KCDSA 및 EC-KCDSA를 기반으로한 부분 은닉서명

윤태은*, 이상곤*

* 동서대학교, 인터넷공학부

Partially Blind Signature Schemes based on KCDSA and EC-KCDSA

Tae-eun Yun*, Sang-gon Lee*

* Department of Internet Engineering, Dongseo Univ.

요 약

부분 은닉서명은 메시지 내용의 일부분만 공개하므로서 익명성과 동시에 공개되는 일부분의 정보를 사용하여 부가적인 기능을 제공할 수 있다. 이러한 부분 은닉서명을 이용하면 전자수표방식과 같은 전자상거래 시스템에서 고객의 익명성을 보호하면서도 공개되는 정보를 금액이나 유효기간으로 사용하여 거스름을 취급할수 있는 방법을 제공할 수 있다. 본 논문에서는 국내 전자서명 기법의 표준으로 제정된 KCDSA를 기반으로 하는 부분 은닉서명 기법 및 EC-KCDSA를 기반으로 하는 부분 은닉서명 기법을 제시하므로서 거스름을 사용할 수 있는 효율적인 전자상거래 기법에 적용되어질 수 있도록 하였다.

I. 서론

전자화폐는 전자상거래에서 지불수단으로 사용하기 위해 개발된 화폐로서, 디지털 정보 형태로 표현되므로 통신망으로 전달이 가능하다. 이상적인 전자화폐란 기존의 실물화폐가 가지고 있는 익명성(anonymity), 분할성(divisibility), 양도성(transferability) 등의 특성을 지녀야 한다.

David Chaum[1]이 처음 소개한 전자화폐는 전자동전(electronic coin)방식[2]과 전자수표(electronic check)방식[3]으로 분류할 수 있다. 전자동전 방식에서는 각 동전이 고정된 액면가를 가지고 있으며, 고객은 지불대금에 맞도록 필요한 개수의 동전을 이용하여 지불한다. 이와는 달리 전자수표방식에서는 시스템이 정해놓은 고정된 금액의 수표 또는 고객이 원하는 금액의 수표를 인출받아 지불한다. 전자수표는 수표 하나만으로도 지불이 가능하기 때문에 여러개의 동전을 사용해야하는 전자동전방식보다는 계산량이나 정보교환량 측면에서 효율적이다.[3]

전자수표방식을 사용하는 경우는 수표를 사용하고 난 후의 거스름돈을 처리해야할 필요성이 있다. 이것을 처리하기 위해 부분 은닉서명을 사용할 수가 있다. 부분 은닉서명을 사용하면 수표의 익명성을 보장하면서 거스름돈을 재사용할 수가 있다. 부분 은닉서명은 M. Abe가 처음 소개하였고[11], 이산대수 문제와 RSA기반으로 Schnorr 서명을 사용하여 설계하였다[4,10]. 최근에는 RSA를 기반으로한 부분 은닉서명을 사용하여 설계된 전자수표시스템도 있다[12].

본 논문에서는 이산대수 문제의 어려움에 기반으로한 방식으로 국내 전자서명 방식의 표준으로 제정된 확인서 이용 전자서명 알고리즘(KCDSA : Korea Certificate-based Digital Signature Algorethm) 과 표준제정이 진행중인 타원곡선을 이용한 확인서 기반 전자서명 알고리즘

(EC-KCDSA)을 기반 하여 제안된 은닉서명 기법 [7]을 참고하여, 부분 은닉서명 기법을 제안한다. 서로 공통으로 공개되어 있는 Info라는 정보를 서명에 참여시켜 비밀키가 없는 공개키 역할을 하게 한다. 이 Info 정보는 수표의 금액이나 유효기간으로 사용될 수 있을 것이다.

본 논문의 구성은 2장에서는 KCDSA를 이용한 부분 은닉서명기법을 제시하고, 3장에서는 EC-KCDSA를 이용한 부분 은닉서명기법을 제시한다. 그리고, 마지막 4장에서는 결론을 맺는다.

