2013 5th International Conference on Intelligent Networking and Collaborative Systems

Secure Distributed Key Generation on Vector Space Access Structures in Bilinear Groups

Jie Zhang
School of Computer Science and Technology
Nanjing Normal University
Nanjing, China
Email: 464516929@qq.com

Futai Zhang
School of Computer Science and Technology
Nanjing Normal University
Jiangsu engineering research center on information
security and privacy protection Technology
Nanjing, China
Email: zhangfutai@njnu.edu.cn

***Abstract*—Distributed key generation is a method for a set of players to generate a pair of public key and private key together, such that the public key is output publicly while the private key is distributed among the players by a secret sharing method. Secure distributed key generation in finite field for discrete-log based cryptosystems has been studied for many year and many protocols have been proposed and widely used in threshold cryptosystems and distributed cryptographic computing. In this paper we focus on secure distributed key generation in bilinear groups and propose such protocol on vector space access structures. The new proposed distributed key generation protocol is secure and has a wide application. We give detailed proof for its security.**

***Keywords*-distributed key generation; vector space access structure; bilinear groups; discrete logarithm; cloud computing security;**

I. Introduction

Distributed key generation(DKG for short) [1], [2] is an essential component of threshold cryptosystem [3], [4], [5] and distributed cryptographic computing. It is mainly used to generate a pair of public key and private key for a cryptosystem by the players together in such a way that the public key is output in the clear while the private key is shared by the players via a secret sharing [6] method.

The first distributed key generation protocol is introduced by T.Pedersen in [7], and it is proofed to be insecure in [1]. R.Gennaro *et al.* specially studied distribute key generation for discrete-log based cryptosystems in [1], [2] and showed a method to establish such secure DKG protocol. Their DKG protocol is for threshold access structure and has been widely used in many threshold cryptosystems. As threshold access structure demands every player an identical power and position, DKG protocol on threshold access structure has some restrictions in practice consequently. For this problem F.Zhang *et al.* studied secure distributed key generation on non-threshold access structure in detail. They proposed a DKG protocol based on vector space access structure in [8] and a DKG protocol based on generalized verifiable secret sharing in [9]. By then, distributed key generation for generating a pair of keys that are elements of finite field, either on threshold access structure or on non-threshold access structure, has been well established.

Recently, pairing-based cryptography has received much attention from cryptographic researchers and many schemes have been proposed [10], [11], [12], [13], [14], [15], [16]. In most pairing-based threshold cryptosystems, the pair of public key and private key are elements from bilinear groups, thus distributed key generation protocol in bilinear groups is an essential component of such cryptosystem. J.Baek and Y.Zheng focused on this topic and proposed such distributed key generation protocol in [17] as a building block of their identity-based threshold signature scheme. Their DKG protocol is for threshold access structure and bilinear group based DKG protocol on non-threshold access structure has not been studied yet.

In this paper we focus on distributed key generation on vector space access structure for generating a pair of keys that are elements of bilinear groups. We propose such protocol and specially discuss its security from two aspects: correctness and secrecy. The new proposed protocol has a wide application in practice.

The rest of the paper is organized as follows. In Section 2 we mainly review the concepts of bilinear pairings, access structure and secure DKG. Then in Section 3 we show the building blocks of our DKG protocol. In Section 4 we give our secure distributed key generation protocol with vector space access structure in bilinear groups in detail. We also specially analyze its security from correctness and secrecy. At last in Section 5 we just conclude this paper.

II. Preliminaries and Definitions

In this section, we briefly review the concepts of bilinear pairings and access structure. Besides we consider two operations on vector space which will be used in the following sections.

A. 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

978-0-7695-4988-0/13 $26.00 © 2013 IEEE
DOI 10.1109/INCoS.2013.153

an additive cyclic group, and G_2 is a multiplicative cyclic group. A map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$ is called a bilinear map 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 G_1 is a bilinear group if there exists a group G_2 and a bilinear map $\hat{e} : G \times G_1 \longrightarrow G_2$ as above, where $\hat{e}$ and the group action in G_1 and G_2 can be computed efficiently.

