情報保護學會論文誌
第13券 第5號, 2003. 10

효율적인 메시지 복호화를 제공하는 이중 전자서명 방식

김 근 옥*, 남 정 현*, 김 승 주**, 원 동 호***

Dual Signature Scheme to provide efficient message decryption

Keun-Ok Kim*, Junghyun Nam*, Seungjoo Kim**, Dong Ho Won***

요 약

대표적인 지불브로커 시스템인 SET의 서명 방식 중 이중 전자서명 방식은 사용자의 지불 정보(신용카드 번호 등)는 상점에 노출되지 않고, 사용자의 주문 정보는 은행에 노출되지 않게하여 사용자의 프라이버시를 지켜주는 것이다. 이러한 서명 방식은 전자상거래의 활성화로 그 필요성이 대두되었다. 하지만, SET의 이중 서명 방식은 계산량과 통신량이 많아 무선 환경에서 사용되기에는 적합하지 않다. 본 논문에서는 통신량을 줄이고자 상점의 주문 정보와 은행의 지불 정보 이용하여 다항식을 생성하는 signcryption 방식을 제안하였다. 기존의 signcryption방식과 이중 서명 방식을 분석하여 문제점을 도출하여 효율적인 전자서명 방식을 제안하고, 그 안전성을 분석한다.

ABSTRACT

A representative payment broker system is SET and one of its signature shcemes is a dual digital signature scheme. A dual digital signature scheme expose neither user's payment information(credit card number etc.) to merchandiser, nor user's order information to bank. So it keeps user's privacy safe. The digital signature scheme like this is being necessary as E-commerce is revitalized. But a dual digital signature of SET is not appropriate for wireless environments because it needs so many computations and communications. In this paper, we propose a signcryption scheme that generates a polynomial using a payment information for merchandiser and an order information for bank in order to reduce communications. We analyze the problem of existing signcryption schemes and dual digital signature schemes. Also we analyze the security properties of the proposed scheme.

keyword : *dual signature, signcryption, polynomial*

Ⅰ. 서 론

전자상거래의 활성화로 인해 상거래의 많은 부분에서 전자 결제 서비스를 이용하고 있다. 하지만, 전자 결제의 특성상 서로 대면하지 않고 온라인 상에서 거래가 이루어지기 때문에 거래 내용에 대한 보호를 위한 요구사항들이 존재한다.

전자 결제 서비스에서 사용되는 전자 화폐는 디지털 정보화, 재사용 불가능성, 익명성, 오프라인성, 양도 가능성, 분할이용 가능성, 부정 사용자의 익명성 취소등의 요구사항을 만족해야 한다. 특히 전자화폐의 익명성은 현금 사용시에는 요구되지 않았지만, 전

* 성균관대학교 전기전자 및 컴퓨터 공학부 정보통신 보호연구실({kokim, jhnam}@dosan.skku.ac.kr)
** 한국정보보호진흥원(sjkim@kisa.or.kr)
*** 성균관대학교 정보통신공학부 정교수(dhwon@dosan.skku.ac.kr)

자화폐 발행시 사용자의 식별 정보를 연계시킴으로써 사용자를 추적할 수 있는 문제로 인한 요구사항이다. 이를 보호하기 위해서는 상점이나 은행이 결탁하여도 이용자의 구매 정보에 관한 프라이버시는 노출되지 않아야 한다. 전자상거래에서는 이러한 사용자의 프라이버시가 보장되는 것이 특징이다.

하지만, 신용카드를 사용해 지불 브로커 시스템을 이용하는 경우 이러한 이용자의 프라이버시가 지켜지기 힘들다. 현재 SET 프로토콜에서는 이러한 문제점을 해결하기 위해 이중 서명(dual signature) 방식을 사용하고 있다. 이 방식의 경우 지불정보와 상품정보 각각에 각 객체(은행, 상점)의 공개키로 암호화 한 후 두 정보의 해쉬값을 연접(concatenation)해서 서명을 수행한다. 이 방법은 사용자의 지불정보와 상품내역 정보를 숨기기 위해 가장 일반적인 방법이지만, 몇가지 문제점이 존재한다. 사용자는 공개키 암호방식을 이용해서 각각의 정보를 암호화 하기 때문에 연산 부담이 매우 크다. 또한 각 정보의 해쉬값을 연접해서 서명을 수행하기 때문에 만약 분쟁 발생시 사용자의 지불정보와 상품정보 중 어떠한 문제인지 판별하기 어렵다. 마지막으로 각각의 정보를 암호화한 암호문 두 개를 연접하고 각각의 해쉬값과 서명값을 모두 상점에 전송해 주기 때문에 통신량이 매우 많다. 유선환경에서는 통신량이 큰 문제가 되지 않을 수도 있지만, 무선 환경의 경우 통신량도 매우 중요한 요구사항이기 때문에 부적합하다고 할 수 있다.

