서명자 검증 가능한 ID-기반 환 서명

김기동 장직현
서강대학교 컴퓨터공학과
pisces99@gmail.com, jchang@alglab.sogang.ac.kr

A Signer Verifiable ID-based Ring Signature Scheme

Ki Dong Kim Jik Hyun Chang
Department of Computer Science and Engineering, Sogang University

요 약

환 서명(ring signature)은 서명자가 자신을 포함한 환(ring)을 구성하여 환의 구성원들의 공개키(public key)들을 이용하여 생성하는 서명이다. 검증자의 입장에서는 누가 서명했는지 알 수 없는 서명자 익명성(signer ambiguity)이 가장 중요한 성질이다. 본 논문에서는, 서명자가 어떤 특정한 정보를 노출함으로써 실제 서명자가 누구인지 알 수 있는 방식(scheme)을 제안한다. 따라서, 필요하다면 서명자는 자신이 실제 서명자임을 다른 사람들에게 증명할 수 있다.

1. 서 론

환 서명(ring signature)[1]은 서명자가 자신을 포함한 환(ring)을 구성하여 자신의 비밀키와 다른 구성원들의 공개키를 이용하여 임의의 메시지에 대해 서명하는 방식이다. 그룹 서명(group signature)과는 달리, 관리자를 따로 두지는 않고 서명자가 자신을 포함한 환 구성원(ring member)들의 공개키와 자신의 비밀키를 이용하여 서명을 생성하고, 서명을 검증하는 사람은 그 서명이 환의 구성원들 중 한 명이 만든 것이라는 것은 알지만 실제 서명자가 누구인지는 알아내기 힘들다. 2001년에 Rivest외 2인[1]이 처음 환 서명의 개념을 제안하였고 그 후 다양한 환 서명 방식[2-6]이 제안되었다.

환 서명을 이용하여 생각해 볼 수 있는 응용(application)중 하나는 중요한 정보를 누가 발설했는지 모르게 노출시키는 것이다. 예를 들어, 테러리스트의 위치를 알고 있는 사람은 그 위치를 경찰에 알리고 싶어 할 것이다. 하지만 그 정보를 노출하는 사람의 신원이 테러리스트에 알려진다면 그 사람은 큰 위협을 받게 될 것이다. 이러한 경우에 환 서명을 이용하여 제보자의 신원을 알리지 않을 수 있다. 반면에 위와 같은 경우, 경찰에 의해 테러리스트가 소탕되고 제보자에게는 보상이 주어져야 할 때 실제 제보자가 누구인지 알 수 있는 방법이 필요하고 그러한 방식들이 전환 가능한 환 서명(convertible ring signature)[7-11]이라는 이름으로 제안되어 왔다.

한편, 전통적인 증명서-기반 공개키 암호 시스템(certificate-based public key cryptosystem)에서의 각 사용자의 공개키는 임의로 만들어진 문자열이었다. 따라서 각 사용자는 자신의 공개키에 대한 유효성을 증명해야 했는데 여기에 많은 자원이 소모된다는 단점을 가진다. 1984년에 Shamir는 사용자의 이름이나 전자우편 주소, 전화번호 등을 공개키로 사용하는 ID-기반 암호 시스템과 서명 시스템[12]을 제안하였다. 이 방법을 사용하면

공개키에 대한 인증과정을 거치지 않아도 되기 때문에 시스템 전체의 효율성이 높아진다는 장점이 있다. 따라서 전환 가능한 환 서명 방식에 ID-기반 서명 방식을 결합함으로써 이전의 방식보다 더 효율적인 서명 방식을 구현할 수 있다.

본 논문에서는 Chow외 2인[14]이 제안한 ID-기반 환 서명 방식(ID-based ring signature scheme)을 이용하여 실제 서명자가 특정한 정보를 노출시키지 않는다면 서명자 익명성이 보장되고, 노출시키면 실제 서명자가 누구인지 알 수 있는 방식을 제안한다.

