Secret Sharing Based On Bilinear Mapping

Caifen Wang[1, 2], Shunchang Su[1]

[1]School of Computer Science and Engineering, Northwest Normal University, Lanzhou, China;

[2]Shenzhen Technical University, Shenzhen, China

Abstract. A new verifiable secret sharing scheme based on bilinear mapping is proposed，the correctness and validation of the scheme are proved, and the security and performance are analyzed and discussed. Compared with most existing schemes, the advantage of this scheme is that participants can verify the correctness of shadow secrets by bilinear mapping, and it is provably secure. The scheme separates the participant's private key calculation from the secret distribution process, and the secret distributor does not need to save the participant's private key safely. It has better security and efficiency, and is more suitable for practical application.

Keywords: Bilinear mapping, secret sharing, multi secret sharing, verifying.

1. Introduction

In the late 1970s, secret sharing was put forward by Shamir [1] and Blakley [2], which is a very important branch in the field of modern cryptography, and it is one of the effective means to solve the data secure storage and access control. Secret sharing has important theoretical significance and wide application value.

Secret sharing can generally be attributed to threshold secret sharing and access structure secret sharing. Based on different application environments, scholars have put forward many new secret sharing schemes，such as Multilevel secret sharing schemes[3] [4] , verifiable secret sharing[5] , secret sharing without secret distributors[6] , and secret sharing that can prevent the restoration of secrets[7], etc. However, the current research on secret sharing schemes mainly focuses on verifiable secret sharing, multi-secret sharing, effective distribution of secret shareing, and resistance to participants' deception. However, the scheme of constructing secret sharing based on new design ideas and mathematical models is obviously lacking. There are many proposed secret sharing schemes including Shamir's Lagrange interpolation scheme, Blakley's vector scheme, Asmuth's Chinese Remainder Theorem scheme, Karnin's matrix multiplication scheme[8] , Naor's visual cryptography image sharing scheme[9] [10] , Santis's multi-resolution filter sharing scheme[11] , bilinear pairing sharing scheme[12], and quantum secret sharing[13] [14] , etc. The proposals of these schemes have greatly enriched the theoretical system of secret sharing.

With the wide application of bilinear pairing in public key cryptography, it will be a new attempt to construct secret sharing scheme by bilinear transformation. In fact, this attempt is reasonable because in a broad sense, secret sharing is actually a special public key algorithm, that is, a secret distributor distributes secret information and multiple participants decrypt and restore the secret. Li Huixian proposed a provably secure secret sharing algorithm based on bilinear transformation. However, this scheme is based on the honesty of participants and costs greatly in the system establishment stage. In summary, eon the basis of previous research on secret sharing，this paper presented a verifiable secret sharing scheme based on bilinear pairings and analyzed its security . Compared with state-of -art secret sharing scheme, in addition to realizing the functions of traditional secret sharing schemes, this scheme has more verifiability and new features.

2. Preliminaries and Definitions

In this section, we gave some basic notions with respect to bilinear pairing and VSS.

2.1 Bilinear Pairings

Let G_1 and G_2 be two groups of order p .suppose G_1 is an additive group and G_2 is a multiplicative group, respectively. A map e：$G_1 \times G_1 \to G_2$ is called a bilinear map or a bilinear pairing if it satisfies the following conditions:

1. Bilinear: for all $g_1, g_2, p \in G_1, e(g_1 + g_2, P) = e(g_1, P)e(g_2, P)$, $e(P，g_1 + g_2) = e(P，g_1)e(P，g_2)$ and $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

2. Non-degeneration: $\exists g \in G_1$, such as $e(g, g) \neq 1$.

3. Computable: for all $g_1, g_2 \in G_1$, there is an efficient algorithm to compute $e(g_1, g_2)$.

We say that G_1 is a bilinear group if there exist a group G_2 and a bilinear map e：$G_1 \times G_1 \to G_2$ as above, where e and the group action in G_1 and G_2 can be efficiently computed.

3. Secret Sharing Model

3.1 Secret Sharing Members

Distributor D: The secret S to be shared is divided into n shadow secrets, generates the user's private key , and sends the user's private key to the user.

User U : The user has a valid user private key.

Participants P_j : Some users participate in secret reconstruction. Participants use their own user private key to obtain shadow secrets and reconstruct secret.

