가중치를 갖는 비밀분산법
(Weighted Secret Sharing Scheme)

박 소 영 † 이 상 호 †† 권 대 성 †††
(So-Young Park) (Sang-Ho Lee) (Dae-Sung Kwon)

요 약 비밀분산법이란 하나의 비밀정보를 다수의 비밀조각으로 분할하여 다수의 신뢰할 수 있는 사람들에게 공유시킴으로써 비밀정보를 안전하게 유지·관리하는 암호학적 방법이다. 그러나 비밀정보를 공유하는 참가자들이 비밀정보 복원에 대해 서로 다른 권한을 가지고 있을 경우, 이러한 참가자들간의 계층구조를 반영할 수 있는 비밀분산법의 설계가 필요하다. 각 참가자들이 갖는 비밀정보에 대한 복원 권한을 가중치로 표현함으로써 가중치에 따른 비밀정보 공유 및 복원이 가능한 가중치를 갖는 비밀분산법을 제안한다.

키워드 : 정보보호, 암호, 비밀분산법

Abstract A secret sharing scheme is a kind of cryptographic protocol to maintain secret information by splitting it to many small pieces of shares and sharing between shareholders. In case of shareholders having different authorization to reconstruct the original secret, it is required a new secret sharing scheme to reflect any hierarchical structure between shareholders. In this paper, we propose a new weighted secret sharing scheme, that is, each shareholder has a weight according to the authorization of reconstructing the secret and an access set which is a subset of shareholders can reconstruct the secret if the sum of weights is equal or greater than a predefined threshold.

Key words : Cryptography, Secret Sharing, hierarchy

1. 서 론

비밀정보를 얼마나 안전하게 유지·관리할 수 있을 것인가 하는 것은 컴퓨터 보안 관련 분야에서 가장 핵심이 되는 문제이다. 비밀분산법(secret sharing scheme)은 이를 위한 하나의 해결책으로 하나의 비밀정보를 다수에게 공유시킴으로써 비밀정보를 안전하게 유지·관리시키는 암호학적 기술이다. 은행에서 비밀금고의 문을 열기 위해서는 적어도 2개 이상의 키가 있어야만 가능하다. 구 소련의 미사일 발사권은 대통령과 국방부 장관 그리고 군 참모총장 세 사람의 키가 모두 있어야만 가능하다. 이와 같이 주요한 비밀정보를 획득하기 위해서는 다수의 합의에 의해서만 가능하게 하는 암호학적 기술이 비밀분산법이다. 이를 위해 분할된 다수의 조각을 비밀조각(share)이라고 한다. 비밀정보에 대한 비밀조각을 생성할 수 있는 사람을 분배자(dealer)라고 하고 각 비밀조각을 분배받는 사람을 참가자(participant 또는 shareholder)라고 한다. 참가자들 중에서 원 비밀정보를 다시 복원할 수 있는 참가자들의 집합을 접근집합(access set)이라고 하며, 원 비밀정보를 복원할 수 있는 참가자들의 관계를 접근구조(access structure)라고 한다.

가장 기본적인 접근구조는 1979년 Blakley[1]와 Shamir[2]가 제안한 방법으로 비밀조각을 공유하는 n명의 참가자 중에서 임의의 t명 이상의 참가자들이 모이면 원 비밀정보를 복원할 수 있고 t명 미만의 참자들만으로는 비밀정보를 복원 할 수 없게 하는 방법으로 (t, n)-임계치법(threshold scheme)이라고 한다.

그러나 응용문제에 따라 임의의 t명에 의해서가 아니라 다양한 접근구조가 반영되는 비밀분산법이 요구된다. 은행이나 군조직 그리고 기업 등에서는 조직 구성원간

· 이 연구는 한국전자통신연구원 부설 국가보안기술연구소 연구비 지원에 의해 연구되었음.
† 학생회원 : 이화여자대학교 컴퓨터학과 과학기술대학원
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
††† 정 회 원 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
논문접수 2001년 5월 14일
심사완료 2001년 11월 7일

에 계층구조가 존재한다. 계층구조란 한 조직 내에서 의사 결정을 위한 각 구성원의 중요도 또는 우선권에 따른 지위를 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. 이와 같은 계층구조를 비밀분산법에 반영할 수 있기 위해서는 비밀정보에 대한 서로 다른 권한을 갖는 참가자들 사이에서 비밀정보를 공유하고 다시 복원할 수 있는 비밀분산법의 설계가 요구된다. 이는 기존의 비밀분산법을 그대로 적용할 수 없으며, 이를 위한 새로운 비밀분산법의 설계가 요구되고, 본 논문에서는 이를 위한 해결책을 제시한다.

비밀정보를 공유하는 각 참가자들이 갖는 비밀정보 복원에 대한 권한을 가중치로 표현하여, 가중치의 합이 사전 정의된 임계값과 같거나 큰 경우에는 비밀정보를 복원할 수 있고, 그렇지 않은 경우에는 비밀정보에 대한 어떤 정보도 획득할 수 없는 완전 비밀분산법(perfect secret sharing scheme)을 제시한다.

