비밀조각의 재사용이 가능한 권한 위임 비밀분산법의 설계

(Design of a Reusable Secret Sharing Scheme in a Hierarchical Group)

양 성 미 † 박 소 영 † 이 상 호 ††
(Seong-Mi Yang) (So-Young Park) (Sang-Ho Lee)

요 약 비밀분산법이란 하나의 비밀정보(secret)를 분산시켜 다수의 참가자에게 공유시키고, 필요시 허가된 참가자 부분집합만이 비밀정보를 복원할 수 있는 암호 프로토콜이다. 비밀정보 복원을 위한 다양한 접근구조를 반영하는 비밀분산법이 제안되었는데, 본 논문에서는 계층구조에 적용 가능하고 재사용이 가능한 새로운 비밀분산법을 제안한다. 즉, 참가자들은 계층구조의 상위 레벨부터 비밀정보 복원에 대한 우선권을 갖고, 상위 레벨에 속하는 참가자들이 부재 시에는 하위 레벨에 속하는 참가자들은 위임티켓(delegation ticket)을 전송하여 비밀정보의 복원 권한을 위임할 수 있다. 또한, 각 참가자는 초기에 생성한 하나의 비밀조각으로 서로 다른 비밀정보를 복원하는데 참여할 수 있도록 함으로써, 계층그룹에서 비밀조각의 재사용이 가능하도록 한다.

키워드 : 정보보호, 암호, 비밀분산법

Abstract A secret sharing scheme is a cryptographic protocol that a dealer distributes shares about a secret to many participants and authorized subsets of the participants can reconstruct the secret. Secret sharing schemes that reflect various access structure were proposed. We propose a new reusable secret sharing scheme in a hierarchical group. Participants have priority about restoration of secret from high position level of tree. And when participants who belong in high position level are absent, they can delegate restoration competence of the secret transmitting delegation ticket to child nodes that it belongs in low rank level. By participants reuse own share and take part in different secret restoration, they who belong on hierarchical group can be possible different secret restoration by each participant's single share.

Key words : Information Security, Cryptography, Secret Sharing Scheme

1. 서 론

인터넷의 발달로 정보 획득과 이용이 보편화되면서 사이버 공간 상에서는 다양한 정보의 교류가 일어나고 있다. 더불어 네트워크 기술이 발전하면서 빠른 속도로 송·수신될 수 있는 환경을 마련하였으나, 불법적인 정보의 유출 등이 쉬워짐으로 비밀문서의 암호키 같은 주요 비밀정보(secret)를 안전하게 유지·관리하는 문제가 대두되었다. 이를 위해 다양한 암호 프로토콜이 연구되고 있는데 그 중 하나가 비밀분산법이다. 비밀분산법이란 하나의 비밀정보를 분산시켜 다수의 참가자들에게 공유시키고, 필요시 허가된 참가자 부분집합만이 비밀정보를 복원할 수 있는 방법이다. 비밀정보는 다항식과 같은 수학적 방법을 이용하여 분할되며, 분할된 정보만으로 원 비밀정보를 알 수 없다. 가장 대표적인 방법은 Shamir[1]와 Blakely[2]에 의해서 제안된 (t, n)-임계치법(threshold scheme)으로 비밀정보를 공유하는 n명의 참가자 중에 임의의 t명 이상의 참가자들이 모이면 원 비밀정보를 복원할 수 있는 방법이다.

비밀분산법은 응용환경에 따라 비밀정보를 복원하기 위해 다양한 접근구조가 반영되어야 한다. 은행이나 군조직 그리고 기업 등을 보면 조직 구성원간에 계층구조가 존재한다. 계층구조란 한 조직 내에서 의사 결정을 위한 각 구성원의 중요도 또는 우선권에 따른 지위를

† 비 회 원 : 이화여자대학교 컴퓨터학과
smyang@bible.ac.kr
soyoung@ewha.ac.kr
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2003년 1월 7일
심사완료 : 2003년 5월 19일