B. Access Structure

Assume D is the dealer who holds a secret to distribute among a set of n participants $H = \{H_1, ..., H_n\}$. An access structure Γ on H specifies a family of qualified subsets that can reconstruct the shared secret. We denote by $\Gamma_0 = \{A_1, ..., A_t\}$ the basis of Γ, that is the set of minimal elements of Γ under inclusion. Here we briefly describe the notion of the most common threshold access structure and the more general vector space one which actually involves the threshold one.

- **Threshold access structure:** The access structure of a (t, n) threshold secret sharing scheme consists of all the subsets with at least t of n participants.
- **Vector space access structure:** Let the secret space $K = GF(q)$ be a finite field and $E = K^t$ a vector space. The access structure Γ is said to be a vector space access structure if there exists a function

$$\psi : \{D\} \cup H \to E$$

such that $A \in \Gamma$ if and only if the vector $\psi(D)$ can be expressed as a linear combination of the vectors in the set $\{\psi(P) | P \in A\}$.

C. Operations on Vector Space

Assume $\alpha = (a_1, ..., a_t)$, $\nu = (v_1, ..., v_t)$, $V = (V_1, ..., V_t)$, where $a_1, ..., a_t, v_1, ..., v_t$ are elements of a finite field K and $V_1, ..., V_t$ are elements of an additive group G_1. In our construction, we use the operation of inner product in K^t, and an operation of an element of K^t with an element in G_1^t.

- $\alpha \bullet \nu = a_1 v_1 + \cdots + a_t v_t$
- $\alpha \circ V = a_1 V_1 + \cdots + a_t V_t$

Obviously the result of the first operation is an element in K and the second belongs to G_1.

D. Secure DKG for Discrete-Log Based Cryptosystems

A distributed key generation protocol is implemented among a set of players $H_1, H_2, ..., H_n$ to generate the secret key and public key of the cryptosystem. The secret key is shared by $H_1, H_2, ..., H_n$ via an access structure, and the public key is output in the clear. A DKG protocol mainly contains two phases:

- **Generating the secret key:** In this phase each participant chooses a random value and distributes it through all the players via a verifiable secret sharing scheme as a dealer. In the end, every player gets his share of the secret key.
- **Extracting the public key:** This phase outputs the corresponding public key in the clear.

Consider a static and strong admissible adversary[18], i.e. the adversary has determined which players to corrupt before the protocol being implemented, and can corrupt all but one player in each authorized subset. The only constraint on this adversary is that at least one authorized subset must remain pure i.e. composed of all uncorrupted players. A secure DKG protocol should satisfy the requirements of correctness and secrecy:

- **Correctness:**
  1) All qualified subsets composed by honest players define the same unique secret key.
  2) All honest players have the same value of public key about the secret key guaranteed by 1.
  3) The secret key is uniformly distributed(and hence the public key).
- **Secrecy:**
  No information on the secret key can be learned by the adversary except for what is implied by the public key.

For more details about distributed key generation, please refer to [1], [2], [8].

III. Building Blocks for Our DKG Protocol

A. Secret Sharing in Bilinear Groups on Vector Space Access Structures

The participants of this system consist a dealer D and a set of n players $H = \{H_1, ..., H_n\}$. Suppose Γ is the vector space access structure with basis Γ_0 defined on H. Both the secret space and the share space are $K = G_1$, where G_1 is an additive group of a prime order q.

To share a random secret S of G_1, the dealer D firstly publishes a map ψ: $\{D\} \cup H \to Z_q^t$. Then D randomly chooses a secret vector $V = (V_1, ..., V_t)$ from K^t such that $\psi(D) \circ V = a_1 V_1 + \cdots + a_t V_t = S$ where $\psi(D) = (a_1, ..., a_t) = \alpha$. Let $\psi(H_j) = (a_{j1}, ..., a_{jt}) = \alpha_j$, then the share distributed to H_j by D is $S_j = \psi(H_j) \circ V = a_{j1} V_1 + \cdots + a_{jt} V_t$.

When a qualified subset $A = \{H_{i_1}, ..., H_{i_l}\}$ of Γ intends to reconstruct the secret, members of A firstly compute χ from $\chi \psi(A) = \psi(D)$, where χ is a vector in Z_q^l and $\psi(A)$ is a matrix establishes its row vectors by $\psi(H_{j_1})$, ..., $\psi(H_{j_l})$. Then the secret can be calculated from $S = \chi \circ S_A$ with $S_A = (S_{j_1}, ..., S_{j_l})$.

