Chinese Journal of Electronics
Vol.23, No.1, Jan. 2014

Efficient and Information-Theoretical Secure Verifiable Secret Sharing over Bilinear Groups*

ZHANG Futai[1,2] and ZHANG Jie[1]

(1.*School of Computer Science and Technology, Nanjing Normal University, Nanjing 210023, China*)

(2.*Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing 210097, China*)

Abstract — Verifiable secret sharing (VSS) is an important technique which has been used as a basic tool in distributed cryptosystems, secure multi-party computations, as well as safe guarding some confidential information such as cryptographic keys. By now, some secure and efficient non-interactive VSS schemes for sharing secrets in a finite field have been available. In this paper, we investigate verifiably sharing of a secret that is an element of a bilinear group. We present an efficient and information-theoretical secure VSS scheme for sharing such a secret which may be a private key for a pairing based cryptosystem. Our performance and security analysis indicates that the newly proposed scheme is more efficient and practical while enjoys the same level of security compared with similar protocols available. We also demonstrate two typical applications of our proposed VSS scheme. One is the sharing of a secret key of Boneh and Franklin's identity-based encryption scheme, and the other is the sharing or the distributed generation of a secret key of the leakage resilient bilinear ElGamal encryption scheme.

Key words — Verifiable secret sharing, Threshold, Bilinear map, Bilinear group, Information-theoretical secure.

I. Introduction

Secret sharing[1] is a fundamental tool of threshold cryptography and distributed computing[2−4]. A secret sharing scheme involves a dealer D and a set P of participants. It allows the dealer D to distribute shares of a secret among participants of P in such a way that only some qualified subsets of P can reconstruct the secret from their shares. Earlier basic secret sharing schemes assume both the dealer and the participants are honest. However this assumption may not be sound in some real applications. In practice, a dealer may not trust some participants, and some of the participants may not trust the dealer either. To solve this kind of distrust, Verifiable secret sharing (VSS)[5] is introduced. In a VSS scheme, participants are able to verify whether the shares distributed to them by the dealer are valid. VSS schemes for sharing secrets in a finite field have been well established and widely used. The first non-interactive verifiable secret sharing scheme was presented by Feldman in Ref.[6]. In Ref.[7] Pedersen presented the first non-interactive and information-theoretic secure VSS scheme. These two VSS schemes for sharing secrets in a finite field are generally known as Feldman-VSS and Pedersen-VSS respectively. They have been used as basic building blocks in distributed key generation and threshold cryptosystems based on the discrete logarithm problem in finite fields. Recently, the bilinear pairing-based cryptography has received much attention from the research community and many bilinear pairing-based cryptographic schemes and protocols[8−17] have been available. For some of these bilinear pairing-based cryptographic schemes, the secret keys may come from a bilinear group rather than a finite field. To share such secret keys, we have to consider verifiably sharing an element of a bilinear group. A notable work in this line was presented by J. Baek and Y. Zheng. In Ref.[9], they showed two secure verifiable secret sharing schemes for sharing secrets in bilinear groups as building blocks of their expected ID-based threshold signature scheme. As the algebraic properties of groups are very different from that of finite fields, we think it is not trivial to generalize the verifiable secret sharing schemes over finite field to secure verifiable secret sharing schemes over bilinear groups. In this paper, we focus on establishing efficient and information-theoretic secure verifiable secret sharing schemes over bilinear groups. We demonstrate such a new VSS scheme. The newly proposed scheme is more efficient compared with J. Baek and Y. Zheng's Unconditionally secure verifiable secret sharing scheme based on the bilinear pairing (UVSSBP)[9]. Therefore, it is quite reasonable to believe that our scheme will have practical applications in threshold cryptosystem such as threshold decryption and threshold signature based on bilinear groups.

II. Preliminaries and Definitions

In this section, we briefly describe the concept of bilinear pairings and the notion of verifiable secret sharing.

1. Bilinear pairings

Let G_1 and G_2 be two groups with the same order q, where q is a large prime. Here, we denote the operation in G_1 addi-

*Manuscript Received Jan. 2013; Accepted Apr. 2013. This work is supported by the National Natural Science Foundation of China (No.61170298) and Natural Science Fund for Colleges and Universities in Jiangsu Province (No.12KJD520007).

tion, while the operation in G_2 is denoted multiplication. A map $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ is called a bilinear map (or a bilinear pairing) if it satisfies the following three conditions:

(1) Bilinear: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.

