전자지불시스템에서 사용 가능한 효율적인 메시지 복호화를 제공하는 EC-Signcryption에 관한 연구

김수연*, 김근옥*, 이승우*, 김현주*, 원동호*

*성균관대학교, 컴퓨터공학과

A Study on EC-Signcryption providing efficient message decryption for Electronic Payment System

Sooyeon Kim*, Keunok Kim*, Seungwoo Lee*, Hyunjue Kim*, Dongho Won*

*Department of Computer Engineering, Sungkyunkwan Univ.

요 약

최근 전자상거래의 발달로 전자화폐의 사용이 증가하고, 이에 전자결제의 안전한 처리를 위한 전자서명의 생성 및 검증과 메시지의 암호화와 복호화 등의 효율적인 연산이 필요하게 되었다. 더욱이 전자상거래가 무선통신 환경으로 확대되며, 적은 메모리 용량을 사용해서 빠른 연산을 수행하고, 적은 통신량을 보장해야 하는 요구사항 등이 증가함에 따라, 이러한 제약사항을 지원할 수 있는 방식이 요구된다. 이러한 전자상거래의 전자지불시스템의 제약사항은 메시지 인증과 은닉성을 동시에 효율적으로 제공하면서 계산량과 통신비용을 줄인 기법인 signcryption 개념과 계산상 효율적인 ECC 기반의 연산을 수행하여 해결 가능하다. 본 논문에서는 기존의 signcryption 방식을 분석하고 문제점을 도출하여, 통신의 각 객체의 비밀정보를 사용한 일차 다항식으로 메시지 복호화를 제공하는 효율적인 EC-Signcryption 방식을 제안한다.

I. 서론

인터넷의 사용이 급격히 증가하면서 전자상거래, 인터넷 서비스 등 네트워크를 이용한 사업들이 증가함에 따라, 기존의 지불 방식으로는 물리적 위치에 상관없이 쉽게 접근해서 빠른 시간에 거래하기가 힘들다는 문제점이 발생했다. 이에 네트워크를 통해 돈을 지불할 수 있는 새로운 방법인 전자지불시스템이 등장했다. 그러나 현재 대부분의 전자상거래에서 이용되고 있는 온라인 입금이나 신용카드를 결제수단으로 한 경우에는, 권한이 없는 자의 접근과 침입, 정보공개 등이 쉬워짐으로써, 사용자의 익명성이 저해되고 프라이버시가 침해될 수 있다. 따라서, 전자상거래가 널리 수용되고 보편화되어 그 효율을 높이기 위해서는 네트워킹 기술 및 정보 과부하 문제가 해결되어야 함은 물론이고, 서비스 및 상품 대금을 지불할 때 사용할 수 있는 안전하고 편리한 전자결제시스템이 구축, 운영되어야 한다. 전자화폐는 기존 실물화폐의 장점 중 익명성, 디지털 정보화, 재사용 불가능성, 오프라인성, 양도 가능성, 분할 이용 가능성, 부정 사용자의 익명성 취소 등의 요구사항을 만족해야 한다. 특히, 전자화폐의 익명성은 현금 사용시에는 요구되지 않았지만, 전자화폐 발생시 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. 현재 이용되고 있는 디지털 서명이나 공개키 암호 방식은 모두 모듈러 멱승과 같은 많은 계산량을 요구하므로 상대적으로 적은 계산 능력을 가진 휴대용 단말기나, 무선통신상에서는 사용하기 어려운 점이 있다. 이러한 문제점을

해결하고자 본 논문에서 제안하는 방식은, 다항식의 값을 구하는 간단한 연산을 적용하여 효율적으로 메시지를 쉽게 복호화 하므로 연산량과 통신량이 줄어든다. 또한, 생성된 다항식에 각 객체의 비밀정보를 대입시키므로 자신에게만 허용된 메시지를 얻을 수 있다는 특징이 있다.

본 논문의 구성은 다음과 같다. 2장에서 기존에 발표된 Y.Zheng의 signcryption 방식에 대해 살펴보고, 3장에서는 무선환경의 전자결제방식에서도 사용 가능하도록 다항식을 이용하여 연산량을 효율적으로 줄인 타원곡선상의 signcryption 프로토콜을 제안한다. 4장에서는 제안한 프로토콜의 효율성과 전자서명으로서의 안전성에 대해 분석하며, 마지막 5장에서 결론 및 향후 연구 과제에 대해 제시한다.

