환 서명에 기반한 부인가능 인증 프로토콜

신기은*, 최형기*
*성균관대학교 정보통신공학부
e-mail : keshin@hit.skku.edu, hkchoi@ece.skku.ac.kr

Deniable Authentication with Verifiable Evidence based on Ring Signature

Ki-Eun Shin*, Hyoung-Kee Choi*
*School of Information and Communication Engineering, Sungkyunkwan University

요 약

부인가능 인증은 수신자가 전송된 메시지에 대한 출처를 확인할 수 있지만, 제 3 자에게는 전송된 메시지의 출처를 증명할 수 없는 인증 메커니즘이다. 이러한 부인가능 인증을 통하여 프라이버시 노출 가능한 전자투표와 전자상거래에서 메시지 전송에 대한 익명성을 보장할 수 있다. 본 논문에서는 그룹 멤버의 익명성을 보장하기 위한 환 서명을 이용하여 부인 가능한 서명을 제안함으로써 서명자의 프라이버시를 보호한다. 또한 추후에 서명에 대한 출처 확인이 필요할 경우, 서명자가 서명 생성을 위한 지식을 증명함으로써 서명에 대한 출처를 제 3 자에게 증명할 수 있다.

1. 서론

인증은 메시지의 출처나 사용자의 신뢰성에 대하여 확인하는 행동이다. 많은 보안 프로토콜에 인증이 적용되었으며, 다양한 표준이 제시되었다. 하지만, 특정 상황에서는 기본적인 인증 메커니즘만으로는 충분하지 않다. 즉, 전자 서명을 통하여 메시지 인증을 제공할 수 있지만, 전자서명을 통한 인증은 잠재적으로 프라이버시 위협에 노출될 수 있다.

예를 들어, 수신자는 메시지와 그에 해당하는 전자서명을 송신자의 허가 없이 제 3 자에게 전달할 수 있다. 메시지와 전자서명을 전달 받은 제 3 자는 전자서명을 검증할 수 있으며, 메시지의 출처를 확인할 수 있다. 이러한 전자서명의 고유한 특징으로 인하여 전자서명은 서명자의 메시지에 대한 서명을 부인할 수 없는 증거를 남긴다. 이로 인하여 프라이버시 침해 문제가 발생한다. 따라서, 최근 프라이버시 침해 문제를 해결하기 위하여 부인 가능한 인증 프로토콜이 제안되었다 [1][2][3][4]. 기존의 전통적인 인증 프로토콜과 비교하여 부인가능 인증은 다음과 같은 두 가지 특징을 갖는다:

1. 의도된 수신자만이 전송 받은 메시지의 출처를 확인할 수 있다.
2. 수신자는 전송 받은 메시지의 출처를 제 3 자에게 증명할 수 없다.

본 논문에서는 그룹 멤버의 익명성 제공을 위한 환 서명을 이용하여 부인가능 인증을 제안한다. 환 서명은 서명자가 임의의 그룹(환)을 구성하여 구성원의 공개키와 서명자의 비밀키를 이용하여 메시지에 서명함으로써 서명자의 신원을 감출 수 있다. 따라서, 환을 서명자와 검증자, 2 명으로 구성함으로써 부인 가능한 서명을 제안한다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 2 장에서는 부인가능 인증에 관한 기존 연구를 알아보고, 3 장에서는 제안한 프로토콜을 설명한다. 4 장에서는 제안한 프로토콜에 대한 보안을 분석하며, 5 장에서는 본 논문의 결론을 내린다.

2. 관련 연구

Dwork 외 2 명 [1]은 영지식 증명에 기반하여 부인가능 인증을 제안하였으며, Aumann 외 1 인 [2]은 소인수 분해문제에 기반하여 부인가능 인증을 제안하였다. 이 외에 다양한 부인가능 인증이 제안되었지만, 송신자가 전송하는 메시지 검증자를 알지 못하는 문제가 존재하였다. 최근에 Lein 외 1 인 [3]은 RSA 나 Elgamal 전자서명 방식의 existential forgery 를 이용하여 이메일을 위한 부인가능 인증 서비스를 제안하였다.

본 논문에서 이용한 환 서명은 Rivest 외 2 인 [4]에 의하여 최초로 제안되었다. 환 서명은 서명자의 익명성을 보장하기 위하여 그룹(환)을 구성하며, 구성원의 공개키와 서명자의 비밀키를 이용하여 메시지에 서명함으로써, 서명 검증자는 전송 받은 메시지가 그룹의 구성원으로부터 서명된 것은 확인 가능하지만 서명자를 확인할 수 없는 방식이다. 이러한 환 서명은 고발과 같이 익명성을 필요로 하는 상황에 쓰일 수 있다.

