지정된 수신자를 갖는 환 서명

이지선° 장직현
서강대학교 컴퓨터학과
jslee702°@sogang.ac.kr, jchang@alglab.sogang.ac.kr

Ring Signatures with a Designated Receiver

Ji-Seon Lee° Jik Hyun Chang
Dept. Computer Science, Sogang University

요 약

환 서명(ring signatures)은 서명자가 자신을 포함한 환(ring)이라고 하는 그룹을 형성하여 서명을 생성하는 방식으로 검증자는 환 소속원 중에서 누가 서명했는지는 알 수가 없고, 서명이 환에 속한 소속원으로부터 왔다는 것만을 알 수 있다. 일반적인 환 서명은 서명자의 비밀키와 다른 환 소속원들의 공개키를 이용하여 서명을 생성하고, 환 소속원들 모두의 공개키를 이용하여 누구나 검증할 수 있다.

본 논문에서는 지정된 수신자만이 검증할 수 있도록 하는 환 서명(ring signatures with a designated receiver) 방식을 제안한다. 또한 환 서명이 기본적으로 서명자 익명성을 보장하기 위해 제안된 서명 방식이므로 그에 부합하는 요구 조건을 분석한다.

1. 서 론

환 서명(ring signatures)[1]은 서명자가 자신을 포함한 환(ring)이라고 불리는 그룹을 형성하여 환을 대신해서 메시지에 서명하는 방식으로, 수신자는 그 서명이 환 소속원 중에서 누구로부터 왔는지 알 수 없다. 즉, 환 소속원 중의 한 명에 의해 서명이 생성되었다는 것은 알 수 있지만 실제 서명자가 누구인지는 서명자 외에는 아무도 알 수 없다. 환 서명에서는 관리자를 따로 두지 않고 서명자가 자신을 포함한 n명의 서명 가능한 소속원들로 구성한 환에서 서명자 자신의 비밀키와 다른 $n-1$ 소속원들의 공개키를 이용하여 서명을 생성한다. 서명자는 생성한 서명을 환 소속원들의 공개키 리스트, 메시지와 함께 수신자에게 보내고, 수신자는 n명의 공개키를 이용하여 서명을 검증한다. 환을 구성하는 누구라도 자신의 비밀키를 이용하여 서명을 생성할 수 있고, 환 소속원들의 공개키 리스트를 받은 누구라도 서명을 검증할 수 있지만, 실제 서명자가 누구인지는 본인 외에는 알 수가 없다. 오직 실제 서명자가 자신을 밝혀야만 서명의 출처를 알 수 있다. 환 서명이라는 용어는 R. Rivest외 2인[1]에 의해 처음으로 사용되었지만, 이미 R. Cramer외 2인[2]에 의해 환 서명 개념은 제안되었다. M. Abe외 2인[3]은 R. Cramer의 위트니스 증명 프로토콜에 기초하여 다양한 키를 갖는 환 서명을 제안하였다. 최근에는 랜덤 오라클 모델에서 안전한 환 서명(provably secure ring signature under the random oracle model)이 Herranz와 Saez[4]에 의해 제안되었다.

지정된 수신자만이 검증할 수 있는 서명 방식은 이전에 김승주외 2인[5]에 의해서 수신자 지정 서명(nominative signatures)이란 명칭으로 제안되었다. 그들이 제안한 수신자 지정 서명 방식에서는 두 가지의 요구 조건을 갖는다. 하나는 지정된 수신자만이 서명자의 서명을 확인할 수 있어야 하는 것이고, 다른 하나는 지정된 수신자만이 필요시에 제3자에게 서명이 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있어야 하는 것이다. 이 두 가지 요구 조건은 지정된 수신자 외에는 그 누구도 서명 검증과 서명 전환이 불가능하도록 한다는 것으로 심지어 서명자조차도 자신이 서명을 생성한 후에 검증할 수 없어야 한다. 이러한 수신자 지정 서명의 목적은 서명의 남용을 서명자가 아닌 수신자가 통제할 수 있도록 하기 위함이다. 즉, 수신자의 프라이버시가 중요한 경우에 이용될 수 있는 서명 방식이다. 하지만 논문 [5]에서 제안된 서명 방식이 지정된 수신자 뿐만 아니라 서명자에 의해서도 검증 가능하고, 제3자가 증명할 수 있는 서명으로 전환 가능하다는 것을 Z. Huang과 Y. Wang[6]은 지적하고 오직 수신자만이 서명 검증과 전환이 가능하도록 만든 새로운 전환식 수신자 지정 서명(convertible nominative signatures)을 제안하였다. 하지만, 이후 W. Susilo와 Y. Mu[7], L. Guo외 2인[8] 등에 의해 전환식 수신자 서명의 보안 요구 조건에 대해 여전히 논의되고 있다.

