

Received November 29, 2019, accepted January 15, 2020, date of publication January 22, 2020, date of current version January 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968728

Information Privacy Protection Based on Verifiable (t, n) -Threshold Multi-Secret Sharing Scheme

NA WANG¹, YUANYUAN CAI², JUNSONG FU³, AND XIQI CHEN¹

¹School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

²National Engineering Laboratory for Agri-Product Quality Traceability and Beijing Key Laboratory of Big Data Technology for Food Safety, Beijing Technology and Business University, Beijing 100048, China

³School of Cyberspace Security and National Engineering Lab for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Yuanyuan Cai (caiyuanyuan@btu.edu.cn)

This work was supported by the China Postdoctoral Science Foundation (2019M650020), Beijing Natural Science Foundation (4184084, 4204107), Fundamental Research Funds for the Central Universities (500419810), Funds of “YinLing” (A02B01C03-201902D0), National Key Technology R&D Program of China (2016YFD0401205), Humanity and Social Science Youth Foundation of Ministry of Education of China (17YJCZH007).

ABSTRACT General secret sharing schemes comprise a secret dealer and a number of participants. The dealer can randomly generate a secret and then distribute shares of the secret to the participants. Verifiable multi-secret sharing enables a dealer to share multiple secrets among a group of participants such that the deceptive behaviors of the dealer and the participants can be detected. However, in the absence of secure channels, few verifiable secret sharing schemes can simultaneously share multiple secrets at one time. In this paper, we present an information privacy protection and verifiable multi-secret sharing scheme with a simple structure and high security. Each participant can verify correctness of the share distribution process based on public information published by the dealer and guarantee validity of the received share to avoid offering fake information in the process of restoring the original secret. Our performance and security analysis indicate that the newly proposed scheme is more efficient and practical while maintaining the same level of security compared with similar protocols available.


INDEX TERMS Privacy protection, verifiable, threshold, multi-secret.

I. INTRODUCTION

Information privacy protection has become an important issue in the field of information security, and secret sharing is a promising technology among privacy protection schemes. In real life, it is dangerous to keep some sensitive and important information, such as passwords of opening bank safes or launching missiles, by a single person, because the information is easy to be damaged, lost or tampered. Therefore, it is urgent to establish novel key dispersion schemes. In the custody system, a secret sharing system is established, which is an important method to protect information security and data security. Since Blakley [1] and Shamir [2] introduced a secret sharing scheme in 1979, secret sharing has been extensively investigated in the literature. In a secret sharing

scheme, the dealer divides the secret into several shares and distribute them among a group of participants. In general, each share alone cannot reveal any useful information about the secret, and some specified subsets of participants are able to re-establish the original secret information in a cooperative manner. Meanwhile, those unauthorized subsets of participants are unable to reconstruct the original secret information.

In recent years, most secret sharing schemes [3]–[6] have strong limitations on the secret sharing process and they can only share one secret at one time among a set of participants, which is of low efficiency, as shown in Fig. 1. However, another drawback in their scheme is the assumption that both the dealer and the participant are unconditionally honest. In this way, the fraud of malicious dealer cannot be discovered. The deceptive behavior of malicious participants is unavoidable in the process of reconstruction. Verifiable multi-secret sharing enables a dealer to share multiple secrets

The associate editor coordinating the review of this manuscript and approving it for publication was Corrado Mencar .

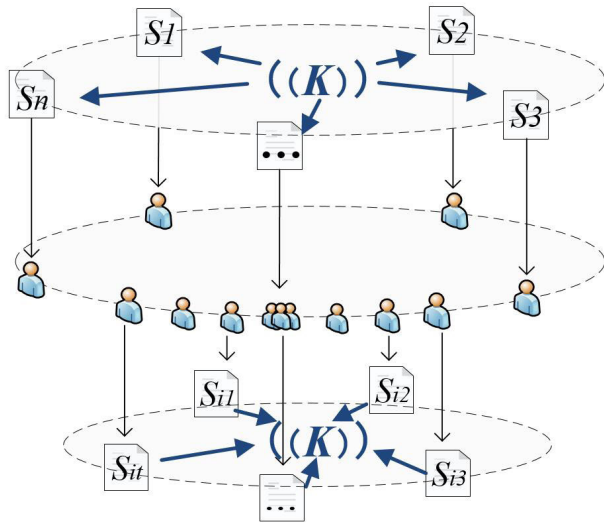


FIGURE 1. Secret distribution process of existing schemes.

among a group of participants such that the deceptive behaviors of the dealer and the participants can be detected.

