Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1037

안전한 채널이 없는 검증 가능한 다중 비밀 공유 방식

김 호 희[†‡]
경북대학교

A Verifiable Secret Sharing Scheme with no Secure Channels

Ho-hee Kim[†‡]
Kyungpook National University

요 약

(t,n) 임계 비밀 공유 방식은 한 신뢰 기관이 n명의 참가자에게 각 할당 값를 나누어 주면 이 중 t명의 참가자들의 할당 값으로 비밀 값을 계산하는 방식이다. 최근 Eslami 등과 Tadayon 등은 한 임계 검증 가능한 다중 비밀 공유 방식을 각각 제안 했는데, 그들의 방식이 안전한 채널을 사용하지 않는다고 했으나, 안전한 채널이 없다면 누구나 할당 값을 가질 수 있고 비밀 값을 구할 수 있다. 본 논문에서 제안된 방식은 안전한 채널을 사용하지 않고, 전송된 메시지로부터 t명의 컴바이너들만 필요한 값을 구해 시스템의 방정식을 풀 수 있고 비밀 값들을 구할 수 있다.

ABSTRACT

A (t,n) threshold secret sharing scheme is the scheme which allows a trusted party to distribute the shares among n participants in such a way that any t of them can recover the original secret, but any group knowing only $t-1$ or fewer shares can not. Recently, Eslami et al. and Tadayon et al. proposed threshold multi-secret sharing schemes, respectively. They proposed that their schemes don't require secure channels. But, without secure channels in their schemes, everyone can get the shares and find the secrets. The proposed scheme does not use secure channels and only t participants can solve the equations of the system from the delivered share shadows and find the secrets.

Keywords: Verifiable multi-secret sharing, Bilinear Maps

I. Introduction

Secret sharing schemes are cryptographic procedures to share a secret among a set of participants such that only authorized subsets can recover the secret. Such schemes were independently introduced by Shamir[1] and Blakley[2] to safeguard cryptographic keys from loss. Recently, secret sharing schemes have found applications in diverse areas such as access control systems, e-voting schemes and digital cash protocols.

The (t,n)-threshold secret sharing scheme which allows a trusted party(called the dealer) to distribute the shares among n participants in such a way that any t of them can recover the original secret, but any group knowing only $t-1$ or fewer shares can not. Shamir's scheme, which is based on polynomial interpolation, and Blakley's scheme, based on the intersection

접수일(2014년 7월 28일), 수정일(1차: 2014년 10월 13일, 2차: 2014년 11월 26일), 게재확정일(2014년 11월 26일)
† 주저자, brtcloud@naver.com
‡ 교신저자, brtcloud@naver.com(Corresponding author)

of affine hyperplanes, are examples of such schemes.

Chor *et* al.[3] proposed a verifiable secret sharing scheme. He and Dawson[4] proposed a multi-secret sharing scheme (MSS) where several secrets can be shared. A verifiable multi-secret sharing scheme (VMSS) can verify the validity of the shares.

Elliptic curves and bilinear maps have been used in providing the verifiability [5-9]. Shi *et* al.[5] proposed a multi-secret sharing scheme based on the signed factorial expansion, where the secret information and the shares are delivered over secure channels. Chen *et* al.[6] proposed a threshold secret sharing scheme, where the participants can compute the shares by the public value over the public bulletin. But, a secure channel is used in the secret reconstruction phase. Wang *et* al.[7] proposed a verifiable threshold multi-secret sharing scheme, where a secure channel is used, too.

Recently, Eslami *et* al.[8] modified Wang *et* al.'s scheme and proposed a threshold multi-secret sharing scheme. They proposed that their scheme does not require a secure channel. But, without secure channels in their scheme, everyone can get the shares and find the secrets. Only t participants must be able to find the secrets. Tadayon *et* al.[9] proposed a verifiable multi-secret sharing scheme. They also proposed that their scheme does not need a secure channel. Their proposition is incorrect for the same reason as Eslami *et* al.'s scheme. Dong *et* al.[10] proposed a multi-secret sharing scheme based on general linear groups, where a secure channel between the dealer and participant is no longer needed. But a secure channel is still used in secret reconstruction phase. Though many secret sharing schemes do not use secure channels between the dealer and the participants, they use impractical secure channels among t participants in the secret reconstruction phase. However, the proposed scheme does not require a secure channel in all phases and only t participants can solve the equations of the system from the delivered share shadows and find the secrets.

