수신자 지정 서명방식

김승주°, 박성준, 원동호
성균관대학교 정보공학과

A Directed Signature

Seung Joo Kim, Sung Jun Park and Dong Ho Won
Department of information Engineering
Sung Kyun Kwan University

요 약

본 논문에서는 undeniable signature의 상대적인 개념인 수신자 지정 서명 방식을 정의하고 이 조건들을 만족하는 수신자 지정 서명 방식 프로토콜을 제안한다.

1. 서 론

메세지 및 사용자에 대한 인증을 동시에 해결할 수 있는 디지틀 서명 기술은 각종 보안 서비스에서 필수 불가결한 도구로 사용된다. 특히 누구나 메세지의 출처와 메세지의 진위여부를 확인할 수 있는 자체 인증기능을 갖는 디지틀 서명은 대부분의 응용분야에서는 매우 유용하다.

그러나 개인적으로나 상업적으로 민감한 응용들에서는 이러한 자체인증은 필요 이상의 과다한 인증 기능(서명의 사본으로 누구나 인증 가능)을 제공함으로서 서명의 사본들이 악용될 수 있는 가능성을 높여주게 된다.

이러한 문제점을 해결하기 위한 서명방식중의 하나가 D.Chaum에 의해 제안된 undeniable signature이다. [1] [2] D.Chaum에 의해 제안된 undeniable signature은 서명자의 도움없이는 서명문을 확인할 수 없게 함으로써 서명자가 서명의 남용을 통제할 수 있는 특징을 가지고 있으며, 서명문의 진위를 확인해주는 confirmation protocol과 자신의 서명문을 부인하지 못하게 하는 disavowal protocol로 구성된다.

한편 임채훈 등은 undeniable signature의 상대적인 개념인 지정된 수신자만이 서명을 인증할 수 있고 필요시 제3자에게 그 서명이 자신에게 발행된 유효한 서명임을 증명할 수 있게 함으로써 수신자 자신이 서명의 남용을 통제할 수 있는 수신자 지정 서명방식(directed signature) 개념을 소개하였으며, 수신자 지정 서명 방식 프로토콜들을 제안하였다. [3]

그러나 임채훈등의 논문에서는 수신자 지정 서명 방식의 요구 조건을 명확히 제시하고 있지 않으며, 제안한 프로토콜들도 그들이 제시한 상황 - 예를 들어, 서명자가 지정 수신자 B에게 서명한 사실을 부인하기 위해 서명자와 지정 수신자 B만이 계산할 수 있는 K를 제3자에게 은밀히 누출시키는 경우. - 을 해결하지 못했다. [4]

본 논문에서는 수신자 지정 서명방식의 정확한 개념과 요구조건등에 대해서 정의하고, 이 조건들을 만족하는 수신자 지정 서명 방식 프로토콜을 제안한다.

2. 수신자 지정 서명방식 (directed signature)

수신자 지정 서명방식이란 지정된 수신자만이 서명을 인증할 수 있고 필요시 제3자에게 그 서명이 자신에게 발행된 유효한 서명임을 증명할 수 있게 함으로써 자신에게 발행된 서명의 남용을 수신자 자신이 통제할 수 있는 서명방식을 말한다.

이는 서론에서도 언급했듯이 서명된 메세지가 수신자의 이해관계나 프라이버시에 관련된 내용인 경우 서명의 수신자가 서명의 사본들이 불법적으로 사용되는 것을 통제할 수 있도록 하자는 것이다.

예를 들어, 세금고지서나 건강기록카드 등에 사용되는 서명은 해당 수신자만이 이를 확인할 수 있으면 충분하며 필요시에는 그 문서가 자신에게 발행된 것임을 증명할 수 있도록 하여 일반적인 서명을 사용했을 때 발생할 수 있는 악용들을 방지할 수 있다는 장점이 있다.

이를 위하여 서명자는 서명을 생성할 때 특정 수신자의 공개키를 결부시킴으로써 그 공개키에 대응하는 비밀키의 소유자만이 서명을 인증할 수 있도록 하고 또한 지정 수신자는 자신이 그 서명을 제시해야 할 필요가 있을 때에는 제3자에게 그 정당성을 증명할 수 있도록 한다.