Ⅱ. 관련연구

1. Signcryption 방식

Signcryption 방식은 1997년 메시지의 기밀성과 인증을 제공하기 위해, 서명을 생성한 후 암호화를 수행하는 signature-then-encryption 방식의 비용을 줄이고자 두 단계의 처리과정을 한 단계로 통합하여 계산량 및 통신비용의 절감을 도모한 방식으로 Y. Zheng[1]에 의해 제안됐으며, 그 내용은 다음 그림 1과 같다.

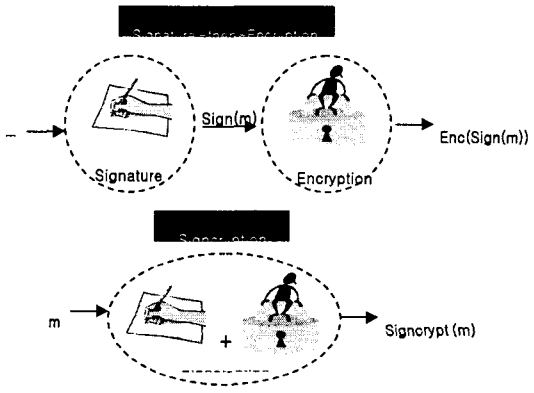

그림 1 signcryption 방식

그러나 초기의 이 방식은 서명의 검증이 지정된 수신자만 가능한 단점 때문에 일반적인 서명 방식에 사용되는데 제약이 있다. Bao와 Deng[2]은 1998년에 이러한 문제점을 보완해서 누구나 검증이 가능하도록 변형된 signcryption 방식을 제안하였다. 하지만 이 방식은 Zheng의 방식에 비해 통신량은 적절히 보장되지만, 계산량 측면에서 비효율적이다. 또한, 현재 네트워크 보안을 위해 널리 사용되고 있는 방화벽에서는 문제가 발생한다. 방화벽을 통과하기 위해서는 정당한 메시지임을 증명해야 하지만, 검증자의 비밀키 없이는 증명할 수 없기 때문이다. C.Gamage[3]는 이를 위해서 1999년 서명 검증시 평문이 필요 없는 새로운 방식을 제안하였다. 본 장에서는 초기에 발표된 Y. Zheng에 의해 제안된 signcryption 방식에 대해 설명한다.

2. Y.Zheng의 signcryption

1) 파라미터 설정

- p : 큰 소수
- q : $p-1$의 큰 약수
- g : mod$p$ 상에서 위수가 q인 정수
- $Hash(\cdot)$: 일방향 해쉬함수
- $KH(\cdot)$: keyed-해쉬함수
- $E(\cdot)$: 대칭키 암호화함수
- $D(\cdot)$: 대칭키 복호화함수
- $k_1 \| k_2$: k_1과 k_2의 연접
- x_a : 사용자 A의 비밀키
- x_b : 사용자 B의 비밀키
- $y_a \equiv g^{x_a} \bmod p$: 사용자 A의 공개키
- $y_b \equiv g^{x_b} \bmod p$: 사용자 B의 공개키

사용자 A가 사용자 B에게 보내고자 하는 메시지에 대한 signcryption 생성 과정은 다음과 같다.

2) Signcryption 생성

사용자 A는 랜덤 비밀 값 x와 사용자 B의 공개키 $y_b \equiv g^{x_b} \bmod p$를 이용하여 세션키 k를 생성한다. 그 후, 그 세션키 k를 k_1과 k_2로 분리하고, 각각 암호화키와 keyed-해쉬함수의 키로 사용한다. 사용자 A는 랜덤 비밀 값 x, keyed-해쉬 값 r, 그리고 자신의 비밀키 x_a를 이용하여 법 q상에서 서명 값 s를 생성하여, (c, r, s)를 사용자 B에게 전송한다.

$$x_R \in \{1,2,\ldots,q-1\} \quad (1)$$

$$k = Hash(y_b^{x} \bmod p) \quad (2)$$

$$k_1 \| k_2 = k \quad (3)$$

$$c = E_{k_1}(m) \quad (4)$$

$$r = KH_{k_2}(m) \quad (5)$$

$$s \equiv \frac{x}{r + x_a} \bmod q \quad (6)$$

3) Unsigncryption

(c, r, s)을 수신받은 사용자 B는 사용자 A의 공개키 $y_a \equiv g^{x_a} \bmod p$와 자신의 비밀키 x_b를 이용하여 세션키 k를 계산하고, 암호화된 메시지 c를 복호화하여, 메시지에 대한 서명 검증을 실시한다.

