Hindawi
Mobile Information Systems
Volume 2020, Article ID 1039898, 9 pages
https://doi.org/10.1155/2020/1039898

Research Article

A New Efficient and Secure Secret Reconstruction Scheme (SSRS) with Verifiable Shares Based on a Symmetric Bivariate Polynomial

Chingfang Hsu,[1] **Lein Harn**,[2] **Shan Wu**,[3] **and Lulu Ke**[1]

[1]*Computer School, Central China Normal University, Wuhan 430079, China*
[2]*Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City 64110, MO, USA*
[3]*School of Management, Huazhong University of Science and Technology, Wuhan 430074, China*

Correspondence should be addressed to Shan Wu; hariny@163.com

Received 9 January 2020; Revised 7 October 2020; Accepted 4 November 2020; Published 15 December 2020

Academic Editor: Prosanta Gope

Secret sharing (SS) schemes have been widely used in secure computer communications systems. Recently, a new type of SS scheme, called the secure secret reconstruction scheme (SSRS), was proposed, which ensures that the secret can only be recovered by participants who present valid shares. In other words, if any outside adversary participated in the secret reconstruction without knowing any valid share, the secret cannot be recovered by anyone including the adversary. However, the proposed SSRS can only prevent an active attacker from obtaining the recovered secret, but cannot prevent a passive attacker from obtaining the secret since exchange information among participants is unprotected. In this paper, based on bivariate polynomials, we propose a novel design for the SSRS that can prevent both active and passive attackers. Furthermore, we propose a verification scheme which can verify all shares at once, i.e., it allows all shareholders to efficiently verify that their shares obtained from the dealer are generated consistently without revealing their shares and the secret. The proposed scheme is really attractive for efficient and secure secret reconstruction in communications systems.

1. Introduction

Secret sharing (SS) schemes have been widely used in secure computer communications systems [1–8]. Blakley [9] and Shamir [10] independently introduced the concept of the secret sharing in 1979. In a (t, n) secret sharing (SS) scheme, the secret s is divided into n shares by a dealer and is shared among n shareholders such that any t or more than t shares can reconstruct the secret, but fewer than t shares cannot obtain any information about the secret s.

Shamir's (t, n) SS scheme used a linear polynomial. But, in practical applications, possible threats make Shamir's secret reconstruction scheme very complicated, especially when there are more than t participants in the secret reconstruction. One straightforward approach to ensure that all participants are shareholders is to use user authentication scheme among all participants at the beginning of the secret reconstruction. This approach is a time-consuming process since user authentication can authenticate one user at a time. In fact, only the dealer needs to know who is the shareholder initially. In the secret reconstruction, shareholders do not need to know each other. The secret can only be reconstructed successfully if all shares are legitimate. If all shares are legitimate shares, the secret can be reconstructed. On the other hand, if there is any illegitimate share, the secret cannot be reconstructed.

Recently, a new type of SS scheme called the secure secret reconstruction scheme [11] (SSR), which ensures that the secret can only be recovered by participants who present valid shares, has been developed. However, the scheme can only prevent an active attacker from obtaining the recovered secret, but cannot prevent a passive attacker from obtaining the secret since exchange information among participants is unprotected.

Chor et al. [12] proposed the notion of verifiable secret sharing (VSS) in which shareholders can verify that their shares are valid without revealing the secrecy of their shares and the secret. Based on security assumptions, there are two different types of VSSs, schemes that are computationally secure and unconditionally secure. Feldman [13] and Pedersen [14] VSSs are based on cryptographic commitment schemes. The security of Feldman's VSS is on the hardness of solving discrete logarithm, while the privacy of Pedersen's VSS is unconditionally secure and the correctness of the shares is based on a computational assumption. Benaloh [15] proposed an interactive VSS which is unconditionally secure. Stinson et al. [16] proposed an unconditionally secure VSS, and Patra et al. [17] proposed a generalized VSS scheme. Stadler [18] proposed the first publicly verifiable secret sharing (PVSS) scheme which allows each shareholder to verify the validity of all shares. Most noninteractive VSSs [13, 14] can only verify the validity of his/her own share, but not of other shareholders' shares. PVSSs [18, 19] use interactive proofs of knowledge. These proofs can be made noninteractive using the Fiat–Shamir technique [20]. The security of Schoenmaker's PVSS [21] is based on the discrete-logarithm problem. The scheme is quite simple, but some noninteractive zero-knowledge proofs have been used. Peng and Wang's PVSS [22] uses a linear code, and Ruiz and Villar's PVSS [23] uses Pailler's cryptosystem [24]. There are noninteractive PVSSs based on bilinear pairing [25, 26]. We can see that most of these VSSs can only verify one share at a time and are computationally secure, which are based on computational assumptions.

In summary, let us briefly clarify differences among the SSR [11], VSS, and Changeable secret sharing scheme [27, 28] (TCSS). These three different schemes have different security features. According to Harn [11], in SSR, the secret can only be reconstructed successfully by all participated shareholders who contributed valid shares. In other words, SSR requires every participated shareholder to contribute a share and the secret cannot be reconstructed if there are fewer than the number of participants in the process. Note that this number may be larger than the threshold. In a VSS, shareholders can verify that their shares are generated consistently by a dealer without revealing their shares and the secret. In a TCSS, the threshold can be dynamically changed in the process.

