# Efficient Verifiable Secret Sharing Scheme over Bilinear Groups

[1]Jie Zhang, [2]Futai Zhang
[1, First Author]*School of Computer Science and Technology, Nanjing Normal University, P.R. China, 464516929@qq.com*
[*2,Corresponding Author] *School of Computer Science and Technology, Nanjing Normal University, P.R. China, zhangfutai@njnu.edu.cn*

## *Abstract*

*A verifiable secret sharing (VSS) scheme is a secret sharing scheme with the special property that every player is able to verify whether the share distributed to him by a dealer is correct. VSS is a fundamental tool of cryptography and distributed computing. VSS schemes for sharing an element in a finite field have been well established for many years. In this paper, we focus on verifiably sharing of a secret that is an element of a bilinear group. Such VSS schemes are necessary for sharing the secret keys of many bilinear pairing-based cryptosystems which have been a hot topic in cryptographic research in recent years. We introduce strict security definitions for such a noninteractive VSS scheme. Then we come up with an efficient VSS scheme for sharing a secret in a bilinear group. Compared with similar protocols available, the newly proposed scheme is more efficient while enjoys the same level of security.*

**Keywords***: secret sharing, verifiable secret sharing, bilinear group, discrete logarithm*

## 1. Introduction

A secret sharing scheme [1] is a method of distributing shares of a secret among a set *P* of participants in such a way that only qualified subsets of *P* can reconstruct the secret from their shares. A verifiable secret sharing (VSS) [2-3]scheme is a secret sharing scheme with the special property that every player is able to verify whether the share distributed to him by a dealer is correct. VSS is a fundamental tool of cryptography and distributed computing [4-6]. Since the introduction of the first non-interactive verifiable secret sharing scheme by Feldman in [7] that is usually known as Feldman-VSS, non-interactive VSS schemes for sharing secrets in a finite field have been well established and widely used.

Recently, the bilinear pairing-based cryptography has received much attention from the research community. By now, many bilinear pairing-based cryptographic schemes and protocols [8-12] have been available. In [8], for the first time, J.Baek and Y.Zheng showed a computationally secure verifiable secret sharing scheme based on the bilinear groups (CVSSBP). Their proposed CVSSBP scheme has been widely used as building blocks in many threshold cryptosystems from the bilinear pairings [13-17].

As in many pairing-based cryptosystems, the secret keys are random elements in some bilinear groups, it is of great importance to investigate the verifiably sharing of such secrets, as well as the distributed generation of such secret keys. We think it is not trivial to generalize the verifiable secret sharing schemes in finite field to secure verifiable secret sharing schemes in bilinear groups since the algebraic properties of groups are very different from that of finite fields. In this paper, we focus on this problem. We demonstrate a new efficient VSS scheme for sharing secrets in bilinear groups. We consider the security notion and gave rigorous proof to our scheme. The newly proposed scheme is more efficient compared with J.Baek and Y.Zheng's CVSSBP scheme. Therefore, it is quite reasonable to believe that our scheme will play a critical role in the threshold cryptosystem such as threshold decryption and threshold signature etc..

The rest of the paper is organized as follows. In **Section 2** we briefly describe the concept of bilinear map, the definition of discrete logarithm problem(DLP) and some related notions of a VSS scheme including the communication model and the definition of security. After that we review the bilinear group-based verifiable secret sharing scheme of J.Baek and Y.Zheng in **Section 3**. In **Section 4** we present our efficient VSS scheme from bilinear groups and analyze its security and efficiency. The

applications of our VSS scheme are discussed in **Section 5**. Finally, in **Section 6** we just conclude this paper.

## 2. Preliminaries and Definitions

In this section, we briefly describe the concepts of bilinear pairings, the definition of discrete logarithm problem and some useful knowledge of verifiable secret sharing.