II. KCDSA 부분 은닉서명

KCDSA 부분 은닉서명에서 사용하는 공개정보와 사용자 변수는 기본 서명방식의 KCDSA와 m을 제외하고 모두 동일하며, 본 논문에서 정의되지 않은 변수 및 용어들은 표준문서에 정의된 내용을 따른다.[6]

1. 시스템 변수

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-1을 나누는 소수로 $2^{|q|-1} < q < 2^{|q|}$, $|q| = 128 + 32j$ $(0 \le j \le 4)$의 크기를 가짐.

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

2. 사용자 변수

x : 0<x<q인 비공개 서명키.

y : $y = g^{x^{-1}} \bmod p$로 계산되는 공개 검증키 (x^{-1}은 mod q로 x의 곱셈에 대한 역원. 즉 $x^{-1}x = 1 \bmod q$인 0과 q사이의 정수를 나타냄)

z : 공개정보 Info의 해쉬코드 h(Info)로서 길이가 $|q|$이다.

m : 메시지 M과 h(Cert_Data)의 해쉬코드, 즉 $h(M \| h(Cert_Data))$에 r를 XOR한 값으로 표준문서 상의 중간값으로 둔다.

3. 서명 생성 과정

공개되는 데이터를 z라 한다. 이것은 나중에 화폐의 금액이나 유효기간으로 활용될수 있다. 만약 z가 zero이면 해쉬함수 입력 뒤에 추가 데이터를 사용하여 새로운 값을 생성한다.

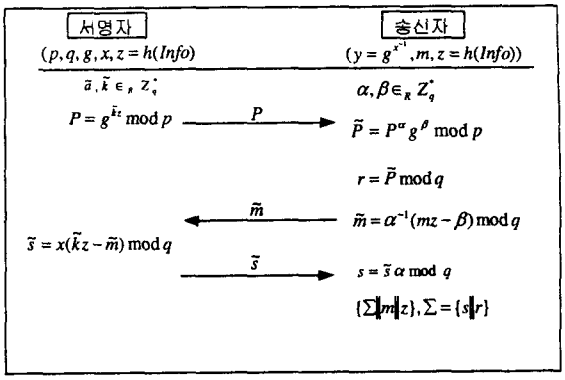

그림 1: KCDSA 부분 은닉서명 과정

그림1과 같은 과정을 거쳐 생성된 서명 데이터는 $\{\Sigma \| m \| z\}$ 이며, 이때 $\Sigma = \{s \| r\}$이다.

4. 서명 검증 과정

① 검증자는 서명된 메시지로부터 검증할 메시지 m, 서명의 첫 부분 s, 서명의 두 번째 부분 r과 공개되는 정보 z를 추출한다.

② 추출된 정보가 $0 < r < 2^{|q|}$이고, $0 < s < q$ 임을 확인한다.

③ 서명자의 공개 검증키 y를 이용하여 $r = y^s g^{mz} \bmod q$ 이 성립하는지 확인한다.

④ ②와 ③의 확인 과정에 이상이 없다면 서명 Σ는 메시지 M에 대하여 공개 검증키 y와 z에 대응하는 비공개 검증키 x로 서명하였음이 확인된 것이다.

5.안정성 검토

KCDSA 부분 은닉서명의 서명 값 $\{s \| r\}$가 은닉되는 메시지 m과 공개되는 정보 z의 유효한 서명 값임을 보이는 식은 다음과 같다.

$$
\begin{aligned}
T &= g^{mz} y^s \\
&= g^{mz} g^{x^{-1}\hat{s}\alpha} \\
&= g^{mz} g^{x^{-1}x(kz-\tilde{m})\alpha} \\
&= g^{mz} g^{kz\alpha - \alpha\tilde{m}} \\
&= g^{mz} \; g^{kz\alpha - \alpha^{-1}(mz-\beta)\alpha} \\
&= g^{mz} \; g^{kz\alpha - mz + \beta} \\
&= g^{kz\alpha + \beta} \\
&= \tilde{P} \bmod q \\
&= r \bmod p
\end{aligned}
$$

r과 $T \bmod q$가 같다는 것은 서명 값 $\{s \| r\}$가 m과 z의 유효한 서명 값임을 의미한다.

