通信情報保護學會論文誌
第6卷 第1號, 1996. 3

영지식 수신자 지정 서명방식

김승주*, 김경신*, 박성준*, 원동호*

Zero-Knowledge Nominative Signatures

Seung Joo Kim, Kyung Sin Kim, Sung Jun Park and Dong Ho Won

요 약

본 논문에서는 특정한 수신자만을 상대로 서명을 발행하여 수신자가 자신에게 발행된 서명을 통제할 수 있는 - 부인 방지 서명방식의 쌍대 개념인 - 수신자 지정 서명방식을 분석하고, 이 요구 조건을 만족하는 수신자 지정 서명방식의 정의를 내린다. 특히, 안전성이 증명되는 영지식 수신자 지정 서명방식 프로토콜을 제안한다.

이러한 서명방식은 특정 수신자의 개입 없이는 그 서명을 인증할 수 없도록 함으로써 수신자의 프라이버시를 높여줄 수 있으므로 여러 가지 응용들에서 매우 유용하게 사용될 수 있을 것이다.

Abstract

In this paper, we propose a new kind of signature scheme, called "nominative signatures", which is the dual scheme of undeniable signatures. Also we construct a zero-knowledge protocol that implements it.

The new technique called ***"nominative signatures"*** achieves these objectives: only ***nominee*** can verify the ***nominator***(signer)'s signature and if necessary, only nominee can prove to the third party that the signature is issued to him(her) and is valid. Contrary to the undeniable signature scheme, nominative signatures are confirmed via a protocol between the nominee and the third party, so the cooperation of the nominee is necessary. That is, not a signer(nominator) but a verifier(nominee) can control the abuse of signatures - undeniable signature cannot be verified without the cooperation of the signer, so the signer controls the abuse of signatures.

Our nominative signatures are very valuable for the case in which the content of signature is concerned with the verifier's privacy.

* 성균관대학교 정보공학과 대학원 정보통신보호연구실

1. 서 론

암호 시스템의 기능은 보호 기능(privacy)과 인증 기능(authentication)으로 나눌 수 있다. 보호 기능은 정보가 노출된다 하여도 키를 알 지 못하는 한 정보의 의미를 파악하지 못하게 하여 정보를 보호하는 것이고, 인증 기능은 정보의 전달 상태 또는 통신시 송·수신자 간의 상대방 확인 기능을 갖춰 분쟁을 해결할 수 있는 요인을 제공하는 것이다. 인증 기능은 "자신이 보낸 정보가 변경되지 않고 상대방에게 정확히 전달되었는가?"를 확인하는 메시지 인증 기능과 정보의 생성·보관·처리 등의 행위에 관여한 사용자가 맞는가를 확인하는 사용자 인증 기능으로 구분할 수 있다. 일상생활에서 우리가 사용하는 서명이나 인감과 같은 효과를 전자적으로 수행하는 전자 서명은 이러한 사용자 인증 기능과 메시지 인증 기능을 모두 만족하여야 한다.

일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 발급될 수 있고, 이 서명 또는 인감을 수신한 사람 역시 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 발급할 수 없어야 한다. 따라서 전자 서명에서도 서명자만이 서명을 생성할 수 있는 유일성, 위조가 불가능한 위조 불가능성, 서명의 진위를 쉽게 확인할 수 있는 진위 확인의 용이성, 자신의 서명을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성 등의 요구 사항을 만족하여야 한다.

대부분의 전자 서명은 공개키 암호 시스템(public key cryptosystem)[1]이나 관용 암호 시스템(conventional cryptosystem)에 의해 구현되는데, 상대적으로 여러 가지 장점을 지닌 공개키 암호 시스템이 많이 사용된다. 이렇게 생성된 전자 서명은 적용하는 환경에 따라 여러 가지 형태로 변형되어 많은 분야에 응용되어 사용될 수 있다.