In practical applications, [3]–[6] can only share one secret during one secret sharing process, and they cannot be used to share multiple secrets simultaneously. To solve this problem, Harn [7] proposed a multi-secret sharing scheme that can detect dishonest dealer and vicious participants at the same time. In order to share any set of secrets, each participant only needs to keep a reusable share. Nevertheless, Lin and Wu [8] pointed out that the shortcoming of Harn's scheme is that it needs to carry out a large number, $\frac{n!}{(n-t)!t!}$, of modular exponentiations and running interactive verification protocol to verify the effectiveness of shares. Chen *et al.* [9] proposed an alternative (t, n) verifiable secret sharing scheme to avoid the shortcomings of the scheme in [7]. Moreover, Lin and Wu [8] prove that the scheme in [7] was inefficient, because the dealer had to record the shares of all participants, which required the execution of $2n$ modular exponents to calculate an n -dimensional verification vector for each shared secret. Consequently, Lin and Wu [8] propose a (t, n) threshold verifiable multi-secret sharing scheme, which is designed based on mathematical difficulties in cryptography. The so-called mathematical difficulty problem refers to the problem of large integer factorization and discrete logarithm. In [10], He *et al.* pointed out that the scheme designed in [8] cannot resist the deception of participants, because dishonest participants can provide false shares to deceive other honest participants. Chang *et al.* [11] improved the scheme proposed in [8]. The improved scheme successfully to a new version which overcomes the shortcomings of the scheme in [8], and is superior to other verifiable multi-secret sharing schemes in terms of computational efficiency. Unfortunately, Huang *et al.* [12] found that the verifiable multi-secret sharing scheme in [11] could not resist the collusion attacks.

One situation is that the dealer can distribute some false shares to the participants, and the other is that malicious

participants deliberately provide false shares to other participants, both of which can result in the secret being unable to be rebuilt successfully. To overcome these drawbacks, several verifiable secret sharing schemes have been proposed in [13]–[17] to resist dishonest dealer or malicious participants. These verifiable secret sharing schemes allow participants to verify correctness of the dealer's share of the distribution phase. At the same time, it also ensures that participants cannot make mistakes in the reconstruction phase. However, these schemes are not verifiable in some specific applications. For the schemes in [13]–[17], each participant can only verify the share they hold, but not all the shares held by other participants in the distribution phase. This makes it impossible for participants to prevent the sharing of malicious participants from being mixed in secret reconstruction process.

Chor *et al.* [18] introduced a practical verifiable secret sharing scheme. In a verifiable secret sharing scheme, participants can verify whether their shares are consistent and they can detect fraudulent behavior by dishonest traders. Verifiable secret sharing scheme is a basic tool in cryptographic research [19]. In order to solve the fraudulent behavior of the participants, we investigated deception immunity secret sharing [20]–[23] and publicly verifiable secret sharing [24]. The publicly verifiable secret sharing scheme presented by Junta *et al.* [24] can detect the cheating behavior of dealers, and it can also detect the cheating behavior of any participant.

Shekhi-Garjan *et al.* [19] proposed the threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem. The challenge of this scheme is to solve equations. It is well known that constructing Lagrange interpolation polynomial is easier to realize than solving equations. The multi-secret sharing scheme designed in [25]–[27] can not avoid the deception of dealer and participants, and its practicability is not high. The verifiable multi-secret sharing scheme proposed in [28], [29] requires a secure channel for secret distribution, and maintaining a secure channel increases the operating cost of the system.

