通信情報保護學會論文誌
第4卷 第2號, 1994. 12

고차잉여류 문제와 이산대수 문제에 기반을 둔 역설적인 id-based 암호시스템

박 성 준*, 원 동 호**

A "paradoxical" identity-based scheme based on γ^{th}-residuosity problem and discrete logarithm problem

Sung Jun Park and Dong Ho Won

요 약

본 논문에서는 certification-based 방식이 아닌 id-based 방식이면서도 사용자가 자신의 비밀키를 선택할 수 있는 역설적인 id-based 방식을 제안한다. 제안한 방식은 Girault가 제안한 self-certified 공개키 개념을 id-based 방식(self-certidifed identity 개념)에 적용한 것이다.

제안한 방식의 안전성은 고차잉여류 문제와 이산대수 문제에 기반을 두고 있다.

Abstract

We propose the truly "paradoxical" identity-based identification scheme, the corresponding signature scheme and identity-based key exchange protocol which any user can choose his(her) own secret key though it is not certification-based method.

The security of our schemes is based on the difficulty of γ^{h}-residuosity problem and discrete logarithm problem simultaneously. Also our schemes are in the level 3 of trust.

In particular, Our schemes are almost as efficient as the Schnorr's scheme.

1. Introduction

There are two methods of eliminating the public key directory from the conventional public key schemes: the one is the identity-based method and the other is the certification-based method.

In the certification-based method, a

* 정 회 원, 성균관대학교 정보공학과 박사과정
** 종신회원, 성균관대학교 정보공학과 교수

trusted center publishes its public key and gives a user A its signature S for the pair of identity Id_A and public key PK_A of A. The user A sends (Id_A, PK_A, S) to the verifier, who checks the validity of PK_A by verifying the trusted center's signature S for (Id_A, PK_A) in place of retrieving PK_A through Id_A from the public key directory.

But in the identity-based method, the public key is replaced by the identity related value of a user.

In general, the major difference between the certification-based method and identity-based method is as follows:

- In certification-based method, any user uses the certificate, but in identity-based method, there is no certificate.
- In certification-based method, the trusted center doesn't know the secret key of user but in identity-based method, the trusted center knows the secret key of every user

And in [G1], M. Girault proposed a "paradoxical" identity-based scheme. But since his scheme used the certificate, we think that his scheme is not a truly identity-based scheme.

Also in [G2], M. Girault introduced the notion of self-certified public key which is intermediary scheme between certification-based method and identity-based method. In the self-certified public key scheme, there is no separate certificate. And he had defined the levels of trust as follows:

- Level 1

The trust center knows user's secret key and, therefore, can impersonate any user at any time without being detected.

- Level 2

The trust center does not know user's secret key. Nevertheless, the trust center can still impersonate a user by generating false certificate.

- Level 3

The trust center does not know user's secret key and can not impersonate a user without being detected.

In this paper, we apply the notion of self-certified public key to the case in which the public key is just the identity (the notion of self-certified identity). Thus we propose a truly "paradoxical" identity-based identification scheme, identity-based signature scheme and identity-based key exchange protocol.

The security of our schemes is based on the difficulty of γ^{th}-residuosity problem and discrete logarithm problem simultaneously. Also our schemes achieve the level 3 of trust.

In particular, Our schemes are almost as efficient as the Schnorr's scheme.[Sc1][Sc2]

2. Preliminaries

We begin with a brief review of terminologies and results in [PW][Z].

For given positive integer γ and n, an integer z is a γ^{th}-residue if $\gcd(z, n) = 1$ and there is an integer x such that $z \equiv x^{\gamma}$ mod n, a γ^{th}-nonresidue otherwise.

The γ^{th}-Residuosity Problam(γ^{th}-RP) means the problem of determining γ^{th}-

residuosity of the given element $z \in Z_n^*$, where Z_n^* is the set of integers relatively prime to n between 0 and n.

When n is a prime, the problem is already solvable. However, for a give composite integer n whose factorization is unknown, this problem is known to be very difficult. If γ is 2, the problem is called Quadratic Residuosity Problem, which is applied to many cryptographic protocols.

We call a triple (n, γ, y) acceptable if n, γ and y satisfy the following three conditions :

(i) n is the product of powers of different odd primes, *i.e.*, $n = n_1 n_2 \ldots n_t$, where each n_i is an odd prime power.

(ii) γ is an odd integer greater than 2 with $\gcd(\gamma, \phi(n_l)) = \gamma$ for just one $1 \le l \le t$, and $\gcd(\gamma, \phi(n_i)) = 1$ for all $i \ne l$, $1 \le l \le t$. For the sake of simplicity, we will assume that $l = 1$.

(iii) y is an element of Z_n^*, written as $y = h_1^{b_l\gamma+e} \prod_{i=2}^{t} h_i^{bj} \bmod n$, where $0 < e < \gamma$, $\gcd(e, \gamma) = 1$, $1 \le b_i \le \phi(n_i)$ for each $i \ne l$, $1 \le j \le t$, and $\langle h_1, h_2, \ldots, h_t \rangle$ is a generator-vector for Z_n^*

There are two other problems related intimately to the γ^{th}-RP. For the completeness, three problems are formally defined as below:

(1) γ^{th}-RP : Given n, γ and an element Z_n^*, decide whether or not z is a γ^{th}-residue (mod n).

(2) Class-index-comparing problem : Given an acceptable triple (n, γ, y) and two elements $z_1, z_2 \in Z_n^*$, judge whether or not z_1 and z_2 have the same class-index with respect to (n, γ, y).

(3) Class-index-finding problem : Given an acceptable triple (n, γ, y) and element $z \in Z_n^*$, find the class-index of z with respect to (n, γ, y).