본 논문에서는 처음으로 지정된 수신자를 갖는 환 서명을 제안한다. 지정된 수신자를 갖는 환 서명은 서명자가 $n-1$명을 선택하고 거기에 자신을 포함한 n명의 환

을 형성하여 자신이 지정한 수신자만이 검증할 수 있도록 서명을 생성하는 방식이다. 제안하는 서명 방식은 기본적으로 환 서명에 기초한 서명 방식이므로 서명자의 익명성을 보장해야 한다. 따라서 수신자 지정 서명(nominative signatures)[5]과는 다른 요구 조건을 필요로 한다. 이 논문에서 제안하는 지정된 수신자를 갖는 환 서명은 서명자의 익명성을 보장해야 할 뿐 아니라 제3자가 자신이 환 소속원인 것처럼 위장하여 서명을 생성할 수 없어야 하며 실제 서명자가 아닌 환 소속원이 실제 서명자인 것처럼 위장해서 서명을 생성할 수도 없어야 한다. 지정된 수신자는 자신만이 검증한 서명을 필요시에 누구나 검증할 수 있는 서명으로 전환할 수 있어야 하고, 실제 서명자는 필요시에 자신이 실제 서명자임을 증명할 수 있어야 한다. 이에 대해서는 3장에서 자세히 논의한다.

본 논문은 모두 6개의 장으로 구성된다. 2장에서는 기존에 제안된 수신자 지정 서명[5]과 환 서명에 기초가 되는 위트니스 구별불가 서명 방식(witness indistinguishable signatures)[3]을 기술하고 3장에서는 제안하는 지정된 수신자를 갖는 환 서명이 만족해야 하는 요구 조건을 분석한다. 4장에서는 지정된 수신자를 갖는 환 서명을 기술하고, 5장에서는 4장에서 제안한 서명 방식이 3장의 요구 조건을 만족함을 보이며 6장에서는 본 논문의 결론을 정리한다.

2. 기존의 서명 방식들

본 장에서는 김승주외 3인에 의해 제안된 영지식 수신자 지정 서명 방식[5]과 D. Cramer외 2인에 의해 제안된 위트니스 증명 프로토콜[2]에 바탕을 둔 위트니스 구별 불가 서명 방식[3]에 대해 살펴본다.

2.1 영지식 수신자 지정 서명 (Zero-knowledge nominative signatures)

서명자 A가 지정 수신자 B만이 확인할 수 있도록 메시지 m을 서명하여 보내고자 하는 경우 다음과 같이 서명을 생성할 수 있다.

p와 q를 큰 소수라고 하고, $< g >$는 mod p상에서 위수가 q인 임의의 수라고 하자. 서명자 A의 비밀키는 $x_A \in Z_q^*$이고 그에 대응하는 공개키는 $y_A = g^{x_A} \bmod p$이다. 마찬가지로 지정된 수신자 B는 비밀키 x_B와 그에 대응하는 공개키 y_B를 갖는다. H는 공개된 해쉬 함수이다.

(1) 서명 생성

서명자는 다음과 같은 과정을 거쳐 메시지 m에 대한 서명 (y_B, t, T, s)를 생성한다.

① A는 랜덤수 $r, R \in Z_q^*$를 선택하여 t와 T를 다음과 같이 계산한다.

