ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

An Efficient (*k/n*) Threshold Secret Sharing with Cheating Detection

Anindya Kumar Biswas

M.Tech. (IT), MAKAUT (Formerly WBUT), Salt Lake, BF-142, Sector-1, Kolkata, India

ABSTRACT: A *k-out-of-n* (*k/n*) threshold secret sharing method is to share a secret among any *k* of *n* participants such that $k \leq n$ and any *k* or more participants can reconstruct the secret from their shares distributed by a trusted dealer. However, there may be some dishonest players who provide fake shares and as a result, only the cheaters would get the real secret while the honest players would get a fake secret. This paper addresses a secret sharing scheme that not only assures correct secret negotiation, but also supports for cheating detection if occurs. For these, Shamir's secret sharing scheme is accompanied with modified Diffie-Hellman key exchange method such a way that the secret in former can be verified against cheating using latter. The proposed modified Diffie-Hellman remain secure under the proposed V-CDH assumption and since Shamir's scheme is information theoretically secure, our secret sharing scheme is secure and provides comparable performance.

KEYWORDS: Shamir's secret sharing, Lagrange interpolation, Diffie-Hellman key exchange, Information theoretic security, CDH assumption.

I. INTRODUCTION

A dealer distributes *n* shares among *n* participants secretly in a *k/n* threshold secret sharing scheme, where the shares are generated using a random (*k-1*)-degree polynomial with coefficients from Z_P^*. The dealer is assumed to be a trusted entity and is responsible for generation and secure distribution of shares. A subset of *n* participants consisting of any *k* members or more in *k/n* scheme can responsibly get the real secret to be shared, however, the number of participants less than *k* have no information about the secret. This model of secret sharing generally consists of two phases called *share generation* and *secret reconstruction*. A dishonest player, however, if present, may hamper the whole intention by providing with a modified share to other participants in a group [3]. This would result in unreal secret generation by honest members but a real secret generation by the miscreants. So, honest players are deprived of their right to get the real secret. Because of the inconsistent shares provided by the dishonest members, cheating easily takes place. To stop the occurrence of such activities of cheating, proper methods must exist to check and detect when occurred.

The *k/n* threshold secret sharing scheme is first proposed by Shamir in [1] and by Blackley independently in [2]. The problem of cheating was first proposed by Tompa and Woll [3], where it is pointed out that Shamir's scheme is not secure against cheating as a single user can cheat other participants by submitting a fake share and a method of detection is also proposed. Several cheating detection protocols have been developed [4, 5, 6, 9] with different features andcapabilities. These papers implement modified Shamir's method with the capability of cheating detection. Harn and Lin's [4] paper also proposed a method of identifying the cheaters. The paper [7] provides a method of cheating detection. The dealer uses *v* number of polynomials. Each polynomial would generate *n* shares, depending on the number of participants. So, in total there are *nv* shares to be distributed. This method has achieved fairness in secret sharing, but it is highly complex at both the dealer's end and receiver's end.

A linear (*k/n*) threshold secret sharing scheme (SSS) based on Shamir's scheme is proposed by Liu-Wang-Yan [11]. It is shown that the scheme is capable of detecting at most *(t-1)* cheaters. The scheme of Liu-Wang-Yan uses two polynomials for generating two shares per participant and two linear equations with a common unknown for cheating detection. A publicly verifiable secret sharing (PVSS) scheme for (*k/n*) threshold based on multilinear Diffie-Hellman assumption is presented by Q. Peng et al. [12]. The secret in this scheme is shared and reconstructed using multiple linear pairing. It uses batch verification for participants' shares, thus effective in computation and communication over others in terms of security level considered. On performance analysis, it is claimed by authors that the scheme is publicly verifiable, secure and useful for different applications.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

The present work on secret sharing with cheating detection is simple and effective as two existing well known/simpler secret negotiation schemes namely Shamir's and Diffie-Hellman's schemes have been used. In brief, after reconstruction of secret using Shamir's method, a modified Diffie-Hellman technique is used for verification and cheating detection of the secret negotiated. For this, two public messages based on Diffie-Hellman, which are broadcasted to all participants along with their secret shares, are used. The rest of the paper is organized as follows. In Section II, the basic concepts of Shamir's scheme and Diffie-Hellman technique are discussed.

II. PRELIMINARIES

Some backgrounds over two well-known key exchange techniques that are incorporated in our work are presented in this section. In 1979, A. Shamir, a pioneer cryptographer and mathematician, used a (*k-1*)-degree polynomial for generating $n \geq k$ shares and reconstructed the same polynomial (and hence, the secret from *k* or more shares) using Lagrange Interpolation. In Shamir's (*k/n*) secret sharing scheme, a trusted dealer considers a random polynomial of degree (*k-1*), generates *n* shares and distributes secretly to all *n* participants. At least any *k* of *n* participants can reconstruct the secret (the constant term of the polynomial) by combining their shares using Lagrange interpolation. It has two phases and they are *share generation* and *secret reconstruction* as described below:

(1) *Share generation phase*: A dealer chooses $f_1, f_2 \ldots f_{k-1} \in Z_P^*$ for the coefficients of a (*k-1*) degree polynomial as $f(z) = f_0 + f_1 * z + \ldots + f_{k-1} * z^{k-1}$, where $f(0) = f_0 = s \in Z_P^*$ be secret to be shared among any *k* participants. The dealer now generates and distributes the shares (i, f(i)) to *n* participants secretly for $i = 1, 2, 3, \ldots, n$.

