KCDSA 및 EC-KCDSA에 근간한 은닉서명

서문석*, 김광조*

*한국정보통신대학원

Blind Signature Schemes based on KCDSA and EC-KCDSA

Moonseog Seo*, Kwangjo Kim*

*Information and Communications Univ.

요 약

은닉서명은 메시지 송신자가 서명자에게 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명 값을 얻기 위한 프로토콜이다. 이러한 은닉서명은 고객의 익명성을 요구하는 전자지불시스템과 같은 암호 프로토콜에 적용되어 참여자의 익명성을 보호하는데 필수적으로 이용되고 있다. 본 논문에서는 국내 전자서명 기법의 표준으로 제정된 KCDSA을 근간으로 하는 은닉서명 방식 및 EC-KCDSA를 근간으로 하는 은닉서명 방식을 제시하고 은닉성에 대한 안전성을 증명하여 사용자의 익명성 보호가 필요한 다양한 응용에 적용되어질 수 있도록 하였다.

I. 서론

은닉서명은 메시지 송신자가 서명자로부터 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 서명 값을 얻기 위한 프로토콜이다. 서명자가 메시지와 그 서명 값을 제시받은 경우에 서명자는 서명 값의 정당성 여부를 검증할 수 있어야 한다. 반면, 서명자는 은닉서명 방식을 통한 자신의 서명프로토콜 수행과정에서 얻은 정보와 서명검증을 위해 수신한 메시지-서명값 쌍을 서로 연결시킬 수 없어야 한다. 은닉서명 방식은 이러한 방식으로 인해 서명 사용자의 익명성을 보호하는 암호 프로토콜의 하나이다.

은닉서명의 개념은 D. Chaum[1]에 의해 처음 소개되었으며 이는 실세계의 화폐

가 가지고 있는 익명성을 전자화폐에 그대로 적용할 수 있도록 하기 위하여 고안되었으며 이를 통해 전자화폐 사용 고객의 프라이버시를 보호할 수 있다. 이처럼 은닉서명 방식은 암호 프로토콜 참여자의 익명성이 요구되어지는 암호 응용분야에 있어서는 필수적으로 요구되어지는 기본적인 암호 기법에 해당된다. 현재까지 제시된 은닉서명 방식으로는 첫째, 인수분해 문제의 어려움에 근간한 RSA 서명방식을 이용한 은닉서명 방식이 있으며 둘째, 유한체 상에서의 이산 로그를 찾는 문제에 근간한 전자서명 방식을 이용한 ElGamal 유형의 은닉서명 방식이 있다. 특히 이러한 이산대수 문제에 근간한 은닉서명의 경우 J. Camenisch 등이 미국 표준인 DSA 및 메시지 복원형 전자서명인 Nyberg-Rueppel 서명 방식을 근간으로 하는 은닉서명 방식을 제시하였으며, P. Horster 등도 이산대수 문제에 근간한 일반적인 형태의 은닉서명 방식을 제시하였다[2, 3, 4, 5, 6]. 최근에는 은닉서명의 완전한 익명성에 의한 역기능을 방지하기 위해 필요시 익명성이 철회될 수도 있는 공정한 은닉서명 기법에 관한 연구도 이루어 지고 있다[8].

본 논문에서는 이산대수 문제에 근간한 전자서명 방식으로 국내 전자서명 방식의 표준으로 제정된 확인서 이용 전자서명 알고리즘(KCDSA : Korean Certificate-based Digital Signature Algorithm)을 근간으로 하여 익명성이 요구되는 다양한 암호 응용에 이용 가능한 은닉서명기법을 제시하고 익명성 보호의 안전성에 대한 증명도 제시한다. 또한 타원곡선을 이용한 서명 방식으로 국내 표준으로 추진 중인 타원곡선을 이용한 확인서 기반 전자서명 알고리즘(EC-KCDSA)을 근간으로 하는 은닉서명 기법도 제시한다[7].