2. 정의와 전제조건

2.1. 정의

정의 1. 서명자 검증 가능한 ID기반 환 서명(signer verifiable ID-based ring signature)은 다음 여섯 개의 알고리즘으로 구성된다.

- **사전설정(setup)** : 주어진 k(security parameter)에 대하여 비밀키 생성기(private key generator, PKG)가 시스템 전체의 공개키(system public key)와 비밀키를 만든다.
- **키 생성(Key Generation)** : PKG는 주어진 임의의 사용자의 식별자(identity)를 이용하여 그 사용자의 비밀키를 만들어 안전한 채널을 통해 해당 사용자에게 돌려준다.
- **서명 생성(Signature Generation)** : 주어진 메시지 m과 n - 1명의 공개키, 그리고 서명자 자신의 비밀키를 이용하여 실제 서명자가 서명을 하여 (메시지, 서명)순서쌍을 만든다.
- **서명 검증(Signature verification)** : (메시지, 서명) 순서쌍과 n개의 식별자 리스트를 가지고 있다면, 임의의 사용자는 주어진 서명이 해당 메시지에 대한 것인지 확인한다.
- **전환(Convert)** : 필요한 경우, 실제 서명자는 특정한 정보를 노출시킴으로써 자신이 실제 서명자임을 공개한다.
- **전환 검증(Convert verification)** : 검증자는 실제 서명자가 노출한 정보를 이용하여 실제 서명자를 확인할 수 있다.

정의 2. 서명자 검증 가능한 ID기반 환 서명은 다음 세 개의 요구사항을 갖는다. [13]

- **서명자 익명성(Signer ambiguity)** : n을 환의 구성원 수라 할 때, 검증자가 성공적으로 서명자를 결정할 수 있는 확률은 $1/n$보다 크지 않아야 한다.
- **위조 불가능성(Unforgeability)** : 환의 구성원 이외의 사용자가 성공적으로 서명을 위조할 수 있는 확률은 무시할 수 있어야 한다.
- **서명하지 않은 사용자에 대한 전환 불가능성(Unconvertibility against nonsigner)** : 실제 서명자가 아닌 다른 환의 구성원이 서명을 성공적으로 전환(convert)할 수 있는 확률은 무시할 수 있어야 한다.

2.2. 겹선형 쌍함수와 그에 관련된 복잡성 가정(Bilinear Pairings and Related Complexity Assumptions)

겹선형 쌍함수(bilinear pairing)는 다양한 암호학 방식에 사용되고 있는 중요한 성질이다. 먼저, $(\mathbf{G}_1, +)$, $(\mathbf{G}_2, \cdot)$를 소수인 위수 q를 갖는 순환 그룹이라 가정한다. 겹선형 쌍함수는 $e : \mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$ 의 형태로 주어지고 다음과 같은 성질들을 만족한다.

1. **겹선형(Bilinearity)** : $\mathbf{G}_1$에 속하는 모든 P, Q, R에 대해 $e(P+Q, R) = e(P, R)e(Q, R)$이고 $e(P, Q+R) = e(P, Q)e(P, R)$이다.
2. **비 퇴화성(Non-degeneracy)** : $e(P, Q) \neq 1$인 P, Q가 $\mathbf{G}_1$에 존재한다.

3. **계산 가능성(Computability)** : $\mathbf{G}_1$에 속하는 임의의 P, Q에 대해 $e(P, Q)$를 계산하는 효율적인 알고리즘이 존재한다.

정의 3. 그룹 **G**의 생성자 P와 세 원소로 구성된 순서쌍 (aP, bP, cP)가 주어졌을 때, Diffie-Hellman 결정 문제(Decisional Diffie-Hellman problem, DDHP)는 $c = ab$인지 아닌지를 결정하는 문제이다.

정의 4. 그룹 **G**의 생성자 P와 두 원소로 구성된 순서쌍 (aP, bP)가 주어졌을 때, Diffie-Hellman 계산 문제(Computational Diffie-Hellman problem, CDHP)는 abP를 계산하는 문제이다.

