

트리 형태의 계층 구조에 적용 가능한 비밀분산법의 설계

(Design of a Secret Sharing Scheme in a Tree-structured Hierarchy)

송 영 원 [†] 박 소 영 [†] 이 상 호 ^{††}
(Young-Won Song) (So-Young Park) (Sang-Ho Lee)

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 레벨부터 비밀정보의 복원에 대한 우선권을 갖는다. 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 과정을 최상위 레벨인 루트부터 비밀정보를 복원하는데 참여 가능한 하위 레벨까지 순차적으로 수행함으로써 제안하는 비밀분산법은 참가자들의 상황에 따라 동적인 접근구조(dynamic access structure)를 갖는다.

키워드 : 정보보호, 암호, 비밀분산법

Abstract A secret sharing scheme is a cryptographic protocol to share a secret among a set of participants P in the way that only qualified subsets of P can reconstruct the secret whereas any other subset of P , non-qualified to know the secret, cannot determine anything about the secret. In this paper, we propose a new secret sharing scheme in hierarchical groups, whose hierarchy can be represented as a tree structure. In the tree structure, participants of higher levels have priorities to reconstruct the secret over participants of lower levels. In the absence of the participant of a higher level, it is possible for this participant to delegate the ability to reconstruct the secret to the child nodes of the next lower level through the transfer of his delegation ticket. This scheme has a dynamic access structure through the recursive delegation process from the root to lower levels where participants aren't absent.

Key words : Cryptography, Secret Sharing

1. 서 론

인터넷을 이용한 디지털화된 정보 이용이 보편화됨에 따라 정보보호 문제가 더욱 중요한 쟁점으로 부각되고 있다. 정보보호를 위한 시스템들은 정보가 손실·파괴 또는 오용되는 것을 방지하면서 동시에 효율적이어야

한다. 비밀분산법은 비밀정보를 안전하게 관리하기 위한 해결책으로써 하나의 비밀정보를 여러 개의 비밀조각(share 또는 shadow)으로 분할시켜 다수의 참가자들에게 공유시키고 필요시 참가자들의 합의에 의해서 비밀정보를 복원하도록 하는 암호 프로토콜이다. 비밀조각을 분배받은 참가자들 가운데 비밀정보를 복원하도록 허가 받은 특정 부분집합의 계(family)를 접근구조(access structure)라고 한다.

이와 같은 비밀분산법은 다수의 합의를 필요로 하는 작업들에 다양하게 적용될 수 있다. 실제로 구 소련의 핵미사일 발사권은 대통령, 국방부 장관, 군사령관 세 명이 나누어 가지고 있어 두 명 이상이 동의해야만 발

[†] 학생회원 : 이화여자대학교 컴퓨터학과
everpro@ewha.ac.kr
soyoung@ewha.ac.kr

^{††} 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2001년 5월 14일
심사완료 : 2002년 1월 14일

사할 수 있었다. 또한 일반적인 은행 금고는 두 개의 열쇠를 은행의 지점장과 부 지점장이 나누어 가지고 있어 이 두 명이 합의를 할 때에만 열 수 있다. 이 외에도 암호 화키의 관리나 다자간 프로토콜(multiparty protocol), 그룹 암호 등의 많은 분야에서 비밀분산법이 이용되고 있다.

가장 기본적인 비밀분산법은 1979년 Shamir[1]와 Blakely[2]에 의해서 처음으로 제안된 (t, n) -임계치법(threshold scheme)이다. 이는 비밀조각을 분배받은 n 명의 참가자들 중에서 임의의 t 명 이상이 모이면 비밀정보를 복원할 수 있으나, t 명 미만의 참가자들만으로는 비밀정보를 복원할 수 없는 방법이다.

그러나 실제 현실에서는 시스템에 따라 임의의 참가자가 아닌 특정한 참가자들로 구성된 접근구조를 갖는 비밀분산법이 필요하다. 예를 들어, 은행의 지점장과 부 지점장 그리고 계원의 계층 구조나 군대의 계층 구조와 같은 조직 내 구성원들의 계층 구조를 반영할 수 있는 비밀분산법이 요구된다.

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 지식 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. 제안하는 비밀분산법은 트리 상의 레벨로 표현되는 계층간의 위임 과정을 최상위 레벨부터 부재중이 아닌 하위 레벨까지 순차적으로 수행함으로써 참가자들의 상황에 따라 동적인 접근구조[4, 5, 6]를 갖는다.

본 논문의 구성은 다음과 같다. 2장에서는 비밀분산법의 기본적인 개념에 대해 설명하고 3장에서는 계층 구조를 반영하는 비밀분산법과 관련된 기존의 연구를 소개한다. 그리고 4장에서는 위임 과정을 통해 계층 구조를 갖는 조직에 적용 가능한 새로운 비밀분산법을 제안하고, 5장에서는 제안한 방법의 완전성과 효율성을 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 기본 개념

