계층구조를 갖는 그룹에서 재사용이 가능한 비밀분산법의 설계

양성미[0]· 박소영· 이상호
이화여자대학교 컴퓨터학과
{wish[0], soyoung, shlee}@ewha.ac.kr

Design of a Reusable Secret Sharing Scheme in a Hierarchical Group

Seong-Mi Yang[0], So-Young Park and Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

비밀분산법이란 하나의 비밀정보(secret)를 분산시켜 다수의 참가자에게 공유시키고, 필요시 허가된 참가자 부분집합만이 비밀정보를 복원할 수 있는 암호 프로토콜이다. 다양한 접근구조를 반영하는 비밀분산법이 제안되었는데, 본 논문에서는 계층구조에 적용이 가능하면서 재사용이 가능한 새로운 비밀분산법을 제안한다. 즉, 참가자들은 트리 상의 상위 레벨부터 비밀정보의 복원에 대한 우선권을 갖고, 상위 레벨에 속하는 참가자들이 부재 시에는 하위 레벨에 속하는 자식 노드들에게 위임티켓(delegation ticket)을 전송하여 비밀정보의 복원 권한을 위임할 수 있고, 각 참가자가 하나의 비밀조각으로 서로 다른 비밀정보를 복원하는데 참여할 수 있도록 함으로써, 계층그룹에서 비밀조각의 재사용이 가능하도록 한다.

1. 서 론

비밀분산법이란 하나의 비밀정보(secret)를 분산시켜 다수의 참가자에게 공유시키고, 필요시 허가된 참가자 부분집합만이 비밀정보를 복원할 수 있는 암호 프로토콜로써, Shamir[1]와 Blakely[2]에 의해서 처음 제안되었다. 가장 대표적인 방법은 (t, n) 임계치법(threshold scheme)으로서, 비밀조각을 분배받은 n명의 참가자들 중에서 임의의 t명 이상이 모이면 비밀정보를 복원할 수 있으나 t명 미만의 참가자들만으로는 비밀정보를 복원할 수 없다.

그러나 응용 시스템에 따라 다양한 접근구조를 반영할 수 있는 비밀분산법이 요구될 수 있다. 계층구조에서 권한 위임에 따른 비밀분산법은 [3]에서 제시되었는데, 처음에는 최상위 레벨만이 비밀정보에 접근할 수 있고, 우선권을 가진 상위 레벨 참가자들의 부재 상황이 발생하면 하위 레벨 참가자들에게 위임 티켓을 발행하여 비밀정보의 복원 권한을 위임한다. 비밀정보 복원 권한 위임은 최하위 레벨 참가자까지 전달될 수 있다. 그러나 이 방법은 비밀정보 하나에 대한 복원으로 여러 개의 비밀정보에 대해서는 매번 비밀조각을 새로 생성하고 전달하는 과정을 거쳐야한다.

본 논문에서는 계층구조를 이루는 그룹에서 참가자들이 처음에 생성된 비밀조각(share)을 재사용하여 임의의 서로 다른 비밀정보를 복원할 수 있는 방법을 제안한다. 참가자들은 스스로 자신의 비밀조각을 생성하고 그에 따른 공개정보를 만들어 공개시키며, 부모 노드 참가자의 부재 상황이 발생하면 전달받은 위임티켓과 생성해 놓은 비밀조각을 이용하여 원 비밀정보를 복원하는데 참여한다. 여기서는 하나의 비밀정보에 대해 위임과정을 거쳐 다시 그 비밀정보로 복원되기까지를 하나의 세션(session)이라고 정의한다. 위임티켓은 매 세션마다 새롭게 생성되는 반면, 각 참가자들의 비밀조각 및 공개정보는 바뀌지 않는다. 또한, 참가자가 비밀조각을 분실했을 경우 다른 참가자 비밀조각의 변경없이 새로운 비밀조각 생성이 가능하다.

2. 관련 연구

다중 비밀분산법(multisecret sharing scheme)과 다중 레벨 비밀분산법(multilevel secret sharing scheme)에 관련된 연구는 다음과 같다.

다중 비밀분산법은 각 참가자가 가진 하나의 비밀조각을 재사용하여 서로 다른 비밀정보를 복원하는 방법으로 Pinch[4]는 공개보드를 사용하여 여러 개의 서로 다른 비밀정보를 복원하는 다중 비밀분산법을 제시하였다. 서로 다른 비밀정보를 복원하기 위해서 비밀조각은 각 비밀정보와 무관하게 생성되어 분배되고 참가자의 부분집합은 분배자가 공개보드에 제시한 비밀복원 정보를 가지고 해당 비밀정보를 복원한다. 하지만 분배자는 모든 참가자의 비밀조각을 모두 알고 있어야한다[4]. Ghodosi[5] 등은 Pinch의 방법에서 속임(cheating)방지 기능을 추가하였다. Pinch의 방법을 기본으로 하되 공개보드의 크기를 줄이는 방법이 Chen[6] 등에 의해 제시되었고, 계산의 효율성을 위해 지수연산을 없애고 해쉬함수기반으로 연산을 만든 방법도 Sun[7]에 의해 만들어졌으며, 이산대수 문제의 키 교환을 이용하여 분배자가 각 참가자의 비밀조각을 모두 알고 있지 않더라도 비밀정보를 복원할 수 있는 방법도 제시되었다[8, 9].

