무선환경에 적합한 효율적인 타원곡선 기반의 Signcryption 방식

*김근옥, 오수현, 원동호

*성균관대학교 정보통신공학부

A Study on an Efficient Signcryption scheme based on Elliptic Curves for Wireless Environment

*Keun-Ok Kim, Soohyun Oh Dongho Won

*School of imformation and communication Engineering, Sungkyunkwan University

요 약

무선 통신의 발달로 무선 단말기 상에서 서명 생성 및 검증과 메시지의 암호화와 복호화 등의 연산의 필요성이 대두되었다. 하지만, 무선 통신이라는 특성상 적은 메모리 용량을 사용해서 빠른 연산을 수행하고, 적은 통신량을 보장해야 한다. 이러한 무선 단말기의 제약사항은 서명과 암호화를 함께 하는 Signcryption 개념과 ECC 기반의 연산을 수행하여 해결할 수 있다.

또한 네트워크상에서의 정보보안을 위해 설치된 방화벽을 통과하기 위해서는 서명의 검증이 필요한데, 서명된 메시지를 암호화 해서 보낼 경우 서명 검증시 수신자의 비밀키가 있어야 메시지를 복원해서 서명을 검증할 수 있기 때문에 이 점을 보완하기 위해 본 논문에서는 서명 검증시에 평문이 필요없는 ECC 기반의 signcryption 방식을 제안한다.

I. 서론

무선 통신의 발달로 메시지의 안전한 서명과 암호화와 더불어 메시지의 연산 속도가 중요하게 대두되고 있다. 1997년 Y.Zheng[1]은 서명한 메시지에 암호화를 수행하는 signature-then-encryption 방식보다 연산 속도면에서 효율적이면서 기밀성과 인증을 동시에 제공할 수 있는 signcryption 방식을 제안하였다. 하지만, 이 방식의 경우 수신자만이 서명을 검증할 수 있다는 단점으로 인해 1998년 Bao[2]에 의해서 수정된 형태의 방식이 나오게 되었다. 그러나, 이 방식의 경우 연산의 효율성 면에서는 기존의 Y.Zheng 방식보다 떨어지므로 본 논문에서 제안하는 프로토콜에서는 ECC기반의 연산으로 효율성의 문제를 해결하고자 한다.

또한 1999년 C.Gamage[3]에 의해서 제안된 Encryted Message Authentication by Firewalls에서는 서명된 메시지가 방화벽을 통과하면서 생길 수 있는 문제에 대해서 언급하고 있다. 정보의 보호를 위해서 네트워크 상의 가장 기본적인 보안장치라고 할 수 있는 방화벽의 경우 정당한 메시지라는 검증 없이는 방화벽을 통과할 수 없다. 그렇기 때문에 방화벽을 통과하기 위해서는 방화벽 상에서 메시지의 검증이 필요한데, 암호화된 메시지에 대해 서명의 정당성을 검증하기 위해서는 수신자의 비밀키가 필요하게 되므로, 이에 따르는 문제점을 해결하고자 C.Gamage는 서명 검증시 평문이 필요없는 방식을 제안하였다.

본 논문에서는 C.Garmage가 제안한 방식을 보다 효율적으로 변형하기 위해 ECC 기반의 연산을 수행하는 프로토콜로 변형하였다.

본론의 Ⅱ장에서는 관련된 C.Garmage의 방식에 대해서 살펴보고 Ⅲ장에서는 타원 곡선 상의 signcryption 프로토콜을 제안한다. 다음으로 제안한 프로토콜의 효율성과 전자서명으로서의 안전성에 대해서 살펴본 후, 결론 및 향후 연구 방향을 제시한다.

II. 연구배경

1. C.Gamage의 signcryption 방식

본 장에서는 1999년 C.Gamage에 의해서 제안된 방화벽에서 원래 메시지의 노출없이 서명을 검증할 수 있는 방식에 대해서 설명한다. C.Gamage가 제안한 방식의 시스템 파라미터는 다음과 같이 설정한다.

1) 변수 설정

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

메시지에 대한 signcryption 생성과정은 다음과 같다.

2) 서명생성

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

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

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

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

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

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

서명을 생성한 후 (c, r, s) 를 보낸다. 방화벽에서는 서명자로부터 온 정보를 가지고 y값을 계산하여 서명의 정당성을 검증한다. 방화벽에서의 서명 검증 과정은 다음과 같다.

