Computers, Materials & Continua
DOI: 10.32604/cmc.2022.027496
Article

Tech Science Press

Protected Fair Secret Sharing Based Bivariate Asymmetric Polynomials in Satellite Network

Yanyan Han[1,2], Jiangping Yu[3], Guangyu Hu[4], Chenglei Pan[4], Dingbang Xie[5], Chao Guo[1,2,6,*] and Abdul Waheed[7]

[1]Department of Electronics and Communication Engineering, Beijing Electronics Science and Technology Institute, Beijing, 100070, China
[2]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710126, China
[3]Department of Cryptography and Technology, Beijing Electronics Science and Technology Institute, Beijing, 100070, China
[4]Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
[5]School of Communication Engineering, Xidian University, Xi'an, 710126, China
[6]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China
[7]University of Management Technology, Lahore-Pakistan, 55300, Pakistan
*Corresponding Author: Chao Guo. Email: guo99chao@163.com
Received: 19 January 2022; Accepted: 08 March 2022

Abstract: Verifiable secret sharing mainly solves the cheating behavior between malicious participants and the ground control center in the satellite network. The verification stage can verify the effectiveness of secret shares issued by the ground control center to each participant and verify the effectiveness of secret shares shown by participants. We use a lot of difficult assumptions based on mathematical problems in the verification stage, such as solving the difficult problem of the discrete logarithm, large integer prime factorization, and so on. Compared with other verifiable secret sharing schemes designed for difficult problems under the same security, the verifiable secret sharing scheme based on the Elliptic Curve Cryptography (ECC) system has the advantages of less computational overhead and shorter key. At present, the binary polynomial is a single secret scheme and cannot provide effective verification. Therefore, based on a Protected Verifiable Synchronous Multi Secret Sharing (PVS-MSS) scheme, this paper is designed based on bivariate asymmetric polynomials. The advanced verifiable attribute is introduced into the Protected Secret Sharing (PSS) scheme. This paper extends the protected synchronous multi-secret sharing scheme based on bivariate polynomial design. The ECC system constructs the security channel between the ground control center and participants and constructs the verification algorithm. Through the verification algorithm, any participant can verify the consistency and effectiveness of the secret shadow and secret share received from other participants or presented by the secret distribution center. Therefore, no additional key agreement protocol is required; participants do not need to negotiate the session key for encryption; the secret share polynomial can generate the session key between participants and speed up the secret reconstruction process. The verification stage has lower computational complexity than the verifiable scheme constructed by Rivest Shamir Adleman

(RSA) and other encryption methods. Chinese Remainder Theorem (CRT) is used to update the secret shadow. The secret shadow does not need to be updated with the change of the scheme shared secret, and the public value update efficiency is higher. Reduce the complexity of sharing secret updates in a synchronous multi-secret sharing scheme.

Keywords: Multi-secret sharing; binary asymmetric; verifiable synchronization; protected; satellite network

1 Introduction

A Satellite network is a comprehensive information system composed of different types of satellites in different orbits, ground control centers, and user terminals. It has the characteristics of wide coverage and flexible networking and is widely used in military, resource survey, meteorology, and other fields. However, Li et al. proposed a resource allocation scheme [1]. Md introduces a method to save satellite space [2]. However, due to the available deployment of satellites, limited onboard resources, transmission data is easy to be intercepted, and other security threats, the secret protection in the process of satellite transmission has also become particularly important.

In 1979, Shamir and Blakley proposed (t, n) threshold secret sharing theory [3,4]. Which will be a secret D into n shares, as long as there is greater than or equal to t participants can reconstruct secrets D, and less than t participants cannot reconstruct secret D. However, the threshold theory can reconstruct secret D through Lagrange interpolation, but it can not ensure its effectiveness for malicious participants and ground control center fraud. There is no guarantee of its effectiveness. Ghodosi analyzed the schemes of Harn et al., which can not detect cheaters in a wide range in the threshold theory [5,6]. Liu et al. proposed a quadratic polynomial algorithm to identify deception [7]. Lin et al. solved the problem that secret reconstruction is not deceived by releasing secret shadows simultaneously [8]. Han pointed out that Theorem 3 related to asynchronous network attack in secret sharing scheme in Tian et al. is incorrect [9,10]. To solve the problem of dishonest participants releasing false secret shares during secret reconstruction, Harn et al. proposed a synchronous rational secret sharing scheme [11]. Harn proposed a new verifiable multi-secret sharing scheme, while Gu made Harn's scheme more flexible [12,13]. Lin proposes a verifiable identity method [14]. Jin et al. proposed a secret sharing scheme based on images, but it costs a lot [15]. Javeed et al. proposed a method to implement ECC [16]. Xue et al. proposed a group key protocol. They shared group key switching authentication between satellites based on secret sharing technology, but they can not verify the secret share and have a high overhead [17].

Many secret sharing technologies exist in satellite network secret sharing schemes, such as literature [18]. We need to ensure the security of multiple nodes in the communication requirements of satellite networks. And the secret-sharing verification shall be distributed in the ground control center and each node satellite. We propose a verifiable secret sharing scheme based on binary asymmetric polynomials. At present, verifiable secret sharing schemes based on bivariate polynomial design are all single secret sharing schemes [19]; Secondly, the primary purpose of the design is to construct an efficient verifiable secret sharing protocol in the presence of different numbers of cheaters. Research status of secret sharing scheme based on bivariate polynomial design: PSS scheme lacks various additional attributes to resist separate spoofing attacks and is suitable for different scenarios [20];