일반적인 응용에서는 누구나 이를 확인할 수 있도록 하는 것은 필수적이므로 일반적인 전자 서명이 매우 유용하게 사용될 수 있다.

그러나 공개키 암호 시스템을 이용한 일반적인 전자 서명 방식[2,3,4,5,6,7,8,9]은 공개키가 모든 사용자에게 공개되기 때문에 통신망에 가입한 사람은 누구든지 메시지의 진위 여부를 확인할 수 있게 되어 필요 이상의 과다한 인증 기회를 제공하게 된다. 이러한 요소는 개인적으로나 상업적으로 민감한 응용 분야에서 임의의 침입자가 전자 서명의 사본을 입수한 경우 이를 확인할 수 있게 되어 서명의 사본이 악용될 수 있는 소지를 제공하게 되며 이로 인해 개인의 이익 또는 사생활이 노출될 가능성이 있게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 서명자나 수신자에 대한 부당 위협 가능성을 줄여 주고 개인의 사생활을 보호할 수 있는 서명 방식이 보다 바람직한 경우가 존재한다.

예를 들어 소프트웨어 공급 회사나 각종 제조업체들이 자사의 제품을 보증하는 전자 서명을 발행할 경우 서명자의 도움이 있어야만 발행된 서명을 확인할 수 있게 하여 그 회사의 제품을 직접 구매한 고객만이 해당 업체와의 대화(interactive protocol)를 통해 자신이 구입한 제품이 진본임을 확인할 수 있게 하고, 후에 구입한 제품에 하자가 있을 경우라도 판매회사가 이를 부인할 수 없도록 할 수 있게 하여 서명자의 서명이 남용되는 것을 막을 수 있고 발행된 서명의 안전성에 대한 위협도 방지할 수 있을 것이다.

D. Chaum의 부인 방지 전자 서명 기법(undeniable signatures)은 이러한 목적에 의해 제안되었다.[10,11] 부인 방지 서명방식은 자신이

발행한 전자 서명이 정당함을 보이는 확인 프로토콜(confirmation protocol)과 자신이 발행한 서명을 후에 부인할 수 없도록 하는 부인 프로토콜(disavowal protocol)로 구성되어 앞에서 언급한 단점을 없앨 수 있어 많은 응용 분야에 적용될 수 있다.

본 논문에서는 부인 방지 서명의 쌍대 개념(dual scheme)인 수신자 지정 서명방식(nominative signatures)의 요구 조건을 분석하고, 이 요구 조건을 만족하는 수신자 지정 서명방식의 정의를 내린다. 특히, 안전성이 증명되는 영지식 수신자 지정 서명방식(zero-knowledge nominative signatures) 프로토콜을 제안한다.[14,15,16,17]

수신자 지정 서명방식이란 서명의 인증시에 특정 확인자만이 서명을 확인할 수 있도록 하되, 만일 그 서명이 문제가 되는 경우라도 확인자의 비밀키를 노출시키지 않고 제3자에게 서명의 출처를 증명함으로서 분쟁의 해결 기능을 제공하는 서명방식을 말한다. 즉, 지정된 수신자만이 서명을 확인할 수 있고 필요시 제3자에게 그 서명이 서명자에 의해 자신에게 발행된 서명임을 증명할 수 있게 함으로써 서명의 남용을 서명자가 아닌 검증자(수신자)가 통제할 수 있는 서명방식을 말한다. - 부인 방지 서명은 서명을 검증하기 위하여 서명자의 도움을 필요로 하나 수신자 지정 서명 방식은 수신자의 도움을 필요로 한다. - 이와 같이 특정 수신자만이 서명을 확인할 수 있도록 하는 수신자 지정 서명방식은 부인 방지 서명방식과는 반대로 발행된 서명이 수신자의 개인적인 이해 관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의없이 서명을 확인할 수 없게 되므로 특정 수신자에 대한 서명의 남용을 방지할 수 있게 된다.

