

Enhancing secret sharing security : A verifiable hierarchical threshold model and cheating detection based on integer factorization

Ali Havasi [†]

Massoud Hadian Dehkordi ^{*}

School of Mathematics and Computer Sciences

Iran University of Science and Technology

Tehran

Iran

Abstract

Secret sharing is the sharing of a secret between n shareholders so that only predefined subsets can retrieve the secret and other subsets called unauthorized subsets can not access the secret. In secret sharing, dishonest shareholders can always get exclusive access to the secret by offering a fake share, and other honest shareholders are deceived by getting a fake secret. Cheating detection is a well-known term in secret sharing that helps prevent cheating by dishonest participants in the secret reconstruction phase. In this paper, we propose a verifiable hierarchical threshold secret sharing model and a cheating detection scheme based on the difficulty of integer factorization. In this scheme, it is possible to verify the combiner by the shareholders so that they can recognize fake combiners, and the combiner in this scheme can never find out the contents of the secret. Also, in this paper, the security of secret restoration has significantly increased.

Subject Classification: 94A62, 94A60, 68P25.

Keywords: Secret sharing, Cheating detection, Hierarchical secret sharing, Cryptography.

1. Introduction

In 1979, Shamir [1] and Blakley [2] independently presented secret sharing schemes as a solution to safeguard cryptographic keys. The literature presents extensive investigations on secret sharing schemes. In these schemes, a dealer divides a secret into n shares and distributes them among n shareholders. Any t

[†] ORCID-ID: 0000-0002-1239-7610

^{*} ORCID-ID: 0009-0003-9753-4307

[†] E-mail: a_havasi@mathdep.iust.ac.ir

^{*} E-mail: mhadian@iust.ac.ir (Corresponding Author)

or more shares can reconstruct the secret, but fewer than t shares cannot. This scheme is known as a (t, n) secret sharing, denoted by $(t, n) - SS$.

Shamir's $(t, n) - SS$, which is information-theoretically secure, operates based on the interpolating polynomial. Generally, it is hypothesized that the dealer distributes the shares to shareholders without mistakes. All shareholders must have full confidence in the validity of the share received.

Tompa and Woll [3] were the first to present the idea of share cheating. They identified a cheating problem where cheaters submit fake shares during the secret reconstruction. Consequently, a false secret is reconstructed by honest shareholders while cheaters can retrieve the actual secret exclusively.

Carpentieri, De Santis, and Vaccaro [4] developed a novel cheating model in which $t - 1$ dishonest participants can cheat the t th honest participant. Tian, Peng, and Ma [5] constructed a publicly verifiable secret sharing (SS) scheme using bilinear pairing based on elliptic curves. The secret part is shared publicly by bilinear pairing, allowing anyone to verify it using interactive or non-interactive protocols.

Pieprzyk and Zhang [6] developed a linear SS scheme with cheating prevention by converting participants' shares into independent sub-shares. Jhanwar and Safavi-Naini [7] suggested a robust $t - 1$ threshold SS scheme equipped with a cheating detection facility. Cabello, Padro, and Saez [8] proposed a cheating detection SS scheme for a general access structure.

Liu et al. [9] presented a cheating detection scheme using two polynomials and two share cheating detection functions. They demonstrated that if a maximum of $t - 1$ dishonest participants modify their shares, the scheme remains cheating-free. In [10], a cheating detectable SS scheme is proposed to detect changes caused by a dishonest participant who modifies shares of an unauthorized subset. This scheme provides protection against adversaries who also have access to leakages from other shares.

In [11], a verifiable multi-secret sharing (VMSS) scheme is introduced, addressing cheating detection and identifying dishonest participants using ℓ -pair cyclic codes. In [12], a cheating detection scheme using an identity verification function with homomorphic multiplication is presented. Cianciullo and Ghodosi [13] proposed a scheme utilizing an algebraic manipulation detection (AMD) code for cheat detection. Participants send their shares to validation servers before reconstruction. These servers evaluate cheating without reconstructing the secret, ensuring secrecy.

In [14], the focus is on hierarchical secret sharing. A new and simpler structure is proposed where the access structure is a tree based on the hierarchical concept of companies, illustrated through their organization chart. Additionally, some of the hierarchies are discussed in references [15, 16].

