서명 요청자의 계산량을 감소시키는 RSA에 기반한 개선된 부분은닉서명 알고리즘

(RSA-Based Enhanced Partially Blind Signature Algorithm Minimizing Computation Of The Signature Requester)

권 문 상 † 조 유 근 ††
(Moon Sang Kwon) (Yookun Cho)

요 약 '부분은닉서명(Partially Blind Signature)' 기법은 전자화폐나 전자투표와 같이 사용자의 프라이버시가 중요시되는 응용에서 사용된다. 본 논문에서는 서명 요청자의 계산량을 줄이는 RSA 알고리즘에 기반한 부분은닉서명 기법을 제안한다. 서명 요청자는 메시지를 은닉하여 서명자에게 전송하고 서명자가 생성한 중간 서명으로부터 최종 서명을 생성하는 과정에서 계산을 필요로 한다. 논문에서 제안하고 있는 기법은 서명 요청자가 적은 계산량을 필요로 하는 모듈러 합과 곱 연산만으로 최종 서명을 계산할 수 있게 하므로 서명 요청자의 계산량을 많이 감소시킨다. 따라서, 이동통신 기기나 스마트카드, 전자지갑 같이 계산능력이 떨어지는 장치들에서 사용하기에 적합하다.

키워드 : 부분은닉서명 ; 은닉서명

Abstract Partially blind signature scheme is used in applications such as electronic cash and electronic voting where the privacy of the signature requester is important. This paper proposes an RSA-based enhanced partially blind signature scheme minimizing the amount of computation of the signature requester. The signature requester needs computation in blinding the message to the signer and in generating the final signature using the intermediate signature generated by the signer. Since the proposed scheme enables the signature requester to get the final signature just by using modular additions and multiplications, it decreases computation of the signature requester considerably. So, the proposed partially blind signature scheme is adequate for devices such as mobile device, smart-card, and electronic purse that have relatively low computing power.

Key words : Partially Blind Signature; Blind Signature

1. 서 론

1983년, D. Chaum이 '은닉서명(Blind Signature)'의 개념을 소개하고 RSA에 기반한 은닉서명 알고리즘을 제안하였다 [1, 2]. 은닉서명은 전자서명의 일종으로 서명 요청자가 서명자에게 메시지의 내용을 보여주지 않은 상태에서 서명자로부터 메시지에 대한 유효한 서명을 얻어내기 위한 서명 기법이다. 서명자는 서명할 때 메시지의 내용과 이에 대한 최종 서명 값을 알지 못한다. 은닉서명에는 서명을 요청하는 요청자(Requester), 서명 요청을 접수하고 정당한 경우 중간서명을 생성하는 서명자(Signer 또는 Notary), 그리고 생성된 서명을 검증하는 검증자(Verifier) 등 3개의 주체가 존재하는데, 여기서 '중간 서명'이라고 하는 이유는 서명자가 생성하는 것이 최종 서명이 아니라 요청자가 그 결과 값으로부터 최종 서명을 계산하기 때문이다. 서명자는 나중에 생성된 서명으로부터 원래의 서명 요청자를 확인할 수도 있고 그렇지 않을 수도 있는데 이는 응용에 따라 달라진다. 이 때, 유효한 서명으로부터 서명을 요청했던 요청자를 도출해 내는 것을 *'연계(Link)'*라고 한다. Horster와 Petersen은 서명의 연계 가능 정도에 따라 은닉서명 기법을 hidden signature, weak blind signature, interactive blind signature, strong blind

† 비 회 원 : 서울대학교 컴퓨터공학과
kmscom@ssrnet.snu.ac.kr
†† 종신회원 : 서울대학교 컴퓨터공학과
cho@ssrnet.snu.ac.kr
논문접수 : 2001년 12월 13일
심사완료 : 2002년 3월 4일

signature 등 4종류로 분류하였는데 [3] 본 논문에서는 요청자가 원하지 않는 경우 연계가 불가능한 'interactive blind signature' 또는 'strong blind signature' 알고리즘에 대해서만 다루도록 한다. 요청자, 서명자, 검증자 등 3 주체가 다음과 같은 특성을 만족해야 한다.

- 서명자가 서명을 생성할 때 서명자는 자신이 서명할 메시지의 내용을 알지 못한다. 이 때, 서명 자체를 생성하는 것이 아니라 그 결과로부터 서명을 계산할 수 있는 '중간 서명'을 생성한다.
- 요청자는 서명자가 생성한 중간 서명으로부터 최종 서명을 생성할 수 있다.
- 검증자는 메시지와 최종 서명으로부터 그 유효 여부를 결정할 수 있다. 하지만, 요청자가 중간 서명을 요구하기 위해 서명자에게 전송했던 데이타와 최종 서명 사이의 관계를 알 수는 없다.
- 서명자가 서로 다른 n개의 데이타에 대해 n개의 중간 서명을 생성한 경우 요청자는 최대 n개의 유효한 서명만 확보할 수 있다. 즉, $n+1$번째 서명을 위조할 수 없다. 이는 서명 결과가 전자화폐 등을 나타내는 경우 꼭 만족해야 할 조건이다.