II. Technical Backgrounds

2.1 Elliptic Curve

Let p be a prime number. An elliptic curve over $GF(p)$ (finite field with p elements) is the set of solutions $(x,y) \in GF(p) \times GF(p)$ of the equation $y^2 \equiv x^3 + ax + b \bmod p$ such that $a,b \in GF(p)$ are constants with $4a^3 + 27b^2 \neq 0 \bmod p$ (together with a point o that is named point at infinity).

The above set with a particular operator "+" forms an abelian group of order q denoted by $E(GF(p))$ and called an elliptic curve group[11].

2.2 Discrete Logarithm problem on Elliptic Curves

Given $P,Q \in E(GF(p))$ such that $kP = Q$ there is no polynomial time algorithm to determine k[11].

2.3 Bilinear Maps

Let G_1 be an additive group generated by P, whose order is a prime q, and G_2 be a multiplicative group of the same order q. Let $e : G_1 \times G_1 \rightarrow G_2$ be a mapping which satisfies the following properties:

1. Bilinear :
$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$,

$e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$,
$e(aP,bQ)=e(P,Q)^{ab}$ where $a,b\in Z_q^*, P,Q\in G_1$.

2. Non-degenerate : There exists $P\in G_1$ such that $e(P,P)\neq 1$.

3. Computability : There is an efficient algorithm to compute $e(P,Q)$ for all $P,Q\in G_1$.

III. Review Of Chen *et al.*'s Scheme

They proposed a dynamic threshold secret sharing scheme[6] using bilinear maps.

Table 1. shows the notations used in this paper.

Table 1. The notations

n	The number of the participants
m	The number of the secrets
q	Prime number
G_1, G_2	Two cyclic groups with prime order q
P	A generator G_1
e	$e: G_1\times G_1\rightarrow G_2$, a bilinear map
$h()$	Hash function, $h: G_1\rightarrow Z_q^*$
t	The threshold
g	A generator, $g\in Z_q^*$

3.1 Initialization Phase

The dealer publishes $\langle q, G_1, G_2, P, e, h\rangle$ on the bulletin. A participant $U_i(1\leq i\leq n)$ picks a random integer $r_i\in Z_q^*$ and submits $P_i=r_iP$ to the dealer. The dealer ensures that $P_i\neq P_j$ where $i\neq j$ in order to keep different participants from using the same secret key and publishes $P_i(1\leq i\leq n)$ on the bulletin.

3.2 Secret Distribution Phase

In this phase, the dealer

1. Picks a random integer $r\in Z_q^*$ and computes the shared secret $s=h(rP)$ and publishes sP on the bulletin.

2. Constructs the matrix $M_{(n+1-t)\times(n+1)}$:

$$M=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & g & \cdots & g^n\\ \vdots & \vdots & \ddots & \vdots\\ 1 & g^{n-t} & \cdots & g^{(n-t)n}\end{bmatrix} \quad (1)$$

3. Constructs the column vector matrix A with the secret:

$$A=[rP, sP_1, sP_2, \ldots, sP_n]^T.$$

4. Publishes $\langle g, C_0, \ldots, C_{n-t}\rangle$ where

$$MA=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & g & \cdots & g^n\\ \vdots & \vdots & \ddots & \vdots\\ 1 & g^{n-t} & \cdots & g^{(n-t)n}\end{bmatrix}\begin{bmatrix}rP\\ sr_1P\\ \vdots\\ sr_nP\end{bmatrix}=\begin{bmatrix}C_0\\ C_1\\ \vdots\\ C_{n-t}\end{bmatrix} \quad (2)$$

3.3 Secret Reconstruction and Verification Phase

The system (2) is a system of $n+1-t$ linear equations in $n+1$ unknowns over G_1. If t-out-of-n participants provide their r_isP, the other $n+1-t$ variables could be recovered, including rP. Therefore, the secret s can be obtained by $s=h(rP)$.

1. $U_i(1\leq i\leq t)$ computes r_isP and securely delivers r_isP to the combiner(one of the participants).

Here, note that secure channels are used among t participants.

2. The combiner receives r_isP and checks if $e(r_isP,P)=e(sP,r_iP)$. This ensures the verifiability of the shares.

3. The combiner can solve the system (2) and can find rP and the secret s.

3.4 Secrets Redistribution Phase

The dealer chooses a new threshold t', a new secret s', and computes new auxiliary information from participants' public keys. Then, the dealer publishes the new information on the bulletin.

IV. Review Of Eslami *et al.*'s Scheme

They proposed a verifiable dynamic threshold multi-secret sharing scheme[8] using bilinear maps.