The structure of this paper is presented as follows. Section 2 introduces the fundamentals of the linear $(t, n) - SS$ scheme. Section 3 presents two polynomials proposed according to the (t, n) threshold SS scheme for cheating

detection, and the related security analysis is reviewed in Section 4. The comparison of the proposed scheme with existing schemes is provided in Section 5. Finally, the conclusion of the study is presented in Section 6.

2. Preliminaries

2.1 Linear secret sharing scheme

According to the definition given in [6], if all shares of secret $u_1, u_2, \dots, u_n$ satisfy the following linear relationship, then (t, n) SS scheme is a linear secret sharing scheme.

$$(u_1, u_2, \dots, u_n) = (r_1, r_2, \dots, r_t)M \quad (1)$$

where M is a $t \times n$ matrix with entries from $\text{GF}(q)$ as public and any $t \times t$ submatrix of it is non-singular, and r_i is randomly selected by the dealer. According to equation (1), it is easy to understand that Shamir's (t, n) secret sharing scheme is a linear scheme.

3. Proposed schemes

In this section, we perform polynomial construction and secret reconstruction based on the number of shares, and we will propose two access structure models. In this scheme, cheating detection is based on the difficulty of finding the factorization of a positive integer, a product of two large prime numbers. Additionally, we do not consider the secret as a polynomial constant and generate a quasi-secret; this ensures that only the original shareholders will be able to retrieve the secret.

3.1. Initialization

Suppose $P_1, P_2, \dots, P_n$ is a group of n participants classified as follows:

$P_{11}, P_{12}, \dots, P_{1m_1}$ (Hierarchical level 1 (CL_1))

$P_{21}, P_{22}, \dots, P_{2m_2}$ (Hierarchical level 2 (CL_2))

$\vdots$

$P_{k1}, P_{k2}, \dots, P_{km_k}$ (Hierarchical level k (CL_k))

The number of shares is determined based on points; that is, everyone receives shares based on the points or grades they have, and the number of shares of shareholder P_i ($i = 1, 2, \dots, n$) is denoted by w_i .

Suppose L shareholders $P_{i_1}, P_{i_2}, \dots, P_{i_L}$ ($1 \leq i_j \leq n$) participate in secret reconstruction and the minimum number of shares to reconstruct the secret is t ; in this case, the threshold is $\sum_{j=1}^L w_{i_j} \geq t$.

If we denote the minimum number of shares of level i shareholders with r_i , then $t \geq \sum_{i=1}^k r_i$.

Type 1 access structure

If the condition is that only one person from each level participates in secret reconstruction, we construct a complete k -partite graph whose vertices are shareholders. In this way, as shown in Figure 1, there is no edge between the shareholders at any level, but there is an edge between the shareholders at different levels.

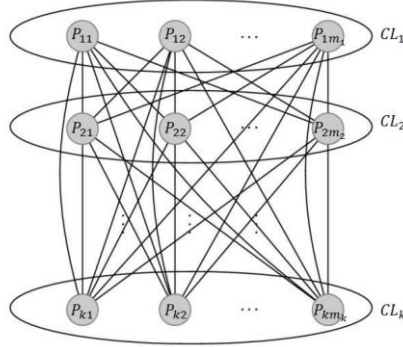


Figure 1
Multi partite complete graph

In this case, the access structure is as follows:

$$\Gamma = \{P_i | \forall j, 1 \leq j \leq k \exists i \ 1 \leq i \leq n \text{ s.t. } P_i \in CL_j, \nexists i' \neq i \ P_{i'} \in CL_j\}$$

and if the induced subgraph on the vertices of Γ is the complete graph of K vertices, i.e. K_k then, the combiner allows participating in the reconstruction of the secret.

Type 2 access structure

If the condition is that at least one person from each level should be present to restore the secret

$$\Gamma = \{P_i | \forall j, 1 \leq j \leq k \exists i \ 1 \leq i \leq n \text{ s.t. } P_i \in CL_j\}$$

At this point, we consider a unique code for every level, and these codes are random numbers of $z_1, \dots, z_k$. Then we send the sum of these codes $F = \sum_{i=1}^k z_i$ to the combiner, where code z_i corresponds to CL_i . When reconstructing the secret, the combiner asks the shareholders to send sums z_i ; if it is equal to F , the combiner allows the reconstruction of the secret.

