일방향 해쉬 함수에 기반한 효율적인 온라인 비밀분산 방식

오 수 현† · 김 승 주†† · 원 동 호†††

요 약

비밀분산이란 비밀정보에 대한 부분 정보를 여러 참가자들에게 분배하였다가 필요한 경우에 허가된 참가들의 협조에 의해서만 복원이 가능하도록 하는 암호학적 기술을 말한다. 이러한 비밀분산은 비밀정보의 관리뿐만 아니라 다자간 프로토콜, 그룹 암호 방식 등의 분야에서 매우 중요한 부분이다. 본 논문에서는 일방향 해쉬함수에 기반한 효율적인 온라인 비밀분산 방식을 제안하고자 한다. 제안하는 방식은 하나의 부분 정보만으로 여러 개의 비밀을 분산할 수 있고, 엑세스 구조가 변하는 경우에 게시판에 공개된 값들만 변경하면 각 참가자들은 기존의 부분 정보를 그대로 사용할 수 있다. 또한 참가자들의 부정이 있는 경우 그 수에 관계없이 항상 부정한 참가자의 신분을 밝혀낼 수 있으며, 기존에 제안된 방식들보다 계산상 효율적이라는 장점이 있다.

Efficient On-line Secret Sharing scheme based on One-way Hash Function

Soo-Hyun Oh† · Seung-Joo Kim†† · Dong-Ho Won†††

ABSTRACT

Secret sharing scheme is a cryptographic protocol in which a dealer distributes shares of a secret among a set of participants such that only authorized set of participants can recover the secret at a later. Secret sharing is an important cryptographic primitive in management of secret information, secure multiparty protocol and group-oriented cryptography, etc. In this paper, we propose an efficient on-line secret sharing scheme based on one-way hash function. This scheme provides the property to share multiple secrets and allows participants to be added/deleted dynamically, without having to redistribute new shares. Proposed scheme has advantage to detect cheating and identify of all cheater, regardless of their number. Futhermore, it is more efficient than previous schemes.

1. 서 론

최근 컴퓨터와 네트워크의 급속한 발전으로 인해 모든 정보는 디지털 문서화되어 처리·전송·저장되고 있다. 따라서 암호학적으로 중요한 비밀 정보뿐만 아니라 그룹이나 회사의 업무에 관련된 여러 중요한 정보들도 개인이나 회사의 컴퓨터에 저장되어 관리하고 있다. 그러나 중요한 비밀 정보를 제 3자로부터 안전한 곳에 저장하여 관리하더라도 관리하는 사람이 해당 비밀 정보에 대한 권리를 남용할 수 있을 뿐만 아니라 천재지변이나 조작 실수로 인한 손상 시 복구하는 것이 불가능하다는 문제점이 있다. 따라서 이러한 문제점을 해결하기 위해, 하나의 비밀 정보를 여러 개의 조각으로 나누어 여러 사람이 관리함으로써 한 사람에

※ 본 논문은 한국 과학 재단의 특정기초연구(97-01-00-13-01-5) 지원 사업에 의해 수행하였습니다.
† 준 회 원 : 성균관대학교 대학원 전기전자및컴퓨터공학과
†† 정 회 원 : 한국정보보호센터 기술부/암호기술팀 과제책임자
††† 종신회원 : 성균관대학교 전기전자및컴퓨터공학부 교수
논문접수 : 1999년 5월 25일, 심사완료 : 2000년 10월 6일

의해 남용될 수 없도록 하거나, 유사시에 손상될 경우를 대비하여 여러 개의 복사본을 다른 컴퓨터에 보관하는 등의 방법을 사용하고 있다. 그러나 전자의 경우에는 조각중 하나라도 손상되는 경우에 본래의 비밀을 복구할 수 없다는 문제점이 있고 후자의 경우에는 제3자의 관점에서 공격할 대상의 수가 증가하므로 관리해야 할 비밀의 수가 증가한다는 단점이 있다. 이러한 문제를 해결할 수 있는 것이 바로 비밀 분산(secret sharing) 방식이다.

비밀분산 방식이란 비밀정보 s에 대한 부분 정보를 n명의 참가자들에게 분배하고 필요한 경우에 허가된 참가자들의 부분 집합에 의해 본래의 비밀을 복원할 수 있도록 하는 암호학적 기술을 말한다. 이는 비밀정보의 관리뿐만 아니라 다자간 프로토콜이나 그룹 암호방식, 키복구 시스템 등에 적용될 수 있다. 이러한 비밀분산 방식은 Blakely[1]와 Shmir[13]에 의해 각각 1979년에 처음으로 제안되었으며 그 중 다항식 보간법을 이용하는 Shamir의 비밀분산 방식은 다음과 같은 특징을 갖는다.

분산하고자 하는 비밀을 s, 비밀분산에 참여하는 전체 참가자의 수가 n명 일 때,

1) t($t \le n$)명 이상의 참가자들은 본래의 비밀 s를 복원할 수 있고,
2) t-1명 이하의 참가자들은 비밀 s에 대해 아무런 정보도 얻을 수 없다.

이와 같은 비밀분산 방식을 (t, n)-역치(threshold) 방식이라 하며, Shamir의 비밀 분산 방식은 각 참가자들이 보관해야 하는 부분 정보의 크기가 본래의 비밀 K의 크기과 거의 같고 허가되지 않은 참가자들이 비밀 K에 대해 아무런 정보도 얻을 수 없는 무조건적으로 안전한 비밀 분산 방식이라는 장점이 있지만, 비밀이 한번 복원된 이후에는 참가자들의 부분 정보를 재사용 할 수 없다는 단점이 있다. 또한, 비밀을 복원할 수 있는 참가자의 집합의 집합인 엑세스 구조가 변하는 경우에 달리는 새로운 다항식을 생성하고 기존의 참가자들에게도 새로운 부분 정보를 분배해야 한다는 문제점이 있다.