위와 같은 수신자 지정 서명방식의 특성을 가지려면 다음의 2가지 요구 조건을 만족해야 한다.

[가정] 서명자 A가 지정된 수신자 B에게 서명문 S를 보낸다.

조건1) 지정된 수신자 B만이 서명문 S를 인증할 수 있다.
(서명자 A조차도 서명문 S를 인증할 수 없다.)

⇒ 이 조건이 만족되어야지만 '수신자 지정'이 된다.

조건2) 지정된 수신자 B만이 필요시에 제3자에게 그 서명이 자신에게 발행된 유효한 서명임을 증명할 수 있다.
(서명자 A조차도 제3자에게 서명문 S가 A가 B에게 발행한 유효한 서명임을 증명할 수 없다.)

⇒ 이 조건을 만족하게 함으로써 자신에게 발행된 서명의 남용을 수신자 자신이 통제할 수 있게 한다.
(서명자 A도 제3자에게 서명문 S가 A가 B에게 발행한 유효한 서명임을 증명할 수 있다면, 수신자 B 자신이 서명의 남용을 통제한다고 볼 수 없다.)

3. 수신자 지정 서명 방식 프로토콜

이 장에서는 2절에서 제시된 수신자 지정 서명 방식의 2가지 요구조건을 만족하는 수신자 지정 서명 방식 프로토콜을 제안한다.

서명자는 서명을 생성할 때 특정 수신자의 공개키를 결부시킴으로써 그 공개키에 대응하는 비밀키의 소유자만이 서명을 인증할 수 있도록 하고 또한 지정 수신자는 자신이 그 서명을 제시해야 할 필요가 있을 때에는 제3자에게 그 정당성을 증명할 수 있도록 한다.

Schnorr의 서명을 변형하면 이와 같은 수신자 지정 서명 방식을 구성할 수 있다. 서명자 A가 지정 수신자 B만이 확인할 수 있도록 메세지 m을 서명하여 보내고자 하는 경우 다음과 같이 서명을 생성할 수 있다. (그림 1. 참조)

[수신자 지정 서명 생성 scheme]

① 서명자 A는 랜덤수 $k \in [1, q)$를 선택하여 $r \equiv y_B^k \bmod p$ 를 계산한다.

② $e = h(r, m)$를 계산하고 $s \equiv k + x_A e \bmod q$ 를 구하면 (r, s)가 메세지 m에 대한 서명이 된다.

③ 이를 받은 지정 수신자 B는 $h(r, m) = e$ 와 $(g^s y_A^{-e})^{x_B} \equiv r \bmod p$ 를 만족하는지 검사함으로써 메세지 m에 대한 서명을 확인할 수 있다.

서 명 자 A		수 신 자 B
① $x_A : 0 < x_A < q$, 비밀키 ② $y_A : y_A \equiv g^{x_A} \bmod p$	p, q, g, h 공개키 { y_A } { y_B }	① $x_B : 0 < x_B < q$, 비밀키 ② $y_B : y_B \equiv g^{x_B} \bmod p$
① random $k \in [1, q)$ ② $r \equiv y_B^k \bmod p$ ③ $e = h(r, m)$ ④ $s \equiv k + x_A e \bmod q$		
	m, (r, s) ------>	
		① $h(r, m) = e$ ② $(g^s y_A^{-e})^{x_B} \equiv r \bmod p$ 이면 서명이 유효

그림 1. 수신자 지정 서명 생성 scheme

여기서 x_B는 지정 수신자 B만이 알고 있으며 그외의 어떤 제3자도 (r, s)와 메세지 m으로부터 서명의 진위 여부를 판별할 수는 없으므로, undeniable signature와는 상대적으로 서명자가 아닌 수신자 자신이 서명의 사본들이 남용되는 것을 막을 수 있다.

