KCDSA를 이용한 공정한 은닉 서명에 관한 연구

오형근°, 이임영
순천향대학교 컴퓨터학부

A Study on Fair Blind Signature based on KCDSA

Hyung-Geun Oh°, Im-Yeong Lee

Department of Computer Science, College of Engineering
Soonchunhyang University

요 약

은닉 서명 기법은 서명 프로토콜에서 서명자로부터 메시지 내용을 은닉시킨채 서명을 확보함으로써 개인의 프라이버시를 보호하기 위한 프로토콜이다. 이러한 은닉 서명은 전자화폐 프로토콜에서 은행으로부터 사용자의 신원을 드러내지 않고 안전하게 은행이 서명한 전자화폐를 받기 위해 사용이 되며 은행과 상점이 공모하더라도 사용자를 추적할 수가 없다. 그러나 이러한 점은 사용자로 하여금 완전한 범죄 활동의 기회를 제공하기 때문에 이에 대한 해결책으로 공정한 은닉 서명 기법이 등장하였다. 이에 본 논문에서는 국내 전자서명 알고리즘 표준인 KCDSA를 이용하여 부정한 서명문의 사용시 신뢰할 수 있는 제3자가 사용자의 신원을 밝혀 낼 수 있는 KCDSA에 기반한 공정한 은닉 서명 기법을 제안한다.

I. 서론

은닉 서명 기법은 전자화폐에 있어서 불추적성을 제공하기 위해 1982년 D.Chaum에 의해 처음으로 제안이 되었다. 은닉 서명의 기본 원리는 묵지가 내장된 봉투로서 설명될 수가 있다. 은행(서명자)이 만원에 해당하는 서명을 한다고 하자. 고객(provider, 제공자)은 묵지가 내장된 봉투에 서명 받을 용지를 넣어 은행에 보내면, 은행은 그 고객의 계좌에서 만원을 인출하고 고객이 보낸 봉투 위에다 서명을 한다. 이 서명은 내장된 묵지에 의하여 봉투 안에 있는 용지에 서명이 된다. 은행은 서명된 그 봉투를 고객에게 보낸다. 고객은 그 봉투를 제거하고 그 안에 있는 용지 위의 서명을 확인하면 된다. 전자화폐 프로토콜에 있어서 이러한 은닉 서명은 필요하게 된다.

전자화폐에 있어서 이러한 익명성은 개인의 사생활 보호라는 긍정적인 측면 이외에 위조된 돈을 식별하는 것을 방해하여 위조된 돈을 검출하지 못하게 하며 돈의 인출과 지불의 연결을 방해함으로써 완전한 돈 세탁(money laundering)과 약탈(blackmailing)을 가능하게 한다. 또한 전자화폐가 약탈자에 의해 약탈되더라도 그 익명성은 유지하게 되며 약탈자는 이러한 전자화폐를 아무런 제재 없이 사용할 수가 있게 된다. 이와 같이 익명성이 보장되는 전자화폐는 범죄자들에 의해 이용이 가능하며 각종 범죄 활동의 도구가 될 수가 있다. 따라서 다양한 단계로 제공될 수 있는 전자화폐의 익명성은 그 강도가 증가할수록 비례하여 잠재적인 위험성도 증가하게 된다. 이에 따라 익명성이 제공된 전자화폐는 그 장점에도 불구하고 많은 부작용을 불러일으키고 있으며 따라서 등장하게 된 요구 조건이 익명성 제어(Anonymity Control)이다. 그러나 이 요구조건 역시 남용하였을 경우 개인의 사생활 침해와 연관될 수가 있기 때문에 사용자 측면의 익명성과 관계 기관의 익명성 제어 부분을 절충한 방법이 필요한데, 이로부터 공정성이라는 개념이 돌출 된다. 다시 말해 공정성이란 사용자의 프라이버시를 만족시키면서 동시에 적법한 과정을 통해 익명성을 제어할 수 있

는 기능을 말한다.

2. 제안방식

본 제안 방식은 전자화폐 프로토콜에 적용할 수 있도록 국내 전자서명 표준인 KCDSA를 변형한 공정한 은닉 서명 방식이다. 또한 서명의 부정 사용시 법원과 같은 신뢰할 수 있는 제3자에 의해 부정 사용자의 신원을 검출할 수 있다.

2.1 시스템 변수

시스템 파라메터는 KCDSA에서 사용한 변수들을 대부분 사용하며 서명문은 서명자가 제공한 파라메터로부터 검증자가 추출한다.

· 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 소수이다.