Reference [21,22], a simple multi-secret sharing scheme, can't resist the invasion of semi-honest people; The Verifiable Multi-Secret Sharing (VMSS) in reference [23] has no protected characteristics. The primary purpose of this scheme research is the verifiable attribute introduced into a secret sharing scheme with protected features like the PSS scheme. Secondly, it extends the similar design of [24] synchronous multi-secret sharing scheme to make it more widely used. The scheme has the following advantages:

- There is no need for a secure channel between that secret distribution center and the participant.
- No additional key agreement protocol is needed: Participants do not need to negotiate extra session keys for encryption. The secret share polynomial can generate session keys among participants, thus accelerating the process of secret reconstruction.
- Protected: The pairwise session key generated by a share polynomial can protect the information exchange between participants in the process of secret reconstruction and resist external attacks.
- ECC realizes verifiable attributes. The verification phase has lower computational complexity than verifiable schemes constructed by RSA and other encryption methods.
- Synchronous multi-secret sharing: the number of optional shared secrets in the secret distribution center is flexible. A single secret reconstruction process can reconstruct multiple shared secret values according to different situations.

Although literature [25] proposed placing some calculations below the ground or LEO, it does not introduce security issues. Therefore, to ensure security under the same premise, we achieve less computing cost, shorter key, and save system resources according to the characteristics of limited satellite resources and limited bandwidth. The ECC system constructs the safety channel between the ground control center and the node satellite. Using CRT to update the secret shadow, the ground control center only needs to publish part of the public value, which makes the public value update more efficient.

2 Preliminary Knowledge

2.1 Shamir Threshold Theory

2.1.1 Key Construction

Let P be a prime number and k be the key $k \in GF(P)$, and the key distribution center D randomly selects an $t-1$ order polynomial $b(x)$ on $GF(P)$, and $k = b(0)$. The key distribution center calculates $k_i = b(i)$, $i = 1, 2, 3, \ldots, n$, k_i distributed to participants as secret shares P_i.

2.1.2 Key Reconstruction

When there are t participants $P_1, P_2, P_3, \ldots, P_t$. We can reconstruct secret k by Lagrange interpolation, and the formula is:

$$k = \sum_{i=1}^{t} k_i \sum_{i=1, j \neq i}^{t} \frac{-j}{i-j} \tag{1}$$

2.2 CRT

Any two prime $n_1, n_2, \ldots, n_s$, any $a_1, a_2, \ldots, a_s$ to make $\exists a \in Z$ content with

$$\begin{cases} \mathrm{a} = a_1 \bmod n_1 \\ \mathrm{a} = a_2 \bmod n_2 \\ \vdots \\ \mathrm{a} = a_s \bmod n_s \end{cases} \tag{2}$$

Set up $M_i = M/n_i, t_i = M_i^{-1} \bmod n_i$, then

$$a = \sum_{i=1}^{s} t_i M_i a_i \tag{3}$$

3 The Project Design

3.1 System Model

Fig. 1 describes the process of participants receiving secrets. Participants' environment is changeable, such as the ocean, wild, etc. Of course, there are various participants, such as individual participants on the ground, ground satellite stations, or satellites in orbit in the air. First, the ground control center distributes secret shares and sends broadcast parameters to Geostationary Earth Orbiting (GEO). Then, GEO sends it to each participant or Low Earth Orbiting (LEO) through the link to get the corresponding secret share. At this time, each participant will generate a unique session key and communicate with each other. The secret can be reconstructed under two different thresholds when ensuring that the participants are honest.

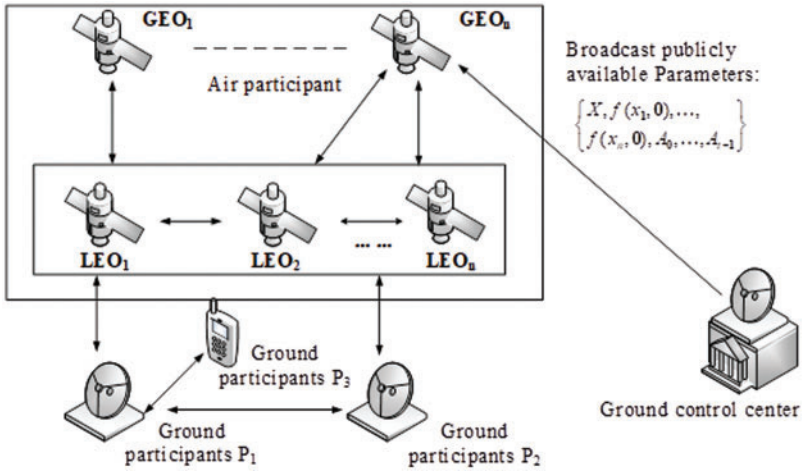

Figure 1: Satellite network secret sharing scheme model

3.2 System Initialization

Suppose there is a trusted ground control center D, a set of actors $\{P_1, P_2, \ldots, P_n\}$. E is an elliptic curve defined on a finite field F_q. Where q is a large prime number that is not equal to 2 or 3. $T \in E(F_q)$ is the base point of an elliptic curve E with upper order ℓ. Public information is $\{F_q, E, T\}$. D select prime $p_0 < \ell$, n different positive integers $p_1, p_2, \ldots, p_n$ meet the following properties:

- $p_0 < p_1, i = 1, 2, \ldots, n.$

■ $p_1, p_2, \ldots, p_n$ mutual prime. And greater than 1.