- $t = g^{R-r} \bmod p$
- $T = y_B^R \bmod p$

② t와 T를 이용하여 다음의 e와 s를 구한다.

- $e = H(y_B, t, T, m)$
- $s = r - x_A e \bmod q$

③ 메시지 m에 대한 서명 (y_B, t, T, s)을 지정 수신자 B에게 보낸다.

(2) 서명 검증

B는 다음과 같이 $e = H(y_B, t, T, m)$를 구하고 다음의 등식이 만족하는지 확인한다.

$$T = (t g^s y_A^e)^{x_B} (\bmod p)$$

(3) 제3자에 대한 영지식 대화형 증명

B는 제3자에게 자신이 지정된 수신자임을 증명하기 위해 자신의 비밀키인 이산대수 x_B를 알고 있다는 사실을 다음의 영지식 프로토콜을 이용하여 증명한다.

① 제3자 C는 랜덤수 $a, b \in Z_q^*$를 선택하여 ch를 계산하여 지정된 수신자 B에게 전송한다.

$$ch = (g^s y_A^e t)^a \cdot g^b \bmod p$$

② B는 $w \in Z_q^*$를 선택해서 h_1, h_2를 계산하여 C에게 보낸다.

$$h_1 = ch \cdot g^w mod p$$

$$h_2 = h_1^{x_B} \bmod p$$

③ C는 단계 ①에서 사용한 a, b를 B에게 전송한다.

④ B는 다음 등식이 만족하면 w를 전송하고, 만족하지 않는다면 프로토콜을 중단한다.

$$ch = (g^s y_A^e t)^a \cdot g^b \bmod p$$

⑤ C는 단계 ②에서 받은 h_1, h_2와 ④에서 받은 w를 이용하여 다음 등식이 만족되는지 검사한다.

$$h_1 = (g^s y_A^e t)^a \cdot g^{b+w} \bmod p$$

$$h_2 = T^a \cdot y_B^{b+w} \bmod p$$

2.2 위트니스 구별불가 서명 (Witness indistinguishable signatures)

위트니스 구별불가 서명 방식은 1994년에 R. Cramer외 2인[2]이 제안한 지식 증명 프로토콜(proof of knowledge protocol)을 바탕으로 M. Abe외 2인[3]이 이산 대수 문제에 기초하여 정리한 서명 방식이다. 이 서명 방식에서는 증명자(prover) A가 검증자(verifier) B에게 어떤 비밀값을 알고 있다는 것을 비밀값을 알리지 않고 증명하는 방법을 이용한다. 실제로 M. Abe외 2인은 이 서명 방식을 바탕으로 환 서명을 제안하였다. 이 절에서는 M. Abe외 2인에 의해 정리된 지식 증명 프로토콜을 바탕으로 한 서명을 살펴본다.

p_i, q_i를 큰 소수라고 하자. $< g_i >$는 mod p_i상에서 위수가 q_i인 임의의 수라고 하자. 모두 n명이 있을 때 x_i는 비밀키이고 y_i는 공개키이다. 즉, $y_i = g_i^{x_i} \bmod p_i$ 이다. H는 공개된 해쉬 함수이고, L은 환 소속원들의 공개키 리스트이다. 서명자 A_u는 비밀키 x_u를 이용하여 다음과 같이 서명을 생성한다.

(1) 서명 생성

① $i = 1, ..., n, i \neq u$, 인 i에 대하여 $s_i, c_i \in Z_{q_i}$를 선택하여 다음과 같이 z_i를 계산한다.

$$z_i = g_i^{s_i} y_i^{c_i} \bmod p_i$$

② r_u를 Z_{q_u}로부터 선택하여 다음을 계산한다.

$$z_u = g_u^{r_u} \bmod p_u$$
$$c = H(L, m, z_0, ..., z_{n-1})$$
$$c_u = c \oplus (c_1 \oplus \cdots \oplus c_{u-1} \oplus c_{u+1} \oplus \cdots \oplus c_n)$$
$$s_u = r_u - c_u \cdot x_u \bmod q_u$$

③ 서명 $\sigma = (L, m, c_1, s_1, \cdots, c_n, s_n)$를 B에게 보낸다.

