자체인증 개인식별정보

박성준°, 양형규, 원동호
성균관대학교 정보공학과

Self-certified Identity

Sung Jun Park , Hyung Kyu Yang and Dong Ho Won
Department of information Engineering
Sung Kyun Kwan University

요 약

본 논문에서는 새로운 개념인 자체인증 특성을 갖는 개인식별정보 방식을 제안한다. 제안한 방식은 자체인증 공개키 개념을 개인식별정보에 적용한 방식이다.
그리고 자체인증 개인식별정보 방식을 사용하여 역설적인 id-based 암호시스템(id-based identification scheme, id-based 서명방식, id-based 키분배방식 등)을 구성하였다.
제안한 방식의 안전성은 고차잉여류 문제와 이산대수 문제에 근거하며,Schnorr 방식과 비슷한 효율성을 가지는 암호시스템이다.

1. 서론

일반적으로 공개키 암호시스템에서의 공개키 디렉토리를 제거하는 방법은 인증자에 기반(certification-based)을 둔 방식과 개인식별정보에 기반(identity-based)을 둔 방식의 2가지 방식이 존재한다.

인증자에 기반을 둔 방식에서는 신뢰하는 센터가 각 사용자의 공개키를 사용자의 개인식별정보와 함께 센터의 비밀키로 서명한 인증자를 발행함으로서 각 사용자의 공개키를 인증하게 된다. 그러나 개인식별정보에 기반을 둔 방식에서는 각 사용자의 개인식별정보 자체가 공개키가 됨으로 특별한 인증 절차를 요구하지 않는다.

위에서 언급된 2방식의 차이점은 다음과 같다.

- 인증자에 기반을 둔 방식
  센터는 각 사용자의 비밀키를 알수 없고,사용자는 인증자를 사용한다.
- 개인식별정보에 기반을 둔 방식
  센터는 각 사용자의 비밀키를 알수 있고,사용자는 인증자를 사용안한다.

Girault는 개인식별정보에 기반을 둔 방식이면서도 센터가 각 사용자의 비밀키를 알수 없는 역설적인 개인식별정보에 기반을 둔 방식을 제안하였다.[G1] 그러나 제안한 방식도 인증자를 사용함으로 엄밀한 의미에서는 개인식별정보에 기반을 둔 방식이라고 볼 수 없다.

또한 Girault는 인증자에 기반을 둔 방식과 개인식별정보에 기반을 둔 방식의 중간 개념인 자체인증 공개키(self-certified public key) 방식을 제안하였다.[G2] 자체인증 공개키 방식은 별도의 인증자를 요구하지 않고 공개키 자체가 인증자 역할을 하는 방식이다. 그러나 자체인증 공개키 방식도 공개키와 다른 별도의 인증자를 두지 않지만,공개키 자체가 인증자 역할을 함으로 엄밀한 의미에서는 역시 개인식별정보에 기반을 둔 방식은 아니다.

특히,Girault는 3가지 신뢰 유형을 정의하였다.

- 신뢰 유형 1
  신뢰 센터가 모든 사용자의 비밀키를 아는 유형인 시스템으로 센터는 언제든지 각 사용자를 흉내낼 수있다.
- 신뢰 유형 2
  신뢰 센터가 각 사용자의 비밀키를 알수는 없으나,사용자를 흉내낼 수가 있다.
- 신뢰 유형 3
  신뢰 센터가 신뢰 유형2와 마찬가지로 각 사용자의 비밀키를 알 수 없고,또한 센터는 각 사용자를 흉내낼 수 없다. 여기서 흉내낼 수 없다 함은 실질적으로는 흉내를 낼 수 있으나 후에 센터의 거짓 행위를 알 수 있다는 것이다.

본 논문에서는 자체인증 공개키 방식을 개인식별정보에 기반을 둔 방식에 적용하여 만든 자체인증 개인식별정보(self-cerrtified identity) 방식을 제안한다. 자체인증 개인식별정보 방식은 자체인증 공개키 방식에서 인증자의 역할을 하는 공개키가 바로 개인식별 정보인 경우이다.

특히,자체인증 개인식별정보 방식을 사용하여 참된 의미의 역설적인 개인식별정보에 기반을 둔 암호시스템(identity-based identification scheme,identity-based signature scheme and identity-based key exchange protocol)을 제안한다.

제안한 방식들의 안전성은 고차잉여류 문제(γ^{th}-residuosity problem)와 이산대수 문제의 어려움에 기반을 두고 있으며,신뢰 유형 3을 만족한다.

더우기 제안한 방식의 효율성은 Schnorr 방식과 유사하다.[Sc1][Sc2]

2. 기본 정리

이 절에서는 본 논문에서 사용하는 기본 개념들을 정리한다.[PW][PJKW][Z]

양의 정수 γ,n이 주어질 때 정수 z가 다음의 조건을 만족하면 γ^{th}-residue라 한다.