(2) *Secret reconstruction phase*: Each party *i* receives his/her share *f(i)* and after exchanges among any other (*k-1*) parties secretly, uses Lagrange's interpolation over *k* shares to reconstruct *f(z)* as

$$f(z) = \sum_{i=1 \text{ to } k} f(i) \prod_{j \neq i} \frac{z-j}{i-j}$$

The constant term of f(z), i.e, f(0) is taken as the secret s negotiated among k parties. The scheme is information theoretically secure. Some of the useful properties of Shamir's threshold scheme [9] are:

(1) *Secure*: Information theoretically secure (without any hard assumption)
(2) *Minimal:* The size of each share does not exceed the size of data, i.e.,
(3) *Extensible:* The threshold *k* is kept fixed; however, secret shares can be added or deleted without affecting the others.
(4) *Dynamic:* Security can be enhanced easily without changing the secret and
Flexible: In organizations, each participant can be supplied with different number of shares according to their importance/hierarchies inside the organization.

In 1976, two famous cryptographers, W. Diffie and M.E. Hellman, proposed a public method of generating a shared private key between two remote participants [8]. It is known as Diffie-Hellman key exchange protocol, which is briefly introduced below. Let *X* and *Y* be two participants. After negotiating a large prime number *P* and a generator *g* for a cyclic multiplicative group of order *P*, they exchange two messages publicly as follows:

(1) *X* randomly selects $a \in Z_P^*$ and sends $A = g^a \bmod P$ to *Y*
(2) *Y* randomly selects $b \in Z_P^*$ and sends $B = g^b \bmod P$ to *X*

Both the participants independently computes a secret key $K = B^a \pmod P = g^{ab} \pmod P$ [$K = A^b \pmod P = g^{ab} \pmod P$)] and thus, the secret *K* is negotiated among *X* and *Y*. The security of this scheme depend on the hardness of Diffie-Hellman problem (CDH).

III. PROPOSED SECRET SHARING SCHEME

Similar to Shamir's scheme, our secret sharing scheme has two parts— (1) Share generation and (2) Secret reconstruction. However, one additional part called cheating detection is included for detection of cheating if some of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

the dishonest participants provide fake shares during secret reconstruction. For this, the proposed work uses both Shamir's and Diffie-Hellman's schemes with some modifications, which are addressed now. In case of Diffie-Hellman

we propose the following:

(1) X (or Y) assumes $a, b \in Z_P^*$ and calculates $K = g^{ab} \pmod P$
(2) X (or Y) transmits the tuple (g^a, K) to Y (or X)
(3) Assume Y (or X) knows b by any other means, thus, the verification of K by Y (or X) can be done using g^aas $K = (g^a)^b \pmod P$ and hence, the verification of b is also established.

The proposed modification of Diffie-Hellman as mentioned above is secured based on a variation of Computational Diffie-Hellman (CDH) assumption called V-CDH (Variation of CDH). CDH assumption is stated below:

Computational Diffie-Hellman (CDH) assumption: Consider a multiplicative group of order P, with generator g. A probabilistic polynomial-time adversary has a negligible probability of computing g^{xy} from the tuple (g, g^a, g^b) for random $a, b \in Z_P^*$.

V-CDH assumption, which is proposed by us, is stated as follows:

V-CDH assumption: A probabilistic polynomial-time adversary has a negligible probability of computing g^b(and b) from g, g^a, g^{ab} for random $a, b \in Z_P^*$, where a large prime P forms a cyclic multiplicative group with a generator g.

On the other hand, the modification of Shamir's secret sharing scheme is done as follows:

(1) Although a dealer randomly selects a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$, where $a_i \in Z_P^*$ for $i = 1 \ldots n$, the secret $s = f(0) = a_0 \in Z_P^*$ is selected in such a way that $(g^a)^{a_0} \bmod P = K$.
(2) In addition to generation of n shares $(i, f(i))$, the dealer also computes a key $K = (g^a)^{a_0} \bmod P$ for a random $a \in Z_P^*$.

Now, the proposed secret sharing scheme with cheating detection is described below:

(1) *Share generation and distribution phase*: Initially, a trusted dealer considers two random numbers $a, a_0 \in Z_P^*$ and calculates a key $K = g^{aa_0} \bmod P$. He/she then selects a random polynomial $f(x)$ with a_0 as the secret and generate shares $(i, f(i))$ for n participants. These shares are secretly distributed, however, the tuple $(g, g^a, K = g^{aa_0})$ are openly broadcasted as a single message to all n participants.
(2) *Secret reconstruction phase:* In this phase, any k out of n participants secretly exchange their shares among them and a polynomial $f'(x)$ (say) is constructed by each of them using the Lagrange interpolation.
(3) *Cheating detection phase:* Each participant of the k-member group computes $K' = (g^a)^{a_0'} \bmod P$ and compares with K. If they are equal, the secret $s = a_0 = f(0) = a_0'$ is correctly negotiated; otherwise cheating has occurred and a_0' is cancelled.