Enemy A: There are two kinds of enemies in the process of secret recovery in terms of internal enemy and external enemy. Internal adversary: a cheater or a conspirator who holds the user's private key in the secret recovery phase; External adversary: an attacker with no distributor distributes the user's private key in the secret recovery phase.

Bulletin board: Used to store public parameters, participants can obtain useful parameter information from the bulletin board, but only distributors have the right to update and modify the bulletin board.

3.2 Secret Sharing Attack Model [15]

In this paper, we mainly focused on two attack models such as external and internal adversaries.

External adversary means that an attacker without user's private key fails to reconstruct secret or acquire secret information by disguising its identity. The attacking ability of external enemies is mainly manifested in two aspects. On the one hand, in the distribution phase, the external adversary modifies the shadow secrets sent by the distributor to the participants; makes the participants reconstruct errors and cheats. On the other hand, in the reconstruction phase, external adversaries impersonate legitimate users, provide false shadow secrets, and result in reconstruction errors and deception.

Internal adversary is an attack that legitimates users with valid shadow secrets sends invalid shadow secret shares to participate in the reconstruction stage, so that other participants cannot recover their secrets and reconstruct their own secrets correctly. Because the internal attacker has valid share and identity, and the attack has concealment.

3.3 Secret Sharing Security Model

Verifiable secret sharing schemes based on bilinear pairings should be correct, secure and verifiable. Therefore, the scheme in this paper must satisfy the following requirements:

Correctness: Any participant greater than or equal to t can reconstruct the secret.

Security: Any participant less than t can not obtain any secret information; If there are external enemies, the scheme can effectively resist external enemy attacks; if there are internal enemies, the scheme can resist internal enemy deception.

Verifiability: Participants can verify the validity of the shadow secrets provided by distributors, and the reconstruction phase can verify the validity of the shadow secrets sent by participants.

4. Scheme Description

Let （G_1,+） and （G_2,●） be cyclic groups of order p, where （G_1,+） is an additive group and （G_2,●） is a multiplicative group, e is bilinear transformations on groups G_1 and G_2 .W is a set of n participants, t is a threshold value, S is a secret .

4.1 Initialization Phase

In this stage, the secret distributor performs the following operations:

1. Randomly select y and $g_2 \in G_1$, and make $g_1 = g^y$.

2. Update g_1, g_2 to bulletin board and save y as distributor's private key.

3. The distributor randomly selects $r(r = 1,2,\cdots,n)$ non-zero constant x_r from Zp and labels U_r .

4.2 Key Generation Stage

In the stage of secret distribution, each participant interacts with the secret distributor. The secret distributor calculates the private key for x_r . The secret distributor performs the following operations.

1. Randomly select t-1 positive integers $\mathrm{y}_1, y_2, \cdots y_{t\text{-}1}$ in Z_p and construct user private key polynomials:

$$\mathrm{H}(x) = y + y_1 x + y_2 x + \cdots + y_{t\text{-}1} x^{t\text{-}1}$$

2. Compute the participant's private key: $\mathrm{K_i} =（g_2)^{H(x_r)} (i \in n)$

Secretly send $\{\mathrm{K_i} =（g_2)^{H(x_i)} \,||\, x_i\}$ to participants U_i .

4.3 Distribution Stage

The distributor randomly selects $a_1, a_2, \cdots, a_{t-1}$ from G_1, S is secret,

Constructing Secret Polynomials $F(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$, and calculate $S_i = F_t(i)(i = 1,2,\cdots,n)$.

Calculation $\partial_i = e(a_i, g)(i \in t-1)$, $\partial_0 = e(S, g)$ .To enable t or more participants to recover the secret S ,the secret distributor randomly selects an integer s and calculates the following information:

$\mathrm{D_{1i}} = e(g_1, g_2)^s S_i x_i (i \in n) \quad D_2 = g^s$

Update $\mathrm{E} = (\partial_0, \partial_1, \partial_2, \cdots, \partial_i, \mathrm{D}_{11}, \mathrm{D}_{12}, \cdots \mathrm{D}_{1i}, \mathrm{D}_2)(\mathrm{i} \in \mathrm{n})$ to bulletin board and destroy.

4.4 Reconstruction Stage

Arbitrary $k(k > t)$ participants gather $\Gamma \subseteq \mathrm{W}$, secrets are obtained in the following ways.