2. 기본 정의 및 개념

참가자들의 집합 $P=\{P_1, \ldots, P_n\}$에 대해서 접근구조(access structure) Γ는 $\Gamma \subset 2^P$로 비밀정보를 복원할 수 있는 P의 부분집합들의 계(family)이다. 접근구조는 단조성(monotone)을 가지며, 임의의 접근 집합 A, B에 대해서 $A \in \Gamma$이고 $A \subset B \subset P$일 때, B가 $B \in \Gamma$이면 접근구조가 단조성을 가진다고 한다[3]. 따라서 접근 구조는 최소접근집합(minimal access set) $\Gamma_0 \subset \Gamma$들의 계로 결정될 수 있다[3].

비밀정보를 k라고 하고, 각 참가자 P_i가 갖는 공유정보를 s_{P_i}라고 했을 때, 참가자 집합 P에 대한 접근구조 Γ에 대해서 (1)비밀정보 복원 권한을 갖는 참가자 부분집합(authorized subsets)은 자신들의 공유정보를 이용하여 비밀정보 k를 복원할 수 있지만, (2)권한이 없는 참가자 부분집합(non-authorized subsets)은 비밀정보 k에 대한 어떤 정보도 획득할 수 없으면 완전 비밀분산법(perfect secret sharing scheme)이라고 한다[3].

임의의 접근구조가 주어졌을 때 이를 반영하기 위한 비밀분산법은 다양하게 존재할 수 있다. 따라서 최적화된 방법을 선별하기 위해서는 비밀분산법의 성능 측정이 필요하다. 시스템의 안전성(security)은 분산되는 정보량에 비례하여 저하된다. 따라서 원 비밀정보량에 대한 각 참가자에게 분배되는 비밀조각의 정보량 비율인 정보비(information rate)[4]는 비밀분산법에서 주요한 성능 측정 기준이다. 비밀정보 k가 가질 수 있는 모든 가능한 값의 개수를 q라고 하고, 가능한 공유정보 집합의 최대 크기를 s라고, $s = \max_{p \in P}|s_P|$, 했을 때, 정보비 $\rho = \frac{\log q}{\log s}$로 정의된다. 즉, 비밀정보가 가지는 비트 길이와 최대 크기의 공유정보가 가지는 비트(bit) 길이 간의 비율을 의미한다. $\rho \leq 1$이며, $\rho = 1$인 경우를 이상적 비밀분산법(ideal secret sharing scheme)이라고 한다[5].

[정의] 가중치를 갖는 비밀분산법

가중치를 갖는 비밀분산법이란, n명의 참가자로 구성된 참가자 집합 $P = \{P_1, \ldots, P_n\}$와, 임계값 $t>1$ 그리고 각 참가자에게 자연수로 표현되는 가중치 $w(P_i) \geq 0$를 부여하는 가중치 함수 $w : P \rightarrow N$가 주어졌을 때, 다음의 접근구조를 갖는 비밀분산법을 의미한다.

참가자 부분 집합 $A \subset P$에 대해서

(1) $w(A) = \sum_{p \in A} w(p) \geq t$ 이면 비밀정보 k를 복원할 수 있고,

(2) 그렇지 않은 경우에는 비밀정보 k에 대한 어떤 정보도 획득할 수 없다.

따라서, 접근집합 Γ은 임의의 부분집합 A에 대해서 $w(A) = \sum_{p \in A} w(p) \geq t$ 인 모든 부분집합들의 집합이다. ■

3. 관련연구

참가자들 사이의 계층구조를 반영하는 비밀분산법의 대표적인 예로서는 멀티 레벨 비밀분산법(multi-level secret sharing scheme)[5]과 가중치를 갖는 임계치법(weighted threshold secret sharing scheme)[6]을 들 수 있다.

멀티 레벨 비밀분산법[5]은 1989년 E. F. Brickell에 의해 제시되었으며, 고차다항식을 이용한 비밀분산법이다. 즉, 각 참가자들은 레벨별로 그룹화 되어있고, 각 레벨에 따라 비밀정보 복원을 위해 필요한 최소 정족수를 다르게 함으로써 참가자간의 계층 구조를 반영하는 비밀분산법이다. 상위 레벨일수록 비밀정보 복원을 위한 정족수가 적고, 하위 레벨일수록 비밀정보 복원을 위한 정족수가 많다. 각 레벨은 다항식의 차수로 표현되므로

레벨 L_i에 포함되는 참가자들은 L_i차 다항식(L_i-degree polynomial)에 의해 생성된 공유정보를 갖는다. 각 참가자는 n차 공유정보 벡터를 가지며, 정보비는 1로서 이상적 비밀분산법(ideal secret sharing scheme)이다.

