A Novel Verifiable Secret Sharing Scheme over Bilinear Groups

[a] Asha Jyothi Ch, [b]G Narsimha, [c]J Prathap
[a]Assistant Professor, Dept. of IT, JNTUHCEJ, Nachupally, Jagtial, India, 505501.
[b]Associate Professor, Dept. of CSE, JNTUHCEJ, Nachupally, Jagtial, India, 505501.
[c]Associate Professor, Dept. of CSE, Sree Chaitanya College of Engg., Karimnagar, 505527.

Abstract

Secret sharing schemes have been proposed to safeguard the cryptographic keys such that the key is not under the control of a single user but over several users. A secret sharing scheme is a method of dividing a secret into shares and distributing them 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) scheme is a secret sharing scheme with an extra principle that every participant can verify whether the share distributed to him is accurate. There exist several VSS schemes for sharing an element chosen from finite field but there are few VSS schemes for sharing an element chosen from bilinear group where such groups are popularly used in pairing based cryptography protocols. In this paper we propose a computationally secure and efficient VSS scheme for sharing an element chosen from bilinear groups.

KEYWORDS—Secret sharing schemes, Verifiable Secret sharing schemes, Bilinear groups, Bilinear maps, Pairings.

I. Introduction

An application of threshold cryptography is the secret sharing scheme. Assume k and n be positive integers such that k ≤ n. A (k, n)-threshold cryptosystem [9] divides the secret S into n shares and distributes them to set of n participants each such that any subset of k participants can construct the value of the secret, but subset of k−1 or fewer participants cannot do so. Most of the cryptographic protocols involve the use of the secret key that is one of input to the encryption and decryption algorithms. Storage of the secret key by a user creates a single point of failure which can be eliminated by sharing the secret key among several users in a threshold fashion. Practical implementation of threshold cryptosystem is possible with a secret sharing mechanism. A (k, n) secret sharing scheme allows a dealer to divide a secret (or secret key) into n shares and distributes the shares to n participants each such that only a qualified subset of k ≤ n participants can correlate to reconstruct the secret from their shares. The secret sharing protocols consists of two phases: *Sharing phase and Reconstruction phase*. During the Sharing phase the Dealer divides secret into n shares and distributed the shares secretly to n participants. During the Reconstruction phase, a group of at least k participants associate to generate the secret from their shares. The popularly used secret sharing scheme is the Shamir secret sharing scheme [2].

Secret sharing schemes [1] does not enable the participants to verify the consistency or integrity of the shares that can be achieved by verifiable secret sharing schemes using auxiliary information called commitments. A verifiable secret sharing scheme [1] [10] is a secret sharing scheme that additionally enables each and every participant to verify that the shares distributed to him by the dealer is consistent without disclosure of the secret and the corresponding shares. In addition to Sharing and Reconstruction phases [3] [4], these schemes have an additional phase called verification phase. The Dealer computes not only n shares but also k commitments during the Sharing phase and the n shares are distributed secretly to n corresponding participants plus the k commitments are broadcasted to the n participants. Each participant when receives their share, can verify the correctness of the share using the verification phase. As and when required a group of k participants can associate to reconstruct the secret from their shares of the secret.

The applications [1] of the verifiable secret sharing schemes are secure multiparty computation protocols. These protocols allow a group of k users to compute $f(x_1, x_2, ..., x_k)$ such that the input x_i is known only to i^{th} user. Threshold cryptography protocols and e-voting and e-auction protocols are examples of secure multiparty computation protocols. In this paper the domain of VSS is a bilinear group.

Another essential concept is the bilinear group which is a group of elliptic curve points that exhibit certain important properties. As the group of points on the elliptic curve exhibits certain special properties, elliptic curves are likely used in cryptography. The elements in these groups are not scalar (single) values but points on an elliptic curve that satisfy specific criteria. Such groups are popularly used in bilinear maps or pairings. The groups used in bilinear map are called bilinear groups i.e., in a bilinear map $f : D_1 X D_1 \rightarrow D_2$, D_1 and D_2 are bilinear groups such that D_1 is additively written abelian group over an elliptic curve $E(F_p)$ and D_2 is a multiplicative abelian group over a large finite field. Elliptic curve cryptography is well known for its stronger security levels with smaller bit lengths and pairing-based cryptography is the special case of elliptic curve cryptography. In many pairing-based cryptographic systems, the secret keys are random elements chosen from some bilinear groups; hence the VSS schemes for sharing an element from bilinear group is very much essential. The first VSS over bilinear group was proposed by J.Baek and Y.Zheng [5]. Later Jie and Futai [4] proposed a computationally efficient VSS over bilinear group than in [5]. In this paper, we propose a new VSS over bilinear group that is computationally efficient than the one in [4] and hence also efficient than in [5].

