundamental of our work. In section 3, we proposed our modified scheme, which includes cheating detection and identification algorithms. Lastly, we conclude our work in section 4.

2. Preliminaries

In this section, we introduce some fundamental backgrounds containing a brief description of Shamir's linear scheme, extended Euclidean algorithm, and security analysis of SSS.

2.1. Shamir's Linear (t,n)-Scheme

Definition 1. A (t, n)-SSS is said to be linear if the n secret pieces (shares) $s_1, s_2, \ldots, s_n$ can be written as:

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \boldsymbol{H} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_t \end{pmatrix}. \tag{1}$$

H is a public matrix of size $n \times t$ with a non-singular $t \times t$ submatrix. The vector $(r_1, r_2, \ldots, r_t)$ is randomly generated by the dealer [8].

Based on the Definition 1, it is clear that Shamir's scheme is a linear scheme which stated as follows:

1. Share distribution stage
   (a) Dealer D generates a prime number $p > \max(s, n)$ with $s \in \mathbb{Z}_p$.
   (b) Dealer D determines a random polynomial over $\mathbb{Z}_p$ notated by $a_0, a_1, \ldots, a_{t-1}$ and choose *secret* $a_0 = s$.
   (c) Dealer D computes n share pieces $s_i = f(i) \bmod p$; $i = 1, 2, \ldots, n$ where $f(x) = \sum_{j=0}^{t-1} a_j x^j$ and distributes each s_i to participants P_i secretly. Each P_i gets pair of share points (x_i, s_i).
2. Secret reconstruction stage.
   Suppose $\mathcal{B} = \{P_1, P_2, \ldots, P_t\}$ is a subset of t participants pooled by dealer to calculate the Lagrange interpolation polynomial i.e $f(x) = \sum_{i=1}^{t} L_i(x) s_i \pmod p$ with $L_i(x) = \prod_{i=1, i \neq t}^{t} \frac{x - x_i}{x_t - x_i}$ $(1 \leq i \leq t)$ and s_i are the value of each share pieces. Then the original secret value will be obtained $s = f(0)$.

It should be noted that an SSS is said to be perfect if it satisfies the following two conditions:

1. Any t or more participants can reconstruct polynomial $f(x)$ such that secret value can be recovered, and
2. Any $t - 1$ or fewer participants will not be able to reconstruct any values.

Even a scheme is not enough to say perfect. The polynomial matrix must also be guaranteed to be consistent so that all the shares are identical, which causes the reconstructed secret to being unique [6].

In the linear scheme, we consider the object of the problem that should be solved as the system of linear equation (SLE) containing t equations and n variables with a hidden secret value in the first coefficient (a_0). The most common solution adopted here is the Gaussian elimination method. So, it is clear that the linearity of the polynomial matrix should be noticed from this typical scheme.

2.2. Extended Euclidean Algorithm

By understanding that generated polynomial matrix should be a linear matrix, the following approach will be related to the recursive technique of the extended Euclidean algorithm [10]. In line with computational SSS works under discrete arithmetic, the multiplication of a polynomial matrix with modulo matrix inverse can increase the

running time. Therefore, Shamir's linear SSS requires a recursive algorithm embedded in both stages.

2.3. Security Analysis of SSS

There are two types of security protocols known in cryptographic security analysis: computational security and unconditional security. Computational security stands to the assumption that an adversary has limited computing power that prevents him from solving complex mathematical problems. While unconditional security means that the security persists even if the adversary has unlimited computing power [11–14]. It led Cabello *et al*. [15] to propose two unconditionally secure linear schemes against cheaters, classified as a robust scheme and a secure scheme. The security is analyzed by calculating the information rate and the probability of successful cheating. The excess information added to the share is required to obtain unconditional security. Mashhadi [16] proposed two publicly verifiable schemes with general access structure. Then Banerjee *et al*. [17] analyzed the security and performance of their modified Shamir's scheme with the underlying hierarchy concept. Both schemes [16, 17] are also robust and secure. Slinko [6] explained that the length of each share in bits should exactly the length of the secret and it cannot be shorter for an ideal scheme, where it must be the perfect scheme and has an information rate value equal to 1. It is known that the information rate can decrease (the level of secrecy decreases) along with the chances of successful cheating. The opportunity should not depend on the assumption of computational resources available to participants.