이러한 문제를 해결하기 위해 C. Cachin은 1995년 *Cryptography and Coding*이라는 국제학술회의에서 온라인 비밀 분산 방식이라는 새로운 개념을 제안하였다[2]. 그 이후로 여러 온라인 비밀 분산 방식이 제안되었으나 다수의 비밀 분산에 적용할 수 없거나 참가자의 부정을 검출할 수 없고 또는 많은 계산량을 요구한다는 등의 단점이 있다. 따라서 본 논문에서는 각 참가자는 하나의 부분 정보만을 보관하고 이를 이용하여 여러개의 비밀을 복원할 수 있고 부정한 참가자의 확인이 가능하며 기존에 제안된 방식들에 비해 계산상 효율적인 새로운 온라인 비밀분산 방식을 제안하고자 한다.

2. 온라인 비밀분산 방식

비밀분산 방식에서 본래의 비밀 s를 복원할 수 있는 허가된 참가자들의 집합의 집합을 액세스 구조(access structure) Γ라 한다. 이러한 엑세스 구조가 동적으로 변하는 경우 즉, 새로운 참가자들이 비밀분산 방식에 참여하거나 기존의 참가자들이 제거되는 경우에 또 다른 부분정보를 재분배하지 않고 이전의 부분정보를 그대로 사용할 수 있는 비밀분산 방식을 온라인 비밀 분산 방식이라 한다.

이러한 온라인 비밀분산 방식은 C. Cachin이 [2]에서 처음으로 제안하였으며 Cachin의 방식은 각 참가자가 본래의 비밀 s와 같은 크기를 갖는 하나의 부분정보만을 이용하여 다수의 비밀을 복원할 수 있는 방식이다. 또한 Cachin이 제안한 방식은 모든 참가자들이 접근할 수 있는 게시판에 인증된 정보를 공개하고 엑세스 구조가 변하는 경우에 그 공개정보들의 값만을 변경하여 기존의 참가자들의 부분정보는 그대로 유지할 수 있게 하였다. 그러나 이 방식을 다수의 비밀 분산에 적용할 경우, 하나의 비밀이 복원된 후에도 다른 비밀들이 안전하기 위해서는 각 참가자들의 부분정보가 다른 참가자들에게 드러나지 않도록 하기 위해 추가적인 계산 과정(distributed computation)[6]이 필요하다는 단점이 있다

이러한 문제점을 해결하기 위해, Pinch는 [11]에서 Diffe-Hellman 문제를 이용한 온라인 비밀분산 방식을 제안하였다. 이 방식은 비밀을 복원하는 과정에서 참가자들의 부분정보가 공개되지 않으므로 추가적인 계산 없이 다수의 비밀분산으로 확장할 수 있다. 그러나 이 방식 또한 비밀복원 과정에서 참가자가 고의로 자신의 부분정보를 바르게 제공하지 않는 경우, 부정한 참가자의 신분을 밝혀낼 수 없다는 문제점이 있다.

따라서 Godoshi 등은 [7]에서 Pinch의 방식이 이러한 문제점이 있음을 지적하고 이를 해결할 수 있는 방식을 제안하였다. Godoshi 등의 방식은 비밀복원 과정 이전에 각 참가자들이 게시판에 공개된 정보들을 이용하여 다른 참가자들이 부분정보를 바르게 제공하는지를 확인할 수 있는 과정을 추가하였다. 그러나 이 방식 또한 과반수 이상의 참가자들이 공모하여 부정하는 경우에는 안전하지 않다는 문제점이 있다.

그 이후에, Yeun 등은 [15,16]에서 Pinch의 방식을 개선하여 비밀복원 과정에 각 참가자들이 제공하는 정보에 디지털 서명을 적용하여 참가자의 부정이 있는 경우, 그 수에 관계없이 항상 부정한 참가자의 신분을 확인할 수 있는 온라인 비밀분산 방식을 제안하였다. 이 방식은 이산대수 문제[15]나 RSA 암호 방식[16]을 이용하여 비밀을 복원하는 과정에서 참가자들의 비밀이 드러나지 않게 하였고 전송 정보에 디지털 서명을 하여 비밀이 제대로 복원되지 않은 경우에 딜러에 의해 부정한 참가자의 신분을 확인할 수 있도록 하였다. 그러나 Yeun 등의 방식은 비밀 분산 및 복원 과정에 이산대수 문제나 RSA 암호 방식을 이용하여 많은 계산량을 요구한다는 단점이 있다. Yeun 등의 방식 중 이산대수 문제를 이용한 Yeun 등의 비밀분산 및 복원 프로토콜은 다음과 같다.

● 시스템 설정

- P : 비밀분산에 참여하는 참가자 $P_i (1 \le i \le n)$의 집합
- D : 각 참가자에게 부분정보를 분배하는 딜러 단, $D \notin P$
- Γ : 엑세스 구조(access structure) ($\Gamma \in 2^{2^P}$)
- Γ^+ : 허가된 참가자의 최소 집합(minimal authorized set)
- K : 분산할 비밀
- f : 충돌 회피성 일방향 해쉬함수
- S_{P_i} : 참가자 P_i의 디지털 서명

● Yeun의 비밀분산 프로토콜

단계 1) 딜러는 큰 소수 p와 위수가 q(단, q|p-1)인 Z_p상의 원소 g를 선택하고 각 참가자의 비밀값 $S_i < q (1 \le i \le n)$를 랜덤하게 선택한다

단계 2) 딜러는 $S_i (1 \le i \le n)$값을 비밀리에 각 참가자에게 전송한 후, 참가자의 ID와 함께 안전하게 저장한다.

단계 3) 딜러는 $X \in \Gamma^+$인 X에 대해 다음과 같이 T_X 값을 계산한다

$$T_X = K - f\left(g_X^{\prod_{P_i \in X} S_i}\right) \pmod p$$

단계 4) 딜러는 각 Γ^+에 속하는 각 원소 X에 대해 (X, g_X, T_X)와 f(K) 값을 게시판에 공개한다.