Our contributions are summarized as follows:

- To make the shares can be flexibly and securely distributed among the participants, we present an information privacy protection and verifiable multi-secret sharing scheme with a simple structure and high security.
- As shown in Fig. 2, a set of secrets can be shared at one time and the reality of the received shares can be verified by the participants based on public information posted by the dealer. In addition, the secret reconstruction protocol can also examine the correctness of the pooled shares to accurately recover the original secrets.
- The scheme we designed is suitable for the environment without safe channels. Through a series of theoretical proofs and performance analysis, it is proved that our scheme is information-theoretical secure and more time-efficient than other schemes.

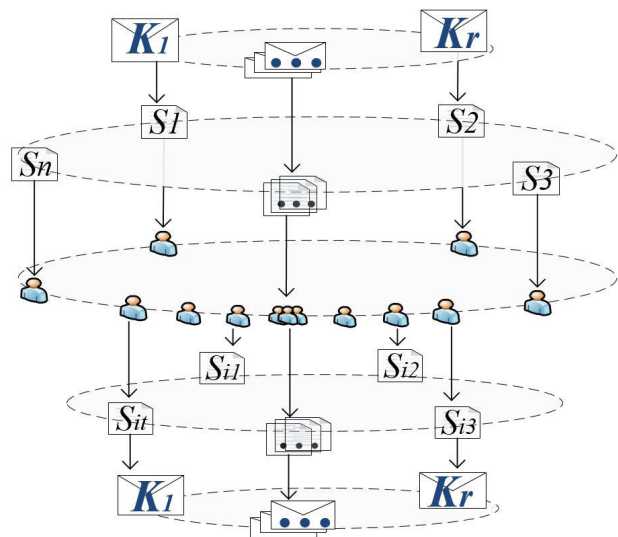


FIGURE 2. Secret distribution process of our scheme.

The rest of this paper is organized as follows: we first introduce some related work to this topic in Section II. Then, a new scheme is proposed in Section III. The security of our scheme is theoretically proved in Section IV. Section V presents the efficiency is evaluated. And Section VI covers the conclusion.

II. RELATED WORK

In this section, we mainly present access structure of (t, n)-threshold secret sharing schemes and properties of verifiable secret sharing (VSS) schemes.

A. ACCESS STRUCTURE

Let $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ be a set of n participants. Let Γ be a set of subsets of \mathcal{P} , i.e., $\Gamma \subseteq 2^{\mathcal{P}}$. The subsets in Γ are those subsets of participants that should be able to compute the secret. Γ is called a *general access structure* and each subset in Γ is called an *authorized subset*.

The method of sharing secret S among the n participants is *perfect secret sharing scheme* if it can realize the access structure with the following two properties: 1. The secret S can be determined by an authorized subset of participants when their shares are placed together; 2. Nothing about secret S can be determined when the shares of an unauthorized subset of participants is pooled.

A (t, n) -threshold secret sharing scheme can map a secret S to a set of shares which are distributed to n participants $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$. In this way, any $t(t \leq n)$ participants can reconstruct secret S by putting their shares together but a group with less than t members cannot do so. All the qualified subsets of \mathcal{P} form the access structure Γ . The set of minimal authorized subsets of Γ is denoted Γ_0 and is called the *basis* of Γ , i.e., $\Gamma = \{C \subseteq \mathcal{P} : B \subseteq C, B \in \Gamma_0\}$. In the case of a (t, n) -threshold access structure, the basis Γ_0 consists of all subsets of exactly t participants.

B. VERIFIABLE SECRET SHARING SCHEME

The verifiable secret sharing (VSS) scheme is a modification of the traditional secret sharing scheme, and it is mainly used to address issues of non-honest distribution center. VSS schemes are designed based on the usual secret sharing schemes with additional verification operations. In the VSS scheme, the dealer distributes not only the shares of the secret but also some extra information about the secret fragments to the participants. Once a member receives his shares, he can verify whether the shares are correct based on the broadcasted information. In the secret reconstruction phase, each participant uses the same method to verify correctness of secret fragments of other members. It can be observed that VSS is able to resist the following two kinds of active attack:

1. Some shares are tampered before being sent to the participants in the secret distribution protocol.
2. Participants submit error shares to the secret reconstruction protocol.

III. PROPOSED SCHEME

In this section, we present an information privacy protection scheme based on verifiable (t, n) threshold multi-secret sharing scheme. The design details are presented as follows. Let D be a dealer and $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ be a set of n participants. The secrets to be distributed are denoted as S_1, S_2, \dots, S_l .