본 논문의 구성은 다음과 같다. 2장에서는 은닉서명 설계를 위한 기본 서명기법으로 사용될 KCDSA 및 EC-KCDSA에 대해 설명하고, 3장에서는 KCDSA에 기반한 은닉서명을 제시한다. 4장에서는 EC-KCDSA 기본 서명기법에 근간한 은닉서명 기법을 제시하며, 5장에서 결론을 맺는다.

II. 기본 서명 기법

은닉서명 방식의 설계를 위한 기본 서명 기법으로 정보처리시스템 또는 정보통신망 환경에서 인증, 무결성 및 부인방지 서비스를 제공하기 위하여 서명자가 전자서명을 생성하거나 검증자가 서명된 메시지를 검증하기 위해 사용하는 전자서명 기법에 대한 국내 표준인 KCDSA 전자서명 방식을 이용한다. 본 논문에서는 기존에 제

시된 KCDSA 전자서명 방식을 메시지 m이 Z_q상에서 선택되고 각종 사용 변수들이 인증된 상태에서 사용된다고 가정하여 은닉성 증명이 용이하도록 다음의 1절(KCDSA 방식)과 같이 단순화할 수 있다. 여기서 제시하고 있는 단순화된 방식은 각종 변수의 인증을 위해 확인서(Certificate)를 도입하고, 서명의 첫 부분인 r의 생성을 위해 $|q|$비트 길이의 출력 값을 갖는 충돌 저항성의 해쉬함수를 적용하면 random oracle model 하에서 안전성 증명이 가능한 원래의 KCDSA 서명 방식으로 전환될 수 있다.

본 장에서 정의되지 않은 변수 및 용어들은 표준문서에 정의된 내용을 준용한다 [7].

1. KCDSA 방식

시스템 변수 및 함수

p : $2^{|p|-1} < p < 2^{|p|}, |p| = 512 + 256i (0 \le i \le 6)$의 크기를 가지며 $(p-1)/2q$ 역시 소수이거나 최소한 q보다 큰 소수들의 곱으로 구성되는 소수.

q : $p-1$를 나누는 소수. $2|q|-1 < q < 2|q|, |q| = 128 + 32j (0 \le j \le 4)$의 크기를 가짐.

g : $a^{(p-1)/q} \bmod p, 1 < a < p-1$이고, $a^{(p-1)/q} \bmod p > 1$을 만족함.

사용자 변수

x : $0 < x < q$를 만족하는 정수로서 랜덤하게 선택된 서명자의 비공개 서명키.

y : $y = g^{x^{-1}} \bmod q$로 계산되는 서명자의 공개 검증키 (x^{-1}는 $xx^{-1} = 1 \bmod q$ 와 $0 < x^{-1} < q$를 만족하는 수).

서명 과정

서명자는 다음과 같은 과정을 거쳐서 서명된 메시지 $\{m \| \Sigma\}$를 출력하며, 서명 Σ는 $\{r \| s\}$이다.

단계 1) 난수 값 k를 $\{1, \ldots, q-1\}$에서 랜덤하게 선택한다.

단계 2) 서명의 첫 부분 $r = g^k \bmod p$를 계산한다.

단계 3) 서명의 두 번째 부분 $s = x(k - m) \bmod q$를 계산한다.

단계 4) 서명 $\Sigma = \{r \| s\}$를 만들어 서명된 메시지 $\{m \| \Sigma\}$를 출력한다.

검증 과정

검증자는 다음과 같은 과정을 거쳐서 수신된 메시지 m의 서명이 Σ인지를 확인할 수 있다.

단계 1) 서명된 메시지 $\{m \| \Sigma\}$로부터 검증할 메시지 m, 서명의 첫 부분 r, 서명의 두번째 부분 s을 추출한다. 이 때 $0 < r < 2^{|q|}$이고 $0 < s < q$임을 확인한다.

단계 2) 서명자의 공개 검증키 y를 이용하여 $r = y^s g^m \bmod p$이 성립하는지 확인한다.

단계 1) 과 단계 2)의 확인 과정이 모두 통과되면 서명 Σ는 받은 메시지 m에 대하여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명하였음이 확인된 것이다.

