서명 요청자의 계산량을 줄이는 RSA 기반 은닉서명

권문상, 조유근

서울대학교, 전기.컴퓨터공학부

User efficient RSA-based blind signature scheme

Moonsang Kwon, Yookun Cho

School of Computer Science and Engineering, Seoul National Univ.

요 약

RSA에 기반한 은닉서명 기법은 Chaum이 처음 제안하였고, Fan-Chen-Yeh가 여기에 랜덤화 특성을 추가한 은닉서명 기법을 제안하였다. 본 논문에서는 Fan-Chen-Yeh가 제안한 은닉서명 기법보다 서명 요청자의 계산량을 95% 이상 줄이는 RSA 알고리즘에 기반한 은닉서명 기법을 제안한다.

I. 서론

1. 은닉서명

1) 연구배경

은닉서명은 디지털 서명 기법의 일종으로 서명을 생성한 서명자라고 하더라도 서명으로부터 그 서명의 요청자를 알아낼 수 없다. 이런 특성을 **연계불가능성(Unlinkability)**이라고 한다[1,2]. 은닉서명 기법은 전자화폐나 전자투표와 같이 화폐의 사용자나 투표자의 익명성이 중요시되는 응용에서 사용된다. 전자화폐의 경우 어떤 구좌에서 인출된 전자화폐인지 전자화폐만 보고 알 수 없도록 하고, 전자투표의 경우 전자투표 결과 값으로부터 누구에게 발급했던 투표용지였는지 알 수 없도록 하는데 은닉서명 기법을 적용할 수 있다.

Chaum은 처음으로 연계불가능성을 만족하는 RSA 알고리즘에 기반한 은닉서명 기법을 제안하였다[1]. 하지만 Chaum이 제안한 은닉서명 기법은 Coron-Naccache-Stern이 제안한 공격방법에 취약하다. 이들이 제안한 공격방법은 선택적 메시지 공격(chosen-message attack)법의 일종으로 서로 다른 $n-1$ 개의 은닉서명 $s_1, s_2, \ldots, s_{n-1}$ 로부터 n번째 서명 s_n을 서명자와 관계없이 위조할 수 있다[3].

Fan-Chen-Yeh는 랜덤화 특성을 가지는 RSA에 기반한 은닉서명 기법을 제안하였다[2]. 이들이 제안한 은닉서명 기법은 서명 요청자가 마음대로 은닉서명 될 메시지를 선택할 수 없기 때문에 선택적 메시지 공격이 불가능하다.

본 논문에서는 Fan-Chen-Yeh가 제안한 은닉서명 기법보다 서명 요청자의 계산량을 더욱 줄이는 새로운 은닉서명 기법을 제안한다.

2) 기본 가정 및 표기법

우리가 논하는 은닉서명 기법은 서명을 요청하는 서명 요청자와 서명을 생성하는 서명자 사이에 수행된다고 가정한다. 서명자는 2개의 서로 다른 소수 p,q를 선택한다. 또, $e \cdot d \equiv 1 \bmod \Phi(n)$ 을 만족하는 2개의 랜덤 수 e,d를 선택한다. 여기서, $n = p \cdot q$ 이고 $\Phi(n) = (p-1) \cdot (q-1)$ 이다. 서명자는 (n,e) 와 단방향 해쉬 함수 h를 공개하고, (p,q,d) 는 개인키로 서명자만 알고 있다. 서명 요청자는 서명자의 공개키 (n,e) 를 미리 알고 있다고 가정한다. 또, $r \in_R Z$ 표기는 집합 Z에서 랜덤수 r을 선택하는 것을 의미한다. Z_n은 1부터 $n-1$ 사이의 정수 집합을 나타내고, Z_n^*은 1부터 $n-1$ 사이의 정수로써 n과 서로 소 관계인 정수들의 집합을 나타낸다.

II. 본문

1. 새로운 은닉서명 기법

여기서는 우리가 제안하는 새로운 은닉서명 기법을 설명한다.