계층구조를 반영하는 비밀분산법으로는 다중레벨 비밀분산법[10], 가중치에 의한 비밀분산법[11] 등이 제시되었으며, 권한위임에 따른 비밀분산법으로는 Ghodosi[12] 등과 송영원[3] 등이 있다. [12]는 레벨 단위의 위임구조를 제시하였고 [3]은 이를 확장하여 개별 위임을 허용하는 반면 비밀조각 분실의 경우나 부정직한 참가자에 대해서는 고려하지 않고 있다.

3. 재사용이 가능한 비밀분산법

본 논문에서 가정하는 계층구조와 위임구조는 [3]과 같이 일반적인 트리 형태의 계층구조와 개별 권한 위임을 허용한다. n명의 참가자로 구성되는 참가자 집합은 $U=\{u_0, u_1, \ldots, u_{n-1}\}$로 표기하고, 이 참가자 집합은 서로 다른 l개의 비밀정보를 복원하는데 참여할 수 있는데, 이 때 서로 다른 비밀정보의 집합은 $K=\{K^{[1]}, K^{[2]}, \ldots, K^{[l]}\}$로 표기한다. 하나의 비밀정보 $K^{[w]}$에 대해 위임과정을 거쳐 다시 복원되는 과정을 세션이라고 한다. 최상위 레벨인 루트 노드 참가자는 u_0로 한 명이고, l개의 비밀정보를 알고 있다.

3.1 비밀조각 생성

최상위 레벨인 루트 노드 참가자 u_0의 비밀조각은 $S_{u_0}^{[w]}=K^{[w]}$이다. 각 내부 노드 참가자 u_i가 l개의 세션을 통해 사용할 비밀조각은 다음과 같이 생성된다.

① 루트 노드 참가자 u_0는 큰 소수 p를 선택하고 공개보드에 게시한다. 모든 계산은 소수 p에 대한 유한체 Z_p상에서 이루어진다.

② u_0는 $[p^{1/2}, p]$사이에서 생성원 g를 선택하여 공개보드에 게시한다.

③ 각 참가자 $u_i(1 \le i \le n-1)$는 $[2, p]$사이에서 자신의 비밀조각 S_{u_i}를 랜덤하게 선택하고, $P_{u_i}=g^{S_{u_i}} \bmod p$를 계산하여 공개보드에 게시한다.

u_0는 각 참가자가 공개하는 P_{u_i}가 중복되지 않는지 검사하여 동일한 값이 생성된 경우는 재생성하도록 조정한다. u_0는 매 세션마다 자신의 비밀조각 S_{u_0}를 새롭게 정의하지만 u_0를 제외한 모든 참가자들은 위 과정을 통해 생성된 비밀조각을 모든 세션에 걸쳐 재사용한다.

3.2 위임과정

비밀정보 복원 권한이 있는 참가자들 중 해당 세션 $[w]$에 참여할 수 없는 참가자 u_i는 자신의 자식 노드 참가자 $c_{i1}, \ldots, c_{it}$에게 세션$[w]$의 권한 위임을 위한 위임티켓 $dt_{u_i}^{[w]}$과 비밀정보 $K^{[w]}$에 대한 비밀복원정보 $T_{u_i}^{[w]}$를 생성하여 전달한다. 위임과정은 매 세션마다 새롭게 수행되며, 세션$[w]$에서의 위임과정은 다음과 같다. 단, w는 $1 \le w \le l$ 이다.

① 루트 노드 참가자 u_0는 위임티켓 $dt_{u_0}^{[w]} \in Z_p$을 랜덤하게 선택하고, $g^{dt_{u_0}^{[w]}} \pmod p$를 계산하여 자식 노드 참가자 $c_{01}, \ldots, c_{0t}$에게 전달한다.