n 명으로 구성된 참가자들의 집합을 $P=\{P_1, \dots, P_n\}$ 이라고 하자. 분배자(dealer)는 하나의 비밀정보를 여러

개의 비밀 조각으로 분할하여 다수의 참가자들에게 분배하는 사람이다. 비밀정보를 복원할 수 있도록 허가 받은 P 의 부분집합의 계(family)를 접근구조 Γ 라고 하며, $\Gamma \subseteq 2^P$ 이다[7]. 접근구조 Γ 는 단조성(monotone)을 만족하는데, 이것은 참가자들의 부분집합 A, B 에 대해서 $A \in \Gamma$ 이고 $A \subset B \subset P$ 이면 $B \in \Gamma$ 을 의미한다[7]. 접근구조 Γ 에 속하는 참가자들의 부분집합 $A \in \Gamma$ 에서 한 명의 참가자라도 줄어들어 비밀정보를 복원할 수 없다면, A 를 최소집합(minimal set)이라고 한다[8]. 그리고 이러한 최소집합들의 계를 최소접근구조(minimal access structure) Γ^- 라고 하며, $\Gamma^- \subset \Gamma$ 이다. 따라서 접근구조는 최소집합을 포함하는 참가자들의 모든 부분집합이 된다.

비밀정보의 집합을 K , 각 참가자 $P_i \in P$ 가 갖고 있는 비밀조각의 집합을 S_{P_i} 라고 하자. 분배자가 비밀정보 $k \in K$ 에 대한 비밀조각 $s_{P_i} \in S_{P_i}$ 를 각 참가자 $P_i \in P$ 에게 분배할 때, 비밀분산법이 다음 두 조건을 만족하면 완전 비밀분산법(perfect secret sharing scheme)[11]이라고 한다.

- (1) 접근구조 Γ 의 원소인 허가 받은 부분집합 $A \in \Gamma$ 에 속하는 참가자들은 비밀정보를 복원할 수 있다.
- (2) 허가 받지 못한 참가자들의 부분집합 $A \notin \Gamma$ 은 무한한 계산적 자원을 갖는다고 해도 비밀정보에 대한 어떠한 정보도 계산할 수 없다.

비밀분산법을 구현하는데 고려해야 할 중요한 요소 가운데 하나는 참가자들에게 분배하는 비밀조각의 크기를 최소화하는 것이다. 이것은 비밀리에 보관해야 하는 정보의 양이 증가함에 따라 시스템의 안전성이 감소하기 때문이다. 비밀정보의 집합 K 의 원소의 수를 $q = |K|$ 라고 하고 각 참가자들이 가진 비밀조각의 집합 S_{P_i} 의 원소의 수 중에서 가장 큰 수를 $s = \max_{P_i \in P} \{ |S_{P_i}| \}$ 라고 하면, 비밀분산법의 정보비율(information rate)[7] ρ 는 비밀정보와 비밀조각의 비트 길이의 비인 $\rho = \frac{\log q}{\log s}$ 이다. 즉, 비밀정보의 정보량과 비밀조각의 최대 정보량의 비율을 의미하며 $\rho \leq 1$ 이다. 정보비율이 $\rho = 1$ 인 비밀분산법을 이상적 비밀분산법(ideal secret sharing scheme)이라고 한다[7].

(t, t) -임계치법은 Karnin, Greene 그리고 Hellman[12]에 의해 연구된 방법으로 참가자 집합의 모든 참가자가 합의해야만 비밀정보를 복원할 수 있는 비밀분산법이다. 이를 구현하기 위한 방법은 다음과 같다.

분배자는 주어진 비밀정보 k 에 대해 k 보다 큰 임의의

소수 q 를 선택하고 모든 계산은 유한체 Z_q 상에서 이루어진다. 다음으로 분배자는 서로 다른 독립적인 $t-1$ 개의 비밀조각 $s_{P_1}, \dots, s_{P_{t-1}} \in Z_q$ 를 임의로 선택한다. 그러면 t 번째 비밀조각 s_{P_t} 는 다음과 같다.

$$s_{P_t} = k - \sum_{i=1}^{t-1} s_{P_i} \pmod{q}$$

분배자는 이렇게 생성한 t 개의 비밀조각들을 t 명의 참가자 집합 $P = \{P_1, \dots, P_t\}$ 에게 분배한다. 비밀정보를 복원하기 위해서는 t 개의 모든 비밀조각들을 모아야만 다음과 같이 비밀정보 k 를 복원할 수 있다.

$$k = \sum_{i=1}^t s_{P_i} \pmod{q}$$

Simmons는 부가 정보에 의해서 비밀분산법이 활성화되기 전까지는 참가자들의 모든 비밀조각이 공개되더라도 비밀정보를 복원할 수 없는 사전분배 비밀분산법(prepositioned secret sharing scheme)을 제안하였다 [13, 14]. (t, n) -임계치법을 예로 들면, n 명의 모든 참가자들이 비밀조각을 공개하더라도 비밀정보를 복원할 수 없고, 부가 정보인 활성화 비밀조각(activating share)이 공개된 후에야 비밀분산 시스템이 활성화되고 비로소 임의의 t 명의 참가자들이 모여 비밀정보를 복원할 수 있다. 이 방법은 활성화 비밀조각의 보안 상태만 안전하게 보장된다면 방대한 양의 비밀조각들을 다소 낮은 보안 레벨로 손쉽게 전송할 수 있는 장점을 갖는다.