이 수신자 지정 전자 서명방식은 개인의 건강 진단서나 생활 기록부, 세금 고지서 등을 특정 단체에서 발급 받아 자신의 필요에 따라 다른 단체에 제출할 때 적용할 수 있다. 즉 발급 단체가 자신의 비밀키와 발급 대상의 공개키를 사용하여 서명을 생성해 전송하면 이 서명의 지정 수신자는 자신의 비밀키를 이용하여 서명을 확인하고 자신이 제출할 단체에 전송하면 된다. 지정 수신자로부터 서명을 전송받은 단체는 지정 수신자가 정당한 수신자임을 확인하면 전송 받은 서명을 정당한 서명으로 받아들이게 된다. 이 때 전송되는 서명은 지정 수신자의 공개키가 결부되어 있으므로 이에 대응하는 비밀키를 모르면 확인할 수 없으므로 임의의 제3자가 어떠한 불법적인 경로를 통해 서명을 입수한다 하여도 이를 사용할 수 없게 되므로 지정 수신자는 자신에게 발행된 서명의 남용을 통제할 수 있게 된다.

2. 수신자 지정 서명방식 : 새로운 개념

본 장에서는 부인 방지 서명의 쌍대 개념인 수신자 지정 서명방식의 개념과 요구조건등에 대해서 정의하고, 형식적인 정의(formal definition)를 내린다.

2.1 수신자 지정 서명방식의 요구조건

수신자 지정 서명방식이란 지정된 수신자(nominee)만이 서명을 확인할 수 있고 필요시 제3자에게 그 서명이 서명자(nominator)에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 함으로써 서명의 남용을 서명자가 아닌 검증자(수신자)가 통제할 수 있는 - 부인 방지 서명방식의 쌍대 개념인 - 서명방식을 말한다. 즉, 부인 방지 서명은 서명을 검증하기 위하여 서명자의 도움을 필요로 하나 수신자 지정 서명방식은 수신자의 도움을 필요로 한다.

수신자 지정 서명방식의 기능이 요구되는 응용의 예를 들어보자.

갑이 모 회사에 그의 성적증명서를 제출해야 한다고 하자. 이때 성적증명서에는 학교장의 직인이 찍히게 된다. 이와 같은 경우에 서명자(nominator)는 학교의 총장이 되고, 검증자(nominee)는 갑, 제3자는 회사가 된다. 즉, 수신자 지정 서명방식은 서명의 수신자가 서명의 사본들이 불법적으로 사용되는 것을 통제할 수 있으므로 서명의 내용이 검증자의 프라이버시와 밀접한 관계가 있는 경우에 유용하게 사용될 수 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.

조건1) 지정된 수신자(nominee)만이 서명자(nominator)의 서명 S를 확인할 수 있다.
(서명자조차도 서명 S를 확인할 수 없다.)

조건2) 지정된 수신자만이 필요시에 제3자에게 서명 S가 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있다.
(서명자조차도 제3자에게 서명 S가 서명자에 의해 수신자에게 발행된 정당한 서명임을 증명할 수 없다.)

Remark: 조건1)이 만족되었을 때 '수신자 지정'이 된다.

조건2)를 만족하게 함으로써 자신에게 발행된 서명의 남용을 수신자 자신이 통제할 수 있게 한다. 서명자도 필요시에 그 서명의 정당성을 제3자에게 증명할 수 있다면, 수신자뿐만이 아닌 서명자(또는 서명자로부터 어떤 유용한 정보를 얻은 제3자)도 서명의 남용을 통제할 수 있다. 즉, 수신자 자신이 서명의 남용을 통제한다고 볼 수 없다.

2.2 수신자 지정 서명방식의 형식적인 정의

수신자 지정 서명방식의 특성을 갖게 하기 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.

