광역 파이프 해쉬 함수에 기반한 안전하고 효율적인 비밀분산

김 희 도[†] · 원 동 호[††]

요 약

본 논문은 광역 파이프 해쉬함수에 기반한 안전하고 효율적인 비밀 분산 방식을 제안하고자 한다. 제안하는 비밀분산방식은 액세스 구조가 변하는 경우에도 공개한 값들만 변경하면 각 참가자에게 새로운 비밀 정보를 재분산 없이 그대로 사용할 수 있다. 또 참가자들의 부정이 있는 경우 그 수에 관계없이 항상 부정한 참가자들의 신분을 밝혀낼 수 있으며, 기존에 제안한 해쉬기반비밀분산 방식들 보다 안전하고, 계산상 효율적이라는 장점을 가지고 있다.

키워드 : 광역파이프해쉬함수, 비밀분산, 다중충돌 공격, 부정한 참가자

Secure and Efficient Secret Sharing Scheme Based on Wide Pipe Hash Function

Hie-Do Kim[†] · Dong-Ho Won[††]

ABSTRACT

In this paper, we propose a secure and efficient secret sharing scheme Based on wide pipe hash function. This scheme provides the property to share multiple secrets and allows participants to be added/deleted dynamically, without having to redistribute new secret shares. Proposed scheme has advantage to detect cheating and identify of all cheater, regardless of their number. Futhermore, it is more secure and efficient than previous schemes based on hash function.

Key Words : Wide Pipe Hash Function, Security Sharing, Multicollision Attack, Forged Participant

1. 서 론

비밀분산이란 비밀정보 S 에 대한 부분정보$S_i \in_r S$ $(1 \le i \le n)$를 n명의 참가자들에게 분배하고 필요한 경우에 허가된 참가자들의 부분 집합에 의해 본래의 비밀을 복원할 수 있도록 하는 암호학적 프로토콜을 말한다. 정보보호를 위해 암호를 사용한 후 키를 분실하거나 손상된 경우 암호문 복호가 불가능할 때 키 복구를 위해 비밀분산 방식을 적용할 수 있다. 이는 비밀정보의 관리뿐만 아니라 다자간 프로토콜이나 그룹 암호방식, 키복구시스템 등 다양한 분야에 적용될 수 있다. 이러한 비밀분산 방식은 Blakely[1]와 Shamir[2]에 의해 각각 1979년에 처음으로 제안되었다.

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 K를 복원할 수 있고,
2) $t-1$명 이하의 참가자들은 비밀 n 에 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 크기와 거의 같고 허가되지 않은 참가자들이 비밀 S 에 대해 아무런 정보도 얻을 수 없는 무조건적으로 안전한 비밀 분산 방식이

† 정 회 원 : 강릉영동대학 부사관과 부교수
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2006년 7월 21일, 심사완료 : 2006년 9월 20일

라는 장점이 있지만, 비밀이 한번 복원된 이후에는 참가자들에게 비밀이 노출되는 단점이 있다. 또한, 비밀을 복원할 수 있는 참가자의 집합인 액세스 구조가 변하는 경우에 딜러는 새로운 다항식을 생성하고 기존의 참가자들에게도 새로운 비밀을 재분배해야 하기 때문에 비효율적이다.

이러한 문제를 해결하기 위해 C. Cachin은 1995년 Cryptography and Coding이라는 국제학술회의에서 온라인 비밀분산 방식이라는 새로운 개념을 제안하였다[3]. 그 이후로 여러 온라인 비밀 분산 방식이 제안되었으나 다수의 비밀분산에 적용할 수 없거나 참가자의 부정을 검출할 수 없고 또는 많은 계산량을 요구한다는 등의 단점이 있다. 계산량을 개선하기위해 Oh 와 Won 이 해쉬 함수 기반 비밀 분산 방식을 제안하였다[4]. 그러나 해쉬 함수기반 비밀분산은 계산상 효율적이나 다중충돌공격(Multicollision Attack)에 노출된다. 따라서 본 논문에서는 기존에 제안된 방식들에 비해 계산상 효율적이고 다중충돌공격(Multicollision Attack)에 안전한 광역 파이프 해쉬 기반비밀분산 방식을 제안하고자 한다.