2. EC-KCDSA 방식

본 방식은 임의의 길이를 갖는 메시지에 대해 확인서를 이용한 부가형 전자서명 알고리즘인 KCDSA를 타원곡선을 이용한 전자서명 알고리즘으로 변형한 방식이다.

공개 정보

$E(F_{p^m})$: 유한체 $GF(p^m)$상에 정의된 타원곡선.

q : $\#E(F_{p^m})$를 나누는 소수. $|q| \geq 160$

G : 위수 q를 갖는 순환군(cyclic group)을 생성하는 타원곡선 $E(F_{p^m})$의 한 점.

$h()$: 충돌 저항성의 해쉬함수. $|h()| \geq 160$.

사용자 변수

x : $0 < x < q$를 만족하는 정수로서 랜덤하게 선택된 서명자의 비공개 서명키.

y : $y = x^{-1}G$로 계산되는 서명자의 공개 검증키 (x^{-1}는 $xx^{-1} = 1 \bmod q$와 $0 < x^{-1} < q$를 만족하는 수).

서명 과정

서명자는 다음과 같은 과정을 거쳐서 서명된 메시지 $\{m \| \Sigma\}$를 출력하며, 서명 Σ는 $\{r \| s\}$이다.

단계 1) 난수 값 k를 $\{1, \ldots, q-1\}$에서 생성한다.

단계 2) 타원곡선의 점 $(x_1, y_1) = kG$를 계산한다.

단계 3) 서명의 첫 부분인 해쉬 코드 $r = h(kG) = h(x_1 \| y_1)$를 계산한다.

단계 4) 서명의 두 번째 부분 $s = x(k - m) \bmod q$를 계산한다.

검증 과정

검증자는 다음과 같은 과정을 거쳐서 수신된 메시지 m의 서명이 Σ'인지를 확인할 수 있다.

단계 1) 서명된 메시지 $\{m \| \Sigma\}$로부터 검증할 메시지 m, 서명의 첫 부분 r,

서명의 두번째 부분 s을 추출한다. 이 때 $0<r<2^{|q|}$이고 $0<s<q$임을 확인한다.

단계 2) 서명자의 공개 검증키 y를 이용하여 타원곡선의 점 $(x_2,y_2)=sy+mG$를 계산한다.

단계 3) $h(x_1 \| y_1)=r$임을 확인한다.

단계 1)에서 단계 3)까지의 확인 과정이 모두 통과되면 서명 Σ는 받은 메시지 m에 대하여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명되었음이 확인된다.

III. KCDSA 은닉서명

KCDSA 은닉서명 방식에서 사용되는 공개정보와 사용자 변수는 기본 서명 방식인 KCDSA와 동일하다.

1. 서명과정

단계 1) 서명자는 난수 값 $\tilde{k}$를 $\{1,...,q-1\}$에서 랜덤하게 선택한다.

단계 2) 서명자는 $\tilde{r}=g^{\tilde{k}} \bmod p$를 계산하여 메시지 송신자에게 전송한다.

단계 3) 메시지 송신자는 임의의 $a,b \in Z_q^*$를 선택하고 $r=\tilde{r}^a g^b \bmod p$를 계산한다.

단계 4) 메시지 송신자는 $\tilde{m}=a^{-1}(m-b) \bmod q$를 계산하여 서명자에게 전송한다.

단계 5) 서명자는 $\tilde{s}=x(\tilde{k}-\tilde{m}) \bmod q$를 계산하여 메시지 송신자에게 전송한다.

단계 6) 메시지 송신자는 m에 대한 서명 값으로 $S=\tilde{s}a \bmod q$와 $R=r \bmod q$를 결정한다.

단계 7) 서명 $\Sigma=\{R \| S\}$를 만들어 서명된 메시지 $\{m \| \Sigma\}$를 출력한다.

2. 검증과정

검증자는 다음과 같은 과정을 거쳐서 수신된 메시지 m의 서명이 Σ인지를 확인할 수 있다.

단계 1) 서명된 메시지 $\{m \| \Sigma\}$로부터 검증할 메시지 m, 서명의 첫 부분 R, 서명의 두 번째 부분 S을 추출한다. 이 때 $0<R<2^{|q|}$이고 $0<S<q$임을 확인한다.