■ **정의 1.** 수신자 지정 서명방식(nominative signatures)은 다음 조건들을 만족하는 $(G_{nominator(signer)}, G_{nominee(verifier)}, Sign, Verify, Conf_{(nominee,\ third\ party)})$이다. :

(1) 키 생성 $(G_{nominator}, G_{nominee})$:

① $G_{nominator}$은 probabilistic polynomial-time algorithm으로, 1^n(the security parameter)을 입력으로 하여, 스트링의 쌍(nominator의 비밀키, nominator의 공개키)을 출력한다.

$$G_{nominator}(1^n) = (G1_{nominator}(1^n), G2_{nominator}(1^n)).$$

② $G_{nominee}$은 probabilistic polynomial-time algorithm으로, 입력 스트링 1^n을 입력으로 하여, 스트링의 쌍(nominee의 비밀키, nominee의 공개키)을 출력한다.

$G_{nominee}(1^n) = (G1_{nominee}(1^n), G2_{nominee}(1^n))$.

(2) Signing (Sign):

Sign은 probabilistic polynomial-time algorithm으로, 입력 스트링 1^n, m(메세지), nominator의 비밀키 $\in G1_{nominator}(1^n)$, nominee의 공개키 $\in G2_{nominee}(1^n)$ 등을 입력으로 하여, 스트링("수신자 지정 서명(nominative signature)")을 출력한다.
$Sign(1^n, m, G1_{nominator}(1^n), G2_{nominee}(1^n))$ (이후, Sign(m)으로 표기).

(3) Verifying (Verify)

Verify은 probabilistic polynomial-time algorithm으로, 입력 스트링 1^n, m(메세지), Sign(m), nominator의 공개키 $\in G2_{nominator}(1^n)$, nominee의 비밀키 $\in G1_{nominee}(1^n)$을 입력으로 하여, 만약 Sign(m)이 $Sign(1^n, m, G1_{nominator}(1^n), G2_{nominee}(1^n))$의 범위 내에 있으면

$$Verify(1^n, G2_{nominator}(1^n), G1_{nominee}(1^n), m, Sign(m)) = 1$$

그렇지 않으면

$$Verify(1^n, G2_{nominator}(1^n), G1_{nominee}(1^n), m, Sign(m)) = 0$$

을 출력한다.

(4) Confirmation ($Conf_{(nominee,\ third\ party)}$)

$Conf_{(nominee,\ third\ party)}$은 nominee 와 제3자(the third party) 사이의 대화형 증명(interactive proof)으로, 일반의 입력 스트링 1^n, m, s(m의 서명으로 생각되는 값), nominator의 공개키 $\in G2_{nominator}(1^n)$, nominee의 공개키 $\in G2_{nominee}(1^n)$을 입력으로 하여, 1("참") 또는 0("거짓")을 출력한다. 여기서, nominee은 auxiliary input, nominee의 비밀키 $\in G1_{nominee}(1^n)$를 가지고 있는 증명자이고, 제3자는 검증자이다.
만약 $s = \Sigma s(m)$ 이면,

모든 m, 임의의 상수 c, 충분히 큰 n에 대하여,

$$Pr(Conf_{(nominee,\ third\ party)}(1^n, m, s, G2_{nominator}(1^n), G2_{nominee}(1^n)) = 1) > 1 - 1/n^c,$$

그렇지 않으면,

$$Pr(Conf_{(nominee,\ third\ party)}(1^n, m, s, G2_{nominator}(1^n), G2_{nominee}(1^n)) = 0) > 1 - 1/n^c,$$

이다.

3. 영지식 수신자 지정 서명방식 프로토콜

이 장에서는 2장에서 제시된 수신자 지정 서명방식의 2가지 요구조건을 만족하는 영지식 수신자 지정 서명방식 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 서명방식을 변형하면 이와 같은 수신자 지정 서명방식을 구성할 수 있다.[4,5] 서명자 A가 지정 수신자 B만이 확인할 수 있도록 메세지 m을 서명하여 보내고자 하는 경우 다음과 같이 서명을 생성할 수 있다 (그림 1. 참조).