The motivation of our paper is to construct an efficient and secure secret reconstruction scheme with verifiable shares. The SSRS can prevent both active and passive attackers at the same time. The scheme is unconditionally secure and can verify all shares at once. Our design is based on symmetric bivariate polynomials. The primary reason to adopt symmetric bivariate polynomials is that shares generated by a symmetric bivariate polynomial can be used to (a) verify all shares at once, (b) recover the secret, and (c) establish pairwise secret keys between shareholders to protect the exchange information in the secret reconstruction. There is no additional user authentication or key distribution needed. Thus, it is very efficient.

Following this line of research, in this paper, we propose a novel design for an efficient and secure secret reconstruction scheme with verifiable shares, where the SSRS can prevent both active and passive attackers. At the same time, our VSS allows all shareholders to verify that their shares obtained from the dealer are valid without revealing their shares and the secret, where shareholders just verify that shares are generated by a symmetric bivariate polynomial consistently. Here, we summarize the contributions of our paper.

(i) A secure secret reconstruction scheme based on symmetric bivariate polynomials is proposed

(ii) The proposed secure reconstruction scheme can prevent both active and passive outside attacks

(iii) An efficient VSS which verifies all shares generated by a symmetric polynomial consistently at once is proposed

The rest of this paper is organized as follows: In the next section, we introduce some preliminaries. In section 3, we describe models of our proposed schemes including scheme description, adversaries, and properties. We propose our secure secret reconstruction with verifiable shares in section 4. The conclusion is included in section 5.

2. Review of SSs Based on Polynomials

In Shamir's (t, n) SS [9], the dealer selects a univariate polynomial, $f(x)$, with degree $t-1$ and $f(0) = s$ where s is the secret. The dealer generates shares, $f(x_i) \bmod p$, $i = 1, 2, \ldots, n$ for shareholders, where p is a prime with $p > s$ and x_i is the public information associated with each shareholder, U_i. Each share, $f(x_i)$, is an integer in $\mathrm{GF}(p)$ Shamir's (t, n) SS satisfies security requirements of a (t, n) SS. That is, (a) with t or more than t shares can reconstruct the secret and (b) with fewer than t shares cannot obtain any information of the secret. Shamir's SS is unconditionally secure.

In Shamir's (t, n) SS, shareholders cannot verify the validity of their shares obtained from the dealer. In 1985, Chor et al. [12] extended the notion of SS and proposed the first verifiable secret sharing (VSS). Verifiability is the property of a VSS which allows shareholders to verify their shares. Invalid shares may be caused either by the dealer during share generation or by channel noise during transmission. VSS is performed by shareholders after receiving their shares from the dealer and before using their shares to reconstruct the secret. If invalid shares have been detected, shareholders can request the dealer to regenerate new shares. There are many (t, n) VSSs [29–34] using bivariate polynomials, denoted them as BVSSs. A bivariate polynomial with degree $t-1$ can be represented as $F(x, y) = \sum_{i=0}^{t-1} \sum_{j=0}^{t-1} a_{i,j} x^i y^j \bmod p$ where $a_{i,j} \in \mathrm{GF}(p)$. We can classify BVSSs into two types, the symmetric BVSSs, denoted as SBVSSs [30, 32, 34], and the asymmetric BVSSs, denoted as ABVSSs, [29, 31, 33]. If the coefficients satisfy $a_{i,j} = a_{j,i}, \forall i, j \in [0, t-1]$, it is a symmetric bivariate polynomial. Shares generated by a bivariate polynomial can be used to establish pairwise keys between any pair of shareholders. In all (t, n) SBVSSs, the dealer selects a bivariate

polynomial, $F(x, y)$ with degree $t-1$ and $F(0,0) = s$ where s is the secret. The dealer generates shares, $F(x_i, y) \bmod p, \quad i = 1, 2, \ldots, n$, for shareholders, where p is a prime with $p > s$ and x_i is the public information associated with each shareholder, U_i. Each share, $F(x_i, y)$ is a univariate polynomial with degree $t-1$. Note that shares generated in an SBVSS satisfy $F(x_i, x_j) = F(x_j, x_i)$, $\forall i, j \in [0, t-1]$ the pairwise key, and $F(x_i, x_j) = F(x_j, x_i)$ can be established between the pair of shareholders, U_i and U_j. In a similar way, in a ABVSS, the dealer generates a pair of shares, $F(x_i, y) \bmod p$ and $F(x, x_i) \bmod p, \quad i = 1, 2, \ldots, n$, for each shareholder and the pairwise secret key, $F(x_i, x_j)$ or $F(x_j, x_i)$, can also be established between the pair of shareholders, U_i and U_j.

3. Model

In this section, we describe the model of the proposed schemes including scheme description, adversaries, and properties.

3.1. Scheme Description. We propose two schemes in this paper.

3.1.1. Scheme for Verification of Shares. A VSS enables shareholders to verify that their shares of a $\forall i, j \in [0, t-1]$ SS are generated by the dealer consistently. In other words, without revealing the secret and the shares, shareholders can verify that any subset of t or more than t shares defines the secret, but any subset of fewer than t shares cannot define the secret. Benaloh [15] presented a notion of t-consistency and uses it to define the objective of a VSS. We include the notion given below.