2. 비밀분산 방식

비밀분산 방식에서 본래의 비밀 K를 복원할 수 있는 허가된 참가자들의 집합을 액세스 구조(access structure) Γ라 한다. 이러한 액세스 구조가 동적으로 변하는 경우 즉, 새로운 참가자들이 비밀분산 방식에 참여하거나 기존의 참가자들이 제거되는 경우에 또 다른 비밀정보를 재분배하지 않고 기존의 비밀정보를 재사용할 수 있는 비밀분산 방식을 C. Cachin이 [3]에서 처음으로 제안하였으며 C. Cachin의 방식은 각 참가자가 본래의 비밀 K와 같은 크기를 갖는 하나의 부분정보만을 이용하여 다수의 비밀을 복원할 수 있는 방식이다. 또한 C. Cachin이 제안한 방식은 모든 참가자들이 접근할 수 있는 게시판에 인증된 정보를 공개하고 액세스 구조가 변하는 경우에 그 공개정보들의 값만을 변경하여 기존의 참가자들의 부분정보는 그대로 유지할 수 있게 하였다. 그러나 이 방식을 다수의 비밀분산에 적용할 경우, 하나의 비밀이 복원된 후에도 다른 비밀들이 안전하기 위해서는 각 참가자들의 비밀정보가 다른 참가자들에게 노출되지 않도록 하기 위해 부가적인 계산 과정이 필요하다는 문제점이 있다[5].

이러한 문제점을 해결하기 위해, Pinch는 [6]에서 Diffie-Hellmen 문제를 이용한 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 악의적으로 자신의 부분정보를 바르게 제공하지 않는 경우, 부정한 참가자의 신분을 밝혀낼 수 없다는 문제점이 있다.

따라서 Ghodoshi 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 확인 할 수 있는 과정을 추가하였다. 그러나 이 방식 또한 과 반수 이상의 참가자들이 공모하여 부정하는 경우에는 안전하지 않다는 문제점이 있다.

그 이후에, Yeun 등은 [8]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 비밀분산 방식을 제안하였다. 이 방식은 이산대수 문제나 RSA 암호 방식을 이용하여 비밀을 복원하는 과정에서 참가자들의 비밀이 노출되지 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.

3. 제안하는 파이프 해쉬 기반 비밀분산 방식

본 장에서는 광역 파이프 해쉬 함수를 이용하여 기존의 비밀분산 방식들을 좀더 안전하고 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. 최근 Lucks[9]은 다중충돌공격(multi-collision attacks)에 안전한 광역 파이프 해쉬 함수를 제안하였다. 본 논문에서는 이산대수 문제 대신 광역 파이프 해쉬 함수를 사용함으로써 이산대수문제 방식에 비해 계산량 측면에서 좀더 효율적이고 해쉬 함수기반 비밀 분산 방식보다 안전하다. 제안하는 비밀 분산 및 복원 프로토콜은 다음과 같다.

3.1 광역 파이프 해쉬 함수

다음과 같이 광역 파이프 해쉬 함수를 정의한다.

[정의 3.1]

$F : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$,

$G : \{0,1\}^n \rightarrow \{0,1\}^w$ 두고, 광역 파이프 해쉬 함수

$H^W : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$이고,

$$H^W(M,x) \triangleq G(H(m_k \| \ldots \| m_1, x))$$

여기서, $x \in \{0,1\}^n$, $y = F_k(x)$, $y \in \{0,1\}^n$, $m \in$

$\{0,1\}^k$, $M = m_k \| ... \| m_1$, $h_i = F_{m_i}(h_{i-1})$, $h_0 = x$, $z = F_{m_k}(...F_{m_1}(x)...)$, $\bar{z} = G(z) = H^W(M,x)$.

3.2 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 ($\Gamma \in 2^p$가 Γ의 원소일 경우, X에 속하는 참가자들의 비밀로부터 본래의 비밀 K를 복원할 수 있고, X가 Γ 의 원소가 아닐 경우에는 비밀을 복원하는 것이 불가능 함.
- Γ^* : Γ의 원소 중 비밀을 복원하는데 필요한 참가자의 수가 가장 적은 것들의 집합
- K : 본래의 비밀
- H^W: 다중 충돌 저항성을 갖는 광역 파이프 해쉬함수
- S_{pi} : 참가자 P_i의 디지털 서명

3.3 비밀분산 프로토콜

단계 1) D는 난수 r 과 각 참가자의 비밀값 $S_i \in_r S$ $(1 \le i \le n)$를 랜덤하게 선택한다.

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

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

$$T_X = K \oplus H^W(S,r) = K \oplus G(H(S_t \| \cdots \| S_1, r)$$
$$= K \oplus G(F_{S_t}(F_{S_{t-1}}(\cdots(F_{S_1}(r)\cdots))).$$

단계 4) D는 각 Γ^*에 속하는 각 원소 X에 대해 (X, r, T_X)와 $H^W(K)$ 값을 게시판에 공개한다.

3.4 비밀복원 프로토콜

단계 1) 참가자 P_i은 X에 해당하는 난수 r과 T_X, $H^W(K)$를 게시판으로부터 읽어온다.