환 서명을 확장한 다양한 환 서명이 제안되었으며, 그 중 서명자가 자신이 환 서명의 실제 서명자라는 것을 증명할 수 있는 서명자 증명 가능한 환 서명(Convertible ring signature)이 제안되었다. 또한, Liu 외 2 명 [5]은 연결성 있는 환 서명(Linkable ring signature)을 제안하였다. 프라이버시 측면을 보완한 환 서명이

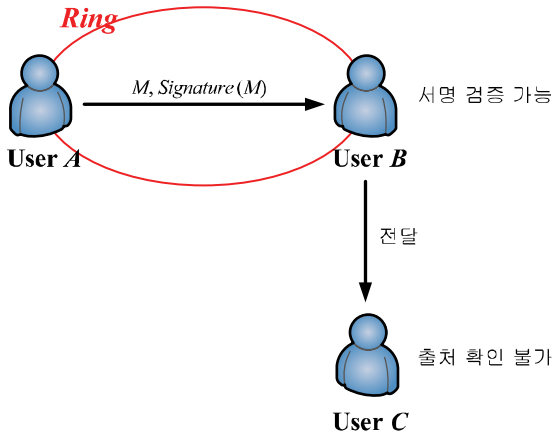

그림 1 부인가능 환 서명

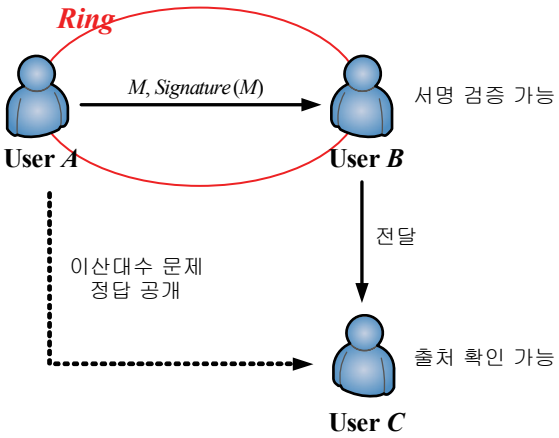

그림 2 서명의 출처 증명

정익래 외 2 명 [6]에 의해서 제안되었으며, 본 논문은 [6]에 기반하여 부인가능 인증 프로토콜을 제안한다.

3. 제안하는 프로토콜

환을 구성하여 메시지에 환 서명을 하는 경우, 수신자는 환 서명 검증 과정을 통하여 메시지의 무결성과 출처를 확인할 수 있다. 하지만, 환 서명이 갖는 고유의 특성으로 인하여, 제 3 자는 서명자의 신원을 확인할 수 없으며 출처가 환(서명자와 서명 검증자)인 것을 확인할 수 있다. 예를 들어, 서명자 A 는 자신의 프라이버시를 보호하기 위하여 서명 검증자 B 와 자신을 멤버로 하는 환을 구성하여 서명을 할 수 있다. B 도 자신과 A 를 멤버로 하여 환을 구성할 수 있으며 유효한 서명을 생성할 수 있기 때문에, 이 서명은 결국 부인 가능한 서명의 효과를 갖는다. 즉, 제 3 자는 B 가 전달한 A 의 환 서명 출처를 확인할 수 없다.

$\mathbb{G} = \langle g \rangle$를 소수인 위수 q 를 갖는 군(group)이라 하자. 이 군은 암호학 이론 분야의 중요한 역할을 하는 이산대수 문제를 내포한다. H는 $\{0, 1\}^* \rightarrow \mathbb{Z}_q$의 해쉬 함수이다. 서명자 A 와 서명 검증자 B는 비밀키와 공개키 쌍을 갖는다 (x_A, $y_A = g^{x_A}$ / x_B, $y_B = g^{x_B}$).

부인가능 환 서명 생성

A 는 메시지 m 을 B 에게 전송하기 위하여 다음과 같은 과정을 통하여 부인가능 환 서명을 생성한다.

1. $\mathbb{G}$에서 K_0 , $\mathbb{Z}_q$ 에서 a 를 임의로 선택한다. $K_1 = K_0^a$를 계산한다.
2. $\mathbb{Z}_q$ 에서 u, v 를 임의로 선택하여 $R_A = g^u$ 와 $R = K_0^v$를 계산한다.
3. $\mathbb{Z}_q$에서 c_B와 s_B를 임의로 선택하여 $R_B = g^{s_B} y_B^{c_B}$ 를 계산한다.
4. $c = H(K_0, K_1, m, R_A, R_B, R)$ 를 계산한다.
5. $c = c_A + c_B \bmod q$ 를 만족하는 c_A 를 계산하고, $s_A = u - x_A c_A \bmod q$ 와 $s = v - ac \bmod q$ 를 계산한다.
6. $\sigma(m) = (K_0, K_1, c_A, c_B, s_A, s_B, s)$ 이 서명이 된다.