(2) Non-degenerate: There exist $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.

(3) Computable: For all $P, Q \in G_1$, there exists an efficient algorithm to compute $\hat{e}(P, Q)$.

We say that a cyclic group G_1 with prime order q is a bilinear group if there exists a group G_2 with the same order q and a bilinear map $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$. For more details about bilinear pairing and bilinear groups, please refer to Refs.[9–17].

2. Modified generalized bilinear inversion problem in $(G_1, G_2, \hat{e})$

Let G_1 and G_2 be two cyclic groups with the same prime order q, and $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ a bilinear pairing. The modified generalized bilinear inversion problem in $(G_1, G_2, \hat{e})$ is: Given a random $\gamma \in G_2$ and a generator P of G_1, compute $W \in G_1$ such that $\hat{e}(W, P) = \gamma$.

3. Verifiable secret sharing

At first, we review some basic notions about verifiable secret sharing including the communication model, the basic components and the security requirements for an information-theoretic secure VSS scheme.

(1) Communication model

The communication model of a verifiable secret sharing scheme is composed of a set of n players $U_1, U_2, \cdots, U_n$ and a dealer D that can be modeled by polynomial-time randomized Turing machines. We suppose they are connected by a complete network of private point-to-point channels. In addition, all the players and the dealer have access to a dedicated broadcast channel[7].

(2) Components of a VSS scheme

A VSS scheme is divided into four phases: initialization, distribution, verification, and reconstruction.

(a) **Initialization** This phase produces necessary parameters of the scheme.

(b) **Distribution** The dealer publishes commitments and distributes shares of the secret to all participants.

(c) **Verification** This phase is executed by the participants to verify whether the shares they received are valid.

(d) **Reconstruction** The participants who intend to recover the secret execute the reconstruction phase together. Actually they need submit their shares and verify the validity of shares supplied by the other participants before reconstruction.

(3) Notions of security

Here we consider a static and strong admissible adversary[7,18]. That means the adversary has determined which participants to corrupt at the start of the protocol, and can corrupt less than participants totally. An information-theoretic secure VSS scheme should satisfy the following requirements.

(a) **Consistency of the shares** The dealer can not pass through verification when he distributes inconsistent shares.

(b) **Privacy of the secret** No information about the secret is revealed to the adversary. This means that: ① The public information does not reveal any information about the secret. ② A static and strong admissible adversary can get no information about the share of any uncorrupted player and the shared secret.

III. Review of Some Information-theoretic Secure VSS Schemes

In this section we review the non-interactive and information-theoretic secure verifiable secret sharing scheme of Pedersen and UVSSBP scheme of J. Baek and Y. Zheng.

1. Pedersen-VSS

(1) Initialization

Assume that p and q are two large primes such that q divides $p-1$. Let G_q be the unique subgroup of Z_p^* of order q, and g, h be two generators of G_q such that nobody knows $\log_g h$. The secret space is $GF(q)$ and the share space is $GF(q)^2$. Let $s \in GF(q)$ be the secret to be shared, n the number of players and t the threshold with the restriction $1 \leq t \leq n < q$.

(2) Distribution

(a) D publishes a commitment to the secret s: $E_0 = E(s, r) = g^s h^r$ for a randomly chosen $r \in Z_q^*$.

(b) D chooses $a_1, \cdots, a_{t-1}$ at random from Z_q and constructs a polynomial $f(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1}$ of degree $t-1$. Compute $s_i = f(i)$.

(c) D chooses $b_1, \cdots, b_{t-1} \in Z_q$ at random and publishes commitments to a_i for $i = 1, \cdots, t-1$: $E_i = E(a_i, b_i) = g^{a_i} h^{b_i}$.

(d) Let $g(x) = r + b_1 x + \cdots + b_{t-1} x^{t-1}$ and set $r_i = g(i)$. D sends (s_i, r_i) secretly to U_i for $i = 1, \cdots, n$.