의미하며, 비밀정보를 공유하는 차원에서는 비밀정보 복원에 대한 상대적 권한을 나타낸다. 즉, 계층에 따라 참가자들이 갖는 비밀정보 복원 권한이 서로 다름을 의미한다. 상위 계층에 포함되는 구성원일수록 비밀정보 복원 권한이 높으므로 더 적은 수로 비밀정보를 복원할 수 있지만, 하위 계층에 포함되는 구성원일수록 비밀정보 복원 권한이 낮아서 비밀정보 복원을 위해서는 상대적으로 더 많은 정족수를 필요로 한다. 또한 이와 같은 그룹들은 서로 다른 임의의 비밀정보에 대해서 다루게 되고 참가자들은 각각의 비밀정보에 대해서도 참여할 수 있는 권한을 가지고 있어야 한다. 이와 같은 계층구조를 비밀분산법에 반영하기 위해서는 비밀정보에 대한 서로 다른 권한을 갖는 참가자들 사이에서 비밀정보를 공유하고 다시 복원하며, 각 참가자의 비밀조각을 재사용하여 서로 다른 비밀정보 복원에 참여 가능한 비밀분산법의 설계가 요구된다.

계층구조를 갖는 비밀분산법의 대표적인 예로 멀티레벨 비밀분산법이 있는데 이것은 계층구조가 레벨 단위로 존재하며, 각 레벨별로 비밀정보 복원을 위한 최소 정족수를 다르게 지정함으로써 레벨이 계층화된다. 즉, 각 레벨별로 고차다항식을 기반으로 하는 서로 다른 임계치법이 적용된다. 이를 좀 더 확장하여 위임을 허용하는 비밀분산법[3]이 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 권한은 최하위 레벨 참가자까지 위임될 수 있다. 그러나 제안된 방법은 비밀정보 하나에 대한 복원으로 임의의 비밀정보에 대해서는 매번 비밀조각을 새로 생성하고 전송하는 과정을 거쳐야 한다.

본 논문에서는 계층구조를 이루는 그룹에서 참가자들이 처음 생성한 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 자신의 비밀조각을 이용하여 원 비밀정보를 복원하는데 참여한다. 하나의 비밀정보에 대해 위임과정을 거쳐 다시 해당 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.

본 논문 2장에서는 비밀분산법의 기본 개념에 대해서 설명하고, 3장에서는 관련 연구로 계층구조를 반영하는 비밀분산법과 다중 비밀분산법 및 개별권한 위임을 허용하는 비밀분산법 등에 대해 소개한다. 4장에서는 본 논문에서 제안하는 프로토콜에 대해 구체적으로 기술하며, 5장에서는 결론을 맺는다.

2. 비밀분산법

비밀분산법이란 비밀정보를 안전하게 유지·관리하기 위한 암호 프로토콜 중의 하나로 원 비밀정보를 다수의 조각으로 분할하여 다수에게 공유시킴으로써 원 정보를 보다 안전하게 유지·관리하는 방법이다. 비밀정보 K에 대해서 분할된 다수의 조각을 비밀조각(share)이라고 하고, 비밀정보를 생성하고 분배하는 사람을 분배자(dealer)라고 하며, 생성된 비밀조각을 가지고 비밀정보 복원에 참여하는 사람을 참가자라고 한다. 참가자 집합은 $U=\{u_1, u_2, \cdots, u_n\}$라고 표기하고 각 참가자 u_i에게 분배되는 비밀조각은 S_{u_i}라고 표기한다. 비밀정보 K는 비밀정보 복원 권한을 가진 각 참가자들의 비밀조각으로부터 다시 복원될 수 있다.

이와 같은 비밀분산법의 대표적인 방법은 (t,n)-임계치법으로 Blakley와 Shamir에 의해 독립적으로 만들어졌다. 이것은 비밀정보 K를 n개의 비밀조각 S_{u_i}로 만들고, 그 중 임의의 t개 이상의 비밀조각이 모이면 원래 비밀정보 K를 완전히 복원할 수 있지만, $t-1$개의 비밀조각으로는 K에 관한 정보를 전혀 얻을 수 없는 방법이다. 따라서 $t-1$개까지 비밀조각를 도난 당해도 비밀정보가 누설되지 않으며, $n-t$개까지 비밀조각을 분실하거나 파괴되어도 원 비밀정보를 복원할 수 있다.