Definition 1. t-consistency: a set of n shares is said to be t-consistent if any subset of t of the n shares defines the same secret.

Harn and Lin [35] modified the definition of t-consistency and introduce a new notion, called strong t-consistency, which can satisfy the security requirements of a (t, n) SS.

Definition 2. Strong t-consistency: a set of n shares are said to be strong t-consistent (i.e., $(t < n)$) if (a) any subset of t or more than t of the n shares defines the same secret and (b) any subset of fewer than t of the n shares cannot define the same secret.

It is obvious that, in a polynomial-based SS, shares generated by a polynomial having exact t degree are strong t-consistent. Shares have the property of strong t-consistency satisfy the security requirements of a (t, n) SS. Verifying the property of strong t-consistency of shares is one of the objectives of our proposed VSS. In our proposed secure secret reconstruction, shares of shareholders are generated by a symmetric bivariate polynomial. Thus, shares can not only be used to recover the secret but also be used to establish pairwise secret keys between shareholders in the secret reconstruction. The second objective of our proposed VSS is to verify that shares are generated by a symmetric bivariate polynomial.

We assume that there are n shareholders, U_i, for $i = 1, 2, \ldots, m$ participated in the VSS. These shareholders want to make sure that their shares, s_i, for $i = 1, 2, \ldots, m$ obtained from the dealer are strong t-consistent and generated by a symmetric bivariate polynomial. In the proposed VSS, each shareholder computes $c_i = F(s_i)$ as his/her released value, where F is a public function. There is an algorithm, VSS, which allows users to verify that all released values are valid, i.e.,

$$\mathrm{VSS}\left\{\forall c_i = F(s_i) \mid i = 1, 2, \ldots, n\right\} = \begin{cases} 0 \longrightarrow \text{exists invalid shares}_i; \\ 1 \longrightarrow \text{all are valid shares.} \end{cases} \tag{1}$$

The proposed VSS is different from most other VSSs which verify one share at a time, but our VSS verifies all shares at once. There are only two possible outcomes of our proposed VSS, that are, either all shares are strong t-consistent and generated by a symmetric bivariate polynomial or there are inconsistent shares. Thus, the proposed VSS is sufficient if all shares are strong t-consistent and generated by a symmetric bivariate polynomial; however, if there are inconsistent shares, it can be treated as a preprocess before applying other VSS to identify invalid shares.

3.1.2. Scheme for Secure Secret Reconstruction. First, we present the notion of a secure secret reconstruction scheme as defined in [11].

Definition 3. Secure secret reconstruction scheme [11]: This scheme ensures that the secret can only be recovered by participants who present valid shares. In other words, if any outside adversary participated in the secret reconstruction, the adversary cannot obtain the secret.

Shamir's secret reconstruction is a secure secret reconstruction if there are exact t participants since only if t valid shares of participants can recover the secret. When there are more than t participants in the secret reconstruction, it can cause a security. Since only t shares are needed to recover the secret, the adversary can still obtain the secret in the secret reconstruction. Employing a user authentication/VSS scheme in prior of the secret reconstruction can solve the security problem. However, this approach adds additional complexity. A secure secret reconstruction scheme is proposed in [11]. In the scheme, Lagrange components, which are linear combination of shares, are used to reconstruct the secret. The scheme uses the Lagrange component to protect the privacy of shares so the adversary cannot take advantage by releasing value last in the secret reconstruction. This scheme is a simple modification of Shamir's (t, n) SS scheme. However, the scheme can only prevent active attackers to obtain the recovered secret, but cannot prevent passive attackers. Our proposed SSRS can prevent both active and passive attackers.

3.2. Adversaries. The adversaries in the secret reconstruction can be classified into two types, the outside adversaries and the inside adversaries. The outside adversaries are attackers who do not have any valid share generated by the dealer. There are two different types of attacks associated with outside adversaries, the active and passive attacks. The active attackers impersonate to be legitimate shareholders participating in the secret reconstruction. On the other hand, the passive attackers wiretapped the communication channels to obtain exchange information among participants in the secret reconstruction. If exchange information in the secret reconstruction is not protected in [11], the recovered secret can also be available to the attackers. In this paper, we propose a secure secret reconstruction scheme that can prevent both active and passive attackers. In our proposed scheme, shares of shareholders can not only be used to recover the secret but also used to protect the exchange information in the secret reconstruction.

The inside adversaries are shareholders who own valid shares obtained from the dealer. The inside attackers may collude together to recover the secret by themselves. We analyze the security whether $t-1$ inside adversaries can collude together to reveal the secret. Furthermore, we also need to assure that, in the verification of shares, shareholders cannot obtain other shareholders' shares and the secret.

3.3. Properties. We discuss properties of two schemes separately.

3.3.1. Scheme for Verification of Shares. We propose a VSS with the following properties:

Correctness: the outcome of this proposed VSS is positive if all shares are t-threshold consistent; otherwise, there are inconsistent shares.

Efficiency: if the outcome of the proposed scheme is negative, the proposed VSS can be treated as a preprocess of other VSS and used to identify inconsistent shares. Thus, the proposed VSS must be efficient.

