트리 형태의 계층구조에 적용 가능한 비밀분산법의 설계

송영원 박소영° 이상호
이화여자대학교 컴퓨터학과
{everpro, soyoung°, shlee}@ewha.ac.kr

Design of a Secret Sharing Scheme in a Tree-Structured Hierarchy

Young-Won Song So-Young Park° Sang-Ho Lee
Dept. of Computer Science & Engineering, Ewha Womans Univ

요 약

비밀분산법은 하나의 비밀정보(secret)를 분산시켜 다수의 참가자(participant)들에게 공유시키고 필요시 허가된 참가자 부분집합만이 비밀정보를 복원할 수 있도록 하는 암호 프로토콜이다. 본 논문에서는 트리(tree) 형태의 계층 구조를 갖는 참가자들에게 적용할 수 있는 새로운 비밀분산법을 제안한다. 참가자들은 트리 상의 상위 레벨에 따라 비밀정보의 복원에 대한 우선권을 갖는다. 그러나 상위 레벨에 속하는 참가자들이 부재 시에는 하위 레벨에 속하는 자식 노드들에게 위임 티켓(delegation ticket)을 전송하여 비밀정보의 복원 권한을 위임할 수 있다. 이러한 위임 과정은 최상위 레벨인 루트부터 비밀정보를 복원하는데 참여 가능한 하위 레벨까지 순차적으로 수행될 수 있으므로, 제안하는 비밀분산법은 참가자들의 상황에 따라 동적인 접근구조(*dynamic access structure*)를 갖는다.

1. 서 론

비밀분산법은 하나의 비밀정보를 여러 개의 비밀조각(share 또는 shadow)으로 분할시켜 다수의 참가자들에게 공유시키고 필요시 참가자들의 합의에 의해서 다시 비밀정보를 복원하도록 하는 암호 프로토콜이다. 비밀조각을 분배받은 참가자들 가운데 비밀정보를 복원하도록 허가받은 특정 부분집합의 계(family)를 접근구조(access structure)라고 한다. 가장 기본적인 비밀분산법은 1979년 Shamir[1]와 Blakely[2]에 의해서 처음으로 제안된 (t, n)-임계치법(threshold scheme)으로, 비밀조각을 분배받은 n명의 참가자들 중에서 임의의 t명 이상이 모이면 비밀정보를 복원할 수 있으나, t명 미만의 참가자들만으로는 비밀정보를 복원할 수 없다.

그러나 응용 시스템에 따라서 임의의 참가자가 아닌 특정 참가자 조합들만이 비밀정보를 복원할 수 있는 다양한 접근구조를 갖는 비밀분산법이 요구된다. 예를 들어, 기업, 은행 그리고 군조직 등은 참가자간에 계층구조가 존재한다. 즉, 각 참가자가 속하는 계층에 따라 정보의 이용 권한이 다르고 비밀정보에 대한 접근 권한도 서로 다르다. 따라서, 이와 같은 계층 구조를 반영하고 허가된 참가자만이 비밀정보를 복원할 수 있는 비밀분산법이 필요하다.

본 논문에서는 트리 형태의 계층 구조를 갖는 참가자 그룹에 적용할 수 있는 새로운 비밀분산법을 제안한다. 참가자들은 트리 상의 상위 레벨부터 비밀정보의 복원에 대한 우선권을 갖는다. 따라서 처음에는 최상위 레벨만이 비밀정보에 접근할 수 있고, 우선권을 가진 상위 레벨에 속하는 참가자들의 부재 상황이 발생하면 하위 레벨인 자식 노드에 해당하는 참가자들에게 위임 티켓을 발행하여 비밀정보의 복원 권한을 위임한다. 하위 레벨의 참가자들은 상위 레벨의 참가자들로부터 위임을 받은 후에야 상위 레벨의 역할을 대행하여 비밀정보를 복원할 수 있다. 이와 같이, 비밀정보를 공유하는 참가자 집합이 트리 형태의 계층구조를 가질 때, 권한 위임에 따라 동적으로 비밀정보를 복원할 수 있는 새로운 완전(perfect) 비밀분산법[3]을 제안한다.

2. 관련 연구

계층 구조를 반영하는 멀티 레벨 비밀분산법(mutilevel secret sharing scheme)[4]은 참가자 집합을 여러 레벨로 나누고 각 레벨에 따라 비밀정보의 복원 권한을 다르게 부여하는 방법이다. 각 레벨마다 접근 구조가 존재하며 이를 구현하기 위해 레벨에 따라 서로 다른 임계치를 갖는 (t, n)-임계치법이 적용된다. 낮은 레벨일수록 각 참가자가 가진 비밀정보의 복원 권한이 작기 때문에 임계치가 크고, 높은 레벨일수록 참가자들의 권한이 크기 때문에 임계치가 작다. 다항식의 차수로 각 레벨이 표현되는 고차 다항식 기반 비밀분산법이다.