Participants enter private key K_i to compute shadow secrets:

$$S_i x_r = D_{1i} \prod_{i \in \Gamma} \left(\frac{1}{e(K_i, D_2)}\right)^{\Delta_i^{\Gamma(0)}}$$

Bring Shadow Secret S and Identity x_i into Validation Equation $e(S_i, g) = \prod_{j=0}^{t-1} \partial_j^{x_i^j}$,if the validation passes, participants reconstruct the secret: $S = \sum_{i=1}^{t} S_i \prod_{1 \le j \le t} \frac{x - x_i}{x_j - x_i}$.

5. Add a New User

When a user U_{n+1} joins the user set, distributor selects an identity x_{n+1} from Z_q ,calculation $H(x_{n+1})$, $S_{n+1} = F(x_{n+1})$ and private key $\mathrm{K_i} =（g_2)^{H(x_{n+1})}$,Secretly send $\{\mathrm{K_{n+1}} =（g_2)^{H(x_{n+1})} \,||\, x_{n+1}\}$ to participant U_{n+1} .

Calculation $D_{1(n+1)} = e(g_1, g_2)^s S_{n+1} x_{n+1}$, Update $D_{1(n+1)}$ to bulletin board.

6. Delete User U_j from the User Set

Distributor randomly chooses integer r ,calculation $D'_{1_j} = e(g_1, g_2)^s S_j r$,update D'_{1_j} to the bulletin board, replace delete D_{1_j} , that is to complete the deletion of user U_j .

7. Safety and Correctness Analysis

7.1 Correctness Analysis

Theorem 1: In the process of secret reconstruction, any participant greater than or equal to t can recover the secret correctly.

$$D_1 \prod_{i\in\Gamma} (\frac{1}{e(D_2,\ K_i)})^{\Delta_{i,\ \Gamma(0)}} = e(g_1, g_2)^s S_i x_r \prod_{i\in\Gamma} (\frac{1}{e(g^s, g_2^{H(i)})})^{\Delta_{i,\ \Gamma(0)}}$$

Proof 1: $= S_i x_r e(g, g_2)^{ys} \prod_{i\in\Gamma} (\frac{1}{e(g, g_2)^{sH(i)\Delta_{i,\ \Gamma(0)}}}) = S_i x_r e(g, g_2)^{ys} \frac{1}{e(g, g_2)^{ys}}$

$= S_i x_r$

Any one or more participants can calculate $S_i x_r$, after the participants get $S_i x_r$,Get S_i with your identity x_i .Bring S_i into validation equation validation, if validation equation holds, shadow secret is correct.

Verification equation: $e(S_i, g) = \prod_{j=0}^{t-1} \partial_j^{x_i^j}$.

Proof:

$$\prod_{j=0}^{t\text{-}1} \partial_j^{x_i^j} = e(S, g) \prod_{j=1}^{t\text{-}1} e(a_i, g)^{x_i^j} = e(S, g) \prod_{j=1}^{t\text{-}1} e(x_i^j a_i, g)$$

$$= e(S + x_i a_1 + \cdots + x_i^{t-1} a_{t-1}, g) = e(S_i, g)$$

Participants calculated: $F_t(x) = (\sum_{i=1}^{t} S_i \prod_{1\le j\le t} \frac{x - x_i}{x_j - x_i})$, restore Secrets S .

Theorem 2: Deleted users U_j can not get the correct shadow secret and participate in secret recovery.

Proof 2: User brings K_i calculation as follows:

$$D_{1j} \prod_{i\in\Gamma} (\frac{1}{e(D_2,\ K_i)})^{\Delta_{i,\ \Gamma(0)}} = S_j r e(g, g_2)^{ys} \frac{1}{e(g, g_2)^{ys}} = S_j r \ .$$

r is chosen randomly by distributors and not published, so users can not determine shadow secrets uniquely and participants can not reconstruct it.

7.2 Safety analysis

Theorem 3: Any legal participant less than t cannot obtain any secret information.

Proof 3: Suppose that $t-1$ collusion participants attempt to submit the user's private key to recover the shadow secret S_i . $x_i S_i = D_{1i} \prod_{i\in\Gamma} (\frac{1}{e(K_i, D_2)})^{\Delta_i, \Gamma(0)}$, from the deduction of correctness, we can see that the finding shadow secret S_i is equivalent to t-1 participants attempting to recover their private key y .The user's private key is defined by the user's private key polynomial. According to the nature of Lagrange interpolation, any legal participant with less than t can not get any information about y,therefore, no shadow of shadow secret can be obtained, that is, no information of shared secret can be obtained.