Security: the VSS must be able to protect the secrecy of shares and the secret in verification.

3.3.2. Scheme for Secure Secret Reconstruction. We propose a secure secret reconstruction scheme with the following properties:

Correctness: the scheme can satisfy the objective as specified in Definition 2.

Efficiency: shares of shareholders obtained initially from a dealer can not only be used to recover the secret but also be used to establish pairwise shared keys of shareholders to protect the exchange information. There is no additional user authentication or key distribution needed.

Security: the scheme must satisfy following security requirements.

(a) Against active outside attack- the scheme can prevent any outsider to impersonate a shareholder participating in the reconstruction to obtain the secret
(b) Against passive outside attack- the scheme can prevent any outsider to obtain the secret by monitoring the communication channels
(c) Against colluded inside attack- the scheme can prevent up to $t-1$ colluded insiders to recover the secret

4. The Proposed Schemes

In Shamir's (t, n) SS, additional key establishment protocol is needed to protect shares in the secret reconstruction; otherwise, any nonshareholders can also recover the secret. Thus, Shamir's (t, n) SS is not a protected secret sharing scheme. In this section, we proposed a (t, n) SS using a bivariate polynomial. There is one major difference between shares generated by a univariate polynomial and by a bivariate polynomial. The shares generated by a univariate polynomial are integers in $\mathrm{GF}(p)$ but shares generated by a bivariate polynomial are univariate polynomials.

4.1. Algorithms. We illustrate this scheme in Figure 1, and a concrete instantiation for Figure 1 is given in Figure 2.

From secret sharing homomorphism, we know that the additive sum of shares of each shareholder is a share on the additive sum of polynomials, $F_1(x_i, y) + F_2(x_i, y) \bmod p$, with $F_1(0,0) + F_2(0,0) = s$. Thus, in the secret reconstruction scheme, the additive sum of shares of each shareholder is used to reconstruct the secret. The objective of our proposed VSS is to verify that all additive sums of two shares of each shareholder are generated by a polynomial satisfying two conditions: (a) the polynomial has $h-1$ degree and (b) the polynomial is a symmetric polynomial. We illustrate this scheme in Figure 3, and a concrete instantiation for Figure 3 is given in Figure 4.

Assume that u (*i.e.*, $t \le u \le n$) shareholders, $\{U_{v_1}, U_{v_2}, \ldots, U_{v_u}\}$, want to reconstruct the secret. We illustrate this scheme in Figure 5, and a concrete instantiation for Figure 5 is given in Figure 6.

4.2. Property Analysis

4.2.1. Scheme for Verification of Shares

Correctness: from secret sharing homomorphism, we know that additive share $v_i(y)$ of each shareholder is a share on the polynomial, $F_1(x, y) + \alpha F_2(x, y) \bmod p$. Since polynomials $F_1(x, y)$ and $F_2(x, y)$ are both symmetric polynomials having $h-1$ degree each, the additive sum of their polynomials, $G(x, y) = F_1(x, y) + \alpha F_2(x, y) \bmod p$, must also be a symmetric polynomial having $h-1$ degree. On the other hand, if $G(x, y) = F_1(x, y) + \alpha F_2(x, y) \bmod p$ is a symmetric polynomial having $h-1$ degree, then it is most likely that the polynomial $F_1(x, y) + F_2(x, y) \bmod p$ is also a symmetric polynomial having $h-1$ degree. This result achieves our VSS objectives.

Shares generation

The dealer selects two h–1 degrees (i.e., with $h = t$. We will explain this condition later in Theorem 1) symmetric polynomials, $F_1(x, y) = \sum_{i=1}^{h-1}\sum_{j=1}^{h-1} a_{i,j} x^i y^j \bmod p$, and $F_2(x, y) = \sum\sum_{j=1}^{h-1} b_{i,j} x^i y^j \bmod p$, where $F_1(0,0) + F_2(0,0) = s$, $a_{i,j}, b_{i,j} \in GF(p)$, $a_{i,j} = a_{j,i}$ and $b_{i,j} = b_{j,i}$, $\forall i, j \in [0, h-1]$, s is the secret, and p is a prime with $p > s$. The dealer computes shares, $s_{i,1}(y) = F_1(x_i, y) \bmod p$ and $s_{i,2}(y) = F_2(x_i, y) \bmod p$, for shareholders, U_i, $i = 1, 2, \ldots, n$, where x_i is the public information associated with each shareholder, U_i. The dealer sends shares, $s_{i,1}(y)$ and $s_{i,2}(y)$, to shareholder U_i secretly.

Figure 1: Share generation.

Shares generation

Suppose that the dealer selects two 1st-degree (i.e., $h = 2$) symmetric polynomials, $F_1(x, y) = 3 = 2x + 2y + xy \bmod p$ and $F_2(x, y) = 1 = x + y + 2xy \bmod p$, where $F_1(0, 0) + F_1(0, 0) = s = 4$ is the secret and $p = 97$ is a prime. The dealer computes shares, $s_{1,1}(y) = 3y + 5 \bmod p$, $s_{1,2}(y) = 3y + 2 \bmod p$ and $s_{2,1}(y) = 4y + 7 \bmod p$, $s_{2,2}(y) = 5y + 3 \bmod p$, for 2 shareholders U_1 and U_2, respectively, where $x_1 = 1$ and $x_2 = 2$. The dealer sends shares secretly.