● Yeun의 비밀복원 프로토콜

비밀을 복원하기 위해 필요한 참가자의 집합을 $X = \{P_1, P_2, \ldots, P_t\}$라 하자

단계 1) 참가자 P_1은 X에 해당하는 g_X, T_X, f(K)를 게시판으로부터 읽어온다

단계 2) P_1은 $g_X^{S_1} \bmod p$를 계산하고 다음과 같이 디지털 서명을 생성한다.

$$S_{P_1} = SIGN_{P_1}(g_X^{S_1} \bmod p \,\|\, X \,\|\, g_X)$$

단계 3) P_1은 S_{P_1}과 $g_X^{S_1} \bmod p$를 P_2에게 전송한다.

단계 4) 각 $P_i (2 < i < t)$는 P_{i-1}로부터 받은 서명을 검증한 후 $(g_X^{S_1 S_2 \cdots S_{i-1}})^{S_i} \bmod p$를 계산하고 다음과 같이 디지털 서명을 생성하여 P_{i+1}에게 Sp_i와 $(g_X^{S_1 S_2 \cdots S_{i-1}})^{S_i} \bmod p$를 전송한다.

$$Sp_i = SIGN_{P_i}((g_X^{S_1 S_2 \cdots S_{i-1}})^{S_i} \bmod p \,\|\, X \,\|\, g_X)$$

단계 5) 참가자 P_t는 P_{t-1}로 부터 받은 서명을 검증하고 다음과 같이 V_X를 계산한다.

$$V_X = g_X^{S_1 S_2 \cdots S_t} \bmod p$$

단계 6) 참가자 P_t는 K'를 복원한다.

$$K' = T_X + f(V_X) \bmod p$$

단계 7) 복원한 비밀이 정확한지 알아보기 위해 f(K')를 계산하여 게시판에 공개된 f(K)값과 비교한다.

이 방식은 엑세스 구조의 동적인 변화나 다수의 비밀분산에 적용할 수 있지만 비밀분산 및 복원 과정에 공개키 암호 방식을 이용하므로 참가자에게 요구되는 계산량이 많다는 단점이 있다. 따라서 다음 장에서는 일방향 해쉬함수를 이용하여 Yeun 등이 제안한 방식

보다 비밀을 분산하거나 복원하는 과정에서 훨씬 적은 양의 계산을 요구하는 효율적인 온라인 비밀분산 방식을 제안하고자 한다.

3. 제안하는 온라인 비밀분산 방식

본 장에서는 일방향 해쉬 함수를 이용하여 기존의 온라인 비밀분산 방식들을 좀더 효율적으로 개선한 방식을 제안하고자 한다. 앞에서 설명한 Yeun 등의 방식에서는 각 참가자들이 이산대수 문제를 이용하여 자신의 비밀정보를 드러내지 않고 다른 참가자들에게 전송하여 비밀을 복원하도록 하였다. 제안하는 방식에서는 이 과정에서 이산대수 문제 대신 일방향 해쉬함수를 사용함으로써 모듈라 멱승을 하는 기존의 방식에 비해 계산량 측면에서 좀더 효율적으로 개선하였다. 제안하는 비밀 분산 및 복원 프로토콜은 다음과 같다

● **시스템 설정**

- P : 비밀분산에 참여하는 참가자 $P_i (1 \le i \le n)$의 집합
- D : 각 참가자에게 부분정보를 분배하는 딜러 단, $D \notin P$
- Γ : 액세스 구조 ($\Gamma \in 2^{|P|}$). X가 Γ의 원소일 경우, X에 속하는 참가자들의 비밀로부터 본래의 비밀 K를 복원할 수 있고, X가 Γ의 원소가 아닐 경우에는 비밀을 복원하는 것이 불가능 함
- Γ^* : Γ의 원소 중 비밀을 복원하는데 필요한 참가자의 수가 가장 적은 것들의 집합
- K : 분산하고자 하는 비밀
- f, h : 충돌 회피성 일방향 해쉬함수
- S_{P_i} : 참가자 P_i의 디지털 서명

● **비밀분산 프로토콜** (그림 1 참조)

단계 1) 딜러는 난수 r과 각 참가자의 비밀값 $S_i \in_R Z$ $(1 \le i \le n)$를 랜덤하게 선택한다.

단계 2) 딜러는 선택한 $S_i (1 \le i \le n)$값을 비밀리에 각 참가자에게 전송한 후, 참가자의 ID와 함께 그 값들을 안전하게 저장한다

단계 3) 딜러는 $X \in \Gamma^*$인 $X = \{P_1, P_2, \cdots, P_t\}$에 대해 난수 r과 참가자의 부분정보를 이용하여 다음과 같이 T_X값을 계산한다.

$$T_X = K \oplus f(h(S_1||r) \oplus h(S_2||r) \oplus \cdots \oplus h(S_t||r))$$

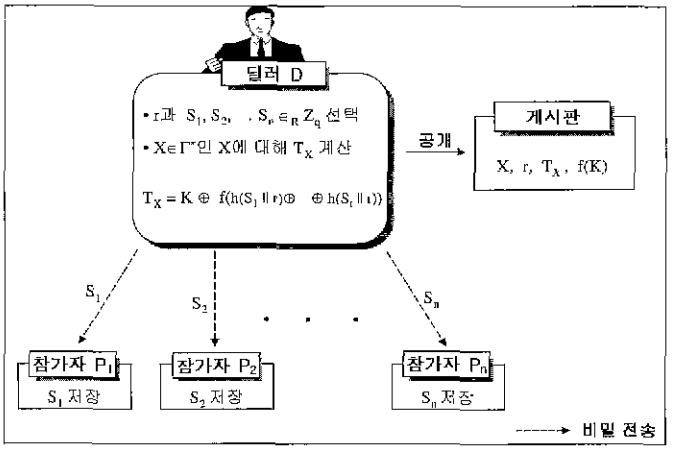
단계 4) 딜러는 각 Γ^*에 속하는 각 원소 X에 대해 (X, r, T_X)와 f(K) 값을 게시판에 공개한다.