정의 5. 만일 그룹 **G**가 DDHP는 polynomial time에 해결되고 CDHP는 그렇지 않다면 그룹 **G**를 Gap Diffie-Hellman group(GDH)이라 정의한다.

본 논문에서는 그룹 $\mathbf{G}_1$이 Gap Diffie-Hellman group임을 가정한다.

3. 효율적인 ID기반 환 서명(Efficient ID-based ring signature)[14]구성

$\mathbf{G}_1$, $\mathbf{G}_2$, e에 대한 정의는 2.2절에 소개된 것과 같다. 두 개의 단 방향 해쉬함수(one-way hash function) $H()$, $H_0()$를 갖고, $H : \{0, 1\}^* \rightarrow \mathbf{G}_1$, $H_0 : \{0, 1\}^* \rightarrow \mathbf{Z}_q^*$이다.

- **사전설정(Setup)** : PKG는 $\mathbf{Z}_q^*$상에서 임의로 x를 선택한다. 이것을 주 비밀키(master secret key)로 갖고 $P_{pub} = xP$를 그에 대응하는 공개키(public key)로 갖는다. 시스템 전체의 공개 파라메터(system parameter)는 $\{\mathbf{G}_1, \mathbf{G}_2, e, q, P, P_{pub}, H, H_0\}$가 된다

- **키 생성(Key generation)** : 식별자 $ID \in \{0, 1\}^*$를 갖는 사용자는 자신의 ID를 PKG에 보낸다. PKG는 $Q_{ID} = H(ID) \in \mathbf{G}_1$으로 계산하여 해당 사용자의 공개키로 결정하고, 그에 대응하는 비밀키는 $S_{ID} = xQ_{ID}$로 계산한다. PKG는 S_{ID}를 안전한 채널을 통하여 해당 사용자에게 전송한다.

- **서명 생성(Signature generation)** : L을 n명의 사용자의 식별자의 집합이라 하고($L = \{ID_1, ID_2, \cdots, ID_n\}$), 실제 서명자의 식별자를 ID_s라 하자. 서명자는 환을 대신하여 임의의 메시지 m에 서명하기 위해서 다음과 같은 과정을 거친다.

  1. $\mathbf{G}_1$상에서 무작위로 U_i를 선택하고 $h_i = H_0(m \| L \| U_i)$를 계산한다. 여기서 i는 $i \in \{1, 2, \cdots, n\}$, $i \neq s$이다.
  2. $\mathbf{Z}_q^*$상에서 무작위로 r_s'을 선택하고 $U_s = r_s' Q_{IDs} - \sum_{i \neq s}\{U_i + h_i Q_{IDi}\}$를 계산한다.
  3. $h_s = H_0(m \| L \| U_s)$와 $V = (h_s + r_s')S_{IDs}$를 계산한다.
  4. m에 대한 서명으로 $\sigma = \{\cup_i\{U_i\}, V\}$를 출력한다.

- **서명 검증(Signature verification)** : 임의의 검증자는 메시지 m과 서명 σ, 식별자의 집합 L을 가지고 다음과 같은 과정을 거쳐 서명을 검증한다.

  1. 모든 $i \in \{1, 2, \cdots, n\}$에 대해 $h_i = H_0(m \| L \| U_i)$를 계산한다.
  2. $e(P_{pub}, \sum_i(U_i + h_i Q_{IDi})) = e(P, V)$인지 확인한다.
  3. 만일 2의 등식이 성립한다면, 수락(accept)하고 성립하지 않으면 거절(reject)한다.

4. 서명자 검증 가능한 ID기반 환 서명(Signer verifiable ID-based ring signature)

본 논문에서는 Chow 외 2인[14]이 제안한 ID기반 환 서명을 바탕으로 하여 전환 가능성(convertibility) 성질을 갖는 새로운 방식을 제안한다. 기본 용어의

정의와 사전설정, 키 생성 알고리즘은 위에 제시된 방법과 같다.