(2) 서명 검증 과정

서명 수신자는 다음이 만족되면 옳은 서명이라고 간주한다.

$$c_1 \oplus \cdots \oplus c_n = H(L, m, g_1^{s_1} y_1^{c_1} \bmod p_1, \cdots, g_n^{s_n} y_n^{c_n} \bmod p_n)$$

이 서명 방식에서 검증자가 알 수 있는 것은 서명이 n명 중 한 명에 의해서 만들어졌다는 것뿐이다. 즉 서명자는 n개의 공개키 중에서 하나에 대응하는 자신의 비밀키를 위트니스(witness)로 하여 비대화식 증명(non-interactive proof)을 한 것이다.

3. 지정된 수신자를 갖는 환 서명 요구 조건

본 논문에서 제안하는 지정된 수신자를 갖는 환 서명 방식은 환 서명에 기초하므로 서명자 익명성(signer anonymity)이 중요한 성질이다. 이 외에도 위조 불가능성(unforgeability), 전환 가능성(convertibility), 지정된 수신자 증명 가능성(designated receiver verifiability), 서명자 증명 가능성(signer verifiability)이 중요한 요구 조건이다.

(1) 서명자 익명성 (signer anonymity)

서명이 환을 구성하는 소속원들 중에서 누군가에 의해 생성되었다는 것은 알 수 있지만, 실제 서명자를 제외하고는 그 누구도 실제 서명자를 알 수 없도록 해야 한다.

(2) 위조 불가능성 (unforgeability)

환 서명은 환을 구성하는 소속원에 의해서만 생성 가능해야 한다. 환에 소속되지 않은 그 누구도 서명을 생성할 수 없어야 한다. 즉, B를 포함하여 그 누구도 서명을 위조할 수 없어야 한다. 또한 환 소속원은 누구라도 서명을 생성할 수 있지만 실제 서명자가 아닌 환 소속원이 실제 서명자인 것처럼 속여서 서명을 생성할 수는 없다. 따라서 실제 서명자 A_u에 의해 생성된 환 서명은 오로지 A_u에 의해서만 생성될 수 있고 그 누구도 A_u가 실제 서명자라는 것을 알 수 없다.

(3) 전환 가능성 (convertibility)

필요한 경우에 지정된 수신자는 자신이 받은 서명을 제3자가 검증할 수 있도록 일반 환 서명으로 전환할 수 있어야 한다.

(4) 지정된 수신자 증명 가능성 (designated receiver verifiability)

지정된 수신자는 생성된 서명이 자신에게 발행된 정당한 서명임을 증명할 수 있어야 한다.

(5) 서명자 증명 가능성 (signer verifiability)

만일 실제 서명자가 자신을 밝혀야 할 필요가 있으면 전송된 서명이 자신이 생성한 서명임을 증명할 수 있어야 한다.

다음 장에서는 지정된 수신자를 갖는 환 서명을 제안하고, 제안한 방식이 위의 다섯 가지의 요구 조건에 부합된다는 것을 증명한다.

4. 지정된 수신자를 갖는 환 서명

M. Abe외 2인[3]은 위트니스 구별불가 서명 방식에서 모든 환 소속원이 다른 p_i와 q_i를 갖도록 했는데, 여기에서는 공통된 p와 q 값을 이용한다. 이전과 같이 환을 구성하는 멤버는 모두 n명이라 가정하고 각 멤버 A_i, $1 \leq i \leq n$, 는 각자 비밀키 x_i와 공개키 $y_i = g_i^{x_i} \bmod p$를 갖는다. 지정된 수신자 B는 비밀키 x_B와 그에 대응하는 공개키 $y_B = g^{x_B} \bmod p$를 갖는다.

4.1 서명 생성 과정

서명자 A_u는 다음과 같은 과정을 거쳐 서명을 생성한다.

(1) 랜덤수 $k \in Z_q^*$를 선택하여 r과 t 값을 구한다.