② 루트 노드 참가자는 자식 노드 참가자의 공개정보인 $P_{c_{01}}, \ldots, P_{c_{0t}}$과 자신이 만든 위임티켓을 이용하여, 각 참가자의 세션비밀조각 $(P_{c_{0j}})^{dt_{u_0}^{[w]}}$을 만든 후, 비밀정보 $K^{[w]}$에 대한 비밀복원정보 T_{u_0}를 다음과 같이 생성하여 공개보드에 게시한다.

$$T_{u_0}^{[w]} = S_{u_0}^{[w]} + \sum_{j=1}^{t}(P_{c_{0j}})^{dt_{u_0}^{[w]}} \quad (j=1, \ldots t)$$

③ 위임을 받은 참가자들 중에서 다시 해당 세션에 참여하지 못하는 참가자 u_i 발생시, ①과 같은 방법으로 위임티켓 $dt_{u_i}^{[w]}$을 선택하고, $g^{dt_{u_i}^{[w]}}$를 계산하여 자식 노드 참가자 $c_{i1}, \ldots, c_{it}$에게 전송한다.

④ 해당 세션의 비밀복원정보 $T_{u_i}^{[w]}$는 u_i의 부모 노드 참가자를 u_{p_i}라고 할 때, 그로부터 받은 위임티켓 계산값 $g^{dt_{u_{p_i}}^{[w]}}$과 자신의 비밀조각 S_{u_i}을 이용하여 생성한 세션비밀조각 $(g^{dt_{u_{p_i}}^{[w]}})^{S_{u_i}}$을 복원할 수 있도록 해준다.

$$T_{u_i}^{[w]} = (g^{dt_{u_{p_i}}^{[w]}})^{S_{u_i}} + \sum_{j=1}^{t}(P_{c_{ij}})^{dt_{u_i}^{[w]}} \quad (j=1, \ldots, t)$$

참가자의 부재로 인한 권한 위임은 단말 노드 참가자까지 반복적으로 위임될 수 있다.

3.3 비밀정보 복원

위임받은 참가자들이 모여 루트 노드 참가자의 비밀정보를 복원하는 과정은 다음과 같다. 위임 과정이 이루어진 가장 하위 레벨의 참가자들부터 부모 노드 참가자의 세션비밀조각을 복원해 나감으로써 최종적으로 루트 노드 참가자의 비밀조각 $S_{u_0}^{[w]}$를 복원하여 비밀정보를 알아낼 수 있다.

마지막 위임을 수행한 참가자를 u_i라고 하면, u_i의 위임을 받은 모든 자식 노드 참가자 $c_{i1}, \ldots, c_{it}$가 모여 다음을 수행한다.

① $c_{i1}, \ldots, c_{it}$는 그들의 비밀조각과 전달받은 위임티켓을 이용하여 자신의 세션비밀조각 $(g^{dt_{u_i}^{[w]}})^{S_{c_{ij}}}$을 계산하고, 다른 참가자들에게 비밀통로를 이용하여 전송한다.

② $c_{i1}, \ldots, c_{it}$는 u_i가 공개한 $T_{u_i}^{[w]}$를 이용하여 부모 노드의 세션비밀조각을 복원한다.

$$(g^{dt_{u_{p_i}}^{[w]}})^{S_{u_i}} = T_{u_i}^{[w]} - \sum_{j=1}^{t}(g^{dt_{u_i}^{[w]}})^{S_{c_{ij}}} \quad (j=1, \ldots, t)$$

부모 노드 참가자의 세션비밀조각을 복원한 자식 노드 참가자들은 다시 부모 노드의 형제 노드 참가자들과 함께 ① - ②과정을 통해 조부모 노드 참가자의 세션비밀조각을 복원할 수 있다. 이러한 과정을 반복적으로 수행

하여 최종적으로 루트 노드 참가자의 비밀조각인 $S_{u_0}^{[w]}$를 알아냄으로서 비밀정보 $K^{[w]}$를 복원할 수 있다.

4. 안전성 및 특성 분석

제안한 논문의 안전성은 다음의 세 가지로 분석될 수 있다.

첫째, 부모 노드 참가자로부터 위임티켓을 받지 못한 참가자들은 각 세션 w의 비밀정보 $K^{[w]}$를 복원할 수 없다. 위임티켓 없이 자신의 세션비밀조각 $(g^{dt_{u_i}^{[w]}})^{S_{c_{ij}}}$을 만드는 것은 불가능하므로, $(g^{dt_{u_k}^{[w]}})^{S_{u_i}} = T_{u_i}^{[w]} - \sum_{j=1}^{t}(g^{dt_{u_i}^{[w]}})^{S_{c_{ij}}}$ 로 계산되어 복원되는 부모 노드 참가자의 세션비밀조각을 알아낼 수 없다. 결과적으로 해당 세션의 비밀정보 $K^{[w]}$를 복원할 수 없다.