### 2.1. Bilinear Pairings

Let $G_1$ and $G_2$ be two groups with the same order $q$, where $q$ is a large prime. Here, we assume that $G_1$ is an additive cyclic group, and $G_2$ is a multiplicative cyclic group. In particular, $G_1$ is a subgroup of the group of points on an elliptic curve over a finite field $E(F_p)$, and $G_2$ is a subgroup of the multiplicative group over a finite field. A map $\hat{e}: G_1 \times G_1 \to G_2$ is called a bilinear map if it satisfies the following three conditions:

- Bilinear: For all $P,Q \in G_1$ and $a,b \in Z_q^*$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$.
- Non-degenerate: There exist $P,Q \in G_1$ such that $\hat{e}(P,Q) \neq 1$.
- Computable: For all $P,Q \in G_1$, there exists an efficient algorithm to compute $\hat{e}(P,Q)$.

### 2.2. Definition of Discrete Logarithm Problem(DLP)

**Definition 1.** Assume $G$ is a cyclic group generated by $g$. Let $h$ be an element from $G$. The discrete logarithm problem in $G$ is:

- Given $G, g, h$, compute $a$ such that $h = g^a$.

### 2.3. Verifiable Secret Sharing

Secret sharing is a way of distributing information to a set of processors such that a quorum of processors is needed to access the information. A verifiable secret sharing scheme is a secret sharing scheme with the special property that every player is able to verify whether the share distributed to him is correct. The basic procedure of a VSS scheme is more or less the same with secret sharing scheme expect an additional verification phase between the original distribution phase and reconstruction phase, which can be easily realized with the public commitments of some secret information during the distribution step.

Here we give the notion of communication model and the requirement of security for a VSS scheme.

- **Communication model:**
  The communication model of a verifiable secret sharing scheme is composed of a set of $n$ players $U_1, U_2, \ldots, U_n$ and a dealer $D$ that can be modelled by polynomial-time randomized Turing machines. They are connected by a complete network of private (i.e. untappable) point-to-point channels. In addition, all the players and the dealer have access to a dedicated broadcast channel.
- **Notions of security:**
  Consider a static and strong admissible adversary [18]. That means the adversary has determined which players to corrupt before the protocol being implemented, and can corrupt less than $t$ players totally. We consider the security of a VSS scheme from the following aspects[19]:
  - The dealer can not pass through verification when he distributes inconsistent shares (i.e. consistency of the shares).

- No useful information about the secret is revealed (i.e. privacy of the secret). It involves two aspect as following:
  1) The public information does not reveal any useful information about the secret and the shares.
  2) A static and strong admissible adversary can not derive the share of any uncorrupted player and consequently the secret.

## 3. Available Scheme

In this section we just review the first non-interactive verifiable secret sharing scheme of Feldman and the bilinear group-based one of J.Beak and Y.Zheng.

### 3.1. Feldman-VSS

#### 3.1.1. Parameters

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 $g$ is a generator of $G_q$. The discrete logarithm problem is intractable in $G_q$. Both the secret space and the share space are the finite field $GF(q)$. Let $s \in GF(q)$ be the secret to be shared. The number of players is $n$ and the threshold is $t$ with the restriction $1 \le t \le n < q$.

#### 3.1.2. Algorithm of sharing

$D$ chooses $a_1,\ldots,a_{t-1}$ from $G_q$. Let $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ where $a_0 = s$.

$D$ computes and publishes $C_i = g^{a_i}$ for $i = 0,\cdots,t-1$ as the commitments of $s$ and $f(x)$.

$D$ computes the share $s_i = f(i) \bmod q$ and sends it secretly to $U_i$ for $i = 1,\cdots,n$.

#### 3.1.3. Algorithm of verification

When $U_i$ has received his share $s_i$ he verifies if

$$g^{s_i} = \prod_{j=0}^{t-1} C_j^{\,i^j} \qquad (1).$$

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

#### 3.1.4. Algorithm of reconstruction

Without loss of generality, we suppose $U_1, U_2, \ldots, U_t$ be the $t$ players to reconstruct the shared secret. Each $U_i$ broadcasts his share $s_i$ to other cooperators, and every participator can check its validity through **Eq.1**. For $i = 1,\cdots,t$, while all $s_i$ have been verified to be valid, every cooperator can reconstruct s by computing

$$s = \sum_{i=1}^{t} s_i \prod_{1 \le j \le t, j \ne i} \frac{i}{i-j}.$$

### 3.2. J.Beak and Y.Zheng's scheme

#### 3.2.1. Parameters

Suppose $G_1$ and $G_2$ are two groups with the same order $q$ and $\hat{e}:G_1\times G_1\to G_2$ is a bilinear map as we defined previously in **Section 2**. Assume that $P$ is a generator of $G_1$ such that nobody knows the discrete logarithm to the base $\hat{e}(P,P)$. Both the secret space and the share space are $G_1$. 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 $1\le t\le n<q$.