● **비밀복원 프로토콜 I** (그림 2 참조)

단계 1) 참가자 P_I은 X에 해당하는 난수 r과 T_X, f(K)를 게시판으로부터 읽어온다.

단계 2) 참가자 P_I은 자신의 부분 정보와 난수 r을 이용하여 $h(S_I||r)$을 계산하고 다음과 같이 디지털 서명을 생성한다.

$$S_{P_I} = Sign_{P_I}(h(S_I||r)||X||r)$$



(그림 1) 제안하는 비밀분산 프로토콜

단계 3) 참가자 P_1은 S_{P_1}과 $g_X^{S_1} \bmod p$를 참가자 P_2에게 전송한다.

단계 4) 각 참가자 $P_i(1 < i < t)$는 참가자 P_{i-1}로부터 받은 서명을 검증한 후 $V_i = h(S_1||r) \oplus h(S_2||r) \oplus \cdots \oplus h(S_i||r)$를 계산하고 다음과 같이 디지털 서명을 생성하여 참가자 P_{i+1}에게 S_{P_i}와 V_i를 전송한다

$$S_{P_i} = Sign_{P_i}(h(S_1||r) \oplus h(S_2||r) \oplus \cdots \oplus h(S_i||r)||X||r)$$

단계 5) 참가자 P_t는 참가자 P_{t-1}로 부터 받은 서명을 검증하고 다음과 같이 V_X를 계산한다.

$$V_X = h(S_1||r) \oplus h(S_2||r) \oplus \cdots \oplus h(S_{t-1}||r) \oplus h(S_t||r)$$

단계 6) 참가자 P_t는 다음과 같이 K'를 복원한다

$$K' = T_X + f(V_X) \bmod p$$

단계 7) 복원한 비밀이 정확한지 알아보기 위해 f(K')를 계산하여 게시판에 공개된 f(K)값과 비교한다

앞에서 설명한 비밀 복원 과정에서는 참가자 P_t가 다른 참가자들보다 먼저 복원하고자 하는 비밀 K를 알게 된다. 이러한 문제를 해결하기 위해 다음에서 설명하는 프로토콜 II를 이용하면 모든 참가자가 동시에 비밀 K 값을 스스로 계산할 수 있게 된다.

● 비밀 복원 프로토콜 II

단계 1) 각 참가자 P_i(단, $P_i \in X$)는 X에 해당하는 난수 r과 T_X, f(K)를 게시판으로부터 읽어온다

단계 2) 각 참가자 P_i는 자신의 비밀정보 S_i와 난수 r을 이용하여 $h(S_i||r)$을 계산하고 다음과 같이 디지털 서명을 생성한다.

$$S_{P_i} = SIGN_{P_i}(h(S_i||r)||X||r)$$

단계 3) 각 참가자 P_i는 X에 속하는 모든 참가자 $P_j(P_j \in X$이고 $P_j \neq P_i)$에게 S_{P_i}와 $h(S_i||r)$를 전송한다.

단계 4) 각 참가자 P_i는 X에 속하는 모든 P_j로부터 받은 서명을 검증하고 다음과 같이 V_X를 계산한다.

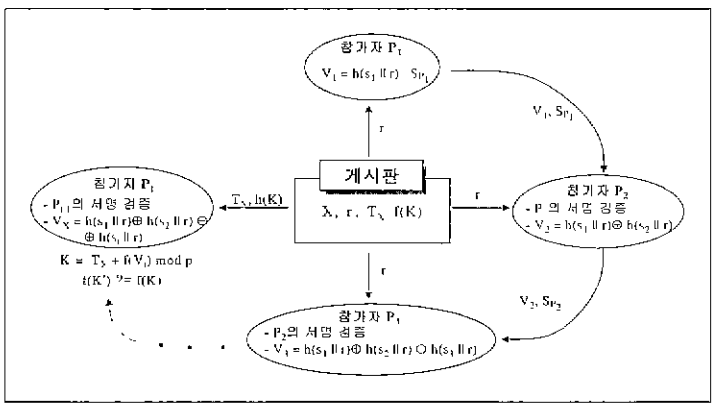
$$V_X = h(S_1||r) \oplus h(S_2||r) \oplus \cdots \oplus h(S_t||r)$$

단계 5) 각 참가자 P_i는 K'를 복원한다.

$$K' = T_X \oplus f(V_X)$$

단계 6) 복원한 비밀이 정확한지 알아보기 위해 f(K')를 계산하여 게시판에 공개된 f(K)값과 비교한다

제안하는 방식의 안전성은 일방향 해쉬 함수에 기반하므로 계산상 안전한 비밀분산 방식이며 각 참가자가 비밀로 간직하는 부분정보의 크기는 비밀 s의 크기와 비슷하므로 이상적인 비밀분산 방식이라 할 수 있다. 그리고 액세스 구조가 변하는 경우에 게시판에 공개된 값들만 변경하면 각 참가자들은 기존의 부분정보를 그대로 사용할 수 있고, 하나의 부분정보를 계 사용하여 여러 개의 비밀을 분산 및 복원할 수 있다. 또한 참가



(그림 2) 제안하는 비밀복원 프로토콜 I

자들이 비밀 복원과정에서 정당하지 않은 부분정보를 제공하는 경우, 그 수에 관계없이 항상 부정한 참가자의 신분을 밝혀낼 수 있으며, 공개키 방식을 이용하는 기존의 방식보다 계산상 효율적이라는 장점이 있다. 제안하는 방식의 이러한 특징에 대해서는 다음 장에서 자세히 살펴보기로 한다.

