韓國 OA學會 論文誌
第5卷 第3號, 2000. 9.

2000-5-3-3-2

디지털 서명과 은닉서명에 관한 연구

이 재 영*, 이 지 영**

A Study on a Blind Signature and Digital Signature

Jae - Young Lee, Ji - Young Lee*

요 약

본 논문에서는 이산대수 문제의 어려움과, 인수분해 문제의 어려움에 기초한 대표적인 디지털 서명들과 그 디지털 서명에 근간한 은닉서명에 대해 연구하고 나아가 제한된 자원을 갖는 환경에서 문제를 일으킬 수 있는 역원의 사용을 배제한 디지털 서명을 제안하고 제안한 디지털 서명에 근간한 새로운 은닉서명을 제안하였다.

Abstract

This paper first examines the problems of digital signatures concerning discrete logarithms and factorizations. Then the study introduces a blind signature that is based on digital signature. It also attempts to propose a new digital signature by excluding the use of inverse which has presumably caused problems in limited resources. Finally, the paper suggests a blind signature that can be offered by this new digital signature.

* 세명대학교 교육대학원 전산교육
** 세명대학교 컴퓨터응용물리학과 교수

Ⅰ. 서론

정보통신기술의 발달과 컴퓨터의 보급이 확대되면서 전자문서를 이용한 전자사서함, 전자상거래, 전자금융, 전자무역 등 정보화 사회에서 요구되는 다양한 서비스를 제공할 수 있게 되었다. 그러나 무한복제가 가능하고 내용의 변경이나 서명자를 확인하기 어려운 전자문서의 특성상 일반문서에 표기되던 수기 서명이나 인장과 같은 효과를 내는 디지털 서명이 필요하게 되었다.

본 논문에서는 중재자를 필요로 하지 않는 공개키 암호 방식을 이용한 디지털 서명 중 이산대수 문제의 어려움에 기초한 ElGamal 디지털 서명의 변형들과 인수분해의 어려움에 기초한 RSA의 서명에 대해 연구하고, 그 디지털 서명들에 근간한 은닉서명에 대해 연구하였다.

스마트 카드와 같이 제한된 자원을 갖는 환경에서는 역원의 계산은 모듈라 멱승을 이용하여 하게되므로 메모리 소자 크기에 영향을 줄 수 있다. 이에 본 논문에서는 역원의 사용을 배제한 디지털 서명과 제안한 디지털 서명에 근간한 은닉서명을 제안하였다.

Ⅱ. 디지털 서명과 디지털 서명에 근간한 은닉서명

공개키 암호 방식을 이용한 서명 방식을 도식적으로 나타내면 그림1과 같다.

일반적으로 디지털 서명이라 하면 공개키 암호 방식을 이용한 디지털 서명 방식을 말한다[2].

은닉서명은 메시지 송신자가 서명자에게 서명메시지 M의 내용을 보여주지 않고 메시지에 대한 유효한 서명을 얻으려 할 때 쓰이는 서명 알고리즘이다. 은닉서명은 실세계의 전자화폐가 가지고 있는 익명성을 전자화폐에 적용할 수 있도록 하기 위하여 고안되었으며 은닉서명의 은닉성을 통해 전자화폐의 사용 고객의 프라이버시를 보호할 수 있게 되었다.

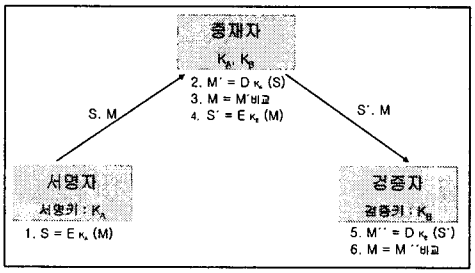

그림 1. 공개키 암호 방식을 이용한 서명 방식

1. 이론적 배경

디지털 서명에는 이산대수 문제의 어려움에 기초한 ElGamal 디지털 서명의 변형들과 인수분해 문제의 어려움에 기초한 RSA 디지털 서명 등이 있다.