비밀분산법은 익명성 파기 전자 지불 시스템(anonymity revocable payment system)과 키 복구 시스템(key escrow system) 등 여러 응용분야에 적용되고 있다. 익명성 파기 전자 지불 시스템은 전자상거래 상에서 전자화폐를 이용한 전자 지불 시스템의 하나로 불법적인 사용자에 대해서는 신원 추적이 가능한 시스템이다. 이와 같이 신뢰기관에 의해서 추적 기능을 제공하기 위해서 비밀분산법이 사용되고 있다.

이 밖에도 분할 가능한 전자 화폐(divisible electronic cash)에서 분할성을 제공하기 위한 암호학적 방법으로 비밀분산법이 사용되고 있고, 이미지를 이용한 시각 암호(visual cryptography)의 주요 기술로 사용되고 있다. 시각 암호는 각각의 개별된 이미지는 의미있는 이미지를 갖고 있지 않지만, 여러 장의 이미지가 겹쳐지면 하나의 의미있는 이미지를 얻을 수 있는 암호 기술을 의미한다.

3. 관련 연구

3.1 계층구조를 반영하는 비밀분산법

계층구조를 반영하는 비밀분산법에는 다중레벨 비밀분산법(multilevel secret sharing scheme)[4]과 가중치에 의한 비밀분산법(weighted threshold secret sharing scheme)[5]이 있다.

다중레벨 비밀분산법이란 1988년 G. J. Simmons에 의해 제안된 것으로 계층구조는 레벨로 구분하여 각 레벨에 속한 참가자들의 비밀정보 복원 권한을 다르게 부여하는 방법이다[4]. 참가자들은 자신이 속하는 레벨별로 그룹화 되고 레벨마다 비밀정보 복원을 위해 필요한 최소 정족수가 다르다. 각 레벨은 그 레벨에서의 최소 정족수에 해당하는 양의 정수값으로 표현된다. 예를 들어 레벨 1인 사람은 혼자서 비밀정보를 복원할 수 있지만, 레벨 2인 사람은 적어도 2사람이 있어야 비밀정보를 복원할 수 있다. 하위 레벨에 속한 참가자들은 상대적으로 더 많은 수가 모여야만 비밀정보를 복원할 수 있다. 이 방법에서는 레벨에 따른 고차 다항식(high-degree polynomial)을 이용하는데 레벨의 수가 증가할수록 계산량이 증가한다.

가중치에 의한 비밀분산법이란 1999년 P. Morillo, C. Padro, G. Saez, J. L. Villar에 의해 처음 제안된 것으로 비밀정보 복원을 위해 각 참가자가 갖는 권한을 가중치로 표현하여 가중치의 합이 사전 정의된 임계치값보다 같거나 크면 비밀정보를 복원할 수 있지만 그렇지 않은 경우에는 비밀정보에 대한 어떠한 정보도 얻을 수 없도록 하는 방법이다. 그러나 이 방법에서는 최소접근집합을 구성하는 최대 원소수가 2이고 최소접근집합을 구성하는 원소 수가 모두 동일해야하는 제약사항을 가지고 있다.

3.2 다중 비밀분산법

다중 비밀분산법(multisecret sharing scheme)이란 임의의 비밀정보들에 대해 각 참가자에게 부여된 하나의 비밀조각을 재사용하여 임의의 서로 다른 비밀정보들을 복원하는 방법이다.

