Linear Threshold Verifiable Secret Sharing in Bilinear Groups

Jie Zhang*

School of Computer Science and Technology,
Nanjing Normal University, Nangjing 210046, China
E-mail:464516929@qq.com
*Corresponding author

Futai Zhang

School of Computer Science and Technology,
Nanjing Normal University, Nangjing 210046, China
E-mail:zhangfutai@njnu.edu.cn

Abstract: In many pairing based cryptosystems, the secret keys are elements of bilinear groups. For safeguarding such secret keys or decrypting or signing in a threshold manner, verifiable secret sharing in bilinear groups is required. In this paper, we show a method of verifiably sharing a random secret in a bilinear group. Our method is simple and practical. It can be regarded as a generalization of threshold linear verifiable secret sharing in finite fields to the case when the secrets are in bilinear groups. We present a general scheme for verifiably sharing secrets in bilinear groups. A modified version of our general scheme with improved efficiency is also introduced.

Keywords: bilinear groups; verifiable secret sharing; linear verifiable secret sharing.

Biographical notes: Jie Zhang is doing her Master's Degree in Computer Applications at School of Computer Science and Technology, Nanjing Normal University, Nanjing, China. Her areas of interest are secret sharing, bilinear pairing.
Futai Zhang has done his Doctor's Degree in Cryptography in the year 2001 from Xidian University. He is presently working as an Professor in the School of Computer Science and Technology, Nanjing Normal University. His research interest is theory of cryptography technology and its applications.

1 Introduction

Secret sharing (Shamir, 1979; Blakley and Kabatianskii, 1994) is a significant technique for safeguarding very confidential information such as cryptographic keys. It has been identified as a fundamental tool in key management, threshold cryptography, and secure multi-party protocols, etc. In a secret sharing scheme, a dealer who holds a secret distributes shares of the secret among a set of participants in such a way that only some qualified subsets of participants can later recover the secret when pulling their shares together. Many of the traditional linear secret sharing schemes are a type of secret sharing schemes where the secret to be shared is an element of a finite field F, and each share is computed as a fixed linear function of the secret and some random field elements chosen by the dealer. In a (t, n) threshold secret sharing scheme, there are n participants, and t or more participants form a qualified subset. The famous Shamir (t, n) threshold secret sharing scheme(Shamir, 1979) is a typical linear threshold secret sharing scheme.

Verifiable secret sharing (VSS for short) is first proposed by B.Chor et al in (Chor et al., 1985) to deal with the problem of cheating from the dealer in traditional secret sharing schemes. In a VSS scheme, participants are able to verify whether the shares they received from the dealer are valid. And in the reconstruction phase, each participants can check if the shares submitted by the other cooperators are correct. Techniques for verifiably sharing a secret that is an element of a finite field have been studied for many years. By now, many schemes within this category, either the threshold ones (Chor et al., 1985; Rabin and Ben-Or, 1989; Feldman, 1987; Pedersen, 1991) or the generalized ones (Zhang et al., 2002), have been available. Nevertheless, there are only a few VSS schemes for sharing a random element of a bilinear group. In (Baek and Zheng, 2004), J.Baek and Y.Zheng investigated such VSS for the first time. They introduced two VSS schemes in bilinear groups as building blocks of their expected ID-based threshold signature and decryption schemes. Their work uses the polynomial interpolation method proposed by A.Shamir to share the

secret and consequently belongs to a particular case of threshold linear VSS.

In this paper, we study the topic of threshold linear verifiable secret sharing in bilinear groups. We generalize the technique of threshold linear verifiable secret sharing in finite fields to the case of bilinear groups. Our method of threshold linear verifiable secret sharing in bilinear groups results in a class of secret sharing schemes that include J.Baek and Y.Zheng's work as a special case. We give analysis for the correctness and the security of the newly proposed scheme in detail. Additionally, we also show a modified version of our scheme that effectively reduces the computational cost for sharing.