[초기화]

공개정보) p : 소수.

q : 소수. 단, q | p-1
α : mod p 상에서 위수가 q인 임의의 수.
v : $v = \alpha^s \pmod p$

비밀정보) s : q 보다 작은 임의의 수

Schnorr에 의하면 p의 길이를 약 512 bits, q의 길이를 약 140 bits 정도로 하는 것이 좋다고 한다.

[수신자 지정 서명 기법]

① 서명자 A는 랜덤수 r, $R \in_R [1, q)$를 선택하여 $x \equiv \alpha^{R-r} \pmod p$, $X \equiv v_B^R \pmod p$를 계산한다.

② $e = h(v_B, x, X, m)$를 계산하고 $y \equiv r - s_A e \pmod q$를 구하면 (v_B, x, X, y)가 메세지 m에 대한 서명이 된다.

③ 이를 받은 지정 수신자 B는 $h(v_B, x, X, m) = e$와 $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$를 만족하는지 검사함으로써 메세지 m에 대한 서명을 확인할 수 있다.

여기서 s_B는 지정 수신자 B만이 알고 있으며 그 외의 어떤 제3자도 (v_B, x, X, y)와 메세지 m으로부터 서명의 진위 여부를 판별할 수는 없으므로, 부인 방지 서명과는 상대적으로 서명자가 아닌 수신자 자신이 서명의 사본들이 남용되는 것을 막을 수 있다.

[제3자에 대한 영지식 대화형 증명 프로토콜]

디지틀 서명의 가장 중요한 기능 중의 하나인 부인방지 기능을 위해서는 이 서명이 문제가 되었을 때 서명자가 이를 부인할 수 없도록 서명의 수신자가 임의의 제3자에게 그 서명의 정당성을 증명할 수 있는 프로토콜이 필수적이다. 즉 지정 수신자 B는 제3자에게 $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$와 $\alpha^{s_B} \equiv v_B \pmod p$를 만족하는 이산대수 s_B를 알고 있다는 사실을 증명할 수 있어야 한다. 이때 제3자는 s_B의 값을 모르지만 지정 수신자 B가 s_B를 소유하고 있음을 확신하게 된다.

이러한 목적으로 사용될 프로토콜로 다음과 같은 프로토콜을 구성할 수 있다. (그림 2. 참조)

서명자(nominator) A		수신자(nominee) B
$s_A \in_R [1, q)$ $v_A \equiv \alpha^{s_A} \pmod p$	p, q, α, h { v_A } { v_B }	$s_B \in_R [1, q)$ $v_B \equiv \alpha^{s_B} \pmod p$
① r, $R \in_R [1, q)$ $x \equiv \alpha^{R-r} \pmod p$ $X \equiv v_B^R \pmod p$ ② $e = h(v_B, x, X, m)$ $y \equiv r - s_A e \pmod q$	m, (x, X, y) →	③ $h(v_B, x, X, m) = e$ $(\alpha^y v_A^e x)^{s_B} \equiv X \pmod p$

그림 1. 수신자 지정 서명 기법

수신자(nominee) B		제 3 자
	ch ←	① a, b $\in_R$ [1, q) ch = $(\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b} \pmod p$
② t $\in_R$ [1, q) $h_1 \equiv ch \cdot \alpha^{t} \pmod p$ $h_2 \equiv h_1^{S_B} \pmod p$	h_1, h_2 →	
	a, b ←	③ 단계 ①에서 사용한 랜덤수 a, b를 전송한다.
④ ch = $(\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b} \pmod p$?	t →	
		⑤ $h_1 = (\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b+t} \pmod p$? $h_2 = X^{a} \cdot v_B^{b+t} \pmod p$?