B. Information-Theoretical Secure Verifiable Secret Sharing in Bilinear Groups on Vector Space Access Structures

- **Parameters:**
  Assume G_1, G_2 are two groups with the same prime order q and $\hat{e}$ is the bilinear map as we refer previously in Section 2. Let P be a random generator of G_1 such that the discrete logarithm problem with basis P in G_1 is intractable, and γ be a random element of G_2 where nobody knows the discrete logarithm of γ. The secret space and the the share space are G_1 and $G_1 \times Z_q$ respectively. The access structure Γ is a vector space access structure with basis Γ_0. Assume S is the secret randomly chosen from G_1 to be shared among n participants and t is the maximum order of the minimum qualified subset.
- **Algorithm of sharing:**
  - The dealer D publishes a map ψ: $\{D\} \cup H \rightarrow Z_q^t$. Assume that $\psi(D) = (a_1, ..., a_t) = \alpha$ and $\psi(H_j) = (a_{j1}, ..., a_{jt}) = \alpha_j$.
  - Choose a secret vector $V = (V_1, ..., V_t)$ from G_1^t such that $\psi(D) \circ V = a_1V_1 + \cdots + a_tV_t = S$. Choose another secret vector $\beta = (b_1, ..., b_t)$ from Z_q^t and set $r = \psi(D) \bullet \beta = a_1b_1 + \cdots + a_tb_t$.
  - Compute and broadcast $E_k = \hat{e}(V_k, P)\gamma^{b_k}$ for $k =$ 1, ..., t.
  - D computes

    $$S_j = \psi(H_j) \circ V = a_{j1}V_1 + \cdots + a_{jt}V_t,$$

    $$r_j = \psi(H_j) \bullet \beta = a_{j1}b_1 + \cdots + a_{jt}b_t$$

    and sends (S_j, r_j) secretly to H_j for $j =$ 1, ..., n.
- **Algorithm of Verification:**
  When H_j has received his share (S_j, r_j) he checks if

  $$\hat{e}(S_j, P)\gamma^{r_j} = \prod_{k=1}^{t} {E_k}^{a_{jk}} \qquad (1)$$

- **Algorithm of Reconstruction:**
  Suggest $A = \{H_{i_1}, ..., H_{i_l}\}$ is a subset of Γ to reconstruct the shared secret. Each participant $H_j (j = i_1, ..., i_l)$ broadcasts his share (S_j, r_j) to others in A. Every one can verify the validity of shares provided by others through Eq. (1).

  After receiving all the valid shares of a qualified subset, the participants firstly compute χ from $\chi\psi(A) = \psi(D)$ where χ is a vector in Z_q^l and $\psi(A)$ is a matrix establishes its row vectors from $\psi(H_{i_1})$, ..., $\psi(H_{i_l})$. Then the secret can be calculated from $S = \chi \circ S_A$ with $S_A = (S_{i_1}, ..., S_{i_l})$. Actually as long as they obtain the shares whose holders are enough to determine a minimum qualified subset in A, the secret can be reconstructed effectively.

IV. Our Secure DKG Protocol with Vector Space Access Structure on Bilinear Groups

A. The Protocol

- **Parameters:**
  Assume G_1, 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. Let P be a generator of G_1 where the discrete logarithm problem with basis P is intractable in G_1, and γ be a random element of G_2 such that no one knows the discrete logarithm of γ. The participants of the system are a set H of n players H_1, ..., H_n. Before the phase of generating secret key, the players decide a vector space access structure Γ on H together, i.e. the map $\psi : \{D\} \cup H \rightarrow GF(q)^t$ as we defined in Section 2. In fact, there does not exist a real dealer D in our system and the players just need determine the vectors $\psi(D) = \alpha = (a_1, \cdots, a_t)$, $\psi(H_i) = \alpha_i = (a_{i1}, \cdots, a_{it})$ for $i = 1, ..., n$ such that α can be expressed as a linear combination of the vectors in the set $\{\psi(P)|P \in A\}$, where A denotes the qualified subset.
- **Generating X:**
  1) – Each H_i chooses a random value S_i from G_1 and a value r_i from Z_q. Then choose a vector $V_i = (V_{i1}, \cdots, V_{it})$ from G_1^t and a vector $\beta_i = (b_{i1}, \cdots, b_{it})$ from Z_q^t such that $S_i = \alpha \circ V_i = a_1V_{i1} + \cdots + a_tV_{it}$ and $r_i = \alpha \bullet \beta_i = a_1b_{i1} + \cdots + a_tb_{it}$. Publish $E_{ik} = \hat{e}(V_{ik}, P)\gamma^{b_{ik}}$ for $k = 1, \cdots, t$.
     Compute $S_{ij} = \psi(H_j) \circ V_i = a_{j1}V_{i1} + \cdots + a_{jt}V_{it}$ and $r_{ij} = \psi(H_j) \bullet \beta_i = a_{j1}b_{i1} + \cdots + a_{jt}b_{it}$ for $j = 1, \cdots, n$. Then H_i sends (S_{ij}, r_{ij}) secretly to H_j.
     – When H_j has received his share (S_{ij}, r_{ij}) he checks if