가중치를 갖는 임계치법[6]은 1999년 P. Morillo, C. Padro, G. saez, J. L. Villar에 의해 제시되었으며 그래프기반[7,8] 비밀분산법이다. 이는 비밀정보 복원을 위해 각 참가자가 갖는 권한을 가중치로 표현하여 가중치의 합에 의해 비밀정보를 복원할 수 있도록 하는 비밀분산법으로 본 논문에서 해결하고자 하는 문제와 동일하다. 그러나 이 방법은 랭크(rank)가 2라는 제약사항을 갖는다. 즉, 비밀정보를 복원하기 위한 최소접근집합(minimal access set)의 최대 원소수가 모두 2 이여야만 한다. 이것은 최소접근집합을 구성하는 부분집합들의 원소수가 모두 최대 두 개이므로 최소접근구조(minimal access structure)가 그래프로 표현 가능하며, 그래프 분할(graph decomposition)방법[9]에 의하여 비밀분산법이 적용될 수 있다. 최소접근구조가 l-가중치 그래프(l-weighted graph)[6]로 표현되었을 때, 제시된 방법의 정보비 $\rho = \frac{1}{\lceil \log_2(l+1) \rceil}$ 이다.

4. 가중치를 갖는 비밀분산법의 설계

본 논문에서는 기존의 계층 구조를 갖는 비밀분산법을 보다 일반화시키고, 기존의 가중치를 갖는 임계치법이 갖는 랭크 2라는 제약사항을 제거함으로써 보다 확장된 가중치를 갖는 비밀분산법을 제시한다.

각 참가자들은 비밀정보 복원 권한에 따라 자연수 값으로 표현되는 가중치를 부여받으며, 비밀정보 복원 권한이 높은 참가자일수록 큰 수의 가중치를 부여받고, 동일한 권한을 갖는 참가자는 동일한 가중치 값을 부여받는다. 그러나 최대 가중치를 갖는 참가자도 혼자서는 비밀정보를 복원할 수 없다. 따라서 최대 가중치를 갖는 참가자는 최하 가중치를 갖는 참가자부터 자신을 제외한 모든 다른 참가자들과 함께 비밀정보를 복원할 수 있다. 그 다음으로 높은 가중치를 갖는 참가자는 자신보다 높은 가중치를 갖는 참가자 또는, 최하 가중치를 갖는 참가자를 제외한 다른 참가자들과 함께 비밀정보를 복원할 수 있다. 또한 가중치의 합에 의해 비밀정보 복원 여부가 결정되므로 상위 가중치를 갖는 참가자들은 더 많은 수의 하위 가중치를 갖는 참가자들에 의해 역할이 대행될 수 있다. 즉, 가중치 집합 $W = \{W_1, \ldots, W_l\}$라고 하고, 가중치 W_i에 해당하는 참가자 수를 N_i라고 하자. 단, 여기서 $W_1 > W_2 > \ldots > W_l > 0$이다. 최대 가중치 W_1을 갖는 참가자들은 W_l 이상의 모든 다른 가중치를 갖는 참가자들과 함께 비밀정보를 복원할 수 있고, W_2를 갖는 참가자들은 W_{l-1} 이상의 모든 다른 가중치를 갖는 참가자들과 함께 비밀정보를 복원할 수 있으며, W_3을 갖는 참가자들은 W_{l-2} 이상의 가중치를 갖는 참가자들과 함께 비밀정보를 복원할 수 있거나 또는 W_{l-2}를 갖는 참가자를 대신하여 W_{l-1} 또는 W_{l-1}과 W_l 모두에 의해서 비밀정보를 복원할 수 있다. $N_{l-1} > 1$인 경우에는 W_{l-1}을 갖는 모든 참가자들이 모여서 W_{l-2}와 대등한 역할을 수행할 수 있고, $N_{l-1} = 1$인 경우에는 W_{l-1}과 W_l을 갖는 모든 참가자들이 모여서 W_{l-2}와 대등한 역할을 수행할 수 있다. 다른 가중치에 대해서도 동일한 방법으로 비밀정보 복원을 위한 접근 집합을 정의할 수 있다.

$t>0$를 비밀정보 복원을 위한 임계값이라고 하고 $w:P \rightarrow N$을 제안하는 비밀분산법의 접근 구조를 정의하는 가중치 함수라고 했을 때, 비밀정보 복원을 위한 최소접근구조는 트리로 표현된다. 트리의 각 노드는 가중치 값을 나타내고, 루트(root)로부터 단말 노드까지의 하나의 경로(path) 상의 모든 노드 집합은 비밀정보를 복원할 수 있는 하나의 참가자 부분 집합을 나타낸다.

4.1 최소접근트리의 구성

적어도 2명 이상의 참가자가 모여야만 비밀정보를 복원할 수 있다고 가정하였으므로, 최소접근집합의 최소 원소 수는 2이다. 따라서, 최소접근트리의 생성 과정은 최소접근집합의 기수가 2인 경우와 3이상인 두 가지 경우로 구분하여 생각할 수 있다.