3.2 Share generation and secret reconstruction

Distribution phase: The dealer creates a scheme similar to Shamir's (t, n) -SS scheme for the secret $S \in GF(q)$. However, in this scheme, the secret is no longer a polynomial constant, as one of the coefficients is considered a large prime number. The dealer chooses two prime numbers, q_1 and q_2 ($q_1 < q_2$), and then calculates $N = q_1 q_2$. q_1 and q_2 must have the same properties as the two primes used in the RSA cryptosystem to prevent efficient factorization of N .

Let S be the secret; the dealer randomly selects numbers $a_1, \dots, a_{t-1}$ and calculates a' as follows:

$$a' = q_1 - S$$

moreover, constructs the polynomial as follows:

$$f(x) = \sum_{i=0}^{t-1} a_i x^i = \underbrace{a' + S}_{a_0=q_1} + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1} \mod q$$

The dealer will send a' to the shareholders; this share is necessary as a quasi-secret to restore the secret. As a result, cheaters cannot obtain the secret without having a' . Then, the dealer calculates the hash value $H = h(a')$ and sends it to the combiner as an identifier.

The dealer also chooses another polynomial $g(x)$ of degree $(t-1)$, called an auxiliary polynomial, as follows:

$$g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{t-1} x^{t-1} \mod q$$

where $b_1, b_2, \dots, b_{t-1} \in \mathbb{Z}_q$ and $b_0 = q_2$. The dealer for each shareholder according to the number of their shares selects L_i distinct non-zero values $x_{i1}, x_{i2}, \dots, x_{i w_i} \in GF(q)$ and broadcasts them. Then it sends the share of each shareholder as follows:

$$P_i = \{(x_{i1}, x_{i2}, \dots, x_{i w_i}), (f(x_{i1}), f(x_{i2}), \dots, f(x_{i w_i})), (g(x_{i1}), g(x_{i2}), \dots, g(x_{i w_i})), a', z_m\}$$

that $P_i \in CL_m$.

Reconstruction phase: If we want conditions 1 or 2, the combiner first checks whether the shareholders can reconstruct the secret. Then, the combiner asks the participants to send their share by sending them a message $H = h(a')$. Participants can verify the combiner by calculating the hash of a' ; if it is correct, they will send their shares. Otherwise, the combiner is a cheater.

Suppose that the combiner gets t shares $s_1, s_2, \dots, s_t$. He reconstructs the polynomial $f(x)$ from $(x_{i_m j}, f(x_{i_m j})), (1 \leq m \leq L, 1 \leq j \leq w_{i_m})$ using Lagrange interpolation formula as:

$$f(x) = \sum_{m=1}^L \sum_{j=1}^{w_{i_m}} f(x_{i_m j}) \left(\prod_{a=1}^{w_{i_m}, a \neq j} \frac{x - x_{i_m a}}{x_{i_m j} - x_{i_m a}} \right)$$

The polynomial $g(x)$ is reconstructed in the same way.

Cheating detection phase: After reconstructing the polynomials f and g , if a_0 and b_0 are two prime numbers whose product is equal to N , then there is no cheating; otherwise, there is cheating. To reconstruct the secret, the combiner sends a_0 to the participants, then each participant calculates $S = a_0 - a'$ and gets the secret.

4. Security analysis

In this section, we conduct a thorough security analysis to demonstrate the resilience of the proposed secret sharing scheme with cheating detection. We explore various potential threats and affirm the scheme's robustness against them.

Theorem 4.1: *The proposed secret sharing scheme is a perfect (t, n) -SS scheme.*

Proof: We want to prove that $t - 1$ shares can not reconstruct the secret. Suppose $P_{i_1}, P_{i_2}, \dots, P_{i_L}$ the maximum number of their shares is $t - 1$ and they want to restore the secret; so we will have:

- $t - 1$ equation of $f(x)$
- $t - 1$ equation of $g(x)$
- $N = q_1 q_2$

In total, we have a $2t - 2 + 1 = 2t - 1$ equation, on the other hand, the number of unknowns

- $S, a_1, \dots, a_{t-1}$ (t unknown)
- $q_2, b_1, b_2, \dots, b_{t-1}$ (t unknown)

We have a total of $2t$ unknowns; therefore, it is not possible to get a unique answer with $2t$ unknowns and $2t - 1$ equations; as a result, the secret is not reconstructed.