본 논문에서는 이러한 이중 서명 방식의 연산량과 통신량을 줄여 무선 환경의 전자 결제방식에서도 사용가능한 효과적인 서명 방식을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 SET 프로토콜에서 사용되는 이중 서명 방식과 서명과 암호화를 함께 수행하는 Signcryption방식에 대해서 알아보며, 3장에서는 Signcryption을 이용한 효과적인 이중서명 방식을 제안한다. 4장에서는 제안한 서명 방식의 안전성을 분석하며, 결론에서 활용분야에 대해서 논한다.

Ⅱ. 배경 이론

2.1 이중 서명 방식

이중 서명 방식은 지불 브로커 시스템인 SET에서 처음으로 사용한 서명 방식으로 사용자의 프라이버시 보장을 목적으로 하고 있다. 이중 서명의 개념은 사용자의 지불 정보(신용카드 번호 등)는 상점에 노출되지 않고, 사용자의 주문 정보는 은행에 노출되지 않게하여 사용자의 프라이버시를 지켜주는 것이다. 이를 위해 SET(Secure Electronic Transaction) 프로토콜에서는 사용자의 지불 정보와 주문 정보를 각 객체의 공개키로 암호화 한 후, 각 정보의 해쉬값을 연접하여 함께 서명하는 방법을 사용하고 있다. SET 프로토콜의 이중 전자 서명 과정은 다음과 같다.

■ 파라미터 설정

- L : 상점에 전달하고자 하는 상품 내역 정보
- P : 은행에 전달하고자 하는 지불 정보
- $h(\cdot)$: 일방향 해쉬 함수
- $E_M(\cdot)$: 상점의 공개키를 이용한 암호화
- $E_B(\cdot)$: 은행의 공개키를 이용한 암호화
- $S_M(\cdot)$: 상점의 비밀키를 이용한 서명
- $S_B(\cdot)$: 은행의 비밀키를 이용한 서명

■ 이중 서명 프로토콜

• 서명 생성

① 사용자의 상품 내역 정보(L)는 상점의 공개키로 지불 정보(P)는 은행의 공개키로 암호화 한다.

$$E_M(L),\ E_B(P)$$

② 상품 내역 정보(L)와 지불 정보(P)의 해쉬값을 구한다.

$$h(L),\ h(P)$$

③ ②의 해쉬값들을 연접하여 사용자의 비밀키로 서명한다.

$$S_u(h(L)||h(P))$$

• 서명 전송

①에서 암호화한 두 개의 정보를 연접하고, 상품 내역 정보(L)와 지불 정보(P)의 해쉬값과 두개의 해쉬값을 연접하여 사용자의 비밀키로 연접한 해쉬값을 서명하여 보낸다.

$$E_M(L)||E_B(P),\ h(L),\ h(P),\ S_u(h(P)||h(L))$$

• 서명 검증

① 전송받은 $h(L)$과 $h(P)$을 이용해서 서명을 검증한다.

② 상점은 자신의 비밀키 $E_M(L)$를 복호화 하여 L을 확인한다.

③ 은행은 ①과 마찬가지로 서명을 검증한다.

④ 은행은 자신의 비밀키로 $E_B(P)$를 복호화 하여 P를 확인한다.

2.2 Signcryption 방식

Signcryption은 서명을 생성한 후 암호화를 수행하는 signature-then-encryption 방식의 비용(cost)를 줄이고자 1997년 Y. Zheng[1]에 의해제안된 방식이다.