Charnes 등은 계층 구조를 갖는 참가자 집합에 대하여 레벨간의 위임(delegation)에 의한 계층적 위임 비밀분산법(hierarchical delegation secret sharing scheme)[5]의 개념을 제시하였다. Charnes는 각 레벨마다 비밀정보에 대한 접근구조와 하위 레벨로의 위임구조가 독립적으로 존재한다고 가정하기 때문에, 권한 위임은 레벨 단위로 이루어지고 위임을 받은 동일한 레벨의 참가자들만이 모여 비밀정보를 복원할 수 있다. 따라서, 서로 다른 레벨에 속하는 참가자들의 조합은 비밀정보를 복원할 수 없다. 위임 과정은 위임티켓(delegation ticket)의 생성과 전달로 이루어지는데, 레벨 i의 접근구조에 속하는 참가자들이 비밀정보를 복원하는데 참여할 수 없는 경우 레벨 i의 위임구조에 속하는 참가자들이 하위 레벨로 위임티켓을 생성해서 전달함으로써 비밀정보의

복원 권한이 위임된다.

3. 트리 형태의 계층구조에 적용 가능한 비밀분산법의 설계

본 논문에서는 Charnes의 계층적 위임 비밀분산법을 확장하여 트리 형태의 계층 구조를 갖는 참가자 집합에 대해, 참가자간 개별 권한 위임을 허용함으로써 서로 다른 레벨의 참가자 조합도 비밀정보를 복원할 수 있는 보다 일반화된 계층 구조를 가지는 비밀분산법을 제안한다.

참가자들은 트리 형태의 계층 구조를 갖고 있어서 트리 상의 상위 레벨부터 비밀정보 복원에 대한 우선권을 가지며, 최상위 레벨은 비밀정보를 알고 있는 한 명의 참가자로 구성된다. 우선권을 갖은 상위 레벨에 속하는 참가자들이 부재 상황이 발생하여 비밀정보를 복원할 수 없는 경우에는 하위 레벨인 자식 노드에 해당하는 참가자들에게 위임 티켓을 생성하여 전송함으로써 비밀정보의 복원 권한을 위임한다. 위임을 받은 하위 레벨의 참가자들은 그들이 가진 비밀조각과 상위 레벨로부터 전송받은 위임티켓으로부터 부모 노드의 역할을 대신하여 비밀정보를 복원하는데 참여할 수 있다. 그러나 위임을 받지 않은 하위 레벨의 참가자들은 자신들의 비밀조각만으로 비밀정보를 복원할 수 없다.

3.1 계층 구조의 표현

참가자들의 집합 $P=\{P_1,\ldots,P_n\}$이 차수(degree)가 2이상인 일반적인 트리 형태의 계층 구조를 가질 때, 이 계층 트리를 T라고 하면 트리의 각 노드는 참가자를, 트리의 각 레벨은 참가자들의 계층을 나타낸다.

트리 T는 다시 각 내부 노드 P_i를 루트로 하고 그의 자식 노드들을 단말 노드로 하는 깊이(depth)가 2인 부트리 T_i들로 나뉘어 질 수 있으며, 이해를 돕기 위해 이후 본문에서는 부트리 T_i의 단말노드들을 $c_{i1},\ldots,c_{it}$라고 표기한다. 각 부트리 T_i는 하나의 위임 단위를 나타내는 것으로, T_i의 루트 P_i가 부재 시 그의 권한을 자식 노드들에게 위임하고, 자식 노드 $c_{i1},\ldots,c_{it}$는 P_i의 비밀조각을 복원함으로써 P_i의 권한을 대행할 수 있다. 즉, P_i의 비밀조각 s_{P_i}는 T_i의 단말 노드 $c_{i1},\ldots,c_{it}$에 의해서 복원 가능한 부 비밀정보(sub-secret)가 된다. 참가자 집합 P에 대한 임의의 계층 트리의 예는 그림 1과 같다.

3.2 위임 과정

위임 과정은 Charnes가 [5]에서 제시한 위임 티켓이라는 개념을 사용한다. 위임과정은 최상위 레벨의 참가자가 부재 시에 처음 발생하게 되며, 위임은 바로 아래 하위 레벨에 속하는 자식 노드들에게 이루어지고, 만약 자식 노드들 중에서도 역시 비밀정보를 복원하는데 참여할 수 없는 참가자 c_{ij}가 있다면, c_{ij}는 자신의 비밀조각에 대한 복원 권한을 다시 그의 자식 노드들에게 위임한다. 이러한 위임 과정은 부모 노드로부터 위임을 받은 자식 노드들 모두가 부재중이 아닐 때까지 반복적으로 수행되며, 따라서 최하위 레벨까지 계속될 수 있다.