4. 제안하는 온라인 비밀분산 방식의 특징

4.1 액세스 구조가 동적으로 변하는 경우

제안하는 비밀분산 방식은 새로운 참가자가 들어오거나 기존의 참가자를 제거하는 등의 동적인 액세스 구조의 변화가 있을 경우에, 나머지 참가자들의 부분정보를 그대로 사용할 수 있는 온라인 비밀분산 방식이다. 따라서 액세스 구조가 변하는 경우, 다음과 같은 과정을 통해 게시판에 공개된 값들만 변경하면 새로운 부분 정보의 비밀 전송없이 기존의 비밀 분산 방식을 그대로 사용할 수 있게 된다. 또한, 제안하는 방식은 참가자의 새로운 참여나 제거뿐만 아니라 비밀 분산에 필요한 참가자의 수 n이나 t 값도 필요에 따라 변경될 수 있다.

단계 1) 딜러 D는 비밀 K에 대한 새로운 액세스 구조 Γ'를 구성한다.

단계 2) 딜러 D는 $X \in \Gamma'$인 X에 대해 새로운 난수 r'를 선택하고 다음과 같이 $T_{X'}$ 값을 새로 계산한다.

$$T_{X'} = K \oplus f(h(S_1||r') \oplus h(S_2||r') \oplus \cdots \oplus h(S_t||r'))$$

단계 3) 딜러 D는 게시판에 새로운 $(X, T_{X'}, r')$를 공개한다.

4.2 부정한 참가자의 신분확인

제안하는 방식은 부정한 참가자의 수에 상관없이 항상 비밀복원 과정에서 올바른 부분정보를 제공하지 않은 참가자들의 신분을 밝혀낼 수 있다. 먼저, 비밀복원 과정에서 임의의 참가자가 정당하지 않은 부분정보를 제공한 경우, 복원된 K'의 해쉬값 f(K')가 게시판에 공개된 해쉬값 f(K)와 다르게 되므로 참가자의 부정을 검출할 수 있다. 이러한 경우에 부정한 참가자의 신분을 확인하기 위한 과정은 다음과 같다.

단계 1) 각 참가자들은 비밀 복원 프로토콜 수행 중에 받은 다른 참가자들의 디지털 서명 S_{P_i} $(1 \le i \le t)$를 딜러에게 제출한다.

단계 2) 딜러는 각 참가자의 공개키를 이용하여 서명을 검증하고 $h(S_i||r)$ $(1 \le i \le t)$을 구한다.

단계 3) 딜러는 저장해둔 각 참가자의 부분정보인 S_i $(1 \le i \le t)$와 공개된 난수 r을 사용하여 $h(S_i||r)$ $(1 \le i \le t)$을 계산한다.

단계 4) 딜러는 자신이 계산한 $h(S_i||r)$ $(1 \le i \le t)$과 각 참가자들이 제출한 $h(S_i||r)$ $(1 \le i \le t)$ 값을 비교한다.

단계 5) 두 값이 같지 않을 경우, 해당하는 참가자 P_i가 정당하지 않은 부분정보를 제공한 부정한 참가자라는 것을 확인할 수 있다.

4.3 다수의 비밀 분산으로의 확장

제안하는 비밀분산 방식은 다음과 같은 방법으로 각 참가자들이 갖고 있는 하나의 부분정보 S_i $(1 \le i \le n)$를 이용하여 여러 개의 비밀을 분산 및 복원하는데 적용할 수 있다

분산하고자 하는 m개의 비밀을 K_l이라 하자.(단, $l = 1, 2, \cdots, m$)

단계 1) 딜러는 새로운 비밀 K_l를 분산할 때마다 이전과 다른 액세스 구조 Γ_l을 구성한다.

단계 2) 딜러는 비밀 K_l을 분산하기 위해, $X \in \Gamma_l$인 X에 대해 난수 r_l를 선택하여 다음을 계산한다. 단, 이때, $X = \{P_1, P_2, \cdots, P_t\}$이라 하자.

$$T_{X,l} = K_l \oplus f(h(S_1||r_l) \oplus h(S_2||r_l) \oplus \cdots \oplus h(S_t||r_l))$$

단계 3) 딜러는 각 비밀 K_l에 대해 $(X, r_l, T_{X,l})$와 $f(K_l)$ $(l = 1, 2, \cdots, r)$을 게시판에 공개한다.

이때, 각각의 비밀 K_l에 대해 서로 다른 난수 r_l을 사용하므로 하나의 비밀이 복원되더라도 다른 비밀들의 안전성에는 아무런 영향을 미치지 않는다.

4.4 기존의 방식들과의 비교

<표 1>은 지금까지 제안된 온라인 비밀분산 방식과 본 논문에서 제안한 방식을 비교한 것이다

먼저, Cachin의 방식은 비밀 분산 및 복원 과정에 덧셈과 같은 적은 계산량만을 요구하지만 부정한 참가자의 신분 확인이나 다수의 비밀 분산에는 적용할 수 없다는 문제점이 있고 Pinch의 방식은 이산대수 문제

〈표 1〉 제안하는 방식과 기존의 방식의 비교

	notice board에 공개하는 정보	부정한 참가자의 검출 및 신분확인	다수의 비밀분산에 적용	복원과정에 요구되는 계산량
Cachin 방식	X∈Γ인 X에 대해, (X, T_X)	불가능	추가적인 계산량 요구	덧셈 : |X|+1 번 해쉬함수 1번
Pinch 방식	(X, T_X, g_X)	불가능	가 능	모듈라 멱승 |X| 번 해쉬함수 : 1 번 덧셈 1 번
Ghodosi 방식	$(X, T_X, g_X, g_X^V, C_X)$	과반수이상이 정직할 경우에만 가능	가 능	모듈라 멱승 : $2\|X\|^2 + \|X\|$ 번 해쉬함수 : |X| 번 덧셈 |X| 번
Yeun 방식	(X, T_X, g_X), f(K), f(K)	가 능	가 능	모듈라 멱승 |X| 번 해쉬함수 1 번 덧셈 1 번 각 참가자당 1번의 서명 생성/검증 필요
제안하는 방식	(X, T_X, r), f(K)	가 능	가 능	해쉬함수 : |X|+1번 Exclusive-or : |X| 번 각 참가자당 1번의 서명 생성/검증 필요

단, 여기서 |X|는 비밀복원에 필요한 참가자의 수를 말한다.