$$y = (y_a g^{r})^{s} \bmod p \quad (7)$$

$$k = hash\,(y^{x_b} \bmod p) \quad (8)$$

$$k_1 \| k_2 = k \quad (9)$$

$$m = D_{k_1}(c) \quad (10)$$

$$KH_{k_2}(m) = r \quad (11)$$

Ⅲ. 제안하는 EC-Signcryption방식

본 논문에서는 기존 signcryption 방식에 비해서 다항식의 값을 구하는 간단한 연산을 함으로써 unsigncryption이 가능한 새로운 EC-Signcryption 방식을 제안한다. 이 방식은 연산 능력이 높은 유선 단말기와 상대적으로 연산 능력이 낮은 무선 단말기 사이의 통신에 매우 유용하게 사용될 수 있다. 서버 S는 사용자 A와 사용자 B에게 각각의 비밀정보를 보내고자 한다. 이런 경우 기존 방식에서는 각각의 객체에게 보낼 정보를 생성하여 전송하게 되고, 이 과정에서 사용자가 증가하면, 서버 S가 생성하는 메시지의 양도 함께 증가하는 단점이 있다. 본 논문에서 제안하는 방식은 사용자 A와 사용자 B에게 각각 보내는 비밀정보를 이용하여 다항식을 생성하고, 이를 이용하여 signcryption을 생성함으로써 객체의 수가 증가해도 메시지의 수는 증가하지 않는 장점이 있고, 또한 동일한 메시지에 각 사용자만이 아는 비밀정보를 이용해서 인가된 메시지만을 unsigncryption 할 수 있기 때문에 통신량을 감소시킬 수 있다.

제안하는 EC-Signcryption 방식의 파라미터는 다음과 같고, 그림 2는 제안하는 EC-Signcryption 방식을 나타낸 것이다.

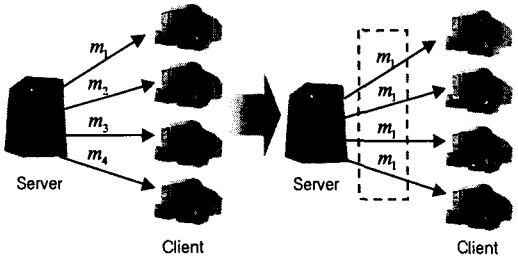

그림 2 제안하는 EC-Signcryption 방식

1. 파라미터 설정

본 논문은 타원곡선 암호를 기반으로 하기 때문에, E는 유한체 $GF(p)$ 상의 타원곡선을 의미하며, G 는 타원곡선 E상의 기본점이고, n은 기본점 G의 위수를 나타낸다. 즉, $nG = 0$이다. 서버 S가 사용자 A에게 보내고자 하는 비밀 정보는 P_A이고, 사용자 B에게 보내고자 하는 비밀 정보는 P_B이다. 사용자 A의 비밀키는 x_A이고, 사용자 B의 비밀키는 x_B, 서버 S의 비밀키는 x_S이다. 여기서 $x_A,\ x_B,\ x_S \in_R \{2,3,\ldots,n-1\}$인 값을 선택한다. 이러한 각각의 비밀키에 해당하는 사용자 A의 공개키는 $Q_A = x_A G$, 사용자 B의 공개키는 $Q_B = x_B G$, 서버 S의 공개키는 $Q_S = x_S G$이다. $Hash(\cdot)$는 해쉬함수, XOR은 eXclusive-OR 연산을 의미하며, $\pi(P)$는 점 P의 x좌표를 의미한다.

2. EC-Signcryption 생성

EC-Signcryption 생성시 사용자 A와 사용자 B에게 보낼 비밀정보를 이용해서 일차함수를 생성하고 이를 이용해서 EC-Signcryption을 생성한다.

① 서버는 $x \in_R \{2,\ldots,n-1\}$를 선택한다.

② 선택한 x를 이용해 $\Pi = Hash(xG)$를 계산한다.

③ 생성할 다항식의 일차항과 상수항의 계수를 $A = \frac{(P_A - P_B)G}{Q_B - Q_A}$, $B = \frac{-P_A Q_A + P_B Q_B}{Q_B - Q_A}$와 같이 생성한다. 즉, 생성한 다항식은

$$F(T)=\frac{(P_A-P_B)G}{Q_B-Q_A}T+\frac{-P_AQ_A+P_BQ_B}{Q_B-Q_A}$$

이다.