은닉서명의 불연계성(Unlinkability) 및 이로 인한 익명성(Anonymity)은 전자화폐나 온라인 투표 등의 응용에 적합하다. 하지만, 은닉서명 기법에서는 서명 안에 공통적인 정보를 넣을 수 없다. 공통적인 정보란 그 값을 통해 서로 다른 서명을 구분할 수 없는 정보로써 전자화폐의 경우 화폐의 가치나 유효기간 등을 예로 들 수 있다. 응용에 따라 은닉서명 기법으로 생성되는 서명에 공통의 정보를 포함시켜야 할 경우가 있다. 예를 들어, 은행에서 발행하는 전자화폐의 경우 화폐의 단위나 유효기간을 은닉서명 안에 포함시키면 은행이 전자화폐의 이중사용(Double Spending)을 방지하기 위해 저장해야 할 정보의 양을 크게 줄일 수 있다 [4]. 이러한 필요로 인해 제안된 것이 *부분은닉서명*(Partially Blind Signature) 알고리즘이다. 부분은닉서명 기법을 사용할 경우 서명자는 자신이 서명할 데이타의 일부분은 알고 있고 나머지 부분은 알 지 못한다. 이 때, 알려진 부분이 공통정보이다. x와 $f(x)$를 각각 서명자의 비밀키 및 공개키라 하고, $S(x, m)$을 메시지 m에 대해 비밀키 x를 사용하여 생성한 서명이라 하자. 또한, 검증함수 $V(f(x), m, S(x, m))$를 사용하여 서명의 유효성을 검증할 수 있다고 가정하자. 부분은닉서명 기법에서 요청자는 랜덤수 r과 은닉함수 $B()$를 사용하여 메시지 m을 '내용확인불가' 메시지인 $B(m, r)$로 만든 후 공통정보 a와 함께 서명자에게 전송한다. a는 서명자가 자신이 만들어 내는 모든 서명에 공통으로 포함되기를 희망하는 값이다. 서명자는 서명 $S(x, a, B(m, r))$을 생성하여 요청자에게 전달하고, 요청자는 은닉해제 함수 $U()$를 사용하여 $U(S(x, a, B(m, r))$ 계산을 통해 최종 서명 $S(x, a, m)$을 얻어낼 수 있다. 일반적인 '부분은닉서명' 기법의 동작방식은 다음과 같다 [4].

1. 요청자가 은닉 메시지 $B(m, r)$을 계산한 후 $\{a, B(m, r)\}$을 서명자에게 전송한다.
2. 서명자는 자신의 비밀키 x를 사용하여 $\{a, B(m, r)\}$을 서명한 $S(x, a, B(m, r))$을 요청자에게 전송한다.
3. 요청자는 $S(x, a, m)=U(S(x, a, B(m, r)),$을 통해서 최종 서명 $S(x, a, m)$을 생성하고 검증식 $V(f(x), a, m, S(x, a, m))$을 통해 서명의 유효성을 검사한다.

서명 요청자는 은닉 메시지 $B(m, r)$을 만들 때와 중간 서명 $S(x, a, B(m, r))$에서 최종 서명 $S(x, a, m)$을 생성할 때 계산을 하는데 지금까지의 부분은닉서명 알고리즘들은 이 과정에서 모듈러 역(Modular Inverse)이나 모듈러 멱승(Modular Exponentiation) 같이 많은 계산량을 필요로 하는 연산을 수행해야 했기 때문에 이동통신 기기나 스마트카드, 전자지갑 같이 계산 능력이 떨어지는 장치들이 사용하기에 어려움이 있었다. 하지만, 최근에 발표된 Fan-Lei 부분은닉서명 기법이나 Chien-Jan-Tseng 부분은닉서명 기법은 서명 요청자가 몇 개의 모듈러 곱(Modular Multiplication) 및 합, 해쉬 연산만으로 최종 서명을 생성할 수 있기 때문에 서명 요청자의 계산량을 크게 줄일 수 있게 되었다 [5,6]. 본 논문에서는 Chien-Jan-Tseng이 제안한 'RSA에 기반한 부분은닉서명 기법'을 개선하여 서명 요청자의 계산량을 더욱 줄이는 새로운 부분은닉서명 알고리즘을 제안하고 보안성을 증명하였다.

본 논문의 구성은 다음과 같다. 2장에서는 지금까지 알려진 몇 가지 부분은닉서명 알고리즘들을 살펴본다. 3장에서는 RSA에 기반한 새로운 '부분은닉서명' 기법을 설명한다. 4장과 5장에서는 새로 제시한 부분은닉서명 기법을 보안적인 측면과 복잡도 측면에서 각각 분석한다. 마지막으로 6장에서 결론을 맺고 향후 연구 과제를 논의한다.

2. 관련 연구

D. Chaum이 1983년에 처음으로 제안한 은닉서명 알고리즘은 RSA 알고리즘에 기초한 것이었다 [1]. 서명자는 (p, q, d)를 개인키로, (e, n)을 공개키로 하고 있

다. 여기서 p, q는 소수이고 $n=p\cdot q$를 만족한다. 또, $e\cdot d\equiv 1 \bmod (p-1)\cdot(q-1)$을 만족한다. 요청자는 서명자에게 메시지를 보내기 전에 메시지의 내용을 은닉하기 위해 메시지 m에 랜덤 수 r^e을 곱한 $r^e\cdot m \bmod n$을 서명자에게 전달한다. 서명자는 메시지의 내용을 모른 채 $\delta'=(r^e\cdot m)^d=r\cdot m^d \bmod n$을 계산하고 그 결과를 요청자에게 돌려준다. 요청자는 $\delta=r^{-1}\cdot\delta'=r^{-1}\cdot r\cdot m^d \bmod n$을 계산하여 최종 서명 $m^d \bmod n$을 얻어낸다. 서명자는 r을 모르기 때문에 서명할 때 m을 알 수 없고, 최종 서명 δ 또한 알 수 없다. 따라서, 최종서명으로부터 주어진 서명의 요청자를 알 수 없다. 즉, 연계가 불가능하다.