The rest of the paper is organized as follows. Section II presents the literature review of the verifiable secret sharing schemes. Section III presents the mathematical background and computationally hard problems essential for the proposed scheme. Section IV presents the methodology of existing VSS schemes over bilinear groups. Section V presents the methodology of proposed model and compares it with the existing schemes mentioned in section IV. Section VI gives the conclusion for this paper.

II. Related Work

In the early days of verifiable secret sharing schemes, the secret is a scalar or single value but with the introduction of pairing based cryptography, there exists highest need of sharing an element from bilinear group which is a point on an elliptic curve. Since many years there exists numerous VSS schemes that share an element chosen from a *finite field* but there are few VSS schemes that share an element chosen from a *bilinear group* where such groups are widely used in pairing related protocols like pairing based cryptography protocols, certificateless cryptography protocols and Identity based cryptography protocols, Functional encryption, Attribute based encryption, Broadcast encryption.

The popularly known non-interactive VSS schemes are Feldman VSS [7] and Pedersen VSS [8]. In non-interactive VSS schemes checking the validity of a share does not require any interaction between dealer and participants. The proposed model is also non-interactive verifiable secret sharing scheme. Feldman [7] and Pedersen [8] consider the secret from finite field, but the proposed scheme considers the secret from bilinear group.

The existing non-interactive VSS schemes that share a secret from bilinear groups like the proposed model are Jie-Futai VSS [4] and Beak-Zheng VSS[5]. The observations made from Beak-Zheng VSS [5] are as follows. The coefficients of the polynomial equation used in the sharing phase are elliptic curve points and hence the sharing phase and reconstruction phases involve the use of elliptic curve arithmetic. It also uses pairing operation in the evaluation of commitments and in the verification phase.

The observations made from Jie-Futai VSS [4] when compared with Beak-Zheng VSS [5] are as follows. Unlike Beak-Zheng VSS [5] the coefficients of polynomial equation used in the sharing phase are finite field values and hence the sharing and reconstruction phases do not involve the use of elliptic curve arithmetic. Alike Beak-Zheng VSS [5] it uses pairing operation to compute the commitments and in the verification phase. As the polynomial evaluation in Jie-Futai VSS [4] involves field arithmetic and in Beak-Zheng VSS [5] involves point arithmetic, Beak-Zheng VSS [5] is more expensive than Jie-Futai VSS [4].

Highlights of the proposed scheme are as follows. Similar to Jie-Futai VSS [4] the coefficients of the polynomial equation are scalar and the computational complexity would be approximately same. The proposed scheme uses different method of handling the problem using different set of mathematical equations when compared to Jie-Futai VSS.

III. Preliminaries

The background mathematical concepts needed for the proposed scheme are the Point arithmetic of the elliptic curves and the bilinear maps or pairings.

A. Elliptic Curve Arithmetic

Consider an elliptic curve E [6] over a prime finite field F_q, denoted by E / F_q and defined by an equation “$y^2 = x^3 + ax + b$” such that a, bÎF_q with the discriminant “$\Delta = 4a^3 + 27b^2 \neq 0$.” The points on E / F_q along with an added point O called the neutral element form a group

G = {(x, y) \ x, yÎF_q, E(x, y) = 0} È {O}.

G under the point addition is a cyclic additive group of order n. Scalar multiplication over E/F_q can be computed with a sequence of point additions as [t]P = P + P +…+ P (t times).

The discrete logarithm problem over G assumed to be incomputable within polynomial time is defined below. The security strength of the schemes described here depends on the hardness of this problem.