(3) Algorithm of verification

When U_i has received his share (s_i, r_i) he verifies if

$$E(s_i, r_i) = \prod_{j=0}^{t-1} E_j^{i^j} \quad (1)$$

If the verification fails, the share (s_i, r_i) assigned to U_i is invalid.

(4) Algorithm of reconstruction

Without loss of generality, we suppose $U_1, \cdots, U_t$ be the t players to reconstruct the shared secret. Each U_i broadcasts his share (s_i, r_i) to other cooperators, and every participator can check its validity through Eq.(1). For $i = 1, \cdots, t$, while all (s_i, r_i) have been verified to be valid, every cooperator can reconstruct s by computing

$$s = \sum_{i=1}^{t} s_i \prod_{1 \leq j \leq t, j \neq i} \frac{i}{i-j} \quad (2)$$

2. UVSSBP scheme of J. Baek and Y. Zheng

(1) Initialization

Suppose G_1 and G_2 are two groups with the same order q and $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is a bilinear map. Assume P is a generator of G_1 and H, I are two random elements of G_1 given to D and no party knows a, $b \in Z_q^*$ such that $H = aP$ and $I = bP$. The secret space is G_1^* and the share space is $G_1 \times Z_q$. Let $S \in G_1$ be the secret to be shared. The number of players is n and the threshold is t with the restriction $1 \leq t \leq n < q$.

(2) Distribution

(a) D chooses a random r from Z_q^* and publishes a commitment to S: $E_0 = E(S, r) = \hat{e}(S, P)\hat{e}(H, I)^r$.

(b) D randomly chooses $A_1, \cdots, A_{t-1}$ from G_1^*. Construct $F(x) = S + A_1 x + \cdots + A_{t-1}x^{t-1}$ and compute $S_i = F(i)$ for $i = 1, \cdots, n$.

(c) D chooses $a_1, \cdots, a_{t-1}$ randomly from Z_q^* and constructs a polynomial $f(x) = r + a_1 x + \cdots + a_{t-1}x^{t-1}$. Then compute $r_i = f(i)$ for $i = 1, \cdots, n$.

(d) For $i = 1, \cdots, t-1$, D broadcasts $E_i = E(A_i, a_i) = \hat{e}(A_i, P)\hat{e}(H, I)^{a_i}$ and sends (S_i, r_i) secretly to U_i for $i = 1, \cdots, t-1$.

(3) Verification

When U_i has received his share (S_i, r_i) he verifies if

$$E(S_i, r_i) = \prod_{j=0}^{t-1} E_j^{i^j} \tag{3}$$

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

(4) Algorithm of reconstruction

Without loss of generality, let $U_1, \cdots, U_t$ be the t players to reconstruct the shared secret. Each U_i broadcasts his share (S_i, r_i) to other cooperators, and every participator can check its validity through Eq.(3). For $i = 1, \cdots, t$, while all (S_i, r_i) have been verified to be valid, every cooperator can reconstruct S by computing

$$S = \sum_{i=1}^{t} S_i \prod_{1 \le j \le t, j \ne i} \frac{i}{i-j} \tag{4}$$

IV. Our Scheme

In this section, we present our efficient and information-theoretical secure verifiable secret sharing scheme from bilinear groups. Then we analyze the security of the newly proposed scheme. We prove that our new scheme satisfies the security requirements for information-theoretic secure verifiable secret sharing schemes. At last we discuss the efficiency of performance of our new scheme. We compare the computational cost of our scheme with that of J. Baek and Y. Zheng's UVSSBP scheme.

1. Description of the scheme

(1) Initialization

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups with the same large prime order q, P a generator of G_1 and $\hat{e} : G_1 \times G_1 \to G_2$ a bilinear map. It is required that the discrete logarithm problem is intractable in both G_1 and G_2. Let $\alpha = \hat{e}(P, P)$ be a generator of G_2. Denote by n the number of participants, and t is the threshold. These parameters can be generated cooperatively by the dealer D and all participants. To generate a random $\beta \in G_2$ such that no party knows the discrete logarithm of β with respect to the base α, the dealer and the players cooperate as follows:

(a) For $i = 1, \cdots, n$ each U_i chooses uniformly at random a $\beta_i \in G_2$ and sends it to D.