• Initialization phase:

The dealer selects two large primes p, q and computes $N = p \cdot q$. The dealer randomly selects a prime Q greater than N and an integer $g \in [\sqrt{N}, N]$ different from p and q . The dealer publishes $\{g, N, Q\}$.

A participant P_i randomly chooses an integer $SK_i \in [2, N]$ as its private key, and computes $PK_i = g^{SK_i} \text{ mod } N$ as its public key. The participant P_i sends PK_i to the dealer D , and D ensures that for $P_i \neq P_j$. Therefore, we can infer that $PK_i \neq PK_j$.

• Construction phase:

In order to share l secrets $\{S_1, S_2, \dots, S_l\}$ in n participants $\{P_1, P_2, \dots, P_n\}$, we need to ensure that at least t participants worked together to recover l secrets in parallel manner during a sharing process. The design details of the secret distribution process are discussed as follows:

- The dealer D randomly chooses an integer $SK_0 \in [2, N]$ as its private key, where SK_0 is interprime of $p - 1$ and $q - 1$. Then, the dealer computes $PK_0 = g^{SK_0} \text{ mod } N$ as its public key.

- D computes M such that $SK_0 \cdot M \equiv 1 \text{ mod } \varphi(N)$, where $\varphi(N)$ denotes Euler function and $\varphi(N) = (p - 1) \cdot (q - 1)$. Then, D publishes M .

- D computes $R_i = PK_i^{SK_0} \text{ mod } N$ and uses $n + l$ points $(0, S_1), (1, S_2), \dots, (l - 1, S_l), (PK_1, R_1), (PK_2, R_2), \dots, (PK_n, R_n)$ constructs the $(n + l - 1)$ -th degree polynomial $f(x) \text{ mod } Q$ as follows:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n+l-1}x^{n+l-1} \text{ mod } Q$$

- D takes out the $n + l - t$ smallest integers $h_1, h_2, \dots, h_{n+l-t}$ from the set $[l, Q - 1] - \{PK_i | i = 1, 2, \dots, n\}$ and computes $f(h_1), f(h_2), \dots, f(h_{n+l-t})$. The final D publishes $(h_i, f(h_i))$, where $i = 1, 2, \dots, n + l - t$.

• **Verification phase:**

The participant P_{v_j} in $A = \{P_{v_1}, P_{v_2}, \dots, P_{v_t}\} \subseteq \Gamma$ first computes $T_{v_j} = PK_0^{SK_{v_j}} \bmod N$, and then verify the following equation with each other.

$$T_{v_j}^M = PK_{v_j} \bmod N,$$

where $v_j \neq v_i$ and $v_j \in \{v_1, v_2, \dots, v_t\} \subseteq \{1, 2, \dots, n\}$. If the above equation holds, any t participants can reconstruct S_i following algorithm of reconstruction.

• **Algorithm of reconstruction:**

In order to reconstruct l secrets, at least t participants need to cooperate with each other. Let the participants in set $A = \{P_{v_1}, P_{v_2}, \dots, P_{v_t}\} \subseteq \Gamma$ cooperate to reconstruct S_1, S_2, \dots, S_l .

First of all, the participants in A constructed $n + l - 1$ -th degree Lagrange interpolation polynomial using $n + l - t$ points $(h_i, f(h_i))$, $i = 1, 2, \dots, n + l - t$, which are previously published by the dealer and t points $(PK_{v_1}, T_{v_1}), (PK_{v_2}, T_{v_2}), \dots, (PK_{v_t}, T_{v_t})$ provided by the participants in A as follows.

$$\begin{aligned} f(x) &= \sum_{i=1}^{n+l-t} f(h_i) \prod_{j=1, j \neq i}^{n+l-t} \frac{x - h_j}{h_i - h_j} + \sum_{i=1}^t T_{v_i} \prod_{j=1, j \neq i}^t \frac{x - T_{v_j}}{T_{v_i} - T_{v_j}} \bmod Q \\ &= a_0 + a_1x + a_2x^2 + \dots + a_{n+l-1}x^{n+l-1} \bmod Q \end{aligned}$$

Therefore, participants in A can share l secrets

$$S_i = f(i - 1) \bmod Q, \quad i = 1, 2, \dots, l.$$

IV. SECURITY ANALYSIS

In this section, we analyze the correctness and security of the proposed scheme by three theorems. Further, the proposed scheme realizes information privacy protection.