하지만, 초기의 이 방식은 서명 검증은 지정된 수신자만이 가능한 단점 때문에 일반적인 서명 방식에 사용되는데 제약이 있다. 1998년 Bao[2]는 이러한 문제점을 보완하고자 기존의 Y. Zheng이 제안한 방식을 수정하여 누구나 검증가능한 signcryption방식을 제안하였다.

하지만 이 방식은 현재 네트워크 보안을 위해 널리 사용되고 있는 방화벽에서는 문제가 발생한다. 방화벽을 통과하기 위해서는 정당한 메시지임을 증명해야 하지만, 검증자의 비밀키 없이는 증명할 수 없기 때문이다. 이를 위해 1999년 C.Gamage[3]는 Encrypted Message Authentication by Firewalls에서 서명 검증시 평문이 필요없는 새로운 방식을 제안하였다. 본장에서는 1999년 제안된 C.Gamage의 방식을 설명한다.

■ 파라미터 설정

- p : 큰 소수
- q : $p-1$의 큰 약수
- g : $\bmod p$ 상에서 위수가 q인 정수
- $Hash(\cdot)$: 일방향 해쉬함수
- x_a : Alice의 비밀키
- x_b : Bob의 비밀키
- $y_a \equiv g^{x_a} \bmod p$: Alice의 공개키
- $y_b \equiv g^{x_b} \bmod p$: Bob의 공개키

Alice가 Bob에게 보내고자 하는 메시지에 대한 signcryption 생성 과정은 다음과 같다.

■ C.Gamage의 signcrypion 방식

• 서명 생성

$x_R \in \{1, \ldots, q-1\}$

$$k = Hash(y_b^x \bmod p) \quad (1)$$

$$y \equiv g^x \bmod p \quad (2)$$

$$c = E_k(m) \quad (3)$$

$$r = hash(y, c) \quad (4)$$

$$s \equiv \frac{x}{r + x_a} \bmod q \quad (5)$$

서명자는 위의 연산을 수행하여 생성한 (c, r, s)를 수신자에게 전송한다. 방화벽에서는 서명자로부터 전송 받은 정보로부터 y 값을 계산하여 방화벽에서는 서명의 정당성을 검증한다. 방화벽에서의 서명 검증 과정은 다음과 같다.

• 방화벽에서 서명 검증

$$y \equiv (y_a g^r)^s \bmod p \quad (6)$$

$$r ? = hash(y, c) \quad (7)$$

방화벽상에서의 서명 검증 후, 서명이 정당하지 않다면 서명문은 방화벽을 통과할 수 없으며, 서명이 정당하다면, 서명문은 수신자에게 전달되고 수신자는 자신의 비밀키를 이용하여 세션키를 구성하고 암호화된 메시지를 복호화해서 원래의 메시지를 얻을 수 있다.

• 서명 검증

$$y \equiv (y_a g^r)^s \bmod p \quad (8)$$

$$k = hash(y^{x_b} \bmod p) \quad (9)$$

$$m = D_k(c) \quad (10)$$

방화벽에서는 평문이 아닌 암호문 자체로 서명 검증이 가능하다.

Ⅲ. 제안하는 이중 서명 방식

제안하는 이중 서명 방식은 기존 방식에 비해 다항식의 값을 구하는 간단한 연산만으로 메시지를 복호화 할 수 있다는 장점이 있다. 이를 위해 지불 정보와 상품 내역 정보를 이용한 일차다항식을 생성한다. 각 객체는 생성된 다항식에 자신의 비밀키를 대

입시키므로 자신에게 허용된 메시지를 얻을 수 있다. 서명자는 생성된 다항식에 한번의 서명만을 수행하며, 기존의 방식과 같이 추가적인 통신 절차가 필요하지 않기 때문에 효과적인 서명 방식이라 할 수 있다.

제안하는 이중 서명 방식은 타원곡선 암호 방식에 기반하기 때문에 다음과 같이 파라미터를 설정한다.