(b) On receiving all β_i for $i = 1, \cdots, n$, D sets $\beta = \prod_{i=1}^{n} \beta_i$.

(c) D publishes $(n, t, q, G_1, G_2, \hat{e}, P, \alpha, \beta, \beta_1, \beta_2, \cdots, \beta_n)$ as public parameters. The secret space is G_1, and the share space is $G_1 \times Z_q$.

(2) Distribution

(a) To generate a secret S to be shared. D picks an $s \in Z_q^*$ and sets $S = sP$.

(b) D chooses $a_1, \cdots, a_{t-1}, b_0, \cdots, b_{t-1}$ from Z_q^* uniformly at random and defines $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$, $g(x) = b_0 + b_1 x + \cdots + b_{t-1}x^{t-1}$ where $a_0 = s$.

(c) D computes and publishes $E_i = E(a_i, b_i) = \alpha^{a_i}\beta^{b_i}$ for $i = 0, \cdots, t-1$ as the commitments of S and $f(x)$.

(d) D computes $S_i = f(i)P$, $r_i = g(i)$ and sends (S_i, r_i) secretly to U_i for $i = 1, \cdots, n$.

(3) Verification

When U_i has received his share (S_i, r_i) he verifies if

$$\hat{e}(S_i, P)\beta^{r_i} = \prod_{j=0}^{t-1} E_j^{i^j} \tag{5}$$

If the verification fails, the share (S_i, r_i) assigned to U_i is invalid.

(4) Reconstruction

Without loss of generality, suppose $U_1, \cdots, U_t$ are the t participants to reconstruct the shared secret.

(a) Each U_i broadcasts his share S_i to other cooperators, and every participator can check its validity through Eq.(5).

(b) For $i = 1, \cdots, t$, while all S_i have been verified to be valid, every cooperator can reconstruct S by computing

$$S = \sum_{i=1}^{t} S_i \prod_{1 \le j \le t, j \ne i} \frac{i}{i-j} \tag{6}$$

2. Security

We analyze the security of our scheme according to the security notions given in Section II.

(1) Consistency of the shares

The following theorem shows that the dealer cannot pass through verification if he distributes inconsistent shares under the assumption that he cannot find $\log_\alpha \beta$ expect with negligible probability in q.

Theorem 1 Under the assumption that Modified generalized bilinear inversion problem in $(G_1, G_2, \hat{e})$ is intractable and the discrete logarithm of β with respect to base α is unknown, the dealer can not compute an inconsistent share that passes the verification successfully with a non-negligible probability.

Proof Assume that D gives an invalid share (S_i', r_i') to participant U_i and (S_i', r_i') satisfies the verification equation. Then we have

$$\hat{e}(S_i', P)\beta^{r_i'} = \alpha^{f(i)}\beta^{g(i)} \tag{7}$$

and hence

$$\hat{e}(S_i', P) = \alpha^{f(i)}\beta^{g(i)-r_i'} \tag{8}$$

where $f(x)$ and $g(x)$ are the polynomials used by D in the distribution phase, and $s_i' \ne f(i)$, $r_i' \ne g(i)$. Set $\alpha^{f(i)}\beta^{g(i)-r_i'} = \gamma$ where γ is the input of the Modified generalized bilinear inversion problem in $(G_1, G_2, \hat{e})$, then D can output $W = S_i'$. This implies that D can successfully find a solution for an instance of the Modified generalized bilinear inversion problem in $(G_1, G_2, \hat{e})$.

On the other hand, with $S_i' = s_i'P$ and $\hat{e}(P, P) = \alpha$ we get

$$\alpha^{s_i'}\beta^{r_i'} = \alpha^{f(i)}\beta^{g(i)} \tag{9}$$

from Eq.(7). Then we have

$$\alpha^{s_i'-f(i)}=\beta^{g(i)-r_i'} \tag{10}$$

As $s_i'\neq f(i)$, $r_i'\neq g(i)$, D can calculate

$$\log_\alpha\beta=\frac{s_i'-f(i)}{g(i)-r_i'} \tag{11}$$

That means D knows the discrete logarithm of β with respect to base α.