4.1.1 원소수가 2인 경우

주어진 가중치 집합 W에서 누구와도 비밀정보를 복원할 수 있는 최대 가중치를 Wh라고 하고, Wh 이외의 가중치와는 비밀정보를 복원할 수 없는 최소 가중치를 Wl 이라고 하자. 가중치 집합에서 이 둘을 제거하고 나면, 다시 남은 가중치 집합에서 Wh와 Wl이 결정된다.

따라서 가중치 집합 W는

$W = Wh_1 \cup Wl_1 \cup Wh_2 \cup Wl_2 \cup \cdots \cup Wh_d \cup Wl_d$,

와 같고, 참가자 집합 P는

$P = WH_1 \cup WL_1 \cup WH_2 \cup WL_2 \cup \cdots \cup WH_d \cup WL_d$,

단, $WH_i = \{P_j \mid w(P_j) = Wh_i,\ P_j \in P,\ 1 \le j \le n\}$,

$WL_i = \{P_j \mid w(P_j) = Wl_i,\ P_j \in P,\ 1 \le j \le n\}$,

$WH_i \neq \varnothing (1 \le i \le d)$이고, $WL_i \neq \varnothing (1 \le i < d)$이며,

$WL_d = \varnothing$이면 $|WH_d| \ge 2$이거나 $WL_d \neq \varnothing$

과 같이 구성된다.

이로부터, 각 가중치 Wh_i $(1 \le i \le d)$에 대해서 Wh_i를 루트(root)로 하고, $Wh_{i+1}, Wh_{i+2}, \ldots, Wh_d, Wl_d, Wl_{d-1},$

... , Wl_i를 자식노드로 하는 트리 T_i를 생성할 수 있다.

4.1.2 원소수가 3 이상인 경우

그러나 최소 가중치 $Wl_i(1 \le i \le d)$들은 다시 보다 작은 하위 가중치들에 의해서 역할이 대행될 수 있다. 즉, 가중치 Wl_i는 $WL_{i-1}(|WL_{i-1}|>1)$ 또는 $WL_{i-1} \cup WL_{i-2}$ $(|WL_{i-1}|=1)$에 의해 대치될 수 있으며 대치되는 참가자 집합을 WL_i'라고 하자.

$$WL_1' = \varnothing,$$
$$WL_2' = \varnothing, \ (|WL_1| = 1)$$
$$= WL_1, \ (|WL_1| > 1)$$

이고, $2<i \le d$에 대해서

$$WL_i' = WL_{i-1}, \ (|WL_{i-1}| > 1)$$
$$= WL_{i-1} \cup WL_{i-2}, \ (|WL_{i-1}| = 1)$$

이다.

WL_i'을 구성하는 참가자들은 Wl_i을 대신하여 모두 필요한 참가자들이므로 $|WL_i'|=NL_i'$이라면 가중치 크기 순에 따라 NL_i'깊이의 사향 트리를 형성한다. 그리고 새롭게 생성된 이 트리들은 4.1.1의 원소가 2인 경우에서 생성된 각 트리에서 다시 Wl_i의 부모노드의 가장 우측 자식노드가 된다. 이 과정은 더 이상 추가되는 노드가 없을 때까지 확장된 트리의 가장 우측 단말 노드인 Wl_j에 대해서 재귀적으로 반복된다. ■

따라서 최소접근트리 T는 $1 \le i \le d$에 대해서 T_i들로 구성되는 포리스트(forest)로 $T = F(T_1, \ldots, T_d)$로 표기한다.

결과적으로, 최소접근집합 Γ_0는 T에서 루트부터 단말 노드까지의 각 경로 상의 모든 노드들을 하나의 부분 집합으로 했을 때, 이 부분 집합들의 계(family)이다.

[예제] 다음의 가중치 집합 $W = \{Wl_1, Wl_2, Wl_3, Wl_4, Wl_5, Wh_5, Wh_4, Wh_3, Wh_2, Wh_1\} = \{1, 2, 6, 24, 48, 49, 73, 91, 95, 96\}$이 주어졌다고 가정한다. 사전 정의된 임계값 $t = 97$이다. 참가자 집합 $P = WH_1 \cup WL_1 \cup WH_2 \cup WL_2 \cup \cdots \cup WH_5 \cup WL_5$과 같고 각 가중치를 갖는 참가자 수는 $NH_1=NH_3=NH_4=NH_5=NL_4=NL_5=1, NH_2=NL_1=2$, $NL_2=3$, $NL_3=4$이다. 즉, 참가자 집합을 가중치로 나열하면 $P=\{1, 1, 2, 2, 2, 6, 6, 6, 6, 24, 48, 49, 73, 91, 95, 95, 96\}$과 같다. 주어진 가중치 집합에 대한 최소접근구조를 표현하는 트리는 다음 그림 1과 같이 구성된다.