1996년 Pinch[6] 등은 공개보드를 사용하여 임의의 서로 다른 비밀정보를 복원하는 다중 비밀분산법을 제시하였다. 서로 다른 비밀정보를 복원하기 위해서 각 참가자의 비밀조각은 분배자에 의해 각 비밀정보들과 무관하게 생성되어 분배된다. 임의의 비밀정보를 복원하기 위해서 사전에 정의된 최소 정족수를 만족하는 참가자 부분집합이 구성되면, 분배자는 이들의 비밀조각과 복원하고자하는 비밀정보를 이용하여 비밀복원정보를 만들어 공개보드에 제시한다. 비밀복원에 참여하는 해당 참가자들은 제시된 비밀복원정보를 이용하여 해당 비밀정보를 복원한다. 이 때, 분배자는 모든 참가자의 비밀조각을 알고 있어야 한다. Ghodosi[7] 등은 Pinch의 방법에서 부정직한 참가자가 참여했을 경우 비밀조각 속임(cheating)으로 비밀정보 복원에 참여한 다른 참가자들은 옳지 않은 비밀정보를 복원하게 하고 부정직한 참가자만이 옳은 비밀정보를 복원할 수 있는 문제점을 발견하여 보완하였고, Chen[8] 등은 Pinch의 방법을 기본으로 하되 공개보드의 크기를 줄이는 방법을 제시하였는데, 이 방법은 Shamir(t, n)-임계치법의 다항식을 이용한다. Sun[9]은 해쉬함수와 덧셈 연산을 기반으로 하여 Pinch 및 Ghodosi의 방법에서 연속적인 지수연산으로 계산상의 효율성 문제와 비밀정보 복원 시 참가자 순서에 의한 참여로 길어졌던 복원 시간의 효율성 문제를 보완하였다.

1998년 Hwang[10] 등은 RSA의 구성요소와 Shamir (t, n)-임계치법를 이용하여 공개키 기반에서 사용할 수 있는 비밀분산법을 제안하였다. 각 참가자는 스스로 비밀조각을 선택하고 그것에 해당하는 공개정보를 공개보드를 통해 게시한다. 임의의 비밀정보를 복원하기 위해서 정족수를 만족하는 참가자 부분집합이 구성되면 분배자는 각 참가자의 공개정보를 이용하여 해당 참가자들과 공유할 수 있는 새로운 키들을 만들고 만들어진 키들을 사용하여 해당 비밀복원정보를 생성한다. 비밀정보가 공개보드에 게시되면 참가자들은 자신의 비밀조각과 게시된 비밀복원정보를 이용하여 원 비밀정보를 복원한다. 이로써 분배자가 각 참가자의 비밀조각을 모두 알고 있지 않더라도 해당 비밀정보를 복원할 수 있다. 이 외에도 이산대수 문제의 키 교환과 라그랑지 보간법(Lagrange interpolation)을 이용한 방법도 제시하였다[11].

3.3 권한 위임에 따른 비밀분산법

권한 위임에 따른 비밀분산법이란 비밀정보 복원 참여 권한을 가진 참가자가 해당 비밀정보 복원 시 참여하지 못할 경우, 그 권한을 다른 참가자들에게 위임하여 위임을 받은 참가자들로 하여금 비밀정보 복원에 참여하게 하는 방법이다.

Ghodosi[12] 등은 계층구조를 갖는 참가자 집합에 대하여 레벨간의 위임(delegation)에 의한 계층적 위임을 허용하는 비밀분산법(hierarchical delegation secret sharing scheme)을 제안하였다. 이 방법은 상위 레벨이 비밀정보 복원에 대한 우선권을 가지며 하위 레벨은 상위 레벨의 권한 위임을 받은 후에 비밀정보 복원에 참여할 수 있다. 여기에서 위임은 레벨간 위임이기 때문에 레벨 i의 참가자들이 부재 시 특정 하위 레벨로 비밀정보 복원 권한을 위임하기 위해서는 i레벨 참가자 부분집합인 위임 구조(delegation access structure)에 속하는

참가자들의 위임 결정 합의가 전제되어야한다. 위임과정은 위임티켓(delegation ticket)의 생성과 전송으로 이루어지며 레벨 단위로 위임이 이루어지므로 위임을 받지 않은 다른 레벨 참가자들의 비밀정보 복원은 불가능하다.

