참가자에게 노출되지 않는 k-생성 비밀분산방식

박 택 진† · 원 동 호††

요 약

비밀분산방식에서, 재구성된 비밀은 참가자에게 노출된다. 동일한 비밀분산 방식을 유지하 기위해서, 새로운 비밀을 생성하고 참가자에게 재분배 하여야 한다. 그러한 재생성과정은 비효율적이다. 본 논문은 참가자에게 노출 되지 않고 고유치에 의해 효율적인 비밀 재생성과 재분배 할 수 있는 방식을 제안한다.

A k-Span Secret Sharing Scheme with Exposing Forged Shadows

Taek-jin Park† · Dong-ho Won††

ABSTRACT

In the secret sharing scheme, the reconstruction secret must to exposed to participants. In order to enforce the same secret sharing schemes, a new secret have to regenerate and redistribute for participants. Such a regeneration process is inefficient because of the overhead in the regeneration. In this paper, we proposed efficient secret regeneration scheme by eigenvalue. it can be also redistribution without revealing with other participants.

키워드 : k-생성 비밀분산 방식(k-Span Secret Sharing Scheme), 위조된 비밀(Forged Shadow), 재생성(Regeneration), 마스터 키 (Master Key), 고유치(Eigenvalue)

1. Introduction

The concept of secret sharing scheme was introduced independently, in 1979, Blackly [1] and Shamir [2]. A secret sharing scheme have a secret to be shared among participants. A (t, n) secret sharing scheme is a method that divides secret into n shares for n participants, such that the secret can be obtain by at least t qualified participants, while less than t participants cannot take any information about the secret. In this paper, we present a k-span secret sharing scheme with exposing forged shadows. Our work tries to solve the secret regeneration problem. One previous work can be found in Dynamic Threshold Scheme [4], but the threshold value is decreased in proportion the number of different secrets which have been revealed. Another previous work is an l-span generalized secret sharing scheme which is proposed by Lein and Hung-Yu Lin [5]. It is impossible to detect unhonest shadowholders. The main idea in our scheme is that master key vector is available for eigenvalue parameter λ^k and it is the n shadows forms an orthogonal subset in the $n+1$ dimensional space and then master key is hidden in the master key vector which is orthogonal with the n shadows subspace [3]. With public $n+1-m$ component of the master key vector space, any m shadows can recover the master key vector and the master key. However, if less than $t(<m)$shadows are forged, it can be used to detect the forged shadows with a very high probability. A k-span secret sharing scheme is proposed to solve the secret regeneration problem by eigenvalue from 1 to k. The shadows can be repeatedly used for k times to generate k differ-

† 정 회 원 : 강릉영동대학 전자정보과 교수
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2003년 4월 8일, 심사완료 : 2004년 7월 28일

ent secrets.

2. Eigenvector and its properties

In order to describe how the proposed scheme works, we give some definitions and theorems in this section [6]. we use these theorem without proof.

[Definition 1] Given a set S of possible secret, a (t, n)-threshold scheme on S is a method of diving each $s_i \in S$ into vector of shares $[s_1, s_2, \cdots, s_n]$ with each such that $s_i \in S$

① Given any set of t or more of the s_i, the secret value s is easily reconstructible.

② Given any set of fewer than t of the s_i, the secret value s is completely undetermined in an information theoretic sense.

[Definition 2] For given threshold scheme, we use eigenvalue λ_j^k, $2 \le j \le n+1$, $k=1,2,\cdots$ and corresponding eigenvectors $\{U_0^i\}$, $1 \le i \le n+1$, to denote the random function which assigns shares $[s_1, s_2, \cdots, s_n]$ of secret value s to participants $p_1, p_2, \cdots, p_n$.

[Definition 3]

Let A be an $(n \times n)$ matrix, A non-zero vector like as

$$(A - \lambda I)^j u = 0$$
$$(A - \lambda I)^{j-i} u \neq 0$$

where I : unit matrix.

is called generalized eigenvector of order j corresponding to λ.

[Theorem 1]

Let A be an $(n \times n)$ matrix, and λ be an eigenvalue of A. Then.

