Rabin 기반의 은닉 서명 프로토콜

*황 성 민°, *최 영 근, *김 순 자
*경북대학교 전자전기공학부

Blind Signature Protocol Based Rabin-Type

*Sung-Min Hwang°, *Yeong-Geun Choe *Soon-Ja Kim
*School of Electronics and Electrical Eng., Kyungpook National University
*{mivri°, ind}@palgong.knu.ac.kr, snjkim@ee.knu.ac.kr

요 약

전자현금(Electronic Cash)이나 전자투표(Electronic Vote)에의 응용을 목적으로 Chaum에 의해 처음으로 RSA 기반의 은닉서명(Blind Signature) 개념을 제안하였다[1]. 휴대폰, 스마트카드와 같은 작은 용량의 메모리와 연산 능력을 가진 장치에서는 연산량이 작은 은닉서명 프로토콜을 필요로 한다. 본 논문에서는 사전계산과 효율적인 이차잉여 선택 방법을 이용해서 Rabin 기반 전자서명 방법에 은닉서명 개념을 도입하여 효율적인 Rabin 기반의 은닉 서명 프로토콜을 제안한다.

1. 서론

최근 이동통신 가입자가 증가하면서 무선인터넷 사용자도 늘어나고 있다. 아울러 무선 인터넷 기반 구조를 이용한 각종 컨텐츠 사업이 활발해지고, 유선에서만 이뤄지던 전자상거래가 무선 환경으로 이동하고 있다. 이런 무선 환경에서는 제한적인 대역폭과 휴대폰, PDA(Personal Device Assistant) 등의 휴대 단말기의 낮은 연산 처리 능력 시스템의 제약조건 때문에 프로토콜 설계시 효율성이 중요시 되고 있다. 또 스마트카드, 자바카드 등이 전자화폐, 신용카드, 직불카드에 이용되면서 연산량을 최소화하는 암호기술이 필수 요건이 되고 있다.

전자화폐나 전자투표와 같은 개인의 프라이버시를 요구하는 응용분야에서는 이를 만족시키기 위해 1982년 Chaum에 의해 처음으로 RSA 서명에 은닉서명을 제안되었고, 그 후 계속 발전하고 있다[1]. 본 논문에서 제안하는 Rabin 기반의 은닉서명 프로토콜은 RSA와 마찬가지로 큰수의 소인수분해의 어려움에 근거를 둔 암호 시스템이다[2, 3]. Rabin은 RSA에 비해 멱승 계산이 작기 때문에 다른 암호시스템보다 효율적이다. 처음 Rabin 기반의 전자서명 방법이 개발된 후 Kurosawa와 Williams에 의해 좀 더 효율성을 개선하고자 연구가 계속 되었고, 그 후 Kurosawa와 Ogata에 의해 다른 Rabin 기반의 서명 방식 보다 효율적인 은닉서명을 제안되었다[4]. 본 논문에서는 효율적인 Rabin 기반의 서명에 은닉서명 기법을 적용시키고 그 효율성과 안전성에 대해 알아보고자 한다. 우선 Rabin 기반의 서명에 은닉서명을 적용시키기 위해 2절에서는 수학적 기본지식을, 3절에서는 Kurosawa가 제안한 Rabin 기반 서명을 살펴보고, 4절에서는 Rabin 기반의 은닉서명을 제안하고, 그 효율성과 안전성을 알아 볼 것이다.

2. 수학적 배경

Rabin 암호 시스템은 이차잉여(quadratic residue)를 이용해서 서명을 생성한다. 이차잉여의 존재유무를 표시하기 위해 *Legendre-Jacobi* 기호를 이용하며 값이 1이면 이차잉여이고, 값이 -1이면 이차비잉여이다. 기호와 계산방법은 다음과 같다.