송영원[3] 등은 Ghodosi[12]의 계층적 위임 비밀분산법을 확장하여 트리 형태의 계층구조를 갖는 집합에 대해 참가자간 개별 위임을 허용하는 비밀분산법을 제시하였다. 참가자들은 트리 형태의 계층구조를 갖는 집합으로 이루어져 있고 최고 레벨에서 비밀정보를 소유한다. 상위 레벨 참가자의 부재시 위임을 통해 하위 레벨의 참가자들에게 위임티켓을 전송함으로 비밀정보 복원 권한을 위임하여 서로 다른 레벨의 참가자 조합이 비밀정보를 복원할 수 있도록 한다. 위임과정 및 비밀정보 복원과정을 보면, 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 전송 받은 위임티켓으로부터 비밀정보를 복원할 수 있다. 하위 레벨의 참가자들이 상위 레벨로부터 위임을 받지 않은 경우에는 자신들의 비밀조각만으로 비밀정보를 복원할 수 없다[3].

4. 계층구조를 갖는 그룹에서 재사용이 가능한 비밀분산법

본 논문에서는 [3]에서 제안된 트리 형태의 계층구조에 적용 가능한 비밀분산법을 확장하여 생성된 비밀조각을 재사용하여 l개의 서로 다른 비밀정보를 복원할 수 있는 방법을 제안한다. 기존의 권한위임에 따른 비밀분산법[3]은 해당 비밀정보에 따라 부모 노드 참가자가 자식 노드 참가자들의 비밀조각을 생성하여 전송하고 위임 및 비밀정보 복원 과정이 끝나면 모든 참가자의 비밀조각을 다시 생성한다. 또한 비밀조각 생성과정에서 부모 노드 참가자들은 자신의 자식 노드 참가자들의 비밀조각을 모두 알고 있다. 또한 상위 레벨부터 위임이 일어나 h번째 계층까지 비밀정보 복원 권한이 전송될 경우, h-1개의 위임티켓이 모두 전송되어야 한다. 제안하는 프로토콜에서는 각 참가자가 임의로 비밀조각을 선택하고 이것을 이산대수 문제에 근거하여 공개정보를 생성하고 공개보드에 게시하여 부모 노드 참가자가 자식 노드 참가자의 비밀조각을 알고 있지 않더라도 프로토콜이 수행될 수 있다. 또한 처음 생성한 비밀조각으로 매 비밀정보의 복원 시 마다 세션비밀조각을 생성하므로 하나의 비밀조각으로 l개의 서로 다른 비밀정보에 대한 복원이 가능하다. 세션비밀조각은 위임티켓과 비밀조각을 이용하여 생성한 값으로 해당 비밀정보에 대해서 상위 레벨로부터 받은 위임권한을 만족한다. 위임을 받은 참가자는 위임한 부모 노드 참가자의 세션비밀조각을 복원하고, 이것으로 부모 노드 참가자가 상위 레벨로부터 받은 위임권한을 동시에 소유하게 된다. 따라서 h번째 계층의 참가자는 하나의 위임티켓만으로 상위 레벨 참가자들과의 비밀정보 복원이 가능하다.

가정하는 계층구조와 위임구조는 [3]과 같이 일반적인 트리 형태의 계층구조와 개별 권한 위임을 허용하는 것으로 참가자들은 그룹의 상위 레벨 참가자부터 비밀정보 복원에 대한 우선권을 가진다. 한 명으로 구성되는 최상위 레벨인 루트 노드 참가자는 비밀정보에 대한 접근 권한을 가지며 우선권을 가진 참가자들이 비밀정보 복원 시 참여할 수 없을 경우 임의의 위임티켓을 생성하여 하위 레벨 참가자들에게 전송한다. 비밀정보 복원 시 자식 노드 참가자는 자신의 비밀조각과 받은 위임티켓으로 세션비밀조각을 생성하고, 이것을 이용하여 같은 계층의 참가자들과 함께 부모 노드 참가자의 세션비밀조각을 복원한다. 부모 노드 참가자의 세션비밀조각에는 상위 레벨로부터 받은 위임권한이 포함되어 있다. 그러나 이것으로 해당 참가자의 비밀조각을 알아낼 수 없다.