λ^k is an eigenvalue of A^k, $k=2,3,\cdots$

[Theorem 2]

an $(n \times n)$ matrix A is diagonalizable if and only if A possesses a set of n linearly independent eigenvectors.

[Corollary 1]

Let A be an $(n \times n)$ matrix. If A has n distinct eigenvalues, then A has a set of n linearly independent eigenvectors.

[Theorem 3] Let U be an n-dimensional vector space. A linear transformation $L : U \rightarrow U$ is diagonalizable if only if there exists a basis for U consisting of eigenvectors for L

Consider the sequence $\{U_k\}$ define by

$$U_1 = LU_0$$
$$U_2 = LU_1$$
$$U_3 = LU_2$$
$$\vdots$$

In general, this sequence is given by

$$U_k = LU_{k-1} \quad k=1,2,\cdots$$

[Theorem 4] Gram-Schmit Process Let W be a p-dimensional subspace of R^n, and let $\{w_1, w_2, \cdots, w_p\}$ be any basis for W. Then the set of vectors $\{u_1, u_2, \cdots, u_p\}$ is an orthogonal basis for W, where

$$u_1 = w_1$$
$$u_2 = w_2 - \frac{u_1^T w_2}{u_1^T u_1} u_1$$
$$u_3 = w_3 - \frac{u_1^T w_3}{u_1^T u_1} u_1 - \frac{u_2^T w_3}{u_2^T u_2} u_2,$$

and where, in general

$$u_i = w_i \sum_{k=1}^{i-1} \frac{u_k^T w_i}{u_k^T u_i} u_k, \quad 2 \le i \le p \qquad (1)$$

3. Our proposed An k-span secret sharing scheme with exposing forged shadows.

The main idea of our proposed a k-span secret sharing scheme with exposing forged shadows used eigenvector from theorem 3 in secret regeneration procedure. The sequence $\{U_k\}$ can be calculated by multiplying power of L. That is

$$U_1 = LU_0$$

$$U_2 = LU_1 = L(LU_0) = L^2U_0$$

$$\vdots$$

$$U_k = L^kU_0 \quad k = 1, 2, \cdots$$

Next, let L have eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_{n+1}$ and corresponding eigenvectors$\{U_0^1, U_0^2, \cdots, U_0^{n+1}\}$. Namely, the set of eigenvectors $\{U_0^1, U_0^2, \cdots, U_0^{n+1}\}$ in U_0 is linearly independent.

Thus, $L(U_0^1) = \lambda_j U_0^1$ for $1 \le j \le n+1$

$$L^k(U_0^j) = \lambda_j^k U_0^j$$

$$U_k^j = L^k(U_0^j) = \lambda_j^k U_0^j \tag{2}$$

3.1 Secret regeneration procedure

Assume that n is total number of shadows to be constructed and $m(\le n)$ is threshold value required to recover the single master key. The secret regeneration and master key reconstruction procedures are described as follows.

Step 1 : The Key Distribution Center(KDC) selects a prime $p(>K)$ first and a master key vector $V_0^1 = (v_0^1, v_0^1, \cdots, v_{0(n+1)})$ with $v_{0(n+1)}{}^1 = K$ and $v_{0j}{}^1 < p$, $1 \le j \le n$.

Step 2 : The KDC randomly selects n vectors $V_0{}^i$ $(2 \le i \le n+1)$ in $Z_p{}^{n+1}$ such that $V_0{}^i$ and $V_0{}^j$ are mutually linear independent where $i \ne j$ and $1 \le i, j \le n+1$.

Step 3 : Apply the "Gram-Schmit Process" [Theorem 4]. KDC can obtain an orthogonal set $U_0 = \{U_0^1, U_0^2, \cdots, U_0^{n+1}\}$ in $Z_p{}^{n+1}$ where $V_0{}^1 = U_0^1$

Step 4 : $L : U_0 \rightarrow U_0$ be a linear transformation. Set of eigenvectors is used as a basis for $Z_p{}^{n+1}$. The vector U_0^1 will also be written component like $(u_{01}{}^1, u_{02}{}^1, \cdots, u_{0(n+1)}{}^1)$.