단계 2) 각 참가자 P_i은 자신의 부분 정보와 난수 r을 이용하여 $H^W(S_i, r)$을 계산하고 다음과 같이 디지털 서명을 생성한다.

$$S_{P_i} = Sign_{P_i}(H^W(S_i r) \| X \| r)$$

단계 3) 참가자 P_i 는 X에 속하는 모든 참가자 P_n ($P_n \in X$ 이고 $P_i \neq P_j$)에게 S_{P_i}와 $H^W(S_i r) \| X \| r$전송한다.

단계 4) 각 참가자 $P_i(1 \le i \le t)$는 참가자 P_{i-1} 로부터 받은 서명을 검증한 후 $V_i = G(H(S_i \| \cdots \| S_1, r)$를 계산하고 다음과 같이 디지털 서명을 생성하여 참가자가 P_{i+1}에게 S_{p_i}와 V_i를 전송한다.

$$S_{P_i} = Sign_{P_i}(H^W(S_i r) \| X \| r)$$

단계 5) 참가자 P_i는 X 에 속하는 모든 P_t로 부터 받은 서명을 검증하고 다음과 같이 V_X를 계산한다.

$$V_X = G(H(S_j \| \cdots \| S_1, r)$$

단계 6) 참가자 P_t는 다음과 같이 K'를 복원한다.

$$K' = T_X \oplus H^W(V_X) \bmod p$$

단계 7) 복원한 비밀이 정확한지 알아보기 위해 $H^W(K')$를 계산하여 게시판에 공개된 $H^W(K)$값과 비교한다.

제안하는 방식의 안전성은 광역 파이프 해쉬 함수에 기반하므로 안전한 비밀분산 방식이며 각 참가자가 비밀로 간직하는 부분정보의 크기는 비밀 S의 크기와 비슷하므로 이상적인 비밀분산 방식이라 할 수 있다. 그리고 액세스구조가 변하는 경우에 게시판에 공개된 값들만 변경하면 각 참가자들은 기존의 부분정보를 그대로 사용할 수 있고, 하나의 부분정보를 재사용하여 다수의 비밀을 분산 및 복원할 수 있다. 또한 참가자들이 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.

4. 제안하는 비밀 분산 방식의 특징

제안하는 방식의 이러한 특징에 대해서는 다음 장에서 자세히 살펴보기로 한다.

4.1 액세스 구조가 동적으로 변하는 경우

제안하는 비밀분산 방식은 새로운 참여자가 있거나 기존의 참여자를 제거하는 등의 동적인 액세스 구조의 변화가 있을 경우에, 나머지 참가자들의 부분정보를 재사용할 수 있는 비밀분산 방식이다. 따라서 액세스 구조가 변하는 경우, 다음과 같은 과정을 통해 게시판에 공개된 값들만 변경하면 비밀정보의 재 전송 없이 기존의 비밀 분산 방식을 그대로 사용할 수 있다. 또한, 제안하는 방식은 참가자의 새로운 참여나 제거뿐만 아니라 비밀분산에 필요한 참가자의

수 n이나 t 값도 필요에 따라 변경할 수 있다.

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

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

$$T_X' = K \oplus H^W(S, r') = K \oplus G(H(S_t \| \cdots \| S_1, r'))$$

단계 3) D는 게시판에 새로운(X, T_X', r')를 모두 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 $H^W(K')$가 게시판에 공개된 해쉬값 $H^W(K)$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 D에게 제출한다.

단계 2) D는 각 참가자의 공개키를 이용하여 서명을 검증하고 $H^W(S_i, r)$ $(1 \le i \le t)$을 구한다.

단계 3) D는 저장해둔 각 참가자의 부분정보인 $S_{P_i}(1 \le i \le t)$ 와 공개된 난수 r을 사용하여 $H^W(S_i, r)$ $(1 \le i \le t)$ 을 계산한다.

단계 4) D는 자신이 계산한 $H^W(S_i, r)$ $(1 \le i \le t)$과 각 참가자들이 제출한 $H^W(S_i, r)$ $(1 \le i \le t)$ 값을 비교한다.