Figure 2: Concrete instantiation for Figure 1.

Verification of shares

Step 1. All shareholders agree to a random integer, $\alpha \in GF(p)$.

Step 2. Each shareholder U_i, uses his/her shares, $s_{i,1}(y)$ and $s_{i,2}(y)$, to compute $v_i(y) = s_{i,1}(y) + \alpha\, s_{i,2}(y) \bmod p$, and makes $v_i(y)$ available to other shareholders.

Step 3. After receiving all $v_i(y)$, $i = 1, 2, \ldots, n$, each shareholder computes $\sum_{i=1}^{n} v_i(y) \prod_{i=1, i\neq 1}^{n} (x - x_l/x_i - x_l) \bmod p = G(x, y)$. If $G(x, y)$ is a symmetric polynomial having h–1 degree, all shares used to recover the secret have been verifiable; otherwise, there are inconsistent shares and new share generation is needed.

Figure 3: Verification of shares.

Verification of shares

Step 1. We can assume that all shareholders agree to a random integer, $\alpha = 2$.

Step 2. Each shareholder, U_1 and U_2, respectively, uses his/her shares to compute $v_1(y) = s_{1,1}(y) + 2s_{1,2}(y) = 9y + 9 \bmod p$ and $v_2(y) = s_{2,1}(y) + 2s_{2,2}(y) = 14y + 13 \bmod p$ and makes it available to other shareholders.

Step 3. After receiving all $v_i(y)$, $i = 1, 2$, each shareholder U_1 and U_2, can, respectively, compute $G(x, y) = 5 + 4x + 4y + 5xy \bmod p$. Here, we can see $G(x, y)$ is a symmetric polynomial having 1st degree; hence, all shares used to recover the secret have been verified.

Figure 4: Concrete instantiation for Figure 3.

Efficiency: our VSS is very efficient since it verifies all shares of secret at once using polynomial interpolation.

Security: in step 2, each released value of shareholder is $v_i(y) = s_{i,1}(y) + \alpha\, s_{i,2}(y) \bmod p$. It is impossible to obtain shares $s_{i,1}(y)$ and $s_{i,2}(y) \bmod p$ from the released

Secure secret reconstruction

Step 1. Each shareholder U_{v_i} uses his/her additive sum of shares, $s_{v_i}(y) = s_{v_i,1}(y) + s_{v_i,2}(y)$, to compute pairwise shared keys, $k_{i,j} = s_{v_i}(x_{v_j}) = F(x_{v_i}, x_{v_j})$, $j = 1, 2, ..., u, j \neq i$, where $k_{i,j}$ is the secret key shared between shareholders, U_{v_i} and U_{v_j}.

Step 2. Each shareholder U_{v_i} computes $c_{i,j} = E_{v_{i,j}}(w_{v_i})$, $j = 1, 2, ..., u, j \neq i$, where $w_{v_i} = s_{v_j}(0) \prod_{l=1, l\neq 1}^{u} (-x_{v_l}/x_{v_i} - x_{v_l}) \bmod p$., and then sends $c_{i,j}$, $j = 1, 2, ..., u, j \neq i$, to other shareholders.

Step 3. After receiving cipher text, $c_{i,j}$, $j = 1, 2, ..., u, j \neq i$, from other shareholders, U_{v_i} computes $D_{k_{i,j}}(c_{i,j})$, $j = 1, 2, ..., u, j \neq i$, where $D_{k_{i,j}}(c_{i,j})$ denotes the decryption of $c_{i,j}$ using the key $k_{i,j}$.

Step 4. Each shareholder U_{v_i} computes $D_{k_{i,j}}(c_{i,j}) = w_{v_j}$, $j = 1, 2, ..., u, j \neq i$. Then, the secret is recovered by computing $\sum_{i=1}^{u} w_{v_j} \bmod p = s$.

Figure 5: Secure secret reconstruction.

Secure secret reconstruction

Step 1. Each shareholder, U_1 and U_2, respectively, uses his/her additive sum of shares, $s_1(y) = s_{1,1}(y) + s_{1,2}(y) = 6y + 7 \bmod p$ and $s_2(y) = s_{2,1}(y) + s_{2,2}(y) = 6y + 7 \bmod p$, to compute pairwise shared keys, $k_{1,2} = k_{2,1} = 19$, where $k_{1,2}$ and $k_{2,1}$ is the secret key shared between shareholders, U_1 and U_2.

Step 2. Each shareholder, U_1 and U_2, respectively, computes $c_{1,2}$ and $c_{2,1}$, where $w_1 = 14$ and $w_2 = -10$, and then sends $c_{i,j}$, $j = 1, 2, ..., u, j \neq i$, to other shareholders.

Step 3. After receiving cipher text, $c_{i,j}$, $j = 1, 2, ..., u, j \neq i$, from other shareholders, U_{v_i} computes $D_{k_{i,j}}(c_{i,j})$, $j = 1, 2, ..., u, j \neq$ i, where $D_{k_{i,j}}(c_{i,j})$ denotes the decryption of $c_{i,j}$ using the key $k_{i,j}$.