     $$\hat{e}(S_{ij}, P)\gamma^{r_{ij}} = \prod_{k=1}^{t} {E_{ik}}^{a_{jk}} \qquad (2)$$

     If Eq.(2) fails, H_j broadcast a *complaint* against H_i.
     – Each H_i who received a *complaint* from H_j broadcast (S_{ij}, r_{ij}) that satisfy Eq.(2).
     – Each player marks as *disqualified* any player that either
       * received *complaints* of all players in one qualified subset or
       * answered to a *complaint* with values that do not satisfy Eq.(2).
  2) Each player builds the set of non-disqualified players $QUAL$.
  3) Each player H_i computes his shares $X_i = \sum_{j \in QUAL} S_{ji}$ and $x_i = \sum_{j \in QUAL} r_{ji}$. The distributed secret value X is not explicitly computed by any party, but it equals to $X = \sum_{i \in QUAL} S_i$.

- **Extracting** $Y = \hat{e}(X, P)$**:**
  1) Each H_i in $QUAL$ broadcasts $A_{ik} = \hat{e}(V_{ik}, P)$ for $k = 1, \cdots, t$.
  2) For $j = 1, ..., n$, every H_j verifies the value broadcast by players in $QUAL$ through the following equation
$$\hat{e}(S_{ij}, P) = \prod_{k=1}^{t} A_{ik}{}^{a_{jk}}. \qquad (3)$$
     If the check succeeds, set $\widetilde{Y_i} = \prod_{k=1}^{t} A_{ik}{}^{a_k}$. Else H_j broadcasts a complaint against H_i and publish S_{ij}, r_{ij}.
  3) For players H_i who receive at least one valid complaint, the other players run the reconstruction phase to compute S_i and set $\widetilde{Y_i} = \hat{e}(S_i, P)$.
  4) Compute $Y = \prod_{i \in QUAL} \widetilde{Y_i}$.

B. Security

We proof the security of our protocol from the two aspects: correctness and secrecy as we mentioned in Section 2.

- **Correctness**:

  Theorem 1 *All qualified subsets composed by honest players define the same unique secret key X.*

  Proof: From the definition of the adversary, we know that there is at lest one qualified subset composed by honest players. Suppose $A = \{H_1, H_2, ..., H_l\}$ is a qualified subset where $H_1, H_2, ..., H_l$ are all uncorrupted players. The share of X possessed by H_i is $X_i = \sum_{j \in QUAL} S_{ji} = \sum_{j \in QUAL} \alpha_i \circ V_j$. The secret determined by A can be reconstructed as following:
  - Players in A calculate out $\mu = (u_1, u_2, ..., u_l)$ such that $u_1\alpha_1 + u_2\alpha_2 + \cdots + u_l\alpha_l = \alpha$.
  - The secret X is determined by $X = \mu \circ (X_1, ..., X_l) = u_1 X_1 + \cdots + u_l X_l$.