4.1 Initialization Phase

This phase is same as Chen *et al.*'s scheme. The dealer publishes $\langle q, G_1, G_2, P, e, h\rangle$. A participant $U_i (1 \le i \le n)$ picks a random integer $r_i \in Z_q^*$ and submits $P_i = r_i P$ to the dealer. The dealer publishes P_i and a generator $g \in Z_q^*$ on the bulletin.

4.2 Secret Distribution Phase

In this phase, the dealer

1. Picks a random integer $s \in Z_q^*$ and publishes sP.
2. Constructs the matrix $M_{(n+m-t)\times(n+m)}$:

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{n+m-t-1} & \cdots & g^{(n+m-t-1)(n+m-1)} \end{bmatrix} \quad (3)$$

Note that the matrix M of Chen *et al.*'s can be constructed by setting $m=1$:

3. Computes sP_i together with $h(sP_i)$ and constructs the matrix A with the secrets K_i $(1 \le i \le m)$:

$$A = [h(sP_1), h(sP_2), \ldots, h(sP_n), K_1, \ldots, K_m]^T.$$

4. Publishes $\langle sP, C_1, \ldots, C_{n+m-t}\rangle$ where

$$MA = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{n+m-t-1} & \cdots & g^{(n+m-t-1)(n+m-1)} \end{bmatrix} \begin{bmatrix} h(sP_1) \\ \vdots \\ h(sP_n) \\ K_1 \\ \vdots \\ K_m \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_{n+m-t} \end{bmatrix} \quad (4)$$

4.3 Secret Reconstruction and Verification Phase

Note that (4) is a system of $n+m-t$ linear equations in $n+m$ unknowns over G_2. Therefore, if t of the unknowns of (4) are determined, the system of $n+m-t$ equations and $n+m-t$ unknowns can be solved to recover the m secrets.

Let t participants $U_i (1 \le i \le t)$ pool their shares. When the combiner receives $r_i sP$, s/he checks whether $e(r_i sP, P) = e(sP, r_i P)$. This ensures the verifiability of the shares.

Here, Eslami *et* al. proposed that their scheme does not require a secure channel. But, without secure channels in their scheme, everyone can get $r_i sP$ and compute $h(r_i sP)$ and can find the secrets.

Therefore, their scheme needs secure channels.

4.4 Secret Redistribution Phase

The dealer chooses a new threshold t', new m' secrets, and the new seed s'. And then proceeds as secrets distribution phase and finally publishes $\langle s'P, C_1', \ldots, C'_{n+m'-t'}\rangle$. They told that their scheme does not need to reconstruct the coefficient matrix (4) and only adds or removes some of its rows and columns.

V. Review Of Tadayon *et al.*'s Scheme

They proposed a verifiable multi-secret sharing scheme[9] using elliptic curve and Lagrange interpolation.

5.1 Initialization Phase

The dealer publishes $\langle q, G_1, G_2, P, e, h \rangle$. A participant $U_i (1 \le i \le n)$ picks a random integer $r_i \in Z_q^*$ and submits $P_i = r_i P$ to the dealer. The dealer publishes P_i on the bulletin.

5.2 Secret Distribution Phase

In this phase, the dealer

1. Picks a random integer $s \in Z_q^*$ and publishes sP.

2. Computes $R_i' = sr_i P$ $(1 \le i \le n)$.

3. Constructs polynomial $f_j(x)$ of degree $(j\text{-}1)$ $(1 \le j \le k)$ as follows:

$$f_j(x) = K_j + d_1 x + d_2 x^2 + \ldots + d_{j-1} x^{j-1} \bmod p.$$

The m secrets K_j are constructed.

4. Computes $V_{ji} = f_j(ID_i)$, ID_i are public identities of the participants. And then, computes $M_{ji} = V_{ji} - h^j(R_i')$ $(1 \le i \le n, 1 \le j \le k)$.

5. Publishes M_{ji} on the public bulletin.

5.3 Secret Reconstruction and Verification Phase

To recover the l th secret, $U_j (1 \le j \le l)$ should do the following steps respectively:

1. Computes $R_j' = r_j sP$ and sends it. When the combiner receives R_j', s/he checks whether $e(r_j sP, P) = e(sP, r_j P)$. This ensures the verifiability of the shares.

