쌍짓기를 리용하지 않는 한가지 무증명서대리서명도식

리설경, 김철은

선행연구[1]에서는 무증명서전자서명도식의 개념을 처음으로 제기하였다. 그후 선행연구[2]에서 한가지 구체적인 무증명서전자서명도식을 제기하고 우연오라클모형하에서 증명가능한 안전성을 가진다는것을 증명하였다. 선행연구[3]에서는 한가지 쌍짓기를 리용하는 무증명서전자서명도식과 무증명서대리전자서명도식을 내놓았다.

그런데 타원곡선군우에서의 쌍짓기연산은 스칼라점곱하기연산보다 계산량이 더 많은것으로 하여 최근에는 쌍짓기를 리용하지 않는 서명도식에 대한 연구가 활발히 진행되고 있다. 선행연구[4]에서는 쌍짓기를 리용하지 않는 무증명서전자서명도식을 내놓았으며 특히 선행연구[5]에서는 ECDSA와 타원곡선군우에서의 리산로그문제에 기초한 열쇠생성알고리듬을 결합하여 반로그문제에 기초한 한가지 쌍짓기를 리용하지 않는 무증명서전자서명도식을 제기하였다.

론문에서는 한가지 쌍짓기를 리용하지 않는 무증명서대리서명도식을 제기하고 반로그문제의 계산복잡성에 기초하여 그것의 안전성을 밝혔다.

1. 무증명서대리서명도식의 구성

원시서명자 A가 자기의 서명권한을 대리서명자 B에게 위탁하였다고 하자. 이때 무증명서대리서명에는 원시서명자 A, 대리서명자 B, 대리서명검증자 V, 열쇠생성중심 KGC가 참가한다. 신분정보는 ID_A, ID_B이고 원시 및 대리서명자, 검증자를 사용자라고 부른다. m_w는 위탁정보를 표시하는데 이 정보에는 원시서명자와 대리서명자의 신분정보 및 위탁기간, 위탁권한의 범위와 일련의 관련파라메터들이 들어있다. Inf_{pro}는 m_w와 원시서명자의 공개열쇠를 리용하여 대리서명자에게 주는 위탁된 서명권한이다. s_p는 대리서명열쇠, $\sigma_p = Sig(s_p, M)$은 대리서명자 B가 생성한 통보문 M에 대한 A의 대리서명이다.

새로 제기하는 대리서명도식을 다음의 다항식시간알고리듬들로 구성한다.

$\leftarrow_R$는 우연선택을 의미하고 $s \cdot P$는 토대점에 관한 타원곡선스칼라점곱하기연산을 나타내며 x_W, y_W, $w \in \{P, P_{KGC}, P_A, P_B, R_A, R_B, V_A, W_A, W_B, W_B'\}$는 타원곡선점들의 x, y 자리표들이고 기호 $\|$는 련결기호이다.

Setup: 입력 1^k, 출력 s, $Params$, KGC가 실행

① $k-$bit 씨수 p와 씨체 F_p우에서 정의된 타원곡선 $E: Y^3 = X^2 + aX + b$를 선택, P를 토대점으로 하며 씨수위수 q를 가지는 타원곡선군 $E(F_p)$ 선택

② $s \leftarrow_R Z_q^*$, $P_{KGC} = s \cdot P$

③ 해쉬함수

$H_1: \{0,1\}^* \rightarrow \{0,1\}^n$, $H_2: \{0,1\}^* \rightarrow Z_q^*$, $H_3: \{0,1\}^* \rightarrow Z_q^*$, $H_4: \{0,1\}^* \rightarrow \{0,1\}^n$, $n > 0$ 선택

④ $Params=\{a,\ b,\ p,\ q,\ P_{KGC},\ P,\ H_1,\ H_2,\ H_3,\ H_4\}$, s 출력

KGC는 $Params$를 공개파라메터로 공개하고 주열쇠 s는 안전하게 보관한다.

Set-User-Key: 입력 $Params,\ ID_i,\ i\in\{A,\ B\}$, 출력 $(X_i,\ x_i)$, 사용자가 실행

① $x_i \leftarrow Z_q^*,\ X_i = x_i \cdot P$

② $(X_i,\ x_i)$ 출력

자체공개열쇠 X_i를 KGC에 보내고 자체비공개열쇠 x_i는 안전하게 보관한다.