Perform the following steps between D and $P_i (i \in [1, n])$ to transmit the master secret shadow $p_1, p_2, \ldots, p_n$ to the participants (for the multi-purpose secret sharing scheme, this stage only needs to be performed once.):

- Step 1:D selects integer d as its private key, satisfies $1 < |d| < \ell$, calculates, and discloses $G = dT$ as its public key.
- Step 2: Each participant $P_i, 1 \leq i \leq n$ randomly selects an integer n_i as its private key, satisfies $1 < |n_i| < \ell$, calculates $T_i = n_i T$ as its public key, and makes it public. ID_i is the identity of participant $P_i, 1 \leq i \leq n$. To ensure the inconsistency between different participants T_i and ID_i, D will request to update T_i and ID_i until when $i \neq j, ID_i \neq ID_j$ and $T_i \neq T_j$ take (T_i, ID_i) public information for P_i.
- Step 3: Both D and P_i can use their private keys and public information to calculate public keys $G_i = dn_i T = (x_i, y_i)$.
- Step 4:D calculates and broadcasts $c_i = p_i x_i, i \in [1, n], G_i = dn_i T = (x_i, y_i)$.
- Step 5: When any participant P_i receives c_i, it can use its private key n_i to get $G_i = dn_i T = (x_i, y_i)$ and then calculate $p_i = c_i x_i^{-1} i \in [1, n]$.

Finally, the ground control center D and participant P_i got the primary secret shadow p_i.

3.3 The Secret to Distribute

Suppose D wants to share k secrets $s_0, s_1, \ldots, s_{k-1}$ and perform secret distribution in the following two cases.

Case 1: When the number of secrets to be shared, k is less than or equal to the threshold value t.

Step 1: D constructs the following binary asymmetric polynomials with the order x as $t-1$ and order y as $h-1, h > t(t-1)$:

$$\begin{aligned} f(x,y) &= s_0 + s_1 x + \cdots + s_{k-1} x^{k-1} + a_{0,0} x^k + \cdots + a_{t-k-1,0} x^{t-1} + a_{0,1} y + a_{1,1} xy + \cdots + \\ &\quad a_{t-1,1} x^{t-1} y + \cdots + a_{0,h-1} y^{h-1} + a_{1,h-1} xy^{h-1} + \cdots + a_{t-1,h-1} x^{t-1} y^{h-1} \bmod \ell \\ &= (s_0 + s_1 x + \cdots + s_k x^{k-1} + a_{0,0} + \cdots + a_{t-k-1}) y^0 + (a_{0,1} + a_{1,1} x + \cdots + a_{t-1,1} x^{t-1}) y^1 + \cdots + \\ &\quad (a_{0,h-1} + a_{1,h-1} x + \cdots + a_{t-1,h-1} x^{t-1}) y^{h-1} \bmod \ell \end{aligned} \tag{4}$$

There are k coefficients about the x term in $f(x, y)$ and $\{s_0, s_1, \cdots, s_{k-1}\}$ is a shared secret set among them.

Step 2: D select n random integers $p_0 \leq y_i < p_i, i \in [1, n]$, so that x_i generated by $x_i = y_i \bmod p_i$ is n unequal integers.

Step 3: D calculate the secret share $f(x_i, 0) \bmod \ell, i \in [1, n]$, $A_0 = s_0 T, A_1 = s_1 T, \ldots, A_{k-1} = s_{k-1} T$ and $A_k = a_{0,0} T, A_{k+1} = a_{1,0} T, \ldots, A_{t-1} = a_{t-k-1,0} T$.

Step 4: D calculates the unique integer $X \bmod \prod_{i=1}^{n} p_i$, calculates any $X \equiv y_i \bmod p_i$ using CRT and value set $\{y_1, y_2, \ldots, y_n\}$ and value set $\{p_1, p_2, \ldots, p_n\}$.

Step 5: D calculates the secret polynomials $g^1_{ID_i}(x) = f(x, ID_i) \bmod \ell$, $g^2_{ID_i}(y) = f(ID_i, y) \bmod \ell$ encrypts them with the participant's public key and elliptic curve cryptography, and sends them to the participant $\{P_1, \ldots, P_n\}$.

Step 6: Open $\{X, f(x_1, 0), f(x_2, 0), \ldots, f(x_n, 0), A_0, A_1, \ldots, A_{t-1}\}$.

Case 2: The number of secrets to be shared k is greater than the threshold value t.

Step 1: D constructs the following binary asymmetric polynomials with the order x as $t-1$ and order y as $h-1$:

$$\begin{aligned} f(x,y) &= s_0 + s_1 x + \cdots + s_{k-1}x^{k-1} + a_{0,1}y + a_{1,1}xy + \cdots + a_{k-1,1}x^{k-1}y + \cdots + \\ &\quad a_{0,h-1}y^{h-1} + a_{1,h-1}xy^{h-1} + \cdots + a_{k-1,h-1}x^{k-1}y^{h-1} \bmod \ell \\ &= (s_1 + s_2 x + \cdots + s_k x^{k-1})y^0 + (a_{0,1} + a_{1,1}x + \cdots + a_{k-1,1}x^{k-1})y^1 + \cdots + \\ &\quad (a_{0,h-1} + a_{1,h-1}x + \cdots + a_{k-1,h-1}x^{k-1})y^{h-1} \bmod \ell \end{aligned} \tag{5}$$

There are k coefficients about the x term in $f(x, y)$, and $\{s_0, s_1, \cdots, s_{k-1}\}$ is a shared secret set among them.

Step 2: D select n random integers $p_0 \le y_i < p_i, i \in [1, n]$, so that x_i generated by $x_i = y_i \bmod p_i$ is n unequal integers.

Step 3: D calculate the secret share $f(x_i, 0) \bmod \ell, i \in [1, n]$, $A_0 = s_0 T, A_1 = s_1 T, \ldots, A_{k-1} = s_{k-1} T$.

Step 4: D calculates the unique integer $X \bmod \prod_{i=1}^{n} p_i$, and calculates any $X \equiv y_i \bmod p_i$ using CRT and value set $\{y_1, y_2, \ldots, y_n\}$ and value set $\{p_1, p_2, \ldots, p_n\}$.