D. Chaum의 은닉서명 기법이 소인수분해 문제의 어려움에 기반한 RSA 알고리즘을 사용한데 반해 이 후에 발표된 논문들은 유한체 상에서 이산 로그(Discrete Logarithm)를 찾는 문제나 재곱근을 구하는 문제(Quadratic Residue)에 기반하고 있다. J. Camenisch 등은 미국 전자서명 표준인 DSS(Digital Signature Standard)에 근간한 은닉 DSA 서명과 메시지를 복원할 수 있는 은닉 Nyberg-Rueppel 서명을 제안하였다[7-9]. 국내에서는 한국형 전자서명 표준인 KCDSA (Korean Certificate-based Digital Signature Algorithm)에 기반한 은닉 KCDSA 알고리즘이 제안되었다[10, 11]. P. Horster 등은 ElGamal 서명 알고리즘에 근간한 일반적인 은닉서명 기법을 제안하였다 [3,12-16]. Pointcheval 등은 Schnorr 서명 알고리즘에 근간한 좀 더 효율적인 은닉서명 기법을 제안하였다 [17,18]. 이 알고리즘들은 모두 이산 로그를 찾는 문제에 기반하여 설계되었는데 이 알고리즘들의 서명자와 요청자 및 검증자의 계산량을 표로 나타내면 표 1과 같다.

모듈러 멱승 연산과 모듈러 역 연산은 거의 같은 양의 계산을 필요로 하며, 모듈러 멱승 계산은 약 $0.3246\times\{\lfloor \log_2 n \rfloor+1\}$번의 모듈러 곱셈 연산이 필요한 것으로 알려져 있다 [19]. 표 1에서 모든 알고리즘들이 요청자가 1회 이상의 모듈러 멱승 연산을 수행해야 하기 때문에 비교적 많은 계산을 해야 함을 알 수 있다.

1996년에 Fan과 Lei가 제안한 은닉서명 알고리즘은 Quadratic Residue(QR) 이론에 기반하고 있다[20-22]. 어떤 수 $a\in Z_n$에 대한 모듈러 n연산에서 $x\in Z_n^*$, $x^2\equiv a \bmod n$을 만족하는 x가 존재하는 경우 a를 Quadratic Residue라고 하고 x를 $a \bmod n$의 제곱근(Square Root) 이라고 한다. 이 때, 모듈러 n 연산에서 n의 약수로 큰 소수를 포함하고 있고 n의 소인수분해 결과가 알려지지 않은 경우 a에 대한 제곱근(Square Root)을 구하는 것이 불가능한 것으로 알려져 있다 [23]. Fan-Lei 은닉서명 알고리즘의 경우 서명을 얻기 위해 요청자는 $14t_m+2t_n$, 즉 14회의 모듈러 곱셈과 2회의 해쉬 계산만 수행하면 되기 때문에 기존의 은닉서명 기법들에 비해 요청자의 계산량을 극적으로 감소시킨 알고리즘이다. 이 알고리즘은 후에 Shao가 은닉서명의 조건을 만족하지 못하므로 은닉서명 기법이 아니라고 주장하였으나 Fan-Lei에 의해 은닉서명 속성을 만족함이 증명되었다[24, 25].

'부분은닉서명' 알고리즘은 '은닉서명' 알고리즘과는 달리 서명자가 생성하는 은닉서명 안에 서명과 분리될 수 없는 정보를 포함하고자 하는 응용에서 사용된다. Abe-Fujisaki는 RSA 알고리즘에 기반한 부분은닉서명 알고리즘을 제안했다[4]. 하지만 이 방법은 서명 요청자의 계산량이 많은 단점이 있다.

Fan과 Lei는 자신들이 제안한 은닉서명 기법에 기반한 새로운 부분은닉서명 알고리즘을 제안하였다[6]. Fan-Lei 부분은닉서명 기법은 Quadratic Residue 이론에 기초하고 있으며 요청자는 20회의 모듈러 곱 연산과 3회의 해쉬 연산만으로 최종 서명을 얻어낼 수 있다. 이것은 기존 기법들이 모듈러 역이나 모듈러 멱승 연산을 수행해야 했던 것에 비교해 볼 때 계산량을 크게 감소시킨다.

Fan-Lei 부분은닉서명 알고리즘이 기존 기법에 비해 서명 요청자의 계산량을 크게 줄이기는 했지만 현재 널리 사용되고 있는 RSA 알고리즘에 기반하지 않았다는

표 1 은닉서명 알고리즘들의 계산량 비교 : t_e, t_m, t_i는 각각 모듈러 멱승(Exponentiation), 곱(Multiplication), 역(Inverse) 연산을 계산하는데 걸리는 시간이다.