그림 2. 제3자에 대한 영지식 대화형 증명 프로토콜

① 제3자(확인자)는 랜덤수 a, b $\in_R$ [1, q)를 선택하여 ch를 계산하여 지정 수신자 B(증명자)에게 전송한다.

$$ch = (\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b} \pmod p$$

② 지정 수신자 B는 랜덤수 t $\in_R$ [1, q)를 선택하여 h_1, h_2를 계산하여 제3자에게 전송한다.

$$h_1 \equiv ch \cdot \alpha^{t} \pmod p$$
$$h_2 \equiv h_1^{S_B} \pmod p$$

③ 제3자는 단계 ①에서 사용한 랜덤수 a, b를 지정 수신자 B에게 전송한다.

④ 수신자 B는 이 a, b가 $ch = (\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b} \pmod p$을 만족하는지 조사하여 이를 만족한다면 단계 ②에서 사용한 랜덤수 t를 전송한다. 이를 만족하지 않는다는 것은 확인자가 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 제3자는 단계 ②에서 받은 h_1, h_2와 단계 ④에서 받은 t를 이용하여 다음을 만족하는지를 검사한다.

$$h_1 = (\alpha^{y}v_A^{e}x)^{a} \cdot \alpha^{b+t} \pmod p \ ?$$
$$h_2 = X^{a} \cdot v_B^{b+t} \pmod p \ ?$$

순서 ① ~ ⑤가 정상적으로 수행되면 제3자는 지정 수신자 B가 $(\alpha^{y}v_A^{e}x)^{S_B} \equiv X \pmod p$와 $\alpha^{S_B} \equiv v_B \pmod p$를 만족하는 이산대수 s_B를 알고 있다는 사실을 확인할 수 있게 된다.

그림 2.에서 주어진 프로토콜은 다음에 주어지는 확률론적 튜링 머신인 simulator M에 의해 영지식 증명 시스템임을 쉽게 증명할 수 있다.[12,13]

[simulator M]

그림 2.의 프로토콜은 어떤 확인자 V'에 대해서도 다음과 같이 시뮬레이트될 수 있다.

① V'로부터 challenge 값, ch를 얻는다.

② e를 선택하여 $h_1' \equiv \alpha^e \pmod p$, $h_2' \equiv v_{nominee}^e \pmod p$를 계산한다.

③ 확인자로부터 (a, b)를 얻는다.
만일 $ch \neq (\alpha^y v_{nominator}^e x)^a \cdot \alpha^b \pmod p$ 이면 중단하고, 그렇지 않으면 단계 ④로 간다.

④ V'를 challenge 값이 보내진 이후까지 다시 감는다.
t를 선택하여 $h_1 = (\alpha^y v_{nominator}^e x)^a \cdot \alpha^{b+t} \pmod p$, $h_2 = X^a \cdot v_{nominee}^{b+t} \pmod p$를 계산한다.

⑤ 확인자로부터 (a', b')를 얻는다.
만일 $ch = (\alpha^y v_{nominator}^e x)^{a'} \cdot \alpha^{b'} \pmod p$ 이면 t를 확인자에게 전송한다. 그렇지 않으면 단계 ④로 간다.

영지식 대화형 증명에서 지정 수신자가 아닌 다른 사람이 s_B를 소유하고 있는 것으로 가장하려고 할 때 확인자를 속일 수 있는 확률은 기껏해야 1/q로 랜덤하게 추측하는 방법뿐이다.

4. 결 론

본 논문에서는 특정한 수신자만을 상대로 서명을 발행하여 수신자가 자신에게 발행된 서명을 통제할 수 있는 - 부인 방지 서명방식의 쌍대 개념인 - 수신자 지정 서명방식을 정의하고, 형식적인 정의를 내렸으며, Schnorr의 디지틀 서명방식을 변형하여 이산 대수 문제에 근거한 수신자 지정 서명 기법과 그 서명의 정당성을 제3자에게 증명할 수 있는 영지식 대화형 증명 프로토콜을 제안하였다.

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

참 고 문 헌

[1] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory IT-22, pp.644-654, 1976.

[2] R. Rivest, A. Shamir, and L. Adleman, "A method for Obtaining Digital Signature and Public key Cryptosystems", Communication of the ACM, pp.120-128, FEB. 1978.