3. 관련 연구

계층 구조를 반영하는 비밀분산법과 관련하여 그 동안의 연구 결과는 다음과 같다. 멀티 레벨 비밀분산법(multilevel secret sharing scheme)은 참가자 집합을 여러 레벨로 나누고 각 레벨에 따라 비밀정보의 복원 권한을 다르게 부여하는 방법이다 [1, 13]. 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. 예를 들어 레벨 1이 최상위 레벨이라고 가정하면, 레벨 1의 참가자들은 비밀정보를 알고 있다. 그러나 레벨 2의 참가자들이 비밀정보를 복원하기 위해서는 적어도 2명이 필요하고, 마찬가지로 레벨 3의 참가자들은 적어도 3명이 필요하다. 또한 서로 다른 레벨이 같이 합의하여 비밀정보를 복원할 수도 있는데 이 때에는 참가자들의 레벨 중에서 가장 낮은 레벨의 임계치를 적용한다. 즉, 레벨 2의 참가자 1명과 레벨 3의 참가자 2명이 모이면 비밀정보를

복원할 수 있다.

Charnes 등은 계층 구조를 갖는 참가자 집합에 대하여 레벨간의 위임(delegation)에 의한 계층적 위임 비밀분산법(hierarchical delegation secret sharing scheme)의 개념을 제시하였다 [3]. 이 개념이 성립하기 위해서는 다음의 두 사실을 가정한다. 첫째는 상위 레벨부터 비밀정보 복원에 대한 우선권을 가지며 하위 레벨은 상위 레벨로부터 권한 위임을 받은 후에야 비밀정보를 복원할 수 있다는 가정이고, 둘째는 레벨 i 의 참가자들이 부재 시에 i 보다 하위의 특정 레벨로 비밀정보의 복원 권한을 위임하기 위해서는 먼저 위임 결정을 내리기 위한 참가자들의 합의가 필요하다는 가정이다. 여기서 각 레벨마다 위임 결정을 내릴 수 있는 참가자들의 부분집합을 위임구조(delegation access structure)라고 한다. 각 레벨마다 비밀정보에 대한 접근구조와 하위 레벨로의 위임구조가 독립적으로 존재한다. 따라서 레벨 단위로 위임이 이루어지고 위임을 받은 동일한 레벨의 참가자들만이 모여 비밀정보를 복원할 수 있기 때문에 서로 다른 레벨에 속하는 참가자들의 조합은 비밀정보를 복원할 수 없다. 위임 과정은 위임티켓(delegation ticket)의 생성과 전달로 이루어지는데, 레벨 i 의 접근구조에 속하는 참가자들이 비밀정보를 복원하는데 참여할 수 없는 경우 레벨 i 의 위임구조에 속하는 참가자들이 하위 레벨로 위임티켓을 생성해서 전달함으로써 비밀정보의 복원 권한이 위임된다.

4. 트리 형태의 계층 구조에 적용 가능한 비밀분산법의 설계

본 논문에서는 Charnes의 계층적 위임 비밀분산법을 확장하여 트리 형태의 계층 구조를 갖는 참가자 집합에 대해 참가자간 개별 위임을 허용하는 비밀분산법을 제안한다. 참가자들의 계층 구조로 트리 구조를 이용함으로써 보다 효과적으로 접근구조를 표현할 수 있다. 기존의 멀티레벨 비밀분산법 [1, 13]은 계층간의 위임 과정이 없기 때문에 하위 레벨의 참가자들도 합의만 하면 비밀정보를 복원할 수 있었다. 제안한 방법은 이를 보완하여 평상시에는 상위 레벨만이 비밀정보에 접근할 수 있고 상위 레벨의 부재 시에만 위임을 통해 하위 레벨의 참가자들도 비밀정보를 복원할 수 있도록 함으로써, 비밀정보의 복원 권한뿐 아니라 복원을 위한 참여 여부에 대해서도 계층간의 위계 구조를 반영한다. 또한 Charnes가 개념을 제시한 계층적 위임 비밀분산법 [3]이 비밀정보의 복원과 권한 위임을 레벨 단위로만 허용하는 것에 반해, 본 논문에서 제안하는 방법은 서로 다른 레벨의 참가자

조합도 비밀정보를 복원할 수 있고 각 참가자마다 개별적인 권한 위임을 허용함으로써 한층 더 확장된 계층 구조를 가지는 비밀분산법을 제안하고 실제 위임 과정과 비밀정보의 분산 및 복원 방법을 구현한다.

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 갖춘 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 전송 받은 위임티켓으로부터 비밀정보를 복원할 수 있다. 하위 레벨의 참가자들이 상위 레벨로부터 위임을 받지 않은 경우에는 자신들의 비밀조각만으로 비밀정보를 복원할 수 없다.

4.1 계층 구조의 표현

참가자들의 집합 P 를 i 개의 계층으로 구분하고, 각 계층에 속하는 참가자들의 집합을 L_1, \dots, L_i 라고 한다. 이러한 계층구조를 트리로 표현하면 트리의 각 노드는 참가자를, 트리의 각 레벨은 참가자들의 계층을 나타낸다. 본 논문에서는 이후로 언급하는 노드의 의미를 참가자 P_i 와 동일시한다.