	Blind RSA	Blind DSA	Blind Nyberg-Rueppel	Blind Horster	Blind Schnorr
요청자	t_i+4t_m	$2(t_e+t_i)+7t_m$	$2t_e+3t_m$	$2t_e+t_i+3t_m$	$2(t_e+t_m)$
서명자	t_e	t_e+2t_m	t_e+t_m	t_e+t_m	t_e+t_m
검증자	$2t_m$	$3t_e+t_i$	$2(t_e+t_m)$	t_e+t_m	$2t_e+t_m$

단점이 있었다. 이에, Chien-Jan-Tseng은 RSA 알고리즘에 기반하면서도 서명자가 모듈러 역이나 멱승 연산을 하지 않고도 최종 서명을 얻어낼 수 있는 부분은닉서명 알고리즘을 제안하였다[5]. 이들이 제안한 부분은닉서명 알고리즘은 RSA 알고리즘에 기반하였고, 서명 요청자는 21회의 모듈러 곱과 2회의 해쉬 연산만으로 최종 서명을 얻어낼 수 있다. 해쉬 연산은 모듈러 곱 연산과 거의 같은 정도의 계산량을 필요로 하기 때문에 Fan-Lei 부분은닉서명 알고리즘과 Chien-Jan-Tseng 부분은닉서명 알고리즘에서 서명 요청자의 계산량은 거의 같다고 할 수 있다.

3. 개선된 부분은닉서명 기법

Chien-Jan-Tseng의 부분은닉서명 기법은 많이 사용되고 있는 RSA 알고리즘에 기반을 두고 있고 서명 요청자의 계산량을 매우 많이 줄이지만 좀 더 서명 요청자의 계산량을 줄일 여지가 있다. 이 장에서는 이를 고려하여 RSA 알고리즘에 기반한 새로운 부분은닉서명 기법을 제안한다.

서명자는 두 개의 큰 소수 p와 q를 생성하고, $\phi(n)=(p-1)\times(q-1)$을 계산한다. 또한, $e\times d\equiv 1 \bmod \phi(n)$, $e=3$인 d를 계산하고 (e, n)을 공개키로 공표 한다. 개인키는 (p, q, d)이고 서명자만 알고 있다. 서명자는 또한 자신이 사용할 단방향 해쉬함수 $h(x)$를 공표한다. 보통 MD5나 SHA1이 사용된다[26, 27]. 서명자의 키에 대한 인증서를 서명 요청자가 이미 가지고 있고 유효하다고 가정한다. 새로운 부분은닉서명 기법은 3단계로 이루어져 있다.

- **서명 요구단계:** 요청자가 서명을 받고자 하는 메시지를 m이라고 하자. 서명에 들어갈 공통의 정보 a는 미리 요청자와 서명자 사이에 알려져 있다고 가정한다.
  1. 요청자는 랜덤 수 $r, u, v\in Z_n$을 선택하고 $\alpha\equiv r^e\cdot h(m)\cdot(u^2+v^2) \bmod n$을 계산한 후 (a, α)를 서명자에게 전송한다.
  2. 서명자는 1개의 랜덤 수 $x\in Z_n$을 선택하여 요청자에게 보낸다.
  3. 요청자는 $\beta\equiv r^e\cdot f(u, v, x) \bmod n$을 만족하는 β를 계산하여 서명자에게 전송한다.
- **중간 서명 생성단계:** 서명자는 $\lambda\equiv\beta^{-1} \bmod n$ $t\equiv\{h(a)\cdot(\alpha\cdot(x^2+1)\cdot\lambda^2)^2\}^d$식을 계산하여 (λ, t) 값을 요청자에게 전송한다.
- **최종 서명 생성단계:** 요청자는 다음과 같이 서명자의 응답으로부터 서명을 계산한다.

$c\equiv g(u, v, x)\cdot\lambda r^e\equiv g(u, v, x)\cdot f(u, v, x)^{-1} \bmod n$

$s\equiv t\cdot r_2 \bmod n$ (a, c, s)가 메시지 m에 대한 서명이 된다. 서명의 유효 여부는 $s^e\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2 \bmod n$식을 만족하는지 여부를 확인함으로써 가능하다.

여기서 $f(u, v, x)=ux\pm v$, $g(u, v, x)=u\mp vx$이거나 $f(u, v, x)=u\pm vx$, $g(u, v, x)=ux\mp v$이다. 이하 증명 및 분석에서는 $f(u, v, x)=ux+v$, $g(u, v, x)=u-vx$라고 가정한다.

정리 1. 위와 같이 계산되는 서명 (a, c, s)가 메시지 m의 서명이라면 $s^e\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2 \bmod n$을 만족한다.

증명.

$s^e\equiv(t\cdot r^2)e\equiv t^e\cdot r^{2e}$

$\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2\cdot r^{-2e}\cdot r^{2e}\leftarrow$ 보조정리 1적용

$\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2 \bmod n$

$\therefore s^e\equiv\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2 \bmod n$

보조정리 1.

$t^e\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2\cdot r^{-2e} \bmod n$

증명.

$$
\begin{aligned}
t^e &\equiv [\{h(a)\cdot(\alpha\cdot(x^2+1)\cdot\lambda^2)^2\}^d]^e \\
&\equiv h(a)\cdot(\alpha\cdot(x^2+1)\cdot\lambda^2)^2 \\
&\equiv h(a)\cdot(r^e h(m)(u^2+v^2)\cdot(x^2+1)\cdot\lambda^2)^2 \\
&\equiv h(a)\cdot(h(m)\cdot r^e\cdot((u^2+v^2)(x^2+1))\cdot\lambda^2)^2 \\
&\equiv h(a)\cdot(h(m)\cdot(u^2x^2+u^2+v^2x^2+v^2)\cdot r^e\cdot\lambda^2)^2 \\
&\equiv h(a)\cdot(h(m)\cdot((ux+v)^2+(u-vx)^2)\cdot r^e\cdot\beta^{-2})^2 \\
&\equiv h(a)\cdot(h(m)\cdot((ux+v)^2+(u-vx)^2)\cdot r^e\cdot \\
&\qquad (r^e(ux+v))^{-2})^2 \\
&\equiv h(a)\cdot(h(m)\cdot((ux+v)^2+(u-vx)^2)\cdot(ux+v)^{-2}\cdot \\
&\qquad r^e\cdot r^{-2e})^2 \\
&\equiv h(a)\cdot(h(m)\cdot(1+((u-vx)(ux+v)^{-1})^2)\cdot r^{-e})^2 \\
&\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2\cdot r^{-2e} \\
&\qquad \leftarrow c=(u-vx)(ux+v)^{-1} \text{ 적용} \\
\therefore\ t^e &\equiv h(a)\cdot(h(m)\cdot(1+c^2))^2\cdot r^{-2e} \bmod n
\end{aligned}
$$