The rest of the paper is organized as follows. In Section 2 we give some basic notions with respect to bilinear pairing and verifiable secret sharing. Then in Section 3 we shortly review J.Beak and Y.Zheng's VSS (Baek and Zheng, 2004) that uses the polynomial interpolation in bilinear groups. In Section 4 we give a detailed description of our VSS scheme in bilinear groups and heuristically analyze its security. After that in Section 5 we show a modified scheme with lower computational cost and analyze its efficiency. At last in Section 6 we just conclude this paper.

2 Preliminaries and Definitions

In this section we give some basic notions with respect to bilinear pairing and verifiable secret sharing.

2.1 Bilinear Pairings

Let G and G_T be two groups of order q for some large prime q. Suppose G is an additive group and G_T is a multiplicative group respectively. A map $\hat{e} : G \times G \longrightarrow G_T$ is called a bilinear map or a bilinear pairing if it satisfies the following conditions(Wu and Tseng, 2011; Kiltz and Pietrzak, 2010; Boneh, D. and Franklin, 2001; Gentry, 2006; Boneh, D. and Boyen, 2004):

1 Bilinear: For all $P, Q \in G$ and $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

2 Non-degenerate: There exist $P, Q \in G$ such that $\hat{e}(P, Q) \neq 1$.

3 Computable: For all $P, Q \in G$, there exists an efficient algorithm to compute $\hat{e}(P, Q)$.

We say that G is a bilinear group if there exists a group G_T and a bilinear map $\hat{e} : G \times G \longrightarrow G_T$ as above, where $\hat{e}$ and the group action in G and G_T can be efficiently computed.

2.2 Notation for Operation

Let G be a group of prime order q, $K = Z_q$ be the finite field with q elements. Assume $\alpha = (a_1, ..., a_t)$, $\beta = (b_1, ..., b_t)$ are vectors with $a_1, ..., a_t, b_1, ..., b_t \in K$ and $B = (B_1, ..., B_t)$ is a vector with $B_1, ..., B_t \in G$. Suppose $M = (m_{ij}) = (M_1, M_2, ..., M_n)$ is a t by n matrix in K, where $M_j (j = 1, ..., n)$ denotes the jth column vector of M. In our construction, we use the operation of inner product $\alpha \bullet \beta$ in K, an operation $\alpha \circ B$ of a t-dimensional vector α in K with a t-dimensional vector B in G, an operation $\alpha * M$ of a t-dimensional vector α in K and a $t \times n$ matrix M in K, and an operation $B \star M$ of a t-dimensional vector B in G with a $t \times n$ matrix M in K. These operations are defined in a very simple and natural way as follows.

- $\alpha \bullet \beta = \beta \bullet \alpha = a_1 b_1 + a_2 b_2 + \cdots + a_t b_t$,
- $\alpha \circ B = B \circ \alpha = a_1 B_1 + a_2 B_2 + \cdots + a_t B_t$,
- $\alpha * M = (\alpha \bullet M_1, \alpha \bullet M_2, ..., \alpha \bullet M_n) = (\sum_{i=1}^{t} a_i m_{1i}, \sum_{i=1}^{t} a_i m_{2i}, ..., \sum_{i=1}^{t} a_i m_{ni}$
- $B \star M = (B \circ M_1, B \circ M_2, ..., B \circ M_n) = (\sum_{i=1}^{t} m_{1i} B_i, \sum_{i=1}^{t} m_{2i} B_i, ..., \sum_{i=1}^{t} m_{ni} B_i)$

2.3 Verifiable Secret Sharing

A verifiable secret sharing(VSS) scheme is a secret sharing scheme that requires the dealer to broadcast some verification information such that each participant can verify the validity of his share. Here we briefly review the the communication model, the building blocks and the security requirements of a VSS scheme.

2.3.1 Communication model.

A verifiable secret sharing scheme involves n participants $P_1, ..., P_n$ and a dealer D. They are connected by a complete network of private point-to-point channels and have access to a dedicated broadcast channel.