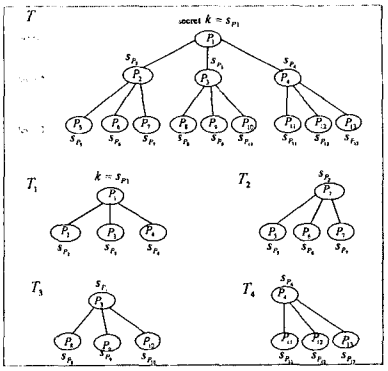

그림 1 계층 구조의 트리 표현 예

모든 내부 노드 P_i는 자식 노드들에게 권한 위임을 할 수 있도록 하기 위해 위임 티켓(delegation ticket) t_{P_i}를 생성하고, 비밀정보 복원에 참여할 수 없게 되면, P_i는 자신의 위임 티켓 t_{P_i}와 함께 P_i가 부모 노드로부터 전달받은 상위 레벨의 위임 티켓들을 가장 왼쪽 자식 노드 c_{i1}에게 전송한다. 위임 과정이 성공적으로 수행되고 나면, P_i의 자식노드 $c_{i1},\ldots,c_{it}$는 위임 티켓 t_{P_i}의 정보와 자신들의 비밀조각으로부터 부모 노드 P_i의 비밀조각 s_{P_i}를 복원할 수 있고, t_{P_i}와 함께 전달받은 다른 위임 티켓들을 이용하여 동일 레벨 또는 상위 레벨의 참가자들과 원 비밀정보 k를 복원할 수 있다.

3.3 비밀정보의 분산과 복원

권한 위임을 통한 비밀정보의 분산 및 복원 과정은 다음과 같다.

■ 비밀정보의 분산

최상위 레벨인 루트 P_1의 비밀조각 $s_{P_1}=k$이다. 비밀정보의 분산은 최상위 레벨인 루트부터 순차적으로 수행되며, (t, t)-임계치법[6]에 의해 부트리 T_i단위로 수행되고 그 과정은 다음과 같다.

① 각 부트리 T_i의 루트인 P_i는 자신이 분배받은 비밀조각 s_{P_i}보다 큰 임의의 소수 q_i를 선택한다. 모든 계산은 소수 q_i에 대한 유한체 Z_{q_i} 상에서 이루어진다.

② 서로 다른 t개의 공개 값 $x_1,\ldots,x_t\in Z_{q_i}$과 비밀 값 $a_{i0},\ldots,a_{i(t-1)}\in Z_{q_i}$을 랜덤하게 선택하여 t-1차 다항식 $f_i(x)=a_{i0}+a_{i1}x+a_{i2}x^2+\ldots+a_{i(t-1)}x^{t-1} \pmod{q_i}$를 생성한다.

③ P_i는 자식노드인 c_{ij}에게 비밀조각 $s_{c_{ij}}=f_i(x_j)$를

계산하여 안전하게 전송한다. 단, $j=1,\ldots,t$이다.

비밀조각을 분배받은 각 내부 노드는 다시 그의 자식 노드들에게 위와 동일한 방법으로 비밀조각을 생성하여 분배한다.

■ **위임 티켓의 생성**

P_i의 위임 티켓 t_{P_i}는 $t_{P_i}=s_{P_i}-a_{i0}(\mathrm{mod}\ q_i)$이다. 위임 티켓 t_{P_i}는 P_i가 비밀정보를 복원하는데 참여할 수 없는 경우에만 가장 왼쪽 자식 노드 c_{i1}에게 전송한다. 이 때 P_i는 자신이 부모 노드로부터 받은 다른 위임 티켓들도 함께 전송한다.

■ **비밀정보의 복원**

비밀정보의 복원은 위임 과정과 반대 순서로 위임 과정이 이루어진 가장 하위 레벨의 참가자들부터 부모 노드의 비밀조각을 복원해나감으로써 결국 루트의 비밀정보 k를 복원할 수 있다. 마지막으로 위임을 수행한 참가자를 P_i라고 하고 위임을 받은 가장 하위 레벨 참가자들을 $c_{i1},\ldots,c_{it}$라고 하자.

① $c_{i1},\ldots,c_{it}$는 그들의 비밀조각으로부터 Lagrange의 보간 다항식[1]을 이용하여 함수 f_i의 상수항 $a_{i0}=f_i(0)$를 구한다.