트리의 각 내부 노드 P_i 는 그 자신을 루트로 하고 자식 노드 c_{i1}, \dots, c_{it} 를 단말 노드로 하는 깊이(depth)가 2인 부트리 T_i 를 형성한다. 각 내부 노드 P_i 는 부재 시 그의 권한을 자식 노드들에게 위임하고, 자식 노드 c_{i1}, \dots, c_{it} 는 P_i 의 비밀조각을 복원함으로써 P_i 의 권한을 대행할 수 있다. 즉, 부트리 T_i 의 루트 P_i 의 비밀조각 s_{P_i} 는 단말 노드 c_{i1}, \dots, c_{it} 에 의해서 복원 가능한 부 비밀정보(sub-secret)이며, 이를 위한 접근구조 Γ_i 가 존재한다.

4.2 위임 과정

본 논문에서 제안하는 방법은 각 내부 노드 P_i 의 비밀조각 s_{P_i} 에 대한 복원 권한을 하위 레벨에게 위임하기 위하여 Charnes가 [3]에서 제시한 위임 티켓이라는 개념을 사용한다. 본 절에서는 실제 위임 티켓을 생성하고 적용하는 방법을 제안하고 이를 이용한 위임 과정을 설명한다.

처음에는 최상위 레벨인 루트 P_1 만이 비밀정보를 알고 있고 다른 참가자들은 비밀정보를 알지 못한다. 그러나 루트 P_1 이 비밀정보를 복원하는데 참여할 수 없는 경우에는 바로 아래 하위 레벨에 속하는 자식 노드들에

게 자신이 갖고 있는 비밀정보에 대한 복원 권한을 위임한다. 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 수도 있다.

모든 내부 노드 P_i 는 자식 노드들에게 권한 위임을 하기 위해 위임 티켓(delegation ticket) t_{P_i} 를 생성한다. 부모 노드로부터 위임을 받은 참가자 P_i 가 비밀정보를 복원하는데 참여할 수 없는 경우, P_i 는 자신의 위임 티켓 t_{P_i} 와 함께 P_i 가 부모 노드로부터 전달받은 상위 레벨의 위임 티켓들을 가장 왼쪽 자식 노드 c_{i1} 에게 전송한다. 위임 과정이 성공적으로 수행되고 나면, P_i 의 자식노드 c_{i1}, \dots, c_{it} 는 위임 티켓 t_{P_i} 의 정보와 자신들의 비밀조각으로부터 부모 노드 P_i 의 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 k 를 복원할 수 있다. 즉, 위임티켓을 전송 받은 노드와 그의 형제 노드들은 위임 티켓을 발행한 상위 레벨 노드의 역할을 대행하게 된다. 만약, 참가자 c_{it} 이 부모 노드 P_i 의 위임 티켓과 P_i 의 부모 노드인 조부모 노드의 위임 티켓을 같이 전달받았다면, 참가자 c_{i1}, \dots, c_{it} 는 먼저 자신의 비밀조각과 부모 노드 P_i 의 위임 티켓 t_{P_i} 로부터 부모 노드 P_i 의 비밀조각 s_{P_i} 를 복원하고, 조부모 노드의 비밀조각을 복원하기 위해 P_i 의 비밀조각 s_{P_i} 와 조부모 노드의 위임 티켓을 P_i 를 대신하여 공개한다.

따라서 제안하는 비밀분산법은 계층적 위임(hierarchical delegation) 과정을 통해 참가자들의 상황에 따라 변화 가능한 동적인 접근구조를 갖는다.

4.3 비밀정보의 분산과 복원

권한 위임을 통한 비밀정보의 분산 및 복원 과정은 다음과 같다. 위임을 받은 하위 레벨의 참가자가 상위 레벨의 역할을 대행하도록 하기 위해서 (t, t) -임계치법 [12]과 사전분배 비밀분산법 [13, 14]을 이용한다.

■ 비밀정보의 분산

최상위 레벨인 루트 P_1 의 비밀조각 $s_{P_1} = k$ 이다. 각 내부 노드 P_i 는 Shamir [1] 방식으로 구현한 (t, t) -임계치법에 의해 P_i 가 임의로 선택한 난수 a_0 를 부 비밀정

보로 하는 비밀조각을 생성하여 자식 노드 c_{i1}, \dots, c_{it} 에게 분배한다. 최상위 레벨인 루트부터 순차적으로 각 내부 노드 P_i 가 자식 노드 c_{i1}, \dots, c_{it} 의 비밀조각을 생성하여 분배하는 과정은 다음과 같다.

① 각 부트리 T_i 의 루트인 P_i 는 자신이 분배받은 비밀조각 보다 큰 임의의 소수 q_i 를 선택한다. 모든 계산은 소수 q_i 에 대한 유한체 Z_{q_i} 상에서 이루어진다.

② 서로 다른 t 개의 점 $x_1, \dots, x_t \in Z_{q_i}$ 를 공개적으로 선택한다.

③ 서로 다른 임의의 정수 $a_0, \dots, a_{t-1} \in Z_{q_i}$ 을 비밀리에 선택한다.

④ $t-1$ 차 다항식 $f_i(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{q_i}$ 를 선택한다.