④ $k=h(\pi(A)\|\pi(B))$를 계산한다.

⑤ 서명 $r=k\oplus\Pi$와, $s=\frac{rx-r-1}{x_S+1} \bmod n$을 계산한다.

제안하는 방식은 기존의 서명 복호화 과정을 간단히 하기 위해 일차다항식 연산을 이용하였기 때문에, 특히 서명 생성 과정의 안전성을 고려해야 한다.

서버 S는 자신이 생성한 A,B,r,s를 사용자에게 전송한다. 전송 과정에서 $A=\frac{(P_A-P_B)G}{Q_B-Q_A}$를 공개 채널상에서 전송하여도 타원곡선 암호 방식은 A,G,Q_A,Q_B를 통해서 (P_A-P_B)을 구하기 힘든 이산대수 문제이기 때문에 안전하고, $B=\frac{-P_AQ_A+P_BQ_B}{Q_B-Q_A}$ 역시 B,Q_A,Q_B가 공개되어도 $-P_A$나 P_B을 구하기 힘든 이산대수 문제이기 때문에 안전하다.

3. 사용자의 EC-Unsigncryption

1) 사용자 A의 EC-Unsigncryption

① 사용자 A는 전송 받은 계수 A,B를 이용해서 다항식 $F(T)=AT+B$를 생성한다.

$$F(T)=\frac{(P_A-P_B)G}{Q_B-Q_A}T+\frac{-P_AQ_A+P_BQ_B}{Q_B-Q_A}$$

② 생성한 다항식에 사용자 A의 비밀키 x_A를 대입하여 $F(x_A)=P_A$를 생성한다.

2) 사용자 B의 EC-Unsigncryption

① 사용자 B는 전송 받은 계수 A,B를 이용해서 다항식 $F(T)=AT+B$를 생성한다.

$$F(T)=\frac{(P_A-P_B)G}{Q_B-Q_A}T+\frac{-P_AQ_A+P_BQ_B}{Q_B-Q_A}$$

② 생성한 다항식에 사용자 B의 비밀키 x_B를 대입하여 $F(x_B)=P_B$를 생성한다.

4. 제안하는 EC-Signcryption의 응용분야

현재 전자결제시스템 중 많이 사용되고 있는 지불 브로커 시스템의 경우, 신용카드 결제시 이용자의 구매 정보에 관한 프라이버시가 노출되기 쉽기 때문에, 전자결제시스템의 중요 요구사항인 익명성을 만족시키기가 어렵다. 이를 지키기 위해서 지불정보와 상품정보 각각에 은행과 상점 각 객체의 공개키로 암호화 한 후, 두 정보의 해쉬값을 연접하여 서명을 수행하는 방식을 사용하고 있다. 이 방식은 사용자의 지불정보와 상품내역 정보를 숨기기 위한 가장 일반적인 방법이다. 하지만, 사용자는 공개키 암호방식을 이용해서 각각의 정보를 암호화하기 때문에 연산 부담이 매우 크다. 그리고, 각 정보의 해쉬값을 연접해서 서명을 수행하기 때문에 만약 분쟁이 발생할 경우, 사용자의 지불정보와 상품정보 중 어떠한 문제인지 판별하기 어렵다. 또한, 각각의 정보를 암호화한 암호문 두 개를 연접하고 각각의 해쉬값과 서명값을 모두 상점에 전송해 주기 때문에 통신량이 매우 많다. 유선 환경에서는 통신량이 큰 문제가 되지 않을 수 있지만, 현재 그 수요가 증가하고 있는 무선 환경의 경우 통신량도 매우 중요한 요구사항이기 때문에 부적합하다고 할 수 있다.

본 논문에서 제안하는 EC-Signcryption 방식은 기존 방식에 비해 일차 다항식의 값을 구하는 간단한 연산만으로 메시지를 복호화 할 수 있다는 장점이 있다. 전자지불시스템에 EC-Signcryption을 적용하면, 상점과 은행의 허가된 메시지를 복호화 하기 위해 일차 다항식의 값만 구하면 되기 때문에 메시지의 복호화가 매우 간소화 될 수 있다.

또한, 제안하는 EC-Signcryption 사용시 기존방식보다 연산속도가 향상된 전자지불시스템을 설계할 수 있다. 사용자는 signcryption 생성시 3번의 스칼라 멀티플리케이션 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. 제안된 방식은 연산량과 통신량이 줄어들기 때문에, 무선 환경의 전자결제시스템에서도 사용 가능한 효과적인 서명 방식이다.