$$\left(\frac{a}{p}\right)_L = a^{(p-1)/2} \bmod p \quad (p\text{는 2보다 큰 소수})$$

$$\left(\frac{a}{N}\right)_J \triangleq \left(\frac{a}{p_1}\right)_L^{e_1} \cdots \left(\frac{a}{p_r}\right)_L^{e_r} \quad (N = p_1^{e_1} \cdots p_r^{e_r}\text{인 합성수})$$

$$\left(\frac{a}{N}\right)_J = \begin{cases} 1 & \text{if } a=1 \\ (-1)^{(N^2-1)/8}\left(\frac{a/2}{N}\right) & \text{if } a=\text{even} \\ (-1)^{(N-1)(a-1)/4}\left(\frac{N \bmod a}{a}\right) & \text{otherwise} \end{cases}$$

또, 서명값 생성을 위해 $a=x^2 \bmod N$ 를 만족하는 x를 찾는 방법은 각각의 $x_p=a^{(p+1)/4} \bmod p$ 와 $x_q=a^{(q+1)/4} \bmod q$ 를 계산한 후 중국인의 나머지(Chiness Remainder Theorem)정리를 이용한다. 여기서 a는 이차잉여이고, N은 p와 q의 곱이다[5].

3. 효율적인 Rabin 타입 전자서명[4]

Kurosawa의 서명을 살펴보기에 앞서 사용되는 파라메타 값을 먼저 설정하면 다음과 같다.

- 비밀키 : 소수 p,q
- 공개키 : $N=p\times q$

Rabin의 전자서명 방법은 서명받고자 하는 문서(M)와 랜덤한 수(R)을 해쉬한 값($h=H(M\|R)$)이 이차잉여가 될 때까지 R값 선택을 반복하게 된다. Kurosawa와 Ogata는 이런 반복과정을 줄이기 위해 항상 이차잉여가 되도록 h값에 대한 이차잉여 유무에 관한 타입을 다음과 같이 정의한다.

$$type(u,v) \triangleq \begin{cases} 0 & \text{if } u=v=1 \\ 1 & \text{if } u=1,\ v=-1 \\ 2 & \text{if } u=-1,\ v=1 \\ 3 & \text{if } u=v=-1 \end{cases}$$

정의된 타입에 의해 이차비잉여일 때는 이차비잉여 값을 곱하므로서 항상 이차잉여가 되도록 한다.
이런 방법을 이용해서 2가지 방식의 서명 알고리즘을 제안했다.

- 기본 서명 방식

① $h=H(M)$
② $u=\left(\frac{h}{p}\right)$, $v=\left(\frac{h}{q}\right)$
③ $type(u,v)=i$에 대해 $a_i h=x^2 \bmod N$인 x를 찾는다.

여기서 a_1는 법 p에 대해서는 이차잉여이고, 법 q에 대해서는 비이차잉여인 값이다. 또, a_2는 법 p에 대해서는 비이차잉여이고, 법 q에 대해서는 이차잉여이다. a_0은 1이고, a_3는 a_1a_2이다.

- 개선된 서명 방식

① $h=H(M)$
② $h_p=h^{(p-3)/4} \bmod p$, $h_q=h^{(q-3)/4} \bmod q$
$h_p^*=h_p h \bmod p$, $h_q^*=h_q h \bmod q$
$u=h_p h_p^* \bmod p$, $v=h_q h_q^* \bmod q$
③ $type(u,v)=i$에 대해 $x_p=\beta_i h_p^* \bmod p$, $x_q=\gamma_i h_q^* \bmod q$
④ x_p와 x_q, 중국인의 나머지정리를 이용해서 x를 찾는다.

여기서 a_i값은 $a_0=1$, $a_1=2$, $a_2=-2$, $a_3=-1$ 로 고정시키고, $\beta_i=a_i^{(p+1)/4} \bmod p$, $\gamma_i=a_i^{(q+1)/4} \bmod q$ 은 효율성을 높이기 위한 사전계산 값이다. 서명값 쌍(M,x)은 $x^2=a_i H(M) \bmod N$을 만족하면 서명값이 유효한 것이고, 만족하지 않으면 위조된 것이다.

4. 제안하는 Rabin 타입 은닉서명 프로토콜

앞에서 살펴본 2가지 방식의 전자서명에 대해 은닉성을 추가하는 방법을 제시하고자 한다. 제시하는 프로토콜에서 사용되는 파라메타값들은 3절에서 사용된 것들을 그대로 사용할 것이다.