And now, we apply the sequence $\{U_k\}$ using Eq.(2), U_k^j can be expressed as a regeneration secret.

$$U_k^j = \lambda_j^k U_0^j, \quad 1 \le j \le n+1 \tag{3}$$

where $\lambda_j{}^k$ is used as k-span parameter $k = 1, 2, \cdots$

Step 5 : The KDC checks whether the $(n \times m)$ matrix $[a_j{}^i] = A$ is rank m. If A doesn't have rank m, go to step 2 where $[a_j{}^i] = u_{0(n+1-m+1)}^{i+1}$

Step 6 : The KDC securely sends initial value $\lambda_j{}^k U_0^j$, as the shadow to the shadowholder j, $2 \le j \le n+1$. $k = 1$

Step 7 : The KDC publishes p and first $n+1-m$ components of the master key U_0^1 for the master key recovery.

3.2 Master key reconstruction

The combination of any m shadows W^i, $1 \le i \le m$, form orthogonal set $U_0 = \{U_0^1, U_0^2, \cdots, U_0^{n+1}\}$, except U_0^1, uniquely determines the master key as follows.

$$\begin{bmatrix} W^1 \\ W^2 \\ \cdot \\ W^m \end{bmatrix} [U_0^1]^T = 0. \tag{4}$$

where T denotes the transpose of matrix.

For more clearly, Eq.(4) can be rewritten as follows.

In Eq.(4), since the $(m \times m)$ matrix $[w_i{}^j]$ $(1 \le j \le m$ and $1 \le i \le n+1)$ is non singular and the vector Z is known, component of master vector U_0^1 is unknown.

$$\begin{bmatrix} w_1^1 & w_2^1 & \cdots & w_{n+1-m}^1 & w_{n-m}^1 & \cdots & w_{n+1}^1 \\ w_1^2 & w_2^2 & \cdots & \cdots & \cdots & \cdots & w_{n+1}^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ w_1^m & w_2^m & \cdots & w_{n+1-m}^m & w_{n-m}^m & \cdots & w_{n+1}^m \end{bmatrix}$$

$$\begin{bmatrix} u_{0(1)}^1 \\ u_{0(2)}^1 \\ \cdot \\ u_{0(n+1-m)}^1 \\ u_{0(n+2-m)}^1 \\ u_{0(n+1)}^1 \end{bmatrix} = 0 \tag{5}$$

Since the first $n+1-m$ component of the master vector U_0^1 are public . Eq.(5) can be reformulated by

$$\begin{bmatrix} w^1_{n+1-m+1} & \cdots\cdots & w^1_{n+1} \\ w^2_{n+1-m+1} & \cdots\cdots & w^2_{n+1} \\ \cdot & \cdots\cdots & \cdot \\ w^m_{n+1-m+1} & \cdots\cdots & w^m_{n+1} \end{bmatrix} \begin{bmatrix} u^1_{0(n+1-m+1)} \\ u^1_{0(n+1-m+2)} \\ \cdot \\ \cdot \\ u^1_{0(n+1)} \end{bmatrix} = \begin{bmatrix} Z^1 \\ Z^2 \\ \cdot \\ Z^m \end{bmatrix} \quad (6)$$

where $Z^i = -\sum_{j=1}^{n+1-m} w_j^i \times u_{0j}^1$, $(1 \le j \le m$ and $n+2-m \le i \le n+1)$

Note that all of Equation (4)~Equation (6) are operated in $GF(P)$. Since the master key is hidden in the master vector U_0^1(i.e., $K = u_{0(n+1)}{}^1$), the combination of any m shadows can be determined using Equation (6).

Compare U_k^1 with $\lambda_j{}^k U_0^j$, if $k \neq k'$, then shadowholder U_0^j define as forged shadow. To regenerate secret, The KDC change only the k of eigenvalue $\lambda_j{}^k$. The KDC can be directly redistributed by changing k of $\lambda_j{}^k$.