(2) Privacy of the secret

To prove that no information about the secret is revealed to the adversary, we give the following two theorems. The first theorem is very easy to prove and shows that the public commitments do not reveal any usable information about the secret, and the second one implies the privacy of the secret in case there exists a static and strong admissible adversary who corrupts up to $k<t$ players.

Theorem 2 For any $s\in Z_q^*$ and for randomly uniformly chosen $r\in Z_q$, $E(s,r)$ is uniformly distributed in G_2.

Proof As r is an element randomly chosen from Z_q, it is apparent that β^r is uniformly distributed in G_2 since β is a generator of G_2. And consequently $E(s,r)=\alpha^s\beta^r$ is uniformly distributed in G_2.

This theorem shows that $E(s,b_0)$ does not reveal any information about s and consequently the secret $S=sP$. Similarly for $i=1,\cdots,t-1$ each $E(a_i,b_i)$ does not reveal any information about a_i. So the public commitments do not reveal any information about the polynomial $f(x)$.

Theorem 3 With the shares of those corrupted participants, a static and strong admissible adversary can not derive any information about the share kept by any honest participant and consequently no information about the secret S.

Proof From Theorem 2, we learn that the adversary can not get any information about the secret polynomial $f(x)$ given the public commitments. Nevertheless according to the algorithm of distribution, to acquire the share owned by an honest participant, the adversary has no choice but compute $f(x)$ merely using the shares of the corrupted participants. Without loss of generality we suppose that the corrupted players are $U_1,\cdots,U_k$ and $k<t$. The adversary has to compute all coefficients $a_1,\cdots,a_{t-1}$ of $f(x)$ from the following system of equations:

$$\begin{cases} a_0P+a_1P+\cdots+a_{t-1}P=S_1\\ a_0P+a_12P+\cdots+a_{t-1}2^{t-1}P=S_2\\ \qquad\vdots\\ a_0P+a_1kP+\cdots+a_{t-1}k^{t-1}P=S_k\end{cases} \tag{12}$$

i.e.

$$\begin{bmatrix} P & P & \cdots & P\\ P & 2P & \cdots & 2^{t-1}P\\ \vdots & \vdots & \ddots & \vdots\\ P & kP & \cdots & k^{t-1}P\end{bmatrix}\begin{bmatrix} a_0\\ a_1\\ \vdots\\ a_{t-1}\end{bmatrix}=\begin{bmatrix} S_1\\ S_2\\ \vdots\\ S_k\end{bmatrix} \tag{13}$$

Let $S_i=c_iP$, the above system of equations is equivalent to

$$\begin{bmatrix} 1 & 1 & \cdots & 1\\ 1 & 2 & \cdots & 2^{t-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & k & \cdots & k^{t-1}\end{bmatrix}\begin{bmatrix} a_0\\ a_1\\ \vdots\\ a_{t-1}\end{bmatrix}P=\begin{bmatrix} c_1\\ c_2\\ \vdots\\ c_k\end{bmatrix}P \tag{14}$$

i.e.

$$\begin{bmatrix} 1 & 1 & \cdots & 1\\ 1 & 2 & \cdots & 2^{t-1}\\ \vdots & \vdots & & \vdots\\ 1 & k & \cdots & k^{t-1}\end{bmatrix}\begin{bmatrix} a_0\\ a_1\\ \vdots\\ a_{t-1}\end{bmatrix}=\begin{bmatrix} c_1\\ c_2\\ \vdots\\ c_k\end{bmatrix} \tag{15}$$

This is a system of linear equations where the rank of the coefficient matrix is less than the number of variables. That means it has not less than q^{t-k} solutions and the probability for the adversary to dope out the genuine $(a_0,\cdots,a_{t-1})$ is not more than $1/q^{t-k}$. Accordingly the probability for the adversary to calculate the correct share of any uncorrupted player is not more than $1/q^{t-k}$. As q is a large primer and $t-k\geq 1$, this probability is negligible. Hence, the adversary who corrupts up to $t-1$ participants gets no information about the shared secret.

The three theorems above show that in our scheme the consistency of the shares depends on a computational assumption while the privacy of the secret is unconditional. This means our scheme is information-theoretical secure.