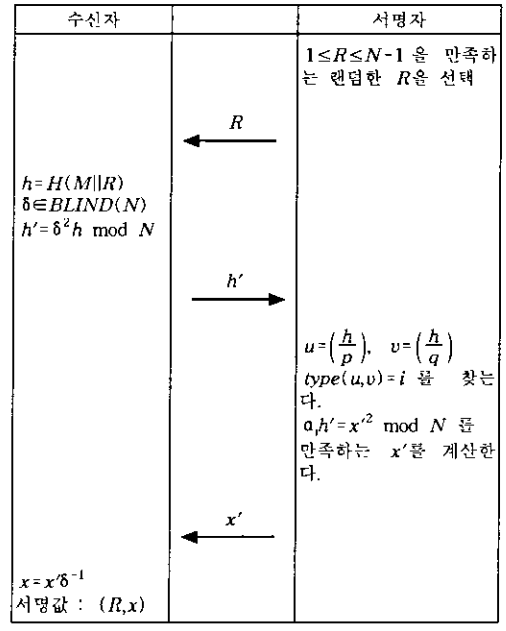

그림 1. 기본 은닉서명 프로토콜

4.1 은닉서명 프로토콜

랜덤한 k비트의 p와 q를 값과 랜덤한 a_1, a_2를 생성한다. 이렇게 해서 공개키와 비밀키가 생성된다. 여기서 비밀키는 두 개의 소수, p와 q이고, 공개키는 $N(=pq), a_1, a_2$이다. 생성된 키쌍을 가지고 은닉성을 추가한 프로토콜은 그림 1, 2와 같다.

4.2 은닉서명 프로토콜 분석

은닉성 제공을 위한 새로운 값을 정의한다.

$BLIND(p)=\{x\in QR(p)\,|\,\exists x^{-1}\in Z_p^*, xx^{-1}\equiv 1 \bmod p\}$

$BLIND(p)$는 이차잉여이고, 법 p에서 역원(inverse)을 갖는 값이다.

은닉서명은 그 기반되는 서명구조를 변형함이 없이 새로운 은닉요소(blind factor) 값만 추가함으로서 사용자의 익명성을 보장할 수 있다. 본 논문에서 제안된 프로토콜이 3절에서 소개한 전자서명 구조를 그대로 갖고 있음을 다음식으로서 증명이 된다.

$H(M\|R)=h=h'\delta^{-2}=x'^2\delta^{-2}=(x\delta^{-1})^2\delta^2=x^2$

따라서, 기반이 되는 전자서명이 갖는 안전성을 그대로 갖는다. 기반이 되는 전자서명인 Rabin 기반의 암호시스템은 랜덤 오라클 모델(random oracle model)아래서 선택적 평문 공격(chosen plaintext attack)에 대해서는 안전하다는 것이 Bellare와

Rogaway에 의해 증명되었다. 본 논문에서 제안하는 방식도 랜덤 오라클 모델을 따르고 있으므로 선택적 평문 공격에 대해서는 안전하다[3, 6, 7, 8, 11].

또, 기존의 반복적 계산에 의해 이차잉여값을 찾는 것을 이차잉여 유무에 따라 4가지 타입을 정의하고 그 타입에 따라 항상 이차잉여가 되게 하므로써 다른 Rabin 기반 서명방식보다도 효율성을 높였다.

$$\begin{cases} E[T_{Rabin}] = T_0 + 4 \times T_1 \\ T_{Basic} = T_0 + T_1 \\ T_{Improved} = T_0 + \min(\tau, T_1) \end{cases}$$

여기서 T_0는 법(modulo) N에서 제곱근을 계산하는데 걸리는 시간이고, T_1은 *Legendre* 기호의 계산 시간이고, τ는 법 p와 법 q에서의 곱셈수행 시간이다.