- $r = g^k \bmod p$
- $t = y_B^k \bmod p$

(2) 랜덤수 $w \in Z_q^*$를 선택하여 다음을 구한다.

- $c_{u+1} = H(L, m, y_B, r^w \bmod p)$

(3) $i = u+1, ..., n-1, n, 1, 2, ..., u-1$에 대해서 다음

을 반복한다.

- 랜덤수 $s_i \in Z_q^*$를 선택한다.
- c_{i+1}을 다음과 같이 구한다.

$$c_{i+1} = H(L, m, y_B, g^{s_i} y_i^{c_i r} \bmod p)$$

(4) 마지막으로 s_u를 계산하여 환을 구성한다.

- $s_u = kw - x_u c_u r \pmod q$

(5) 서명자 A_u는 서명 $\sigma = (L, m, y_B, c_1, s_1, s_2, \cdots, s_n, t)$를 지정된 수신자 B에게 보낸다.

4.2 지정된 수신자에 의한 서명 검증 과정

서명을 받은 수신자는 자신의 비밀키 x_B를 이용하여 다음과 같이 서명을 검증한다.

(1) 우선 B는 r 값을 구한다.

- $r = t^{x_B^{-1}} \bmod p$

(2) 구한 r 값을 이용하여 다음의 과정을 거쳐 서명을 검증한다.

- $2 \le i \le n$ 인 i에 대하여 다음을 구한다.

$$c_i = H(L, m, y_B, g^{s_{i-1}} y_i^{c_{i-1} r} \bmod p)$$

(3) 다음의 등식이 성립하는지 본다.

$$c_1 = H(L, m, y_B, g^{s_n} y_n^{c_n r} \bmod p)$$

등식이 성립하면 옳은 서명임을 검증할 수 있다.

4.3 서명 전환과 제3자 검증 과정

지정된 수신자 B가 서명이 실제로 환 소속원 중 한 명으로부터 왔다는 사실을 증명하기 위해 자신이 구한 r값과 서명을 공개한다. 즉 B는 다음과 같이 전환된 서명을 공개한다.

$$\sigma' = (\sigma, r) = ((L, m, y_B, c_1, s_1, s_2, \cdots, s_n, t), r)$$

여기서 r 값은 B만이 계산할 수 있다. 이렇게 전환된 서명을 받은 제3자는 그 누구라도 4.2 절의 (2)번과 (3)번 과정을 통하여 공개된 서명이 실제로 환 소속원로부터 왔다는 것을 검증할 수 있다.

4.4 수신자 증명 과정

지정된 수신자 B가 주어진 서명이 자신에게 왔다는 것을 증명하기 위해서, 즉 자신이 지정된 수신자임을 증명하기 위해서 제3자에게 자신의 비밀키 x_B를 알고 있다는 것을 D. Chaum이 제안한 영지식 부인방지 서명 방식(zero-knowledge undeniable signatres)[9]에서 이용되었던 서명 확인 프로토콜(confirmation protocol)로 다음과 같이 증명할 수 있다. 제3자는 C라고 명칭하고 전환된 서명 σ'을 가지고 있다.

(1) C는 두 개의 랜덤수 $a, b \in Z_q$를 선택하여 z 값을 계산하여 B에게 보낸다.

$$z = r^a g^b \bmod p$$

(2) B는 랜덤수 $d \in Z_q$을 선택하여 다음의 e, f 값을 C에게 보낸다

- $e = z^d \bmod p$
- $f = e^{x_B} \bmod p$

(3) C는 z 값을 생성할 때 사용했던 a, b를 B에게 보낸다.

(4) B는 받은 a, b를 이용해서 z 값이 맞는지 계산한다. 맞다면 (2)번에서 선택했던 d를 C에게 보낸다. C는 다음 두 개의 등식이 맞는지 확인한다. 맞다면 지정된 수신자는 B라는 것이 증명된다.