따라서 주어진 가중치를 갖는 참가자 집합에 대한 최소접근구조 Γ_0는 다음과 같다.

Γ_0={{96,96},{96,95},{96,91},{96,73},{96,49},{96,48},{96,24},{96,6},{96,2},{96,1},{95,95},{95,91},{95,73},{95,49},{95,48},{95,24},{95,6},{95,2},{91,91},{91,73},{91,49},{91,48},{91,24},{91,6},{73,73},{73,49},{73,48},{73,24},{49,49},{49,48},{95,1,1},{91,2,2,2},{91,2,2,1,1},{73,6,6,6,6},{49,24,6,6,6,6},{73,6,6,6,2,2,2},{73,6,6,6,2,2,1,1},{49,24,6,6,6,2,2,2},{49,24,6,6,6,2,2,1,1}}

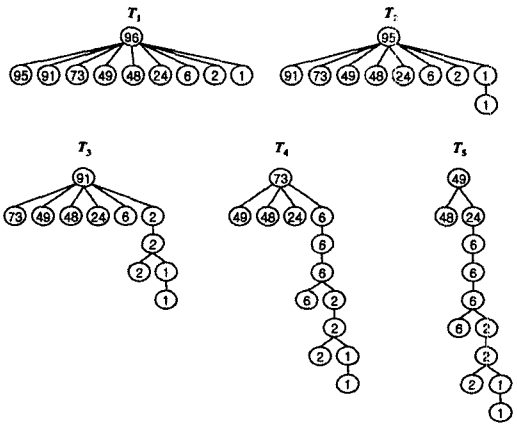

그림 1 최소접근구조를 나타내는 트리

4.2 가중치 함수

각 참가자들에게 비밀정보 복원 권한에 따른 가중치 부여 방법은 다음과 같다. 우선, 최소 가중치는 1이라고 한다. WL_i은 가중치 Wl_i을 갖는 참가자들의 집합이며, $NL_i=|WL_i|$이다.

Wl_i의 초기값은

$$Wl_1 = 1$$
$$Wl_2 = Wl_1 + 1, \ (NL_1=1)$$
$$= Wl_1 \times NL_1, \ (NL_1>1)$$

이고,

i 번째 하위 가중치$(3 \le i \le d-1)$

$$Wl_i = Wl_{i-1} \times NL_{i-1}, \ (NL_{i-1}>1)$$
$$= Wl_{i-1} + (Wl_{i-2} \times NL_{i-2}), \ (NL_{i-1}=1)$$이다.

가중치 Wl_i가 NL_{i-1}에 따라서 다르게 정의되는 이유는 가중치 Wl_{i-1}를 갖는 모든 참가자들에 의해서는 역할이 대행될 수 있지만, $NL_{i-1}=1$인 경우에는 Wl_{i-1} 혼자서 Wl_i의 역할을 대행해서는 안되므로, 더 낮은 가중치 Wl_{i-2}를 갖는 참가자들과 함께 가중치 Wl_i를 대신할 수 있도록 하기 위함이다. 그러나 하위 가중치를 갖는 참가자 조합이 바로 상위 가중치를 갖는 모든 참가자들을 대신할 수 있는 것은 아니며, 상위 가중치를 갖는 단 한 사람의 역할을 대신할 수 있다.

Wl_d의 값은 $WL_d=\varnothing$인 경우와 $WL_d \neq \varnothing$경우로 구분하여 생각할 수 있다.

d번째 가중치는 $WL_d \neq \varnothing$ 경우는

$$Wl_d = Wl_{d-1} \times NL_{d-1},\ (NL_{d-1} > 1)$$
$$= Wl_{d-1} + (Wl_{d-2} \times NL_{d-2}),\ (NL_{d-1} = 1)$$

이고, 임계값 t는

$$t = (2 \times Wl_d) + 1,\ (NL_d = 1)$$
$$= (Wl_d \times NL_d) + 1,\ (NL_d > 1)$$이다.

임계값 t가 위와 같이 정의되는 이유는 가중치 Wl_d는 보다 큰 가중치 Wh_d를 갖는 어떤 참가자와 함께 비밀정보를 복원할 수 있으나, Wl_d이하의 가중치를 갖는 참가자와는 비밀정보를 복원할 수 없어야 하기 때문이다.

$WL_d = \varnothing$인 경우는

$$Wh_d = (Wl_{d-1} \times NL_{d-1}) + 1,\ (NL_{d-1} > 1)$$
$$= Wl_{d-1} + (Wl_{d-2} \times NL_{d-2}) + 1,\ (NL_{d-1} = 1)$$

이고, 임계값 t는

$$t = 2 \times Wh_d$$이다.