정리 1과 보조정리 1은 새로 제안한 부분은닉서명의 검증식이 성립함을 보이고 있다. $f(u, v, x)$와 $g(u, v, x)$식의 다른 경우에도 정리 1 및 보조정리 1과 같이 증명됨을 확인할 수 있다.

4. 보안성 분석

이 장에서는 새로 제안한 부분은닉서명 알고리즘의 보안적인 측면을 분석한다. $f(u, v, x)=ux+v$, $g(u, v, x)=u-vx$라고 가정한다. 다른 경우에도 비슷하게 분석

할 수 있다.

4.1 알고리즘 랜덤화

제안된 알고리즘은 서버가 랜덤 수 x를 선택하여 전체 프로토콜이 운용되도록 하는 랜덤화(Randomization) 기법을 사용하고 있는데 이는 선택적 메시지 공격(chosen-text attack)을 막기 위해서이다[28]. 제안된 알고리즘에서 서명자가 랜덤 수 x를 요청자에게 전달하고 요청자는 이를 사용하여 프로토콜을 진행해야 한다. 요청자가 랜덤요소 (x^2+1)을 제거하려면 $\beta^2=(x^2+1) \bmod n$을 만족하는 β를 계산할 수 있어야 한다. 하지만, 요청자는 n에 대해 p, q를 모르기 때문에 (x^2+1)의 제곱근(Square Root)을 구할 수 없다 [23, 29]. 만일 서명자가 먼저 랜덤 수 x를 선택하여 요청자에게 전송하고 요청자가 이에 맞게 (a, α, β)를 서명자에게 전송하도록 한다면 요청자는 $\alpha=(x^2+1)^{-1}\times\alpha'$이 되도록 설정하여 랜덤 항목 x를 제거할 수 있을 것이다. 따라서, 서명자가 선택하는 x는 요청자가 예측 불가능한 랜덤 수이어야 한다.

4.2 부분은닉 속성 측면

제안된 부분은닉서명 알고리즘에서 요청자는 공통정보 a를 제거할 수 없어야 한다. 요청자가 공통정보 a를 제거하려면 $\alpha^2\equiv h(a)^{-1} \bmod n$을 만족하거나 $h(a)\equiv\beta^4 \bmod n$을 만족하는 α나 β를 계산할 수 있어야 한다. 하지만 요청자는 n에 대해 p, q를 모르기 때문에 제곱근이나 거듭제곱근을 구할 수 없다[23, 29].

4.3 위조 불가능성

공격자는 서명을 위조할 수 없어야 한다. 공격자가 유효한 서명들을 가지고 있지 않은 경우를 고려해 보자. $h(a)$, $h(m)$, c가 주어진 경우 공격자는 $s\equiv\{h(a)\cdot(h(m)\cdot(1+c^2))^2\}^d \bmod n$을 계산할 수 있어야 하는데 이것은 d를 모르기 때문에 불가능하다. 만약 s, $h(a)$, $h(m)$이 주어진 경우라면 $c\equiv((s^e\cdot h(a)^{-1})^{1/2}\cdot h(m)^{1/2}-1)^{1/2} \bmod n$을 만족하는 c를 계산할 수 있어야 하지만 역시 p와 q를 모르기 때문에 불가능하다[23, 29]. 이제 유효한 서명 (a, c, s, m)이 주어진 경우를 고려해 보자. $h(m)\neq(m') \bmod n$인 새로운 메시지 m'에 대한 서명 s'을 생성하려면 $(h(m)^{-1}\cdot\cdot h(m'))^{2d}$을 계산할 수 있어야 한다. 즉, s'은 아래 식을 통해 계산할 수 있다.

$$s'\equiv s\cdot(h(m)^{-1}\cdot h(m'))^{2d}\equiv(h(a)\cdot(h(m')\cdot(1+c^2))$$

그러나, 공격자는 임의의 메시지 m'에 대해 $h(m')^{2d}$을 계산할 수 없기 때문에 이 것은 불가능하다. 이제 2개 이상의 유효한 서명 (a, c_1, s_1, m_1), (a, c_2, s_2, m_2)이 주어진 경우를 고려해 보자. 두 서명으로부터 아래의 식을 유도할 수 있다.

$$(s_1s_2)^e\equiv h(a)^2(h(m_1)h(m_2))(1+c_1^2)(1+c_2^2))^2 \bmod n$$

공격자가 새로운 서명 (a, c_3, s_1s_2, m_3)을 만들려면 아래의 식을 만족하는 c_3, m_3을 계산할 수 있어야 한다.

$$c_3\equiv((h(a)(h(m_1)h(m_2)(1+c_1^2)(1+c_2^2))^2\cdot h(m_3)^{-1})^{1/2}-1)^{1/2} \bmod n$$

그러나, 공격자는 n의 소인수분해 결과를 모르기 때문에 위 식을 만족하는 c_3을 계산할 수 없다[23, 29].