- **서명 생성(Signature generation)** : 위와 마찬가지로 실제 서명자의 식별자를 ID_s라 하고 n명의 사용자의 식별자(identity)의 집합을 L이라 한다. 서명자는 임의의 메시지 m에 서명하기 위해서 다음과 같은 과정을 거친다

  1. $\mathbf{G}_1$상에서 무작위로 U_i를 선택하고 $h_i = H_0(m \| L \| U_i)$를 계산한다. 여기서 i는 $i \in \{1, 2, \cdots, n\}$, $i \neq s$이다.

  2. $\mathbf{Z}_q^*$상에서 r_s'을 무작위로 선택하고 $\mathbf{G}_1$상에서 r을 무작위로 선택하여 다음을 계산한다.

  $t = H_0(U_1 \| U_2 \| \cdots \| U_{s-1} \| U_{s+1} \| \cdots \| U_n \| r)$

  $k = H_0(r_s' \| t)$

  $U_s = kQ_{IDs} - \sum_{i \neq s}\{U_i + h_iQ_{IDi}\}$

  $h_s = H_0(m \| L \| U_s)$

  $V = (h_s + k)S_{IDs}$

  3. m에 대한 서명으로 $\sigma = \{\cup_i\{U_i\}, V, t\}$를 출력한다.

- **서명 검증(Signature verification)** : 임의의 검증자는 메시지 m과 서명 σ, 식별자의 집합 L을 가지고 다음과 같은 과정을 거쳐 서명을 검증한다.

  1. 모든 $i \in \{1, 2, \cdots, n\}$에 대해 $h_i = H_0(m \| L \| U_i)$를 계산한다.

  2. $e(P_{pub}, \sum_i(U_i + h_iQ_{IDi})) = e(P, V)$인지 확인한다.

  3. 만일 2의 등식이 성립한다면, 수락(accept)하고 성립하지 않으면 거절(reject)한다.

- **전환(Convert)** : 실제 서명자 ID_s가 자신의 식별자를 공개해야 할 필요가 있는 경우, $U_1 \| U_2 \| \cdots \| U_{s-1} \| U_{s+1} \| \cdots \| U_n \| r$ 을 공개한다.

- **전환 검증(Convert verification)** : 임의의 검증자는 $t = H_0(U_1 \| U_2 \| \cdots \| U_{s-1} \| U_{s+1} \| \cdots \| U_n \| r)$임을 확인하고 만일 이것이 맞다면 검증자는 식별자가 ID_s인 사용자가 실제 서명자임을 확신한다.

5. 보안 요구조건 분석

서명자 익명성 및 위조 불가능성(Signer ambiguity and unforgeability) : 본 논문에서 제안하고 있는 방식은 Chow 외 2인[14]이 제안한 서명방식에 기반을 두고 있고, 서명 생성과정에서 r값이 무작위로 선택되기 때문에 보안 증명과정에 차이가 없다. Chow 외 2인[14]의 방식은 이미 서명자 익명성 및 위조 불가능성의 두 가지 요구사항에 대해 안전하다고 증명이 되었기 때문에 본 논문에서 제안하고 있는 서명 방식 역시 위 두 가지 요구사항을 만족한다.

서명하지 않은 사용자에 대한 전환 불가능성(Unconvertibility against nonsigner) : 임의의 공격자가 전환 검증 과정을 만족시키기 위해서는 $t = H_0(U_1 \| U_2 \| \cdots \| U_{s-1} \| U_{s+1} \| \cdots \| U_n \| r)$를 만족하는 r값을 선택할 수 있어야 한다. H_0는 단 방향 해쉬 함수(one-way hash function)이기 때문에 t값에서 r값을 알아내기는 힘들고 r값은 $\mathbf{G}_1$상에서 무작위로 선택된 수이므로 공격자가 임의로 선택한 값이 r값과 같아질 수 있는 확률은 무시할 수 있다.