⑤ P_i 는 자식노드인 부트리 T_i 의 단말 노드 c_{ij} 에게 비밀조각 $s_{c_{ij}} = f_i(x_j)$ 를 계산하여 안전하게 전송한다. 여기서 $j=1, \dots, t$ 이다.

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

다음으로 P_i 가 자신의 위임 티켓 t_{P_i} 를 생성하는 방법은 다음과 같다.

$$t_{P_i} = s_{P_i} - a_0 \pmod{q_i}$$

결국, 위임티켓 t_{P_i} 는 사전분배 비밀분산법의 활성화 비밀조각과 같은 역할을 한다. P_i 는 자식노드 c_{i1}, \dots, c_{it} 의 비밀조각을 비밀분산법을 초기화할 때 미리 분배하고, 위임 티켓 t_{P_i} 는 자신이 비밀정보를 복원하는데 참여할 수 없는 경우에만 가장 왼쪽 자식 노드 c_{i1} 에게 전송한다. 이 때 P_i 는 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 k 를 복원할 수 있다.

P_i 의 비밀조각 s_{P_i} 를 복원하기 위한 과정은 다음과 같다.

먼저, P_i 의 위임을 받은 모든 자식 노드 c_{i1}, \dots, c_{it} 가 모인다.

① P_i 의 자식 노드 c_{i1}, \dots, c_{it} 는 그들의 비밀조각으로부터 함수 f_i 의 상수항 $a_0 = f_i(0)$ 를 Lagrange의 보간 다항식[1]을 이용하여 구한다.

② c_{i1}, \dots, c_{it} 는 a_0 와 c_{i1} 이 공개하는 P_i 의 위임 티켓 t_{P_i} 와 함께 P_i 의 비밀조각 $s_{P_i} = a_0 + t_{P_i}$ 를 복원한다.

따라서 상위 레벨의 부모 노드로부터 위임 티켓을 전달받지 못하면 하위 레벨의 자식 노드들은 그들이 가진 비밀조각만으로는 부모 노드의 비밀 조각을 복원할 수 없다. 부모 노드로부터 전달받은 부모 노드보다 상위 레벨의 위임 티켓들은 위임 티켓을 발행한 참가자들의 비밀조각을 복원하기 위해 사용된다. 부모 노드의 비밀조각을 복원한 자식 노드들은 다시 부모 노드의 형제 노드들과 함께 조부모 노드의 비밀조각을 복원할 수 있다. 이러한 과정을 루트까지 반복적으로 수행하여 최종적으로 비밀정보를 복원한다.

참가자 집합 P_1, \dots, P_n 에 대해서 각 참가자 P_i 의 비밀조각 s_{P_i} 를 복원하기 위한 접근구조 Γ_i 는 다음과 같다.

$$\Gamma_i = P_i + t_{P_i} \cdot \Gamma_{c_{i1}} \cdot \dots \cdot \Gamma_{c_{it}}$$

여기서 '+'의 양쪽 피연산자는 최소접근구조의 각 원소를 나타내고, ' \cdot '는 연결된 피연산자들의 조건이 모두 만족되어야 함을 의미한다[6, 9, 10]. 즉, 접근구조 Γ_i 는 P_i 와 $t_{P_i} \cdot \Gamma_{c_{i1}} \cdot \dots \cdot \Gamma_{c_{it}}$ 를 최소접근구조의 각 원소로 가지므로, P_i 자신 또는 자신의 위임티켓 t_{P_i} 와 모든 자식 노드들의 접근구조의 결합에 의해서 P_i 의 비밀조각 s_{P_i} 를 복원할 수 있다.

루트 P_1 은 비밀정보 k 를 알고 있으므로 P_1 의 비밀조각인 $s_{P_1} = k$ 이다.

그리고 단말 노드 P_j 의 비밀조각에 대한 접근구조 Γ_j 는 바로 자기 자신 P_j 뿐이므로 다음과 같다.

$$\Gamma_j = P_j$$

■ 예제

그림 1의 T 와 같은 트리 구조를 갖는 계층 조직을 가정한다. 참가자들의 집합 $P = \{P_1, \dots, P_{13}\}$ 은 3개의 계층 L_1, L_2, L_3 로 구분된다. 비밀정보는 k 이고 루트 P_1 의 비밀조각 $s_{P_1} = k$ 이다.

먼저, 각 참가자에게 비밀조각을 생성하여 분배하기 위하여 최상위 레벨부터 각 부트리 T_i 의 루트 P_i 는 다음 과정을 수행한다.

① P_i 는 자신의 비밀조각 s_{P_i} 보다 큰 임의의 소수 q_i 를 선택한다. 모든 계산은 소수 q_i 에 대한 유한체 Z_{q_i} 상에서 이루어진다. 여기서 $i=1, \dots, 4$ 이다.

② 다음으로 P_i 는 자식 노드의 수만큼 t 개의 서로 다른 점 $x_j = j$ 를 공개적으로 선택한다. 여기서 $j=1, \dots, t$ 이다.

③ 서로 다른 임의의 정수 $a_0, \dots, a_{t-1} \in Z_{q_i}$ 을 비밀리에 선택하여 $t-1$ 차 다항식 $f_i(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$

$(t-1)x^{t-1} \pmod{q_i}$ 를 생성한다.