■ 파라미터 설정

- E : $GF(p)$ 상의 타원곡선
- G : E(타원곡선) 위의 기본점
- n : 기본점 G의 위수 (즉, $nG=0$)
- P : 은행에 보내고자 하는 지불 정보
- L : 상점에 보내고자 하는 상품 내역 정보
- x_M : 상점의 비밀키 (단, $x_M \in_R \{2,3,\ldots,n-1\}$)
- x_B : 은행의 비밀키 (단, $x_B \in_R \{2,3,\ldots,n-1\}$)
- x_U : 사용자의 비밀키 (단, $x_U \in_R \{2,3,\ldots,n-1\}$)
- $Q_M = x_M G$: 상점의 공개키
- $Q_B = x_B G$: 은행의 공개키
- $Q_U = x_U G$: 사용자의 공개키
- $Hash(\cdot)$: 해쉬함수
- XOR : eXclusive-OR 연산
- $\pi(P)$: 점 P의 x좌표

■ 제안하는 Signcryption 방식

• Signcryption 생성

- 선택 $x \in_R \{2,\ldots,n-1\}$
- 계산 $\Pi = Hash(xG)$
- 계산 $A_i = \frac{(P-L)G}{Q_B - Q_M}$, $B_i = \frac{-PQ_M + LQ_B}{Q_B - Q_M}$
- 계산 $\pi(A_i)$, $\pi(B_i)$
- $r = (\pi(A') \| \pi(B'))\ XOR\ \Pi$
  ($A' = Hash(\pi(A_1) \| \pi(A_2) \| \ldots \| \pi(A_i))$
  $B' = Hash(\pi(B_1) \| \pi(B_2) \| \ldots \| \pi(B_i))$)
- $s = \frac{rx - r - 1}{x_U + 1} \mod n$

제안하는 방식은 기존의 signcryption 방식에 비해 상대적으로 메시지의 복호화 과정이 간단하기 때문에 서명 생성 과정의 안전성을 고려해야 한다.

먼저 서명 생성 과정에서는 보내고자 하는 메시지의 크기를 고려해야 한다. 이 경우 P와 L의 크기는 위수 n보다 크기 때문에 보내고자 하는 메시지를 n 크기만큼 나눠야 한다. 즉 P와 L은 실제로 n의 크기에 따라 $P_1, P_2, \ldots, P_i$와 $L_1, L_2, \ldots, L_i$로 나눠지기 때문에 생성되는 A, B 또한 $A_1, A_2 \ldots A_i$, $B_1, B_2 \ldots B_i$로 i개가 생성된다. 본 논문에서는 이렇게 생성된 i개의 메시지에 대해서 하나의 서명을 생성하기 위해서 A', B'를 사용한다. A', B'는 생성된 $\pi(A), \pi(B)$의 모든 메시지 블록을 연접한 값의 해쉬값을 말한다.

사용자는 자신이 생성한 $\pi(A_i), \pi(B_i), r, s$를 상점에 전송한다. 전송 과정에서 $\pi(A_i) = \pi(\frac{(P-L)G}{Q_B - Q_M})$를 공개 채널상에서 전송하여도 타원곡선 암호 방식은 A_i, G, Q_A, Q_B를 통해서 $(P-L)$을 구하기 힘든 이산대수 문제이기 때문에 안전하고, $\pi(B_i) = \pi(\frac{-PQ_M + LQ_B}{Q_B - Q_M})$ 역시 B_i, Q_M, Q_B가 공개되어도 $-P$나 L을 구하기 힘든 이산대수 문제이기 때문에 안전하다.

만약 상점에 접근하기 위해서 방화벽(Firewall)을 통과해야 한다면, 제안된 서명은 검증자의 비밀키나 평문 없이도 서명의 정당성을 검증될 수 있다.

• 방화벽에서의 서명 검증

- 계산 $X = \frac{1+r+s}{r} G + \frac{s}{r}$

$$= \frac{1+r+s}{r} G + \frac{s}{r} x_U G$$

$$= \frac{G}{r}\{(1+r) + s(1+x_U)\}$$

$$(\leftarrow \text{대입} : s = \frac{rx - r - 1}{x_U + 1})$$

$$= \frac{G}{r}(1 + r + rx - r - 1) = xG$$

- 계산 $\Pi = Hash(X)$
- 서명 검증 $r \stackrel{?}{=} (\pi(A') \| \pi(B'))\ XOR\ \Pi$

방화벽에서 서명의 정당성이 검증되면 상점에서는 전송받은 $\pi(A), \pi(B)$를 이용해서 다항식을 생성한다. 상점과 은행의 복호화 과정은 각각 다음과 같다.