Step 4. Each shareholder U_{v_i} computes $D_{k_{i,j}}(c_{i,j}) = w_{v_j}$, $j = 1, 2, ..., u, j \neq i$. Then, the secret is recovered by computing $w_1 + w_2 =$ s = 4. Hence, the secret is securely and correctly reconstructed.

Figure 6: Concrete instantiation for Figure 5.

value. Furthermore, in step 3, the recovered polynomial, $G(x, y) = F_1(x, y) + \alpha F_2(x, y) \bmod p$, does not reveal the secrecy of individual polynomials, $F_1(x, y)$ and $F_2(x, y) \bmod p$. Thus, the secret cannot be obtained in this VSS scheme.

4.2.2. Scheme for Secure Secret Reconstruction

Correctness: according to the Lagrange interpolation formula, we can get $\sum_{i=1}^{u} s_{v_i}(y) \prod_{l=1, l\neq i}^{u} (x - x_{v_l}/x_{v_i} - x_{v_l}) \bmod p = F_1(x, y) + F_2(x, y)$. Thus, in step 4 of scheme 3, we get $\sum_{i=1}^{u} w_{v_i} \bmod p = \sum_{i=1}^{u} s_{v_i}(0) \prod_{l=1, l\neq i}^{u} (-x_{v_l}/ x_{v_i} - x_{v_l}) \bmod p = F_1(0, 0) + F_2(0, 0) = s$ This concludes that, for any qualified subset, $A = \{U_{v_1}, U_{v_2}, \ldots, U_{v_u}\} \in \Gamma$ of shareholders can work together to recover the secret. Hence, it holds that $H(s \mid A) = 0$.

Efficiency: in this scheme, each share, $s_{i,j}(y)$, $j \in [1, 2]$, is a univariate polynomial with degree $h - 1$ Thus, each shareholder needs to store $2h$ coefficients of a univariate polynomial. The memory storage of each shareholder is $2h \log_2 p$ bits, where p is the modulus. Horner's rule [24] can be used to evaluate polynomials. In the following discussion, we show the cost for computing $w_{v_i} = s_{v_i}(0) \prod_{l=1, l\neq i}^{u} (-x_{v_l}/x_{v_i} - x_{v_l}) \bmod p$ in the secret reconstruction. From Horner's rule,

evaluating a polynomial of degree $h-1$ needs $h-1$ multiplications and h additions. Since multiplication takes more time than addition, the performance is only addressed to the number of multiplications needed. The computational cost in step 2 of scheme 3 to compute w_{v_i} is to evaluate one polynomial. The computational cost in step 1 of scheme 3 to compute pairwise shared keys, $k_{i,j} = s_{v_i}(x_{v_j}), \quad j = 1, 2, \ldots, u, j \neq i$, is to evaluate $u-1$ polynomials, where u is the number of shareholders participated in the secret reconstruction. Overall, the computational cost to reconstruct the secret of each shareholder is to compute uh multiplications.

Security: in this section, we will first prove that the scheme meets the security requirements as discussed in Section 3.3.

Against both active and passive inside attacks: in the proposed scheme, the information exchanged among shareholders is encrypted using pairwise shared keys. Since a nonshareholder does not own any share generated by the dealer, the nonshareholder cannot decrypt any cipher text. Thus, the recovered secret is not available to the nonshareholder. In other words, the nonshareholder obtains no information on s.

Against colluded inside attack

Theorem 1. *With $h = t$, the proposed scheme satisfies both security requirements of a (t, n) SS. That is, (a) with t or more than t shares can recover the secret and (b) with fewer than t shares cannot recover the secret.*

Proof. Since polynomials $F_1(x, y) = \sum_{i=0}^{h-1}\sum_{j=0}^{h-1} a_{i,j}x^i y^j \bmod p$ and $F_2(x, y) = \sum_{i=0}^{h-1}\sum_{j=0}^{h-1} b_{i,j}x^i y^j \bmod p$ are symmetric polynomials with $a_{i,j} = a_{j,i}$ and $b_{i,j} = b_{j,i}, \forall i, j \in [0, h-1]$ containing $(h(h+1)/2)$ different coefficients in each polynomial, there are $h(h+1)$ different coefficients in total. In the proposed scheme, each share, $s_{i,j}(y), j \in [1, 2]$, is a univariate polynomial with degree $h-1$. In other words, each shareholder can use his shares, $s_{i,1}(y)$ and $s_{i,2}(y)$, to establish $2h$ linearly independent equations in terms of the coefficients of the polynomials.

With $t-1$ colluded shareholders together, it can establish $2h(t-1)$ equations; at the same time, their shares contain $2C_2^{t-1} = (t-1)(t-2)$ points on the bivariate polynomial. Thus, these $t-1$ colluded shares can be used to establish $2h(t-1) - (t-1)(t-2)$ linear independent equations in terms of the coefficients of the bivariate polynomial. If $h(h+1) > 2h(t-1) - (t-1)(t-2)$, these $t-1$ colluded shareholders cannot recover the bivariate polynomials. Since $h = t$, as specified in the share generation, we have $h(h+1) > 2h(t-1) - (t-1)(t-2)$. Hence, any $t-1$ colluded shareholders cannot recover the secret. This conclusion is obtained without making any computational assumption.