④ 비밀조각 $s_{c_j} = f_j(x_j)$ 를 생성하여 자식 노드 c_j 에게 안전하게 분배한다. 여기서 $j=1, \dots, t$ 이다.

P_i 의 위임 티켓 $t_{P_i} = s_{P_i} - a_{10} \pmod{q_i}$ 이다.

- 부트리 $T_1 : f_1(x) = a_{10} + a_{11}x + a_{12}x^2 \pmod{q_1}$
 $s_{P_2} = f_1(x_1), s_{P_3} = f_1(x_2), s_{P_4} = f_1(x_3)$
 $t_{P_1} = s_{P_1} - a_{10} \pmod{q_1}$

- 부트리 $T_2 : f_2(x) = a_{20} + a_{21}x + a_{22}x^2 \pmod{q_2}$
 $s_{P_5} = f_2(x_1), s_{P_6} = f_2(x_2), s_{P_7} = f_2(x_3)$
 $t_{P_2} = s_{P_2} - a_{20} \pmod{q_2}$

- 부트리 $T_3 : f_3(x) = a_{30} + a_{31}x + a_{32}x^2 \pmod{q_3}$
 $s_{P_8} = f_3(x_1), s_{P_9} = f_3(x_2), s_{P_{10}} = f_3(x_3)$
 $t_{P_3} = s_{P_3} - a_{30} \pmod{q_3}$

- 부트리 $T_4 : f_4(x) = a_{40} + a_{41}x + a_{42}x^2 \pmod{q_4}$
 $s_{P_{11}} = f_4(x_1), s_{P_{12}} = f_4(x_2), s_{P_{13}} = f_4(x_3)$
 $t_{P_4} = s_{P_4} - a_{40} \pmod{q_4}$

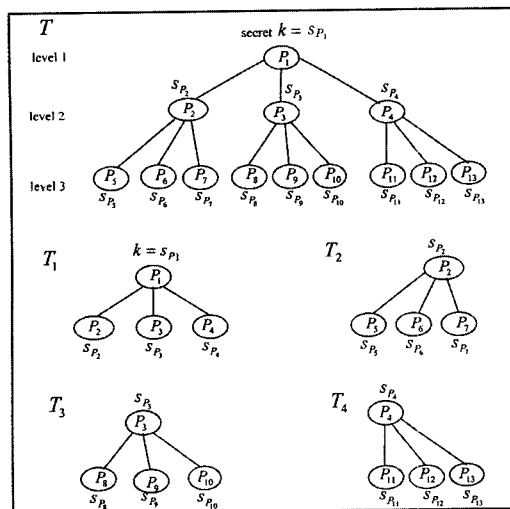


그림 1 계층 구조의 트리 표현 예

만약 루트 P_1 의 부재 상황이 발생하면 P_1 은 위임 티켓 t_{P_1} 을 P_2 에게 전송한다. 그러면 최소집합인 $\{P_2, P_3, P_4\}$ 가 그들의 비밀조각을 공개하여 a_{10} 를 구하고 P_2 가 P_1 의 위임 티켓 t_{P_1} 을 공개하여 $a_{10} + t_{P_1} = s_{P_1}$ 인 비밀정보 k 를 복원할 수 있다.

만약 P_2 역시 부재 상황이 발생하면 P_2 는 자신의 위

임 티켓 t_{P_2} 와 P_1 으로부터 받은 위임 티켓 t_{P_1} 을 함께 P_5 에게 전송한다. 그러면 참가자들의 부분집합 $\{P_3, P_4, P_5, P_6, P_7\}$ 이 최소집합이 되고 P_5, P_6, P_7 이 그들의 비밀조각을 공개하여 a_{20} 를 구하고 P_5 가 공개하는 위임 티켓 t_{P_2} 를 합하여 $a_{20} + t_{P_2} = s_{P_2} = s_{P_1}$ 인 P_2 의 비밀조각을 복원한다. 그리고 이렇게 복원된 P_2 의 비밀조각과 P_3, P_4 의 비밀조각을 이용하여 a_{10} 를 구하고 P_2 가 공개하는 P_1 의 위임 티켓 t_{P_1} 을 합하여 비밀정보 k 를 복원한다.

각 참가자 P_i 에게 분배되는 비밀조각 s_{P_i} 의 접근구조 Γ_i 는 다음과 같다. 여기서 $i=1, \dots, 13$ 이다.

$$\Gamma_1 = P_1 + t_{P_1} \cdot \Gamma_2 \cdot \Gamma_3 \cdot \Gamma_4,$$

$$\Gamma_2 = P_2 + t_{P_2} \cdot \Gamma_5 \cdot \Gamma_6 \cdot \Gamma_7,$$

$$\Gamma_3 = P_3 + t_{P_3} \cdot \Gamma_8 \cdot \Gamma_9 \cdot \Gamma_{10},$$

$$\Gamma_4 = P_4 + t_{P_4} \cdot \Gamma_{11} \cdot \Gamma_{12} \cdot \Gamma_{13},$$

$$\Gamma_5 = P_5, \quad \Gamma_6 = P_6, \quad \Gamma_7 = P_7$$

$$\Gamma_8 = P_8, \quad \Gamma_9 = P_9, \quad \Gamma_{10} = P_{10}$$

$$\Gamma_{11} = P_{11}, \quad \Gamma_{12} = P_{12}, \quad \Gamma_{13} = P_{13}$$

5. 분석

5.1 완전성(perfect secret sharing scheme)