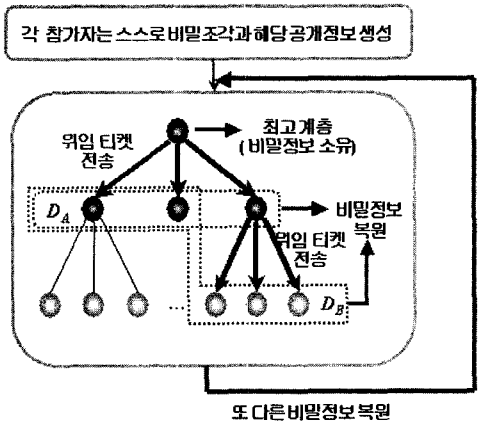

그림 1 전체 흐름도

제안하는 논문에서는 n명의 참가자로 구성되는 참가자 집합을 $U=\{u_0, u_1, \ldots, u_{n-1}\}$로 표기한다. 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 세

션이라고 한다. 최상위 레벨인 루트 노드 참가자는 u_0이고, l개의 비밀정보를 알고 있다.

4.1 비밀조각 생성

비밀조각 생성 단계는 l번의 세션에서 단 한번 일어나는 과정으로 루트 노드 참가자를 제외한 나머지 각 참가자가 자신의 비밀조각을 생성하는 단계이다. 최상위 레벨인 루트 노드 참가자 u_0의 비밀조각은 $S_{u_0}^{[w]} = K^{[w]}$이고, 각 내부 노드 참가자 u_i가 l번의 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 생성원 g를 선택하여 공개보드에 게시한다.

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

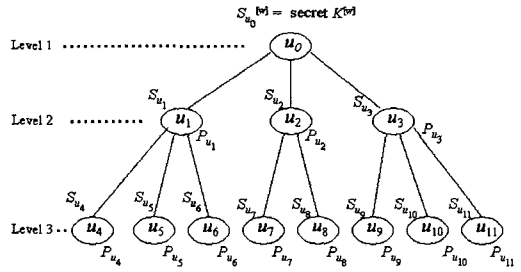

그림 2 계층구조의 그룹 표현 예

u_0는 각 참가자가 공개하는 P_{u_i}가 중복되는지를 검사하여 동일한 값이 생성된 경우는 재생성하도록 조정한다. u_0는 매 세션마다 자신의 비밀조각 $S_{u_0}^{[w]}$을 새롭게 정의하지만 u_0를 제외한 모든 참가자들은 위 과정을 통해 생성된 비밀조각을 모든 세션에 걸쳐 재사용한다.

4.2 위임과정

위임과정은 비밀정보 복원 권한이 있는 참가자들 중 해당 세션$[w]$에 참여할 수 없는 참가자 u_i가 자신의 자식 노드 참가자 $c_{i1}, \ldots, c_{it}$에게 세션$[w]$의 권한 위임을 위한 위임티켓 $g^{dt_{u_i}^{[w]}}$과 비밀정보 $K^{[w]}$에 대한 비밀복원정보 $T_{u_i}^{[w]}$를 생성하여 전달하는 과정이다.

u_i는 자신의 세션비밀조각과 그리고 자식 노드 참가자들에게 전송하는 위임티켓 그리고 해당 참가자들의 공개정보를 이용하여 비밀복원정보 $T_{u_i}^{[w]}$를 만들고, 자신이 생성한 하나의 위임티켓만 자식 노드 참가자들에게 전달한다.

이것은 매 세션마다 새롭게 수행되며, 세션$[w]$에서의 위임과정은 다음과 같다. 단, w는 $1 \le w \le l$ 이다.

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

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

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

③ 위임을 받은 참가자들 중에서 다시 해당 세션에 참여하지 못하는 참가자 u_i 발생시, ①과 같은 방법으로 위임비밀조각 $dt_{u_i}^{[w]}$을 선택하고, 위임티켓 $g^{dt_{u_i}^{[w]}}$을 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 $g^{dt_{u_{p_i}}^{[w]}}$과 자신의 비밀조각 S_{u_i}을 이용하여 생성한 세션 비밀조각 $(g^{dt_{u_{p_i}}^{[w]}})^{S_{u_i}}$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.