Step 5: D calculates the secret polynomials $g^1_{ID_i}(x) = f(x, ID_i) \bmod \ell$, $g^2_{ID_i}(y) = f(ID_i, y) \bmod \ell$, encrypts them with the participant's public key and elliptic curve cryptography, and sends them to the participant $\{P_1, \ldots, P_n\}$.

Step 6: D calculates $h_1 = f(1, 0), h_2 = f(2, 0), \ldots, h_{k-t} = f(k-t, 0)$ and discloses it in [26,27].

Step 7: Open $\{X, f(x_1, 0), f(x_2, 0), \ldots, f(x_n, 0), A_0, A_1, \ldots, A_{k-1}\}$.

3.4 Secret Verification

Because the PVS-MSS scheme has protected properties, resistance to reconstruct phase external attacks, but internal attackers, will reduce the schema's safety. Because internal attackers can be arbitrary tamper with the secret shadow, whether conspired with the collusion attack, internal attackers benefit maximization (the remaining honest refactoring can't get the Shared secret). Therefore, the scheme of PVS-MSS has two different secret numbers. Taking $k \le t$ as an example, we use elliptic curve addition structure to realize the following verification algorithm:

- Step 1: Any refactor P_i can verify whether the secret share $f(x_i, 0) \bmod \ell$ disclosed by the ground control center D is correct by the following verification equation.

$$f(x_i, 0)T = \sum_{j}^{t-1} x_i^j A_j, i = 1, 2, \ldots, n \tag{6}$$

- Step 2: The PVS-MSS scheme does not lose generality. Any reconstructor P_i can verify the secret shadow x_j sent by other participants through the following verification equation.

$$f(x_j, 0)T = \sum_{i=0}^{t-1} x_j^i A_i, j = 1, 2, \ldots, t, i \ne j \tag{7}$$

3.5 Secret Refactoring

In the secret reconstruction stage, if the set of reconstructors participating in the protocol is $\{P_1, P_2, \ldots, P_m\}$.

Step 1: Any two reconstructors P_i and P_j can obtain the shared session key by combining the identity information ID_i and ID_j calculating their secret share polynomial:

$$k_{i,j} = g^1_{ID_i}(ID_j) = g^2_{ID_j}(ID_i) = f(ID_i, ID_j) \mod \ell \tag{8}$$

Step 2: Any reconstructor P_i uses $k_{i,j}$ to calculate $c_{i,j} = Enc_{k_{i,j}}(x_i)$. $c_{i,j} = Enc_{k_{i,j}}(x_i)$ will send P_j through the authenticated broadcast channel ϑ. $Enc_{k_{i,j}}(x_i)$ represents symmetric encryption. Similarly, any reconstructor P_j calculates $c_{j,i} = Enc_{k_{i,j}}(x_i)$ using the key $k_{i,j}$ and sends it to P_i through the authenticated broadcast channel ϑ.

Step 3: When the reconstructor P_i receives ciphertext $c_{j,i}, j \in \{1, 2, \ldots, u\}\backslash\{i\}$, P_i can decrypt ciphertext $Dec_{k_{i,j}}(c_{k_{i,j}}) = x_j$ separately, $Dec_{k_{i,j}}(c_{j,i})$ represents the ciphertext $c_{j,i}$ decrypted with $k_{j,i}$.

Step 4: Each refactorer is divided into the following two cases to reconstruct the shared secret value:

■ Case 1: When the number of shared secrets k is less than or equal to the threshold value t:

$$\begin{aligned} f(x,0) &= s_0 + s_1 x + \cdots + s_{k-1}x^{k-1} + a_{1,0}x^k + \cdots + a_{t-k-1,0}x^{t-1} \bmod \ell \\ &= \sum_{i=1}^{t} f(x_i, 0) \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} \bmod \ell \end{aligned} \tag{9}$$

■ Case 2: When the number of shared secrets k is greater than the threshold value t:

$$\begin{aligned} f(x,0) &= s_0 + s_1 x + \cdots + s_{k-1}x^{k-1} \bmod \ell \\ &= \sum_{i=1}^{t} f(x_i, 0) \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} + \sum_{i=1}^{k-t} f(i, 0) \prod_{j=1, j\neq i}^{k-t} \frac{x - j}{i - j} \bmod \ell \end{aligned} \tag{10}$$

The coefficient set $\{s_0, s_1, \ldots, s_{k-1}\}$ in $f(x, 0)$ is the reconstructed secrets.

3.6 The Secret to Update

When the PVS-MSS scheme shares a secret update, the polynomial constructed by the synchronous multi-secret sharing scheme also needs to be updated, and the public value of the scheme also needs to be updated. YCH and other schemes adopt a bivariate univariate function to ensure that the ground control center D does not need to re-issue secret shadow to each participant for the next new secret sharing [28]. The master secret shadow of the scheme is also multi-purpose without initialization. Only the ground control center D needs to update some public values. In particular, the new X is very high. According to the CRT theorem in Section 2.2 of this paper, $X = \sum_{i=1}^{n} y_i M_i M'_i \bmod \left(\prod_{i=1}^{n} p_i\right)$, $M_i = \prod_{j=1, j\neq i}^{n} p_j$ requirement $M_i M'_i \equiv 1 \bmod p_i$ once the value $M_i M'_i, i = 1, 2, \ldots, n$ is calculated by D, can be saved and reused. Each secret update stage, D only needs to select a new y_i and use $M_i M'_i$ to calculate a new X disclosure.

4 Project Analysis

4.1 Correctness Analysis

Theorem 4.1: The PVS-MSS scheme has any reconfigurable secret greater than or equal to t reconfigurator.