Theorem 1: Verification is successful if the participant P_{v_j} follows the protocol accurately.

Proof: If the participant P_{v_j} follows the protocol accurately, then we have the following:

$$\begin{aligned} T_{v_j}^M &= (PK_0^{SK_{v_j}})^M \bmod N \\ &= PK_0^{SK_{v_j} \cdot M} \bmod N \\ &= (g^{SK_0})^{SK_{v_j} \cdot M} \bmod N \\ &= (g^{SK_{v_j}})^{SK_0 \cdot M} \bmod N \\ &= (PK_{v_j})^{SK_0 \cdot M} \bmod N \\ &= PK_{v_j} \bmod N, \end{aligned}$$

Theorem 1 shows that if the participant has deceptive behaviors, the other participants cannot pass the verification. This completes the proof.

TABLE 1. Analysis of computational cost.

Scheme	Initialization		Construction Dealer D	Verification Each P_i	Recovery Each P_i
	Dealer D	Each P_i			
[19]	0	1	$n + 1$	0	t
[25]	$2n$	1	0	-	$t - 1$
[26]	0	1	n	-	t
[27]	n	1	n	-	$t - 1$
[28]	0	1	$n + t$	$t + 1$	$(t - 1)(t + 1)$
[29]	n	1	$n + 1$	$t + 1$	$t - 1$
Our scheme	0	0	$n + 1$	$t - 1$	t

Theorem 2: An adversary cannot obtain any useful information about secret S_1, S_2, \dots, S_l from public information.

Proof: No matter whether the adversary is an outside attacker or an internal corrupter, they cannot obtain any information about l secrets.

Case 1: It is impossible for an adversary to construct $f(x)$ directly from the $n + l - t$ points disclosed by the dealer, because the number of public points is less than the power of the $n + l - 1$ -th degree polynomial $f(x)$. Thus, the adversary will not get any information about l secrets.

Case 2: If a corrupt participant becomes an adversary, it is impossible to get any information about l secrets. This is reasonable considering that it is difficult for an adversary to solve SK_i by using the equation about the participant's private key SK_i . For equation $PK_i = g^{SK_i} \bmod N$, given PK_i, g, N , it is difficult to get the private key SK_i of the participant P_i , that equals to solve the discrete logarithm. Similarly, for equation $T_{v_i} = PK_0^{SK_{v_i}} \bmod N$, given T_{v_i}, PK_0, N , it is difficult to solve the private key SK_i of the participant P_i .

This completes the proof.

Theorem 3: The secret $S_i (i = 1, 2, \dots, l)$ can not be recovered if the participant in the set $A_k \in \Gamma_0$ is absent.

Proof: From conditions of the theorem, we know that $A_k \in \Gamma_0, t = |A_k|$. We only consider the following situation: when the size of A_k is $t - 1$, the secret $S_i (i = 1, 2, \dots, l)$ can not be recovered. Apparently, for a set of participants less than $t - 1$ in A_k , it is also impossible to recover the secret $S_i (i = 1, 2, \dots, l)$.

The following equations can be constructed based on the $n + 1 - t$ points $(h_i, f(h_i))$, $i = 1, 2, \dots, n + l - t$, provided by the dealer and the $t - 1$ points $(PK_{v_1}, T_{v_1}), (PK_{v_2}, T_{v_2}), \dots, (PK_{v_{t-1}}, T_{v_{t-1}})$, provided by the $t - 1$ participants in A_k :

$$\left\{ \begin{aligned} a_0 + a_1h_1 + a_2h_1^2 + \dots + a_{n+l-1}h_1^{n+l-1} &= f(h_1) \\ &\vdots \\ a_0 + a_1h_{n+l-t} + a_2h_{n+l-t}^2 + \dots + a_{n+l-1}h_{n+l-t}^{n+l-1} &= f(h_{n+l-t}) \\ a_0 + a_1PK_{v_1} + a_2PK_{v_1}^2 + \dots + a_{n+l-1}PK_{v_1}^{n+l-1} &= T_{v_1} \\ &\vdots \\ a_0 + a_1PK_{v_{t-1}} + a_2PK_{v_{t-1}}^2 + \dots + a_{n+l-1}PK_{v_{t-1}}^{n+l-1} &= T_{v_{t-1}}. \end{aligned} \right.$$

TABLE 2. Compare the performance features of the schemes.