- $e = (r^a g^b)^d \bmod p$
- $f = (t^{a+d} y_B^{b+d}) \bmod p$

4.5 서명자 증명 과정

환 소속원 중 서명자가 자신이 실제 서명자임을 증명할 필요가 있을 때에는 다음과 같이 자신을 증명할 수 있다.

(1) 실제 서명자 S_u는 자신의 ID와 서명 생성 시에 임의로 선택했던 w를 공개한다.

(2) 제3자는 다음의 등식이 성립하는지 확인한다. 만일 성립하면 실제 서명자임이 증명된다.

$$r^w = g^{s_u} y_u^{c_u r} \bmod p$$

5. 요구 조건 분석

이 장에서는 4장에서 제안한 서명 방식이 3장에서 기술한 요구 조건들을 만족함을 증명한다.

(1) 서명자 익명성 (signer anonymity)

서명자의 익명성을 보장하기 위하여 지정된 수신자를 포함한 어느 제3자도 실제 서명자를 알아낼 확률이 $1/n$임을 보인다. n명의 소속원 중 A_u, $1 \le u \le n$, 를 임의의 서명자라고 할 때, A_u는 서명을 생성하기 위하여 랜덤수 r, w와 $n-1$개의 $s_i, i = u+1, \ldots, n, 1, \ldots, u-1$,를 선택해야 한다. 이렇게 랜덤수를 선택할 확률은 다음과 같다.

$$\frac{1}{(q-1)(q-1)(q-2)(q-n)}$$

이 확률은 모든 환 소속원들에게 똑같다. 따라서 서명자의 익명성은 보장된다.

(2) 위조 불가능성 (unforgeability)

다음과 같이 두 가지 경우로 나누어서 위조 불가능성을 얘기할 수 있다. 첫째로, 제안된 서명은 환 소속원 외에 누구도 생성할 수 없어야 한다. 둘째로, 실제 서명자가 아닌 임의의 환 소속원이 자신이 실제 서명자인 것처럼 위장할 수는 없어야 한다.

첫 번째의 경우를 가정하자. 즉, 환 소속원이 아닌 제3자가 서명을 위조하려고 한다고 하자. 제3자는 환 소속원 중의 한 명을 임의로 선택하여 4.1절의 서명 생성 과정을 따라서 서명을 생성하려고 할 것이다. 선택한 임의의 소속원을 A_u라고 하면, 마지막 단계에서 s_u를 계산하려고 할 때 A_u의 비밀키를 알아야 한다. 즉, 제3자는 적어도 환 소속원 중의 한 명의 비밀키를 알아야만 서명을 위조할 수 있다.

다음으로 실제 서명자가 아닌 환 소속원이 실제 서명자인 것처럼 위장하려고 한다고 가정하자. 실제 서명자를 A_u라고 하자. 실제 서명자가 아닌 환 소속원은 4.1절의 서명 생성 과정을 따라서 A_u의 서명을 만들려고 할 것이다. 하지만 마지막 단계에서 s_u를 계산하려고 할 때 위장하고자 하는 실제 서명자의 비밀키 x_u를 알아야 하므로 임의의 환 소속원이 실제 서명자인 것처럼 위조해서 서명을 생성하는 것은 불가능하다.

(3) 전환 가능성 (convertibility)

지정된 수신자 B는 제3자에게 자신이 받은 환 서명을 공개해야 할 필요가 있을 때 다음을 공개한다.

$$\sigma' = (\sigma, r) = ((L, m, y_B, c_1, s_1, s_2, \cdots, s_n, t), r)$$

B가 σ'을 공개하면 이를 가지고 B가 검증하는 것과 같은 과정을 이용해서 누구라도 서명을 검증할 수 있다. 즉, σ가 환 소속원으로부터 왔다는 것을 확인할 수 있다. 여기에서 r값은 B만이 계산 가능하므로 지정된 수신자 B만이 서명을 전환할 수 있다.

(4) 수신자 증명 가능성 (designated receiver verifiability)

지정된 수신자는 생성된 서명이 자신에게 발행된 정당한 서명임을 증명할 수 있어야 한다. 4.4절에서 수신자가 자신의 비밀키 x_B를 안다는 것을 영지식 증명 방법을 이용하여 증명하는 과정을 보였다. 따라서 수신자 증명은 가능하다.