• 상점의 메시지(L) 복호화

- 다항식 생성 $F(T) = \pi(A)T + \pi(B)$

$$(\leftarrow \text{대입} : A = \frac{(P-L)G}{Q_B - Q_M}, B = \frac{-PQ_M + LQ_B}{Q_B - Q_M})$$

$$F(T) = \pi(\frac{(P-L)G}{Q_B - Q_M})T + \pi(\frac{-PQ_M + LQ_B}{Q_B - Q_M})$$

〔표 1〕 제안하는 방식의 특징

	기존의 dual signature scheme	제안하는 dual signature scheme	분석
연산량	생성 : 3 modular exponentiation	생성 : 3 scalar multiplication	modular exponentiation에 비해 scalar multiplicaton의 연산 속도가 더 빠름
	검증 : 2 modular exponentiation	검증 1 multiplication on Finite Field	mudular exponentiation에 비해 유한체 상의 multiplicaton은 매우 빠름
통신량	RSA $\|2H(\cdot)\|+4\|n\|$ (단, $n=1024$)	$\|H(\cdot)\|+3\|n\|$ (단, $n=160$)	RSA에 비해 약 14%
	ElGamal $\|2H(\cdot)\|+4\|q\|$ (단, $q=160$)		ElGamal에 비해 약 66%
특 징	• 연산량과 통신량의 감소 • 메시지 복호화의 간소화 • 분쟁 발생시 기존 서명방식의 문제점 해결		

- 다항식에 상점의 비밀키 x_M 대입

$$F(x_M)=\pi(\frac{(P-L)G}{Q_B-Q_M})\cdot x_M+\pi(\frac{-PQ_M+LQ_B}{Q_B-Q_M})$$
$$=\pi\{\frac{1}{Q_B-Q_M}(PQ_M-LQ_M-PQ_M+LQ_B)\}$$
$$=\pi[\frac{1}{Q_B-Q_M}\{L(Q_B-Q_M)\}]=L$$
$$\therefore\ F(x_M)=L$$

• 은행의 메시지(B) 복호화

- 다항식 생성 $F(T)=\pi(A)T+\pi(B)$

$$(\leftarrow\text{대입}: A=\frac{(P-L)G}{Q_B-Q_M},\ B=\frac{-PQ_M+LQ_B}{Q_B-Q_M})$$
$$F(T)=\pi(\frac{(P-L)G}{Q_B-Q_M})T+\pi(\frac{-PQ_M+LQ_B}{Q_B-Q_M})$$

- 다항식에 은행의 비밀키 x_B 대입

$$F(x_B)=\pi(\frac{(P-L)G}{Q_B-Q_M})\cdot x_B+\pi(\frac{-PQ_M+LQ_B}{Q_B-Q_M})$$
$$=\pi\{\frac{1}{Q_B-Q_M}(PQ_B-LQ_B-PQ_M+LQ_B)\}$$
$$=\pi[\frac{1}{Q_B-Q_M}\{P(Q_B-Q_M)\}]=P$$
$$\therefore\ F(x_B)=P$$

■ 제안한 Signcryption 방식의 특징

제안한 이중 서명 방식은 타원곡선 암호 방식과 signcryption 방식을 이용하여 연산 속도를 향상시켰으며, 보내고자 하는 메시지를 하나의 일차 함수로 표현하여 통신량을 감소시켰다. 상점과 은행의 허가된 메시지 복원하기 위해 일차 다항식의 값만을 구하면 되기 때문에 메시지 복원이 매우 간소화되었으며, 기존 이중 서명 방식에서 나타났던 분쟁시 발생할 수 있는 서명의 문제를 해결하였다.

• 연산 속도의 향상

사용자는 signcryption 생성시 3번의 스칼라 멀티플리케이션(scala multiplication) 연산을 수행한다. 이에 반해 상점과 은행은 메시지 복원시 스칼라 멀티플리케이션 연산 없이 한번의 유한체상의 곱셈 연산만을 수행한다. 이는 메시지 복호시 기존에 제안된 방식들에 비해 매우 빠르다. 또한 제안된 방식은 타원곡선 암호 방식을 기반으로 수행되기 때문에 기존의 RSA나 ElGamal방식에 비해서도 상대적으로 연산 속도가 빠른다.