2.3.2 Building blocks.

A VSS scheme contains three basic algorithms as follows:

- **Algorithm of distribution:** This algorithm is executed by the dealer to publish commitments that used for verification and distribute shares to the participants.
- **Algorithm of verification:** The participants run this algorithm to verify whether the shares they received are valid.
- **Algorithm of reconstruction:** A qualified subset of participants execute this algorithm to recover the shared secret together.

2.3.3 Security requirements.

Assume a static and strong admissible adversary (Gennaro, 1996), i.e. the adversary has determined which participants to corrupt at the start of the protocol, and can corrupt less than t participants totally. A secure VSS scheme should satisfy the following requirements.

- The adversary cannot acquire the secret from public information.
- The adversary cannot calculate the secret from the shares of those corrupted participants.
- The adversary cannot prevent the t or more honest participants from reconstructing the secret.

3 Related Works

In this section we briefly review the method of sharing a point in a group G(Baek, J. and Zheng, 2004) and J.Beak and Y.Zheng's VSS (Baek and Zheng, 2004) that uses the polynomial interpolation in bilinear groups.

3.1 Secret Sharing over G

- *Parameters*

  Let G be a group of a prime order q. Suppose the dealer D holds a random secret $S \in G^*$ to be shared among n participants $P_1, ..., P_n$ and t is the threshold such that $1 \leq t \leq n < q$.

- *Distribution phase*

  1 Pick $A_1, ..., A_{t-1}$ uniformly at random from G^*. Construct a polynomial $F(x) = S + A_1 x + \cdots + A_{t-1}x^{t-1}$.

  2 Compute $S_i = F(i)$ for $i = 1, ..., n$ and secretly send S_i to P_i.

- *Reconstruction phase*

  Suppose $\Phi \subseteq \{1, ..., n\}$ be a set such that $|\Phi| \geq t$ where $|\cdot|$ denotes the cardinality of a given set. The secret can be reconstructed by computing $S = \sum_{i\in\Phi} c_{0i}^{\Phi} S_i$ where $c_{0i}^{\Phi} = \prod_{j\in\Phi, j\neq i} \frac{j}{j-i} \in Z_q$.

3.2 J.Beak and Y.Zheng's VSS in Bilinear Groups

- *Parameters*

  Let $(G, G_T, q, P, \hat{e})$ be a set of parameters as defined in Section 2, that is, G is a bilinear group of a lager prime order q, P is a generator of G such that computing discrete logarithm with respect to the basis P is infeasible in G and $\hat{e}$ is a bilinear map. Suppose $S \in G^*$ is the secret to be shared. The number of participants is n and the threshold is t with the restriction $1 \leq t \leq n < q$. Note that here the operation in group G is denoted by addition.

- *Algorithm of sharing*

  1 D chooses $A_1, ..., A_{t-1}$ uniformly at random from G^*. Construct $F(x) = S + A_1 x + \cdots + A_{t-1}x^{t-1}$ and compute $S_i = F(i)$ for $i = 1, ..., n$.

  2 Send S_i secretly to P_i for $i = 1, ..., n$. Broadcast $E_0 = \hat{e}(S, P)$ and $E_i = \hat{e}(A_i, P)$ for $i = 1, ..., t-1$.

- *Algorithm of verification*

  When P_i has received his share S_i he verifies if

  $$\hat{e}(S_i, P) = \prod_{j=0}^{t-1} {E_j}^{i^j} \tag{1}$$

  If the verification fails, the share S_i assigned to P_i is invalid.

- *Algorithm of reconstruction*

  Without loss of generality, we suppose $P_1, ..., P_t$ be the t participants to reconstruct the shared secret. Each P_i broadcasts his share S_i to the other cooperators, and every participator can check its validity through Equation 1. For $i = 1, ..., t$, while all S_i have been verified to be valid, every cooperator can reconstruct S by computing

  $$S = \sum_{i=1}^{t} S_i \prod_{1\leq j\leq t, j\neq i} \frac{i}{i-j} \tag{2}$$

4 Linear Threshold VSS in Bilinear Groups

In this section we integrate the techniques of linear threshold VSS in finite field and J.Beak and Y.Zheng's VSS in Bilinear Groups to get a method of linear threshold VSS in bilinear groups. In what follows we give a detailed description of the resulted VSS scheme and a heuristic analysis on its security.