#### 3.2.2. Algorithm of sharing

$D$ chooses $A_1,\ldots,A_{t-1}$ from $G_1$. Let $F(x)=A_0+A_1x+\cdots+A_{t-1}x^{t-1}$ where $A_0=S$.

$D$ computes and publishes $C_i=\hat{e}(A_i,P)$ for $i=0,\cdots,t\text{-}1$ as the commitments of $S$ and $F(x)$.

$D$ computes the share $S_i=F(i)\bmod q$ and sends it secretly to $U_i$ for $i=1,\cdots,n$.

#### 3.2.3. Algorithm of verification

When $U_i$ has received his share $S_i$ he verifies if

$$\hat{e}(S_i,P)=\prod_{j=0}^{t-1}C_j{}^{i^j} \quad (2).$$

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

#### 3.2.4. Algorithm of reconstruction

Without loss of generality, we suppose $U_1,U_2,\ldots,U_t$ be the $t$ players to reconstruct the shared secret. Each $U_i$ broadcasts his share $S_i$ to other cooperators, and every participator can check its validity through **Eq.2**. For $i=1,\cdots,t$, while all $S_i$ have been verified to be valid, every cooperator can reconstruct $S$ by computing

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

When $q$ is large enough this scheme satisfies the two demands of security as we defined in **Section 2**, which means their scheme is computational secure. For more details, please refer to [10].

## 4. Our Scheme

In this section, we present our efficient verifiable secret sharing scheme based on bilinear groups. Then we analyze the security of the newly proposed scheme with detailed demonstration. At last we discuss the computational cost and compare our scheme with J.Beak and Y.Zheng's scheme in a table.

### 4.1 Description of the scheme

#### 4.1.1 Parameters

Let $G_1$ and $G_2$ be two groups with the same order $q$ and $\hat{e}:G_1\times G_1\to G_2$ a bilinear map as we defined before. Choose a random generator $P$ from $G_1$ such that nobody knows the discrete logarithm to the base $\hat{e}(P,P)$. Both the secret space and the share space are $G_1$. Suppose the number of players is $n$ and the threshold is $t$ with the restriction $1\le t\le n<q$. The common parameters of this scheme are $\langle G_1,G_2,\hat{e},P,\hat{e}(P,P),t,n\rangle$.

#### 4.1.2 Algorithm of sharing

$D$ chooses $s$ randomly from $Z_q^*$ and sets the secret $S=sP$.

$D$ chooses $a_1,\ldots,a_{t-1}$ from $Z_q^*$ and establishes a polynomial $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$ where $a_0=s$.

$D$ computes and publishes $C_i=\hat{e}(P,P)^{a_i}$ for $i=0,\cdots,t\text{-}1$ as the commitments of $S$ and $f(x)$.

$D$ computes the share $S_i=f(i)P \bmod q$ and sends it secretly to $U_i$ for $i=1,\cdots,n$.

#### 4.1.3 Algorithm of verification

When $U_i$ has received his share $S_i$ he verifies if

$$\hat{e}(S_i,P)=\prod_{j=0}^{t-1}C_j^{\,i^j} \qquad (3).$$

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

#### 4.1.4 Algorithm of reconstruction

Without loss of generality, we suppose $U_1,U_2,\ldots,U_t$ be the $t$ players to reconstruct the shared secret. Each $U_i$ broadcasts his share $S_i$ to other cooperators, and every participator can check its validity through **Eq.3**. For $i=1,\cdots,t$, while all $S_i$ have been verified to be valid, every cooperator can reconstruct $S$ by computing

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

### 4.2 Security

The security of our scheme is based on the intractability to calculate the discrete logarithm on $G_1$ and $G_2$. We analyze our scheme's security from two aspects as we define before in **Section 2**.