를 이용하여 다수의 비밀 분산에는 적용할 수 있으나 Cachin의 방식과 같이 부정한 참가자를 확인할 수 없다는 문제점이 있다. 또한, Ghodosi의 방식은 참가자의 과반수 이상이 정직할 경우에만 부정한 참가자의 신분을 확인할 수 있을 뿐 아니라 비밀을 복원하기 위해 많은 양의 모듈라 멱승이 필요하다는 단점이 있다. 다음으로 Yeun 등이 제안한 방식은 부정한 참가자의 확인이나 다수의 비밀 분산에 적용은 가능하니 이산대수 문제나 소인수 분해 문제 등을 이용하므로 비밀을 복원하기 위해 각 참가자에게 모듈라 멱승의 계산을 요구한다는 단점이 있다.

반면에, 제안하는 방식은 앞에서 설명한 바와 같이, 비밀복원 과정에 전송되는 값에 각 참가자의 디지털 서명을 적용하여 부정한 참가자의 검출 및 신분 확인이 가능하고, 각 비밀마다 서로 다른 난수 r을 사용하면 하나의 부분정보만으로 다수의 비밀을 분산하는 것이 가능하다. 또한 비밀복원 과정에서 참가자들에게 해쉬 함수와 exclusive-or와 같은 적은 계산량만을 요구하므로 모듈라 멱승을 필요로하는 기존의 방법들에 비해 계산상 효율적이라는 장점이 있다

5. 응용 분야

비밀 분산 방식은 비밀 정보의 관리 뿐만 아니라 안전한 백업 시스템, 그룹 암호 방식, 키 복구 시스템 등에 응용될 수 있다. 따라서, 본 절에서는 제안하는 온라인 비밀 분산 방식을 키 복구 시스템과 인터넷 백업 시스템 등에 적용시키고 이로 인해 얻을 수 있는 장점들을 분석한다

5.1 키복구 시스템

최근 개방된 네트워크 상에서 전송되는 정보의 기밀성을 유지하기 위해 전자 상거래와 같은 실생활에서의 암호 방식의 사용이 증대되고 있다. 그러나 실생활에서의 암호의 사용은 개인의 프라이버시의 보호나 네트워크 상에서의 인증 등과 같은 많은 긍정적인 면을 갖고 있지만 최근에는 이와 더불어 개인이 자신의 정보를 보호하기 위해 암호를 사용한 후에 사용한 키를 분실하거나 키가 손상된 경우 암호문의 복호가 불가능하다는 것과 범죄자들이 암호를 이용하는 경우 이에 대한 추적이 불가능하다는 등의 암호의 역기능이 대두되고 있다 이러한 문제점을 해결하기 위해 제안된 방식이 법 집행 기관이 합법적 상황하에서 암호문을 복호하거나 사용자가 자신의 비밀키를 분실했을 때와 같은 유사시에 허가된 사람에게 복호할 수 있는 능력을 제공하는 키 복구 시스템(Key Recovery System)이다.

이러한 키 복구 시스템은 구성 요소의 특징에 따라 크게 위탁 방식과 캡슐화 방식, 그리고 TTP 기반의

방식으로 나눌 수 있는데 그 중 키 위탁 방식은 사용자의 비밀키나 비밀키의 부분 또는 키 관련 정보를 하나 이상의 신뢰 기관에 위탁하는 방식으로 위탁되는 키는 사용자가 오랫동안 사용하게 되는 키(long term key)이다. 이 방식에서는 사용자의 비밀키가 위탁 기관에 직접 맡겨져야 하므로 유사시에 키복구를 확실하게 수행할 수 있다는 장점이 있지만 개인의 프라이버시가 전적으로 위탁 기관에 의존한다는 문제점을 안고 있다. 따라서, 비밀 분산 방식을 이용하여 각 사용자의 비밀키를 몇 개의 위탁 기관에 나누어 보관하고 필요한 경우에 정해진 수 이상의 위탁 기관의 동의에 의해서만 사용자의 비밀키를 복원할 수 있도록 하여 위탁 기관의 권리 남용을 방지할 수 있도록 하고 있다.

이러한 키 위탁 시스템에 기존의 비밀 분산 방식 대신 제안하는 온라인 비밀 분산 방식을 적용하는 경우에는 다음과 같은 장점을 얻을 수 있다.

① 위탁 기관이 추가되거나 제거되는 경우 기존의 위탁 기관의 비밀 정보는 그대로 이용할 수 있다

제안하는 방식은 액세스 구조가 동적으로 변하는 경우에도 기존 참가자들의 부분 정보는 그대로 사용할 수 있는 온라인 비밀 분산 방식이므로 키 위탁 시스템의 위탁 기관이 새로 추가되거나 기존의 위탁 기관이 제거되는 경우 새로운 부분 정보를 재분배 할 필요가 없다.

② 각 위탁 기관은 하나의 부분 정보를 이용하여 여러 사용자의 비밀키 복원 가능하다

제안하는 비밀 분산 방식은 각 참가자들이 하나의 부분 정보를 이용하여 여러 개의 비밀을 복원하는 것이 가능하므로 각 위탁 기관은 하나의 부분 정보만을 보관하고 이를 이용하여 다수의 사용자의 비밀키를 복원할 수 있다.