가중치 Wh_d는 비밀정보 복원을 위해 필요한 최소 가중치 Wl_d가 존재하지 않으므로, $NH_d = |WH_d| \geq 2$이여야 하고, 적어도 두 명 이상의 가중치 Wh_d를 갖는 참가자가 비밀정보를 복원할 수 있어야 하므로 t는 위와 같이 정의되고. Wh_d는 가상의 Wl_d가 가질 수 있는 값보다 커야 하므로 위와 같이 정의된다.

나머지 Wh_i 값들은 $Wh_i = t - Wl_i$ $(1 \leq i \leq d)$로 정의된다.

4.3 비밀분산법

가중치를 갖는 각 참가자들에게 공유정보를 생성하는 방법에 대해서 설명한다. 각 참가자에게 공유정보를 생성하기 위해서 (2, n)-임계치법과 (t, n)-임계치법을 사용한다. 공유하고자 하는 비밀정보를 k라고 하자. 참가자집합의 최소접근구조는 Wh_i $(1 \leq i \leq d)$를 루트로 하는 d개의 트리로 구성된다. 각 트리 T_i에 대해서 비밀정보 k와 임의로 선택된 난수 $a_1, a_2, \ldots, a_d$를 이용하여 $f_i(x) = kx + a_i$의 일차다항식을 생성하여 각 트리 T_i에게 다항식 $f_i(x)$를 배분한다[10]. 각 트리 T_i들은 주어진 다항식을 이용하여 다음의 알고리즘에 의해 트리 상의 모든 노드들에 대한 공유정보를 생성한다.

[알고리즘 A] 가중치를 갖는 비밀분산법

(1) 트리 T_i의 루트 값은 가중치 Wh_i이다. NH_i는 가중치 Wh_i를 갖는 참가자들의 수이다. $NH_i + 1$개의 난수 $x_1, x_2, \ldots, x_{NH_i}, x_{NH_i+1}$를 선택하여 주어진 다항식으로부터 공유정보 $s_j = f_i(x_j)$를 생성한다. 생성된 공유정보 $s_1, s_2, \ldots, s_{NH_i}$는 가중치 Wh_i를 갖는 각 참가자들에게 분배하고, s_{NH_i+1}은 Wh_i의 자식노드의 가중치를 갖는 모든 참가자들에게 분배한다. 가장 우측 자식노드가 단말노드이면 공유정보 생성 알고리즘은 종료하고 그렇지 않으면 단계 (2)를 수행한다. 단계 (2)를 수행하기 이전에 부 마스터 키(sub master key) sk와 새로운 인덱스 z를 다음과 같이 $sk = s_{NH_i+1}$와 $z = i$로 지정한다.

(2) 우측 자식노드가 단말노드가 아닌 경우는 WL_{z-1}을 우측 자식노드로 가지는 경우와 $WL_{z-1} \cup WL_{z-2}$를 우측 자식노드로 가지는 두 가지 경우로 구분된다.

i) WL_{z-1}을 자식노드로 가지는 경우

임의의 $(NL_{z-1}, NL_{z-1}+1)$-임계치법에 의해서 sk를 비밀정보로 하는 새로운 공유정보 $s_{x_1}, s_{x_2}, \ldots, s_{x_{NL_{z-1}}}, s_{x_{NL_{z-1}+1}}$를 생성한 후 $s_{x_1}, s_{x_2}, \ldots, s_{x_{NL_{z-1}}}$는 WL_{z-1}의 각 참가자들에게 분배하고 $s_{x_{NL_{z-1}+1}}$은 잉여 공유정보로 남겨둔다.

$sk = s_{x_{NL_{z-1}+1}}$이고, $z = z - 1$로 지정한다.

ii) $WL_{z-1} \cup WL_{z-2}$을 자식노드로 가지는 경우

임의의 (2,n)-임계치법에 의해서 sk를 비밀정보로 하는 새로운 공유정보 s_{x_1}, s_{x_2}를 생성한 후, s_{x_1}은 WL_{z-1}에게 분배하고 WL_{z-2}의 참가자들에게는 다시 s_{x_2}를 비밀정보로 하는 $(NL_{z-2}, NL_{z-2}+1)$-임계치법에 따른 새로운 공유정보 $s_{y_1}, s_{y_2}, \ldots, s_{y_{NL_{z-2}}}, s_{y_{NL_{z-2}+1}}$를 생성하여 $s_{y_1}, s_{y_2}, \ldots, s_{y_{NL_{z-2}}}$는 WL_{z-2}의 참가자들에게 분배하고 $s_{y_{NL_{z-2}+1}}$은 잉여 공유정보로 남겨둔다.

$sk = s_{y_{NL_{z-2}+1}}$이고, $z = z-2$로 지정한다.