1) 서명요청 및 생성

① 서명 요청자는 메시지 m에 대해 서명을 얻기 위해 $r \in_R Z_n^*$, $u,v \in_R Z_n$을 선택하고

$$\alpha \equiv r^e h(m)(u^2+v^2) \bmod n \quad (1)$$

을 계산하여 서명자에게 전송한다.

② 서명자는 α를 수신한 후, $x \in_R Z_n$를 선택하여 서명 요청자에게 전송한다.

③ 서명 요청자는

$$\beta \equiv r^e(u-vx) \bmod n \quad (2)$$

을 계산하여 서명자에게 전송한다.

④ 서명자는

$$\begin{cases} \lambda \equiv \beta^{-1} \bmod n \\ t \equiv \{\alpha(x^2+1)\beta^{-2}\}^d \bmod n \end{cases} \quad (3)$$

을 계산하여 (λ,t)를 서명 요청자에게 전송한다.

⑤ 서명 요청자는

$$\begin{cases} c \equiv (ux+v)r^e\lambda \bmod n \\ s = rt \bmod n \end{cases} \quad (4)$$

식을 통해 최종서명 (c,m,s)를 생성한다.

2) 서명검증

최종서명 (c,m,s)는

$$s^e \equiv h(m)(c^2+1) \bmod n \quad (5)$$

식을 통해 서명을 검증한다.

3) 검증식 증명

먼저 새로운 은닉서명 기법의 검증식 (5)가 만족됨을 증명한다.

정리 1. (c,m,s)가 II장 2절에서 제안한 은닉서명 기법을 통해 생성된 유효한 서명이라면 증명식 (5)를 만족한다.

증명. 식 (1),(2)를 식 (3)에 대입하면

$$\begin{aligned}
&\alpha(x^2+1)\beta^{-2} \\
&= r^e h(m)(u^2+v^2)(x^2+1)r^{-2e}(u-vx)^2 \\
&= r^{-e} h(m)(u^2+v^2)(x^2+1)(u-vx)^2 \\
&= r^{-e} h(m)(\{(ux+v)(u-vx)^{-1}\}^2+1) \\
&= r^{-e} h(m)(c^2+1)
\end{aligned}$$

이므로

$$\begin{aligned}
s = rt &\equiv r\{r^{-e}h(m)(c^2+1)\}^d \\
&\equiv rr^{-1}\{h(m)(c^2+1)\}^d \\
&\equiv \{h(m)(c^2+1)\}^d \bmod n
\end{aligned}$$

이다. 따라서,

$$\begin{aligned}
s^e &\equiv [\{h(m)(c^2+1)\}^d]^e \\
&\equiv h(m)(c^2+1) \bmod n \quad \text{이다.}
\end{aligned}$$

보조정리 1: $c=(ux+v)(u-vx)^{-1}$ 이다.

증명. 식 (4)에서

$$\begin{aligned}
\text{우변} &= (ux+v)r^e\lambda \\
&\equiv (ux+v)r^e\{r^e(u-vx)\}^{-1} \\
&\equiv (ux+v)r^e r^{-e}(u-vx)^{-1} \\
&\equiv (ux+v)(u-vx)^{-1}
\end{aligned}$$

따라서, $c=(ux+v)(u-vx)^{-1}$ 이다.

2. 분석

여기서는 새로 제안한 은닉서명 기법의 계산량과 보안성을 분석한다.

1) 계산량 비교

여기서는 RSA 알고리즘에 기반한 기존의 은닉서명 기법들과 본 논문에서 제안하는 새로운 은닉서명 기법의 서명 요청자의 계산량을 비교한다. 일반적으로 모듈러 n 연산에서 모듈러 멱승과 모듈러 역 연산은 거의 같은 계산량을 필요로 하는 것으로 알려져 있으며 모듈러 멱승 연산은 약 $0.3246\times\{\lfloor \log_2 n \rfloor+1\}$ 회의 모듈러 곱 연산이 필요한 것으로 알려져 있다[4]. 표 1에서 요청

표 1: 은닉서명 기법들의 계산량
비교($e=3$, $\lfloor \log_2 n \rfloor = 1024$ 인 경우)