#### 4.2.1 Consistency of the shares

The following theorem shows that the dealer can not pass through verification if he distributes inconsistent shares as long as DLP on $G_1$ and $G_2$ is intractable.

**Theorem 1.** The probability for the dealer to compute an inconsistent share for any player that passes the verification successfully is neligible.

***Proof.*** From the properties of admissible bilinear pairing and the intractability of discrete logarithms in group $G_1$ and $G_2$, the share $S_i$ is completely determined by $\hat{e}(S_i,P)$, the coefficient $a_i$ of the polynomial $f(\mathrm{x})$ is uniquely fixed by $C_i$. Hence, the polynomial $f(\mathrm{x})$ is completely defined by $C_0,C_1,...,C_{t\text{-}1}$. Notice that the share $S_i$ for player $U_i$ is valid if and only if $\hat{e}(S_i,P)=\prod_{j=0}^{t-1}C_j{}^{i^j}$. As $\prod_{j=0}^{t-1}C_j{}^{i^j}=\prod_{j=0}^{t\text{-}1}(\hat{e}(P,P)^{a_j})^{i^j}=\hat{e}(P,P)^{\sum_{j=0}^{t\text{-}1}a_j i^j}=\hat{e}(P,P)^{f(i)}$, we have $\hat{e}(S_i,P)=\prod_{j=0}^{t-1}C_j{}^{i^j}$ iff $\hat{e}(S_i,P)=\hat{e}(P,P)^{f(i)}$ iff $\hat{e}(S_i,P)=\hat{e}(f(i)P,P)$ iff $S_i=f(i)P$.

This implies that the probability for the dealer to compute an inconsistent share $S_i'\neq f(i)P$ for any player $U_i$ such that $\hat{e}(S_i',P)=\prod_{j=0}^{t-1}C_j{}^{i^j}$ is negligible.

#### 4.2.2 Privacy of the secret

To show that no useful information about the secret is revealed we give the following two theorems with brief proof. The first one shows that the open commitments do not reveal any useful information about the secret and the shares, and the second one implies the secrecy of the secret while there exists a static and strong admissible adversary who corrupts up to $k$ players, where $k<t$.

**Theorem 2.** Under the difficulty of calculating discrete logarithm in $G_1$ and $G_2$, the adversary can not get any useful information about the secret $S$ and the share possessed by any players from the public information, i.e. the commitments of the secret $S$ and the polynomial $f(x)$ do not reveal any useful information about the secret and the shares.

***Proof.*** The public commitments are $C_i=\hat{e}(P,P)^{a_i}$ for $i=0,\cdots,t\text{-}1$. As computing the discrete logarithm to the base $\hat{e}(P,P)$ is difficult in $G_2$, the adversary can not derive any useful information about $S$ and $f(x)$ from the public commitments.

Secondly, according to the algorithm of distribution the share $S_i$ for each $U_i(i=1,...,n)$ satisfies: $S_i=f(i)P$. Thus without knowing $f(x)$ it is intractable to obtain any useful information about $S_i$.

**Theorem 3.** With the shares of those corrupted participants, a static and strong admissible adversary can not derive the share kept by any other honest one and consequently the secret $S$.

***Proof.*** We learn that the adversary can not get any useful information about the secret polynomial $f(x)$ from Theorem 2. Nevertheless according to the algorithm of distribution, to acquire the shares of those honest players, the adversary has no choice but compute $f(x)$ merely using the shares of the corrupted ones. Without loss of generality we suppose that the corrupted players are $U_1,U_2,\ldots,U_{\mathrm{k}}$ and $k<t$. The adversary has to compute all coefficients of $f(x)$ from the following system of equations :

$$\begin{cases} a_0P+a_1P+\cdots+a_{t-1}P=S_1 \\ a_0P+a_1 2P+\cdots a_{t-1}2^{t-1}P=S_2 \\ \qquad\qquad\qquad\qquad\vdots \\ a_0P+a_1kP+\cdots a_{t-1}k^{t-1}P=S_k \end{cases},$$

i.e.