Extract-Partial-Private-Key: 입력 $Params,\ ID_i,\ s,\ X_i,\ i\in\{A,\ B\}$, 출력 $(R_i,\ d_i)$, KGC가 실행

① $z_i = H_1(a\|b\|x_P\|y_P\|x_{P_{KGC}}\|y_{P_{KGC}}\|ID_i),\ i\in\{A,\ B\}$

② $r_i \leftarrow_R Z_q^*,\ R_i = r_i \cdot P + X_i$

③ $\lambda_i = H_2(x_{R_i}\|y_{R_i}\|z_i)$

④ $d_i = (r_i + s\lambda_i) \bmod q$

⑤ $(R_i,\ d_i)$ 출력

KGC는 $(R_i,\ d_i)$를 사용자에게 보낸다. 여기서 d_i는 신분이 ID_i인 사용자의 부분비공개열쇠, R_i는 부분공개열쇠이다.

Set-Private-Key: 입력 $Params,\ ID_i,\ R_i,\ d_i,\ X_i,\ x_i,\ i\in\{A,\ B\}$, 출력 s_i, 사용자가 실행

① $z_i = H_1(a\|b\|x_P\|y_P\|x_{P_{KGC}}\|y_{P_{KGC}}\|ID_i),\ i\in\{A,\ B\}$

② $d_i \cdot P = R_i - X_i + H_2(x_{R_i}\|y_{R_i}\|z_i)\cdot P_{KGC}$인가 검증

③ $(R_i,\ d_i)$가 유효하면 $s_i = (x_i + d_i) \bmod q$ 출력

신분정보가 ID_i인 사용자는 s_i를 자기의 완전한 비공개열쇠(서명열쇠)로 안전하게 보관한다.

Set-Public-Key: 입력 $Params,\ ID_i,\ R_i,\ i\in\{A,\ B\}$, 출력 P_i, 사용자가 실행

$P_i = R_i$를 출력, 사용자는 P_i를 자기의 완전한 공개열쇠로 한다.

Extract-Proxy-Key: 입력 $Params,\ ID_i,\ P_i,\ s_i,\ i\in\{A,\ B\},\ m_w$, 출력 s_p, 사용자들이 실행

① 원시서명자 A

$$z_A = H_1(a\|b\|x_P\|y_P\|x_{P_{KGC}}\|y_{P_{KGC}}\|ID_A)$$

$$w_A \leftarrow_R Z_q^*,\ W_A = w_A \cdot P$$

$$h_A = H_3(m_w\|x_{W_A}\|y_{W_A}\|x_{P_A}\|y_{P_A}\|x_{P_B}\|y_{P_B}\|z_A)$$

$$V_A = h_A(w_A + s_A)\cdot P$$

A는 서명권한 $Inf_{pro} = (m_w,\ W_A,\ V_A)$를 B에게 위탁

② 대리서명자 B

$$z_A = H_1(a\|b\|x_P\|y_P\|x_{P_{KGC}}\|y_{P_{KGC}}\|ID_A)$$

$$\lambda_A = H_2(x_{P_A}\|y_{P_A}\|z_A)$$

$$h_A = H_3(m_w\|x_{W_A}\|y_{W_A}\|x_{P_A}\|y_{P_A}\|x_{P_B}\|y_{P_B}\|z_A)$$

$V_A = h_A(W_A + P_A + \lambda_A \cdot P_{KGC})$가 성립하는가 검증

성립하지 않으면 서명권한을 다시 보낼것을 요구

성립하면

$$h_B = H_3(m_w \| x_{W_A} \| y_{W_A} \| x_{P_A} \| y_{P_A} \| x_{P_B} \| y_{P_B} \| z_B)$$

$$s_P = (x_{V_A} + h_B s_B) \bmod q$$

여기서 x_{V_A}는 V_A의 x자리표이며 대리서명자는 s_p를 서명열쇠로 한다.

Proxy-Signature-Generation: 입력 $Params,\ ID_B,\ m_w,\ s_P,\ W_A,\ M \in \{0,\ 1\}^*,\ P_i,\ i \in \{A,\ B\}$, 출력 σ_P, 대리서명자가 실행

$$z_B = H_1(a \| b \| x_P \| y_P \| x_{p_{KGC}} \| y_{p_{KGC}} \| ID_B)$$

$$h_B = H_3(m_w \| x_{W_A} \| y_{W_A} \| x_{P_A} \| y_{P_A} \| x_{P_B} \| y_{P_B} \| z_B)$$

$$h = H_4(h_B \| M),\ w_B \leftarrow_R Z_q^*,\ W_B = w_B \cdot P$$

$$u = x_{W_B} \bmod q,\ v = w_B{}^{-1}(us_P + h) \bmod q$$

$$\sigma_P = (u,\ v)$$

대리서명자는 $(M,\ m_w,\ W_A,\ V_A,\ \sigma_P)$를 검증자에게 보낸다.