한편 디지탈 서명의 가장 중요한 기능 중의 하나인 부인방지 기능을 위해서는 이 서명이 문제가 되었을때 서명자가 이를 부인할 수 없도록 서명의 수신자가 임의의 제3자에게 그 서명의 정당성을 증명할 수 있는 프로토콜이 필수적이다. 즉 지정 수신자 B는 제3자에게 $(g^s y_A^{-e})^{x_B} \equiv r \bmod p$ 를 만족하는 이산대수 x_B를 알고 있다는 사실을 증명할 수 있어야 한다. 이러한 목적으로 사용될 프로토콜로 Chaum의 zero-knowledge confirmation protocol을 변형하여 다음과 같은 프로토콜을 구성할 수 있다. (그림 2. 참조)

[제3자에 대한 증명 프로토콜]

① 제3자(확인자)는 랜덤수 $R_3 \in [1, q)$를 선택하여 $C \equiv (g^s y_A^{-e})^{R_3} \bmod p$ 를 계산하여 C를 지정 수신자 B (증명자)에게 전송한다.

② 지정 수신자 B (증명자)는 랜덤수 $R_B \in [1, q)$를 선택하여 $R \equiv (C^{R_B})^{x_B} \bmod p$ 를 계산, 제3자(확인자)에게 전송한다.

③ 제3자(확인자)는 자신의 랜덤수 R_3를 지정 수신자 B (증명자)에게 전송한다.

④ 지정 수신자 B (증명자)는 제3자(확인자)로부터 받은 R_3를 이용하여 단계 ①에서 제3자(확인자)가 적법한 challenge값을 전송했는지를 확인한다. 만일 적법하다면 자신의 랜덤수 R_B를 제3자(확인자)에게 전송하고 그렇지 않다면 프로토콜을 종료한다.

⑤ 제3자(확인자)는 지정 수신자 B(증명자)로부터 받은 R_B를 이용하여 $R \equiv r^{R_3 R_B} \bmod p$ 가 성립하는지를 조사한다.

수 신 자 B		제 3 자
	C <----	① random $R_3 \in [1, q)$ ② $C \equiv (g^s y_A^{-e})^{R_3} \bmod p$
① random $R_B \in [1, q)$ ② $R \equiv (C^{R_B})^{x_B} \bmod p$	R ---->	
	R_3 <----	
	R_B ---->	① $R \equiv r^{R_3 R_B} \bmod p$?

그림 2. 제3자에 대한 증명 프로토콜

위의 프로토콜에서도 Chaum의 프로토콜과 마찬가지로 x_B를 모르는 공격자가 이 프로토콜을 성공적으로 통과할 수 있는 가능성은 $1/q$로 이들을 랜덤하게 추측하는 것과 마찬가지라는 것을 보일 수 있으며 또한 유사한 방법으로 simulator를 구성할 수 있다. [5]

4. 결 론

본 논문에서는 특정한 수신자만을 상대로 서명을 발행하여 수신자가 자신에게 발행된 서명을 통제할 수 있는 - undeniable signature의 상대적인 개념인 - 수신자 지정 서명 방식을 정의하였으며, Schnorr의 디지탈 서명방식을 변형한 수신자 지정 서명 생성 scheme과 그 서명의 정당성을 제3자에게 증명할 수 있는 프로토콜을 제안하였다.

이러한 서명방식은 보통의 서명방식이 누구나 인증 가능하다는 사실로 인해 이를 악용할 수 있는 가능성이 높다는 사실에 근거하여 특정 수신자의 개입없이는 그 서명을 인증할 수 없도록 함으로써 수신자의 프라이버시를 높여줄 수 있으므로 여러가지 응용들에서 매우 유용하게 사용될 수 있을 것이다.

참 고 문 헌

[1] D. Chaum and H. Antwerpen, "Undeniable signature", Proc. Crypto'89.

[2] D. Chaum, "Zero-knowledge undeniable signature", Proc. Eurocrypt'90.

[3] 임채훈, 이필중, "상호 신분 인증 및 디지틀 서명기법에 관한 연구", 통신정보보호학회논문집 제2권 제1호, 1992.

[4] 김승주, 박성준, 원동호, "수신자 지정 서명방식에 대한 고찰", 한국정보처리응용학회 학술발표논문집 제1권 2호, 1994.

[5] J. Boyar,D. Chaum,and I. Damgard, "Convertible undeniable signature", Proc. Crypto'90.

[6] T. Okamoto and K. Ohta, "How to utilize the randomness of zero-knowledge proofs", Proc. Crypto'90.