〈Table1〉 Comparition of our scheme with the other well-known scheme

scheme	time complexity	space complexity	detect ability	expose ability	secret span
Shamir	$O(m \log^2 m)$	1	×	×	×
Blakley	$O(m^3)$	$m/(n+1)$	×	×	×
Tompa	$O(m \log^2 m)$	$1/m$	$m-1$	×	×
Asmuth	$O(m)$	$1/2^*$	$m-1$	$\lfloor m-1/2 \rfloor$	×
C.S.Laih	$O(m^3)$	$m/n+1$	$m-1$	$\lfloor m-1/2 \rfloor$	×
Our scheme	$O(m^3)$	$m/n+1$	$m-1$	$\lfloor m-1/2 \rfloor$	k

* : $\lfloor (m-1/2) \rfloor$

3.3 security analysis

① The prosed scheme satisfies the Definition 1, that is, knowledge of any $m-1$ or fewer shadows provides no more information about the master key then was known before.

② Suppose $A \in \Gamma$, and let A_R be its reconstruction matrix. Let A and A_R be similar, meaning that for some nonsingular matrix P,

$$A_R = P^{-1}AP$$

Being similar means that A and B represent the same linear transformation of the vector space R_n or C^n.

Then

$$f_{AR}(\lambda) = \det(A_R - \lambda I) = det(P^{-1}AP - \lambda I)$$
$$= [det\, P^{-1}]\, det(A - \lambda I)[detP]$$
$$= det(P^{-1}[A - \lambda I]P) = det(A - \lambda I) = f_A(\lambda)$$

since $detP^{-1}detP = det(P^{-1}P) = 1$.

This says that the similar matrices have the same eigenvalues.

We have that their coefficients are invariant.

From the theorem 1, We have

$$Au_j = \lambda_j u_j, \quad j = 1, \cdots, n$$

Thus the columns $u_1, \cdots, u_n$ are orthogonal eigenvector of A. There is an orthogonal basis for the associated vector space V consisting of eigenvectors of A, for a Hermitian matrix A, the eigenvalues are all real.

u^H gives $u^HAu = \lambda u^Hu$ forming the Hermitian transpose of this equation and making use of the property $A^H = A$ gives

$$u^HAu = \lambda^* u^Hu$$

where λ^* is the complex conjugate of λ. However $u^Hu \neq 0$, unless u is a null vector. Hence it follows that $\lambda^* = \lambda$ and λ must be real. It is also possible to show that the eigenvectors can be written in real form. $A^HA = I$ takes the place of the orthogonal transformation matrix. All the eigenvalues of a Hermitian matrix can be shown to be real. Thus, all of the shares are from the same domain as the secret. Our proposed scheme based on eigenvalue be equivalent to *ideal* secret sharing scheme.

③ *ideal* scheme can provide perfect security at any time regardless how many previous master key and public

shadows are known [4]. If the master keys, U_0^1, are kept secret, our scheme also provide Shannon perfect security.

3.4 Access structure

Given a secret sharing scheme, the structure, Γ, define as the set of subsets of participants that can determine the secret. In this paper, we assume that every participant has equal privilege and restrict our attention to secret sharing schemes in which Γ is monotone, that is, if $B \in \Gamma$, and if B is contained in C, then $C \in \Gamma$. Our scheme satisfies the Definition 2. A perfect secret sharing scheme is *ideal* if all of the shares are from the same domain as the secret. The monotone set of subsets, Γ, called an *ideal* access structure if there is some *ideal* secret sharing scheme for which Γ is the access structure.

3.5 Dynamic Threshold Scheme

Dynamic Threshold Scheme [4] or, more precisely, the (d, m, n, t) threshold/ramp scheme, where d, m, and n are the number of secrets, threshold value of shadows, and number of all shadows, respectively, and t indicates time. To compared conventional threshold/ramp scheme, at least one of the previous issued n shadows need to be changed whenever the master key need to be update for security reasons. But this scheme have a drawback that the threshold value is decreased in proportion the number of different secrets which have been revealed. Another previous work is an l-span generalized secret sharing scheme which is proposed by Lein and Hung-Yu Lin [5]. Each participant may be designated with a different privilege. It is impossible to detect unhonest shadowholders.

