식별정보 기반 비밀 분산

정영석*, 문종철*, 이상환*, 이래*, 서인석*, 원동호**
*국가보안기술연구소, **성균관대학교
e-mail : yschung11@etri.re.kr

Identity-Based Secret Sharing

Youngseok Chung*, Jongcheol Moon*, Sanghwan Lee*, Rae Lee*, Inseok Seo, Dongho Won**
*National Security Research Institute
**Dept. of Information and Communication Engineering, Sungkyunkwan Universisy

요 약

본 논문에서는 식별 정보 기반의 비밀 분산 방식을 제안한다. 본 방식에서는 비밀 정보를 분할한 부분 정보에 딜러와 참가자의 식별정보가 포함된다. 각 식별정보는 비밀 분할 및 복원 과정에서 딜러와 참가자, 참가자와 참가자 간 상대방을 인증하는데 사용된다. 또한 참가자 간에는 상호 부분 정보의 송·수신 외에 딜러와의 통신 등 별도의 통신 과정 없이 부분 정보의 검증이 이루어진다.

1. 서론

비밀 분산은 특정 참가자 그룹만이 복원해 낼 수 있도록 하나의 비밀 정보를 다수의 부분 정보로 분할하여 참가자들에게 분배하는 방식이다.

(k,n) threshold scheme을 사용한 비밀 분산 방식[1]은 딜러가 비밀 정보를 n개의 부분 정보로 분할하여 각각 n명의 참가자들에게 분배하고, 비밀 복원 시 k명 이상의 참가자가 모여 비밀 정보를 복원하는 방식이다. 이 방식에서 참가자들은 딜러로부터 전달 받은 부분 정보가 자신에게 전달된 올바른 정보인지 확인할 수 없다. 이러한 점을 보완하여 참가자가 딜러로부터 수신한 부분 정보의 정당성을 검증할 수 있는 방식[4]과 부분 정보를 수신한 참가자 뿐만 아니라 비밀 복원에 참가하는 모든 참가자들이 딜러와의 통신을 통해 상대방 참가자의 부분 정보를 검증할 수 있는 방식[6] 등이 제안되었다.

이에 본 논문에서는 비밀 정보 분할 시 참가자가 딜러로부터 전송 받은 부분 정보의 정당성을 검증함과 동시에 딜러를 인증할 수 있으며, 비밀 정보 복원 시 딜러와 상대방 참가를 동시에 인증할 수 있는 식별정보 기반 비밀 분산(IDB-SS : Identity-based Secret Sharing) 방식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 제안하는 IDB-SS의 개요에 대해 알아보고, 3장에서는 IDB-SS의 구성요소에 대해 알아본다. 4장에서 IDB-SS 방식에 대해 설명하며, 5장에서 IDB-SS의 안전성을 분석한다. 그리고 6장에서 결론을 맺는다.

2. 개요

IDB-SS 방식에서는 기존에 제안된 방식에서와 마찬가지로 딜러가 하나의 비밀 정보를 다수의 부분 정보로 분할하여 참가자들에게 분배한다. 그리고 각 참가자들은 딜러로부터 수신한 부분 정보의 정당성을 검증한다. 또한 비밀 정보 복원을 위해 모인 참가자들은 상대방이 제시한 부분 정보의 정당성을 검증한다. 그러나 기존의 방식이 갖는 단점을 보완하고자 IDB-SS 방식은 다음과 같은 특성을 지닌다.

첫째, 부분 정보의 생성 과정에서 참가자의 식별정보를 입력 파라미터로 사용하기 때문에 별도의 파라미터를 사용할 경우에 존재하는 파라미터와 해당

참가자간의 맵핑 정보를 참가자들에게 전송할 필요가 없다. 둘째, 부분 정보의 검증 정보를 생성하는 과정에서 딜러 및 참가자의 식별정보가 포함되기 때문에 비밀 분할 및 복원 과정에서 참가자들은 딜러와 상대방 참가자를 인증을 할 수 있다. 즉 검증 정보 검증 시 신뢰할 수 있는 딜러가 부분 정보를 생성하였다는 사실과 부분 정보의 수신자가 정당한 참가자라는 사실을 모든 참가자들이 확인할 수 있다. 셋째, 모든 비밀 정보 분할 및 복원 과정은 식별정보를 기반으로 이루어진다. 따라서 상대방을 인증하는데 공개키 인증서를 사용할 필요가 없으므로 공개키 인증서의 유효성 검증 절차가 존재하지 않는다.