4.1 Description of the Scheme

- *Parameters*

  Let G be an additive cyclic group of a large prime order q, G_T a multiplicative group of the same order, and $\hat{e} : G \times G \longrightarrow G_T$ a bilinear map. Let P be a generator of G such that the discrete logarithm problem with basis P in G and the discrete logarithm problem with basis $\hat{e}(P, P)$ in G_T are intractable. We denote by D the dealer, $P_1, P_2, ..., P_n$ the n participants (or share holders), and t the threshold. Both the secret space and share space are G. Suppose the secret to be shared is a random element $S \in G$.

- *Distribution*

  1 D chooses a random non-zero vector $\alpha = (a_1, ..., a_t)$ with $a_1, ..., a_t \in GF(q)$ and a $t \times n$ matrix $C = (c_{ij})$ with $c_{ij} \in GF(q)$, where any t column vectors of C are linearly independent and any $t-1$ column vectors of C cannot linearly express α.

2 D randomly chooses a vector $B = (B_1, ..., B_t)$ from $U(S) = \{(B_1, ..., B_t) \in G^t | \alpha \circ B = \sum_{i=1}^{t} a_i B_i = S\}$.

3 D Calculates $A_i = \hat{e}(B_i, P)$ for $i = 1, ..., t$, $(S_1, S_2, ..., S_n) = B \star C = (B \circ C_1, B \circ C_2, ..., B \circ C_n) = (\sum_{i=1}^{t} c_{i1} B_i, \sum_{i=1}^{t} c_{i2} B_i, ..., \sum_{i=1}^{t} c_{in} B_i)$ where $C_k (k = 1, ..., n)$ denotes the kth column vector of C.

4 D sends S_j to P_j secretly and publishes α, C, A_i for $i = 1, ..., t$.

- *Verification*

  Each P_j can verify the validity of his share through

$$\hat{e}(S_j, P) = \prod_{k=1}^{t} {A_k}^{c_{kj}}. \quad (3)$$

  If the equation does not hold, then the share S_j given to P_j is invalid.

- *Reconstruction*

  When the distribution is verified to be correct, any t or more participants can cooperatively reconstruct the secret. Assume $P_{i_1}, ..., P_{i_k}$ are k participants to recover S where $k \geq t$, they firstly calculate $\gamma = (r_1, ..., r_k)$ from $r_1 C_{i_1} + r_2 C_{i_2} + \cdots + r_k C_{i_k} = \alpha$, where C_{i_j} denotes the i_jth column vector of C for $j = 1, ..., k$. Then every P_{i_j} provides his share S_{i_j} to the other cooperators, and each participator can verify the validity of S_{i_j} through Equation 3. If all shares of those cooperators are correct, the secret can be computed from

$$S = \gamma \circ (S_{i_1}, ..., S_{i_k}) = \sum_{j=1}^{k} r_j S_{i_j}. \quad (4)$$

The new scheme proposed above is a generalization of J.Baek and Y.Zheng's scheme in Section 3. Obviously J.Baek and Y.Zheng's VSS scheme based on bilinear groups in Section 3 can be seen as such a linear VSS scheme by taking $\alpha = (1, 0, ..., 0)$, $B = (S, A_1, ..., A_{t-1})$ and $C = (C_1, ..., C_n)$ where $C_i = (1, i, ..., i^{t-1})^T$ for $i = 1, ..., n$.

4.2 Correctness

To show the correctness of our scheme, we need to check the correctness of the equation for verification and correctness of the formula for reconstructing the shared secret.

