Future Generation Computer Systems 52 (2015) 109–115

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Information-theoretical secure verifiable secret sharing with vector space access structures over bilinear groups and its applications

Jie Zhang [a], Futai Zhang [a,b,*]

[a] School of Computer Science and Technology, Nanjing Normal University, 210097, Nanjing, China
[b] Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, 210097, Nanjing, China

HIGHLIGHTS

- We present an information-theoretical secure VSS scheme with vector space access structure over bilinear groups.
- We convert the scheme to a modified one with improved efficiency.
- We show the application of our schemes in Boneh and Franklin's identity-based encryption scheme.
- We show how to use our scheme to realize distributed key generation and distributed decryption in bilinear ElGamal encryption system.

ARTICLE INFO

Article history:
Received 28 June 2014
Received in revised form
15 October 2014
Accepted 14 November 2014
Available online 24 November 2014

Keywords:
Verifiable secret sharing
Information-theoretical secure
Vector space access structure
Bilinear pairing
Pairing-based cryptosystem

ABSTRACT

As a basic tool, Verifiable Secret Sharing (VSS) has wide applications in distributed cryptosystems as well as secure multi-party computations. A number of VSS schemes for sharing a secret from a finite field, both on threshold access structures and on general access structures, have been available. In this paper, we investigate the verifiably sharing of a secret that is a random element from a bilinear group on vector space access structures. For this purpose, we present an information-theoretical secure VSS scheme, and then convert it to a modified one with improved efficiency. The performance and the security of the proposed schemes are analyzed in detail. Two examples are given to illustrate the applications of our proposed VSS schemes. One is the secure sharing of an organization's private key in Boneh and Franklin's identity-based encryption system, and the other is the distributed key generation and distributed decryption for bilinear ElGamal encryption system, both with vector space access structures.

1. Introduction

Secret sharing [1] is a fundamental tool for safe guarding cryptographic keys, distributed cryptosystems and secure multi-party computation, etc. It is a technique of distributing shares of a secret among a set P of participants in such a way that only some predetermined subsets called qualified subsets of P can reconstruct the secret by pooling their shares together. Earlier basic secret sharing schemes are threshold ones which assume both the dealer and the participants are honest and require all participants possess exactly the equal position, power and reliability. However, in real world applications, a dealer or some participants may not always behave honestly. They may not fully trust each other. Apart from this, in many occasions the participants may possess different status, different power and different reliability.

In order to solve the reasonable distrust between the dealer and participants, verifiable secret sharing (VSS) [2] was introduced. In a VSS scheme, participants are able to verify whether the shares distributed to them by the dealer or submitted by other participants are valid. To meet with the possible requirement for different power and reliability among different participants, general secret sharing schemes have been investigated, which can be used to share a secret on any access structures as needed and do not have to assume the same position of share-holders. By now, a number of VSS schemes for sharing secrets from a finite field, either on threshold access structures [3,4] or on general access structures [5], have been available.

The vector space construction [6,7] is a method to implement secret sharing schemes for a family of access structures that includes threshold access structures as a particular case. Some VSS schemes in finite field on vector space access structures have

[*] Corresponding author at: School of Computer Science and Technology, Nanjing Normal University, 210097, Nanjing, China.
E-mail address: zhangfutai@njnu.edu.cn (F. Zhang).

http://dx.doi.org/10.1016/j.future.2014.11.013
0167-739X/© 2014 Elsevier B.V. All rights reserved.

been presented. Recently, the bilinear pairing-based cryptography has received much attention from the research community. Many bilinear pairing-based schemes and protocols have been proposed [8–13]. We notice that in some of the pairing-based cryptographic schemes, the secret keys come from a bilinear group rather than a finite field. To share and manage such secret keys, we have to consider the verifiably sharing for secrets from a bilinear group, and such schemes with threshold access structures [14–16] have been available by now. However, few VSS schemes for sharing secrets from a bilinear group on vector space access structures can be found in the literature. For the good properties of vector space access structures and the prosperous of pairing-based cryptosystems, in this paper we study VSS on vector space access structures that shares secrets from bilinear groups and put forward a basic VSS scheme with detailed description and particularly analyze its security and computational cost. Then we give a modified one with improved efficiency while enjoy the same level of security with the first one.