단계 2) 서명자의 공개 검증키 y를 이용하여 $R=y^S g^m \bmod q$이 성립하는지 확인한다.

단계 1) 과 단계 2)의 확인 과정이 모두 통과되면 서명 Σ는 받은 메시지 m에 대하여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명하였음이 확인된 것이다.

3. 안전성 검토

KCDSA은닉서명의 서명 값 $(R \| S)$가 m의 유효한 서명 값임을 보이는 식은 다음과 같다.

$$\begin{aligned} T &= (g^m y^S) \\ &= g^m g^{x^{-1}sa} \\ &= g^m g^{(\tilde{k}-\tilde{m})a} \\ &= g^m g^{(\tilde{k}a-m+b)} \\ &= g^{\tilde{k}a+b} \\ &= r \bmod p \end{aligned}$$

R과 $T \bmod q$가 같다는 것은 서명 값 $(R \| S)$가 메시지 m의 유효한 서명 값임을 의미한다.

서명기법은 보통 서명자가 서명프로토콜을 수행하면서 얻은 모든 은닉된 정보인 서명자 뷰(V)가 메시지 송신자가 은닉서명을 얻기 위해 생성한 정보사이에 통계적인 독립성(Statistically independent)이 유지된다면 이러한 서명기법은 은닉성에 대한 안전성이 증명되는 은닉서명으로 불린다[6]. KCDSA은닉서명 프로토콜에서 메시지 서명자의 익명성 보호를 위한 은닉성의 증명을 위해서는 서명자가 서명 프로토콜을 수행하면서 얻은 정보인 $r, \tilde{m}, \tilde{s}$으로 구성된 서명자의 뷰(V)와 임의의 유효 메시지 서명 값 쌍 m, R, S가 주어진 경우, 랜덤하게 선택된 은닉요소인 a, b의 유일한 쌍이 존재함을 보이면 된다.

정리 1 : $S, \tilde{s} \in Z_q^*$ 및 (m, R, S)와 $(\tilde{m}, \tilde{r}, \tilde{s})$의 임의의 쌍에 대해 다음을 만족하는 유일한 $a, b \in Z_q^*$가 존재한다.

$$r = \tilde{r}^a g^b \pmod p \pmod q \tag{1}$$

$$m = a\tilde{m} + b \pmod q \tag{2}$$

$$S = \tilde{s}a \pmod q \tag{3}$$

증명 : 다음을 만족하는 $a, b \in Z_q$를 선택한다.

$$a = S\tilde{s}^{-1} \pmod q \tag{4}$$

$$b = (m - \tilde{m}S\tilde{s}^{-1}) \pmod q \tag{5}$$

(4)과 (5)로부터 은닉서명의 검증식을 이용하면 다음의 식을 얻을 수 있다.

$$
\begin{aligned}
a\tilde{k}+b &= (S\tilde{s}^{-1})\tilde{k}+(m-\tilde{m}S\tilde{s}^{-1}) \\
&= m+S(\tilde{s}^{-1}\tilde{k}-\tilde{m}\tilde{s}^{-1}) \\
&= m+S((\tilde{m}+x^{-1}\tilde{s})\tilde{s}^{-1}-\tilde{m}\tilde{s}^{-1}) \\
&= m+Sx^{-1} \pmod q
\end{aligned} \tag{6}
$$

즉 $\tilde{r}^{a}g^{b}=g^{a\tilde{k}+b}=g^{m+Sx^{-1}}=g^{m}y^{S}=r \pmod p$가 성립된다. a,b가 위 (6)식을 만족해야 하기 때문에 선택된 a,b는 유일하게 존재한다[6, 9].

IV. EC-KCDSA 은닉서명

EC-KCDSA 은닉서명 방식에서 사용되는 공개정보와 사용자 변수는 기본 서명 기법인 EC-KCDSA와 동일하다.

1. 서명과정

단계 1) 서명자는 난수 값 $\tilde{k}$를 Z_q^* 상에서 랜덤하게 선택한다.

단계 2) 서명자는 $P=\tilde{k}G=(x_1,y_1)$를 계산하여 메시지 송신자에게 전송한다.