Prove: Suppose $t \leq m \leq n$ reconstructor sets $\{P_1, P_2, \ldots, P_m\}$ to want reconstruct the shared secret, in which any refactorers P_i and P_j content $\forall i, j \in [1, m]$ and $i \neq j$. When the number of shared secrets k is less than or equal to the threshold value t, the order $f(x, 0)$ is known to be $t - 1$, and any reconstructor P_i uses $k_{i,j}$ encryption to calculate $c_{i,j} = Enc_{k_{i,j}}(x_i)$ and sends it to P_j through the

authenticated broadcast channel ϑ. Similarly, any reconstructor P_j calculates $c_{j,i} = Enc_{k_{i,j}}(x_i)$ using the key $k_{i,j}$ and sends it to P_i through the authenticated broadcast channel ϑ. When the reconstructor P_i receives the ciphertext $c_{j,i}, j \in \{1, 2, \ldots, u\}\backslash\{i\}$. P_i can decrypt the ciphertext $Dec_{k_{i,j}}(c_{j,i}) = x_j$. Separately because the polynomial $f(x, 0)$ containing the secret value is a univariate polynomial, P_i gets $x_j, j = 1, 2, \ldots, m, j \neq i, f(x_1, 0), f(x_2, 0), \ldots, f(x_m, 0)$ disclosed by ground control center is exactly m pairs of interpolation points on $f(x, 0)$. Using Lagrange interpolation polynomial, the unique $f(x, 0)$ can be obtained from Eq. (9). Similarly, when the number of shared secrets k is greater than the threshold value t, it is known that order $f(x, 0)$ is $k - 1$, after any refactorer P_i obtains $m - 1$ x_j through the secret refactoring phase. Combined with the public value of the ground control center, it is exactly the $m + k - t$ pairs of interpolation points on $f(x, 0)$. Using Lagrange interpolation formula and secret sharing homomorphism, get a unique $f(x, 0)$ from Eq. (10). The coefficient set $\{s_0, s_1, \ldots, s_{k-1}\}$ in $f(x, 0)$ is the reconstructed secrets.

4.2 Safety Analysis

Theorem 4.2: When $k \leq t$ or $k > t$, When the scheme satisfies the condition $th > (t-1)(t+h)$ or $kh > (t-1)(t+h)+(k-t)$, any access set composed of less than t refactorers cannot be reconstructed. And no one can get any secret information.

Prove: The secret share $f(ID_i, 0) \bmod p$ is generated by the secret polynomial. The secret share is used as the interaction value during reconstruction. The secret shadow is the public value ID_i; the secret share of the PVS-MSS scheme is the public value $f(x_i, 0) \bmod \ell$, and the secret shadow x_i is the interaction value during reconstruction. Under the two schemes, the information obtained by the internal conspirators is of the same nature and the same attack methods, and both are to reconstruct $f(x, 0)$. Therefore, the proof process of this theorem is the same as that of Theorem 4.1 in Section 4.1 of this paper, so it will not repeat here.

Theorem 4.3: The main secret shadow $p_1, p_2, \ldots, p_n$ in the scheme cannot calculate from the public parameter G, T_i, c_i.

Prove: Suppose an attacker $\mathcal{A}$ wants to calculate the main secret shadow $p_1, p_2, \ldots, p_n$ from the public parameter $G = dT, T_i = n_i T, c_i = p_i x_{dn_i T}$. Unless $\mathcal{A}$ can calculate $dn_i T = (x_{dn_i T}, y_{dn_i T})$ from $T_i = n_i T, G = dT$, which is equivalent to solving the computational Diffie-Hellman problem on elliptic curves or directly solving $T_i = n_i T, G = dT$ is equivalent to solving the discrete logarithm problem of an elliptic curve (ECDLP). We can't solve these problems under the current computing power.. Therefore, only after the participant P_i uses its private key n_i to calculate $n_i G = n_i dT$, can it obtain the corresponding master secret shadow p_i.

Theorem 4.4: It is computationally difficult to calculate the secret $s_0, s_1, \ldots, s_{k-1}$ from the public value $A_0, A_1, \ldots, A_{k-1}$.

Prove: $A_i = s_i T, A_i \in < T >$ is the public value used in the verification phase. If the attacker $\mathcal{A}$ wants to obtain s_i directly from the public value $A_i = s_i T$. In that case it is equivalent to solving the discrete logarithm problem on an elliptic curve (ECDLP). So it isn't easy to calculate secrets $s_0, s_1, \ldots, s_{k-1}$.

Theorem 4.5: The scheme resists internal and external attacks in the reconstruction process.

Prove: Suppose there is an internal attacker $\mathcal{A}$, who has identity information ID_i and secret shadow x_i. His attack method is to provide a false secret shadow x_i' to the honest reconstructor in the process of secret reconstruction. The values $f(x_i, 0), i = 1, 2, \ldots, n$ and $A_k, k = 1, 2, \ldots, t-1$ used for verification in the verification phase of the scheme are both public. At this time, any reconstructor P_i calculates

$R = \sum_{k=0}^{t-1} x_i'^k A_k$ and checks whether the equation $R = f(x_i, 0)T$ is true. If inequality $R \neq f(x_i, 0)T$ holds, then $\mathcal{A}$ is identifie as an internal attacker.

In the reconstruction process, The encryption of the session key $k_{i,j}$ protects the interaction between any two reconstructors P_i and P_j. The secret polynomial generates the session key. Therefore, the external enemy without any secret share polynomial information cannot participate in the reconstruction process to steal the secret.