3. Results and Discussion

3.1. Recursive Algorithm Design

The main problem here is reconstructing the secret value to obtain the original value (a valid one). Shamir's linear scheme is a Shamir's scheme represented in matrix multiplication $HX = Y$ where there is a minimum of T square submatrix that will reconstruct the secret. Let $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x_{t-1}$ where $a_j = a_{j-1} + a_{j-2} \pmod p$ is a polynomial equation generated in the share distribution stage, forming the submatrix T. Also, suppose (x_i, s_i) with $s_i = f(x_i)$ for $i = 1, 2, \ldots, t$ is a sequence of t value pairs representing the identity and share, which will reconstruct the secret respectively. Then the matrix equation associated with the SLE in it is $TX = Y$, it can be written

$$\begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 & \cdots & x_1^{t-2} & x_1^{t-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \cdots & x_2^{t-2} & x_2^{t-1} \\ 1 & x_3 & x_3^2 & x_3^3 & \cdots & x_3^{t-2} & x_3^{t-1} \\ & & \vdots & & \ddots & \vdots & \\ 1 & x_{t-1} & x_{t-1}^2 & x_{t-1}^3 & \cdots & x_{t-1}^{t-2} & x_{t-1}^{t-1} \\ 1 & x_t & x_t^2 & x_t^3 & \cdots & x_t^{t-2} & x_t^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{t-2} \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{t-1} \\ s_t \end{bmatrix} \tag{2}$$

Reconstructing the secret means solving the SLE (2) in the most efficient way possible. As in general SLE solutions, in the initial step, (2) is represented as an augmented matrix $G = (T|Y)$ of size $t \times (t+1)$,

$$G = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 & \cdots & x_1^{t-2} & x_1^{t-1} & s_1 \\ 1 & x_2 & x_2^2 & x_2^3 & \cdots & x_2^{t-2} & x_2^{t-1} & s_2 \\ 1 & x_3 & x_3^2 & x_3^3 & \cdots & x_3^{t-2} & x_3^{t-1} & s_3 \\ & & \vdots & & \ddots & & \vdots & \\ 1 & x_{t-1} & x_{t-1}^2 & x_{t-1}^3 & \cdots & x_{t-1}^{t-2} & x_{t-1}^{t-1} & s_{t-1} \\ & 1 & x_t & x_t^2 & x_t^3 & \cdots & x_t^{t-2} & x_t^{t-1} & s_t \end{bmatrix} \tag{3}$$

Then by utilizing the submatrix T structure, the Vandermonde matrix, the SLE (2) solution can be formulated recursively with Gaussian elimination and multiplication of modulo matrix inverse. Finally, obtained

$$a_{t-1} = \frac{s_t^{(t-2)} - s_{t-1}^{(t-2)}}{x_t - x_{t-1}} \tag{4}$$

and

$$a_{t-2} = s_{t-1}^{(t-2)} - (x_1 + x_2 + \cdots + x_{t-2} + x_{t-1})a_{t-1} \tag{5}$$

Since $a_j = a_{j-1} + a_{j-2} \pmod{p}$ for $j = 0, 1, \ldots, (t-1)$, the polynomial f can be reconstructed using the recursive formula:

$$a_{t-k} = a_{t-k+2} + a_{t-k+1} \pmod{p} \text{ for } k = 3, 4, 5, \ldots, t \tag{6}$$

which consequently the secret value $s = a_0$ and detection parameter $p_D = \sum_{j=0}^{t-1} a_j$ can be known.

3.2. Modified Linear Scheme with Recursive Algorithm

A new modified scheme is constructed with a linear approach and inserts recursive techniques on both algorithms, share distribution, and secret reconstruction. The resulting scheme is a perfect and very simple yet still guaranteed to be secure against cheating. The algorithm in the reconstruction stage is already equipped with a mechanism to detect cheating and identify the cheater(s) without using Lagrange interpolation anymore. The p and secret s value generated greatly affect the security level of the built scheme. This is as shown if $|p| = B$, then $|s| = \frac{B}{2} = b$. Then b and p_D will be the detection parameters of cheating and the guarantee for recovering the original secret value.