6. 결론

환 서명 방식의 가장 중요한 성질 가운데 하나는 실제 서명자가 누구인지 알 수 없다는 것이다. 하지만 위의 예에서도 알 수 있듯이 응용에 따라 실제 서명자가 누구인지 아는 것이 중요한 상황이 발생하게 되고 기존의 환 서명 방식으로는 그것을 알아낼 수가 없다. 그래서 본 논문에서는 전환 가능한 환 서명 방식을 이용하여 실제 서명자가 자신을 포함하여 n명으로 구성된 환을 만들고, 그 환을 대신하여 메시지에 대한 서명을 만든 후, 필요에 따라 자신의

식별자를 노출할 수 있는 서명을 제안하였다. 실제 서명자가 특정 정보를 노출하기 전에는 검증자가 실제 서명자가 누구인지 알 수 없고 실제 서명자가 원하는 경우에만 그의 존재를 알 수 있다. 안전성에 대한 증명은 Chow 외 2인[14]의 방식과 유사하다.

7. 참고 문헌

[1] Rivest, R.L., Shamir, A., and Tauman:, Y.: 'How to leak a secret'. Proc. Advances in Cryptology, ASIACRYPT'01, 2001, (Lect. Notes Comput. Sci., 2248), pp. 552-565

[2] Abe, M., Ohkubo, M., and Suzuki, K.: '1-out-of-n signatures from a variety of keys'. Proc. Advances in Cryptology-AISACRYPT'02, 2002, (Lect. Notes Comput. Sci., 2501), pp. 415-432

[3] Zhang, F., and Kim:, K.: 'Id-based blind signature and ring signature from pairings'. Proc. Advances in Cryptology-ASIACRYPT'02, 2002, (Lect. Notes Comput. Sci., 2501), pp. 533-547

[4] Boneh, D., Gentry, C., Lynn, B., and Shacham:, H.: 'Aggregate and verifiably encrypted signatures from bilinear maps'. Proc. Advances in Cryptology-EUROCRYPT'03, 2003, (Lect. Notes Comput. Sci., 2656), pp. 416-432

[5] Bresson, E., Stern, J., and Szydlo:, M.: 'Threshold ring signatures and applications to ad-hoc groups'. Proc. Advances in Cryptology-CRYPTO'02, 2002, (Lect. Notes Comput. Sci., 2442), pp. 465-480

[6] Kuwakado, H., and Tanaka:, H.: 'Threshold ring signature scheme based on the curve'. Proc. IEEE Int. Symp. on Information Theory, 2003, p. 139

[7] Boyar, J., Chaum, D., and Damgard:, I.: 'Convertible undeniable signatures'. Proc. Advances in Cryptology-CRYPTO'90, 1991, (Lect. Notes Comput. Sci., 537), pp. 189-205

[8] Kim, S.J., Park, S.J., and Won:, D.H.: 'Convertible group signature'. Proc. Advances in Cryptology-ASIACRYPT'96, 1996, (Lect. Notes Comput. Sci., 1163), pp. 311-321

[9] Damgard, I., and Pedersen:, T.: 'New convertible group signature schemes'. Proc. Advances in Cryptology-EUROCRYPT'96, 1996, (Lect. Notes Comput. Sci., 1070), pp. 372-386

[10] Araki, S., Uehara, S., and Imamura:, K.: 'The limited verifier signature and its application', IEICE Trans. Fundam., 1999, E82-A, (1), pp. 63-68

[11] Lyuu, Y.-D., and Wu:, M.-L.: 'Convertible group undeniable signatures'. Proc. ICISC, 2002, (Lect. Notes Comput. Sci., 2587), pp. 48-61

[12] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 84, LNCS 196, Springer-Verlag, 1984, pp. 47-53

[13] Lee, K., -C., Wen, H., -A. and Hwang, T. : 'Convertible ring signature'. IEE Proc. - Commun., Vol 152, No. 4, August 2005

[14] Sherman S. M. Chow, Siu-Ming Yiu, and Lucas C. K. Hui : 'Efficient Identity Based Ring Signature' Proc. ACNS 2005, (Lect. Notes Comput. Sci., 3531), pp. 499-512