On the other hand, when there are t or more than t shareholders trying to recover the secret, with their shares together, they can establish $2ht$ equations; at the same time, their shares contain $2C_2^t = t(t-1)$ points on the bivariate polynomial. Thus, their shares can be used to establish $2ht - 2C_2^t$ linear independent equations in terms of the coefficients of the bivariate polynomials. If $2ht - 2C_2^t \geq h(h+1)$, these t or more than t shareholders can recover the bivariate polynomials. Since $h = t$, as specified in the share generation, we have $2ht - 2C_2^t \geq h(h+1)$. Hence, any t or more than t shareholders can recover the secret. □

Corollary 1. *For any given threshold, t, the degree of the symmetric polynomial, $F(x, y)$, can be t.*

Proof. The proof is straightforward. □

4.3. Comparison. Since the proposed schemes are based on bivariate polynomials with multiple features, our comparison with other schemes is a high-level comparison only. In a whole, compared with previous related schemes, our proposed VSS and SSRS schemes have the following advantages:

(1) The proposed secure secret reconstruction scheme with verifiable shares is unconditionally secure, which is based on symmetric bivariate polynomials.

(2) The proposed VSS is different from most other VSSs which verify one share at a time; but our VSS verifies all shares at once. There are only two possible outcomes of our proposed VSS, that is, either all shares are strong t-consistent and generated by a symmetric bivariate polynomial or there are inconsistent shares. Thus, the proposed VSS is sufficient if all shares are strong t-consistent and generated by a symmetric bivariate polynomial; however, if there are inconsistent shares, it can be treated as a preprocess before applying other VSS to identify invalid shares.

(3) Previous SSRS can only prevent active attackers to obtain the recovered secret, but cannot prevent passive attackers. Our proposed SSRS can prevent both active and passive attackers.

(4) In our proposed SSRS, shares of shareholders are generated by a symmetric bivariate polynomial. The shares generated by a symmetric bivariate polynomial can be used to (a) verify all shares at once, (b) recover the secret, and (c) establish pairwise secret keys between shareholders to protect the exchange information in the secret reconstruction. There is no additional user authentication or key distribution needed. Thus, it is very efficient.

5. Conclusions

A novel design for an efficient SSRS with verifiable shares is introduced in the paper. This SSRS uses bivariate polynomials to generate shares, where shares of shareholders can be used to (a) verify all shares at once, (b) recover the secret, and (c) establish pairwise secret keys between shareholders to protect the exchange information in the secret reconstruction. Moreover, we propose an efficient verification scheme which allows all shares to be verified at once. Security and performance analysis are also included. The

proposed scheme is more attractive to be applied in most communications systems.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Grant nos. 61772224 and 61872152), the Fundamental Research Funds for the Central Universities (no. CCNU19TS019), and the Research Planning Project of National Language Committee (no. YB135-40).

References

[1] L. Harn, C. Hsu, M. Zhang, T. He, and M. Zhang, "Realizing secret sharing with general access structure," *Information Sciences*, vol. 367-368, pp. 209–220, 2016.

[2] C.-F. Hsu, L. Harn, Y. Mu, M. Zhang, and X. Zhu, "Computation-efficient key establishment in wireless group communications," *Wireless Networks*, vol. 23, no. 1, pp. 289–297, 2017.

[3] L. Harn and C. F. Hsu, "A practical hybrid group key establishment for secure group communications," *The Computer Journal*, vol. 60, no. 11, pp. 1582–1589, 2017.

[4] L. Harn and C. F. Hsu, "(t, n) multi-secret sharing scheme based on bivariate polynomial," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1495–1504, 2017.

[5] L. Harn, C.-F. Hsu, and B. Li, "Centralized group key establishment protocol without a mutually trusted third party," *Mobile Networks and Applications*, vol. 23, no. 5, pp. 1132–1140, 2018.

[6] C. F. Hsu, L. Harn, and B. Zeng, "UMKESS: user-oriented multi-group key establishments using secret sharing," *Wireless Networks*, vol. 26, no. 3, pp. 1–10, 2018.

[7] L. Harn, C. F. Hsu, Z. Xia, and J. Zhou, "How to share secret efficiently over networks," *Security and Communication Networks*, vol. 2017, Article ID 5437403, , 2017.

[8] M. Fuyou, X. Yan, W. Xingfu et al., "Randomized component and its application to (t, m, n)-group oriented secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 889–899, 2014.

[9] G. R. Blakley, "Safeguarding cryptographic keys,"vol. 48, pp. 313–317, in *Proceedings of the AFIPS'79 National Computer Conference*, vol. 48, pp. 313–317, AFIPS Press, New York, NY, USA, June 1979.

[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[11] L. Harn, "Secure secret reconstruction and multi-secret sharing schemes with unconditional security," *Security and Communication Networks*, vol. 7, no. 3, pp. 567–573, 2014.

[12] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science*, pp. 383–395, IEEE Press, Portland, OR, USA, October 1985.

[13] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pp. 427–437, Los Angeles, CA, USA, October 1987.