3) 방화벽에서 서명 검증

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

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

방화벽상에서 서명 검증을 한 후, 서명이 정당하지 않다면 서명문은 방화벽을 통과할 수없으며, 서명이 정당하다면, 서명문은 수신자에게 전달되고 수신자는 자신의 비밀키를 이용해서 송신자와의 세션키를 생성해 암호화된 메시지를 복호화해서 원래의 메시지를 얻을 수 있다.

4) 서명검증

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

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

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

방화벽에서 실제 메시지가 필요없이 암호문 자체로 서명 검증이 가능하다.

III. 제안하는 ECC 기반의 signcryption 방식

본 논문에서 제안하는 프로토콜은 무선 통신상에서 가장 중요시 여겨지고 있는 서명의 생성과 암호화 연산시 걸리는 시간의 효율성을 고려하여 타원곡선 기반의 signcryption 방식을 제안한다.. 이 방식은 C.Gamage가 제안한 것과 마찬가지로 네트워크 상의 방화벽에서 메시지의 원문이 필요없이 서명 검증이 가능하도록 설계되었다.

1. 제안하는 프로토콜

제안하는 프로토콜의 시스템 파라미터는 다음과 같이 설정한다.

1) 변수 설정

- E : $GF(q)$ 상의 곡선
- G : 곡선 위의 기본점
- n : G의 위수 (i.e. nG =0)
- d_A : A의 비밀키 $d_A \in \{2, \ldots, n-1\}$
- Q_A : A의 공개키 $d_A G = Q_A$
- d_B : B의 비밀키 $d_B \in \{2, \ldots n-1\}$
- Q_B : B의 공개키 $d_B G = Q_B$
- x : $x \in \{2, \ldots, n-1\}$에서 랜덤하게 수
- Hash (·) : 일방향 해쉬함수

ECDSA에서 정의한 변수를 사용하며, 키 값은 주로 160 비트 이상을 사용한다. 메시지에 대한 signcryption 생성과정은 다음과 같다.

2) 서명 생성

$$\Pi = Hash(xG) \quad (11)$$

$$c = E_{x_1}(M) \quad (12)$$

$$(x_1, y_1) = xQ_B \quad (13)$$

$$r = c \ XOR \ \Pi \quad (14)$$

$$s = \frac{rx - r - 1}{d_A + 1} \bmod n \quad (15)$$

타원곡선 기반의 암호시스템에서는 주요 연산이 스칼라 곱셈이기 때문에 이 연산을 줄이고자 메시지를 암호화할 때와 검증자와의 세션키를 생성할 때에만 스칼라 곱셈을 사용하였다. 또한 서명을 생성할 때 연산의 용이한 XOR연산을 사용하였다.

방화벽에서 서명을 검증하는 과정은 다음과 같다.

3) 방화벽에서 서명 검증

$$\Pi = hash\ (P) \tag{16}$$

$$P = \frac{1+r+s}{r} G + \frac{s}{r} Q_A \tag{17}$$

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

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

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

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

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

$$= xG$$

$$r = ?\ \ c\ \ XOR\ \ \Pi \tag{18}$$

방화벽에서 서명을 검증하기 위해 사용되는 연산은 두 번의 스칼라 곱셈이 사용되며, 검증시에 원래의 메시지없이 암호화된 메시지를 이용해서 서명 검증이 가능하다. 방화벽에서는 계산된 P값을 서명된 메시지와 함께 검증자에게 보내준다.

4) 서명 검증

$$c = r\ XOR\ \Pi \tag{19}$$

$$(x_1, x_2) = (P)d_A \tag{20}$$

$$D_{x_1}(c) = M \tag{21}$$

정당한 메시지를 얻기 위해서는 검증자의 비밀키를 이용해여 서명자와의 세션키를 생성해서 암호문을 복호화 할 수 있다. 세션키 생성시 방화벽으로부터 이미 계산된 P값을 받아서 자신의 비밀키만을 곱하기 때문에 연산이 훨씬 간단해 진다.

2. 제안하는 프로토콜의 효율성 분석

기존에 제안되었던 다른 프로토콜들에 비해서 본 논문에서 제안하는 프로토콜은 타원곡선 암호시스템을 기반으로 하기 때문에 통신량에 있어서도 충분히 효율적이라고 할 수 있다. 또한 기존에 2002년 4월에 발표된 Proxy-Signcryption 방식에 비해 서명 생성시와 서명 검증시에 연산량에 대해서도 효율적이다. 다음 표 1에서는 기존에 소개되었던 Signcryption 방식과 이번에 제안한 방식의 효율성을 분석하였다.