3. IDB-SS의 구성 요소

IDB-SS는 다음과 같이 4개의 알고리즘으로 구성된다.

(1) 분할 알고리즘 : (k,n) threshold scheme을 이용하여 비밀 정보를 분할하여 n개의 부분 정보를 생성한다.
(2) 분배 알고리즘 : 부분 정보로부터 검증 정보를 생성하고, 검증 정보로부터 분배 정보를 생성한다.
(3) 검증 알고리즘 : 딜러가 공개한 정보, 식별정보, 검증 정보를 이용하여 부분 정보 또는 분배 정보가 정당한 딜러로부터 정당한 참가자에게 분배되었는지 검증한다.
(4) 복원 알고리즘 : 비밀 복원에 참가한 모든 참가자의 식별정보와 부분 정보로부터 비밀 정보를 복원한다.

4. 제안하는 IDB-SS 방식

제안하는 IDB-SS는 분할 과정과 복원 과정으로 이루어진다. 분할 과정에서 딜러는 분할 알고리즘을 이용하여 비밀 정보를 분할하여 부분 정보를 생성하고, 분배 알고리즘을 이용하여 분배 정보를 생성한 후 각 참가자들에게 전송한다. 그리고 참가자들은 검증 알고리즘을 이용하여 딜러를 인증하고 자신의 분배 정보를 검증한다.

복원 과정에서 각 참가자들은 검증 알고리즘을 이용하여 딜러와 상대방 참가자를 인증하고 상대방 참가자의 분배 정보를 검증한다. 그리고 복원 알고리즘을 이용하여 부분 정보들로부터 비밀 정보를 복원한다.

(1) 사전 설정

분할하고자 하는 비밀 정보를 S라 가정한다. 비밀 분할 및 복원에 참가하는 n명의 참가자를 $P_i(1 \le i \le n)$ 라 하고 이들의 집합을 P ($P_i(1 \le i \le n) \in P$)라 하며 각 참가자들의 식별정보를 $ID_i(1 \le i \le n)$라 가정한다. 그리고 S를 분할하여 부분 정보를 생성·분배하는 딜러를 $D \notin P$, 딜러의 식별정보를 ID_D라 가정한다. P의 부분 집합들 중 비밀 복원의 권한이 부여된 부분 집합들의 집합을 Γ라 할 때 비밀 복원을 수행할 수 있는 k명의 참가자들의 집합을 $R \in \Gamma(|R| = k)$, $R = \{P_i | 1 \le i \le k\}$이라 한다.

비밀 분할 및 복원을 수행하기 위해 D가 선택한 큰 소수를 p, Z_p 상에서 위수가 q인 원시 원소를 g라 한다($g^q = 1(mod p)$). p보다 크며 크기가 비슷한 두 소수를 u, v라 하고 이들의 곱을 n 이라 한다. 이때 u, v는 D만이 알고 있는 값이다. 또한 일방향 해쉬 함수를 h라 하고 p, q, g, n과 h는 모든 참가자들에게 공개된다고 가정한다.

(2) 분할 과정

□ 부분 정보 및 분배 정보 생성

D는 다음의 과정을 통해 S를 부분 정보로 분할하고 이를 이용하여 분배 정보를 생성한다.