〈표 1〉 제안하는 방식과 기존의 방식의 비교

	게시판에 공개하는 정보	부정한 참가자의 검출 및 신분확인	다수의 비밀분산에 적용	복원과정에 요구되는 계산량	비고
Cachin 방식	$X \in \Gamma$ 인 X 에 대해 (X, T_X)	×	추가적인 계산량 요구	덧셈 : $\|X\|-1$번 해쉬함수 : 1번	
Pinch 방식	(X, T_X, g_X)	×	○	모듈라 멱승 : $\|X\|$ 번 해쉬함수 : 1번 덧셈 : 1번	
Ghodosi 방식	$(X, T_X, g_X, g_X^{V_0}, C_X)$	과반수이상이 정직할 경우에만 가능	○	모듈라 멱승 : $2\|X\|^2-\|X\|$번 해쉬함수 : $\|X\|$번 덧셈 : $\|X\|$번	
Yeun 방식	$(X, T_X, g_X), f(K), f(K)$	○	○	모듈라 멱승 : $\|X\|$번 해쉬함수 : 1번 덧셈: 1번 각 참가자당 1번의 서명 생성 검증 필요	
Oh-Won 방식	$(X, T_X, r), f(K)$	○	○	해쉬함수 : $\|X\|+1$번 Exclusive-or : $\|X\|$번 각 참가자당 1번의 서명 생성/검증 필요	
제안하는 방식	$(X, T_X, r), H^W(K)$	○	○	광역파이프해쉬함수 : $\|X\|+1$번 Exclusive-or : $\|1\|$번 각 참가자당 1번의 서명 생성/검증 필요	다중충돌공격에 안전

단, 여기서 $|X|$는 비밀 복원에 필요한 참가자의 수를 말한다.

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 $H^W(S_i, r)$ $(1 \le i \le t)$를 이용하여 여러 개의 비밀을 분산 및 복원하는데 적용할 수 있다. 분산하고자 하는 m개의 비밀을 K_l이라 하자. (단,$l = 1, 2, ..., m$)

단계 1) D는 새로운 비밀 K_l를 분산할 때마다 이 전과 다른 액세스 구조 Γ_l을 구성한다.

단계 2) D는 비밀 K_l 을 분산하기 위해, $X \in \Gamma_l$ 인 X에 대해 난수 r_l를 선택하여 다음을 계산한다. 단, 이때, $X = \{P_1, P_2, ..., P_r\}$ 이라 하자.

$$T_{X_l} = K_l \oplus H^W(S, r_l) = K \oplus G(H(S_i \| \cdots \| S_1, r_l)$$

단계 3) D는 각 비밀 K_l에 대해(X, r_l, T_{X_l})와 $H^W(K_l)$을 게시판에 공개한다.

이때, 각각의 비밀 K_l 에 대해 서로 다른 난수 r을 사용하므로 하나의 비밀이 복원되더라도 다른 비밀들의 안전성에는 아무런 영향을 미치지 않는다.

6. 결 론

본 논문에서는 광역 파이프 해쉬함수에 기반한 효율적인 비밀분산 방식을 제안하였다. 제안하는 방식은 액세스 구조가 변하는 경우에 게시판에 공개된 값들만 변경하면 각 참가자들은 비밀정보를 재분산 없이 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, 비밀복원 과정에서 Exclusive-or를 한번만 요구하고 광역파이프 해쉬 함수를 사용하므로 기존에 제안된 해쉬 함수에 기반한 방식보다 더 안전하다는 장점이 있다.

참 고 문 헌

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

[2] AdiShamir, How to share a secret, Communication of the ACM, 21 : 120-126. 1979.

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

[4] Soo-Hyun Oh, Seung-Joo Kim, Dong-Ho Won, Efficient On-line Sharing Scheme based on One-way Hash Function. The transactions of the Korea Information Processing Society, Vol.7-C NO.10, pp.3128-3137, October, 2000.

[5] 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 Theorem Computing pp.218-229, 1987.

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

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

[8] Chan Yeob Yeun, Chris J. Mitchell, Mike Burmester, An Online Secret Sharing Scheme which Identifies All Cheater, Proc. of NORDSEC 98. The Third Noridic Workshop on Information Security Singapore, Dec., 1998.

[9] Stefan Lucks, A Failure-Friendly Design Principle for Hash Functions, ASICRYPT 2005, LNCS 3788, pp.474C 494, 2005.

김 희 도

e-mail : hdkim@gyc.ac.kr
1985년 서울산업대학교 전자공학과 (학사)
1988년 한양대학교 전자통신공학과 (석사)
1999년 성균관대학교 전기전자 및 컴퓨터공학과 수료
1994년~현재 강릉영동대학 부사관과 부교수
관심분야 : 정보보호 및 암호

원 동 호

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

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본동경공업대학 객원연구원

1988년~1999년 성균관대학교 교학처장, 전기전자컴퓨터공학부장, 정보통신대학원장 정보통신기술연구소장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

현 재 성균관대학교 정보통신공학부 교수, 정통부지정 정보보호 인증기술 연구센터장, 성균관대학교 연구처장

관심분야 : 암호이론, 정보이론