4.4 불연계성

불연계성을 만족시키려면 검증자가 서명을 검증할 때 서명으로부터 요청자를 알아낼 수 없어야 한다. 즉, 어떤 요청자의 요청으로 해당 서명이 생성되었는지 검증할 수 없어야 한다. 정리 2는 이러한 불연계성(Unlinkability) 요구사항이 만족됨을 보이고 있다.

정리 2. 임의의 유효한 서명 (a, c, s, m)과 서명자가 과거에 서명을 생성하면서 저장해 둔 각각의 정보 $(a, \alpha_i, x_i, \beta_i, t_i)_{1\le i\le n}$들에 대해 다음 검증식들을 만족하는 r'_i, u'_i, v'_i를 계산해 낼 수 있다.

$$\alpha_i\equiv(r'_i)^e\cdot h(m)\cdot(u'^2_i+v'^2_i) \bmod n \quad \text{식(1)}$$

$$u'_ix_i+v'_i\equiv\beta_i\cdot(r'_i)^{-e} \bmod n \quad \text{식(2)}$$

$$u'_i-v'_ix_i\equiv c(u'_ix_i+v'_i)\equiv c\beta_i\cdot(r'_i)^{-e} \bmod n \quad \text{식(3)}$$

$$s\equiv t_i(r'_i)^2 \bmod n \quad \text{식(4)}$$

증명. (a, c, s, m)은 유효한 서명이므로 식(5)를 만족한다.

$$s^e\equiv h(a)\{h(m)(1+c^2)\}^2 \bmod n \quad \text{식(5)}$$

또, 각 $(a, \alpha_i, x_i, \beta_i, t_i)_{1\le i\le n}$들에 대해 식(6)이 만족된다.

$$t_i^e\equiv h(a)\{\alpha_i(x_i^2+1)\beta_i^{-2}\}^2 \bmod n \quad \text{식(6)}$$

식(4-6)으로부터 식(7)을 계산할 수 있다.

$$(r'_i)^e\equiv(s^et_i^{-e})^{1/2}\equiv\{h(m)(1+c^2)\alpha_i^{-1}(1+x_i^2)^{-1}\beta_i^2\} \bmod n \quad \text{식(7)}$$

또, 식(2,3)으로부터 아래와 같이 u'_i과 v'_i를 계산할 수 있다.

$$u'_i\equiv\beta_i(r'_i)^{-e}(c+x_i)(1+x_i^2)^{-1} \bmod n \quad \text{식(8)}$$

$$v'_i\equiv\beta_i(r'_i)^{-e}(1-cx_i)(1+x_i^2)^{-1} \bmod n \quad \text{식(9)}$$

식(7-9)를 식(1)의 우변에 대입하면,

$$\text{우변}\equiv(r'_i)^e\cdot h(m)\cdot\beta_i^2(r'_i)^{-2e}(1+x_i^2)^{-2}\{(c+x_i)^2+(1-cx_i)^2\}$$

$$\equiv(r'_i)^{-e}\cdot h(m)\cdot\beta_i^2(1+x_i^2)^{-2}\{c^2+x_i^2+1+c^2x_i^2\}$$

$$\equiv(r'_i)^{-e}\cdot h(m)\cdot\beta_i^2(1+x_i^2)^{-2}\{(1+c^2)(1+x_i^2)\}$$

$$\text{djj}\equiv(r'_i)^{-e}\cdot h(m)\cdot\beta_i^2(1+x_i^2)^{-1}(1+c^2)$$

표 2 부분은닉서명 알고리즘들의 계산량 비교 : t_e, t_m, t_i, t_h는 각각 모듈러 멱승(Exponentiation), 곱셈(Multiplication), 역(Inverse), 해쉬 연산을, $t_{1/8}$은 3제곱근을 계산하는데 걸리는 시간이다.

	Fan-Lei 알고리즘[6]	Abe-Fujisaki 알고리즘[4]	Chien-Jan-Tseng 알고리즘[5]	제안된 알고리즘
수학적 기반	QR	RSA	RSA	RSA
랜덤화	사용	지원 안함	사용	사용
요청자 계산량	$20t_m+3t_h$	$2t_e+t_i$ $+t_h+4t_m$	$21t_m+2t_h$	$18t_m+2t_h$
서명자 계산량	$t_{1/8}+t_i+9t_m$	t_i+t_e	$t_i+t_e+6t_m$	$t_i+t_e+6t_m$

$\equiv \{h(m)(1+c^2)\alpha_i^{-1}(1+x_i^2)^{-1}\beta_i^2\}^{-1}\cdot h(m)\cdot$

$\beta_i^2(1+x_i^2)^{-1}(1+c^2)\equiv\alpha_i$이다. 즉, 식(1)이 만족됨을 확인할 수 있다.

정리 2는 모든 유효한 서명 (a,c,s,m)에 대해 서명자가 서명을 생성할 때마다 저장해 두었던 각 정보 $(a,\alpha_i,x_i,\beta_i,t_i)_{1\le i\le n}$들이 만족시키는 r'_i, u'_i, v'_i들을 계산해 낼 수 있음을 보이고 있다. 이것은 어떤 정보 $(a,\alpha_i,x_i,\beta_i,t_i)_{1\le i\le n}$가 주어진 서명과 연관되었을 확률이 $\frac{1}{n}$이 된다는 뜻이므로 $n\ge 2$인 경우 서명자는 어떤 서명을 특정 서명 요청자와 연관시킬 수 없다.