4.3 비밀정보 복원

위임받은 참가자들이 모여 루트 노드 참가자의 비밀정보를 복원하는 과정은 다음과 같다. 위임과정이 이루어진 가장 하위 레벨의 참가자들부터 부모 노드 참가자의 세션비밀조각을 생성해 나감으로써 최종적으로 루트 노드 참가자의 비밀조각 $S_{u_0}^{[w]}$을 복원하여 원 비밀정보 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 전송받은 위임티켓을 이용하여 자신의 세션비밀조각 $(g^{dt_{u_{p_i}}^{[w]}})^{S_{c_{ij}}}$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.

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

부모 노드 참가자의 세션비밀조각을 복원한 자식 노드 참가자들은 부모 노드 참가자의 세션비밀조각에 포함된 상위 레벨의 위임권한을 동시에 소유하게 된다. 이들은 다시 부모 노드의 형제 노드 참가자들과 함께 ① - ②과정을 통해 조부모 노드 참가자의 세션비밀조각을 복원할 수 있다. 이러한 과정을 반복적으로 수행하여 최종적으로 루트 노드 참가자의 비밀조각인 $S_{u_0}^{[w]}$를 알아냄으로서 비밀정보 $K^{[w]}$를 복원할 수 있다.

상위 레벨의 부모 노드로부터 위임티켓을 받지 못한 참가자는 그들이 가진 비밀조각만으로 부모 노드 참가자의 세션비밀조각을 복원할 수 없고, 다른 참가자의 위임티켓 $g^{dt_{u_i}^{[w]}}$을 얻었다 하더라도 해당 참가자의 비밀조각을 알지 못하므로 비밀정보 복원에 참여할 수 없다.

4.4 비밀조각 재사용

각 참가자의 비밀조각을 재사용하여 또다른 비밀정보를 복원하기 위해서 4.2와 4.3의 과정을 반복 수행한다. 예를 들어 비밀정보 $K^{[w+1]}$을 복원한다고 하면 루트 노드 참가자 u_0의 비밀조각은 $S_{u_0}^{[w+1]}=K^{[w+1]}$ 가 된다. 자식 노드 참가자 $c_{01},\ldots,c_{0t}$에게 세션 $[w]$에서 사용하였던 위임티켓과는 다른 위임티켓을 선택하여 위임과정을 수행한다($g^{dt_{u_0}^{[w]}} \neq g^{dt_{u_0}^{[w+1]}}$). 비밀정보 복원권한이 또다시 하위 레벨로 위임될 때, 해당 참가자 u_i 또한 w번째 세션에서 사용했던 위임비밀조각과는 다른 $dt_{u_i}^{[w+1]}$을 임의로 선택하여 위임티켓을 생성한다. 이 때 새로 생성된 위임티켓으로 인해 각 참가자가 만들게되는 세션비밀조각 $(g^{dt_{u_i}^{[w+1]}})^{S_{c_{ij}}}$은 매 세션마다 서로 다르게 되고 비밀복원정보 $T_{u_i}^{[w+1]}$도 변하게 된다. 따라서 w번째 비밀정보 $K^{[w]}$에서 u_i의 자식 노드 참가자들이 u_i의 세션비밀조각 $(g^{dt_{u_i}^{[w]}})^{S_{u_i}}$을 알고 있다 하더라도 $w+1$번째 비밀정보 복원 시에는 사용할 수 없고, 세션 $[w]$에서는 위임권한을 받았지만 세션 $[w+1]$에서 위임권한을 받지 않은 참가자 역시 비밀정보 복원과정에 참여할 수 없다. 이로써 각 참가자들은 비밀조각의 변경없이 재사용하여 비밀정보를 복원할 수 있다.

5. 안전성 및 특성 분석

5.1 안전성 분석

제안한 논문의 안전성은 다음의 네 가지로 분석될 수 있다.

첫째, 다른 참가자 u_i의 세션비밀조각을 알게되더라도 u_i의 비밀조각에 대한 정보를 얻을 수 없다. u_i의 세션비밀조각은 $(g^{dt_{u_i}^{[w]}})^{S_{u_i}} \pmod p$로 이산대수 문제의 어려움에 근거하여 유한체 Z_p상에서 $g^{dt_{u_i}^{[w]}}$만을 알고 있는 참가자가 S_{u_i}를 찾는 것은 어렵다.