• 통신량의 감소

기존에 소개된 이중 서명 방식은 각각 메시지의 암호문과 해쉬값, 서명값이 전송되기 때문에 전송되는 메시지는 RSA 방식의 경우 $|2H(\cdot)|+4|n|$ (단, $n=1024$)이고, ElGamal 방식의 경우 $|2H(\cdot)|+4|q|$ (단, $q=160$)이다.

본 논문에서 제안된 방식은 $|H(\cdot)|+3|n|$ (단, $n=160$)이기 때문에 ElGamal 방식에 비해서도 약 40%의 통신량이 감소되었다.

• 메시지 복호화의 간소화

제안된 방식은 메시지 복호화시 객체의 비밀키를 다항식에 대입하여 일차 다항식의 값을 구하기 때문에 유한체상의 곱셈 연산만으로도 허용된 메시지의

복호화가 가능하다. 특히 상점과 은행의 다른 두 객체에서 동시에 메시지를 복호화 하고자 할때 같은 다항식에 각각 객체의 비밀키값을 대입하여 허용된 정보를 얻기 때문에 메지시 복호화가 매우 간단하다.

• 분쟁 발생시 기존 서명 방식의 문제 해결

SET 프로토콜에서 이중 서명 방식은 각각 정보의 해쉬값을 구해 연접하여 서명을 생성한다. 그렇기 때문에, 이 서명 방식은 분쟁 발생시 분쟁의 원인이 지불정보(P)인지 상품 내역 정보(L)인지 판단하기가 모호하다. 이를 보완하기 위해 본 논문의 서명 방식에서는 서명에 사용된 A, B 정보를 모두 확인할 수 있기 때문에 서명의 분쟁 발생시 문제의 원인을 판별하는데 용이하다.

Ⅳ. 제안한 Signcryption 방식의 안전성 분석

본 장에서는 제안된 signcryption 방식이 전자서명의 조건과 암호화의 조건의 안전성을 분석한다.

■ 전자서명의 안전성 분석

- **위조 불가(unforgeable)** 본 서명 방식은 서명 s 생성시 사용자의 비밀키 x_U를 사용하기 때문에 합법적인 사용자만이 서명을 생성할 수 있다.
- **사용자 인증(user authentication)** 기존의 signcryption 방식과 다르게 본 방식은 서명 검증시 검증자의 비밀키가 필요하지 않기 때문에 서명 생성자의 공개키를 이용해서 누구든지 서명 검증이 가능하고, 사용자를 인증할 수 있다.
- **부인 불가(nonrepudiation)** 본 서명 방식은 서명 생성시 사용자의 비밀키 x_U를 사용하기 때문에 사용자만이 합법적인 서명을 생성할 수 있다. 만약 서명자가 서명을 부인 할 경우 별도의 특수서명인 부인 방지 서명을 이용해서 서명의 부인을 방지할 수 있다.
- **변경 불가(unalterable)** 서명 생성시 문서 내용이 함께 계산되기 때문에 만약 서명 후 문서의 내용을 바꾸면 원래의 서명값과 같지 않은 서명값이 생성된다. 그렇기 때문에 서명 생성후 문서의 변경은 불가능하다.
- **재사용 불가(not reusable)** 문서의 서명 생성시 서명 생성자의 비밀키와 문서의 내용이 함께 계산되기 때문에 생성된 서명값을 다른 문서의 서명으로 재사용이 불가능 하다.

■ 암호화의 안전성 분석

- **무결성(message integrity)** 서명 검증시 전송받은 A_i, B_i, r, s를 이용하여 서명을 검증하기 때문에 전송된 메시지의 무결성을 확인할 수 있다.
- **기밀성(Confidentiality)** 메시지의 복호화시 각 객체의 비밀키를 대입하기 때문에 정당한 비밀키를 가지고 있는 객체만 허용된 메시지를 얻을 수 있다.

Ⅴ. 결 론

본 논문에서는 전자 결제 시스템의 대표적인 브로커 시스템인 SET 프로토콜에서 사용되고 있는 이중 서명 방식을 개선하고자 하였다. 연산의 효율성을 위해서 타원곡선 암호 방식에 기반한 signcryption 방식을 이용하였으며, 네트워크상의 방화벽에서도 검증자의 비밀키나 원래의 메시지 없이도 서명의 정당성을 검증할 수 있게 하였다.