3. Computational cost

To compare the computational cost of the newly proposed scheme with that of J. Baek and Y. Zheng's scheme, we count the number of those time-consuming operations in different phases of both schemes and list them in Table 1. We use **P**, **S** and **E** to denote the operation of a bilinear pairing, a scalar multiplication in G_1 and an exponentiation in G_2 respectively.

As in J. Baek and Y. Zheng's UVSSBP the initialization algorithm does not give definite procedures of generating the parameters, we just consider the distribution phase, verification phase and reconstruction phase in this table. And in the reconstruction phase we assume there are t participants and the cost of verification is not included as it is the same in the two schemes.

Table 1. Comparison of computational cost

	UVSSBP	Our new scheme
Distribution phase	$t\mathbf{P}+(t-1)n\mathbf{S}+t\mathbf{E}$	$(n+1)\mathbf{S}+2t\mathbf{E}$
Verification phase	$t\mathbf{P}+n(t+1)\mathbf{E}$	$t\mathbf{P}+n(t+1)\mathbf{E}$
Reconstruction phase	$t\mathbf{S}$	$t\mathbf{S}$

The comparison reveals that in our scheme, the operations of computing bilinear pairing and scalar multiplication in G_1 are greatly reduced, although exponentiation in G_2 increases. As computing bilinear pairings is the most time-consuming operation, it is quite reasonable to say that our newly proposed scheme has a lower computational cost than J. Baek and Y. Zheng's UVSSBP. As the communication cost is the same in the two schemes, our scheme is more efficient under the same level of security.

V. Applications

Our information theoretic secret sharing scheme over bilinear groups has wide applications especially in the case where the secret S to be shared is in a bilinear group G_1 and the discrete logarithm of S to a given generator P of G_1 is known to the dealer. Here, we give two typical examples.

The first one is to share a secret key of the identity-based cryptosystem of Boneh and Franklin[12] employing the Private key generation center (PKG) as a dealer. This is a preferable choice for sharing the secret key of an identity for threshold realization of decryption or signature in Boneh and Franklin's identity-based setting. For an identity ID, the secret key for ID can be computed by the PKG as $d_{ID} = sH(ID)$, where s is the master secret key only known to the PKG. When asked to share the secret key of identity ID in a set of n designated participants with threshold t, the PKG can play the role of the dealer and shares d_{ID} using our sharing scheme. Having shared the secret key $d_{ID} = sH(ID)$ of identity ID, t or more than t participants can cooperate to decrypt ciphertexts or sign messages on behalf of identity ID using threshold decryption or signature techniques.

The second is the sharing or distributed generation of a user's secret key in the bilinear ElGamal encryption scheme[11] which has been proved leakage resilient. This is necessary for safe guarding the secret key or for the purpose of threshold decryption. In the bilinear ElGamal encryption scheme, a user picks uniformly at random an $x \in Z_q^*$, and sets its secret key as $SK = xP$, public key as $PK = \hat{e}(P, P)^x$. So, our sharing scheme can directly be used to sharing such a secret key. To distributed generate such a secret key, the n participants $P_1, P_2, \cdots, P_n$ can execute in a parallel manner our sharing scheme n times with the same threshold t. Each P_i acts as a dealer once and shares its random choice of x_iP. At last, the generated secret key is the sum of all those correctly shared x_iP, and has been shared by the n participants with threshold t. An attacker corrupts up to $t-1$ participants can get no information about the shared secret key, while the public key can be computed by each participant.

VI. Conclusions

We concentrate on verifiably sharing a secret from a bilinear group. An efficient and information-theoretic secure scheme for sharing such a secret has been presented. The new scheme is more efficient compared with J. Baek and Y. Zheng's UVSSBP scheme while enjoys the same level of security. Similar to Feldman VSS, Pedersen VSS, and the UVSSBP scheme of J. Baek and Y. Zheng, our scheme is also homomorphic. This property makes it easy to convert our scheme into a proactive verifiable secret sharing scheme and also makes our scheme applicable to a number of real application environments. Thus it is quite reasonable to believe that our scheme will have wide applications in multi-party computation in bilinear groups, distributed key generation and threshold cryptosystems based on bilinear groups.