Ⅳ. 제안한 EC-Signcryption 방식의 안전성

본 장에서는 제안된 EC-Signcryption 방식이 전자서명의 조건과 암호화에 필요한 조건을 만족시키고 있는지에 대한 안전성을 분석한다.

1. 전자서명의 안전성 분석

본 서명 방식은 서명 s 생성시 서버 S의 비밀키 x_S를 사용하기 때문에 합법적인 사용자만이 서명을 생성할 수 있는 위조 불가(unforgeable)의 성질을 만족시키며, 기존의 signcryption 방식과 다르게 본 방식은 서명 검증시 검증자의 비밀키가 필요하지 않기 때문에 서명 생성자의 공개키를 이용해서 누구든지 서명 검증이 가능하고, 사용자를 인증할 수 있는 사용자 인증(user authentication)을 제공한다.

또한, 서명 생성시 문서 내용이 함께 계산되기 때문에 만약 서명 후 문서의 내용을 바꾸면 원래의 서명값과 같지 않은 서명값이 생성된다. 그렇기 때문에 서명 생성 후 문서의 변경은 불가능한 변경 불가(unalterable)의 성질과 문서의 서명 생성시 서명 생성자의 비밀키와 문서의 내용이 함께 계산되기 때문에 생성된 서명값을 다른 문서의 서명으로 재사용이 불가능한 재사용 불가(not reusable) 성질을 만족한다.

2. 암호화의 안전성 분석

서명 검증시 전송 받은 A, B, r, s를 이용하여 서명을 검증하기 때문에 전송된 메시지의 무결성을 확인할 수 있고, 메시지의 복호화시 각 사용자의 비밀키를 대입하기 때문에 정당한 비밀키를 가지고 있는 사용자만 허용된 메시지를 얻을 수 있기 때문에 기밀성(confidentiality)을 만족한다.

V. 결론 및 향후 연구 과제

전자상거래가 급속도로 발전함에 따라 기밀성, 인증 및 부인봉쇄 등과 같은 문제를 해결하기 위해 공개키 암호 방식이 가장 많이 사용되고 있다. 최근 무선환경에서의 전자결제가 증가하며, 지불시 사용되는 무선단말기 등의 연산 속도와 통신량을 고려한 프로토콜의 필요성이 대두되었다.

본 논문에서는 기존 암호방식보다 빠른 속도와 적은 통신량의 조건을 만족하기 위해서, 서명과 암호화를 함께 함으로써 상대적으로 계산 능력이 뛰어난 서버에 의존하여 암호화 및 서명을 생성하므로 비용과 시간을 줄일 수 있는 signcryption 방식을 사용하였다. 또한, 연산 속도를 줄이고, 기존의 RSA 암호방식보다 키의 길이를 짧게 하기 위해서 타원곡선 기반의 연산을 수행했으며, 다항식의 사용으로 연산량을 줄였기 때문에 계산비용을 절감할 수 있는 서명 방식을 제안하였다. 제안된 signcryption 방식은 타원곡선 암호방식과 기존의 signcryption 방식을 이용하여 연산 속도를 향상시켰으며, 보내고자 하는 메시지를 하나의 일차 함수로 표현하여 통신량을 감소시켰다. 각 통신 객체의 허가된 메시지를 복원하기 위해서는, 일차 다항식의 값만을 구하면 되기 때문에 메시지의 unsigncryption시에 계산량이 매우 적다.

본 논문의 EC-Signcryption은 서명 생성과 검증시 연산 과정에 대한 효율성 면에서 뛰어나기 때문에, 무선환경의 단말기나 스마트 카드, 보안 모듈 등을 사용한 전자상거래에 응용하여 유용하게 사용될 수 있을 것이다. 향후, 제안하는 signcryption 방식을 적용한 전자지불시스템을 개발하여 효율성과 경제성이 고루 갖춰진 이상적인 전자결제시스템에 대한 연구가 필요하다.

참고문헌

[1] Yuliang Zheng, "Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)," Advances Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

[2] Feng Bao and Robert H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key," Proc. of PKC'98, Springer-Verlag, pp. 55-59, 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] Atsuko Miyaji, "A message recovery signature scheme equivalent to DSA over elliptic curves," ASIACRYPT'96, 1996

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

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

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