③ 무정한 위탁 기관의 검출 및 확인이 가능하다.

제안하는 비밀 분산 방식은 비밀 복원 과정에 각 참가자가 제공하는 정보에 디지털 서명을 생성하여 함께 제공하므로 부정한 위탁 기관이 고의적으로 정당하지 않은 값을 제공하여 비밀키의 복구를 방해하려는 경우 이를 검출하고 해당하는 위탁 기관을 확인할 수 있다.

④ 계산상 효율적이다.

제안하는 비밀 분산 방식은 비밀 복원 과정에서 각 참가자에게 해쉬 함수나 exclusive-or와 같은 적은 계산량만을 요구하므로 각 사용자의 비밀키를 복원하는데 기존의 방식에 비해 계산상 효율적이다.

5.2 인터넷 백업 시스템

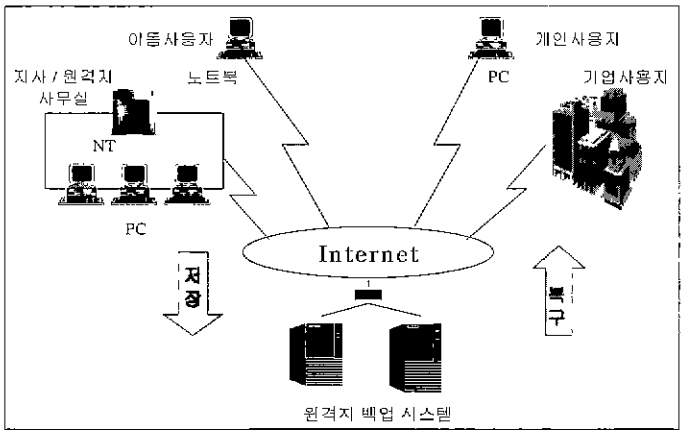
최근 컴퓨터 사용의 급격한 증가와 인터넷의 활성화로 인해 개인 컴퓨터의 데이터는 단순한 흥미와 자료의 수준에서 벗어나 그 자체만으로도 중요한 가치를 지니게 되었다. 그러나 개인의 컴퓨터나 소규모 기업의 컴퓨터는 지금까지 확실한 백업 방안 없이 바이러스나 인위적인 조작 실수와 도난 및 천재지변에 노출된 채로 방치되어 왔다. 그러므로 개인 컴퓨터의 중요한 데이터들도 어딘가에 안전하게 보관해야 할 필요성이 대두되었고 이러한 문제를 해결하기 위해 최근에 인터넷 백업 시스템(Internet Backup Service)이라는 새로운 인터넷 서비스가 시행되고 있다.

인터넷 백업 시스템이란 개인이나 기업의 컴퓨터에 저장된 중요한 데이터를 각종 재해에 대비하여 인터넷을 통해 원격지에 안전하게 저장 및 보관하는 서비스이다(그림 3 참조). 기존의 데이터 백업 방식은 별도의 하드디스크에 저장하거나 CD, 플로피 디스크 등에 저장하여 보관하는 방식을 사용하여 왔다. 하지만 이러한 방식들은 개인의 취급 부주의나 도난 또는 천재지변을 통해서 단번에 소실되어 버릴 수 있다는 취약점을 가지고 있다. 인터넷 백업 시스템은 개인의 데이터를 원격지에 저장함으로써 각종 재해에 대비할 수 있고 인터넷 연결만으로 가정이나 회사뿐만 아니라 세계 어느 곳에서나 자유롭게 데이터를 저장 및 복구하면서 지속적인 작업을 할 수 있는 이동성을 제공하고 비밀리에 보관되어야 하는 중요한 문서나 법적 효력을 지니는 계약서, 합의서 등을 안전하게 저장할 수 있으며 개인적으로 백업 장비를 구입하고관리 인원을 배치하는 것보다 훨씬 더 저렴한 비용으로 백업 장비를 이용할 수 있다는 장점이 있다

본 논문에서는 이러한 인터넷 백업 시스템에 제안하는 온라인 비밀 분산 방식을 적용하여 사용자의 요구에 맞게 여러 가지 안전성을 갖는 데이터 백업 서비스를 제공할 수 있는 인터넷 백업 서비스를 제안하고자 한다. 기존의 인터넷 백업 시스템에 제안하는 온라인 비밀 분산 방식을 적용하는 경우 다음과 같은 장점이 있다.

① 높은 안전성을 제공할 수 있다.

소규모의 기업이나 개인이 암호학적 비밀 정보(예를 들어, 회사나 개인의 비밀키나 계약서 등과 같은 중요



(그림 3) 인터넷 백업 시스템의 개요

한 데이터를 원격지에 보관하는 경우, 원격지 데이터베이스의 손상에 의한 개인의 데이터 손실을 막기 위해 보통 동일한 데이터를 몇 개의 다른 저장 장치에 중복하여 저장한다. 이러한 경우 제안하는 온라인 비밀 분산 방식을 적용하여, 각 저장 장치에 동일한 내용의 데이터를 보관하는 것이 아니라 비밀 정보의 부분 정보만을 보관하고 필요한 경우 본래의 비밀을 복원하도록 할 수 있다. 따라서, 공격자가 원격지의 저장 장치에 접근하여 하나의 비밀을 얻게 되더라도 사용자의 본래의 비밀은 안전하게 되므로 즉 더 높은 안전성을 갖는 인터넷 백업 서비스를 제공할 수 있게 된다.

② 사용자의 요구에 따라 여러 가지 수준의 서비스를 제공할 수 있다.

제안하는 온라인 비밀 분산 방식을 인터넷 백업 시스템에 적용하는 경우에, 저장하는 데이터의 중요도에 따라 비밀 분산에 필요한 (t, n) 값을 선택적으로 적용할 수 있도록 하여 사용자의 요구에 따라 여러 형태의 서비스를 제공할 수 있다.