(5) 서명자 증명 가능성 (signer verifiability)

만일 서명자가 자신이 실제 서명자임을 밝혀야 한다면, 서명자는 자신의 ID와 서명 생성 시에 선택했던 w를 공개한다. 서명자의 ID와 w를 받은 검증자는 다음의 등식이 만족하는지 본다.

$$r^w = g^{s_u} y_u^{c_v r} \bmod p$$

만일 등식이 만족되면, 실제 서명자는 공개키 y_u를 갖는 서명자이고, 만일 등식이 만족되지 않으면, 해당 ID를 가진 자는 실제 서명자가 아니다. 여기에서 w는 실제 서명자가 서명 생성 시에 임의로 선택하여 공개하지 않는 값이므로, 실제 서명자가 아닌 환 소속원이 자신이 마치 실제 서명자인 것처럼 증명하려면 이 값을 알아야 한다. 이 확률은 $1/q$ 이므로 실제 서명자가 아닌 환 소속원이 마치 자신이 실제 서명자인 것처럼 증명하기는 어렵다.

6. 결 론

본 논문에서는 서명자 자신은 익명으로 서명을 생성하고 지정된 수신자만이 검증할 수 있도록 하는 환 서명방식을 제안하였다. 서명을 생성하려고 하는 서명자가 자신을 포함한 n명의 환을 구성하여 서명을 생성하므로 환 외부에서는 n명 중 누가 실제 서명자인지 알 수 없다. 또한 환 소속원들도 실제 서명자 외에는 누가 서명을 생성했는지 알 수 없다. 지정된 수신자는 수신한 서명을 자신의 비밀키를 이용하여 검증함으로서 지정된 수신자만이 서명을 검증할 수 있다. 이러한 지정된 수신자를 갖는 환 서명은 환 소속원 중에 누군가가 비밀 정보에 대한 확신을 특정인에게만 주기 위해 만들어진 개념이기 때문에 지정된 수신자만이 비밀에 대한 확신을 가질 수 있다. 추가적으로 필요에 따라 수신자는 서명을 제3자가 검증할 수 있는 환 서명으로 전환 가능하며, 수신자가 자신에게 온 서명임을 제3자에게 증명할 수도 있고, 실제 서명자가 자신이 보낸 서명임을 증명할 수도 있다.

7. 참고 문헌

[1] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret", ASIACRYPT 2001, LNCS 2248, Springer-Verlag, pp. 552-565, 2001.

[2] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols", CRYPTO '94, LNCS 839, Springer-Verlag, pp.174-187, 1994.

[3] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n Signatures from a Variety of Keys", ASIACRYPT 2002, LNCS 2501, Springer-Verlag, pp. 415-432, 2002.

[4] J. Herranz and G. Saez, "Forking Lemmas for Ring Signature Schemes", INDOCRYPT 2003, LNCS 1403, Springer-Verlag, pp. 406-421, 2003.

[5] S. J. Kim, S. J. Park, and D. H. Won, "Zero Knowledge Nominative Signatures", Proc. of PragoCrypt '96, International Conference on the Theory and Applications of Cryptology, pp. 380-392, 1996.

[6] Z. Huang and Y. Wang, "Convertible Nominative Signatures", ACISP 2004, LNCS 3108, Springer-Verlag, pp. 348-357, 2004.

[7] W. Susilo and Y. Mu, "On the Security of Nominative Signatures", ACISP 2005, LNCS 3547, Springer-Verlag, pp.329-335, 2005.

[8] L. Guo, G. Wang, and D.S. Wong, "Further Discussions on the Security of a Nominative Signature Scheme", Cryptology ePrint archive, http://eprint.iacr.org/2006/007.

[9] D. Chaum, "Zero-Knowledge Undeniable Signatures", EUROCRYPT '90, LNCS 473, Springer-Verlag, pp. 458-464, 1991.