가장 우측 자식노드들을 구성하는 최소 가중치 Wl_z가 다시 보다 작은 가중치를 갖는 참가자들을 우측 자식노드로 가지는 경우에는 단계 (2)의 과정을 반복하고, 그렇지 않은 경우에는 잉여 공유정보는 버리고 알고리즘을 종료한다. ■

알고리즘 (1)단계에서 루트 값을 갖는 가중치는 동일한 가중치를 갖는 다른 참가자들은 물론 자식 노드에 해당하는 보다 작은 가중치를 갖는 참가자들과 함께 비밀정보를 복원할 수 있다. 따라서 루트 값의 가중치를 갖는 참가자들은 (2, n)-임계치법에 따른 서로 다른 공유정보를 부여받는다. 자식 노드에 해당하는 참가자들은 루트 값에 해당하는 가중치를 갖는 참가자와 함께만 비밀정보를 복원할 수 있고, 자식 노드에 해당하는 참가자들끼리는 비밀정보를 복원할 수 없어야 하므로 동일한 공유정보를 부여받는다.

알고리즘 (2)단계는 비밀정보를 복원하기 위한 최소 참가자 수가 2를 넘어서는 경우이다. 2명의 참가자가 비밀정보를 복원할 수 있는 최소 가중치가 보다 더 작은 가중치의 조합으로 대치될 수 있다. 따라서, 보다 더 작

은 가중치를 갖는 참가자 조합이 모여서 바로 상위 가중치를 갖는 참가자의 역할을 대행할 수 있어야 하기 때문에 바로 위 가중치를 갖는 참가자들이 갖는 공유정보를 다시 비밀정보로 하는 비밀분산법에 의해 새로운 공유정보를 부여받는다.

4.4 안전성 분석

최소접근구조를 구성하는 각 트리는 동일한 비밀정보에 대해서 서로 다른 난수를 상수항으로 하는 다항식으로부터 각 트리를 이루는 노드들인 참가자들에게 공유정보를 생성한다. 따라서 각 참가자가 가지는 여러 개의 공유정보는 모두 서로 다른 다항식에서 생성된 값이므로 각 참가자가 갖는 다수의 공유정보로부터 원 비밀정보에 대한 어떤 정보도 얻을 수 없다.

최소접근구조를 포함하는 참가자 부분집합은 비밀정보를 복원할 수 있다. 최소접근구조가 사전 정의된 임계값과 같아지는 최소 참가자 집합을 정의하고 있으므로, 최소접근구조를 만족하지 않는 참가자 집합은 비밀정보에 대한 어떤 정보도 얻을 수 없다. 비밀정보 복원을 위한 최소 참가자 수가 2명 이상인 경우는 최소 가중치가 보다 작은 하위 가중치를 갖는 참가자 집합에 의해서 대치되는 경우이고, 공유정보 생성 [알고리즘 A]에 따라서 보다 작은 하위 가중치는 바로 위 가중치를 갖는 참가자의 공유정보를 다시 비밀정보로 하여 새로운 공유정보를 부여받기 때문에, 최소접근구조를 정의하는 참가자 집합을 포함하지 않으면 비밀정보 복원이 가능한 공유정보를 알 수 없으므로 비밀정보의 복원이 불가능하다. 따라서 가중치를 갖는 비밀분산법은 완전 비밀분산법(perfect secret sharing scheme)이다.

5. 정보비 분석

정보비는 비밀분산법의 성능측정 기준 중의 하나로서, 비밀정보와 그에 따른 공유정보가 가지는 비트 길이로 정보비를 나타내는 것을 의미한다. 본 논문에서 제시한 가중치를 갖는 비밀분산법에 따르면 각 참가자는 하나의 비밀정보에 대해서 하나 이상의 공유정보를 부여받는다. 따라서, 각 참가자가 갖는 공유정보의 개수 중에서 최대 개수를 m이라고 하면, 가중치를 갖는 비밀분산법의 정보비 ρ는 $\rho = \frac{1}{m}$과 같다[8].

최소접근구조를 구성하는 각 트리에 대해서 공유정보를 생성하는 [알고리즘 A]가 수행되기 때문에, 각 참가자들은 자신이 포함되는 트리의 개수만큼의 서로 다른 공유정보를 부여받는다. 최소접근구조를 구성하는 트리의 최대 개수 d는 서로 다른 가중치의 개수를 l개라고 했을 때, $\frac{l}{2}$개를 넘지 않는다. 이것은 가중치 집합 W가 $W = Wh_1 \cup Wl_1 \cup Wh_2 \cup Wl_2 \cup \cdots \cup Wh_a \cup Wl_d$와 같이 자신과 동일한 가중치 혹은 보다 작은 가중치를 갖는 참가자와 함께 비밀정보를 복원할 수 있는 가중치 집합과 그렇지 못한 가중치 집합으로 구분되고, 각 트리를 구성하는 루트에 해당하는 가중치는 자신과 동일한 가중치 혹은 보다 작은 가중치를 갖는 참가자와 함께 비밀정보를 복원할 수 있는 가중치이기 때문에 $\frac{l}{2}$개를 넘지 않는다. 따라서, 각 참가자가 갖는 최대 공유정보의 개수 또한 $\frac{l}{2}$개를 넘지 않는다.