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

· α, β : 검증자가 선택하는 은닉 인자

$\alpha, \beta \in_R Z_q^*$

· $h(\cdot)$: $|q|$ 비트 길이의 출력값을 갖는 충돌저항성의 해쉬함수.

· x : $0 < x < q$인 비공개 서명키

· y : $y = g^x \bmod p$로 계산되는 공개 검증키

· *Cert_Data* : 서명자의 *ID*, 시스템 변수 p, q, g와 공개검증키 y 등을 포함하는 공개키 확인서의 생성에 이용되는 사용자의 인증 데이터

· z : *Cert_Data*의 해쉬코드이다. 즉, $z = h(Cert\_Data)$.

· m : 서명될 메시지로서 $0<m<p$

· H : 메시지의 해쉬코드. 즉, $H = h(Z \,||\, m')$

· k' : $0 < k' < q$인 일회용 난수값.

· r : $r = mg^{\alpha} r'^{\beta} \bmod p$

· E : $E = m' + H \bmod q$로 계산되는 서명과정 중의 중간값.

· s : $s = xE + k' \bmod q$로부터 검증자가 추출한다. 즉, $s = s'\beta + \alpha \bmod q$

2.2 초기화 단계

● 사용자

· *ID* : 사용자 식별값으로 사용자가 랜덤하게 선택하며 비밀로 보관한다. $ID \in_R Z_p$

· I : 사용자가 생성하여 서명자에게 등록.

$I = g_1^{ID} \bmod p$

● 서명자

· p, q : 은닉 KCDSA 서명 방식에서 사용한 소수로서 서명자가 생성하여 공개한다.

· g_1, g_2, g_3 : GF(p)상의 원시원으로 서명자가 생성하여 공개한다.

· 개인키 : $x \in_R Z_p$

· 공개키 : $y = g_1^x \bmod p$

● 법원

· 개인키 : $X_T \in Z_p^*$

· 공개키 : $y_T \equiv g_2^{X_T} \bmod p$

2.3 서명 단계

서명 단계를 통해 사용자는 서명자로부터 은닉된 서명문을 얻는다. 이때 사용자의 프라이버시 보호를 위해 KCDSA 프로토콜을 변형하여 은닉 서명문을 생성하며, 부정행위 발생시에 법원에 의해 사용자의 신원을 검출할 수 있도록 하기 위해 사용자가 추적 인자를 생성하여 서명자에게 제공한다. 이때 추적 인자값은 서명자가공개한 값과 사용자가 생성한 I값, 그리고 법원의 공개키 값을 이용하여 생성하며 서명자는 사용자가 생성한 추적 인자가 올바르게 생성되었는지 확인한다.

● Step 1

사용자는 랜덤하게 $v \in Z_p^*$를 생성한다. 그리고 추적인자 A_1'과 A_2'을 생성하여 서명자에게 전송한다.

$$A_1' \equiv y_T^v \bmod p, \quad A_2' = I \cdot g_2 \cdot (g_3)^{v'^{-1}} \bmod p$$

● Step 2

서명자는 A_1', A_2'를 올바르게 생성하였는지 확인한 뒤 $k' \in_R Z_q$를 생성하고 이를 이용하여 r'을 생성한다. 그리고 r'을 사용자에게 전송한다.

$$\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1} y_T', \quad r' = g_1^{k'} \bmod p$$

● Step 3

사용자는 은닉 인자 $\alpha \in_R Z_q^*$와 $\beta \in_R Z_q^*$를 생성하고 이를 이용하여 서명자가 전송한 r'과 r값을 계산한다. 다시 이 r값과 은닉 인자 β를 이용하여 s값을 구하기 위해 은닉된 값 m'을 서명자에게 전송한다.

$$r = Ig_1^{\alpha} r'^{\beta} \pmod p \quad I' = \gamma\, \beta^{-1} \pmod q$$

● Step 4

서명자는 사용자로부터 받은 I'과 z를 연접하여 해쉬코드 값 H를 계산하고 이 값과 다시 I'을 이용하여 E값을 계산한다. 그리고 은행의 비밀키 값 x를 이용하여 s'을

계산하고 s'를사용자에게 전송한다.

$$H = h(z|I),\quad E = I + H \bmod q$$

$$s' = xE + k \bmod q$$

- Step 5

사용자는 서명자가 계산하여 보내 준 값 s'으로부터 s를 추출해 낸다. step 3에서 계산한 r과 s'으로 추출한 s 값이 서명문으로 구성한다. 사용자는 서명자로부터 전송되어 온 s'값을 이용하여 서명문이 올바른 서명문인지 검사하게 된다.