4.2.1 Correctness of verification

On one hand, if D performs the algorithm of *distribution* correctly, then the following equation holds:

$$(S_1, ..., S_n) = B \star C$$
$$= (\sum_{k=1}^{t} c_{k1} B_k, \sum_{k=1}^{t} c_{k2} B_k, ..., \sum_{k=1}^{t} c_{kn} B_k).$$

So we have

$$\begin{aligned} \hat{e}(S_j, P) &= \hat{e}(\sum_{k=1}^{t} c_{kj} B_k, P) \\ &= \hat{e}(B_1, P)^{c_{1j}} \cdots \hat{e}(B_t, P)^{c_{tj}} \\ &= \prod_{k=1}^{t} {A_k}^{c_{kj}} (j = 1, ..., n) \end{aligned}$$

On the other hand, if the equation for verification holds, that is $\hat{e}(S_j, P) = \prod_{k=1}^{t} {A_k}^{c_{kj}}$. Then

$$\begin{aligned} \hat{e}(S_j, P) &= \prod_{k=1}^{t} {A_k}^{c_{kj}} \\ &= \hat{e}(B_1, P)^{c_{1j}} \cdots \hat{e}(B_t, P)^{c_{tj}} \\ &= \hat{e}(c_{1j} B_1, P) \cdots \hat{e}(c_{tj} B_t, P) \\ &= \hat{e}(c_{1j} B_1 + \cdots + c_{tj} B_t, P) \end{aligned}$$

So we have $S_j = c_{1j} B_1 + \cdots + c_{tj} B_t = C_j \circ B$. This means the share S_j is valid if and only if $\hat{e}(S_j, P) = \prod_{k=1}^{t} {A_k}^{c_{kj}}$.

4.2.2 Correctness of reconstruction

From the *distribution* algorithm we have $S = \alpha \circ B$ and $S_j = C_j \circ B$ where C_j denotes the jth column vector of C, $j = 1, ..., n$. As any $k \geq t$ column vectors of C can linearly express α, there must be a vector $x = (x_1, ..., x_k)$ such that $x_1 C_{i_1} + \cdots + x_k C_{i_k} = \alpha$ for any k column vectors of $C_{i_1}, \cdots, C_{i_k}$ of C. Here we assume the k correct shares used to recover the secret is $S_1, ..., S_k$, and $\gamma = (r_1, ..., r_k)$ satisfies $r_1 C_1 + \cdots + r_k C_k = \alpha$, i.e. $(a_1, ..., a_t) = (r_1 c_{11} + \cdots + r_k c_{1k}, ..., r_1 c_{t1} + \cdots + r_k c_{tk})$. Then

$$\begin{aligned} S &= \alpha \circ B \\ &= (r_1 c_{11} + \cdots + r_k c_{1k}) B_1 + \cdots + \\ &\quad (r_1 c_{t1} + \cdots + r_k c_{tk}) B_t \\ &= r_1 (c_{11} B_1 + \cdots + c_{t1} B_t) + \cdots + \\ &\quad r_k (c_{1k} B_1 + \cdots + c_{tk} B_t) \\ &= r_1 S_1 + \cdots + r_k S_k \\ &= \gamma \circ (S_1, ..., S_k). \end{aligned}$$

Thus, the *reconstruction* algorithm is correct.

4.3 Security

We analyze the security of our scheme according to the security requirements given in Section 2.

Theorem 1: *Under the difficulty of calculating discrete logarithm to the basis P in G, the probability for the adversary to acquire the secret from public information is $1/q$.*

proof: The public information is $\alpha, C, A_i (i = 1, ..., t)$. As the discrete logarithm to the basis P is difficult to calculate in G, the discrete logarithm to basis $\hat{e}(P, P)$ in G_T is intractable too. Thus the adversary cannot calculate B_i from $A_i = \hat{e}(B_i, P)$ for $i = 1, ..., t$. Without knowing $B = (B_1, ..., B_t)$, the adversary has to guess S from the secret space G. That is, the probability for the adversary to acquire the secret from public information is $1/q$. □

As q is a large prime, the probability $1/q$ can be neglected. We can conclude that under the intractability of calculating discrete logarithm to the basis P in G, the adversary cannot acquire the secret from public information.

