타원곡선을 이용한 Proxy-Signcryption 방식

홍종국, 이임영
순천향대학교 정보기술공학부
e-mail:siro1hope@hanmail.net, imylee@sch.ac.kr

Proxy-Signcryption Scheme Using Ellipitc Curves

Jong-kook Hong, Im-yeoung Lee
Division of Information Technology, Soon-chun-hyang University

요 약

인터넷 이용 확산과 휴대용 단말기 사용자의 증가로 무선 인터넷 서비스의 수요가 증대되고 있는 가운데 많은 응용 서비스들이 제공되고 있다. 이러한 서비스의 제공에 있어 특히, 기밀성과 인증성 그리고 안전성이 보장되어야 하며, 계산량 및 통신량에 있어 효율성이 높아야 할 것이다.

본 논문에서는 무선인터넷 서비스 제공을 고려하여 사용자 요구에 빠른 응답을 제공하고 휴대용 단말기의 계산 부담을 줄일 수 있는 타원곡선을 이용한 proxy-signcryption 방식을 제안한다.

1. 서론

컴퓨터 보급의 확산과 무선 이동 통신의 발전으로 기존 유선망을 이용하여 제공되던 많은 서비스들이 무선 인터넷을 통해 제공되고 있다. 무선 인터넷은 휴대용 단말기를 통해 무선으로 인터넷에 접속하여 데이터 통신이나 인터넷 서비스를 이용하는 것을 말하며, 넓은 의미로는 무선 LAN이나 광대역 무선 가입자망(Broadband Wireless Local Loop:B-WLL) 등 고정 무선 인터넷 서비스를 포함한다. 이러한 무선 인터넷을 통해 사용자들은 휴대용 단말기를 이용하여 증권거래, 이동 뱅킹, 전자상거래 등 다양한 멀티미디어 서비스를 제공받을 수 있다.

그러나 이러한 무선 인터넷의 이용은 즉시성과 이동성이 주는 편리함 이외에 사용자 인증 및 데이터 기밀성, 부인봉쇄 등 많은 부분에서 문제가 발생할 수 있다. 이러한 문제점은 디지털 서명과 암호화 통신을 통하여 해결할 수 있다. 그러나 이러한 방식은 묘듈러 멱승과 같은 많은 계산량을 필요로 하기 때문에 상대적으로 계산 능력이 떨어지는 휴대용 단말기에서는 사용하기가 어렵다.

이러한 문제점을 해결하기 위해 1997년 Y.Zheng에 의해 제안된 signcryption 기법은 디지털 서명과 암호를 동시에 수행하여 계산량 및 정보전송에 있어 효율성을 제공하기 위한 개념으로 확대될 수 있다.[1] 그 후 C.Gamage 등에 의해 계산량이 상대적으로 뛰어난 Agent를 이용함으로서 사용자 단말기의 계산량을 감소시킨 proxy-signcryption 방식이 제안되었으며, 이 외에도 많은 방식들이 제안되고 있다.[2]

본 논문에서는 무선인터넷 서비스 제공에 있어 사용자 요구에 빠른 응답을 제공하고 휴대용 단말기의 계산 부담을 줄일 수 있는 타원곡선을 이용한 proxy-signcrytpion 방식을 제안한다. 2장에서는 무선 인터넷 서비스에 필요한 요구사항을 살펴보고 3장에서는 타원곡선 암호와 signcryption 방식에 대해 알아볼 것이며, 4장에서 타원곡선 기반의 제안 방식을 설명한다. 마지막으로 5장에서 결론을 맺는다.

2. 요구사항 분석

본 장에서는 무선 인터넷 서비스를 고려하여 신뢰성과 효율성을 제공하기 위한 요구사항을 살펴본다.

1) 기밀성 : 무선 이동 통신을 통해 송신자가 메시지를 송신할 경우 제 3자의 도청으로부터 안전하고 정확한 방법으로 정당한 수신자에게 전송되어야 한다.
2) 인증성 : 메시지 송·수신시 출처가 누구이며, 전송 도중 불법적인 제 3자로부터 위조 및 변경되지 않았음을 보증하는 것으로서 디지털 서명 기법이 적용된다.
3) 부인 봉쇄 : 메시지의 송·수신 여부에 대하여 무선 이동 통신 당사자간에 부인은 방지되어야 한다.
4) 유효성 : 일반 네트워크에 비해 상대적으로 계산 능력이 떨어지는 무선 단말기 사용자 측면에서도 충분히 사용 가능해야 한다.
5) 안전성 : 무선 이동 통신에서 메시지 송·수신에 대한 참여개체의 위조 및 변조가 불가능해야한다.
6) Forward Secrecy : Long term key(프로토콜의 세션키를 생성하기 위해 사용되는 키)의 분실 및 노출로 인해 이전에 생성된 프로토콜의 세션키가 공개되어서는 안된다.