Functionality	[19]	[25]	[26]	[27]	[28]	[29]	Our scheme
Resist cheating by the dealer D	YES	NO	NO	NO	YES	YES	YES
Resist cheating by dishonest participant P_i	YES	NO	NO	NO	YES	YES	YES
Without secret channel	YES	NO	NO	NO	NO	NO	YES
Recover multi-secrets in parallel	YES	YES	YES	YES	NO	NO	YES
Reuse of the secret shadows	NO	NO	NO	NO	NO	NO	YES

i.e.

$$\begin{pmatrix} f(h_1) \\ \vdots \\ f(h_{n+t-t}) \\ T_{v_1} \\ \vdots \\ T_{v_{t-1}} \end{pmatrix} = D \begin{pmatrix} a_0 \\ \vdots \\ a_{n+t-t} \\ a_{n+t-t+1} \\ \vdots \\ a_{n+t-1} \end{pmatrix}$$

where,

$$D = \begin{pmatrix} 1 & \dots & h_1^{n+t-t} & h_1^{n+t-t+1} & \dots & h_1^{n+t-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 1 & \dots & h_{n+t-t}^{n+t-t} & h_{n+t-t}^{n+t-t+1} & \dots & h_{n+t-t}^{n+t-1} \\ 1 & \dots & PK_{v_1}^{n+t-t} & PK_{v_1}^{n+t-t+1} & \dots & PK_{v_1}^{n+t-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 1 & \dots & PK_{v_{t-1}}^{n+t-t} & PK_{v_{t-1}}^{n+t-t+1} & \dots & PK_{v_{t-1}}^{n+t-1} \end{pmatrix}$$

These are systems of linear equations where the rank of coefficient matrices is less than the number of variables, which means that the equations has at least Q answers and the probability for a set of participants less than $t - 1$ in A_k to pick out the genuine $\{a_0, \dots, a_{n+t-t}, a_{n+t-t+1}, \dots, a_{n+t-1}\}$ is not more than $\frac{1}{Q}$. As Q is a large primer, this probability can be ignored. Theorem 3 is proved.

V. PERFORMANCE ANALYSIS

In this section, we compare our scheme with the existing schemes in terms of main performance features and computational cost.

When comparing the computational costs of our scheme with those of other similar schemes, we listed the number of the most time-consuming operations in each phase of these schemes. The most time-consuming operation we consider here is the modular exponentiation. Table 1 lists the main computational costs of our new scheme as well as the main computational costs of the other six schemes. As shown in Table 1, our scheme is the most effective one compared to other schemes in the initialization and construction phases. The efficiency of our scheme is slightly higher than that of the schemes in [19], [25]–[27], and lower than that of the

schemes in [28] and [29]. The computational costs of these seven schemes are almost the same in the recovery phase. Since we have added conformance tests to prevent cheating between dealer and participants, the verification phase of our new scheme requires more modular exponentiation than the schemes in [19], [25]–[27]. Such an increase in computational costs is necessary to prevent cheating on dealer and participants.

We also compare the main performance features of our new scheme with other schemes. Table 2 shows that our new scheme has all the performance features. In [19], participants hold different shares in different rounds of multi-secret sharing, which increasing the storage space of the system. None of the schemes proposed in [25]–[27] can resist deceit between dishonest distributors and participants. The scheme in [28], [29] cannot implement multi-secret sharing in parallel. It requires a secure channel in the secret distribution process. However, maintaining a secure channel will increase the cost of system operation.