① Z_p 상에서 임의의 원소 $a_i(1 \le i \le k-1)$를 선택하여 다음과 같은 $k-1$차 방정식 $f(x)$를 구성한다.

$$f(x) = S + \sum_{i=1}^{k-1} a_i \cdot x^i \,(mod p) \quad \cdots\cdots (1)$$

② 각 참가자들의 식별정보 $ID_i(1 \le i \le n)$를 이용하여 부분 정보 $s_i(1 \le i \le n)$를 생성한다.

$$s_i = f(ID_i) = S + \sum_{j=1}^{k-1} a_j \cdot {ID_i}^j (mod p) \quad \cdots\cdots (2)$$

③ 각 참가자들의 부분 정보에 대한 검증 정보 S_i $(1 \le i \le n)$를 생성한다.

$$S_i = g^{s_i} (mod p) \quad \cdots\cdots (3)$$

④ 공개 검증 함수 $F(x)$를 생성한다.

$$F(x) = \prod_{i=0}^{k-1} (g^{a_i})^{x^i (mod q)} (mod p),\ (a_0 = S) \quad \cdots\cdots (4)$$

⑤ S_i에 대한 분배 정보 $D_i (1 \le i \le n)$를 생성한다.

$$e_i = h(ID_i \| ID_D) \quad \cdots\cdots (5)$$
$$d_i = h(ID_i \| ID_D)^{-1} (mod \phi(n)) \quad \cdots\cdots (6)$$
$$D_i = S_i^{d_i} (mod n) \quad \cdots\cdots (7)$$

⑥ 생성된 $F(x)$는 모든 참가자들에게 공개하고 s_i $(1 \le i \le n)$와 $D_i (1 \le i \le n)$는 각 참가자들에게 전송한다. 이 때, s_i는 비밀리에 전송한다.

□ 분배 정보 검증

P_i는 다음의 과정을 통해 s_i와 D_i가 D로부터 자신에게 전송된 올바른 정보인지를 검증한다. 즉 s_i를 검증함과 동시에 D를 인증한다.

① ID_i와 $F(x)$를 이용하여 계산한 S_i와 s_i로부터 계산한 S_i가 서로 일치하는지 확인한다.

$$F(ID_i) = S_i = g^{s_i} (mod p) \quad \cdots\cdots (8)$$

② 자신의 식별정보와 D의 식별정보를 이용하여 e_i를 생성하고, 식 (8)에서 생성한 S_i와 D_i로부터 생성한 S_i가 서로 일치하는지 확인한다.

$$S_i = D_i^{e_i} (mod n) \quad \cdots\cdots (9)$$

(3) 복원 과정

□ 분배 정보 검증

비밀 복원에 참여한 모든 참가자들은 상대방 참가자의 분배 정보를 D가 생성하여 올바르게 분배하였는지 검증한다. 즉 상대방 참가자의 분배 정보를 검증함과 동시에 상대방 참가자와 D를 인증한다. P_i가 P_j의 분배 정보를 검증하는 과정을 보면 다음과 같다.

① 검증하고자 하는 P_j의 식별정보 ID_j와 $F(x)$를 이용하여 S_j를 생성한다.

$$S_j = F(ID_j) \quad \cdots\cdots (10)$$

② P_j의 식별정보와 D의 식별정보를 이용하여 e_j를 생성한다.

$$e_j = h(ID_j \| ID_D) \quad \cdots\cdots (11)$$

③ (10)에서 생성한 S_j와 D_j, e_j로부터 생성한 S_j가 서로 일치하는지 확인한다.

$$S_j = D_j^{\ e_j} (mod n) \quad \cdots\cdots (12)$$

□ 비밀 정보 복원

비밀 복원에 참가한 참가자들의 $S_i (1 \le i \le k)$에 대한 검증을 완료한 후 다음과 같이 (ID_i, s_i)를 이용하여 S를 복원한다.

$$S = \sum_{i=1}^{k} s_i \cdot \prod_{1 \le j \le k, i \ne j} \frac{ID_i}{ID_j - ID_i} (mod p) \quad \cdots\cdots (13)$$

5. 안전성 분석

(1) 비밀 정보에 대한 보호

k-1개 이하의 부분 정보 s_i로부터 S를 유추하기 위해서는 식 (2)의 모든 a_i를 알아야 한다. 그런데 a_i는 식 (4)에서와 같이 모듈러 p 상에서 g의 멱승으로 계산되어 공개되기 때문에 공개된 값으로부터 a_i를 구하는 것은 이산 대수 문제를 푸는 것과 동일하다.[7] 또한 a_i 없이 S를 유추하는 것은 $\frac{1}{p}$의 확률로만 가능하다. 따라서 공개된 정보로부터 S를 유추해 내는 것은 계산상으로 불가능하다.