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

셋째, 위임을 받지 않은 참가자가 다른 레벨 혹은 같은 레벨의 다른 참가자의 위임티켓 $g^{dt_{u_i}^{[w]}}$의 정보만으로 비밀정보 복원에 참여할 수 없다.

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

비밀복원정보 $T_{u_i}^{[w]}$는 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.

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

5.2 특성 분석

제안한 논문은 [3]의 논문과 비교하여 다음의 세 가지 특성을 갖는다.

첫째, 참가자가 비밀조각을 분실했을 경우, 다른 참가자 비밀조각의 변경없이 새로운 비밀조각 생성이 가능하다. 비밀조각 생성 단계에서 루트 노드 참가자를 제외한 각 참가자는 유한체 Z_p상의 일정한 간격에서 임의로 비밀조각을 선택하고 이를 공개정보를 통해 게시한다. 이와 같이 생성된 비밀조각들은 각기 어떠한 값으로 연관되어 생성된 값이 아니기 때문에 참가자가 비밀조각을 분실했다 하더라도 다른 참가자의 비밀조각과 같은 값이 아니라면 임의의 값으로 재생성이 가능하다.

둘째, 모든 참가자의 비밀조각은 비밀성을 만족한다. 부모 노드 참가자가 비밀조각을 생성해 전달해주는 방식이 아니라 각 참가자가 임의로 선택하고 해당 공개정보를 이용하여 비밀정보 복원에 참여하기 때문에 부모 노드 참가자라고 해서 자식 노드 참가자의 비밀조각을

알 수 없다.

셋째, 위임과정에서 해당 참가자는 자신이 생성한 하나의 위임티켓만 전송한다. h번째 계층의 참가자 c_{i1}, …, c_{it}에 의해 복원되는 부모 노드 참가자의 세션비밀조각에는 상위 레벨에서 받은 위임티켓의 정보가 포함되어있다. 따라서 $h-1$개의 위임티켓을 받지 않더라도 상위 레벨 참가자의 세션비밀조각만 복원해 나가면 위임권한을 자동적으로 부여받을 수 있다.

6. 결 론

정보화 사회로 진행됨에 따라 공공기관, 병원, 기업등의 각 문서들이 데이타베이스에 저장 가능한 전자 문서의 형태로 바뀌어가고 있다. 더불어 인터넷을 통한 다양한 정보의 교류로 인해 정보보호의 문제가 대두됨에 따라 다양한 암호 프로토콜의 방법이 연구되고 있다. 비밀분산법은 비밀정보 보호를 위한 암호 프로토콜 중의 하나로 주요 비밀정보에 대해 수학적 방법 등을 이용하여 다수의 비밀조각으로 분할하여 다수에게 공유시킴으로원 비밀정보를 안전하게 관리하는 방법이다.

본 논문에서는 대규모 기업체와 같이 계층구조가 형성되어 비밀정보 복원권한 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 비밀조각과 위임권한이 수학적 방법에 의해 동시에 만족되는 세션비밀조각을 생성하여 하위 레벨로 전달하는 하나의 위임티켓만으로도 상위 레벨의 모든 위임권한을 받을 수 있다. 복원된 비밀정보로 인하여 참가자들의 비밀조각도 드러나지 않아 재사용이 가능하다.

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," Proc. of AFIPS, vol. 48, pp. 313-317, 1979.

[3] 송영원, 박소영, 이상호, "트리형태의 계층구조에 적용가능한 비밀분산법의 설계", 한국정보과학회 논문지(컴퓨터 시스템 및 이론), 제29권 4호, 2002.

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

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

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

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[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.

양 성 미

2001년 2월 대진대학교 컴퓨터공학과 학사. 2003년 2월 이화여자대학교 컴퓨터학과 석사. 2003년 3월~현재 한국성서대학교 정보통신학과 및 교양학부 강사 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

정보과학회논문지 : 시스템 및 이론
제 30 권 제 8 호 참조