With regard to the applications of our schemes, we take Boneh and Franklin's identity-based encryption [17] and bilinear pairing-based ElGamal encryption [10] as two specific examples. We show how to use our VSS schemes to share the private key of an organization in Boneh and Franklin's identity-based encryption system, and how to generate in a distributed manner a secret and public key pair of bilinear ElGamal encryption system, both with vector space access structures. Similar applications can be easily implemented in some other pairing-based cryptosystems.

Organization:

In Section 2 we briefly describe the concepts of bilinear pairing and access structure and some related mathematical operations. Then in Section 3 we present a basic VSS scheme for sharing a random secret of a bilinear group on vector space access structures with detailed description. We also analyze the security and computational cost of our basic scheme. After that in Section 4 we give a modified VSS scheme with a brief analysis of its security and computational cost. Besides, we illustrate the applications of our schemes in Section 5. At last we conclude our paper in Section 6.

2. Preliminaries and definitions

We firstly give a brief review of some basic concepts such as bilinear pairing and access structure. Then we give two mathematical operations on vector space and bilinear group which will be used in the construction of our VSS schemes.

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. A map $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ is called a bilinear pairing (or 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 pairing $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ as above, where $\hat{e}$ and the group action in G_1 and G_2 can be computed efficiently.

2.2. Access structure

A secret sharing scheme involves a dealer D who holds the secret and a set $H = \{H_1, \dots, H_n\}$ of participants (share-holders) who receive shares of a secret from the dealer. An access structure Γ on H specifies a family of qualified subsets of H that are allowed to reconstruct the shared secret using their secret shares. We denote by $\Gamma_0 = \{A_1, \dots, A_m\}$ 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 access structure which actually contains the threshold one.

- **Threshold access structure**: A (k, n) threshold access structure consists of all those subsets of H containing at least t of the n share-holders.
- **Vector space access structure**: Let the secret space $K = GF(q)$ be a finite field and $L = K^t$ the vector space over K with dimension t. An access structure Γ is said to be a vector space access structure if there exists a function

  $$\psi : \{D\} \cup H \to L \tag{1}$$

  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 $\{\psi(P) | P \in A\}$.

The vector space construction is a method to implement secret sharing schemes for vector space access structures that include threshold access structures as a particular case. Obviously Shamir's threshold scheme [1] can be seen as a vector space secret sharing scheme by taking $\psi(D) = (1, 0, \dots, 0)$ and $\psi(H_i) = (1, x_i, \dots, x_i^{t-1})$, where $x_1, x_2 \dots, x_n$ are n distinct, nonzero elements of K [18].

2.3. Notations for two mathematical operations

Let G_1, q be the same as specified in Section 2.1. Denote by $K = GF(q)$ the finite field with q elements. Assume $\alpha = (a_1, \dots, a_t)$, $v = (v_1, \dots, v_t)$, $V = (V_1, \dots, V_t)$, where $a_1, \dots, a_t$, $v_1, \dots, v_t$ are elements of finite field K and $V_1, \dots, V_t$ are elements of the additive group G_1. In our construction, we will 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. They are defined as follows.

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

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

3. Verifiable secret sharing on vector space access structures over bilinear groups

In this section, firstly we show a technique of sharing a secret that is a random element of a bilinear group on vector space access structures. Then we present the corresponding information-theoretical secure VSS scheme. After that we demonstrate the correctness and analyze the security and the computational cost of our scheme.

3.1. Secret sharing on vector space access structures over bilinear groups

Let D be the dealer and $H = \{H_1, \dots, H_n\}$ a set of n players (share-holders). Suppose Γ is the vector space access structure with basis Γ_0 defined on H. Both the secret space and the share space are G_1 which is an additive bilinear group with order q as specified in Section 2.