3.2.1. Share distribution stage

Algorithm 1. Share distribution to n participants.

Input : p, t, n.

1. Dealer D generates a prime number $p > (s, n)$ such that $s \in \mathbb{Z}_{2^b}$.
2. Dealer D determines the number of participants n and thresholds $t; n, t \in \mathbb{Z}^+$.
3. Dealer D defines random polynomial $f(x) = \sum_{j=0}^{t-1} a_j x^j$ over $\mathbb{Z}_p$.
4. Dealer D computes the share value of each n participant that is $s_i = f(x_i)$ mod

$p; i = 1, 2, \ldots, n$ and distributes them to P_i.

Output : pair of share pieces value (x_i, s_i).

It is important to recall that Shamir's linear scheme is a Shamir's scheme represented in terms of matrix multiplication $HX = Y$ and can be viewed as SLE with:

1. H is a matrix of size $n \times t$ whose i-th row for $i = 1, 2, \ldots, n$ is a vector $(1, x_i, x_i^2, \ldots, x_i^{t-1})$ with x_i as the representation of the identity of i-th participant.
2. Y is a column matrix of size $n \times 1$ whose i-th entry for $i = 1, 2, \ldots, n$ is s_i, representing the *share* value of i-th participant.
3. X is a column matrix of size $t \times 1$, a variable matrix in SLE when H and Y are known.

Based on this, it can be easily observed that any submatrix T of size $t \times t$ of H is a Vandermonde matrix in which T is guaranteed to be non-singular. If there is no change in the value (i.e., cheating) on the share s_i, it can also be guaranteed that the SLE definitely is consistent.

3.2.2. Secret reconstruction stage

Algorithm 2. Cheating detection.

This is a procedure for cheating detection at $m = t$, where the sub-SLE solution $X = T^{-1}Y$ is calculated and tested for conformity with the detection parameters b and p_D. If it is proven that no cheating is found, the original secret value s can be reconstructed. The vectors in this algorithm are stored as a list.

Input : t, m, G, Y, b, p_D.

1. Pools a list of ordered pairs G that will reconstruct the secret, consisting of m participants and their share value pairs.
2. Computes the sub-SLE solution $X = T^{-1}Y$ such that $X = F$.

Output : There is no cheating and s is the original secret, else

Output : There is cheating, $s = 0$.

Algorithm 3. Cheating detection and identification for $m\,(\geq t)$.

This is a procedure to detect and identify cheating and then reconstruct the original secret value with $0 \leq k \leq m - t$. Two detection parameters b and p_D are available, which will test the consistency of the calculated sub-SLE. The vectors in this algorithm are stored as a list. The input procedure includes t, m, G, Y, b, p_D.

1. Determine the number of m participants who will reconstruct the secret with $m = t + l; 0 \leq l \leq n - t$.
2. Pool a list of ordered pairs G to reconstruct the secret, consisting of m participants and their share value pairs.
3. Let k represents the number of participants who cheated,
4. For $0 \leq k \leq l$, the output is $[s, K]$ with K the set of identities of participants who commit cheating.
5. For $l \leq k \leq m$, the output is 0 and the original secret cannot be reconstructed. This happens because $k > m - t$.

Remark 1. The time complexity of Algorithm 2 is $\boldsymbol{T}_{det}(n) = \mathbf{O}(n)$, and Algorithm 3 is $\boldsymbol{T}_{ident}(n) = \mathbf{O}\left(n^3 + n\log n\right)$. Both algorithm class is a polynomial running time.

Theorem 1. *The proposed modified linear scheme is a perfect* (t, n) *-SSS and the probability of successful secret reconstruction is* $\epsilon = 2^{-\alpha b}$.

Proof. Assume the number of participants working together to pool pairs of share values is less than t, for example $(t - a)$, the sub-SLE solution is guaranteed not to be unique even if the actual s_i value is given. In this case, the value of the X matrix that satisfies the sub-SLE is p^{α} but the value of X which has a structure corresponding to F is only 2^{ab}. So, the probability of getting the correct value of s is 2^{-ab}. As Ahzan *et al.* [1] have shown, $(t - 1)$ participants in Shamir's linear scheme will not get the real secret because the calculated matrix is not linearly independent, so does our modified linear scheme. □

Theorem 2. *The modified linear scheme can detect cheating if* $m = t$ *with a probability of detection error* $\epsilon < 2^{-b}$.