5. 복잡도 분석

요청자는 서명 요구단계에서 8회의 모듈러 곱셈과 1회의 해쉬 계산이 필요하고, 최종 서명 생성 및 확인단계에서 10회의 모듈러 곱셈과 1회의 해쉬 계산이 필요하다. 서명자의 경우 중간 서명 생성단계에서 6회의 모듈러 곱셈과 1회의 모듈러 역 및 모듈러 멱승 계산을 필요로 한다. 이를 기존 부분은닉서명 알고리즘들과 비교하면 표 2와 같다.

[5]에서 서명자의 계산량을 $t_i+2t_e+6t_m$이라고 하였으나 실제 서명자의 계산량은 다음과 같이 $t_i+2t_e+6t_m$임을 알 수 있다.

β^{-1} 계산 : 모듈러 역 1회

$t'\equiv h(a)(\alpha(x^2+1)\beta^{-2})^2$ 계산 : 모듈러 곱 6회

$t\equiv t'^{d} \bmod n$ 계산 : 모듈러 멱승 1회

따라서, 제안된 알고리즘은 서명자의 경우 Chien-Jan-Tseng과 같은 양의 계산을 필요로 하고 요청자의 경우 모듈러 곱셈 연산을 3개 줄인다. 이는 기존 기법에 비해 약 14% 정도의 계산량 감소이다. 만약 e가 3이 아니라 랜덤수로 선택된다면 Chien-Jan-Tseng 알고리즘의 경우 $3t_e+15t_m+2t_n$만큼의 계산량을 필요로 하고, 제안된 알고리즘의 경우 $2t_e+14t_m+2t_n$ 만큼의 계산량을 필요로 한다. 이는 $t_e\approx 0.3246\times\{[\log_2 n]+1\}\times t_m$이고 $t_m=t_n$임을 고려해 볼 때 약 33% 정도의 계산량 감소 결과를 얻을 수 있음을 알 수 있다.[5, 19].

6. 결 론

부분은닉서명 알고리즘은 서명자가 은닉데이타에 대한 서명을 생성하면서 자신이 생성하는 서명의 일부로 공통의 정보가 포함되기를 희망할 때 사용하는 알고리즘이다. 지금까지 여러 가지 부분은닉서명 기법들이 제안되었지만 대부분의 경우 요청자가 비교적 많은 계산량을 요구하는 모듈러 멱승이나 모듈러 역 계산을 필요로 하는 것들이었다. 하지만 최근에 몇 번의 모듈러 곱연산만으로 부분은닉서명을 생성할 수 있는 기법들이 제안되었다 [5,6]. 특히 Chien-Jan-Tseng이 발표한 부분은닉서명 기법은 널리 사용되고 있는 RSA 알고리즘에 기반하고 있기 때문에 의미가 크다고 하겠다.

본 논문에서는 Chien-Jan-Tseng이 제안한 부분은닉서명 알고리즘을 더욱 최적화하여 서명 요청자의 계산량을 줄이는 부분은닉서명 알고리즘을 제안하고 이를 분석하였다. 제안된 부분은닉서명 알고리즘은 Chien-Jan-Tseng의 부분은닉서명 기법과 같이 RSA 알고리즘에 기반하고 있으면서 서명 요청자의 계산량을 좀 더 줄이고 있다. 제안된 알고리즘은 서명 요청자의 계산량을 매우 적게 요구하기 때문에 계산능력이 떨어지는 이동 기기나 전자 지갑, 스마트카드 같은 응용에서 사용하기에 적합하다. 또한, 부분은닉 속성을 이용하여 전자화폐나 전자투표 같은 응용을 개발할 때 사용될 수 있다.

향후 연구과제로 본 논문에서 제안한 효율적인 부분은닉서명 기법을 바탕으로 하여 '공평한 부분은닉서명(Fair partially blind signature) 기법'이나 '그룹 부분은닉서명(Group partially blind singature) 기법', '임계

부분은닉서명(Threshold partially blind signature) 기법' 등에 대해 연구해야 할 것이다.

참 고 문 헌

[1] Chaum, D., *"Blind Signatures for Untraceable Payments,"* Advances in Cryptology - CRYPTO'82, Lecture Notes in Computer Science, Springer-Verlag, pp. 199-203, 1983.

[2] Chaum, D., *"Blind Signature System,"* In D. Chaum, editor, Advances in Cryptology - CRYPTO'83, Lecture Notes in Computer Science, Springer-Verlag, pp. 153-153, 1984.

[3] Horster, P. and Petersen, H., *"Classification of blind signature schemes and examples of hidden and weak blind signatures,"* Presented at the Rump Session of Eurocrypt '94, Perugia, Italy, 6 pages, 1994.

[4] Abe, M. and Fujisaki, E., *"How to Date Blind Signatures,"* Advances in Cryptology - Asiacrypt'96, Lecture Notes in Computer Science 1163, Springer Verlag, pp. 244-251, 1996.

[5] Chien, H.Y., Jan, J.K. and Tseng, Y.M., *"RSA-Based Partially Blind Signature with Low Computation,"* In Proceedings of the Eighth International Conference on Parallel and Distributed Systems, pp. 385-389, 2001.

[6] Fan, C.I. and Lei, C.L., *"Low-computation partially blind signatures for electronic cash,"* IEICE Trans. Fundamentals, Vol.E-81-A, No.5, pp. 818-824, 1998.