둘째, 위임티켓에 대한 공개정보 $g^{dt_{u_i}^{[w]}}$만으로, 위임을 받지 않은 참가자는 비밀정보 복원에 참여할 수 없다.

$$T_{u_i}^{[w]} = (g^{dt_{u_k}^{[w]}})^{S_{u_i}} + \sum_{j=1}^{t}(P_{c_{ij}})^{dt_{u_i}^{[w]}} \quad (j=1,\ldots,t)$$

비밀복원정보는 위의 식과 같이 생성되고, 비밀정보 복원에 참여할 참가자들의 공개정보 역시 공개되어있다. 그러나 이산대수 문제의 어려움에 따라 $g^{dt_{u_i}^{[w]}}$만으로는 $dt_{u_i}^{[w]}$를 알 수 없고, 위임을 받지 않은 참가자는 위임을 받은 참가자들의 세션비밀조각을 생성할 수 없으므로 비밀정보 복원에 참여할 수 없다.

셋째, 위임을 받은 자식 노드 참가자들이 부모 노드 참가자의 세션비밀조각 $(g^{dt_{u_k}^{[w]}})^{S_i}$을 복원하더라도, 다른 세션의 비밀정보는 복원할 수 없다. 다른 세션에서는 다른 위임티켓을 받아 세션비밀조각을 계산하므로 매번 다른 값이 생성된다.

또한 제안한 논문은 다음의 두 가지 특성을 갖는다.

첫째, 참가자가 비밀조각을 분실했을 경우, 다른 참가자 비밀조각의 변경없이 새로운 비밀조각 생성이 가능하다. 각 참가자의 비밀조각은 다른 참가자의 비밀조각과 서로 연관되어 생성된 값이 아니고, 서로 다른 랜덤한 값으로만 선택된 것이기 때문에 다른 참가자의 비밀조각은 변경하지 않아도 재생성이 가능하다.

둘째, 부모 노드 참가자라고 해서 자식 노드 참가자의 비밀조각을 알 수 없으며, 분배자 없이 비밀정보의 공유가 가능하다.

5. 결론

본 논문에서는 대규모 기업체와 같이 계층구조가 형성되어 비밀정보 복원 권한 위임이 가능한 그룹에서, 각 참가자가 가진 하나의 비밀조각을 재사용하여 임의의 서로 다른 비밀정보를 복원할 수 있도록 하는 비밀분산법을 제안하였다.

서로 다른 임의의 비밀정보를 복원하기 위해서 위임권한을 받지 못한 참가자는 비밀정보 복원에 참여할 수 없으며, 복원된 비밀정보를 사용하여 다른 비밀정보를 복원하는 것은 불가능하다. 또한 복원된 비밀정보로 인하여 참가자들의 비밀조각도 드러나지 않는다.

향후 연구과제로는 부정직한 참가자들을 포함하는 경우 이를 탐지하고 방지할 수 있는 방법이 필요하다.

6. 참고문헌

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," Proc. of AFIPS, vol. 48, pp. 313-317, 1979.

[3] 송영원, 박소영, 이상호, "트리형태의 계층구조에 적용 가능한 비밀분산법의 설계," 한국정보과학회 논문지(컴퓨터 시스템 및 이론), 제 29권 4호, 2002.

[4] R. G. E. Pinch, "Online multiple secret sharing," Electronics Letters, vol. 32, no. 12, pp. 1087-1088, 1996.

[5] H. Ghodosi, J. Pieprzyk, G. R. Chaudhry and J. Seberry, "How to prevent cheating in Pinch's scheme," Electronics Letters, vol. 33, no. 17, pp. 1453-1454, 1997.

[6] L. Chen, D. Gollmann, C. J. Mitchell and P. Wild, "Secret sharing with reusable polynomials," Proc. of Information Security and Privacy - ACISP'97, LNCS, vol. 1270, pp. 183-193, 1997.

[7] H. M. Sun, "On-line multiple secret sharing based a one-way function," Computer Communications, vol. 22, pp. 745-748, 1999.

[8] R. J. Hwang and C. C. Chang, "An on-line secret sharing scheme for multi-secrets," Computer Communications, vol. 21, no. 13, pp. 1170-1176, 1998.

[9] W. B. Lee and C. C. Chang, "A dynamic secret sharing scheme based on the factoring and Diffie-Hellman problems," IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, vol. E81-A, no. 8, pp. 1733-1738, 1998.

[10] E. F. Brickell and D. M. Davenport, "On the Classification of Ideal Secret Sharing Scheme," Journal of Cryptology, vol. 4, pp. 123-134, 1991.

[11] P. Morillo, C. Padro, G. Saez and J. L. Villar, "Weighted threshold secret sharing schemes," Information Processing Letters 70, pp. 211-216, 1999.

[12] H. Ghodosi, J. Pieprzyk, C. Charnes and R. Safavi-Naini. "Secret sharing in hierarchical groups," Proc. of Information and Communication Security - ICICS'97, LNCS, vol. 1334, pp. 81-86, 1997.