제안한 방식은 메시지 복호시 연산의 효율성을 위해서 보내고자 하는 두 개가 메시지를 이용하여 다항식을 생성하였다. 생성한 다항식을 이용해서 메시지의 복호시에 객체의 비밀키를 대입하여 간단히 메시지를 복원할 수 있다. 이는 무선 환경에서 사용되기에 적합하다고 생각된다. 제안하는 방식을 역으로 사용하여 두 개의 메시지에 대한 signcyrption의 생성은 유선 단말기에서 수행하고, 서명의 검증을 무선 단말기에서 수행한다면, 매우 효과적일 것으로 기대된다. 무선 단말기의 제약을 극복하기 위해 한 번의 스칼라 멀티플리케이션으로도 메시지의 복호화가 가능하기 때문이다.

본 서명 방식은 향후 연구를 통해 여러개의 메시지를 하나의 다항식으로 생성하여, 한번의 서명으로 여러 객체에게 각각의 필요한 메시지를 전달 할 수 있는 서명 방식으로 발전시킬 수 있을 것이다. 이러한 서명 방식은 멀티 유저(multi-user)를 대상으로 하는 현대의 많은 인터넷 환경에 응용되기에 적합하다.

참 고 문 헌

[1] Yuliang Zheng, "Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)", CRYPTO'97, 1997.

[2] Feng Bao and Robert H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key", PKC'98, 1998.

[3] Chandana Gamage, Jussipekka Leiwo, and Yuliang Zheng, "Encyrpted Message Authentication by Firewalls", PKC'99, 1999.

[4] Moonseog Seo and Kwangjo Kim, "Electronic Funds Transfer Protocol Using Domain-Verifiable Signcryption Scheme", ICISC'99, 1999.

[5] Dae Hyun Yum and Pil Joong Lee, "New signcryption schemes based on KCDSA", ICISC 2001, 2001.

[6] 홍종국, 이임영, "타원곡선을 이용한 Proxy-Signcryption 방식", 2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호, 2002.

[7] Atsuko Miyaji, "A message recovery signature scheme equivalent to DSA over elliptic curves", ASIACRYPT'96, 1996.

[8] ISC/CD 15946-4, "Digital signatures giving message recovery", 2001.

[9] IEEE P1363a/D2, Standard Specifications for Public Key Cryptography, 2000.

[10] Kaisa Nyberg and Rainer A. Rueppel, "Message Recovery for signature Schemes Based on the Discrete Logarithm Problem", Eurocrypt '94, LNCS 950, pp.182~193.

[11] "External Interface Guide to SET Secure Electronic Transaction", Visa, MasterCard, 1997.9.24.

[12] "SET Secure Electronic Transaction LLC", www.setco.ore, 1999.7.

[13] IEEE P1363a/D2, Standard Specifications Public Key Cryptography, 2000.

〈著者紹介〉

김 근 옥 (Keun-Ok Kim) 학생회원
2002년 2월 : 서울여자대학교 수학과 졸업(이학사)
2002년 3월~현재 : 성균관대학교 정보통신공학부 석사 과정

남 정 현 (Jung-Hyun Nan) 학생회원
1997년 2월 : 성균관대학교 정보공학과 졸업(공학사)
2002년 5월 : M.S. Computer Science, University of Louisiana at Lafayette
2003년 3월~현재 : 성균관대학교 정보통신공학부 박사과정

김 승 주 (Seung-Joo Kim) 정회원
1994년 2월 : 성균관대학교 정보공학과 졸업(공학사)
1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사(암호학 전공)
1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사(암호학 전공)
1998년 12월 ~ 현재 : 정보보호진흥원(KISA) 암호기술팀장
2000년 6월 ~ 현재 : 한국정보통신기술협회(TTA) 정보통신기술위원회 암호기술연구반 의장
2002년 4월 ~ 현재 : 한국정보통신기술협회 국제 표준화 전문가

원 동 호 (Dongho Won) 정회원
성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~1999년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호인증기술연구센터장, 성균관대학교 연구처장