부분 은닉서명은 Masayuki Abe가 개발한 서명 기법으로 은닉되는 m과 공개되는 z정보가 서명자의 서명을 받게되지만 서명자는 서명된 데이터와 m을 연관시키는 것이 계산적으로 용이하지가 않다[4]. 일반 은닉서명에서 서명자는 서명 내용을 전혀 알 수 없지만 부분 은닉서명에서 서명자는 z정보가 서명에 포함된다는 것을 확신할 수 있다. 즉, 서명자와 메시지송신자가 동의한 어떤 정보를 은닉서명에 포함시킬 수 있다. 또한 은닉서명은 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[5]. KCDSA 부분 은닉서명 프로토콜에서 메시지 서명자의 익명성 보호를 위한 은닉성의 증명을 위해서는 서명자가 서명 프로토콜을 수행하면서 얻은 정보인 $\tilde{m}, P, \hat{s}$으로 구성된 서명자의 뷰와 임의의 유효메시지 서명 값 쌍 m, r, s 가 주어진 경우, 랜덤하게 선택된 은닉요소인 α, β의 유일한 값 쌍이 존재함을 보이면 된다[7].

① $s, \tilde{s} \in Z_q^*$ 및 $(P, \tilde{m}, \hat{s})$와 (r, m, s)의 임의의 쌍에 대해 다음을 만족하는 유일한 $\alpha, \beta \in Z_q^*$가 존재한다.

$$r = P^{\alpha} g^{\beta} (\bmod p) (\bmod q) \quad (1)$$

$$mz = \alpha \tilde{m} + \beta \ (\bmod q) \quad (2)$$

$$s = \hat{s}\alpha \ (\bmod q) \quad (3)$$

$$\hat{kz} = \hat{s} x^{-1} + \tilde{m} \quad (4)$$

② 다음을 만족하는 $\alpha, \beta \in_R Z_q^*$를 선택.

$$\alpha = s\, \hat{\tilde{s}}^{-1} (\bmod q) \quad (5)$$

$$\beta = (mz - \tilde{m}\alpha) \quad (6)$$

식(5), (6)으로부터 은닉서명 검증식을 이용하면 다음의 식을 얻을 수 있다.

$$\begin{aligned} &\alpha \tilde{kz} + \beta \\ &= s\, \hat{\tilde{s}}^{-1} \hat{kz} + (mz - \tilde{m}\alpha) \\ &= mz + s(\hat{\tilde{s}}^{-1} \hat{kz} - \tilde{m}\, \hat{\tilde{s}}^{-1}) \\ &= mz + s(\hat{\tilde{s}}^{-1} (\hat{s} x^{-1} + \tilde{m}) - \tilde{m}\, \hat{\tilde{s}}^{-1}) \\ &= mz + sx^{-1} + s\, \hat{\tilde{s}}^{-1} \tilde{m} - s\, \hat{\tilde{s}}^{-1} \tilde{m} \\ &= mz + sx^{-1} \end{aligned} \quad (7)$$

α, β가 위 (7)식을 만족해야 하기 때문에 선택된 α, β는 유일하게 존재한다[5, 7, 9]. 그러므로, 메시지 m은 완전히 은닉이 되었고, 공개정보 z는 서명에 포함되어 있다는 것을 확신할 수 있다.

III. EC-KCDSA 부분 은닉서명

EC-KCDSA 부분 은닉서명에서 사용하는 공개정보와 사용자 변수는 기본 서명방식의 EC-KCDSA와 m을 제외하고 모두 동일하다.