[조건] $gcd(z,n)=1$이고 $z \equiv x^{\gamma} \bmod n$를 만족하는 x가 존재한다

위의 조건을 만족하지 않는 z는 γ^{th}-nonresidue라 한다.

γ^{th}-Residuosity 문제 (γ^{th}-RP)란 주어진 양의 정수 $z \in Z_n^*$ 의 γ^{th}-Residuosity를 결정하는 것이다.

n이 소수인 경우 위의 문제는 쉽게 해결되지만,n의 소인수를 알 수 없는 합성수인 경우 위의 문제는 매우 어렵다고 알려져 있다.

(n,γ,y)가 아래의 3조건을 만족할 때 acceptable이라 한다.

(조건 1) $n=n_1n_2...n_t$,여기서 각 n_l 는 홀수의 소수이다

(조건 2) γ는 $1 \le l \le t$인 하나의 l에 대해 $gcd(\gamma,\phi(n_l))=\gamma$ 이고,나머지 i에 대해 $gcd(\gamma,\phi(n_l))=1$인 2보다 큰 홀수이다

(조건 3) $y = h_1^{b_1\gamma+e}\prod_{j=2}^{t} h_j^{b_j} \bmod n$, 여기서 모든 $i\neq1, 1\le j\le t$에 대해 $0<e<\gamma$, $\gcd(e,\gamma)=1, 1\le b_j\le\phi(n_j)$이고 $\langle h_1, h_2, \ldots, h_t\rangle$는 Z_n^* 의 generator-vector이다

Acceptable한 triple (n,γ,y)과 $z \in Z_n^*$ 가 주어졌을 때 $z=y^i u^\gamma \bmod n$를 만족하는 i를 z의 class-index 라 한다.

γ^{th}-RP와 관련된 2가지 다른 문제가 있다.

(1) γ^{th}-RP

(2) Class-index-comparing 문제 : an acceptable (n,γ,y)과 $z_1, z_2 \in Z_n^*$ 이 주어졌을 때 z_1 과 z_2 의 class-index를 비교하는 문제

(3) Class-index-finding 문제 : an acceptable triple (n,γ,y)과 $z \in Z_n^*$ 가 주어졌을 때 z의 class-index를 찾는 문제

Zheng은 다음의 관계를 증명하였다.[Z][ZMH]

(a) γ^{th}-RP와 Class-index-comparing 문제는 동치이다;

(b) γ^{th}-RP와 Class-index-comparing 문제는 Class-index-finding 문제로 귀착된다;

(c) $\gamma=O(\text{poly}(k))$인 경우 γ^{th}-RP와 Class-index-comparing 문제는 Class-index-finding 문제와 동치이다;

박성준외 2인은 위의 관계 (c)를 확장한 다음의 관계 (c')를 증명하였다.[PW]

(c') $\gamma = (O(\text{poly}_1(k_1)))^{O(\text{poly}_2(k_2))}$인 경우 γ^{th}-RP와 Class-index-comparing Class-index-finding 문제와 동치이다;

3. 제안한 자체인증 개인식별정보 방식

3.1 초기화

n은 다음의 형태를 가지는 2 소수 p,q의 곱이다.즉,n=pq.

[형태] $p=2\gamma^s p'+1$, $q=2fq'+1$, 여기서 f,p',q'는 서로 다른 소수이고,
$\gcd(\gamma,q')=1, \gcd(\gamma,f)=1$.

y는 $(\gamma^s)^{th}$-nonresidue mod n이고 (n,γ^s,y)는 acceptable triple이다. 또한 b의 mod n 상의 order는 f이다.

신뢰 센터의 공개키는 (n,γ^s,y,b,f)이고,비밀키는 (p',q')이다.

사용자는 자신의 비밀키로 f보다 적은 임의의 수 s를 선택하고 자신의 개인식별정보 I와 b^s를 신뢰 센터에 제출한다. 신뢰 센터는 다음의 수식을 만족하는 i와 x를 계산한다.

[수식] $I=b^{-s}y^{-i}\, x^{-\gamma^s} \bmod n$

여기서 i는 $(Ib^s)^{-1} \pmod n$의 class-index이다.

신뢰 센터는 구한 i와 x를 사용자에게 분배한다. 특히 여기서 i와 x는 비밀일 필요가 없다. 즉,사용자의 비밀키는 s뿐이다.