[7] National Institute of Standards and Technology, *"Digital signature standard (DSS),"* Federal Information Processing Standards Publication FIPS PUB 186, U.S. Department of Commerce, May 1994.

[8] Nyberg, K. and Rueppel, R., *"A new signature scheme based on the DSA giving message recovery,"* Proc. 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, 4 pages, Nov. pp. 3-5, 1993.

[9] Camenisch, J.L., Piveteau, J-M. and Stadler, M.A., *"Blind Signatures Based on the Discrete Logarithm Problem,"* Proc. Eurocrypt'94, Springer Verlag, pp. 428-432, 1994.

[10] KCDSA Task Force Team., *"KCDSA : The Korean Certicate-based Digital Signature Algorithm,"* Contribution to IEEE P1363a, August 1998.

[11] 서문석,김광조, *"KCDSA 및 EC-KCDSA에 근간한 은닉 서명,"* Conference on Information Security and Cryptology (CISC'99), Vol.9, No.1, pp. 141-150, 1999.

[12] ElGamal, T., *"A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms,"* IEEE Transactions on Information Theory, Vol.31, No.4, pp. 469-472, Jul. 1985.

[13] Horster, P., Petersen, H. and Michels, M., *"Meta message recovery and meta blinded signature schemes based on the discrete logarithm problem and their applications,"* Advances in Cryptology - Asiacrypt'94, Lecture Notes in Computer Science 1163, Springer Verlag, pp. 185-196, 1994.

[14] Horster, P., Michels, M. and Petersen, H., *"Efficient blind signature schemes based on the discrete logarithm problem,"* Technical Report TR-94-6, University of Technology Chemnitz-Zwickau, 4 pages, Jun 1994.

[15] Horster, P., Michels, M. and Petersen, H., *"Meta-ElGamal signature schemes,"* Proc. 2. ACM conference on Computer and Communications security, Fairfax, Virginia, 2-4, pp. 96-107, Nov. 1994.

[16] Horster, P., Michels, M. and Petersen, H., *"Meta Message recovery and Meta Blind signature schemes based on the discrete logarithm problem and their applications,"* Advances in Cryptology - Asiacrypt '94, University of Wollongong, NSW, Australia, Nov. 28 - Dec. 1st, 12 pages, 1994.

[17] Schnorr, C.P., *"Efficient Identification and Signatures for Smart Cards,"* In G. Brassard, editor, Advances in Cryptology - CRYPTO'89, Vol.435, Lecture Notes in Computer Science, Santa-Barbara, California, Springer Verlag, pp. 235-251, 1990.

[18] Pointcheval, D. and Stern, J., *"Provably Secure Blind Signature scheme,"* Advances in Cryptology - Asiacrypt'96, Lecture Notes in Computer Science 1163, Springer Verlag, pp. 252-265, 1996.

[19] Chen, C.Y., Chang, C.C. and Yang, W.P., *"Hybrid method for modular exponentiation with precomputation,"* Electronics Letters, Vol.32, No.6, pp. 540-541, 1990.

[20] Fan, C.I. and Lei, C.L., *"An Efficient Blind Signature Scheme Based on Quadratic Residues,"* IEE Electronics Letters, Vol.32, No.9, pp. 814-816, 1996.

[21] Fan, C.I. and Lei, C.L., *"Low-Computation Blind Signature Schemes Based on Quadratic Residues,"* IEE Electronics Letters, Vol.32, No.17, pp. 1569-1570, 1996.

[22] Fan, C.I. and Lei, C.L., *"User efficient blind signatures,"* Electronics Letters, Vol.34, No.6, pp. 544-546, 1998.

[23] Menezes, A.J., Ooschot, P.C. and Vanstone, S.A., *"Handbook of Applied Cryptography,"* Boca Raton, ISBN:0-8493-8523-7, pp. 74-75, 1997.
[24] Shao, Z., *"Improved user efficient blind signatures,"* Electronics Letters, Vol.36, No. 16, pp. 1372-1374, 2000.
[25] Fan, C.I. and Lei, C.L., *"Cryptanalysis on improved user efficient blind signatures,"* Electronics Letters, Vol.37, No.10, pp. 630-631, 2001.
[26] Rivest, R.L., *"MD5 Message-Digest Algorithm,"* IETF RFC 1321, Apr. 1992.
[27] FIPS 180-1., *"Secure Hash Standard,"* NIST. US Dept. of Commerce, 1995.
[28] Desmedt, Y. and Odlyzko, A.M., *"A chosen text attack on the RSA cryptosystem and some discrete logarithms schemes,"* Advances in Cryptology - Crypto'85 (H. C. Williams, ed.), Lecture Notes in Computer Science, Vol.218, Springer Verlag, pp. 516-521, 1986.
[29] Rabin, M., *"Digitalized Signatures and Public-Key Functions as Intractable as Factorization,"* MIT Technical Report, MIT/LCS/TR-212, 1979.

권 문 상
1991년 ~ 1995년 서울대학교 컴퓨터공학과 학사. 1995년 ~ 1997년 서울대학교 컴퓨터공학과 석사. 1997년 ~ 현재 서울대학교 컴퓨터공학과 박사과정. 관심분야는 운영체제, 시스템 및 네트워크 보안, 암호학 등

조 유 근
1971년 서울대학교 공대 졸업. 1978년 미네소타대학교 전산학과 박사. 1979년 ~ 현재 서울대학교 컴퓨터공학부 교수. 관심분야는 알고리즘, 운영체제, 데이타 구조 등