이산대수 문제의 어려움이란 $GF(P)$의 원소 G ($G^Q \bmod P = 1$, $G \neq 1$를 만족하는 G)로 생성되는 부분 곱셈군 $\langle G \rangle$의 주어진 원소 Y에 대하여 $Y = G^X \bmod P$를 만족하는 X를 찾는 문제이며, 이러한 이산대수 문제가 쉽게 풀리면 디지털 서명 알고리즘은 전혀 안전하지 않게 된다. 따라서 이산대수 문제를 푸는 것이 계산상 불가능하도록 소수 P와 Q의 크기를 선택해야 한다.

또한, 인수분해 문제의 어려움이란 $N = P \cdot Q$ (P와 Q는 소수)에서 P와 Q를 알고서 N을 구하기는 쉽지만 N만을 알고 P와 Q을 찾기란 어렵다는 것이다.

인수 분해의 문제 역시 P, Q를 찾아내는 것이 계산상 불가능하도록 소수 P와 Q의 크기를 선택해야 한다.

2. 대표적인 디지털 서명들과 그에 근간한 은닉서명

RSA 디지털 서명 방식은 Rivest, Shamir, Adleman에 의해 제안된 서명 방식으로[5] 인수분해 문제의 어려움에 기초한 서명 방식이다. 서명의 생성은 상당히 많은 계산량이 필요하나 검증은 빠르게 수행될 수 있다.

표 1. 공개키 알고리즘을 이용한 대표적 디지털 서명

디지털서명	서명자		검증자
RSA	$S = H^d \bmod n$	M, S →	$H = S^e \bmod n$
Schnorr	$r = g^k \bmod p$ $e = h(r \parallel M)$ $S = k + x \cdot e \bmod q$	M, S, e →	$v = g^S \cdot y^e \bmod p$ $e' = h(v \parallel M)$
KCDSA	$r = g^k \bmod p$ $S = x(k - H) \bmod q$	H, r, S →	$R = y^S g^H \bmod p$

현재 산업계에서 사용되는 대부분의 디지털 서명은 RSA를 기반으로 하고 있다. 그러나 RSA는 서명의 생성과 검증 사이에 서로 역관계가 성립되어 서명방식이 암호화와 복호화 용으로 전용될 수 있다는 우려 때문에 비밀성을 배제하고 순수하게 서명만이 요구되는 경우에 사용된다.

Schnorr 디지털 서명은 Schnorr가 제안한 서명 방식으로 이산대수 문제의 어려움에 기초한 방식이며 ElGamal 디지털 서명의 변형이다[17][18]. Schnorr 디지털 서명은 계산의 효율성을 위해 부분체 $GF(q)$를 처음으로 사용한 서명 방식으로 Schnorr 디지털 서명의 경우에는 메시지의 해쉬 과정에서 난수 r이 추가되므로 메시지만으로 해쉬하는 경우보다 높은 안전성을 제공한다[1].

KCDSA는 이산대수 문제의 어려움에 기초한 ElGamal 서명 방식의 변형으로 국내에서 디지털 서명 표준으로 제안된 방식이다[3].

표1은 대표적 디지털 서명을 도식적으로 표현한 것이고 표2는 표1의 디지털 서명에 근간한 은닉 서명들이다

Ⅲ. 제안한 디지털 서명과 은닉서명

1. 역원의 사용을 배제한 디지털 서명

일반 컴퓨터에서의 역원의 계산은 확장된 유클리드 알고리즘(extended Euclid algorithm)을 이용하면 모듈라 멱승에 비해 무시할 수 있을 정도의 시간에 계산이 가능하여 역원의 계산에 걸리는 시간이 디지털 서명의 전체적인 시간에 문제를 주지 않는다. 그러나 스마트 카드와 같이 제한된 자원을 갖는 환경에서는 역원을 계산할 때 모듈라 멱승을 이용하여 하므로 전체적인 디지털 서명 시간에 문제를 줄 수 있다. 때문에 디지털 서명의 전체적인 알고리즘에 역원의 사용은 피하는 것이 바람직하다[2][4].

서명과정

1. 서명자는 난수 k ($0 < k < q$)를 선택한다.
2. 서명자는 선택한 난수 k를 이용하여 식(1)과 같이 r을 구한다.