  As $X_i = \sum_{j \in QUAL} S_{ji} = \sum_{j \in QUAL} \alpha_i \circ V_j$, we have
$$\begin{aligned} X &= u_1 X_1 + \cdots + u_l X_l \\ &= u_1 \sum_{j \in QUAL} S_{j1} + \cdots + u_l \sum_{j \in QUAL} S_{jl} \\ &= u_1 \sum_{j \in QUAL} \alpha_1 \circ V_j + \cdots + u_l \sum_{j \in QUAL} \alpha_l \circ V_j \\ &= \sum_{j \in QUAL} u_1\alpha_1 \circ V_j + \cdots + \sum_{j \in QUAL} u_l\alpha_l \circ V_j \\ &= \sum_{j \in QUAL} (u_1\alpha_1 + \cdots + u_l\alpha_l) \circ V_j \\ &= \sum_{j \in QUAL} \alpha \circ V_j \\ &= \sum_{j \in QUAL} S_j. \end{aligned}$$
  Obliviously, the secret determined by any qualified subset with all players being honest equals to the X generated by our protocol. That means all qualified subsets composed by honest players determine the same unique secret key X. ■

  Theorem 2 *All honest players have the same value of the public key $Y = \hat{e}(X, P)$ with X guaranteed by Theorem 1.*

  Proof: From the algorithm of extracting the public key we know that $Y = \prod_{i \in QUAL} \widetilde{Y_i}$. In the protocol the values $\widetilde{Y_i}$ are calculated either through $\widetilde{Y_i} = \prod_{k=1}^{t} A_{ik}{}^{a_k}$ if the public values A_{ik} has been verified to be correct through Eq.(3), or else by $\widetilde{Y_i} = \hat{e}(S_i, P)$ where S_i is reconstructed by the players. As
$$\begin{aligned} \widetilde{Y_i} &= \prod_{k=1}^{t} A_{ik}{}^{a_k} = \prod_{k=1}^{t} \hat{e}(V_{ik}, P)^{a_k} \\ &= \prod_{k=1}^{t} \hat{e}(a_{ik} V_{ik}, P) = \hat{e}(\sum_{k=0}^{t} a_{ik} V_{ik}, P) \\ &= \hat{e}(S_i, P), \end{aligned}$$
  then
$$\begin{aligned} Y &= \prod_{i \in QUAL} \widetilde{Y_i} = \prod_{i \in QUAL} \hat{e}(S_i, P) \\ &= \hat{e}(\sum_{i \in QUAL} S_i, P) = \hat{e}(X, P). \end{aligned}$$
  This means the players who act correctly get the same value of public key. ■

  Theorem 3 *The secret key X is uniformly distributed in G_1, and hence the public key Y is uniformly distributed in G_2.*

  Proof: The secret key X is defined as $X = \sum_{i \in QUAL} S_i$, thus as long as there is one value S_i in this sum is chosen at random from G_1, X is uniformly distributed in G_1. In the protocol we can see that the set $QUAL$ is determined by all the honest players and some of the corrupted players who executed correctly in Step 1-2 of **Generating** X in the protocol. Thus there must be at least one S_i with $i \in QUAL$ is uniformly distributed in G_1, which guarantees that $X = \sum_{i \in QUAL} S_i$ is uniformly distributed in G_1 and consequently $Y = \hat{e}(X, P)$ is uniformly distributed in G_2. ■

- **Secrecy:**

  We employ the same concept of **simulatability** to state the secrecy of our DKG protocol as in [1]: for every static and strong admissible adversary $\mathcal{A}$, there exists a simulator SIM such that on input an element Y in G_2 produces an output distribution which is polynomially indistinguishable from $\mathcal{A}$'s view of a run of the DKG protocol that ends with Y as its public key output.

We firstly provide a simulator SIM for our DKG protocol, and then we will show that the view of the adversary $\mathcal{A}$ that interacts with SIM on input Y is the same as the view of $\mathcal{A}$ that interacts with the honest players in a regular run of the protocol that outputs the given Y as the public key.

- **Algorithm of simulator** SIM Denote by $\mathcal{B} = \{H_{i_1}, ..., H_{i_m}\}$ the set of players controlled by the adversary, and by $\mathcal{G}$ the set of honest players run by the simulator SIM. Note that no subset of $\mathcal{B}$ is a qualified subset and there is at least one subset in $\mathcal{G}$ is a qualified subset. The algorithm of simulator is implemented as follow.

  ∗ Input public key Y.