② $c_{i1},\ldots,c_{it}$는 a_{i0}와 c_{i1}이 공개하는 P_i의 위임 티켓 t_{P_i}와 함께 P_i의 비밀조각 $s_{P_i}=a_{i0}+t_{P_i}$를 복원한다.

상위 레벨의 부모 노드로부터 위임 티켓을 전달받지 못하면 하위 레벨의 자식 노드들은 그들이 가진 비밀조각만으로는 부모 노드의 비밀 조각을 복원할 수 없으며, 부모 노드의 비밀조각을 복원한 자식 노드들은 다시 부모 노드의 형제 노드들과 함께 조부모 노드의 비밀조각을 복원하여 최종적으로 루트의 비밀정보를 복원한다.

4. 정보비(information rate) 분석

정보비는 비밀정보의 정보량과 비밀조각의 정보량의 비율[3]로, 비밀정보 k의 집합 K에 대해서 $q=|K|$ 라고 하고, 각 참가자들이 갖는 비밀조각 집합 중 최대 비밀조각 집합을 $s=\max_{P_i\in P}\{|S_{P_i}|\}$라고 했을 때, 정보비 $\rho=\frac{\log q}{\log s}$로 정의된다[3]. 제안한 방법에서 각 참가자는 하나의 비밀조각과 상위 레벨로부터 건네받은 위임티켓을 갖는다. 위임티켓 또한 활성화 비밀조각[7]의 하나이므로 제안한 방법의 정보비는, 각 참가자 P_i가 부모 노드로부터 전송 받은 총 위임 티켓의 개수를 $N(P_i)$ 라고 했을 때, $\rho=\frac{1}{1+\max_{P_i\in P}N(P_i)}$이다.

만약 트리의 단말 노드까지 비밀정보의 복원 권한이 위임된다면, 단말노드가 갖게 되는 위임 티켓의 총 개수는 일반적으로 트리 T의 깊이 $d(T)$에 비례하므로 $\rho\geq\frac{1}{d(T)}$ 이다.

5. 결 론

본 논문에서는 트리 형태의 계층 구조를 갖는 참가자 그룹에 적용할 수 있는 비밀분산법을 제안하였다. 제안한 방법은 트리 상의 부모 노드와 자식 노드간의 위임 과정을 위임 티켓을 사용하여 상위 레벨부터 순차적으로 수행함으로써 참가자들의 상황에 따라 동적인 접근구조를 가지는 비밀분산법이다. 또한 멀티레벨 비밀분산법[4]과 계층적 위임 비밀분산법[5] 각각의 장점을 모두 수용함으로써 한층 확장된 접근구조와 비밀정보 접근 제한을 가능하게 하였다.

제안한 방법은 (t, t)-임계치법[6]과 사전분배 비밀분산법[7]을 바탕으로 접근구조를 만족하는 참가자만이 비밀정보를 복원할 수 있고, 그렇지 않는 참가자들은 원 비밀정보에 대해 어떤 정보도 획득할 수 없으므로 완전 비밀분산법이다. 정보비는 위임티켓의 개수에 반비례하므로 트리의 깊이를 $d(T)$라고 했을 때, $\rho\geq\frac{1}{d(T)}$이다.

실제로 많은 조직들이 트리 형태의 계층 구조를 취하므로 제안한 방법은 전자문서 결재 시스템이나 비밀분산법 기반 대리 서명 등의 다양한 분야에 응용될 수 있다.

참 고 문 헌

[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," AFIPS Conference Proceedings, vol. 48, pp. 313-317, 1979.

[3] E. F. Brickell and D. R. Stinson, "Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes," Journal of Cryptology, vol. 5, pp. 153-166, 1992.

[4] G. J. Simmons, "How to (Really) Share a Secret," Advances in Cryptology - Crypto'88, Lecture Notes in Computer Science, vol. 403, pp. 390-448, 1990.

[5] H. Ghodosi, J. Pieprzyk, C. Charnes and R. Safavi-Naini. "Secret Sharing in Hierarchical Groups," Information and Communication Security - ICICS'97, Lecture Notes in Computer Science, vol. 1334, pp. 81-86, 1997.

[6] E. D. Karnin, J. W. Greene and M. E. Hellman, "On Secret Sharing Systems," IEEE Transactions on Information Theory, vol. IT-29, no. 1, pp. 35-41, 1983.

[7] G. J. Simmons, "Prepositioned Shared Secret and/or Shared Control Schemes," Advances in Cryptology - EUROCRYPT'89, Lecture Notes in Computer Science vol. 434, pp. 436-467, 1990.