1. 시스템 변수

$E(F_{p^m})$: 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. $|h()| \geq 160$

2. 사용자 변수

x : $0<x<q$인 비공개 서명키.

y : $y = x^{-1}G$로 계산 되는 서명자의 공개 검증키

z : 공개정보 Info의 해쉬코드 h(Info)로서 길이가 $|q|$이다.

m : 메시지 M과 h(Cert_Data)의 해쉬코드, 즉 $h(M \| h(Cert_Data))$에 r를 XOR한 값으로 표준문서 상의 중간값으로 둔다.

3. 서명생성과정

공개되는 데이터를 z라 한다. 이것은 나중에 화폐의 금액이나 유효기간으로 활용될수 있다. 만약 z가 zero이면 해쉬함수 입력 뒤에 추가 데이터를 사용하여 새로운 값을 생성한다.

그림2와 같은 과정을 거쳐 생성된 서명 데이터는 $\{\Sigma \| m \| z\}$이며, 이때 $\Sigma = \{s \| r\}$이다.

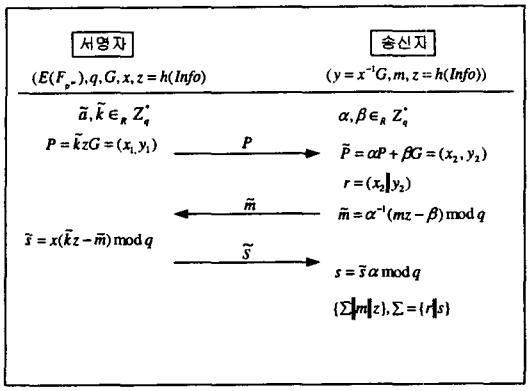

그림 2. EC-KCDSA 부분 은닉서명 과정

4. 서명 검증 과정

① 검증자는 서명된 메시지로부터 검증할 메시지 m, 서명의 첫 부분 s, 서명의 두 번째 부분 r과 공개되는 정보 z를 추출한다.

② 추출된 정보 중 $0<s<q$임을 확인한다.

③ 서명자의 공개 검증키 y를 이용하여 $r=h(x_2 \| y_2)$ 이 성립하는지 확인한다. 이때 $(x_2, y_2) = mzG + sy$ 이다.

④ ②와 ③의 확인 과정에 이상이 없다면 서명 Σ는 메시지 M에 대하여 공개 검증키 y와 z에 대응하는 비공개 검증키 x로 서명하였음이 확인된 것이다.

5. 안전성 검토

EC-KCDSA 부분 은닉서명의 서명 값 $\{s \| r\}$가 은닉되는 메시지 m과 공개되는 정보 z의 유효한 서명 값임을 보이는 식은 다음과 같다.

$$\begin{aligned}\hat{P} &= mzG + sy \\ &= mzG + \hat{s}ax^{-1}G \\ &= mzG + x(\hat{k}z - \tilde{m})ax^{-1}G \\ &= mzG + \hat{k}zaG - \tilde{m}aG \\ &= mzG + a\hat{k}zG - mzG + \beta G \\ &= a\hat{k}zG + \beta G\end{aligned}$$

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

EC-KCDSA 부분 은닉서명 프로토콜 역시 KCDSA와 같은 방법으로 증명 할 수 있다.

① $s, \tilde{s} \in Z_q^*$, $P=(x_1, y_1)$, $\hat{P}=(x_2, y_2)$는 타원곡선 $E(F_{p^m})$상의 점이라 할 때 $(\tilde{m}, P, \tilde{s})$와 (m, r, s)의 임의의 쌍에 대해 다음을 만족하는 유일한 $\alpha, \beta \in Z_q^*$가 존재한다.

$$T = (\alpha P + \beta G) = (x_2, y_2) \quad (8)$$

$$r = h(x_2 \| y_2) \quad (9)$$

$$mz = \alpha\tilde{m} + \beta \pmod q \quad (10)$$

$$s = \hat{s}\alpha \pmod q \quad (11)$$

$$\hat{k}z = \hat{s}x^{-1} + \tilde{m} \quad (12)$$

② 다음을 만족하는 $\alpha, \beta \in_R Z_q^*$를 선택한다.