   $r = g^k \bmod p$ 식(1)
3. 서명자는 해쉬 함수 h로 식(2)과 같이 서명 메시지 M을 서명할 수 있는 크기 H로 압축한다.

   $H = h(M)$ 식(2)
4. 서명자는 난수 k와 서명키 x를 이용하여 식(3)과 같이 서명 값 S를 구한다.

   $S = (k - xH) \bmod q$ 식(3)
5. 검증자에게 H, r, S를 전송한다.

검증과정

1. 서명자의 공개 검증키 y와 서명자에게 받은 H, r, S를 이용하여 식(4)과 같이 R을 구한다.

표 2. 디지털 서명에 근간한 은닉서명

은닉서명	메시지 송신자		서명자
RSA에 근간한 은닉서명	$K_1 \equiv r^e H \bmod n$ $S \equiv \frac{K_2}{r} \bmod n$ $\equiv H^d$	K_1 → ← K_2	$n = p \cdot q$ $\gcd(e, \phi(n)) = 1$ $e \cdot d \equiv 1 \bmod \phi(n)$ $K_2 \equiv K_1^d \bmod n$
Schnorr에 근간한 은닉서명	$r = r' g^{-\alpha} y^{-\beta} \bmod p$ $e' = H(r \parallel M)$ $e = e' + \beta$ $S = s - \alpha \bmod q$	← r' e → ← s	$r' = g^k \bmod p$ $s = (k + xe) \bmod q$
KCDSA에 근간한 은닉서명	$r = r'^{\alpha} g^{\beta} \bmod p$ $m = \alpha^{-1}(M - \beta) \bmod q$ $S = s\alpha \bmod q$ $R = r \bmod p$	← r' m → ← s	$r' = g^k \bmod p$ $s = x(k - m) \bmod q$

$R = y^H g^S \bmod p$ 식(4)

2. $R = r$이 성립하는지 확인한다.

$R = r$ 이면 정당한 서명자로부터의 서명임을 확인한다. 검증식 R이 성립하면 서명 값 S는 서명 메시지 M에 대하여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명되었음이 확인된다.

$$\begin{aligned} R &= y^H g^S \bmod p \\ &= y^H g^{(k - xH)} \\ &= (g^x)^H g^{(k - xH)} \\ &= g^{xH} g^{k - xH} \\ &= g^{xH - xH + k} \\ &= g^k \\ &= r \end{aligned}$$

2. 제안한 디지털 서명에 근간한 은닉서명

제안된 은닉서명 방식에서 사용되는 공개정보와 시스템 변수는 제안된 은닉서명이 앞선 제안한 디지털 서명에 근간한 것이므로 제안한 디지털 서명에 쓰인 것과 동일하다.

서명과정

1. 서명자는 난수 k ($0 < k < q$)를 선택한다.
2. 서명자는 난수 k를 이용하여 식(5)과 같이 r'를 구하고 메시지 송신자에게 전송한다.

$r' = g^k \bmod p$ 식(5)

3. 메시지 송신자는 해쉬 함수 h를 이용하여 식(6)과 같이 서명 메시지 M을 H로 압축한다.

$H = h(M)$ 식(6)

4. 메시지 송신자는 서명자에서 전송 받은 r'와 난수 $\alpha, \beta \in {}_R Z_q$를 선택하여 식(7)과 같이 r 을 계산한다.

$r = r'^{\alpha} y^{\beta} \bmod p$ 식(7)

5. 메시지 송신자는 난수 $\alpha, \beta \in {}_R Z_q$와 H를 이용하여 식(8)과 m을 구하고 서명자에게 전송한다.

$m = \alpha^{-1}(H - \beta) \bmod q$ 식(8)

6. 서명자는 난수 k와 서명키 x, 메시지 송신자에게서 전송 받은 m을 이용하여 식(9)와 같이 서명 s를 구하고 이것을 메시지 송신자에게 전송한다.