In the view of the above shortcomings, this paper proposed a verifiable (t, n) threshold multi-secrets sharing scheme based on the difficulty of discrete logarithm, which has the following properties: 1) it can prevent cheating between dealer and participants; 2) it does not need to maintain the secure channel in the secret distribution, so that the scheme can be applied in the system where there is no secure channel; 3) It realizes the sharing of multi-secrets in parallel through one-time secret sharing process; 4) it allows participants to reuse their shares in different rounds of multi-secret sharing.

VI. CONCLUSION

The multi-secret sharing scheme provides a practical technique for sharing multiple secrets among a group of participants. Verifiable multi-secret sharing schemes not only share multiple secrets among a group of participants, but also detect cheating by dealers or participants. They are important tools for preserving multiple secrets (such as cryptography keys) and designing secure multi-party protocols. In this study, we present an information privacy protection based on verifiable (t, n) -threshold multi-secret sharing scheme. Moreover, we seamlessly integrate the verification algorithm to our secret sharing scheme so that one can verify the correctness of the shares. The new scheme we designed can be used in the environment without secure channels. We evaluate the performance of the proposed verifiable multi-secret sharing scheme through theoretical analysis and a series of simulations. Results prove that the scheme can provide effective

information privacy protection. In addition, we assessed the time efficiency of the proposed programme and simulation results illustrate that the scheme is also very efficient.