기법 / 특징	Chaum	Fan-Chen-Yen	제안된 기법
랜덤화 지원	×	○	○
서명자 계산량	t_e	t_i+t_e + $4t_m$	t_i+t_e + $4t_m$
요청자 계산량	t_i+6t_m	$2t_i+16t_m$	$16t_m$
요청자 상대적 계산량 감소	95%	97%	0%

자의 계산량은 최종서명을 계산하고 검증하는데 필요한 모든 계산을 합한 것이다. t_i, t_e, t_m 은 각각 모듈러 역, 멱승 및 곱 연산을 수행하는데 걸리는 시간을 나타낸다. 요청자의 상대적 계산량 감소는 기존 기법의 계산량을 t_{old}, 제안된 기법의 계산량을 t_{new}라고 했을 때,

$$\frac{t_{old}-t_{new}}{t_{old}} \times 100$$

식을 사용하여 계산한 것이다.

제안된 기법의 경우 식 (3)에서 서명자가 $\lambda=\beta^{-1}$ 을 계산해서 돌려주기 때문에 서명 요청자의 계산량이 기존 기법에 비해 크게 감소하게 되었다. 서명 요청자는 최종서명을 계산한 후 서명이 유효한지 검사하기 때문에 서명자가 틀린 λ 값을 반환할 수 없다.

2) 보안성 분석

은닉서명도 디지털 서명의 일종이므로 디지털 서명이 만족해야 할 특성인 위조 불가능성을 만족해야 한다. 이와 더불어, 서명자라고 하더라도 서명으로부터 서명 요청자를 도출할 수 없어야 한다. 여기서는 본 논문에서 제안하고 있는 새로운 은닉서명 알고리즘이 위조 불가능성과 연계불가능성 조건을 만족함을 증명한다.

① 위조불가능성 분석

정리 2: Ⅱ장 2절에서 제안한 은닉서명 기법에서 서명 요청자는 서명자가 선택한 랜덤 수 x를 제거할 수 없다.

증명. 서명 요청자가 랜덤 수 x를 제거하려면 식 (3)에서 t가 계산될 때 (x^2+1) 이 상쇄되도록 할 수밖에 없다. 왜냐하면 α는 x값을 알기 전에 결정해야 하기 때문에다. 식 (3)에서 x값을 제거하려면 $\beta^2 \equiv (x^2+1) \bmod n$ 이 되는 β 값을 식 (2)에서 서명자에게 전송해야 한다. 그러나, 서명 요청자는 n에 대한 소인수 분해 결과를 모르기 때문에 $\beta^2 \equiv (x^2+1) \bmod n$ 을 만족하는 (x^2+1) 의 제곱근 $\beta \in Z_n^*$을 계산할 수 없다 [5]. 따라서, 서명 요청자는 x를 제거할 수 없다.

정리 3: 공격자는 Ⅱ장 2절에서 제안한 은닉서명 기법에서 생성된 서로 다른 2개의 서명 (c_1, m_1, s_1) , (c_2, m_2, s_2) 로부터 새로운 서명을 계산해 낼 수 없다.

증명. 공격자는 두 서명으로부터 다음 식을 계산해 낼 수 있다.

$$(s_1 s_2)^e \equiv h(m_1)h(m_2)(c_1^2+1)(c_2^2+1)$$

이 식으로부터

$$h(m_3)(c_3^2+1)$$
$$\equiv h(m_1)h(m_2)(c_1^2+1)(c_2^2+1) \bmod n$$

을 만족하는 (m_3, c_3) 를 계산할 수 있다면, 공격자는 새로운 서명 $s_3=(c_3, m_3, s_1 s_2)$ 를 계산할 수 있다. 그러나, 공격자는 n에 대한 소인수 분해 결과를 모르기 때문에 c_3을 계산할 수 없다 [5].

② 연계불가능성

은닉서명이 만족해야 할 조건중의 하나는 서명으로부터 서명 요청자를 도출할 수 없어야 하는 것이다. 정리 4는 서명자가 각 서명의 생성과정에서 오고 가는 모든 정보를 기록해 두었다고 할지라도 서명으로부터 서명 요청자를 도출할 수 없음을 보인다.