단계 3) 메시지 송신자는 임의의 $a,b\in Z_q^*$를 선택하고 $\tilde{P}=aP+bG=(x_2,y_2)$을 계산한다.

단계 4) 메시지 송신자는 $\tilde{m}=a^{-1}(m-b) \bmod q$를 계산하여 서명자에게 전송한다.

단계 5) 서명자는 $\tilde{r}=h(x_1 \| y_1)$과 $\tilde{s}=x(\tilde{k}-\tilde{m}) \bmod q$를 계산하여 메시지 송신자에게 $\tilde{s}$를 전송한다.

단계 6) 메시지 송신자는 m에 대한 서명 값으로 $s=\tilde{s}a \bmod q$과 $r=h(x_2 \| y_2)$를 결정한다.

단계 7) 서명 $\Sigma=\{r \| s\}$을 만들어 서명된 메시지 $\{m \| \Sigma\}$를 출력한다.

2. 검증과정

검증자는 다음과 같은 과정을 거쳐서 수신된 메시지 m의 서명이 Σ인지를 확인할 수 있다.

단계 1) 서명된 메시지 $\{m \| \Sigma\}$로 부터 검증할 메시지 m, 서명의 첫 부분 r, 서명의 두 번째 부분 s를 추출한다. 이 때 $0<s<q$임을 확인한다.

단계 2) 서명자의 공개 검증키 y를 이용하여 $r=h(x_2 \| y_2)$이 성립하는지 확인한다. 이때 $(x_2,y_2)=mG+sy$이다.

단계 1) 과 2)의 확인 과정이 모두 통과되면 서명 Σ는 수신한 메시지 m에 대하

여 공개 검증키 y에 대응하는 비공개 서명키 x로 서명하였음이 확인된 것이다.

3. 안전성 검토

EC-KCDSA 은닉서명의 서명 값 $\{r \| s\}$가 m의 유효한 서명 값임을 보이는 식은 다음과 같다.

$$\begin{aligned}\tilde{P} &= mG + sy \\ &= mG + \tilde{s}ax^{-1}G \\ &= mG + x(\tilde{k} - \tilde{m})ax^{-1}G \\ &= mG + (\tilde{k} - a^{-1}m + a^{-1}b)aG \\ &= mG + \tilde{k}aG - mG + bG \\ &= \tilde{k}aG + bG \\ &= (x_2, y_2)\end{aligned}$$

r과 $h(x_2 \| y_2)$가 같다는 것은 서명 값 $\{r \| s\}$가 메시지 m의 유효한 서명 값임을 의미한다.

EC-KCDSA 은닉서명 프로토콜의 은닉성을 증명하기 위해서는 KCDSA 은닉서명 프로토콜의 증명 방식과 동일하게 서명자의 뷰(V)와 임의의 유효 메시지 서명 값 쌍이 주어진 경우, 은닉요소 a, b의 유일한 쌍이 존재함을 보이면 된다.

정리 2 : $S, \tilde{s} \in Z_q^*$, $P = (x_1, y_1)$, $\tilde{P} = (x_2, y_2)$는 타원곡선 $E(F_{p^m})$상의 점이라 할 때 (m, r, s)와 $(\tilde{m}, \tilde{r}, \tilde{s})$의 임의의 쌍에 대해 다음을 만족하는 유일한 a, b가 존재한다.

$$\tilde{P} = aP + bG = (x_2, y_2) \tag{7}$$

$$r = h(x_2 \| y_2) \tag{8}$$

$$m = a\tilde{m} + b \pmod{q} \tag{9}$$

$$S = \tilde{s}a \pmod{q} \tag{10}$$

증명 : 다음을 만족하는 $a, b \in Z_q^*$를 선택한다.

$$a = S\tilde{s}^{-1} \pmod{q} \tag{11}$$

$$b = (m - \tilde{m}S\tilde{s}^{-1}) \pmod{q} \tag{12}$$

(11)과 (12)로부터 은닉서명의 검증식을 이용하면 다음의 식을 얻을 수 있다.