③ 효율적인 데이터 저장·복구 및 가 가능하다.

제안하는 온라인 비밀 분산 방식은 비밀 분산 및 복원에 요구되는 계산량을 해쉬 함수의 계산만으로 개선하였으므로 사용자들은 인터넷을 통해 어느 곳에서나 원격지의 서버에 접속하여 효율적으로 데이터를 저장하거나 복원할 수 있다.

6. 결 론

본 논문에서는 하나의 부분정보만으로 여러 개의 비밀을 분산할 수 있는 일방향 해쉬함수에 기반한 효율적인 온라인 비밀분산 방식을 제안하였다. 제안하는 방식은 액세스 구조가 변하는 경우에 게시판에 공개된 값들만 변경하면 각 참가자들은 기존의 부분정보를 그대로 사용할 수 있으며, 각 참가자들의 부분정보는 본래 비밀정보 s와 동등한 크기를 갖는다. 더욱이 참가자들의 부정이 있는 경우 그 수에 관계없이 부정한 참가자의 신분을 밝혀낼 수 있고 기존에 제안된 방식들에 비해 계산상 효율적이라는 장점이 있다.

따라서, 이러한 비밀분산 방식은 비밀정보의 관리나 키복구 시스템, 인터넷 백업 시스템 등에 활용할 수 있을 것으로 기대한다.

참 고 문 헌

[1] G. R. Blakely, "Safeguarding cryptographic key," In proceeding of AFIPS National Computer Conference, pp.313-317, 1979

[2] C. Cachin, "On-line secret sharing," In C. Boyd, editor, Proceeding of the 5th IMA conference on Cryptography and Coding, pp.190-198, Springer-Verlag, 1995

[3] L. Chen, D. Gollmann, C. J. Mitchell and P. wild, "Secret sharing with Reusable Polynomial," ACISP '97, pp.183-193, 1997

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trransaction on Information Theory IT-22, pp.644-654, 1976.

[5] P. Fedlman, "A Practical scheme for Non-interactive

Verifiable secret sharing," Proceeding of the 28th Annual Symposium on the Foundation of Computer Science, pp.427-437, 1987

[6] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in Proc 19th ACM Symposium on Theory of Computing (STOC), pp 218-229, 1987

[7] H. Ghodosi, J. Pieprzyk, G. R. Chaudhry, J. Seberry, "How to prevent cheating in Pinch's scheme," Electronic Letters, 33(17) : 1453-1454, 1997

[8] H. Y Lin and L. Harn, "A Generalized Secret Sharing Scheme with Cheater Detection," Advances in Cryptology-ASIACRYPT'91 Proceeding, Springer-Verlag, pp.149-158, 1993

[9] A. Menezes, P. van Oorschot, S Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996

[10] T. P. Pederson. "Distrobuted provers with Applications to Undeniable signatures," Advances in Cryptology-EUROCRYPT'91 Proceeding, Springer-Verlag, pp.221-242, 1991

[11] R. G. E. Pinch, "On-line multiple secret sharing," Electronic Letters, 32(12) : 1087-1088, 1996

[12] R. Rivest, A. Shamir, and L. Adleman, "A method for Obtaining Digital signature and Public key Cryptosystems," Communication of the ACM, pp. 120-128, FEB. 1978.

[13] Adi Shamir, "How to share a secret," Communication of the ACM, 21 : 120-126, 1979

[14] M. Tompa, H. Woll, "How to share a secret with cheater," Journal of Cryptology, 1 : 133-138, 1988

[15] Chan Yeob Yeun, Chris J. Mitchell, "How to identify all cheater in Pinch's scheme," JWIS '98, Japan-Singapore Joint Workshop on Information Security, Singapore, Dec. 1998.

[16] Chan Yeob Yeun, Chris J. Mitchell, Mike Burmester, "An Online Secret Sharing which Identifies All Cheater," Proceeding of NORDSEC '98, The Third Nordic Workshop on Secure IT Systems, Norway, Nov. 1998

[17] Y. Zheng, T Hardjono and J. Seberry, "Reusing share in secret sharing schemes," The Computer Journal 37, pp.199-205, 1994

[18] FIPS PUB-185 Escrowed Encryption Standard, 1993

[19] http://www.zoi.net/internet/index.htm

오 수 현

e-mail : shoh@dosan.skku.ac.kr

1998년 성균관대학교 정보공학과 졸업(공학사)

2000년 성균관대학교 전기전자 및 컴퓨터 공학과 대학원 졸업(공학석사)

2000년~현재 성균관대학교 전기전자 및 컴퓨터 공학과 박사 과정

관심분야 : 암호 이론, 정보 이론

김 승 주

e-mail : skim@kisa.or.kr

1994년 성균관대학교 정보공학과 졸업(공학사)

1996년 성균관대학교 정보공학과 대학원 졸업(공학석사, 암호학 전공)

1999년 성균관대학교 정보공학과 대학원 졸업(공학박사, 암호학 전공)

1999년~현재 한국정보보호센터 기술부/암호기술팀 과제책임자

2000년~현재 한국정보통신기술협회, 정보보호 기술위원회, 암호 기 술 연구반 의장

관심분야 암호학, 정보 이론, 암호키 복구 기술, 소프트웨어 역분석 방지 기술

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

1976년 성균관대학교 전자공학과 졸업(학사)

1978년 성균관대학교 전자공학과 (석사)

1988년 성균관대학교 전자공학과 (박사)

1978년~1980년 한국전자통신연구소 연구원

1985년~1986년 일본 동경공대 객원 연구원

1996년~1998년 정보화 추진위원회 자문위원

1982년~현재 성균관대학교 전기전자 및 컴퓨터공학부 교수

1999년~현재 한국통신정보보호학회 부회장

1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 학부장

1999년~현재 성균관대학교 정보통신대학원 원장

관심분야 : 암호 이론, 정보 이론