서명 검증

메시지 m 에 대한 서명 $\sigma(m) = (K_0, K_1, c_A, c_B, s_A, s_B, s)$ 을 검증하기 위하여 B 는 다음 식을 만족하는지 확인한다.

$$c = H(K_0, K_1, m, g^{s_A} y_A^{c_A}, g^{s_B} y_B^{c_B}, K_0^s K_1^c) \qquad (1)$$

만약 식 (1)을 만족한다면, 서명의 출처를 A 로 확인할 수 있다. 만족하지 않는다면, 메시지 m 을 버린다.

4. 보안 분석

정리 1. 서명자 A 와 수신자 B 만이 해당 환 서명을 생성할 수 있다.

공격자가 A, B 를 환의 구성원으로 하여 메시지 m 에 대한 서명을 하기 위하여, s_A 를 계산해야만 한다. 하지만 s_A 를 얻기 위해서는 x_A (A 의 비밀키)를 알아야만 한다. 즉, 공격자가 환(A 와 B 를 구성원으로 하는 그룹) 서명을 하기 위해서는 A, B 의 비밀키 중 적어도 하나를 알아야만 한다.

정리 2. 서명 수신자 B 는 제 3 자에게 메시지 m 에 대한 서명 $\sigma(m)$ 의 출처가 A 인 것을 증명할 수 없다.

수신자 B 가 제 3 자인 C 에게 전송 받은 메시지 m 과 해당 서명 $\sigma(m)$ 을 전송할 경우, B 는 해당 메시지 m 의 출처가 A 인 것을 증명할 수 없다. B 는 자신과 A 의 환을 구성하여 메시지 m 에 대한 신뢰성 있는 환 서명 $\sigma'(m)$ 을 생성할 수 있으므로, C 는 B 가 증명하려는 메시지의 출처를 확인할 수 없다 (즉, A 와 B 모두 신뢰성 있는 환 서명을 생성할 수 있다). 그림 1 은 부인 가능 환 서명을 나타낸다.

정리 3. 서명의 출처를 실제 서명자는 증명할 수 있다.

서명자는 이후에 자신이 실제 서명자라는 것을 제 3 자에게 증명할 수 있다. 메시지 m 에 대한 서명 $\sigma(m)$ 의 출처를 실제 서명자가 이산대수 문제에 대한 해답을 보여줌으로써 증명할 수 있다.

즉, $K_1 = K_0^a \bmod q$ 를 만족하는 a 값을 보여줌으로

써 실제 환 서명자를 증명할 수 있다. 그림 2는 서명의 출처를 증명하는 과정이다.

5. 결론

전자 서명을 통하여 메시지에 대한 신뢰성과 출처를 제공할 수 있다. 하지만 전자 서명 고유의 특징으로 인하여, 서명 검증자뿐만 아니라 제 3 자까지 메시지의 출처를 확인할 수 있다. 따라서, 서명자의 프라이버시를 침해하는 결과가 발생하며, 이를 해결하기 위한 부인 가능한 서명에 대한 연구가 필요하다.

본 논문에서는 제 3 자의 서명 검증을 막기 위하여 환 서명을 이용하였다. 서명자와 서명자가 선택한 검증자를 환의 구성원으로 하여 환 서명을 함으로써, 검증자는 수신한 메시지에 대한 서명을 검증할 수 있다. 하지만, 환 서명의 특징으로 인하여 제 3 자는 서명에 대한 출처를 확인할 수 없다. 따라서, 전자서명에서 발생하는 프라이버시 노출 문제를 해결하였다.

또한, 본 논문에서는 서명자가 이산대수 문제 해법을 제시함으로써 이후에 서명자가 자신이 실제 서명자인 것을 증명할 수 있다.

참고문헌

[1] C. Dwork *et al*., “Concurrent Zero-knowledge” Proc. 30th ACM STOC 1998, pp. 409-418

[2] Y. Aumann *et al*., “Efficient Deniable Authentication of Long Message” Int. Conf. on Theoretical Computer Science in Honor of Professor Manuel Blum’s 60th birthday Apr. 1998

[3] Lein Harn *et al*., “Design of Fully Deniable Authentication Service for E-mail Applications” IEEE Communications Letters Mar. 2008, pp. 219-221

[4] Ronald L. Rivest *et al*., “How to Leak a Secret” Asiacrypt 2001, LNCS pp. 552-565

[5] Joseph K. Liu *et al*., “Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups” ACISP 2004, LNCS pp. 325-335

[6] Ik-rae Jeong *et al*., “Ring Signature with Weak Linkability and Its Applications” IEEE Trans. On Knowledge and Data Engineering Aug. 2008, pp. 1145-1148