2. The combiner computes $V_{lj} = M_{lj} + h(R_j')$ using R_j' and public value M_{lj}.

3. The combiner computes the secret K_l using Lagrange formula:

$$K_l = \sum_{j=1}^{l} V_{lj} \prod_{r=1, r \ne j}^{l} \frac{0 - ID_r}{ID_j - ID_r} \bmod p$$

Here, Tadayon et al. proposed that their scheme does not need a secure channel. But without secure channels, everyone can get R_j' and compute V_{lj} using public value M_{lj}. Finally, everyone can find the secret K_l using public values ID and p. Therefore, their scheme needs secure channels.

5.4 Secret Redistribution Phase

The dealer chooses new values for new secrets, and constructs new polynomials and then chooses new value $s \in Z_q^*$ and refreshes the value R_i' and computes new values for M_{ji} $(1 \le i \le n, 1 \le j \le k)$.

VI. The proposed scheme

The proposed scheme is a verifiable (t,n) threshold multi-secret sharing scheme, which does not use secure channels.

6.1 Initialization Phase

The dealer selects an elliptic curve E defined over $GF(p)$ with order q and a base point P. And then, publishes system parameters $\langle G_1, G_2, P, q, e, h \rangle$. A participant U_i $(1 \le i \le n)$ picks a random integer $r_i \in Z_q^*$ and submits $r_i P$ and $r_i^{-1} P$ to the dealer.

6.2 Secret Distribution Phase

In this phase, the dealer

1. Chooses $s \in Z_q^*$ and computes sP and computes $sr_i P$ and $sr_i^{-1} P$ and publishes sP,

r_iP and $sr_i^{-1}P$ on the public bulletin.

2. Constructs the column vector matrix A with the secrets $K_i \in Z_q^*(1 \le i \le m)$:

$$A = [h(sr_1P), h(sr_2P), \ldots, h(sr_nP), K_1, \ldots, K_m]^T$$

3. Chooses the threshold t, randomly selects a generator $g \in Z_q^*$ and constructs the matrix $M_{(n+m-t)\times(n+m)}$:

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{n+m-t-1} & \cdots & g^{(n+m-t-1)(n+m-1)} \end{bmatrix} \quad (5)$$

4. Publishes $\langle g, C_1, \ldots, C_{n+m-t} \rangle$ where

$$MA = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & g & \cdots & g^{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{n+m-t-1} & \cdots & g^{(n+m-t-1)(n+m-1)} \end{bmatrix} \begin{bmatrix} h(sr_1P) \\ \vdots \\ h(sr_nP) \\ K_1 \\ \vdots \\ K_m \end{bmatrix}$$

$$= \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_{n+m-t} \end{bmatrix} \quad (6)$$

6.3 Secret Reconstruction and Verification Phase

1. $U_i(1 \le i \le t)$ computes $r_i sr_j^{-1}P$ $(1 \le j \le t, i \ne j)$ by multiplying the public value $sr_j^{-1}P$ by r_i. And then, U_i delivers it to the combiner U_j.

2. When the combiner U_j receives $r_i sr_j^{-1}P$, s/he checks whether $e(r_i sr_j^{-1}P, P) = e(r_iP, sr_j^{-1}P)$, using the public values r_iP and $sr_j^{-1}P$. This ensures the verifiability of the shares from U_i.

3. Then, U_j multiplies $r_i sr_j^{-1}P$ by r_j and finally finds sr_iP.

Here, because of no secure channels, everyone can get $r_i sr_j^{-1}P$ but the only U_j knowing r_j can find sr_iP from $r_i sr_j^{-1}P$.

Like Eslami *et* al.'s scheme, if t of the unknowns of (6) are determined, the system of $n+m-t$ equations and $n+m-t$ unknowns can be solved to recover K_i $(1 \le i \le m)$. M is a Vandermonde matrix on distinct elements. Therefore, det(M)≠0 and its inverse can be computed to obtain the secrets. Thus, only t participants can solve the equations of the system and find the secrets K_i with no secure channels.

6.4 Secret Redistribution Phase

This phase is same as Eslami *et* al.'s scheme.

VII. Security and Discussion

1. The dealer can not cheat the public values.: Each participant $U_i(1 \le i \le n)$ submits r_iP and $r_i^{-1}P$ to the dealer. The dealer does not know r_i and r_i^{-1}. And then, the dealer publishes sP, r_iP and $sr_i^{-1}P$ on the public bulletin. U_i can verify r_iP and $sr_i^{-1}P$ by multiplying P by r_i and multiplying sP by r_i^{-1}.