[3] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory 31, pp.469-472, 1985.

[4] C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Advances in Cryptology - CRYPTO '89 Proceedings, Berlin: Springer-Verlag, pp.239-252, 1990.

[5] C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Journal of Cryptology, v.4, n.3, pp.161-174, 1991.

[6] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp.47-53, 1985.

[7] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solution to Identifi-

cation and Signature Problem", . Crypto'86, pp.186-194, 1987.

[8] L. C. Guillou, J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing both Transmission and Memory", EUROCRYPT'88, pp.123-128. 1988.

[9] L. C. Guillou, J. J. Quisquater, "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge" CRYPTO'88, pp.216-231. 1988.

[10] D. Chaum and H. Antwerpen, "Undeniable signature", Proc. Crypto'89, pp.212-216.

[11] D. Chaum, "Zero-knowledge undeniable signature", Proc. Eurocrypt'90, pp.458-464.

[12] J. Boyar, D. Chaum, and I. Damgard, "Convertible undeniable signature", Proc. Crypto'90, pp.195-208.

[13] T. Okamato and K. Ohta, "How to utilize the randomness of zero-knowledge proofs", Proc. Crypto'90,pp. 437-456.

[14] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures", Proc. ICEIC'95, pp.II-68~II-71, 1995.

[15] 김승주, 박성준, 원동호, "수신자 지정 서명방식에 대한 고찰", 한국정보처리응용학회 학술발표논문집 제1권 제2호, pp. 530-533, 1994.

[16] 김승주, 박성준, 원동호, "수신자 지정 서명방식", 통신정보보호학회 학술발표논문집 Vol.4 No.1 pp.24-28, 1994.

[17] 김승주, 박성준, 원동호, "효율적인 수신자 지정 서명방식", 대한전자공학회 학술발표논문집 Vol.18 No.1 pp.222-224, 1995.

□ 著者紹介

김 승 주(金 昇 柱, Seung Joo Kim)

1971년 9월 22일생
1994년 2월 성균관대학교 정보공학과 졸업 (공학사)
1996년 2월 성균관대학교 대학원 정보공학과 졸업 (공학석사)
1996년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정

김 경 신(金 庚 信, Kyung Sin Kim)

1960년 7월 24일생
1983년 2월 성균관대학교 전자공학과 졸업 (공학사)
1995년 2월 성균관대학교 대학원 전자공학과 졸업 (공학석사)
1993년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정
1984년 12월~ 1991년 2월 삼성전자(주) 컴퓨터부문 선임연구원
1991년 3월 ~ 1995년 2월 연암공업전문대학 전자계산과 조교수
1995년 3월 ~ 현재 인덕전문대학 방송통신과 조교수

※ 주관심분야 : 암호이론, 정보이론, 방송기술

박 성 준(朴 性 俊, Sung Jun Park)

1960년 10월 29일생
1983년 2월 한양대학교 수학과 졸업 (이학사)
1985년 2월 한양대학교 대학원 수학과 졸업 (이학석사)
1985년 1월 ~ 1994년 3월 한국전자통신연구소 부호기술부 선임연구원
1992년 3월 ~ 1996년 2월 성균관대학교 대학원 정보공학과 졸업 (공학박사)

※ 주관심분야 : 암호이론, 계산이론, 정보이론

원 동 호(元 東 豪, Dong Ho Won)

1949년 9월 23일생
1976년 2월 성균관대학교 전자공학과 졸업 (공학사)
1978년 2월 성균관대학교 대학원 전자공학과 졸업 (공학석사)
1988년 2월 성균관대학교 대학원 전자공학과 졸업 (공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경공대 객원연구원
1982년 3월 ~ 현재 성균관대학교 공과대학 정보공학과 교수
1991년 ~ 현재 한국통신정보보호학회 편집이사

※ 주관심분야 : 암호이론, 정보이론