REFERENCES

- [1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirement Knowl. (MARK)*, vol. 48, Jun. 1979, pp. 313–317
- [2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [3] G. Reza, "Resolving a common vulnerability in secret sharing scheme-based data outsourcing schemes," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 2, pp. 1–11, 2019.
- [4] X. Zhang, J. Duan, and J. Zhou, "A robust secret sharing QR code via texture pattern design," in *Proc. Asia-Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Nov. 2018, pp. 903–907.
- [5] R. L. De Souza, M. Vigil, R. Custodio, F. Caullery, L. Moura, and D. Panario, "Secret sharing schemes with hidden sets," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, vol. 1, Jun. 2018, pp. 713–718.
- [6] I. Cascudo, J. Skovsted Gundersen, and D. Ruano, "Improved bounds on the threshold gap in ramp secret sharing," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4620–4633, Jul. 2019.
- [7] L. Harn, "Efficient sharing (broadcasting) of multi-secret," in *Proc. Comput. Digit. Techn.*, vol. 142, 1995, pp. 237–240.
- [8] T. Y. Lin and T. C. Wu, "(t, n) threshold verifiable multi-secret sharing scheme based on factorization intractability and discrete logarithm module a composite problems," *IEEE Proc. Comput. Digital Tech.*, vol. 146, pp. 264–268, Sep. 1999.
- [9] L. Chen, C. D. Gollmann, J. Mitchell, and P. Wild, "Secret sharing with reusable polynomials," in *Proc. ACISP, 1997*, pp. 183–193.
- [10] W.-H. He and T.-S. Wu, "Comment on Lin–Wu (t, n)-threshold verifiable multiset sharing scheme," *IEE Proc. Comput. Digit. Techn.*, vol. 148, no. 3, p. 139, May 2001.
- [11] T. Y. Chang, M. S. Hwang, and W. P. Yang, "An improvement on the Lin–Wu (t,n) threshold verifiable multi-secret sharing scheme," *Appl. Math. Comput.*, vol. 163, pp. 169–178, Apr. 2005.
- [12] M. Huang, J. Zhang, and S. Xie, "A secure and efficient (t, n) threshold verifiable multi-secret sharing scheme," in *Computational Intelligence and Security (Lecture Notes in Computer Science)*, vol. 3802. Berlin, Germany: Springer-Verlag, 2005, pp. 532–537.
- [13] S. Mashhadi, "Secure publicly verifiable and proactive secret sharing schemes with general access structure," *Inf. Sci.*, vol. 378, pp. 99–108, Feb. 2017.
- [14] K. Peng, "Critical survey of existing publicly verifiable secret sharing schemes," *IET Inf. Secur.*, vol. 6, no. 4, pp. 249–257, Dec. 2012.
- [15] Y. Liu, F. Zhang, and J. Zhang, "Attacks to some verifiable multi-secret sharing schemes and two improved schemes," *Inf. Sci.*, vol. 329, pp. 524–539, Feb. 2016.
- [16] T.-Y. Wu and Y.-M. Tseng, "A pairing-based publicly verifiable secret sharing scheme," *J. Syst. Sci. Complex.*, vol. 24, no. 1, pp. 186–194, Feb. 2011.
- [17] J. Zhang and F. Zhang, "Information-theoretical secure verifiable secret sharing with vector space access structures over bilinear groups," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.*, 2014, pp. 318–329.
- [18] B. Chor, S. Goldwasser, and S. Micali, "Verifiable secret sharing and achieving simultaneity in the presence of faults," *Proc. 26th IEEE Symp. Found. Comput. Sci. (FOCS)*, Washington, DC, USA, Oct. 1985, pp. 251–260.
- [19] M. Sheikhi-Garjan, M. Bahramian, C. Doche, "Threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem," *IET Inf. Secur.*, vol. 13, no. 3, pp. 278–284, 2019.
- [20] J. Pieprzyk and X. M. Zhang, "Constructions of cheating immune secret sharing," in *Information Security and Cryptology (Lecture Notes in Computer Science)*, vol. 2288. Berlin, Germany: Springer-Verlag, 2001, pp. 226–243.
- [21] J. Pieprzyk and X. M. Zhang, "On cheating immune secret sharing," *Discrete Math. Theor. Comput. Sci.*, vol. 6, no. 4, pp. 253–264, 2004.
- [22] R. D. Prisco and A. D. Santis, "Cheating immune (2,n)-threshold visual secret sharing," *Security and Cryptography for Networks (Lecture Notes in Computer Science)*. Berlin, Germany: Springer, 2006, pp. 216–228.
- [23] X. M. Zhang and J. Pieprzyk, "Cheating immune secret sharing," in *Proc. 3rd Int. Conf. Inf. Commun. Secur. (ICICS)*, vol. 2229. Berlin, Germany: Springer-Verlag, 2001, pp. 144–149.
- [24] J. Imai, M. Mimura, and H. Tanaka, "Verifiable secret sharing scheme using hash values," in *Proc. 6th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Nov. 2018, pp. 405–409.
- [25] E. Zhang, X. Duan, and S. Yiu, "Server-aided multi-secret sharing scheme for weak computational devices," *Comput., Mater. Continua*, vol. 56, no. 3, pp. 401–414, 2018.
- [26] L.-J. Pang and Y.-M. Wang, "A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing," *Appl. Math. Comput.*, vol. 167, no. 2, pp. 840–848, Aug. 2005.
- [27] H. X. Li, C. T. Cheng, and L. J. Pang, "A new (t,n)-threshold multi-secret sharing scheme," in *Proc. Int. Conf. Comput. Inf. Sci.* Berlin, Germany: Springer, 2005, pp. 421–426.
- [28] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Comput. Standards Inter.*, vol. 29, no. 1, pp. 138–141, Jan. 2007.
- [29] Z. Eslami and J. Zarepour Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," *Inf. Sci.*, vol. 180, no. 15, pp. 2889–2894, Aug. 2010.



NA WANG received the Ph.D. degree from the School of Mathematical Sciences, Xiamen University, in 2018. She is currently a Postdoctoral Fellow with the School of Computer Science, Beijing University of Posts and Telecommunications. Her research interests include cryptography, message sharing, and information security issues in distributed and cloud systems.



YUANYUAN CAI received the Ph.D. degree in software engineering from Beijing Jiaotong University, in 2016. She is currently a Lecturer with the School of Computer and Information Engineering, Beijing Technology and Business University. Her research interests include semantic computing, information security, natural language processing, and data mining.



JUNSONG FU received the Ph.D. degree in communication and information system from Beijing Jiaotong University, in 2018. He is currently an Assistant Professor with the School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interests include in-network data processing, network security and information privacy issues in distributed systems, and the Internet of Things.



XIQI CHEN is currently pursuing the B.S. degree in the Internet of Things engineering with the Beijing University of Posts and Telecommunications. She is also participating on a Project of the National University Student Innovation Program. Her research interest is information security on the Internet of Things.

...