2. A participant can not change his share and send another value to the combiners. : When U_i $(1 \le i \le t)$ delivers $r_i sr_j^{-1}P$ $(1 \le j \le t, i \ne j)$ to the combiners, no one can extract $r_i sr_j^{-1}$ from $r_i sr_j^{-1}P$, due to the elliptic curve discrete logarithm problem(ECDLP). The shares provided by participants during the reconstruction phase can be verified so that cheaters are identified by checking $e(r_i sr_j^{-1}P, P) = e(r_iP, sr_j^{-1}P)$ using the public values r_iP and $sr_j^{-1}P$. This ensures the verifiability of the shares from U_i.

3. The proposed scheme does not require secure channels.: Everyone can get $r_i sr_j^{-1}P$ and verify it. When $U_i(1 \le i \le t)$ provides

$r_i sr_j^{-1}P$ $(1 \le j \le t, i \ne j)$ to U_j with no secure channels, only U_j knowing r_j can find sr_iP from $r_i sr_j^{-1}P$ by multiplying $r_i sr_j^{-1}P$ by r_j. Then, (6) is reduced to a system of $n+m-t$ equations and $n+m-t$ unknowns with coefficient matrix M. Thus, only t participants are able to find the secrets.

Table 2. shows the comparison with Eslami *et* al.'s and Tadayon *et* al.'s. $k(>m)$ means the number of polynomials.

The proposed scheme with no secure channels requires more public values than Eslami *et* al.'s and less than Tadayon *et* al.'s.

Table 2. Comparison with Eslami *et al.*'s and Tadayon *et al.*'s

	Eslami *et al.*'s scheme	Tadayon *et al.*'s scheme	The proposed scheme
Secure channel	necessary	necessary	not necessary
Public values	$2n+2+m-t$	$(k+2)n+1$	$3n+2+m-t$
Verifiab-ility	Yes	Yes	Yes

VIII. Conclusion

This paper presents a verifiable (t,n) threshold multi-secret sharing scheme, which does not need impractical secure channels. With no secure channels, the shares can be delivered to the only combiners. Thus, only t participants are able to find the secrets.

References

[1] A. Shamir, "How to share a secret," *Communication of the ACM*, vol. 22, no.11, pp. 612 - 613, Nov. 1979.

[2] G. Blakley, "Safeguarding crypto- graphic keys," *AFIPS Conference Proceedings*, 48, pp. 313 - 317, 1979.

[3] B. Chor and S. Goldwasser, "Verifiable Secret Sharing and achieving simultaneity in the presence of faults," *Proc. of 26th IEEE Symposium. FOCS*, pp. 383-395, Oct. 1985.

[4] J. He and E. Dawson, "Multistage secret sharing based on one-way function," Electronics Letters, vol.31, no. 19, pp. 1591-1592, Sep. 1994.

[5] R. Shi, H. Zhong and L. Huang, "A (t,n)-Threshold Verified Multi-secret Sharing Scheme based on ECDLP," *8th ACIS International Conference*, vol. 2, pp. 9-13, July 2007.

[6] W. Chen, L. Xiang, B. Yuebin and G. Xiaopeng, "A New Dynamic threshold Secret sharing Scheme from bilinear Maps," *International Conference on Parallel Processing Workshops*, pp. 19-22, Sep. 2007.

[7] S. J. Wang, Y. R. Tsai, and J. J. Shen, "Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ecc," *Wireless Personal Communications*, Springer, vol. 56, no.1, pp. 173 - 182, Jan. 2011.

[8] Z. Eslami and K. Rad, "A New Verifiable Multi-secret sharing Scheme Based on Bilinear Maps," *Wireless Personal Communications*, Springer, vol. 63, no. 2, pp. 459-467, March 2012.

[9] M. H. Tadayon, H. Khanmohammadi, and S. Arabi, "An attack on a dynamic multi-secret sharing scheme and enhancing its security," Electrical Engineering (ICEE), 21st Iranian Conference, pp. 1-5, May 2013.

[10] X. Dong and Y. Zhang, "A Multi-secret sharing scheme based on general linear groups," 3rd International Conference on Information Science and Technology, pp. 480-483, March 2013.

[11] D. R. Stinson, *Cryptography Theory And Practice*, CRC press, 2006.

〈저자소개〉

김 호 희 (Ho-hee Kim) 정회원
1993년 2월: 경북대학교 전자공학과 졸업
1996년 2월: 경북대학교 전자공학과 석사
2013년 8월: 경북대학교 전자공학과 박사졸업
〈관심분야〉 정보보호, 전자공학