본 논문에서는 비밀정보의 분산과 복원을 위해 (t, t) -임계치법[12]과 사전분배 비밀분산법[13, 14]을 이용한다. 따라서 이 두 가지를 적용함에 따른 완전성이 증명된다면 본 논문에서 제안하는 방법은 완전 비밀분산법임이 증명된다. 여기서 완전 비밀분산법이란 접근구조에 속하는 허가 받은 참가자들의 부분집합은 비밀정보를 복원할 수 있으나, 허가 받지 못한 참가자들의 부분집합은 무한한 계산적 자원을 갖는다고 해도 비밀정보에 대한 어떠한 정보도 계산할 수 없는 비밀분산법을 말한다.

먼저 (t, t) -임계치법은 이를 구현하기 위해 이미 완전하다고 증명된 Shamir[1] 방식을 이용하므로 완전성이 증명된다. 또한 사전분배 비밀분산법을 적용하면서 활성화 조각으로 이용되는 내부 노드의 위임 티켓은 부모 노드로부터 분배받은 비밀조각과 자신이 Shamir 방식을 구현하기 위해 임의로 선택하는 난수의 차이이다. 따라서 서로 다른 참가자가 생성하는 위임 티켓은 임의적이고 독립적이며 위임 티켓들 간에는 상호 연관성이 존재하지 않는다. 즉, 위임 티켓을 전달받은 참가자들은 상위 레벨 참가자들의 비밀조각을 복원할 수 있지만, 위임 티켓을 전달받지 못한 참가자들은 상위 레벨 참가자들의 비밀조각에 대한 어떠한 정보도 알 수 없다. 따라

서 사전분배 비밀분산법을 적용하는 것 역시 완전성이 증명된다.

각 내부 노드 P_i 의 비밀조각을 복원하고자 할 경우, (t, t) -임계치법에 의해 P_i 의 모든 자식 노드 c_{i1}, \dots, c_{it} 가 모여 상수항 a_{i0} 를 계산해 내더라도 사전분배 비밀분산법의 활성화 비밀조각인 P_i 의 위임 티켓 t_{P_i} 가 없이는 P_i 의 비밀조각 s_{P_i} 를 복원할 수 없다. 또한 P_i 의 제일 왼쪽 자식 노드 c_{i1} 이 P_i 의 위임 티켓 t_{P_i} 를 전송 받았더라도 P_i 의 자식 노드 c_{i1}, \dots, c_{it} 모두의 합의 없이는 P_i 의 비밀조각 s_{P_i} 를 복원할 수 없다. 따라서 P_i 로부터 비밀조각의 복원 권한을 위임받지 못한 P_i 의 자식 노드 이외의 참가자들은 P_i 의 비밀조각에 대한 어떠한 정보도 알 수 없으므로, 본 논문에서 제안하는 방법은 완전 비밀분산법이다.

5.2 정보비율(information rate)

정보비율은 비밀정보의 정보량과 비밀조각의 최대 정보량의 비율이다. 비밀정보의 집합 K 에 대한 정보량을 $H(K)$ 라고 하고 각 참가자 P_i 가 가지는 비밀조각의 집합 S_{P_i} 에 대한 정보량을 $H(S_{P_i})$ 라고 하면 $H(S_{P_i}) \geq H(K)$ 이고, 각 참가자 P_i 의 위임 티켓 t_{P_i} 의 정보량을 $H(t_{P_i})$ 라고 하면 $H(t_{P_i}) \geq H(K)$ 이다[3]. 각 참가자 P_i 가 부모 노드로부터 전송 받아 갖고 있는 위임 티켓의 총 개수를 $N(P_i)$ 라고 하면 본 논문에서 제안하는 비밀분산법의 정보비율은 다음과 같다[7].

$$\rho = \frac{1}{1 + \max_{P_i \in P} N(P_i)}$$

만약 트리의 단말 노드까지 비밀정보의 복원 권한이 위임된다면, 단말노드가 갖게 되는 위임 티켓의 총 개수는 일반적으로 트리 T 의 깊이 $d(T)$ 에 비례한다. 따라서 정보비율을 다음과 같이 일반화하여 나타낼 수 있다.

$$\rho \geq \frac{1}{d(T)}$$

5.3 응용 분야

현실 사회에서 비밀정보를 공유하는 대부분의 참가자 조직들이 트리 형태의 계층 구조를 갖는 것을 감안할 때, 제안한 방법은 계층 구조를 가지는 조직 내에서 비밀정보의 유지·관리를 위한 분야에 다양하게 적용될 수 있으며 참가자 부재 시 권한 위임의 기능을 필요로 하는 응용 분야에도 적용될 수 있다. 대표적인 응용 분야를 예로 들면, 전자 문서 결재 시스템이나 비밀분산법 기반의 대리 서명이 있다.