IV. SECURITY AND PERFORMANCE ANALYSIS

The proposed secret sharing scheme is based two existing secure cryptosystems namely Shamir's and Diffie-Hellman's methods, and thus, our scheme is secure. We know that Shamir's scheme is information theoretically secure as it satisfies the following two conditions:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

(1) For any *k*-tuple of distinct indexes $i_1, i_2, \cdots, i_k, 1 \le i_j \le n$, the entropy $H\left(S \middle| D_{i_1}, D_{i_2}, \cdots, D_{i_k}\right) = 0$, where D_1, D_2, $\cdots$, D_n be the sets in which shares to *n* participants are taken and S be a set of secrets corresponding to Z_P^*.

(2) For any $j < k$, for any *j*-tuple of distinct indexes $i_1, i_2, \cdots, i_j, 1 \le i_j \le n$, the entropy $H\left(S \middle| D_{i_1}, D_{i_2}, \cdots, D_{i_j}\right) = H(S)$.

On the other hand, Diffie-Hellman key exchange protocol is also secure as the underlying DHP (Diffie-Hellman Problem) and DLP (Discrete Logarithm Problem) are hard. Both the problems are stated below:

DHP: No polynomial time algorithm exists for computing $g^{ab} \pmod P$ from the tuple (g^a, g^b).
DLP: No polynomial time algorithm exist for computing a or b from g^a or g^b, respectively.

Since the solution of DHP depends on the solution of DLP, the security of Diffie-Hellman protocol depends on the DLP. Since our V-CDH assumption is hard, the proposed modification of Diffie-Hellman is also secure. However, the public messages (K, g^a) sent over open channel may be modified by attacker(s), and thus, they must be transmitted through an authenticated channel for providing overall security of our secret sharing scheme. Although our scheme is based on both information theoretic and hard assumption, the secret sharing is purely information theoretic and thus, in terms of security, it is equivalent to Shamir's scheme. In addition, our scheme satisfies all the properties of Shamir's scheme except for the share-size, which is *3* times larger than the share-size in Shamir's scheme. However, this overhead is compensated by incorporating cheating detection facility in our scheme.

V. CONCLUSION

A secret sharing scheme with cheating detection is proposed. It uses Shamir's scheme for secret negotiation among any *k*-member group, however, the cheating detection has been incorporated using modified Diffie-Hellman key exchange technique. Our scheme is secure and correctly detects the cheating provided the Diffie-Hellman public messages are authentically transmitted to the participants. The performance of the proposed scheme is comparable with Shamir's one, however, it requires three times more share-size for detection of cheating.

REFERENCES

1. Shamir, "How to Share a Secret", Communications of ACM, 22: 612-613, 1979.
2. G.R. Blakley, "Safeguarding cryptographic keys", In Proceedings of AFIPS'79, vol. 48, pp.313-31(1979).
3. M. Tompa and H. Woll, "How to share a secret with cheaters", Journal of Cryptology, vol.1, pp. 133-138, 1989.
4. L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme", Designs, Codes and Cryptography, vol. 52, pp. 15-24, 2009.
5. S. Obana, "Almost optimum t-cheater identifiable secret sharing schemes", vol. 6632, LNIC Science, pp. 284-302, Springer, 2011.
6. Y. Liu, Z. Wang and W. Yan, "Linear (k, n) secret sharing scheme with cheating detection", Ubiquitous Computing and Communications, IEEE Computer Society, pp. 1942-1947, 2015.
7. Youliang Tian, Jianfeng Ma, Changgen Peng, Qi Jiang, "Fair (t, n) threshold secret sharing scheme", IET Inf. Secure, 2013, Vol. 7, Iss. 2, pp. 106–112, 2012.
8. Whitefield Diffie and Martin E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, NO. 6, November 1976.
9. S. O. A. T. Araki, "Almost Optimum Secret Sharing Schemes Secure Against Cheating for Arbitrary Secret Distribution", Advances in Cryptology ASIACRYPT, 2006.
10. Mahalaxmi et al., "International Journal of Innovative Research in Computer and Communication Engineering", ISSN(Online): 2320-9801, 2014.
11. Y. Liu, Z. Wang and W. Yan, 'Linear (k, n) secret sharing scheme with cheating detection,' Ubiquitous Computing and Communications, IEEE Computer Society, pp. 1942-1947, 2015.
12. Q. Peng and Y. Tian, 'A publicly verifiable secret sharing scheme based on multilinear Diffie-Hellman assumption,' International Journal of Network Security, vol. 18, no. 6, pp. 1192-1200, 2016.

BIOGRAPHY

Anindya Kumar Biswas is a student and researcher in the Information Technology Department, Maulana Abul Kalam Azad University of Technology (formerly WBUT), Govt. of West Bengal. He received Bachelor of Technology (B.Tech) degree in 2015 in Computer Science and Engineering. His research interests are Computer Networks (wireless Networks), cryptography, manets, image processing etc