Theorem 2: *An adversary who corrupts up to $t-1$ participants cannot get any information about the shared secret except what is implied by the public information.*

proof: According to the algorithm of *reconstruction*, to acquire the secret S, the adversary has to get t or more shares. Thus he need to calculate at lest one more shares of honest participants from the shares of those corrupted ones. From Theorem 1 we know that the adversary cannot acquire the vector B from public information. However, according to the algorithm of *distribution*, to acquire the shares of those honest participants, the adversary has no choice but compute B merely using the shares of the corrupted ones. Without loss of generality we suppose that the corrupted participants are $P_1, ..., P_{t-1}$, the adversary has to compute $B_1, ..., B_t$ from the following system of equations:

$$\begin{cases} lS_1 = C_1 \circ B = c_{11}B_1 + c_{21}B_2 + \cdots + c_{t1}B_t \\ S_2 = C_2 \circ B = c_{12}B_1 + c_{22}B_2 + \cdots + c_{t2}B_t \\ \vdots \\ S_{t-1} = C_{t-1} \circ B = c_{1,t-1}B_1 + c_{2,t-1}B_2 + \cdots \\ \qquad + c_{t,t-1}B_t \end{cases} \tag{5}$$

This system of equations has t unknowns $(B_1, ..., B_t)$ and $t-1$ equations. Let $S_i = s_i P, i = 1, 2, ..., t-1, B_j = x_j P, j = 1, 2, ..., t$. Then the above system of equations is reduced to the following system of linear equations in $GF(q)$:

$$\begin{cases} ls_1 = c_{11}x_1 + c_{21}x_2 + \cdots + c_{t1}x_t \\ s_2 = c_{12}x_1 + c_{22}x_2 + \cdots + c_{t2}x_t \\ \vdots \\ s_{t-1} = c_{1,t-1}x_1 + c_{2,t-1}x_2 + \cdots + c_{t,t-1}x_t \end{cases} \tag{6}$$

It is obvious that this system of linear Equation 6 has a solution $x_1 = b_1, x_2 = b_2, ..., x_t = b_t$ if and only if the former system of Equation 5 has a solution $B_1 = b_1 P, B_2 = b_2 P, ..., B_t = b_t P$. As the rank of the coefficient matrix of Equation 6 is $t-1$, it has exactly q solutions. Thus the system of Equation 5 has also exactly q solutions. In these q solutions, only one is the correct $B_1, ..., B_t$ used by the dealer in the distribution phase. So the probability for the adversary to get the correct $B_1, ..., B_t$, and hence get the shared secret is $1/q$. □

Theorem 3: *When $t \leq (n+1)/2$ the adversary cannot prevent t or more honest participants from reconstructing the secret.*

proof: From the definition of static and strong admissible adversary we know that the adversary has determined which participants to corrupt at the start of the protocol, and can corrupt less than t participants totally. This means there are at least $n - t + 1$ honest participants. As $t \leq (n+1)/2$, the number of honest participants is not less than $n - t + 1 \geqslant t$. So we can conclude that the adversary cannot prevent the t or more honest participants from reconstructing the secret when $t \leq (n+1)/2$. □

4.4 Computational Cost

To analyze the computational cost of our scheme, here we just count those time-consuming operations in different phases. Let $\mathcal{P}$, $\mathcal{S}$ and $\mathcal{E}$ denote the operation of bilinear pairing from G^2 to G_T, scalar multiplication in G and exponentiation in G_T respectively. In the distribution phase we consider the computational cost of D in calculating all the public information and shares, in verification phase we consider the cost for all of the n participants in verifying their shares, and at last in the reconstruction phase we assume there are t participants and the cost of verification is not included. The result is listed in the following table.

Table 1 Computational cost of the new scheme in different phases.