Theorem 4: An external adversary cannot recover a secret by sending a false user's private key.

Proof 4: External adversaries submit fake user private key K_t to participate in recovery and obtain $x_r S_i$, but it does not have user identity, so it can not get real shadow secret, so it can not participate in secret reconstruction.

7.3 Performance analysis

This section mainly analyzed the performance of this scheme from the aspects of calculation and storage.

1. In terms of computational complexity: In the whole scheme, the process of computational complexity is in the key generation stage and the distribution stage. In the key generation stage, the distributor calculates the user's private key for each participant. The number of exponential operations to be performed on group G_1 is $2n+1$.The largest amount of computation in the distribution phase is the $n+1$ exponential operation needed in D_{1i} calculation. Comparing with the traditional scheme, the computational complexity is within acceptable range.

2. Storage: The storage capacity of the scheme mainly includes the size of bulletin board information and confidential information. The bulletin board information will not leak any information about the secret, and will not affect the security of the scheme. It can be stored by multiple participants. For distributors, only the distributor's private key needs to be stored, and participants only need to store the participant's private key, which will not cause too much burden to the system.

3. Overall aspect: Compared with the traditional secret sharing scheme, the shadow secret computing process and secret recovery algorithm are separated. The calculation of participant's private key has nothing to do with the shared secret. Even if the participant obtains the shadow secret, the distribution initiative of the secret is still in the hands of the distributor, therefore, this scheme is more secure.

8. Summary

In this paper, a secret sharing scheme based on bilinear pairings and its extension scheme was proposed by using the properties of bilinear pairings. The analysis showed that this scheme is a provably secure and effective secret sharing scheme, which is safer than the existing scheme and has more practical application value.

Reference

[1].Shamir A. How to Share a Secret[J]. Communications of the Acm, 2011, 22(22):612-613.

[2].Blakley G. Safeguarding Cryptographic Keys[C]//Proc. of AFIPS'79National Computer Conference. New York, USA: AFIPS Press,1979.

[3].J. He, E. Dawson, Multistage secret sharing based on one-way function, Electron. Lett. 30 (1994) 1591–1592.

[4].Crescenzo G D. Sharing one secret vs. sharing many secrets[J]. Theoretical Computer Science, 2003, 295(1-3):123-140.

[5].Tompa M, Woll H. How to Share a Secret with Cheaters[J]. Journal of Cryptology, 1989, 1(3):133-138.

[6].Obana S, Kurosawa K. Veto is impossible in secret sharing schemes[J]. Information Processing Letters, 1996, 58(6):293-295.

[7]. Bonis A D, Santis A D. Randomness in secret sharing and visual cryptography schemes[J]. Theoretical Computer Science, 2004, 314(3):351-374.

[8]. Karnin E D, Greene J, Hellman M E. On secret sharing systems[J]. IEEE Trans on It, 1983, 29(1):35-41.

[9]. Naor M, Shamir A. Visual Cryptography[J]. Lecture Notes in Computer Science, 1994, 950(9):1-12.

[10]. Li P, Yang C N, Kong Q. A novel two-in-one image secret sharing scheme based on perfect black visual cryptography[J]. Journal of Real-Time Image Processing, 2018, 14(1):41-50.

[11]. Santis A D, Desmedt Y, Frankel Y, et al. How to share a function securely[C]. Twenty-sixth Acm Symposium on Theory of Computing. DBLP, 1994.

[12]. Li Huixian, Pang Liaojun. Provable Secret Sharing Scheme Based on Bilinear Transform [J]. Journal of Communications, 2008, 29 (10): 45-50.

[13]. Liu C J, Li Z H, Bai C M, et al. Quantum-Secret-Sharing Scheme Based on Local Distinguishability of Orthogonal Seven-Qudit Entangled States[J]. International Journal of Theoretical Physics, 2018.

[14]. Qin Sujuan, Liu Tailin, Wen Qiaoyan. Quantum secret sharing based on entanglement exchange and local operation [J]. Journal of Beijing University of Posts and Telecommunications, 2005, 28 (4): 74-77

[15]. Li Jieping, Wei Xingjia. Secret Sharing Scheme Based on Chinese Remainder Theorem [J]. Communication Technology, 2018 (3).