$s = (k - xm) \bmod q$ 식(9)

7. 메시지 송신자는 서명자에게 전송 받은 s로부터 서명 메시지 M에 대한 서명 값 S와 R을 식(10), 식(11)과 같이 결정한다.

$$S = s\alpha \bmod q \qquad \text{식(10)}$$

$$R = r \bmod p \qquad \text{식(11)}$$

검증과정

1. 서명자의 공개 검증키 y를 이용하여 식(12)와 같이 R을 구한다.

$$R = g^S y^H \bmod p \qquad \text{식(12)}$$

2. $R = r$이 성립하는지 확인한다.

   $R = r$ 이면 정당한 서명자로부터의 서명임을 확인한다.

검증식 R의 식이 성립하면 서명 값 S는 서명 메시지 M에 대하여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명되었음이 확인되는 것이다.

$$\begin{aligned} R &= g^S y^H \bmod p \\ &= g^{s\alpha} g^{xH} \\ &= g^{(k-xm)\alpha} g^{xH} \\ &= g^{\alpha k - \alpha xm} g^{x(\alpha m+\beta)} \\ &= g^{\alpha k - \alpha xm} g^{\alpha xm + x\beta} \\ &= g^{\alpha k + x\beta} \\ &= r'^{\alpha} y^{\beta} \\ &= r \end{aligned}$$

Ⅳ. 안전성 및 효율성

일반 컴퓨터에서는 확장된 유클리드 알고리즘(extended Euclid algorithm)을 이용해 역원을 계산하므로 본 논문에서 제안한 디지털 서명과 위에서 비교한 기존의 다른 디지털 서명들과 전체적인 서명 시간의 차이는 없다고 할 수 있다. 그러나 역원이 사용된 디지털 서명은 스마트 카드와 같이 제한된 자원을 갖는 환경에서는 역원을 계산할 때 모듈라 멱승을 이용하여 구현되므로 문제가 있을 수 있다.

각 사용자는 비밀키를 안전하게 가지고 있지만 ElGamal형 서명의 경우 메시지를 서명할 때 난수가 사용이 되는데 만약 난수가 노출이 될 경우 전송 정보로부터 비밀키를 복구할 수 있으므로 난수의 안전한 보관과 서명의 길이가 약속된 길이가 아닐 경우 쉽게 서명을 위조할 수 있으므로 서명의 길이도 확인하는 것이 서명의 안전성에 중요하다.

Ⅴ. 결론

본 논문은 공개키 암호 방식을 이용한 것으로 디지털 서명 중 이산대수 문제의 어려움에 기초한 것 ElGamal형 디지털 서명과 인수분해 문제의 어려움에 기초한 RSA 디지털 서명에 대해 연구하였다.

일반 컴퓨터에서의 역원의 계산은 확장된 유클리드 알고리즘(extended Euclid algorithm)을 이용하면 모듈라 멱승에 비해 무시할 수 있을 정도의 시간에 계산이 가능하다. 그러나 스마트 카드와 같이 제한된 자원을 갖는 환경에서는 역원의 계산 시 모듈라 멱승을 이용하여 구현하므로 역원의 사용은 피하는 것이 좋다. 이에 본 논문에서는 역원의 사용이 배제된 디지털 서명을 제안하였고 제안한 디지털 서명에 근간한 은닉서명을 제안하였다. 제안한 역원의 사용을 배제한 디지털 서명은 스마트 카드와 같이 제한된 자원을 갖는 환경에서는 기존의 역원을 이용한 디지털 서명보다 전체적인 서명 시간이 짧을 것으로 기대한다.

참고문헌

[1] 오중효, "암호IC 카드를 사용한 디지털 서명 시스템 및 응용"

[2] 원동호, "현대암호학"
[3] Task Force Team, "A Proposal for Digital Signature Standard" ASIACRYPT '96 Rump session.
[4] 임채훈, 이필중, 강신각, 박성준 "확인서 이용 부가형 디지털서명 방식 표준(안)"
[5] R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. of the ACM, vol.21, no.2, pp.120-126, Feb. 1978.
[6] C.P.Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol.4, no.3, pp.161-174, 1991.
[7] T.ElGamal, "A Public Key Cryptosystem and a Siganture Scheme Based on Discrete Logarithms," IEEE Trans. Inform. Theory, IT-31, pp.469-472, 1985.

저 자 소 개

이재영
세명대학교 교육대학원
전산교육학과

이지영
OA학회 제 4권4호 참조