	$\mathcal{P}$	$\mathcal{S}$	$\mathcal{E}$
Distribution phase	t	nt	0
Verification phase	n	0	nt
Reconstruction phase	0	t	0

From Table 1 we can see that in the distribution phase the new scheme takes t bilinear pairings and nt scalar multiplications in G, and in the verification phase it needs n bilinear pairings and nt exponentiations in G_T. The reconstruction phase just needs t scalar multiplications in all.

5 A Modified Scheme With Improved Efficiency

In this section we show a modified scheme with higher efficiency compared with the previous one. This scheme

demands the dealer knows the discrete logarithm of the secret, thus it applies to situations where the secret can be generated by the dealer firstly choosing its discrete logarithm. We just give the description of the modified scheme and analyze its efficiency. The analysis of correctness and security are similar to that of the previous one and hence is omitted.

5.1 Description of the Scheme

- *Parameters*
  The common parameters $(G, G_T, \hat{e}, q, P, \hat{e}(P,P), n, t)$ are defined the same as before. G and G_T are groups with the same large prime order q where G is an additive group and G_T is a multiplicative group. P is a generator of G such that computing discrete logarithm to the basis P in G is intractable. $\hat{e} : G \times G \longrightarrow G_T$ is a bilinear map. Both the secret space and the share space are G. D is the dealer and $P_1, ..., P_n$ are the n participants. t is the threshold.
  Before executing the algorithm of distribution, the dealer first chooses an element s from Z_q^* and sets $S = sP$ be the secret to be shared.

- *Distribution*

  1 D uniformly chooses a random non-zero vector $\alpha = (a_1, ..., a_t)$ with $a_1, ..., a_t \in GF(q)$ and a $t \times n$ matrix $C = (c_{ij})$ over $GF(q)$, where any t column vectors of C are linearly independent and any $t-1$ column vectors of C cannot linearly express α.

  2 D chooses a random vector $\beta = (b_1, ..., b_t)$ such that $\alpha \bullet \beta = \sum_{k=1}^{t} a_k b_k = s$.

  3 D computes $(s_1, s_2..., s_n) = \beta * C = (\beta \bullet C_1, \beta \bullet C_2, ..., \beta \bullet C_n)$ where $C_k (k = 1, ..., n)$ denotes the kth column vector of C, $A_i = \hat{e}(P,P)^{b_i}$ for $i = 1, ..., t$.

  4 For $j = 1, ..., n$, D sets $S_j = s_j P$ and sends S_j to P_j secretly. D the broadcasts α, C, A_i for $i = 1, ..., t$.

- *Verification*
  Each P_j can verify the validity of his share through $\hat{e}(S_j, P) = \prod_{k=1}^{t} A_k{}^{c_{kj}}$ for $j = 1, ..., n$.

- *Reconstruction*
  When the distribution is verified to be correct, any t or more players can cooperate to reconstruct the secret. Assume $P_1, ..., P_k$ are $k (k \geq t)$ participants intend to recover S, they firstly calculate a vector $\gamma = (r_1, ..., r_k)$ from $(C_1, ..., C_k)(r_1, ..., r_k)^T = r_1 C_1 + r_2 C_2 + \cdots + r_k C_k = \alpha$, where $C_j (j = 1, ..., k)$ denotes the jth column vector of C. Then every P_j provides his share S_j to the other cooperators, and each participant can verify the validity of S_j through $\hat{e}(S_j, P) = \prod_{i=1}^{t} A_i{}^{c_{ij}}$. If all shares of those cooperators are correct, the secret can be computed from $S = \gamma \circ (S_1, ..., S_k) = \sum_{j=1}^{k} r_j S_j$.

5.2 Computational Cost

To compare the computational cost of the newly proposed scheme with J.Baek and Y.Zhang's scheme in Section 3 and the scheme proposed in Section 4, we count those time-consuming operations in different phases and list them in the following table. The notation is defined the same as in Section 4.

Table 2 Comparison of the three schemes in computational cost.