3.2 개인식별정보에 기반을 둔 개인식별 방식

본 절에서는 개인식별방식을 제안한다.
A가 B에게 자신이 A임을 증명하고자할 때의 프로토콜은 다음과 같다.
1) A는 [0,f-1]상의 임의의 랜덤수 r를 선택한다.
   $v=b^r \pmod n$를 계산한 후 자신의 개인식별정보 I와 v를 B에게 전송한다
2) B는 $[0,2^t-1]$상의 랜덤수 e를 선택하여 A에게 전송한다
   여기서 t는 보통 20에서 70사이이다
3) A는 $z = r + se \pmod f$를 계산하고, z,i,x를 B에게 전송한다
4) B는 $(Iy^i x^{\gamma^s})^e b^z \pmod n = v$를 검증한다

위의 프로토콜은 다음을 만족한다.
1) 완전성
   B는 확률 1로 A를 인증한다.
2) 건전성
   s를 모르고서는 위의 프로토콜을 통과할 확률이 $1-2^{-t}$ 이다.
3) 안전성
   위의 프로토콜은 minimum knowledge 특성을 갖는다.

서론에서 언급했듯이 본 방식에서는 특별한 인증자를 두지 않는다. 물론 신뢰 센터는 각 사용자의 개인식별정보에 대응되는 비밀키 s와 i,x를 계산할 수 있어서 A로 가장할 수가 있게된다. 그러나 이러한 행위는 신뢰 센터만이 할 수 있으므로, 2개의 비밀키가 존재한다는 것은 바로 신뢰센터의 속임수를 의미함으로 제안한 방식은 신뢰 유형3을 만족하게 된다.

3.3 개인식별정보에 기반을 둔 서명방식

본 절에서는 개인식별방식을 제안한다.
A가 평문 m에 서명하고자할 때의 프로토콜은 다음과 같다.
1) A는 [0,f-1]상의 랜덤수 r를 선택한다
   $v=b^r \pmod n$와 e=h(v,m)를 계산한다
   여기서 h는 공통의 해쉬함수이다
2) A는 $z = r + se \pmod f$를 계산한 후 z,i,x,e를 B에게 전송한다
3) B는 $(Iy^i x^{\gamma^s})^e b^z \pmod n = v$를 계산한다
4) B는 e=h(v,m)를 검증한다

위에서 제안한 프로토콜도 완전성, 건전성,minimum knowledge특성을 갖는다.

3.4 개인식별정보에 기반을 둔 키분배 프로토콜

본 절에서는 마지막으로 개인식별방식을 제안한다.
A와 B가 공통키를 분배하고자할 때의 프로토콜은 다음과 같다.
1) A는 I_A,i_A,x_A 를 B에게 전송한다
   그리고 B는 I_B,i_B,x_B 를 A에게 전송한다

2) A와 B는 공통키 K를 다음의 식에 의해 얻는다

$$K = (I_A y^{i_A} x_A^{\gamma^*})^{s_B} = (I_B y^{i_B} x_B^{\gamma^*})^{s_A} = b^{-s_A s_B} \bmod n$$

4. 결론

본 논문에서는 자체인증 공개키 개념(notion of self-certified public key)을 개인식별정보에 기반을 둔 방식에 적용한 새로운 자체인증 개인식별정보 방식을 제안하였다. 더우기 고차잉여류 문제와 이산대수 문제에 근거하여 자체인증 개인식별방식을 만족하는 개인식별방식,서명방식,키분배방식 등을 제안하였다.

본 논문에서 제안한 방식들은 현재 한국통신에서 국제특허 출원중이다.

[참고 문헌]

[G1] M. Girault,"An identity-based identification scheme based on discrete logarithms modulo a composite number", EUROCRYT'90, pp.481-486,1991.

[G2] M. Girault,"Self-certified public keys", EUROCRYPT'91, pp.490-497,1991.

[GP] M. Girault and J. C. Pailles,"An identity-based identification scheme providing zero-knowledge authentication and authenticated key exchange",Proc. of ESORICS'90,pp173-184,1990.

[GQ] L. C. Guillou, J. J. Quisquater,"A Paradoxical Identity-based Signature Scheme Resulting from Zero-Knowledge",CRYPTO'88, pp.216-231,1988.

[PW] S. J. Park and D. H. Won,"A Generalization of Public Key Residue Cryptosystem",Proceeding of JW-ISC'93,pp.202-206,1993.

[S] A. Shamir,"Identity-based Cryptosystems and Signature Scheme", CRYPTO'8 pp.47-53,1984.

[Sc1] Schnorr,"Efficient Identification and Signatures for Smart Cards", EUROCRYPT'89, pp.686-689,1989.

[Sc2] Schnorr,"Efficient Identification and Signatures for Smart Cards", CRYPTO'89, pp.239-252,1989 and J. of Cryptology, Vol.4, No.3,pp.161-174,1991.

[ZMH] Y. Zheng,T. Matsumoto,and H. Imai,"Residuosity Prblem and its Applications to Crytpography",Trans. IEICE, vol.E71, No.8, pp.759-767,1988.

[Z] Y. Zheng,"A Study on Probabilistic Cryptosystems and Zero-knowledge Protocol",Master thesis,Yokohama National University,1988.

본 논문은 한국통신에서 시행한 장기기초연구과제 사업의 연구결과입니다