Discrete Logarithm Problem (DLP): Given two group elements P and Q of G, find an integer nÎ$_R$ $Z_q^{¿}$, such that Q = [n]P whenever such an integer exists.

B.Bilinear Maps

Let D_1, D_2 and D_3 be three cyclic groups of the same order q, a prime. Consider D_1, D_2 as additive groups over an elliptic curve and D_3 as a multiplicative group of a large extension finite field. Assume that discrete logarithm problem (DLP) is hard in D_1, D_2 and D_3. A mapping f : D_1 x D_2 → D_3 is called a cryptographic bilinear map or bilinear pairing if it satisfies three properties namely non-degeneracy, bilinearity and computability. The pairing is said to be symmetric if $D_1 = D_2$ that is f: D_1 x $D_1 \rightarrow D_3$.

Bilinearity: f([a]X_1, [b]Y_1) = f(X_1, Y_1)^{ab} for all a,bÎ $Z_q^{¿}$ and X_1 ÎD_1, Y_1 ÎD_2.

Non-degeneracy: For all XÎD_1\{0} there exists YÎD_2 with f(X, Y) ≠ 1.

Computability: For all XÎD_1, YÎD_2, f(X, Y) can be computable in a reasonable amount of time.

IV. Existing VSS schemes over bilinear group

Let G_1 be the bilinear group with the order q and f: G_1 x $G_1 \rightarrow G_2$ be the symmetric pairing as defined above. Assume P is a generator of G_1 such that discrete logarithm to the base of f(P, P) is computationally infeasible and secret S is an element from G_1 that is to be shared using the verifiable secret sharing scheme. Assume dealer D, n group of participants and threshold k with the condition that $1 \leq k \leq n < q$.

A. Jie Zhang and Futai Zhang VSS Scheme

This VSS scheme when compared to J.Beak and Y.Zheng's VSS scheme [5] differs only in sharing phase and the rest of verification and reconstruction phases remain the same.

Sharing Phase

Step 1. Dealer D chooses s Î$_R$ $Z_q^{¿}$ and sets the secret S = [s]P. S certainly belongs to G_1 as P is from G_1.

Step 2. D chooses a_1, ..., a_{k-1} Î$_R$ $Z_q^{¿}$ and constructs a polynomial fn(x) = $a_0+a_1x+...+a_{k-1}x^{k-1}$ where $a_0 = s$.

Step 3. D calculates and publishes $CM_i = f(P,P)^{a_i}$ for i = 0,..., k -1 as the commitments of S and fn(x) .

Step 4. For i = 1,...,n, D calculates the share SH_i = [fn(i)]P mod q and sends it secretly to participant R_i.

Verification Phase

When participant R_i has received his share SH_i he verifies its integrity using the k commitments as

$$f(SH_i, P) = \prod_{j=0}^{k-1} CM_j^{i^j} \qquad (1)$$

If the above verification succeeds, the share SH_i assigned to R_i is valid otherwise invalid.

Reconstruction Phase

Suppose R_1, R_2,..., R_k be the k participants who wish to reconstruct the shared secret. Each R_i broadcasts his share SH_i to other k-1 co-operators, and every participant can check its integrity through Eq.1. For i = 1 to k, once all SH_i have been verified to be valid, every co-operator can reconstruct S by computing

$$S = \sum_{i=1}^{k} SH_i \prod_{1 \leq j \leq k, j \neq i} \frac{j}{i-j}$$

V. The Proposed Scheme

Let f: G_1 x $G_1 \rightarrow G_2$ be the symmetric pairing as defined above. Assume P and Q as generators of G_1. Assume dealer D, n group of participants and threshold k with the condition that $1 \leq k \leq n < q$. Similar to Jie and Futai scheme, the proposed scheme considers the secret S = [s]P where s Î$_R$ $Z_q^{¿}$. The three phases of the proposed VSS scheme are as follows.

Sharing Phase

This phase is implemented by the Dealer and involves the computation of n shares and k commitments. To share the secret S as S Þ (SH_1, SH_2, …, SH_n)

Step 1. Dealer D chooses s Î$_R$ $Z_q^{¿}$ and sets the secret S = [s]P. S certainly belongs to G_1 as P is from G_1.