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

Let $S_i = b_i P$, the above system of equations equivalent to

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & k & \cdots & k^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} P = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix} P,$$

i.e.

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & k & \cdots & k^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}.$$

This is a system of linear equations where the rank of coefficient matrix is less than the number of variables. That means it has not less than $q^{t-k}$ answers and the probability for the adversary to dope out the genuine $(a_0,...,a_{t-1})$ is not more than $\frac{1}{q^{t-k}}$. Accordingly the probability to calculate the share of any uncorrupted player is not more than $\frac{1}{q^{t-k}}$. As $q$ is a large primer and $t-k \geq 1$, this probability can be ignored.

The above theorems claim that our scheme satisfies the security requirements defined in **Section 2**, and hence the scheme is computationally secure.

### 4.3 Computational Cost

To compare the computational cost of the newly proposed scheme with J.Beak and Y.Zheng's scheme, we count those time-consuming operations in different phases and list them in the following table. Let $T_p$, $T_s$ and $T_e$ denote the operation of bilinear pairing from $G_1$ to $G_2$, scalar multiplication in $G_1$ and exponentiation in $G_2$ respectively. In the reconstruction phase, we assume there are $t$ participants and the cost of verification is not included.

**Table 1.** Computation cost comparison

| Different phase | J.Beak and Y.Zheng's scheme | The newly proposed scheme |
|---|---|---|
| Distribution phase | $tT_p+n(t-1)T_s$ | $nT_s+tT_e$ |
| Verification phase | $nT_p+ntT_e$ | $nT_p+ntT_e$ |
| Reconstruction phase | $tT_s$ | $tT_s$ |

Obviously, although exponentiation in $G_2$ increases in our scheme, we just need compute $n$ bilinear pairings totally and the scalar multiplication in $G_1$ is reduced to 0. As computing bilinear pairings is the most time-consuming operation, it is quite reasonable to say that our newly proposed scheme has a smaller computational cost totally when the common parameters stay the same with

J.Beak and Y.Zheng's scheme. That means our scheme is more efficient under the same level of security.

## 5. Applications of Our Scheme

Our VSS scheme is applicable to share a secret in a bilinear group for which the dealer knows its discrete logarithm with respect to a given basis. Two direct applications of our VSS scheme are threshold realization of some identity based cryptosystems and distributed master key generation for some identity based cryptosystems.

We notice that there are many identity based cryptosystems in which a private key of a user is an element (or elements) of a bilinear group for which the PKG knows its (their) discrete logarithm (logarithms) to a given (publicly known) basis. For threshold realization of these identity based cryptosystems, it is convenient and preferable to choose the PKG as the dealer for sharing a private key of a designated identity. In such a way, no single player will know the complete private key for decrypting or signing. Otherwise, the complete private key for decrypting or signing should be generated by the PKG and is given to a player who is nominated as the dealer. From the view point of security, the latter method is not preferable and may have to resort to a less efficient sharing scheme. Boneh and Franklin's IBE [11], Water's IBE [20], and Hess's IBS [21] are along this class of identity based cryptosystems.

To enhance the security guarantee of the master secret key of an identity based cryptosystem, a good choice is to use distributed PKGs. In this case, it is preferable to let all PKG members generate the master secret key using a distributed key generation protocol. Making use of the similar techniques as in [4], our VSS schem can be turned into distributed master key generation protocol for some identity based cryptosystems such as the ones listed above.

## 6. Conclusions

In this paper we presented an efficient verifiable secret sharing scheme. The new scheme is more efficient compared with J.Baek and Y.Zheng's CVSSBP scheme while enjoys the same level of security. Therefore, it is quite reasonable to believe that our scheme will play a critical role in the threshold cryptosystems such as threshold decryption, threshold signature, and distributed master key generation for some identity based cryptostems, etc..

## Acknowledgement

This work is supported by National Natural Science Foundation of China (No.61170298), Natural Science Foundation of Jiangsu Province (No.BK2011101).