4. Conclusion

In this paper, we proposed k-span secret sharing scheme with exposing forged shadows. The major advantage of proposed scheme change only the k of eigenvalue parameter λ_j^k for secret regeneration . Also the reconstruction secret must be revealed but our scheme make redistribution without revealing with other participants. Our work have shorter tags and more span secret. It can be reduce the overhead in the regeneration and redistribution for shadows.

Reference

[1] G. R. Blakley, "Safeguarding Cryptographic Keys," in Proc. Amer. Fed. Inform. Proc. Soc. NCC, Vol.48, pp. 313-317, June, 1977.

[2] A, shmir, "How to Share a Secret," Communication ACM, Vol.22, No.11, pp.612-613, Nov., 1979.

[3] C. S. Laih, M. D. Lin and T. Hwang, "A new threshold scheme with detecting and exposing forged shadows," ISITA '90, pp.1053-1056, November, 1990.

[4] C. S. Laih, L. Harn, J. Y. Lee and T. Hwang, "Dynamic Threshold Scheme Based on the Definition of Cross-Product in an N-Dimensional Linear Space," Proc. Crypto '87, Springer-Verlag, pp.286-279.

[5] L. Harn and Hung-Yu Lin, "A ℓ-Span Generalized Secret Sharing Scheme," Proc. Crypto '92, Springer-Verlag, pp. 558-565.

[6] Lee W., Johnson R., Dean Riess Jimmy T., Arnold, "Introduction to Linear Algebra," Addison-Wesley. Inc. 1993.

[7] S. C. Kothari, "Generalized Linear Threshold Scheme," in Proc Cryto '86, Springer-Verlag, pp.231-241.

[8] Mathematica lCryptology for Computer Scientists and Mathematicians, WAYNE PATTERSON, ROWMAN & LITTLEFIELD Publishers.

[9] W. Diffie and M. E. Hellman, "New Directions In Cryptography," IEEE Transaction on Information Theory, Vol IT-22, pp.644-65, 1976.

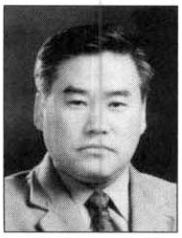
[10] C. Asmuth and J. Bloom, "A Modular Approach To Key Safeguarding," IEEE Transaction on Information Theory, Vol.IT-29, No.2, pp.208-210, March, 1983.

[11] M. Tompa and H. Woll, "How To Share A Secret With Cheaters," Crypto '86 pp.261-265.

[12] Benaloh, j. and J. Leichter, generalized Secret Sharing and Monotone Functions, Advances in Cryptography - Crypto '86, A. M. Odlyzko (ed.), Springer-Verlag, Lecture Notes in Computer Science, Vol.236, pp.213-222, 1987.

[13] Ernest F. Brickell, Some Ideal Secret Sharing Schemes, Proc. Crypto '88, Springer-Verlag, pp.468-475.

[14] Ernest F. Brickell and Daniel M. Davenport, On the Classification of Ideal Secret Sharing Schemes, Proc. Crypto '88, Springer-Verlag, pp.279-285.



박 택 진

e-mail : tjpark@gyc.ac.kr

1985년 서울산업대학교 전자공학과(학사)

1990년 한양대학교 전자공학과(석사)

1998년 KAIST/성균관대학교 전기전자 및 컴퓨터공학과 박사과정 수료

1993년~현재 강릉영동대학 전자정보과 조교수

관심분야 : 정보보호 및 암호, hyperelliptic curve

원 동 호

e-mail : dhwon@simsan.skku.ac.kr

성균관대학교 전자공학과(학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임 연구원

1985년~1986년 일본동경공업대학 객원 연구원

1988년~1999년 성균관대학교 교학처장, 전기전자컴퓨터공학부장, 정보통신대학원장 정보통신기술연구소장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

현재 성균관대학교 정보통신공학부 교수, 정통부지정 정보보호 인증기술 연구센터장, 성균관대학교 연구처장

관심분야 : 암호이론, 정보이론