3. 관련 연구

3.1 타원곡선 암호

유한체 $GF(p^m)$상에서 정의된 타원곡선 군은 다음의 3차 방정식을 만족하는 순서쌍 (x, y)들과 무한원점 O을 포함한 집합이며, 이 집합은 가환군 형태를 이룬다.[3]

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$
$$(x, y, a_1, a_2, a_3, a_4, a_6) \in GF(p^m)$$

다음은 Weierstrass 형태의 타원곡선을 설명한다.

$$y2 = x3+ax+b \ (a, b \in GF(p^m))$$
$$4a^3 + 27b^2 \neq 0$$

타원곡선 상의 덧셈 연산은 다음 규칙을 따른다.

1) $O + O = O$, $P + O = P$, $P + Q = O$ (모든 $P=(x, y)$, $Q=(x, -y) \in E$)
2) $P \neq Q$일 경우의 덧셈 연산
$$P + Q = (\lambda^2 - x_1 - x_2, \ \lambda(x_1 - x_3) - y_1)$$
$$\lambda = (y^2 - y_1) / (x_2 - x_1)$$
3) $P = Q$일 경우의 덧셈 연산
$$P = (x, y) \in E, \ (y \neq O)$$
$$2P = (\lambda^2 - 2x, \ \lambda(x - (\lambda^2 - 2x)) - y)$$
$$\lambda = (3x^2 + a) / (2y)$$

타원곡선 E상의 한 점을 G라고 하고 e가 정수일 때, $P = eG$에서 정수 e를 찾는 것을 타원곡선 이산대수문제라고 한다.

3.2 Signcryption 방식

본 절에서는 Y.Zheng이 제안한 signcryption 방식에 대해 간략히 기술한다.[1]

3.2.1 시스템 계수

- p : 512 bit 이상의 큰 소수
- q : q|p-1
- g : 위수가 q인 Z_p 상의 원소
- x_*, y_* : *의 비밀키 및 공개키($x_* \in {}_RZ_q$, $y_* \in g^{x*} \bmod p$)
- KH( ) : keyed 해쉬 함수
- E( )/D( ) : 관용 암호/복호 알고리즘

3.2.2 프로토콜

signcryption		unsigncryption
$x \in_R Z_n^*$ $k = h(y_B^x \bmod p)$ $k = k_1 \| k_2$ $r = KH_{k2}(m)$ $s = x/(r+x_A) \bmod q$ $c = E_{k1}(m)$	c, r, s ===>	$k = h((y_A g^r)^{s \cdot x_B} \bmod p)$ $k = k_1 \| k_2$ $m = D_{k1}(c)$ $KH_{k2}(m) = r$을 만족하면 m을 받아들인다.

이 방식은 제 3자에게 signcryption을 증명하는 과정에서 제 3자가 암호문을 복호하기 위한 키를 계산할 수 있어 기밀성을 제공하지 못하며, 서명자가 자신의 비밀키를 분실하거나 제 3자에 의해 노출될 경우, 이전에 서명된 모든 메시지가 노출될 수 있다는 단점이 있다.

3.3 Proxy-Signcryption 방식

계산능력이 뛰어난 proxy agent로 하여금 대신 서명을 수행하게 함으로서 서명 위임자의 계산량을 줄인 방식이다.[2] 시스템계수는 위 방식과 동일하다.

3.3.1 프로토콜

1) 대리 서명용 키 생성 및 확인

서명 위임자 A	==>	Proxy agent P
$x \in_R [1, 2, \ldots, q-1]$ $K \equiv g^x \bmod p$ $x_{AP} \equiv x_A + x \cdot K \bmod p$	K, x_{AP}	$g^{x_{AP}} \stackrel{?}{=} y_A \cdot K^K \bmod p$를 확인함으로서 대리서명용 키가 정당한지 검증

2) 서명 수행 및 검증 과정

Proxy agent P	==>	확인자 B
$x' \in_R [1, 2, \ldots, q-1]$		$y_{AP} = y_A \cdot K^K \bmod p$
$k = y_B^{x'} \bmod p$		$K=(y_{AP} \cdot g^{r'})^{s'x_B} \bmod p$
$k = k_1 \| k_2$	c, r',	$K = k_1 \| k_2$
$c = E_{k1}(m)$	s', K	$m = D_{k1}(c)$
$r' = KH_{k2}(m)$		$KH_{k2}(m) = r'$를
$s' = x' / (r'+x_{Ap}) \bmod q$		만족하면 m을 받아들임

본 방식은 서명 위임자가 proxy agent를 가장하여 정당한 서명을 생성할 수 있으므로 proxy agent를 보호할 수 없다. 또한 대리 서명키 x_{AP}가 드러날 경우 x_B값을 모르는 사람도 키 k를 계산하여 signcrypt된 문서를 복구할 수 있게되어 forward secrecy를 제공하지 못한다.