(2) 부분 정보에 대한 보호

S_i로부터 s_i를 유추하기 위해서는 식 (3)에서 보는 바와 같이 모듈러 p 상에서 g의 멱승인 s_i를 구해야 한다. 이는 이산 대수 문제를 푸는 것과 동일하므로 계산상 불가능하다.[7]

(3) 분배 정보에 대한 보호

식 (7)에서 임의의 s_i'과 ID_i'에 대한 분배 정보

D_i'를 계산하기 위해서는 $d_i' = h(ID_i' \| ID_D)^{-1} (mod \phi(n))$ 인 d_i'을 알아야 한다. d_i'를 계산하는 것은 $\mathrm{mod}\phi(n)$을 계산하는 것보다 쉽지 않으며 n을 소인수 분해하는 것보다 쉽지 않다.[8] 따라서 정당한 D가 아닌 공격자가 임의의 부분 정보에 대한 임의의 분배 정보를 생성하는 것은 계산상 불가능하다.

6. 결론

본 논문에서는 딜러와 참가자의 식별정보가 부분 정보에 포함된 식별정보 기반의 비밀 분산 방식을 제안하였다. 부분 정보를 검증하는 과정에서 식별정보를 사용함으로써 참가자와 참가자간, 참가자와 딜러간 명시적으로 인증을 수행할 수 있었고, 딜러와 참가자간 별다른 통신 과정 없이 부분 정보를 검증할 수 있었다. 또한 비밀 분산을 수행하면서 각 참가자들이 특정 수 미만의 부분 정보와 공개 정보를 이용하여 비밀 정보를 계산하는 것과 딜러가 각 참가자에게 비밀리에 전송한 부분 정보를 공개 정보로부터 계산하는 것, 그리고 정당한 딜러가 아닌 공격자가 임의의 부분 정보를 생성하여 비밀 복원에 참여하는 것이 불가능함을 보였다.

제안한 방식은 복잡한 인증 과정이 없는 효율적인 키복구 시스템을 설계하는데 적용될 수 있을 것으로 판단되며, 향후 분배 정보의 검증 후 부분 정보를 안전하게 전송할 수 있는 방법에 대한 연구가 필요하다.

참고문헌

[1] A. Shamir, "How to share a secret", Communications of the ACM, 22(11), pp.612-613, 1979.

[2] M. Tompa, H. Woll, "How to share a secret with cheaters", Journal of Cryptology, 1(2), pp.133-138, 1988.

[3] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults", Proceedings of the 26th IEEE Symposium on Foundation of Computer Science, pp.383-395, 1985.

[4] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", Proceedings of the 28th IEEE Symposium on Foundation of Computer Science, pp.427-437, 1987.

[5] Torben P. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing", Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, pp.129-140, 1991.

[6] M. Stadler, "Publicly verifiable secret sharing", Advances in Cryptology - EUROCRYPT'96, 1070 of LNCS, pp.190-199, 1996.

[7] W. Diffie, M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, IT-22, pp.472-492, 1976.

[8] R.Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, 21(2), pp.120-126, 1978.

[9] M. Girault, "Self-certified public keys", Advances in Cryptology - EUROCRYPT'91, 547 of LNCS, pp.490-497, 1991.

[10] H.Petersen, P. Horster, "Self-certified keys - concepts and applications", Proceedings of Conference on Communications and Multimedia Security, 1997.

[11] S. Kim, S. Oh, S. Park, D. Won, "Verifiable Self-Certified Public Keys", Proceedings of INRIA Workshop on Coding and Cryptography, pp.139-148, 1999.