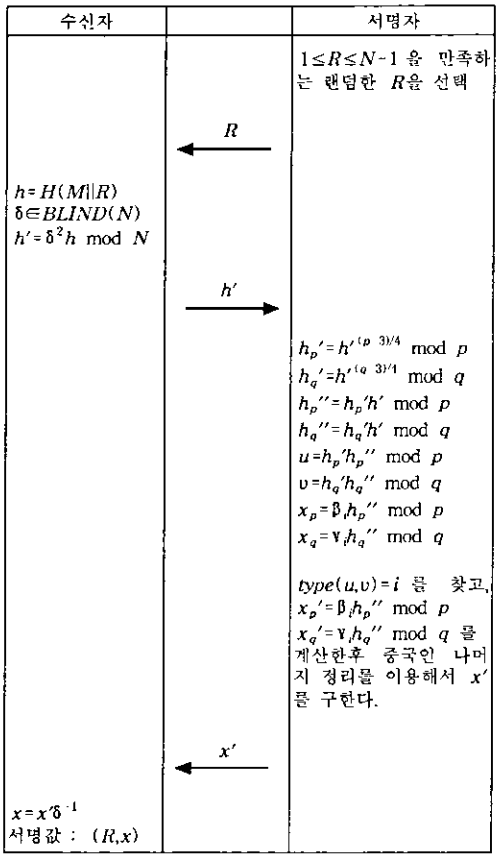

그림 2. 개선된 은닉서명 프로토콜

5. 결론 및 향후 연구

본 논문에서는 기존의 효율적인 Rabin 기반의 전자서명 방법에 은닉성을 추가한 프로토콜을 제안하였다. 제안한 프로토콜이 기반 전자서명 구조를 그대로 갖고 있으면서 익명성을 갖는 것을 보였고, 그에 대한 선택적 평문 공격에 대한 안전성과 다른 Rabin 암호 시스템과의 효율성도 비교하였다.

최근에는 전자현금과 전자투표처럼 은닉서명 응용에 익명성 오용을 방지하기 위한 공정성 기능에 관한 연구가 필요하다[9, 12]. 따라서 공정성 기능을 추가한 Rabin 암호 시스템 기반의 은닉서명 방법을 향후 추가 연구가 필요하다.

또한 Rabin 기반의 전자서명은 선택적 암호문 공격(chosen ciphertext attack)에 취약하므로 이에 대한 연구도 진행되어야 한다.

6. 참고문헌

[1] D. chaum. "Blind Signatures for Untraceble Payments,". In *Crypto'82*, Plenum pages 199-203, 1983

[2] M. Rabin, "Digtal signatures," In *Foundations of secure computation*, R.A. Millo et. l. eds, Academic Press, 1978

[3] M. Rabin, "Digital signatures and public key functions as intractable as factorization," *MIT Laboratory for Computer Science Report TR-212*, January 1979

[4] K. Kurosawa and W. Ogata. "Efficient Rabin type Digital Signature Scheme,". *Designs, Codes and Cryptography*, 1998

[5] L. Adleman, K. Manders and G. Miller. "On taking roots in finite fields,". In *Proceedings of 18th IEEE symposium on Foundations of Computer Science*, pages 175-178, 1977

[6] M. Bellare and P. Rogaway. "Random oracles are practical: a paradigm for designing efficient protocols,". In *Proceeding of 1st CCCS, pages 62-73*, 1993

[7] M. Bellare and P. Rogaway. "The Exact Security of Digital Signature - How to Sign with RSA and Rabin,". In *Proc. of Eurocrypt'96, LNCS 1070, pages 399-416*, 1996

[8] A. Juels, M. Luby and R. Ostrovsky. "Security of Blind Digital Signatures," In *Crypto'97*, LNCS 1294, pages 150-164, 1977

[9] S. von Solms and D. Naccache. "On blind signatures and perfect crimes," in Computer & Security, 11(6):581-583

[10] R. L. Rivest, A. Shamir and L .Adleman. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems,". In *Communications of the ACM*, vol.21, no.2, pages 120-126, 1978

[11] D. Pointcheval and J. Stern. "Security Arguments for Digital Signatures and Blind Signatures,". In *Journal of Cryptology*, vol.13, no 3. pages 361-396, 2000

[12] J. Camenish and U. Maurer. "Digital Payment Systems with Passive Anonymity Revoking Trustees," in *Journal of Computer Security*, vol. 5, no. 1, IOS Press, 1997