Proof. Under this scheme, cheating detection is carried out by pooling all share values of m participants and calculating the sub-SLE solution $X = T^{-1}Y$ based on a recursive formula determined by a trusted dealer. Suppose the value of the first entry of $X \notin \mathbb{Z}_{2^b}$ or its entries does not have a recursive pattern as the initial F. In that case, it is strongly suspected –so it can be detected– that there is cheating, whether intentional or not, during the collection of value pairs (x_i, s_i) so that $\epsilon < 2^{-b}$. □

Theorem 3. *The modified linear scheme can detect and identify cheating if* $m - k \geq t$.

Proof. The cheating detection procedure can be carried out in this scheme if there are $m \geq t$ participants and at the same time identify the cheater(s) if there are $0 \leq k \leq m - t$ cheating. It means that a combination $\begin{pmatrix} m-k \\ t \end{pmatrix}$ of participants who will reconstruct the original secret is available. Assume the number of cheating is not exceed the honest participants involved in the reconstruction; this is in line with the principle of majority rule proposed by Rabin & Ben-Or [5]. Thus, our procedure is effective up to t cheating, more effective than the Liu [8] and Ahzan *et al.* [1] schemes. The sub-SLE solution $X = M_L^{-1}Y$ is calculated by the recursive formula a_{t-k} for $k = 3, 4, 5, \ldots, t$ and also applies more detailed provisions as explained in the proof of Theorem 2. □

3.3. Security Analysis

Unconditional security of our linear modified scheme is focused on the following three main points:

1. Data confidentiality (secret). The secret value can be reconstructed only if $m \geq t$ participants are available. In the cheating detection and identification algorithm, one of the detection parameters stores essential information in the form of a secret key. So even if cheating is found, this scheme will return the original secret as long as $0 \leq k \leq m - t$. The secret authenticity and originality of our scheme are guaranteed to be safe. Previously, it was mentioned in the share distribution stage that the parameters p and s greatly determine the strength and weakness of the scheme' security. If p is determined as B, then s is chosen as b. While the information rate $\rho = \frac{\log|S|}{\log|V|} = \frac{1}{2}$, meaning that the size of the secret s taken is quite small in $\mathbb{Z}_p$ but guaranteed to be easily found by honest participants and in legitimate channels.

2. Data integrity (share). The basic assumption here, dealer D is a trusted party and all distributed shares have been stored in legitimate channels as n-pair shares (x_i, s_i). Though it is not the share's identity that determines the successful reconstruction, which will be possible to detect the identity of the shareholder participant who committed the cheating with an embedded recursive algorithm. This is because the consistency of the polynomial matrix can be maintained. However, the incompatibility of share values still may likely occur, it indicates cheating. The original secret value can be reconstructed as long as the number of forged shares is not more than $(m - k)$. That is the limit of our scheme's cheating identification capability. The released share key has fit the ideal size as a private key cryptographic scheme. So, it is clear that the integrity of the scheme is very well preserved.
3. Flexibility of shareholders (threshold). The number of participants who take part in the secret reconstruction process is referred to as the threshold. Theoretically and practically, Shamir's scheme never limits the shareholder participants who are allowed to participate in this process in a particular order. Anyone can participate randomly to pool their share value and then evaluate the secret value with a recursive algorithm that the dealer has prepared.

Based on the explanations above, our modified linear scheme is proven to be an unconditionally secure scheme and has fulfilled all the conditions of a perfect scheme.

4. Conclusion

A secret sharing scheme is appropriate to protect essential information data in a secure channel from various fraud attacks. As a mathematical study, the existing assumptions have been built close to ordinary phenomena. In this paper, a modified linear scheme based on Shamir's with the application of a recursive algorithm on secret reconstruction was chosen as a solution to overcome cheating attacks.