5 Scheme Comparison and Performance Analysis

The PVS-MSS scheme's main parameters, characteristics, and cost are compared with existing schemes. Compared with synchronous multi-secret sharing schemes such as [21,28–31], the PVS-MSS scheme introduces verifiability. There is no need to maintain an additional secure channel between the ground control center and participants. Compared with the verifiable multi-secret sharing schemes in [23,32–35], PVS-MSS scheme participants do not need additional key negotiation mechanisms, which reduces the actual operating cost of the scheme. In the PVS-MSS scheme, the security of the safety channel between the ground control center and participants is based on the Discrete Logarithm Problem of Elliptic Curve (ECDLP). In [32], security is based on the Discrete Logarithm Problem (DLP). Under the same security level, the required parameter bit length is smaller. The amount of calculation is smaller. For example, under the security of 256 bits of the symmetric key, the minimum bit length of the parameter ℓ of the PVS-MSS scheme is 512, while under the same security level, the bit length of Rivest Shamir Adleman/Digital Signature Algorithm (RSA/DSA) module is at least 15360. When the key length is the same, there is little difference between ECC and RSA. Therefore, the PVS-MSS scheme requires fewer resources and faster calculation speed based on the ECC initialization and verification stage. Compared with [23], when $k > t$, if k is close to t, the updated public value of PVS-MSS scheme is less. As shown in Tab. 1, the main parameters and attributes of synchronous multi-secret sharing are compared in detail. The scheme in this paper has the characteristics of shadow update, verifiability, and less public values.

Table 1: Comparison of synchronous multi secret sharing schemes

Scheme	Participant safe passage	D safety channel	Security assumptions	Shadow update	Verifiable	Public value
Shao's [32]	NO	YES	DLP	YES	YES	$n + 2k - t + 1(k > t)$ $n + k - t(k > t)$
Zhao's [33]	NO	YES	DLP	NO	YES	$n + k + 1(k \leq t)$ $n\,(k \leq t)$
D's [35]	NO	NO	DLP-RSA	YES	YES	$2n + k - t + 1(k > t)$ $2n + 1\ (k \leq t)$
Wang's [36]	NO	YES	DLP	YES	YES	$2(n + k - t)$

(Continued)

Table 1: Continued

Scheme	Participant safe passage	D safety channel	Security assumptions	Shadow update	Verifiable	Public value
Sheikhi's [23]	NO	YES	ECDLP	YES	YES	$n+k+t+1(k>t)$ $n(k\leq t)$
Xue's [17]	YES	YES	RSA	YES	YES	$n+2k$
Ours	YES	YES	ECDLP	YES	YES	$n+2k-t+1(k>t)$ $n+t+1(k\leq t)$

In the initialization stage of the PVS-MSS scheme, the ground control center and participant calculate G_i, T_i, G by elliptic curve scalar multiplication. Therefore, there are $3n+1$ elliptic curve scalar multiplication operations. This calculation process is for the reusability of secret shadows and only needs to be performed once. In the secret distribution stage, the ground control center executes the algorithm in two different cases, including the secret polynomial calculation of each participant. At this time, only the main operations are considered. The two different cases are t and k times elliptic curve scalar multiplication, respectively. In the secret verification phase, each participant needs t elliptic curve scalar multiplication operations to verify a single secret shadow. It needs t^2 elliptic curve scalar multiplication operations to verify its correctness and other secret shadows. In the secret reconstruction stage, the PVS-MSS scheme shares the secret on the coefficient of $f(x,0)$, so the calculation cost in the secret reconstruction stage is the same as that in the scheme [23,28,30,31,33,36], both of which are Lagrange interpolation calculations, and the worst is Lagrange interpolation of k points. Suppose T_M is the operation time of elliptic curve scalar multiplication. T_H is the operation time of bivariate one-way function. $T_L(t)$ is the operation time of t point interpolation. T_E is the BP operation time on the elliptic curve. $T_{eq}(t)$ is the solution operation time of t linear equations. T_P is the modular power operation time. Tab. 2 shows the comparison of computing overhead. We can find the running time required by the PVS-MSS scheme. The scheme calculates the overhead in the distribution phase; when $k\leq t$, it is tT_M; when $k>t$, it is kT_M. The scheme calculates the cost of the verification phase; when $k\leq t$, it is t^2T_M; when $k>t$, it is k^2T_M. This scheme calculates the cost of the reconstruction phase; when $k\leq t$, it is $T_L(t)$; when $k>t$, it is $T_L(k)$.

Table 2: Comparison of computing overhead

Scheme	Distribute	Verification	Restructure
Wang's [37]	$(n+1)T_M$	$2t\mathrm{T}_E$	$T_{eq}(t)$
D's [35]	$n(T_p+T_H)$	$n(T_p+T_H)$	$T_L(k)$
Sheikhi's [23]	tT_M	t^2T_M	$T_L(t)$
Wang's [36]	$(n+1)T_P$	tT_P	$T_L(n+k)$
Ours	$tT_M(k\leq t)$ $kT_M(k>t)$	$t^2T_M(k\leq t)$ $k^2T_M(k>t)$	$T_L(t)(k\leq t)$ $T_L(k)(k>t)$

6 Parameter Analysis

6.1 Secret Share Leakage Probability of Satellite Nodes

Reference [38] shows that the probability of secret share leakage of a single satellite is an exponential function, expressed by $f(x)$, and the function varying with time x is:

$$f(x) = 1 - e^{-\lambda x} \tag{11}$$

We can see from Fig. 2 that the abscissa shown in the figure below is time, and the ordinate is leakage probability. With the increase of time X, the leakage probability also increases, and the lower the leakage rate λ at the initial time, the lower the leakage probability at the same time.