$$\alpha = s\,\hat{s}^{-1} \pmod q \quad (13)$$

$$\beta = (mz - \tilde{m}\alpha) \quad (14)$$

식(13), (14)로부터 은닉서명 검증식을 이용하면 다음의 식을 얻을 수 있다.

$$\begin{aligned}&\alpha\hat{k}\tilde{z} + \beta \\ &= s\,\hat{s}^{-1}\hat{k}z + (mz - \tilde{m}\alpha) \\ &= mz + s(\hat{s}^{-1}\hat{k}z - \tilde{m}\,\hat{s}^{-1}) \\ &= mz + s(\hat{s}^{-1}(\hat{s}x^{-1} + \tilde{m}) - \tilde{m}\,\hat{s}^{-1}) \\ &= mz + sx^{-1} + s\,\hat{s}^{-1}\tilde{m} - s\,\hat{s}^{-1}\tilde{m} \\ &= mz + sx^{-1}\end{aligned} \quad (14)$$

α, β가 위 (14)식을 만족해야 하기 때문에 선택된 α, β는 유일하게 존재한다. 그러므로, 메시지 m은 완전히 은닉이 되었고, 공개정보 z는 서명에 포함되어 있다는 것을 확신할 수 있다.

IV. 결 론

전자상거래가 상당히 활성화 되었고, 이제는 실생활과 같은 화폐를 전자상거래에 사용 할 수 있어야 한다. 그러므로, 정해진 금액의 전자동전보다는 실물화폐와 같은 전자수표방식이 필요하다. 본 논문에서는 국내 전자서명 방식 표준인 KCDSA와 EC-KCDSA에 기반으로 하여 부분 은닉서명 기법을 제시하였으며, 은닉성요소와 공개정보가 포함되는 부분을 증명하였다. 이 부분 은닉서명은 사용자의 완전한 익명성의 요구 및 거스름을 필요로 하는 전자상거래 프로토콜에 사용 될 수 있을 것이다. 또한, EC_KCDSA같은 경우는 기존의 암호방법 보다 키의 길이가 상당히 짧기때문에 Smart Card를 사용한 전자상거래에도 응용되어 질수 있다.

참고문헌

[1] David Chaum, "Blind Signature for Untraceable Payments." *Crypto'82, pp. 199~203, 1982.*

[2] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash", *Crypto'88, Springer Verlag, LNCS 403, pp. 319~327, 1988.*

[3] David Chaum, "Online Cash Checks", *Eurocrypt'89, Springer Verlag, LNCS 434, pp. 288~293, 1989.*

[4] Masayuki Abe and Jan Camenisch, "Partially Blind Signature Schemes." *Proc of the 1997 Symp. on Cryptography and Information Security Workshop, 1997.*

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

[6] http://www.kisa.or.kr/technology/sub1/index-PKC.htm

[7] Moonseog Seo and Kwangjo Kim, "Blind Signature Schemes based on KCDSA and EC-KCDSA", *CISC'99, Vol.9, No.1, pp.141-150, 1999. 11.6.*

[8] Masayuki Abe and Tatsuaki Okamoto, "Provably Secure Partially Blind Signature", *CRYPTO2000, LNCS 1880, Spriger-Verlag, pp. 271~286, 2000.*

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

[10] M.Abe and J.Camenisch. "Partially blind signatures." *In the 1997 Symposium on Cryptography and Information Security, 1997.*

[11] M.Abe and E. Fujisaki. "How to date blind signatures." *In K.Kim and T. Matsumoto, editors, Advances in Cryptology - ASIACRYPT '96, LNCS 1163, Springer-Verlag, pp. 244~251, 1996.*

[12] Sangjin Kim, Ihwa Choi, Heekuck Oh, "Refunds Reusable Online Electronic Check System." *Journal of KIISC VOL.11, No.1, 2001, pp.73~85. 2001.2.*