Theorem 4.2: *No adversary will be able to recover the secret with a man-in-the-middle attack.*

Proof: Assuming that the adversary A can intercept the transmitted message H by a valid combiner, then mimic it to t legitimate shareholders and impersonate as a valid combiner. Shareholders receive message H from A , and if it's valid, they send their shares to A . However, A , even after recovering the polynomials f and g , cannot obtain the secret S because it requires a' , which is only available to the original shareholders. As a result, adversary A cannot recover the secret through a man-in-the-middle attack.

Theorem 4.3: *The probability that $L - 1$ shareholders can deceive the L th shareholder and reconstruct a wrong secret is $\varepsilon = 0$.*

Proof: Suppose $P_{i_1}, P_{i_2}, \dots, P_{i_{L-1}}$ are cheaters who intend to deceive shareholder P_L during the secret reconstruction process. For this purpose, they construct polynomials:

$$\begin{aligned} f'(x) &= a'_0 + a'_1 x + a'_2 x^2 + \dots + a'_{t-1} x^{t-1} \\ g'(x) &= b'_0 + b'_1 x + b'_2 x^2 + \dots + b'_{t-1} x^{t-1} \end{aligned}$$

In a way that $f'(x_{i_{Lj}}) = 0$ and $g'(x_{i_{Lj}}) = 0$ for $(1 \leq j \leq w_{i_L})$. shareholders $P_{i_1}, P_{i_2}, \dots, P_{i_{L-1}}$ calculate the new shares as follows:

$$P_{i_m} = \{(x_{i_m1}, x_{i_m2}, \dots, x_{i_m w_{i_m}}), (f(x_{i_m1}) + f'(x_{i_m1}), \dots, f(x_{i_m w_{i_m}}) + f'(x_{i_m w_{i_m}})), (g(x_{i_m1}) + g'(x_{i_m1}), \dots, g(x_{i_m w_{i_m}}) + g'(x_{i_m w_{i_m}}))\}$$

And the share of shareholder P_L is calculated as:

$$P_{i_L} = \{(x_{i_L1}, x_{i_L2}, \dots, x_{i_L w_{i_L}}), (f(x_{i_L1}) + f'(x_{i_L1}), \dots, f(x_{i_L w_{i_L}}) + f'(x_{i_L w_{i_L}})), (g(x_{i_L1}) + g'(x_{i_L1}), \dots, g(x_{i_L w_{i_L}}) + g'(x_{i_L w_{i_L}}))\}$$

In this case, two polynomials $f''(x)$ and $g''(x)$ are reconstructed.

$$\begin{aligned} f''(x) &= f(x) + f'(x) = (a_0 + a'_0) + (a_1 + a'_1)x + \\ &\quad (a_2 + a'_2)x^2 + \dots + (a_{t-1} + a'_{t-1})x^{t-1} \\ g''(x) &= g(x) + g'(x) = (b_0 + b'_0) + (b_1 + b'_1)x + \\ &\quad (b_2 + b'_2)x^2 + \dots + (b_{t-1} + b'_{t-1})x^{t-1} \end{aligned}$$

We know that for shareholder P_L to be deceived, it must hold that $(a_0 + a'_0) \cdot (b_0 + b'_0) = N$. However, this is not feasible because the product of any two numbers other than q_1 and q_2 is not equal to N . Therefore, one of these two numbers must be q_1 and the other q_2 . Since $q_1 < q_2$, the constant factor $f(x)$ must be q_1 . In this case, $a_0 = q_1$, and we have:

$$S = a_0 - a'$$

Therefore, the probability that $L - 1$ shareholders can deceive shareholder P_L is $\varepsilon = 0$, and the possibility of cheating does not exist.

5. Comparison with some existing schemes

In most existing schemes in the field of cheat detection, participants are divided into two groups: honest and dishonest. Honest participants play the role of detecting cheaters among the set of dishonest participants.

Therefore, there is a threshold value for the number of dishonest participants for detection by the cheating detectable secret sharing scheme. In this paper, this threshold value is referred to as the cheat detection capability.

In this section, the proposed scheme is compared with existing cheat detectable secret sharing schemes in terms of cheat detection, the maximum number of detectable cheats, the combiner's verification capability, and the success probability in cheating. Referring to Table 1 in our scheme, the success probability of cheating by dishonest participants is $\varepsilon = 0$, meaning that in our proposed scheme, the possibility of cheating does not exist, demonstrating the effectiveness of our scheme compared to existing ones.