정리 4: Ⅱ장 2절에서 제안한 은닉서명 기법에서 서명자가 n개의 서로 다른 서명을 생성해 내는 동안 모든 정보 $(\alpha_i, x_i, \beta_i, t_i)_{1 \le i \le n}$ 를 저장해 두었다고 하자. 유효한 서명 (c, m, s) 가 주어진 경우 서명자는 각각의 기록들에 대해 다음

식들을 만족하는 (r_i', u_i', v_i') 을 계산할 수 있다.

$$\alpha_i \equiv (r_i')^e h(m)(u_i'^2 + v_i'^2) \bmod n \quad (6)$$

$$u_i' - v_i' x_i \equiv \beta_i (r_i')^e \bmod n \quad (7)$$

$$u_i' x_i + v_i' \equiv c\beta_i (r_i')^e \bmod n \quad (8)$$

$$s \equiv r_i' t_i \bmod n \quad (9)$$

증명. (c,m,s) 은 유효한 서명이므로 식 (10)을 만족한다.

$$s^e \equiv h(m)(c^2+1) \bmod n \quad (10)$$

또, 각 $(\alpha_i, x_i, \beta_i, t_i)_{1 \le i < n}$ 들에 대해 식 (11)이 만족된다.

$$t_i^e \equiv \alpha_i (x_i^2+1)\beta_i^2 \bmod n \quad (11)$$

식 (9-11)로부터 식 (12)를 계산할 수 있다.

$$r_i' \equiv \{\alpha_i^{-1}(x_i^2+1)\beta_i^2 h(m)(c^2+1)\}^d \quad (12)$$

식 (7,8)로부터 u_i'과 v_i'을 다음과 같이 계산할 수 있다.

$$u_i' \equiv \beta_i (r_i')^{-e}(1+cx_i)(1+x_i^2)^{-1} \quad (13)$$

$$v_i' \equiv \beta_i (r_i')^{-e}(c-x_i)(1+x_i^2)^{-1} \quad (14)$$

식 (12-14)를 식 (6)의 우변에 대입하면

$$\begin{aligned} \text{우변} &\equiv (r_i')^e h(m)\beta_i^2 (r_i')^{-2e}(1+x_i^2)^{-2} \\ &\quad \times \{(1+cx_i)^2 + (c-x_i)^2\} \\ &\equiv (r_i')^{-e} h(m)\beta_i^2 (1+x_i^2)^{-2} \\ &\quad \times \{(1+c^2)(1+x_i^2)\} \\ &\equiv (r_i')^{-e} h(m)\beta_i^2 (1+x_i^2)^{-1}(1+c^2) \\ &\equiv \alpha_i' \bmod n \end{aligned}$$

서명자가 모든 기록들에 대해 식 (6-9)를 만족하는 (r_i', u_i', v_i') 를 계산할 수 있기 때문에 2개 이상의 서명이 발급된 경우 서명자라고 하더라도 유효한 서명을 특정 기록과 연관시킬 수 없다. 따라서, 서명으로부터 서명 요청자를 도출할 수 없다.

III. 결론

본 논문에서는 서명 요청자의 계산량을 기존 기법에 비해 최고 97%까지 줄이는 RSA 알고리즘에 기반한 은닉서명 기법을 제안하고 계산량과 보안성을 증명하였다. 서명 요청자의 계산량이 매우 적기 때문에 이동 기기와 같이 계산능력이 떨어지는 저전력 시스템에서 유용하게 사용될 수 있을 것이다.

참고문헌

[1] D. Chaum, "Blind Signatures for Untraceable Payments," Crypto'82, LNCS, pp. 199-203, 1983.

[2] C.I. Fan, W.K. Chen and Y.S. Yeh, "Randomization enhanced Chaum's blind signature scheme", Computer Communications, vol. 23, no. 17, pp. 1677-1680, Nov. 2000.

[3] J. Coron, D. Naccache and J. Stern. "On the security of RSA padding". Crypto'99, LNCS, pp. 1-18, 1999.

[4] C.I. Fan, and C.L. Lei, "User efficient blind signatures". Electronics Letters, vol.34, no.6, pp. 544-546, 1998.

[5] M. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization", MIT Technical Report, MIT/LCS/TR-212, 1979.