전자 문서 결재 시스템은 참가자간의 계층 구조가 가장 두드러지게 반영되는 응용 분야로, 전자 문서의 사용

이 활성화 될수록 매우 중요한 역할을 담당하고 있다. 본 논문에서 제안하는 방법은 전자 결재 시스템에서 문서 결재 참가자의 부재 시에 권한 위임을 받은 하위 레벨의 대리자가 문서 결재를 수행하기 위한 방법으로 활용될 수 있고, 결재된 문서의 정당성을 검증할 수 있는 기능을 함께 제공할 수 있다.

또한 앞의 활용 예를 더욱 확장하여 비밀분산법 기반 대리서명(proxy signature)에도 적용될 수 있다. 대리서명 기법은 정당한 대리 서명자가 원 서명과 동일한 효력을 갖는 대리서명을 생성하고 이 서명을 수신한 사람은 누구든지 서명의 정당성을 확인할 수 있는 암호학적 프로토콜이다. 제안한 비밀분산법을 대리서명에 응용하면 단 한 사람의 대리 서명자가 아닌 다수의 대리 서명자가 하나의 원 서명과 동일한 효력을 갖는 대리 서명을 생성할 수 있는 기법을 제안할 수 있다.

6. 결론

오늘날 중요하게 대두되고 있는 정보보호 문제를 해결하기 위한 하나의 방법인 비밀분산법은 비밀정보를 분산시켜 다수의 참가자들에게 공유시키고 필요시 참가자들의 합의에 의해서만 비밀정보를 복원할 수 있도록 하는 암호 프로토콜이다.

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 접근 구조를 가지는 비밀분산법이다. 이는 트리 구조를 이용함으로써 기존의 비밀분산법들에 비해 보다 효과적으로 계층 구조를 갖는 참가자들의 접근구조를 표현한다. 또한 멀티레벨 비밀분산법[1, 13]과 계층적 위임 비밀분산법[3] 각각의 장점을 모두 수용함으로써 한층 확장된 접근구조와 비밀정보 접근 제한을 가능하게 한다. 현실적으로 비밀정보를 안전하게 유지·관리하기 위한 대부분의 조직들이 트리 형태의 계층 구조를 취하므로 제안한 방법은 전자문서 결재 시스템이나 비밀분산법 기반의 대리 서명과 같은 비밀분산법을 필요로 하는 다양한 분야에 응용될 수 있다.

제안한 방법은 비밀정보의 분산과 복원을 위해서 완전성이 증명된 (t, t) -임계치법[12]과 사전분배 비밀분산법[13, 14]을 적용하는 완전 비밀분산법이다. 정보비율은 참가자들이 갖는 위임 티켓의 최대 개수에 반비례하며, 트리 상의 최하위 레벨까지 위임이 이루어진다면

트리의 깊이에 비례하게 된다.

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] 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.
- [4] C. Blundo, A. Cresti, A. De Santis, L. Gargano, and U. Vaccaro, "Fully Dynamic Secret Sharing Schemes," *Advances in Cryptology - CRYPTO'93*, Lecture Notes in Computer Science, vol. 773, pp. 110-125, 1994.
- [5] H. Ghodosi, J. Pieprzyk, C. Charnes and R. Safavi-Naini, "Cryptosystems for Hierarchical Groups," *Information Security and Privacy - ACISP'96*, Lecture Notes in Computer Science, vol. 1172, pp. 275-286, 1996.
- [6] K. M. Martin, "Untrustworthy Participants in Perfect Secret Sharing Schemes," In *Cryptology and Coding III*, pp. 255-264, 1993.
- [7] 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.
- [8] D. R. Stinson, "An Explication of Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 2, pp. 357-390, 1992.
- [9] J. Benaloh and J. Leichter, "Generalized Secret Sharing and Monotone Functions," In *Advances in Cryptology-CRYPTO'88*, Lecture Notes in Computer Science, vol. 403, pp. 27-35, 1990.
- [10] G. J. Simmons, W. Jackson and K. Martin, "The Geometry of Shared Secret Schemes," *Bulletin of the ICA*, vol. 1, pp. 71-88, 1991.
- [11] D. R. Stinson and S. A. Vanstone, "A Combinational Approach to Threshold Schemes," *Advances in Cryptology - Proceedings of CRYPTO'87*, vol. 293, pp. 330-339, 1988.
- [12] 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.
- [13] 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.

- [14] 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.



송 영 원

2000년 2월 이화여자대학교 컴퓨터학과 학사. 2000년 3월 ~ 현재 이화여자대학교 컴퓨터학과 석사과정. 관심분야는 암호학, 정보이론, 네트워크 보안



박 소 영

1998년 2월 이화여자대학교 컴퓨터학과 학사. 2000년 2월 이화여자대학교 컴퓨터학과 석사. 2000년 3월 ~ 현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 정보보호, 암호프로토콜, 암호 알고리즘



이 상 호

1979년 2월 서울대학교 계산통계학과 학사. 1981년 2월 한국과학기술원 전산학과 석사. 1987년 8월 한국과학기술원 전산학과 박사. 1983년 9월 ~ 현재 이화여자대학교 컴퓨터학과 교수. 2000년 ~ 현재 한국정보과학회 총무이사, 정보보호연구회 부위원장. 관심분야 정보보호, 암호프로토콜, 알고리즘 설계, 계산기하, 그래프 드로잉, 데이터 마이닝, Bioinformatics