References

[1] A. Shamir, "How to share a secret", *Communications of the ACM*, Vol.22, No.11, pp.612–613, 1979.

[2] R. Gennaro, S. Jarecki, H. Krawczyk, *et al.*, "Secure distributed key generation for discrete-log based cryptosystems", *Journal of Cryptology*, Vol.20, No.1, pp.51–83, 2007.

[3] R. Gennaro, S. Jarecki, H. Krawczyk, *et al.*, "Revisiting the distributed key generation for discrete-log based Cryptosystems", in *RSA-CT '03, LNCS. 2612* (G Goos *et al.* eds), Springer-Verlag, pp.373–390, 2003.

[4] R. Gennaro, S. Jarecki, H. Krawczyk, *et al.*, "Robust threshold DSS signatures", *Information and Computation*, Vol.164, No.1, pp.54–84, 2001.

[5] B. Chor, S. Goldwasser, S. Micall, *et al.*, "Verifiable secret sharing and achieving simultaneity in the presence of faults", *Proceeding of 26th FOCS* (Manuel Blum *et al.* eds), pp.383–395, 1985.

[6] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", *Proceeding of the 28th IEEE Symposium on the Foundations of Computer Science* (Laszlo Babai *et al.* eds), pp.427–437, 1987.

[7] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing", *Cryptology-Crypto'91* (Santa Barbara), *LNCS 576* (Joan Feigenbaum ed), pp.129–140, 1992.

[8] J. Baek, Y. Zheng, "Identity-Based Threshold Decryption", *in International Workshop on Public Key Cryptography, LNCS 2947*, F. Bao *et al.* (Eds.), pp.262–276, 2004.

[9] J. Baek, Y. Zheng, "Identity-based threshold signature scheme from the bilinear pairings", *Proceedings of the International Conference on Information and Technology: Coding and Computing* (Shahram Latifi *et al.* eds), Las Vegas, pp.124–128, 2004.

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

[11] E. Kiltz, K. Pietrzak, "Leakage resilient ElGamal encryption. ASIACRYPT", *LNCS 6477* (M Abe ed), Singapore, pp.595–612, 2010.

[12] D. Boneh, M. Franklin, "Identity-based encryption from the weil pairing", *SIAM J. Computing*, Vol.32, No.3, pp.586–615, 2003.

[13] C. Gentry, "Practical identity-based encryption without random oracles", in *Advances in Cryptology-EUROCRYPT 2006, LNCS 4004* (Serge Vaudenay ed.), St. Petersburg, pp.445–464, 2006.

[14] D. Boneh, Xavier Boyen, "Short Signatures Without Random Oracles", *Advances in Cryptology-EUROCRYPT 2004, LNCS 4004* (Christian Cachin, Jan L. Camenisch eds.), Interlaken, pp.56–73, 2004.

[15] J. Xu, Z. Zhang, D. Feng, "Identity based threshold proxy signature", *Chinese Journal of Electronics*, Vol.15, No.1, pp.183, 2006.

[16] L. Zhang, F. Zhang, X. Huang, "A secure and efficient certificateless signature scheme using bilinear pairing", *Chinese Journal of Electronics*, Vol.18, No.1, pp.145–148, 2009.

[17] Y. Sun, H. Li, "ID-based signcryption KEM to multiple recipients", *Chinese Journal of Electronics*, Vol.20, No.2, pp.317–322, 2011.

[18] R. Gennaro, "Theory and practice of verifiable secret sharing", *Ph.D.Thesis, MIT*, pp.51–107, 1996.

ZHANG Futai was born in Shaanxi Province in 1965. He received his Ph.D. degree in Cryptography from Xidian University in 2001. He is now a professor and Ph.D. supervisor of Nanjing Normal University. His research interests include cryptography and information security. (Email: zhangfutai@njnu.edu.cn)

ZHANG Jie was born in Shandong Province in 1986. She graduated from the Department of Computer Science and Technology, Dezhou University in 2010. Now she is a M.E. candidate in the School of Computer Science and Technology, Nanjing Normal University, Nanjing, China. Her research interests are secret sharing and bilinear pairing based cryptography.