Step 2. D chooses a_1, ..., a_{k-1} Î$_R$ $Z_q^{¿}$ and constructs a polynomial fn(x) = $a_0+a_1x+...+a_{k-1}x^{k-1}$ where a_0 = s.

Step 3. For i = 1,...,n, D calculates the share SH_i = [fn(i)]P mod q and sends it secretly to participant R_i.

Then computes the k commitments and broadcasts to n users as

Step 4. D calculates and publishes $CM_i = [a_i]Q$ for i = 0,...,k -1 as the commitments of S and fn(x) .

Verification Phase

When participant R_i has received his share SH_i he verifies its integrity using the k commitments as

$$CM = \sum_{j=0}^{k-1} [i^j] CM_j \qquad (2)$$

$$f(SH_i, Q) = f(P, CM) \qquad (3)$$

If the above verification succeeds, the share SH_i assigned to R_i is valid otherwise invalid.

Reconstruction Phase

Suppose R_1, R_2,..., R_k be the k participants who wish to reconstruct the shared secret. Each R_i broadcasts his share SH_i to other k-1 co-participants, and every participant can check its integrity through Eq.2, 3. For i = 1 to k, once all SH_i have been verified to be valid, every co-operator can reconstruct S by computing

$$S = \sum_{i=1}^{k} SH_i \prod_{1 \le j \le k, j \ne i} \frac{j+1}{i-j}$$

When compared to Jie-Futai VSS that uses only one generator P of G_1, the proposed scheme uses two generators P and Q of G_1. The secret to be shared S = [s]P is based on generator P and the public commitments in Jie-Futai VSS CM_i = $f(P,P)^{a_i}$ are based on P where as in the proposed scheme $CM_i = [a_i]Q$ are based on Q. From these equations, in the worst case the probability that public commitments reveal any information about polynomial coefficients a_i's is very less in the proposed model when compared to Jie-Futai VSS scheme.

Reference [3] is a two-party key agreement protocol based on Verifiable secret sharing scheme over bilinear groups. It internally uses Jie-and-Futai VSS scheme; which can be replaced with the proposed scheme.

A. Security Discussions

The security of the proposed scheme is based on the infeasibility to calculate the discrete logarithm on G_1 and G_2. We analyze security of the proposed scheme from two aspects:

- The verification phase fails if the dealer distributes inconsistent shares.
- The public information does not reveal any useful information about the secret and the shares.

Case 1. Correctness of the shares

The following theorem proves that the verification process fails when the dealer distributes inconsistent shares.

Theorem 1. The probability that the dealer calculates an incorrect share for any participant that passes the verification phase is negligible.

Proof. From the verification phase of section V, the share SH_i is valid if and only if $f(SH_i, Q) = f(P, CM)$.

If we expand CM = $\sum_{j=0}^{k-1}[i^j]CM_j = \sum_{j=0}^{k-1}[i^j][a_j]Q$ =$[a_0]Q + [a_1 i]Q + ...+ [a_{k-1}i^{k-1}]Q=[a_0 + a_1 i + a_{k-1}\ i^{k-1}]Q = [fn(i)]Q$. Therefore from this derivation $f(SH_i, Q) = f(P, [fn(i)]Q) = f([fn(i)]P, Q)$. Hence $SH_i = [fn(i)]P$.

Hence the probability that the dealer finds an inconsistent share $SH_i' \neq [fn(i)]P$ for any participant R_i such that $f(SH_i', Q) = f(P, CM)$ is negligible.

Case 2. Confidentiality of the secret

Theorem 2. Under the intractability of discrete logarithm on G_1, the adversary can get no useful information about the secret S and the share possessed by any participant from the public commitments. Without knowing the polynomial fn(x), one cannot derive any useful information about the secret and the shares.

Proof. The publicly known commitments are $CM_i = [a_i]Q$ for i = 0,...,k -1. As discrete logarithm problem is intractable on G_1, adversary cannot derive any useful information about ai's and hence the polynomial fn(x).

From the proof of above "Theorem 1," we know that $SH_i = [fn(i)]P$. Thus without knowledge of fn(x), it is impossible to obtain any useful information about the shares SH_i and hence the secret S.