$$s = s'\beta + \alpha \bmod q \quad I \stackrel{?}{=} g_1^{-s} y^{r+\beta H} r \bmod p$$

여기서, H는 인출단계를 수행하기 전에 서명자로부터 받은 z값을 이용하여 계산한다.

$$H = h(z|I)$$

그리고나서, 서명문을 구성하기 전에 사용자는 공개 파라메터 p, y_T, g_2와 v, A_2'을 바탕으로 추적 인자를 A, A_1, A_2, A_3를 생성하여 서명문을 구성한다.

$$A \equiv (A_2' \cdot y_T)^v \cdot I \bmod p,\quad A_1 \equiv g_2^v \bmod p,$$

$$A_2 \equiv I^v \bmod p,\quad A_3 \equiv I \cdot (y_T)^v \bmod p$$

서명문 : $[(r, s), A, A_1, A_2, A_3]$

이때, 추적 파라메터에 대한 유효성 검증은 수신자에 의해 이루어지며 유효하지 않을 경우 서명문의 수신은 거부가 된다.

$$A \stackrel{?}{=} A_1 \cdot A_2 \cdot A_3 \cdot g_2 \bmod p$$

- **사용자 신원 검출 단계**

사용자 신원 검출 단계는 사용자가 서명자로부터 받은 은닉 서명문을 사용하고 난 후에 서명문을 받은 서명자가 법원에 사용자 신원 파악을 의뢰하면서 사용자 추적이 이루어진다.

step 1 : 서명자는 서명문으로부터 A_1, A_3를 법원에 전송

step 2 : 법원은 A_1과 A_3로부터 $A_3' \equiv ID^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하고, 다시 ID를 계산한다.

$$A_3' \equiv A_3^{X_T^{-1}} \bmod p \equiv I^{X_T^{-1}} \cdot g_2^v \bmod p$$

$$A_3'/A_1 \bmod p \equiv I^{X_T^{-1}} \cdot g_2^v / g_2^v \bmod p$$

$$\equiv ID^{X_T^{-1}} \bmod p$$

$$\therefore\ I = (I^{X_T^{-1}})^{X_T} \bmod p$$

3. 결론

정보화 사회가 도래와 함께 개인 정보 유출에 대한 경각심이 높아지면서 그 중요성은 날로 커지고 있으며 전자화폐와 같은 프로토콜에서는 사용자의 익명성을 위해 은닉 서명이라는 특수 서명 방식을 이용하여 사용자의 프라이버시를 보호하고 있다. 그러나 익명성 제공과 이로 인해 발생할 수 있는 문제점들은 전자화폐 시스템 구축시 사용자와 금융당국 간에 대립되고 있는 분야들로서 두 개체들의 요구 사항을 모두 만족시켜야 한다.

이에 본 고에서는 익명성을 제공하는 시스템에 있어서 발생할 수 있는 문제점들을 해결하기 위해 공정한 은닉 서명 방식을 제안하고 있다. 특히, 국내 전자서명 표준 알고리즘인 KCDSA를 전자화폐 프로토콜에 적용할 수 있도록 변형한 은닉 KCDSA 서명 방식을 제안하고 있으며 또한 서명문의 부정한 사용시에 법원에 의해 사용자의 신원을 파악할 수 있도록 하고 있다. 이렇게 정립된 모델을 통해 전자화폐 프로토콜 설계시 발생할 수 있는 문제점들을 해결하고 모든 사용 객체들과 통화 당국에 있어서 공정한 전자화폐 모델을 설계할 수 있는 기반을 제공할 수 있을 것이다.

참고문헌

[1] D.Chaum, "Blind Signautures for untraceable payments", In Advances in Cryptology, Crypto'82, pp 199-203, 1983

[2] S. von Solms and D. Naccache, "On Blind Signatures and Perfects Crimes", Computers and Security, 11 (1992) pp. 581-583

[3] G.Davida, Y.Frankel and Y.Tsiounis, "Anonymity Control in E-Cash Systems", In Proceedings of the 1st Financial Cryptography conference, Anguilla, BWI, February24-28, 1997.
http://www.ccs.neu.edu/home/hiannis/pubs.html

[4] M.Stadler, J-M.Piveteau and J.Camenisch, "Fair Blind Signatures", Advances in Cryptology-Proceedings of Eurocrypto '95, pp.209-219, 1995.

[5] 오형근, 이임영, "익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집 Vol 8. No 1. pp 109-121. 1998.

[6] 정보통신단체표준, 부가형 전자서명 방식 표준 - 제2부 : 확인서 이용 전자서명 알고리즘, 1998, http://www.kisa.or.kr