4. 제안방식

본 장에서는 무선환경을 고려하여 휴대용 단말기의 계산량에 대한 부담을 줄이고 기밀성과 인증성을 제공하는 타원곡선 기반 proxy-signcryption을 제안한다.

4.1 시스템 계수

- A, P, B : 서명 위임자, 대리 서명자, 검증자
- E : GF(p^m)상의 타원곡선 (단, $p \geq 2^{160}$, m=1 이거나 p=2, $m \geq 2^{160}$)
- q : 크기가 $|p^m|$인 큰 소수
- G : 위수가 q인 점
- d_* : *의 개인키 ($d_* \in_R [1, \ldots, q-1]$)
- Q_* : *의 공개키 ($Q_* = d_* \cdot G$)
- H( ) : 일방향 해쉬함수
- KH( ) : keyed 해쉬함수
- E( )/D( ) : 관용 암호/복호 알고리즘

4.2 프로토콜

1) 서명 위임자 A

- 서명 위임자는 랜덤하게 x를 선택하고 K와 D_{AP}를 생성하여 대리 서명자에게 전송한다.

$x \in_R [1, \ldots, q-1]$
$K = x \cdot G$
$D_{AP} \equiv d_A + x \cdot K \bmod q$

2) 대리 서명자 P (Proxy Agent)

- 대리 서명자는 전송된 위임 정보가 정당한지 확인하고 전송 정보로부터 다음과 같이 D_{AP}'를 생성한다.

$Q_{AP} \equiv Q_A + K \cdot K \bmod q$를 확인
$D_{AP}' = D_{AP} + d_P \cdot Q_P \bmod q$ 생성

- 대리 서명자는 랜덤하게 유일한 x′ 를 선택하고 k를 생성한다.

$x' \in_R [1, \ldots, q-1]$
$k = H(x' \cdot Q_B)$
$k = (k_1 \| k_2)$

- 다음과 같이 signcryption을 생성한다.

$r' = KH_{k2}(m)$
$R = r \cdot Q_P \bmod q$
$s' \equiv (x' - r' \cdot d_P)/(D_{AP}') \bmod q$
$c = E_{k1}(m)$

- 계산된 정보를 검증자 B에게 전송한다.

$(c, R, s', K) \rightarrow B$

3) 검증자 B

- 검증자는 수신된 정보와 자신의 개인키를 이용하여 k를 계산한다.

$Q_{AP}' \equiv Q_A + K \cdot K + Q_P \cdot Q_P \bmod q$
$k \equiv H(d_B(s \cdot Q_{AP}' + R) \bmod q)$
$k = (k_1 \| k_2)$

- k값을 이용하여 다음과 같이 메시지를 복호화한다.

$m = D_{k1}(c)$

- 단, $KH_{k2}(m) = r$인 경우에만 정당한 signcryption으로 받아들인다.

검증자의 비밀키를 이용하여 세션키를 계산하는 과정은 다음 식과 같다.

$$
\begin{aligned}
& d_B(s \cdot Q_{AP}' + R) \bmod q \\
& \equiv d_B(((x' - r \cdot d_P) \cdot Q_{AP}')/D_{AP}' + R) \bmod q \\
& \equiv d_B((x' \cdot Q_{AP}' - r \cdot d_P \cdot Q_{AP}')/D_{AP}' + R) \bmod q \\
& \equiv d_B(G(D_{AP}'(x' - r \cdot d_P)/D_{AP}') + r \cdot d_P) \bmod q \\
& \equiv Q_B(x' - r \cdot d_P + r \cdot d_P) \bmod q \\
& \equiv Q_B(x') \bmod q \\
& \equiv H(x' \cdot Q_B \bmod q) \equiv k
\end{aligned}
$$

다음은 제안방식의 전체 프로토콜 흐름을 나타낸 것이다.