[14] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology-Crypto'91, Lecture Notes in Computer Science*, vol. 576, pp. 129–140, Springer-Verlag, Berlin, Germany, 1992.

[15] J. C. Benaloh, "Secret sharing homomorphisms: keeping shares of a secret secret," in *Advances in Cryptology-CRYPTO'86, Lecture Notes in Computer Science*, vol. 263, pp. 251–260, Springer-Verlag, Berlin, Germany, 1987.

[16] D. R. Stinson and R. Wei, "Unconditionally secure proactive SS with combinatorial structures,"vol. 1758, pp. 200–214, in *Proceedings of the SAC99; Selected Areas in Cryptography, 6th Annual International Workshop*, vol. 1758, , Springer-Verlag, Kingston, Canada, August 1999.

[17] A. Patra, A. Choudhary, and C. P. Rangan, "Efficient statistical asynchronous verifiable secret sharing with optimal resilience,"vol. 5973, pp. 74–92, in *Proceedings of the ICITS'09 Information Theoretic Security*, vol. 5973, pp. 74–92, Springer-Verlag, Shizuoka, Japan, December 2010.

[18] M. Stadler, "Publicly verifiable secret sharing," in *Advances in Cryptology-Eurocrypt'96*, vol. 1070, pp. 190–199, Springer-Verlag, Berlin, Germany, 1996.

[19] E. Fujisaki and T. Okamoto, "A practical and provably secure scheme for publicly verifiable secret sharing and its applications," in *Advances in Cryptology-Eurocrypt'98, Lecture Notes in Computer Science*, vol. 1403, pp. 32–46, Springer-Verlag, Berlin, Germany, 1998.

[20] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Advances in Cryptology-CRYPTO 1986, Lecture Notes in Computer Science*, vol. 263, pp. 186–194, Springer-Verlag, Berlin, Germany, 1987.

[21] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic," in *Advances in Cryptology-Crypto'99, Lecture Notes in Computer Science*, vol. 1666, pp. 148–164, Springer-Verlag, Berlin, Germany, 1999.

[22] A. Peng and L. Wang, "One publicly verifiable secret sharing scheme based on linear cod," in *Proceeding of the 2nd Conference on Environmental Science and Information Application Technology*, pp. 260–262, Wuhan, China, July 2010.

[23] A. Ruiz and J. L. Villar, "Publicly verifiable secret sharing from Paillier's cryptosystem," in *Proceedings of the WEWoRC'05: Western European Workshop on Research in Cryptology*, pp. 98–108, Leuven, Belgium, July 2005.

[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science*, vol. 1592, pp. 223–238, Springer-Verlag, Berlin, Germany, 1999.

[25] Y. Tian, C. Peng, and J. Ma, "Publicly verifiable secret sharing schemes using bilinear pairings," *International Journal of Network Security*, vol. 14, no. 3, pp. 142–148, 2012.

[26] T.-Y. Wu and Y.-M. Tseng, "A pairing-based publicly verifiable secret sharing scheme," *Journal of Systems Science and Complexity*, vol. 24, no. 1, pp. 186–194, 2011.

[27] L. Harn and C.-F. Hsu, "Dynamic threshold secret reconstruction and its application to the threshold cryptography," *Information Processing Letters*, vol. 115, no. 11, pp. 851–857, 2015.

[28] K. Meng, F. Miao, W. Huang, and Y. Xiong, "Threshold changeable secret sharing with secure secret reconstruction," *Information Processing Letters*, vol. 157, Article ID 105928, 2020.

[29] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, "Efficient multiparty computations secure against an adaptive adversary," in *LNCS, Advances in Cryptology-EUROCRYPT'99*, vol. 1592, pp. 311–326, Springer, Berlin, Germany, 1999.

[30] M. Fitzi, J. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan, S. Halevi, "Round-optimal and efficient verifiable secret sharing," in *Proceedings of the Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006*, T. Rabin, Ed., vol. 3876, pp. 329–342, Springer, New York, NY, USA, March, 2006.

[31] R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin, "The round complexity of verifiable secret sharing and secure multicast," in *Proceedings of the STOC 33rd Annual ACM Symposium on Theory of Computing*, pp. 580–589, Hersonissos, Greece, July 2001.

[32] J. Katz, C. Koo, and R. Kumaresan, "Improved the round complexity of VSS in point-to-point networks,"vol. 5126, pp. 499–510, in *Proceedings of ICALP'08 International Colloquium on Automata, Languages, and Programming*, vol. 5126, pp. 499–510, Springer, Reykjavik, Iceland, July 2008.

[33] R. Kumaresan, A. Patra, and C. P. Rangan, "The round complexity of verifiable secret sharing: the statistical case," in *Advances in Cryptology-ASIACRYPT 2010*, vol. 6477, pp. 431–447, Springer, Berlin, Germany, 2010.

[34] V. Nikov and S. Nikova, "On proactive secret sharing schemes," in *Selected Areas in Cryptography LNCS*, vol. 3357, pp. 308–325, Springer, Berlin, Germany, 2005.

[35] L. Harn and C. Lin, "Strong (*n*, *t*, *n*) verifiable secret sharing scheme," *Information Sciences*, vol. 180, no. 16, pp. 3059–3064, 2010.