$$
\begin{aligned}
a\tilde{k}+b &= (S\tilde{s}^{-1})\tilde{k}+(m-\tilde{m}S\tilde{s}^{-1}) \\
&= m+S(\tilde{s}^{-1}\tilde{k}-\tilde{m}\tilde{s}^{-1}) \\
&= m+S((\tilde{m}+x^{-1}\tilde{s})\tilde{s}^{-1}-\tilde{m}\tilde{s}^{-1}) \\
&= m+Sx^{-1} \pmod q
\end{aligned} \tag{13}
$$

즉 $aP+bG=a\tilde{k}G+bG=(a\tilde{k}+b)G=(m+Sx^{-1})G=mG+Sy=(x_2,y_2)$ 이 되고 $r=h(x_2 \| y_2)$ 가 성립된다. a,b 가 위 (13)식을 만족해야 하기 때문에 선택된 a,b 는 유일하게 존재한다[6, 9].

V. 결론

암호 응용프로토콜의 개발에는 근간이 되는 암호 기술이 절대적으로 필요하다. 익명성이 요구되는 다양한 응용 프로토콜의 개발 분야에 있어 국가 표준인 KCDSA 서명 방식을 근간으로 하는 은닉서명 기법을 활용하여 각종 암호 응용프로토콜 개발 및 구현에 적용이 가능하리라고 생각한다. 본 논문에서는 국내 전자서명 방식 표준인 KCDSA 및 EC-KCDSA에 근간한 은닉서명 기법을 제시하였으며 은닉서명의 안전성 요소인 은닉성 및 서명위조 방지 중 은닉성 요소에 대해 증명을 하였다. 이러한 은닉서명 기법은 전자현금 프로토콜과 같은 사용자의 완전한 익명성이 요구되는 응용 프로토콜에 사용될 수 있을 것이다[8, 10].

본 논문에서 제시하고 있는 은닉서명에 대한 서명위조 가능성으로부터의 안전성 증명이 요구되어지며 이와 관련한 연구가 추후 연구과제이다.[9].

참고문헌

[1] D. Chaum, “Blind Signature Systems”, Advances in Cryptology-CRYPTO '83, Plenum, p. 153, 1983.

[2] J. Camenisch, J-M Piveteau, M. Stadler, “Blind Signatures Based on the Discrete Logarithm Problem”, Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 428-432, 1994.

[3] NIST FIPSPUB 186, Digital Signature Standard(DSS), National Institute of Standards and Technology, U.S. Department of Commerce, November 1994.

[4] K. Nyberg, R. Rueppel, “A New Signature Scheme based on the DSA giving Message Recovery”, Proc. 1st ACM Conference on Computer and

Communications Security, Fairfax, Virginia, Nov. 3-5. 4pages, 1993

[5] P. Hoster, M. Michels, H. Petersen, "Efficient Blind Signature Schemes Based on the Discrete Logarithm Problem", Technical Report TR-94-6-D, 1994

[6] P. Hoster, M. Michels, H. Petersen, "Meta-Message Recovery and Meta-Blind Signature Schemes Based on the Discrete Logarithm Problem and Their Applications", Advances in Cryptology -ASIACRYPT'94, LNCS 917, Springer-Verlag, pp. 224-237, 1994

[7] C.H. Lim, P.J. Lee, "A Study on the Proposed Korean Digital Signature Algorithm", Advances in Cryptology-ASIACRYPT'98, LNCS 1514, Springer-Verlag, pp. 175-186, 1998

[8] M.Stadler, J-M Piveteau, J. Camenisch, "Fair Blind Signature", Advances in Cryptology-EUROCRYPT '95, LNCS 921, Springer-Verlag, pp. 209-219, 1995.

[9] D. Pointcheval, J. Stern, "Provably Secure Blind Signature Schemes", Advances in Cryptology-ASIACRYPT '96, LNCS 1163, Springer-Verlag, pp. 252-265, 1996.

[10] S. Brands, "Untraceable Off-line Cash in Wallet with Observers", Proc. of Crypto '93, LNCS 773, Springer-Verlag, pp. 302-318, 1993.