## References

[1] Adi Shamir, “How to share a secret”, Communications of the ACM, vol. 22, no. 11, pp.612-613, 1979.

[2] Benny Chor, Shafi Goldwasser, Silvio Micali, Baruch Awerbuch, “Verifiable secret sharing and achieving simultaneity in the presence of faults”, In Proceeding of the 26th Annual Symposium on Foundations of Computer Science, pp.383-395, 1985.

[3] Changlu Lin, Lein Harn, “Unconditionally Secure Verifiable Secret Sharing Scheme”, AISS: Advances in Information Sciences and Service Sciences, Vol. 4, No. 17, pp.514-518, 2012.

[4] Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, Tal Rabin, “Secure distributed key generation for discrete-log based cryptosystems”, In Proceeding of Eurocrypt'99, pp.295-310, 1999.

[5] Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, Tal Rabin, “Revisiting the distributed key generation for discrete-log based Cryptosystems”, In Proceeding of RSA Security'03, 2003.

[6] Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, Tal Rabin, "Robust threshold DSS signatures", In Proceeding of the 15th annual international conference on theory and application of cryptographic techniques, pp.354-371, 1996.
[7] Paul Feldman, "A practical scheme for non-interactive verifiable secret sharing", In Proceeding of the 28th IEEE Symposium on the Foundations of Computer Science, pp.427-437, 1987.
[8] Joonsang Baek, Yuliang Zheng, "Identity-based threshold signature scheme from the bilinear pairings", In Proceeding of the international Conference on Information and Technology: Coding and Computing, 2004.
[9] Tsu-Yang Wu, Yuh-Min Tseng, "A paring-based publicly verifiable secret sharing scheme", Systems Science and Complexity, vol. 24, no. 1, pp.186-194, 2011.
[10] Eike Kiltz, Krzysztof Pietrzak, "Leakage resilient elGamal encryption", ASIACRYPT, pp.595-612, 2010.
[11] D.Boneh, M.Franklin, "Identity-based encryption from the weil pairing", SIAM J. of Computing, vol. 32, no. 3, pp.586-615, 2003
[12] Craig Gentry, "Practical identity-based encryption without random oracles", In Proceeding of Cryptology-EUROCRYPT 2006, 2006.
[13] Hong Yuan, Futai Zhang, Xinyi Huang, Yi Mu, Willy Susilo, Lei Zhang, "Certificateless threshold signature scheme from bilinear maps", Information Sciences, vol. 180, no. 23, pp.4714-4728, 2010.
[14] Hong Sun, Li Guo, Aimin Wang "A forward secure threshold signature scheme based on bilinear pairing", In Proceeding of Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference, 2010.
[15] Dianjun Lu, Bingru Zhang, Haixing Zhao, Xinyan Li, "A threshold proxy signature scheme from bilinear pairings", In Proceeding of Wireless Communications, Networking and Mobile Computing, 5th International Conference, 2009.
[16] Xiaofeng Cheng, Fangguo Zhang, Divyan M.Konidala, Kwangjo Kim, "New ID-based threshold signature scheme from bilinear pairings", In Proceeding of Indocrypt, pp.371-383, 2004.
[17] Yongxuan Sang, Jiwen Zeng, Zhongwen Li, Lin You, "A Secret Sharing Scheme with General Access Structures and its Applications", IJACT: International Journal of Advancements in Computing Technology, Vol. 3, No. 4, pp.121-128, 2011
[18] Rosario Gennaro, "Theory and practice of verifiable secret sharing", [Ph.D.Thesis], MIT, pp.51-107, 1996
[19] Torben Pryds Pedesen, "Non-interactive and information-theoretic secure verifiable secret sharing", Computer Science, vol.576, pp.129-140, 1992.
[20] Brent Waters, "Efficient identity-based encryption without random oracles", In Proceeding of Cryptology-EUROCRYPT 2005, pp.114-127, 2005.
[21] Florian Hess, "Efficient identity based signaure schemes bases on pairings", Computer Science, vol. 2595, pp.310-324, 2003.