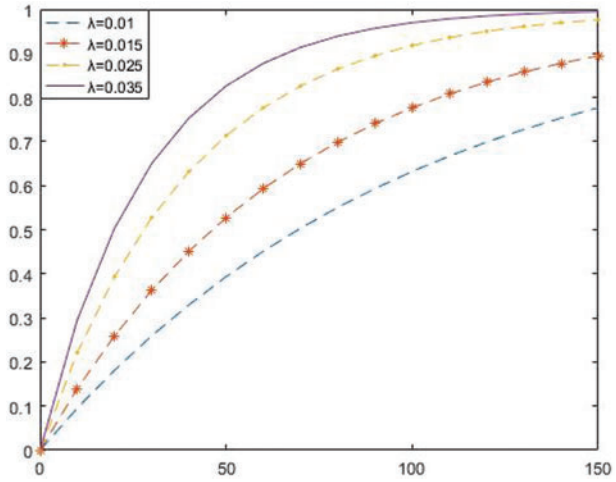

Figure 2: Secret failure rate

6.2 Satellite Network Security Quality

Reference [39] shows that the key of each satellite network node is different. Hence, the attack on a satellite nodes is a a Bernoulli process, and the probability that the secret share obtained by the attacker is less than t in one cycle:

$$P = \sum_{i=0}^{t-1} C_a^i (1 - e^{-\lambda F})^i (e^{-\lambda F})^{a-i} \tag{12}$$

When $a = 25$, $\lambda = 0.015$, Fig. 3 shows the impact of the threshold value t , and key cycle F update on satellite network security. P increases with the increase of t, and the threshold value t also increases with the increase of cycle F.

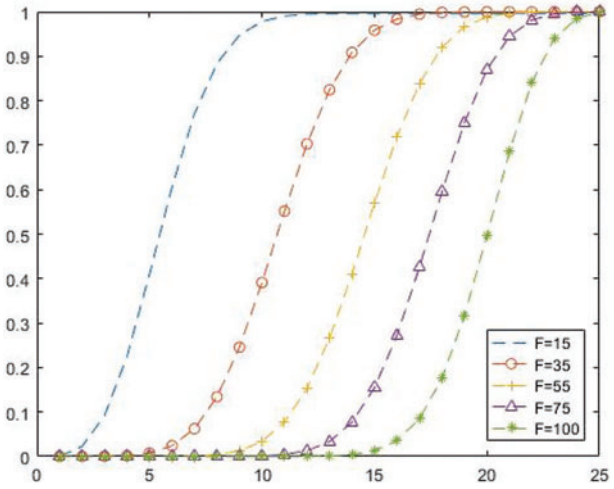

Figure 3: Satellite network security quality

7 Conclusion

It is advanced to propose a protected synchronous multi-secret sharing scheme based on binary asymmetric polynomials. It is very advanced to introduce verifiable attributes into the PSS scheme. This scheme extends the protected synchronous multi-secret sharing scheme based on binary polynomial design. This scheme is suitable for the secret sharing of satellite networks. The ECC system is used to interact with the main secret shadow safely, and a verification algorithm is constructed. Through the verification algorithm, any participant can verify the consistency and effectiveness of the secret shadow received from other participants or the secret share presented by the ground control center. We discuss the correctness of the algorithm in Section 4.1 of this paper. Whether the number of shared secrets is greater than or less than the threshold, we can get the unique polynomial from the Lagrange difference formula and the additive homomorphism of secret sharing $f(x, 0)$. We discussed security in Section 4.2 of this article. We discuss the security of the algorithm from four aspects. We use ECDLP to ensure that attackers cannot calculate secret shadows from public values; we prove the effectiveness of resisting internal and external attacks in the reconstruction process. In Section 4.3, we discuss the computational overhead of existing schemes. Our algorithm is based on ECDLP for protection, compared with RSA/DSA; when the key is the same at the same security level, the amount of calculation is not different. This scheme uses ECC in the initialization and verification phase, which requires fewer resources and faster computing speed. The Lagrange difference calculates the cost in the secret reconstruction phase, and the worst is the Lagrange difference of k points. The system simulation and other compilation will be completed in further work. The ground control center does not directly issue the secret shadow but uses CRT to calculate the unique public value X. Participants can calculate the required secret shadow through the main secret shadow and X. When the shared secret needs to be updated, the participant's main secret shadow and private key do not need to be updated. The public value X update is very efficient, reducing the complexity of sharing secret updates in a synchronous multi-secret sharing scheme, ensuring the security of secrets, and saving satellite network resources. Our scheme can send messages in satellite networks. We can also use it in key management, secure multi-party computing, image, and audio secret sharing. Our scheme is also very suitable for situations where specific participants are present simultaneously. The secret share polynomial can also generate

the session key to protect the information exchange between participants. In this way, the participants can communicate without redistributing the key in the secret distribution center, which significantly improves the security of the session and reduces the time of generating the session key.

Acknowledgement: We gratefully acknowledge anonymous reviewers who read drafts and made many helpful suggestions.