결과적으로 제시한 가중치를 갖는 비밀분산법에 대한 정보비 $\rho = \frac{1}{m} \geq \frac{1}{d} \geq \frac{l}{2}$이므로, 최소접근구조를 구성하는 트리 개수 d에 대해서 정보비 $\rho \geq \frac{1}{d}$이다.

6. 결론

본 논문에서는 비밀정보를 공유하는 각 참가자가 비밀정보 복원에 대해 서로 다른 권한을 가지는 경우에 대해 보다 일반적인 비밀분산법을 제시하였다. 가중치를 갖는 비밀분산법은 비밀정보 복원에 대한 권한을 임의의 자연수 값에 해당하는 가중치로 표현함으로써 비밀정보를 복원하고자 하는 참가자 집합의 가중치의 합이 사전 정의된 임계값과 같거나 크면 비밀정보를 복원할 수 있고, 그렇지 않은 경우에는 비밀정보에 대한 어떤 정보도 얻을 수 없다.

비밀정보를 복원하기 위한 최소접근구조가 트리 형태로 구성되고, 트리의 각 패스 상의 모든 노드들이 최소접근집합을 구성한다. 따라서, 기존의 가중치를 갖는 임계치법이 가지는 랭크 2라는 제약사항을 제거함으로써 보다 일반적인 접근 구조를 반영하였다.

다음 (표 1)은 계층 구조를 반영하는 비밀분산법인 멀티레벨 비밀분산법과 랭크 2 가중치를 갖는 임계치법과의 간단한 비교 분석을 나타낸 것이다.

표 1 기존 연구와의 비교

방법 / 평가 기준	멀티레벨 비밀분산법	랭크 2 가중치를 갖는 임계치법	가중치를 갖는 비밀분산법
계층구조	레벨 단위	각 참가자 단위	각 참가자 단위
기본연산	(t, n)-임계치법	$(2, n)$-임계치법	$(2, n)$, (t, n)-임계치법 혼용
정보비	1	$1/\log k$ (k-가중치 그래프)	$1/d$ (d는 부트리의 개수)
최소접근집합 제약사항	없음	최대 2 명	없음

제안된 방식의 정보비는 최소접근구조를 구성하는 트리 개수를 d라고 했을 때, $\rho \geq \frac{1}{d}$ 로서 기존의 가중치를 갖는 임계치법이 가지는 정보비 보다는 효율성이 다소 떨어진다. 그러나 이것은 최소접근구조인 포리스트 T를 구성하는 방법을 개선시킴으로써 정보비를 향상시킬 수 있다. 즉, T의 각 부트리에서 경로 길이가 3이상인 각 경로에 대해서, 루트를 제외한 나머지 자식노드들을 하나의 새로운 추상 노드로 묶음으로써, 최소접근구조를 그래프로 표현할 수 있고, 최소접근구조가 그래프로 표현되면, 그래프 분할 방법에 의해 정보비를 향상시킬 수 있다.

참 고 문 헌

[1] G. R. Blakley, "Safeguarding Cryptographic Keys," Proceeding of AFIPS, vol. 48, pp. 313-317, 1979.

[2] A. Shamir, "How to Share a Secret," Communication of the ACM, vol. 22, pp. 612-613, 1979.

[3] J. Benaloh, 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.

[4] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, "On the Information Rate of Secret Sharing Schemes," Theoretical Computer Science, vol. 154(2), pp. 283-306, 1996.

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

[6] P. Morillo, C. Padro, G. Saez, J. L. Villar,"Weighted Threshold Secret Sharing Schemes," Information Processing Letters 70, pp. 211-216, 1999.

[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] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the Size of Shares for Secret Sharing Schemes," Journal of Cryptology, vol. 6, pp. 157-169, 1993.

[9] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, "Graph Decompositions and Secret Sharing Schemes," in Advances in Cryptology-EUROCRYPT '92, Lecture Notes in Computer Science, vol. 658, pp. 1-24, 1994.

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

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 ~ 현재이화여자대학교 컴퓨터학과 교수. 2000년 ~ 현재 한국정보과학회 총무이사, 정보보호연구회 부위원장. 관심분야는 정보보호, 암호프로토콜, 알고리즘 설계, 계산기하, 그래프 드로잉, 데이터 마이닝, Bioinformatics

권 대 성

1992년 2월 서울대학교 수학과 학사. 1994년 2월 서울대학교 수학과 석사. 1999년 2월 서울대학교 수학과 박사. 1999년 4월 ~ 2001년 2월 고등과학원 박사 후 연구원. 2001년 3월 ~ 현재 국가보안기술연구소 선임연구원. 관심분야는 정보보호, 암포프로토콜, 암호 알고리즘