표 1 : signcryption 방식의 효율성 비교

	주요 연산량	통신량	문제점 및 보완점
Zhen	1 2	$\|KH(\cdot)\|+\|q\|$	수신자만 서명 검증
Bao	2 3	$\|KH(\cdot)\|+\|q\|$	누구나 서명 검증
Gamage	2 3	$\|KH(\cdot)\|+2\|q\|$	평문없이 서명 검증
제안된 방식	3 3	$\|KH(\cdot)\|+2\|n\|$	통신의 효율성

제안된 프로토콜은 타원곡선 연산을 기반으로 하기 때문에 기본적으로 키의 비트수가 유한체에서의 연산에 비해 작다. 예를 들면 RSA 1024 비트와 같은 안전성을 가질 수 있는 것이 타원곡선에서는 160비트 정도이다. 그렇기 때문에 같은 연산을 하더라도 RSA 1024 비트에서의 모듈리 지수승 연산과 ECC 160 비트의 스칼라 곱셈 연산은 연산 자체보다는 키 비트수 때문에 타원곡선 암호 상에서의 연산이 더 빠른 것이다. 그리am로 제안된 프로토콜은 비록 서명 생성시 주요 연산을 다른 프로토콜에 비해 한번 더 수행했지만, 다른 프로토콜의 연산보다 효율적이다. 둘째로 통신량을 살펴보면, 앞에서와 마찬가지로 타원곡선상의 연산이기 때문에 $|n|$의 값이 상대적으로 작아 통신량에 있어서도 매우 효율적이라고 할 수 있다. 또한 방화벽에서 서명 검증을 위해 생성한 결과값을 서명문과 함께 검증자에게 보내줌으로써 실질적으로 서명을 검증하는 검증자의 계산을 줄여주는 효과가 있다. 결과적으로 서명 검증자는 스칼라 곱셈연산을 한 번 수행함으로써 암호화된 메시지를 얻을 수 있다.

3. 제안하는 프로토콜의 안전성 분석

본 장에서는 제안하는 프토콜이 전자서명과 메시지 암호화에 필요한 조건을 만족시키고 있는지에 대해 분석한다.

1) 전자서명의 조건

· 위조 불가 : 서명 생성자의 비밀키인 d_A 로 서명을 생성했기 때문에, 비밀키를 모르는 다른 사람이 서명을 생성·위조할 수 없다.

· 서명자 인증 : 서명자의 공개키 Q_A가 들어가기 때문에 누구든지 서명자를 검증할 수 있다.

· 부인 불가 : 서명 생성시 서명 생성자의 비밀키를 사용했기 때문에 서명자는 자신의 서명 내용에 대해서 부인할 수 없다.

· 변경 불가 : 서명문에는 서명자의 비밀키가 들어가 있고, signcrypton의 경우 서명문이 암호화 되었기 때문에 서명된 내용을 변경할 수 없다.

· 재사용 불가 : 서명 생성시 난수인 x를 사용하였기 때문에 다른 문서의 서명으로 재사용할 수 없다.

2) 암호화 조건

· 무결성 : 원래의 메시지를 서명 검증자와 서명 생성자만이 알 수 있는 세션키로 암호화 하기 때문에 메시지의 무결성을 보장할 수 있다.

· 기밀성 : 세션키로 암호화 하기 때문에 세션키를 알지 못하는 다른 사람은 메시지의 내용을 알 수 없으므로 기밀성을 보장할 수 있다.

Ⅳ. 결론 및 향후 연구방향

무선 통신의 발달과 함께 무선 단말기 상에서의 서명 생성과 암호화 연산이 필요하게 되었다. 하지만, 무선 단말기가 갖는 제약조건 때문에 연산 속도와 통신량을 고려한 프로토콜의 필요성이 대두되었다.

본 논문에서는 위의 조건을 만족하기 위해서 첫째로 서명과 암호화를 함께 함으로써 비용과 시간을 줄여줄 수 있는 signcryption 방식과 둘째로 연산 속도를 줄이기 위해서 타원곡선 기반의 연산을 수행했으며, 마지막으로 네트워크 상의 방화벽에서도 메시지 원문없이 서명을 검증할 수 있는 방식을 제안하였다.

제안된 프로토콜의 서명 생성시와 검증시 연산 과정에 대해서 좀 더 효율성 면에서 연구가 이루어진다면, 무선 단말기나 보안 모듈 등에서 유용하게 사용될 수 있을 것이다.

참고문헌

[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