B. Cost Comparison Mathematically

Here the computational cost of the newly proposed scheme is compared with the existing VSS schemes over bilinear group that are cited in [4] and [5] using the operations in different phases. The time-consuming operations considered for cost estimation are: T_f the time taken for a bilinear pairing operation, T_s the time taken for a scalar multiplication in G_1, and T_e the time taken for a exponentiation in G_2. The time factors are related as $T_s < T_e < T_f$, the time complexity of a pairing [6] is several times the time complexity of scalar multiplication. The computational cost in the three different phases for the schemes in [4], [5] and the proposed model are given in "Table I" below. Consider the secret is divided into n shares and require at least k shares for reconstruction.

TABLE I. Mathematical Computational cost in three phases

Phase	Beak-Zheng scheme	Jie-Futai scheme	Proposed scheme
Sharing Phase	$kT_f + n(k-1)T_s$	$nT_s + kT_e$	$(n + k)T_s$
Verification Phase	$nT_f + nkT_e$	$nT_f + nkT_e$	$2kT_f + kT_s$
Reconstruction Phase	kT_s	kT_s	kT_s

In [4] Jie and Futai proposed a VSS that is efficient than Beak and Zheng VSS scheme. Here from the above table comparing the proposed scheme with that of Jie-Futai VSS: In the sharing phase both differ such that Jie-Futai with kT_e and proposed scheme with kT_s where $T_s < T_e$. In verification phase $kT_s < nkT_e$ and $2kT_f$ is approximately greater than or equal to nT_f where k £ n. In reconstruction phase both takes same amount of time. Finally the overall complexity of the proposed scheme is approximately equal or less than Jie-Futai VSS but a different methodology is followed by proposed scheme that is more secure in terms of public commitments because they are based on Q rather than P.

VI. Conclusion

AWith the popularity of pairing based cryptography, the use of bilinear groups also has increased tremendously. In all most all of the pairing related protocols, the elements are chosen randomly from the bilinear groups and to share such elements among n participants there is utmost need for verifiable secret sharing schemes over bilinear groups. There exist few such schemes in literature say JieFutai VSS [4] and BeakZheng [5]. In this paper, we proposed an efficient verifiable secret sharing scheme over bilinear groups. We also proved mathematically that the proposed scheme is computationally secure and efficient than the existing similar schemes.

References

[1] Verifiable secret sharing - Wikipedia – https://en.wikipedia.org/wiki/Verifiable_secret_sharing.

[2] Sorin Iftene, "Secret Sharing Schemes with Applications in Security Protocols", Thesis, Alexandru Ioan Cuza, University of Iasi, Romania, October 2006.

[3] Ch. Asha Jyothi, G. Narsimha, J. Prathap, " Two-Party Key Agreement Protocol for MANETs based on Verifiable Secret Sharing Scheme", International Journal of Applied Engineering Research, Volume 10, Number 16 (2015) pp. 36890-36894.

[4] Jie Zhang, Futai Zhang, "Efficient Verifiable Secret Sharing Scheme over Bilinear Groups," Advances in Information Sciences and Service Sciences(AISS) vol. 4, Number 23, pp. 256-264, Dec 2012.

[5] Joonsang Baek, Yuliang Zheng, "Identity-based threshold signature scheme from the bilinear pairings", International Conference on Information and Technology: Coding and Computing, 2004.

[6] Amr Farouk, Ali Miri, Mohamed M. Fouad, Ahmed A. Abdelhafez, "Efficient Pairing-Free, Certificateless Two-Party Authenticated Key Agreement Protocol for Grid Computing," IEEE 2014, pp. 279-284.

[7] P. Feldman, "A Practical Scheme for Non-interactive Verifiable Secret Sharing," In IEEE FOCS'87, 1987, pp. 427-437.

[8] T. P. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," Advances in Cryptology CRYPTO'91, 1991, pp. 129-140.

[9] Hitoshi Asaeda, Musfiq Rahman, Mohammad Hossein Manshaei, Yasuko Fukuzawa, "Implementation of group member authentication protocol in mobile ad-hoc networks," IEEE Wireless Communications and Networking Conference WCNC 2006, pp. 2205 – 2210.

[10] G.R.Blakley,"Safeguarding cryptographic keys," National Computer Conference, vol. 48, 1979, pp. 313-317.