The linear and recursive approach to the polynomial matrix produces detection parameters that can guarantee the original secret value remains in a secure channel and is quickly recovered by a group of m trusted participants. When reconstructing the secret value, this scheme can automatically detect up to k cheating and at the same time identify the cheater(s) as long as the number of cheatings is $0 \leq k \leq m - t$. Thus, the recursive approach to this modified linear scheme is not only effective in maintaining secret security and overcoming fraud attacks but is also efficient in terms of algorithm construction and time complexity (polynomial time). The scheme is proven to be unconditionally secure.

References

[1] Z. N. Ahzan, S. Guritman, and B. P. Silalahi, "Deteksi dan Identifikasi Pelaku Kecurangan Skema Pembagian Rahasia Linear Berbasis Skema Shamir," *Jurnal Karya Pendidikan Matematika*, vol. 7, no. 1, pp. 27–41, 2020.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, nov 1979, doi: http://dx.doi.org/10.1145/359168.359176.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *1979 International Workshop on Managing Requirements Knowledge (MARK)*. IEEE, jun 1979, pp. 313–318, doi: http://dx.doi.org/10.1109/MARK.1979.8817296.

[4] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, oct 1989, doi: http://dx.doi.org/10.1007/BF02252871.

[5] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing - STOC '89*. New York, New York, USA: ACM Press, 1989, pp. 73–85, doi: http://dx.doi.org/10.1145/73007.73014.
[6] A. Slinko, "Ways to merge two secret sharing schemes," *IET Information Security*, vol. 14, no. 1, pp. 146–150, jan 2020, doi: http://dx.doi.org/10.1049/iet-ifs.2019.0210.
[7] D. Becerra and G. Vega, "Secret Sharing Scheme with Efficient Cheating Detection," in *Proceedings of the 2nd International Conference on Networking, Information Systems and Security - NISS19*. New York,: ACM Press, 2019, pp. 1–7, doi: http://dx.doi.org/10.1145/3320326.3320331.
[8] Y. Liu, "Linear (k,n) secret sharing scheme with cheating detection," *Security and Communication Networks*, vol. 9, no. 13, pp. 2115–2121, sep 2016, doi: http://dx.doi.org/10.1002/sec.1467.
[9] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences*, vol. 453, pp. 21–29, jul 2018, doi: http://dx.doi.org/10.1016/j.ins.2018.04.043.
[10] K. H. Rosen, *Discrete Mathematics and Its Application*, 8th ed. New York: McGraw-Hill Education, 2019.
[11] L. Harn, C.-F. Hsu, Z. Xia, and J. Zhou, "How to Share Secret Efficiently over Networks," *Security and Communication Networks*, vol. 2017, pp. 1–6, 2017, doi: http://dx.doi.org/10.1155/2017/5437403.
[12] A. Patra and D. Ravi, "Beyond Honest Majority: The Round Complexity of Fair and Robust Multi-party Computation," in *Advances in Cryptology – ASIACRYPT*, 2019, pp. 456–487, doi: http://dx.doi.org/10.1007/978-3-030-34578-5_17.
[13] L. Harn, Z. Xia, C. Hsu, and Y. Liu, "Secret sharing with secure secret reconstruction," *Information Sciences*, vol. 519, pp. 1–8, may 2020, doi: http://dx.doi.org/10.1016/j.ins.2020.01.038.
[14] M. Xiao and Z. Xia, "Security Analysis of a Multi-secret Sharing Scheme with Unconditional Security," in *SpaCCS 2020, LNCS*, 2021, ch. 12383, pp. 533–544, doi: http://dx.doi.org/10.1007/978-3-030-68884-4_44.
[15] S. Cabello, C. Padró, and G. Sáez, "Secret sharing schemes with detection of cheaters for general access structure," *Des. Codes Cryptogr.*, vol. 25, no. 2, pp. 175–188, 2002.
[16] S. Mashhadi, "Secure publicly verifiable and proactive secret sharing schemes with general access structure," *Information Sciences*, vol. 378, pp. 99–108, feb 2017, doi: http://dx.doi.org/10.1016/j.ins.2016.10.040.
[17] S. Banerjee, D. S. Gupta, and G. P. Biswas, "Hierarchy-based cheating detection and cheater identification in secret sharing schemes," in *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*. IEEE, mar 2018, pp. 1–6, doi: http://dx.doi.org/10.1109/RAIT.2018.8389094.