  ∗ Perform Step 1-2 of **Generating** X in protocol **DKG** on behalf of the uncorrupted players in $\mathcal{G}$. At the end of Step 2 the following holds:

    1) The set $QUAL$ is well defined and $\mathcal{G} \in QUAL$. For $i \in \mathcal{G}$ all the V_i, β_i are chosen at random.
    2) The view of the adversary consists of the secret vectors V_i, β_i for $i \in \mathcal{B}$, the shares (S_{ij}, r_{ij}) for $i \in QUAL$ and $j \in \mathcal{B}$, and all the public values E_{ik} for $i \in QUAL, k = 1, ..., t$.
    3) SIM knows all the vectors V_i, β_i for $i \in \mathcal{G}$ and thus possesses the shares (S_{ij}, r_{ij}) for $i \in \mathcal{G}, j = 1, ..., n$. For $i \in QUAL \bigcap \mathcal{B}$, as there is at least one qualified subset in $\mathcal{G}$ that run by SIM, the shares (S_{ij}, r_{ij}) for $j = 1, ..., n$ can be reconstructed by SIM. In a word, SIM knows all the (S_{ij}, r_{ij}) for $i \in QUAL, j = 1, ..., n$.

  ∗ Perform the following computations:

    · Compute $A_{ik} = \hat{e}(V_{ik}, P)$ for $i \in QUAL \setminus \{h\}, k = 1, ..., t$, where h can be any random element in $QUAL \bigcap \mathcal{G}$.

    · Set $\widetilde{Y_h}^* = Y \prod_{i \in QUAL \setminus \{h\}} \widetilde{Y_i}^{-1}$

    · Compute the vector $A^*_{hk} = \hat{e}(V^*_{hk}, P)$ for $k = 1, ..., t$ from the following equation:

$$\begin{cases} \hat{e}(\alpha \circ V^*_h, P) = \hat{e}(S^*_h, P) = \widetilde{Y_h}^* \\ \hat{e}(\alpha_{i_1} \circ V^*_h, P) = \hat{e}(S_{hi_1}, P) \\ \vdots \\ \hat{e}(\alpha_{i_m} \circ V^*_h, P) = \hat{e}(S_{hi_m}, P) \end{cases} \tag{4}$$

i.e.

$$\begin{cases} \hat{e}(V^*_{h1}, P)^{a_1} \cdots \hat{e}(V^*_{ht}, P)^{a_t} \\ = {A_{h1}}^{a_1} \cdots {A_{ht}}^{a_t} = \widetilde{Y_h}^* \\ \hat{e}(V^*_{h1}, P)^{a_{i_1 1}} \cdots \hat{e}(V^*_{ht}, P)^{a_{i_1 t}} \\ = {A_{h1}}^{a_{i_1 1}} \cdots {A_{ht}}^{a_{i_1 t}} = \hat{e}(S_{hi_1}, P) \\ \vdots \\ \hat{e}(V^*_{h1}, P)^{a_{i_m 1}} \cdots \hat{e}(V_{ht}, P)^{a_{i_m t}} \\ = {A_{h1}}^{a_{i_m 1}} \cdots {A_{ht}}^{a_{i_m t}} = \hat{e}(S_{hi_m}, P) \end{cases} \tag{5}$$

  ∗ Broadcast A_{ik} for $i \in \mathcal{G} \setminus \{h\}$ and A^*_{hk} for $k = 1, ..., t$.

  ∗ Perform Step 2-4 of **Extracting** Y in protocol **DKG** on behalf of the honest players.

- **Analysis of simulatablility** The probability distribution of $\mathcal{A}$'s view from the uncorrupted parties in a regular run of our DKG protocol is as following:

  ∗ The shares S_{ij} and r_{ij} for $i \in \mathcal{G}, j \in \mathcal{B}$ are uniformly distributed in G_1 and Z_q respectively.

  ∗ Public values E_{ik}, A_{ik} for $i \in \mathcal{G}, k = 1, ..., t$ satisfy the verification equations (2) and (3) respectively for all $j \in \mathcal{B}$.