Proxy-Signature-Verification: 입력 $Params,\ ID_B,\ P_i,\ i \in \{A,\ B\},\ M,\ m_w,\ W_A,\ V_A,\ \sigma_P$ 출력 True/Error, 대리서명검증자가 실행

① 통보문 M이 위탁정보 m_w를 리용하여 결정된 통보문인가를 검사한다. 성립하지 않으면 이 서명을 거절한다.

$$z_B = H_1(a \| b \| x_P \| y_P \| x_{p_{KGC}} \| y_{p_{KGC}} \| ID_B)$$

$$h_B = H_3(m_w \| x_{W_A} \| y_{W_A} \| x_{P_A} \| y_{P_A} \| x_{P_B} \| y_{P_B} \| z_B)$$

$$O_B = x_{V_A} \cdot P + h_B \cdot (P_B + \lambda_B \cdot P_{KGC}),\ h = H_4(h_B \| M)$$

$$v_1 = v^{-1}h \bmod q,\ v_2 = v^{-1}u \bmod q$$

$$W_B' = v_1 \cdot P + v_2 \cdot O_B,\ u' = x_{W_B'} \bmod q$$

② $u = u'$를 검증하고 성립하면 True, 아니면 Error를 출력한다.

2. 안전성분석

서명도식의 정확성은 다음의 식으로부터 나온다.

$$\begin{aligned}
W_B' &= v_1 \cdot P + v_2 \cdot O_B = \\
&= v^{-1}h \cdot P + v^{-1}u \cdot (x_{V_A} \cdot P + h_B \cdot (P_B + \lambda_B \cdot P_{KGC})) = \\
&= v^{-1}(h + u(x_{V_A} + h_B(x_B + r_B + \lambda_B s))) \cdot P = \\
&= w_B(h + us_P)^{-1}(h + u(x_{V_A} + h_B(x_B + r_B + \lambda_B s))) \cdot P = \\
&= w_B \frac{h + u(x_{V_A} + h_B(x_B + r_B + \lambda_B s))}{h + us_P} \cdot P = \\
&= w_B \frac{h + u(x_{V_A} + h_B(x_B + r_B + \lambda_B s))}{h + u(x_{V_A} + h_B(x_B + d_B))} \cdot P = \\
&= w_B \cdot P = W_B
\end{aligned}$$

P를 토대점으로 하는 순환군 $G=<P>$에서 $\forall Q\in G$, $a\cdot P=Q$인 $a\in Z_q^*$을 계산하는 문제를 리산로그문제라고 부르고 DLP로 표시한다.[1, 2, 5]

또한 $\forall Q\in G$, $u=F(v^{-1}\cdot P+u\cdot Q)$인 $(u,\ v)$를 구하는 문제를 반로그문제라고 부른다.[5] 여기서 $F(X)$는 점 X의 x자리표이다.

대리서명에 참가하는 사용자의 공개열쇠를 교체할수는 있으나 KGC의 주열쇠를 알수 없는 적수를 1형태적수 혹은 외부적수라고 하고 A_I로 표시한다.[1] KGC의 주열쇠를 알수 있으나 사용자의 비공개열쇠를 알거나 교체할수 없는 적수를 2형태적수 혹은 내부적수라고 하고 A_{II}로 표시한다. 목표 ID_*과 그것의 공개열쇠에 따르는 타당한 서명을 생성하는 1형태적수 A_I를 A_{I_a}로 표시한다.

론문에서 제기한 대리서명도식의 안전성은 다음의 정리에 의하여 담보된다.

정리 1 만일 확률적다항식시간적수 A_{I_a}가 우연오러클모형에서 대리서명도식에 대한 공격실험에서 무시할수 없는 확률로 성공할수 있다면 군 $E(F_P)$에서의 반로그문제는 다항식시간내에 풀수 있다.

정리 2 만일 확률적다항식시간적수 A_{II}가 존재하여 대리서명도식을 파괴하기 위한 경기에서 무시할수 없는 확률로 성공할수 있다면 군 $E(F_P)$에서의 반로그문제는 다항식시간내에 풀수 있다.

참 고 문 헌

[1] S. S. Al-Riyami et al.; LNCS, 2894, 452, 2003.

[2] R. Castro, R. Dahab; IACR ePrint, 196, 1, 2007.

[3] Bo Yang et al.; IACR ePrint, 721, 1, 2013.

[4] J. Baek et al.; LNCS 3650, 134, 2005.

[5] Z. Cheng et al.; IACR ePrint, 386, 1, 2018.

주체108(2019)년 6월 10일 원고접수

A Pairing-Free Certificateless Proxy Signature Scheme

Ri Sol Gyong, Kim Chol Un

In this paper, we construct a pairing-free certificateless public key proxy signature scheme which is based on semi-logarithm problem on the elliptic curve group and prove its security.

Key words: certificateless proxy signature scheme, pairing, semi-logarithm problem