Funding Statement: This work is supported by The State Key Laboratory of Integrated Services Networks, Xidian University (ISN22-13).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Li, J. Xie, M. Xia, Q. Li, M. Li *et al.,* "Dynamic resource pricing and allocation in multilayer satellite network," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3619–3628, 2021.
[2] M. A. Ullah, T. Alam, A. F. Almutairi and M. T. Islam, "Low profile uhf antenna design for low earth-observation cubesats," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 2533–2542, 2022.
[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Int. Workshop on Managing Requirements Knowledge (MARK)*, New York, NY, USA, pp. 313–318, 1979.
[5] H. Ghodosi, "Comments on Harn–Lin's cheating detection scheme," *Designs Codes and Cryptography*, vol. 60, no. 1, pp. 63–66, 2011.
[6] L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme," *Designs Codes and Cryptography*, vol. 52, no. 1, pp. 15–24, 2009.
[7] Y. Liu, C. Yang, Y. Wang, Z. Lei and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences*, vol. 453, no. 1, pp. 21–29, 2018.
[8] H. Y. Lin, L. Harn, "Fair reconstruction of a secret," *Information Processing Letters*, vol. 55, no. 1, pp. 45–47, 1995.
[9] L. Harn, "Comments on 'fair (t, n) threshold secret sharing scheme'," *IET Information Security*, vol. 8, no. 6, pp. 303–304, 2014.
[10] Y. Tian, J. Ma, C. Peng and J. Qi, "Fair (t, n) threshold secret sharing scheme," *IET Information Security*, vol. 7, no. 2, pp. 106–112, 2013.
[11] L. Harn, C. Lin and Y. Li, "Fair secret reconstruction in (t, n) secret sharing," *Journal of Information Security and Applications*, vol. 23, pp. 1–7, 2015.
[12] 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.
[13] W. Y. Gu, F. Y. Miao and X. T. He, "Fair secret sharing scheme based on bivariate symmetric polynomials," *Computer Engineering and Applications*, vol. 52, no. 13, pp. 38–42+109, 2016.
[14] L. Mei, C. Xu, L. Xu, X. Yu and C. Zuo, "Verifiable identity-based encryption with keyword search for IoT from lattice," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2299–2314, 2021.
[15] X. Jin, L. Su and J. Huang, "A reversible data hiding algorithm based on secret sharing," *Journal of Information Hiding and Privacy Protection*, vol. 3, no. 2, pp. 69–82, 2021.
[16] K. Javeed, X. Wang and M. Scott, "High performance hardware support for elliptic curve cryptography over general prime field," *Microprocessors and Microsystems*, vol. 51, no. 6, pp. 331–42, 2017.
[17] K. Xue, W. Meng, H. Zhou, D. S. L. Wei and M. Guizani, "A lightweight and secure group Key based handover authentication protocol for the software-defined space information network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3673–3684, 2020.

[18] L. Zhang, Y. Wang and H. Zhu, "Safeguarding UAV-enabled wireless power transfer against aerial eavesdropper: A colonel blotto game," *IEEE Wireless Communications Letters*, vol. 11, no. 3, pp. 503–507, 2021.
[19] L. L. Yu and W. Z. Du, "Secret sharing scheme based on symmetric bivariate polynomial," *Computer Engineering and Applications*, vol. 56, no. 13, pp. 120–123, 2020.
[20] L. Harn, C. F. Hsu, Z. Xia and J. W. Zhou, "How to share secret efficiently over networks," *Security and Communication Networks*, vol. 2017, pp. 1–6, 2017.
[21] T. Zhang, X. H. Ke and Y. X. Liu, "(t, n) multi-secret sharing scheme extended from Harn-Hsu's scheme," *Eurasip Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 71, 2018.
[22] L. Harn, C. F. Hsu, "(t, n) multi-secret sharing scheme based on bivariate polynomial," *Wireless Personal Communications*, vol. 95, pp. 1495–1504, 2017.
[23] Maryam, G. S., Mojtaba, B., Christophe *et al.,* "Threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem," *IET Information Security*, vol. 13, no. 3, pp. 278–284, 2019.
[24] D. Tang and H. P. Shu,"Bivariate polynomial based secret sharing technology study," *Computer Applications and Software*, vol. 29, no. 7, pp. 112–114, 2012.
[25] L. Zhang, L. Hong, C. Guo, H. T. Xu, L. Y. Song *et al.,* "Satellite-aerial integrated computing in disasters: User association and offloading decision," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Dublin, Ireland, pp. 554–559, 2020.
[26] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[27] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[28] C. C. Yang, T. Y. Chang and M. S. Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.
[29] C. W. Chan and C. C. Chang, "A scheme for threshold multi-secret sharing," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 1–14, 2005.
[30] L. J. Pang, Y. Liu and Y. M. Wang, "An efficient. Threshold multi-secret sharing scheme," *Chinese Journal of Electronics*, vol. 34, no. 4, pp. 587–589, 2006.
[31] X. W. Zhong, L. Z. Xiong and Z. H. Xia, "A secure visual secret sharing scheme with authentication based on QR code," *Journal on Big Data*, vol. 3, no. 2, pp. 85–95, 2021.
[32] J. Shao and Z. Cao, "A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme," *Applied Mathematics and Computation*, vol. 168, no. 1, pp. 135–140, 2005.
[33] J. Zhao, J. Zhang and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 138–141, 2007.
[34] J. Shao, "Efficient verifiable multi-secret sharing scheme based on hash function," *Information Sciences*, vol. 278, no. 1, pp. 104–109, 2014.
[35] M. H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards & Interfaces*, vol. 30, no. 3, pp. 187–190, 2008.
[36] N. Wang, Y. Y. Cai, J. Fu and X. Q. Chen, "Information privacy protection based on verifiable (t, n)-Threshold multi-secret sharing scheme," *IEEE Access*, vol. 8, pp. 20799–20804, 2020.
[37] S. J. Wang, Y. R. Tsai and C. C. Shen, "Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ECC," *Wireless Personal Communications*, vol. 56, no. 1, pp. 173–182, 2011.
[38] H. F. Chen, W. D. Zhao and G. B. Xi, "Security analysis for proactive secret sharing system," *Zhejiang Daxue Xuebao (Gongxue Ban)/Journal of Zhejiang University*, vol. 40, no. 8, pp. 1358–1357, 2006.
[39] C. Y. Luo, W. Li, H. L. Li and B. Jian, "Measurement method for space networks authenticated key security under distributed CA," *Dianzi Yu Xinxi Xuebao/Journal of Electronics and Information Technology*, vol. 31, no. 10, pp. 2316–2320, 2009.