  In the **algorithm of simulator** SIM with the uncorrupted players implements Step 1-2 of **Generating** X as in our real DKG protocol. Note that at the end of Step 2 the shares (S_{ij}, r_{ij}) for $i \in \mathcal{G}, j \in \mathcal{B}$ have been determined and the verifications for public values E_{ik}, $i \in \mathcal{G}, k = 1, ..., t$ have finished. Thus the distribution of S_{ij}, r_{ij} is polynomially indistinguishable from our real DKG protocol and the public values E_{ik} satisfy Eq. (2). Then consider the public values $A^*_{ik}, i \in \mathcal{G}, k = 1, ..., t$. For $i \in \mathcal{G} \setminus \{h\}, k = 1, ..., t$, as A^*_{ik} equal to the corresponding A_{ik}, they can pass through the verification equation (3). For $i = h$, note that A^*_{hk} is calculated from the set of equations (4), and thus satisfy every equation in (4) and (5). Obviously in (5) every equations except the first one is actually a verification equation from Eq.(3) where $j = i_1, ..., i_m \in \mathcal{B}$, that means those A^*_{hk}s satisfy the verification equation (3). In a word, the public values $A^*_{ik}, i \in \mathcal{G}, k = 1, ..., t$ satisfy Eq.(3). Now we can conclude that simulator SIM that on input an element Y in G_2 produces an output distribution which is polynomially indistinguishable from $\mathcal{A}$'s view of a run of the DKG protocol that ends with Y as its public key output, i.e. our DKG protocol satisfy the requirement of secrecy.

V. Conclusion

In this paper we proposed a secure DKG protocol on vector space access structures. The new proposed protocol is run by a set of players on vector space access structures to generator a pair of public key and secret key that are elements of bilinear groups. We specially discussed it security from two aspects: correctness and secrecy in our paper. Our work has a wide application for generating distributed keys in situation that the users do not possess exactly the same power and position.

Acknowledgment

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

References

[1] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, *Secure distributed key generation for discrete-log based cryptosystems*, Eurocrypt'99, 1999.

[2] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, *Revisiting the distributed key generation for discrete-log based Cryptosystems* RSA Security'03, 2003.

[3] R. Gennaro, S. Jarecki, H. Krawczyk and T.Rabin, *Robust threshold DSS signatures*, Information and Computation 164, pp.54C84,2001.

[4] V. Shoup and R.Gennaro, *Securing threshold cryptosystems against chosen cyphertext attack*, EUROCRYPT'98, pp.1-16,1998.

[5] V. Shoup, *Practical threshold signaturs*, EUROCRYPT'2000, pp.207-220, 2000

[6] A. Shamir,*How to share a secret*, Comm. ACM 22, pp.612-613,1979.

[7] T. Pedersen, *A threshold cryptosystem without a trusted party*, Eurocrypt'91, Lecture Notes in Computer Science, pp 522-526, 1991.

[8] F. Zhang, *Distributed key generation based on vector space access structures*, Acta electronica Sinica, pp 816-819, 2005.

[9] F. Zhang, Y. Wang, *Distributed key generation based on generalized verifiable secret sharing*, Acta electronica Sinica, pp 580-584, 2003.

[10] D. Boneh and M. Franklin, *Identity-based encryption from the weil pairing*, SIAM J.Computing, 32(3):586-615, 2003.

[11] J. Baek and Y. Zheng, *Identity-based threshold signature scheme from the bilinear pairings*, Proceedings of the international Conference on Information and Technology: Coding and Computing, 2004.

[12] E. Kiltz and K. Pietrzak, *Leakage resilient ElGamal encryption*, ASIACRYPT, pages595C612,2010.

[13] T. Y. Wu and Y. M. Tseng, *A paring-based publicly verifiable secret sharing scheme*, Journal of Systems Science and Complexity, 2011.

[14] H. Yuan, F. Zhang, X. Huang, Y. Mu, W .Susilo and L. Zhang, *Certificateless threshold signature scheme from bilinear maps*, Information Sciences 180,2010.

[15] H. Sun and L. Guo, *A forward secure threshold signature scheme based on bilinear pairing*, Intelligent Computing and Intelligent Systems (ICIS),2010 IEEE International Conference, 2010.

[16] C. Gentry, *Practical identity-based encryption without random oracles*, In Advances in Cryptology-EUROCRYPT 2006, Lecture Notes in Computer Science. Springer-Verlag, 2006.

[17] J. Baek, Y. Zheng, *Identity-based threshold signature scheme from the bilinear pairings*, full version, available at http://phd.netcomp.monash.edu.au/joonsang.

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