Table 1
Comparison of the proposed scheme with the other cheating detection.

Schemes	Maximum cheaters detect	Probability of successful cheating	Combiner verification
Pieprzyk and Zhang	1	$\varepsilon = \frac{1}{q}$	×
Liu et. al. Scheme	$t - 1$	$\varepsilon = \frac{1}{q}$	×
K. Sato and S. Obana	$t - 1$	$\varepsilon = \frac{1}{q}$	×
Cabello et al.	$t - 1$	$\varepsilon = \frac{2}{q}$	×
Proposed	$t - 1$	$\varepsilon = 0$	✓

6. Conclusions

In this paper, we introduce a cheating detection method based on factorizing a positive integer formed by two large prime numbers. We also enhance security by generating a quasi-secret, restricting secret reconstruction to principal shareholders. This ensures the authenticity of the combiner, preventing access to the secret.

Our approach, akin to the Shamir scheme but using two polynomials for cheating detection, proves applicable in practical environments and other Shamir-based threshold encryption systems, effectively detecting cheating. This study contributes to developing new methods and improving existing tools in secret sharing and information security.

The efficiency of our approach encompasses:

- Participants may not receive an equal number of shares.
- Classification of shareholders.
- Verification of the combiner's authenticity.
- After polynomial reconstruction, the secret remains undisclosed; only shareholders can access it.

References

- [1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613 (1979).
- [2] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing Requirements Knowledge*, International Workshop on, pp. 313-313, IEEE Computer Society (1979).

- [3] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133-138 (1989).
- [4] M. Carpentieri, A. D. Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 118-125, Springer (1993).
- [5] Y. Tian, C. Peng, and J. Ma, "Publicly variable secret sharing schemes using bilinear pairings," *Int. J. Netw. Secur.*, vol. 14, no. 3, pp. 142-148 (2012).
- [6] J. Pieprzyk and X.-M. Zhang, "Cheating prevention in linear secret sharing," in *Australasian Conference on Information Security and Privacy*, pp. 121-135, Springer (2002).
- [7] M. P. Jhanwar and R. Safavi-Naini, "On the share efficiency of robust secret sharing and secret sharing with cheating detection," in *International Conference on Cryptology in India*, pp. 179-196, Springer (2013).
- [8] S. Cabello, C. Padro, and G. Saez, "Secret sharing schemes with detection of cheaters for a general access structure," *Designs, Codes and Cryptography*, vol. 25, pp. 175-188 (2002).
- [9] Y. Liu, "Linear (k, n) secret sharing scheme with cheating detection," *Security and Communication Networks*, vol. 9, no. 13, pp. 2115-2121, 2016.
- [10] S. Dutta, S. Jiang, and R. Safavi-Naini, "Lower bounds on the share size of leakage resilient cheating detectable secret sharing," in *International Conference on Cryptology and Network Security*, pp. 468-493, Springer (2023).
- [11] M. A. Hossain and R. Bandi, "A variable multi-secret sharing scheme based on intersection pair of cyclic codes," *International Journal of Foundations of Computer Science*, pp. 1-21 (2023).
- [12] K. Sato and S. Obana, "Cheating detectable secret sharing scheme from multiplicative homomorphic authentication function," in 2021

Ninth International Symposium on Computing and Networking Workshops (CANDARW), pp. 372-378, IEEE (2021).

- [13] L. Cianiullo and H. Ghodosi, "Outsourced cheating detection for secret sharing," *International Journal of Information Security*, vol. 20, no. 6, pp. 871-878 (2021).
- [14] G. Meriem and S. Bouroubi, "A new ideal secret sharing scheme based on a tree," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1-18 (2021).
- [15] H.-M. Sun, S.-P. Shieh, "Constructing perfect secret sharing schemes for general and uniform access structures," *Journal of information science and engineering*, vol. 15, no. 5, pp. 679-689, 1999.
- [16] N. M. Al-Saidi, N. Rajab, M. Md. Said, and K. Kadhim, "Perfect secret sharing scheme based on vertex domination set," *International Journal of Computer Mathematics*, vol. 92, no. 9, pp. 1755-1763 (2015).

Received July, 2024