	Section 3	*Section 4*	*Section 5*
distribution	$t\mathcal{P} + n(t-1)\mathcal{S}$	$t\mathcal{P} + nt\mathcal{S}$	$n\mathcal{S} + t\mathcal{E}$
verification	$n\mathcal{P} + nt\mathcal{E}$	$n\mathcal{P} + nt\mathcal{E}$	$n\mathcal{P} + nt\mathcal{E}$
reconstruction	$t\mathcal{S}$	$t\mathcal{S}$	$t\mathcal{S}$

From Table 2 we see the modified scheme takes less bilinear pairings totally than the former two, and scalar multiplications in this scheme is reduced. As computing bilinear pairings is the most time-consuming operation, it is reasonable to say that the modified scheme has a smaller computational cost.

6 Conclusion

In this paper, we have investigated verifiable secret sharing in bilinear groups. Two linear threshold verifiable secret sharing schemes in bilinear groups have been presented. The first scheme is a general one for sharing any randomly chosen secret in a bilinear group. And the second one is a modified scheme with improved efficiency for sharing a secret whose discrete logarithm is known to (and only to) the dealer. Our sharing method is a generalization of the technique of linear verifiable secret sharing in finite fields to the case of bilinear groups. And hence our schemes can be applied in safeguarding the secret keys of some pairing based cryptosystems, distributed key generation for cryptosystems with secret keys in some bilinear groups and public keys in the range groups of the corresponding bilinear pairings.

References

Baek, J. and Zheng, Y. (2004) 'Identity-based threshold signature scheme from the bilinear pairings' *Information Technology: Coding and Computing*, pp. 124–128.

Baek, J. and Zheng, Y. (2004) 'Identity-Based Threshold Decryption', *Lecture Notes in Computer Science*, Vol. 2947, pp. 262–276.

Blakley, G.R. and Kabatianskii, G.A. (1994) 'Linear algebra approach to secret sharing schemes', *Computer Science*, Vol. 829, pp. 33–40.

Boneh, D. and Boyen, X. (2004) 'Short Signatures Without Random Oracles', *Advances in Cryptology-EUROCRYPT, lecture notes in Computer Science*, Vol. 3027, pp. 56–73.

Boneh, D. and Franklin, M. (2001) 'Identity-based encryption from the weil pairing', *Advances in CRYPTO*, Vol. 2139, pp. 213–229.

Chor, B., Goldwasser, S., Micall, S. and Awerbuch, B. (1985) 'Verifiable secret sharing and achieving simultaneity in the presence of faults' *the 26th FOCS*.

Feldman, P. (1987) 'A practical scheme for non-interactive verifiable secret sharing', *The 28th IEEE Symposium on the Foundations of Computer Science*, pp. 427–437.

Gennaro, R. (1996) 'Theory and practice of verifiable secret sharing', *Ph.D.Thesis, MIT*, pp. 51–107.

Gentry, C. (2006) 'Practical identity-based encryption without random oracles' *In Advances in Cryptology-EUROCRYPT 2006, lecture notes in Computer Science*, Vol. 4004, pp. 445–464.

Kiltz, E. and Pietrzak, K. (2010) 'Leakage resilient ElGamal encryption', *ASIACRYPT*, Vol. 6477, pp. 595–612.

Pedersen, T. (1991) 'Non-interactive and information-theoretic secure verifiable secret sharing', *Cryptology-Crypto'91*, pp. 129–140.

Rabin, T., Ben-Or, M. (1989) 'Verifiable secret sharing and multiparty protocols with honest majority', *the twenty-first annual ACM symposium on Theory of computing*, pp. 73–85.

Shamir, A. (1979) 'How to share a secret', *Comm.ACM 22*, pp. 612–613.

Wu, T.Y. and Tseng,Y.M. (2011) 'A paring-based publicly verifiable secret sharing scheme', *Systems Science and Complexity*, Vol. 24, pp.186–194.

Zhang, F., Zhang, F. and Wang, Y. (2002) 'A secure and efficient general VSS protocol' *Software*, Vol. 13, pp 1187–1192.