서명 위임자 A	공개정보 (E,q,G,Q_A)	대리 서명자 P (Proxy Agent)
$x \in_R [2, \ldots, q-2]$ $K = x \cdot G$ $D_{AP} \equiv d_A + x \cdot K \bmod q$	K, D_{AP} ======>	$Q_{AP} \equiv Q_A + K \cdot K \bmod q$를 확인 $D_{AP}' = D_{AP} + d_P \cdot Q_P \bmod q$

대리 서명자 P (Proxy Agent)	공개정보 (E,q,G,Q_P)	검증자 B
$x' \in_R [2, \ldots, q-2]$ $k = H(x' \cdot Q_B)$ $c = E_{k1}(m)$ $r = KH_{k2}(m)$ $R = r \cdot Q_P$ $s \equiv (x' - r \cdot d_P) / (D_{AP}') \bmod q$	(c, r, s, K) =======>	$Q_{AP}' \equiv Q_A + K \cdot K + Q_P \cdot Q_P \bmod q$ $k \equiv H(d_B(s \cdot Q_{AP}' + R) \bmod q)$ $m = D_{k1}(c)$ $KH_{k2}(m) = r$이면 m을 받아들인다.

[그림 1] 제안방식 흐름도

4.3 제안 방식 고찰

2장에서 제시한 요구사항 만족도를 살펴보고 계산량 및 통신 효율성에 대해 분석한다.

1) 기밀성 : 검증자 만이 서명을 확인 할 수 있으며, d_B와 D_{AP}'를 모르는 제 3자는 키를 계산할 수 없으므로 불법적 도청자로부터 서명 메시지의 기밀성을 확보할 수 있다.
2) 인증성 : 지정된 수신자만이 서명을 검증할 수 있으며, 전송된 정보의 검증에 있어 송신자의 비밀키에 대응하는 공개키를 이용하여 검증함으로서 인증성을 제공한다.
3) 부인봉쇄 : 서명 생성시 서명 위임자 및 대리 서명자의 비밀정보를 포함시킴으로서 부인봉쇄 기능을 제공한다.
4) 효율성 및 안전성 : 서명 생성에 있어 계산 능력이 뛰어난 proxy agent를 이용함과 동시에 타원곡선 이산대수문제에 기반하여 각 개체들의 연산량을 줄이고 있다. 또한, 위임정보 및 위임 서명 생성시 서명 위임자와 대리 서명자의 개인키를 포함시켜 생성함으로서 이 두 개체에 의한 불법적 서명생성을 막고 있다.
5) Forward Secrecy : 정당한 수신자는 개인키 d_B를 이용하여 다음 식의 좌변을 통해 정당성을 확인한다.

$$d_B(s \cdot Q_{AP}' + R) \bmod q = Q_B(s \cdot D_{AP}' + r \cdot d_P) \bmod q$$

그러나 정당하지 못한 수신자는 우변 식을 통해 공격을 시도할 것이며, 대리 서명자의 개인키 d_P를 알지 못하는 사람은 키를 계산할 수 없다. 반면 d_P가 노출될 경우에도 r을 알지 못하면 키 k를 계산할 수 없다. 따라서 대리 서명자의 개인키에 대한 forward secrecy를 제공한다.

6) 계산량 및 통신량 : 타원곡선 암호를 이용할 경우 RSA나 DSA보다 약 10배 정도 빠른 수행속도를 가지며, 키 길이에 있어서도 160 비트의 키 길이를 가지고 RSA 1024 비트의 키 길이가 갖는 안전도를 제공한다. 또한, 짧은 키 길이는 키 쌍과 시스템 매개 변수 저장에 드는 비트 크기를 줄일 수 있으며, 암호화된 메시지나 서명을 전송하기 위한 비트 코드를 줄일 수 있다.

5. 결론

이동 통신상에서 계산 능력이 떨어지는 휴대용 단말기를 고려하여 기밀성 및 인증성, 효율성을 제공할 수 있는 전자서명 방식은 무선 인터넷 서비스의 제공에 있어 중요한 이슈가 되고 있다.

이에 본 논문에서는 작은 키 길이를 가지고 다른 공개키 스킴과 같은 안전도를 제공할 수 있는 타원곡선 기반의 proxy-signcryption 방식을 제안하였다. 향후 제안된 방식을 무선 인터넷 서비스에 적용하기 위해서는 추가적인 연구가 진행되어야 할 것이다.

참고문헌

[1] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," Proc. ISW'97, LNCS 1397, pp.291-312, 1998.

[2]C. Gamage, J. Leiwo and Y. Zheng, "An Efficient Scheme for Secure Message Transmission using Proxy-Signcryption," Proceeding of the Twenty Second Australasian Computer Science Conference, pp.18-21, Jan, 1999.

[3]K. Araki, T. Satoh, and S. Miura, "Overview of Elliptic Curve Cryptography(Extended Abstract," Proceedings of PKC'98, Pacifico Yokohama, Japan, pp.5-6, February, 1998

[4] 최용락, 소우영, 이재광, 이임영, 컴퓨터 통신 보안, 2001. 2. 28, 도서출판 그린