Zheng *et al* proved that above definitions had following relations.[Z][ZMH]

(a) γ^{th}-RP and Class-index-comparing problem are equivalent;

(b) γ^{th}-RP and Class-index-comparing problem are reducible to the Class-index-finding problem;

(c) γ^{th}-RP and Class-index-comparing problem are equivalent to the Class-index-finding problem when $\gamma = O(\text{poly}(k))$, where poly(.) denotes a polynomial.

Park *et al* proved that above (c) relation can be extenced to the below relation (c'). [PW]

(c') γ^{th}-RP and Class-index-comparing problem are equivalent to the Class-index-finding problem when $\gamma = (O(\text{poly}_1(k_1)))^{O(\text{poly}_2(k_2))}$, where poly_1(.) and poly_2(.) denote a polynomial.

3. The Proposed Identity-based Schemes

3.1 Set-up

Let n be the product of two primes p and q such that $p = 2\gamma^s p' + 1$ and $q = 2fq' + 1$, where f, p' and q' are distinct primes and $\gcd(\gamma, q') = 1$, $\gcd(\gamma, f) = 1$. In the basic version, f is 140-bit long, p' and q' are 210-bit long, γ is 128-bit long, so n is 688-bit long. Let y be a$(\gamma^s)^{th}$-nonresidue mod n

and (n, γ^s, y) be a acceptable triple and the order of b modulo n be f.

The public key of trust center is a (n, γ, y, b, f) and the secret key of trust center is a pair(p', q').

Each user chooses a secret key s, smaller than f, and send the identity I and b^s to the trust center. Then trust center compute i and x where i is the class-index of $(Ib^s)^{1}$ (mod n) and $I = b^s y^i x^{\gamma}$. And the trust center send the i and x to the user I. Here i and x need not to be secret, that is, the only secret key of user is s.

3.2 Identity-based identification scheme.

Now we describe the our identity-based identification scheme. Our scheme is similar to the Schnorr's scheme.

When Alice wants to prove to Bob she is Alice, the protocol is as follows:

1) Alice choose a random integer r in the interval [0, f-1], calculates $v = b^r$ (mod n) and sends her identity I and v to the verifier.
2) Bob picks a random integer e in the interval [0, 2^t-1](where, typically, t lies between 20 and 70) and sends it to Alice
3) Alice calculates $z = r +$ se(mod f) and sends z, i, x to Bob
4) Bob check that $(Iy^i x^{\gamma})^e b^z$ (mod n) $= v$.

It can be proven that :

- Alice will be accepted by Bob with probability almost 1(completeness)
- an imposter, who does not know s, will be deteted with probability $1-2^{t}$ (soundness)
- the protocol herdly reveals anything about s (minimum knowledge)

Note that there is no certificate to check. Of course, the trust center can still compute "false" secret keys linked to Alice, by choosing a number s' and computing the i' and x'. But, since only the trust center is able to compute the index i and x, the existence of two different i, i' and x, x' for the same user is in itself a proof that the turst center has cheated. This shows that our scheme reaches the level 3 of trust.

3.3 Identity-based signature scheme

In this subsection, we describe the our identity-based signature scheme. Our scheme is similar to the Schnorr's scheme.

When Alice wants to sign the message m, the protocol is as follows :

1) Alice choose a random integer r in the interval [0, f-1], calculates $v = b^r$ (mod n) and $e = h(v, m)$ where h is a hash function.
2) Alice calculates $z = r +$ se (mod f) and sends z, i, x, e to Bob.
3) Bob compute the value v such that $(Iy^i x^{\gamma})^e b^z$ (mod n) $= v$.
4) Bob check that $e = h(v, m)$.

It can be proven that :

- Bob will be accepted the valid signature 1.(completeness)
- an imposter, who does not know s, cannot generate a valid signature. (soundness)

3.4 Identity-based key exchange protocol

Finally we describe the our identity-based key exchange protocol.

When Alice and Bob want to share a secret key,

1) Alice sends I_A, i_A, x_A to Bob, and Bob sends I_B, i_B, x_B to Alice.
2) Alice and Bob can get a common secret key K such that

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

This protocol is clearly related to Diffie-Hallman's one, but, contrary to it, makes Alice sure that she shares K with Bob and conversly.

4. Conclusion

In this paper, we apply the notion of self-certified public key to the case in which the public key is just the identity. This notion can be called the notion of self-certified identity. Then we propose a truly "paradoxical" identity-based identification scheme, identity-based signature scheme and identity-based key exchange protocol using the notion of self-certified identity.

The security of our schemes is based on the difficulty of γ^{th}-residuosity problem and discrete logarithm problem simultaneously. Also our schemes achieve the level 3 of trust.

In particular, Our schemes are almost as efficient as the Schnorr's scheme.

Reference

[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, pp 173-184, 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'84, pp. 47-53, 1984.

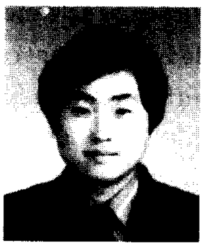
[Sc1] Schnorr, "Efficient Identification and Signatures for Smart Cards", EUROCRYPT'89, pp. 686-689,1989.

[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, 1998.

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

□ 著者紹介



박 성 준 (朴 性 俊, Sung Jun Park) 정회원

1960년 10월 29일생
1983년 2월 한양대학교 수학과 졸업(이학사)
1985년 2월 한양대학교 대학원 수학과 졸업(이학석사)
1985년 1월 ~ 1994년 3월 한국전자통신연구소 부호기술부 선임연구원
1992년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정

※ 주관심분야 : 암호이론, 계산이론, 정보이론

원 동 호 (元 東 豪, Dong-Ho Won) 종신회원

1949년 9월 23일생
1976년 2월 성균관 대학교 전자공학과 졸업 (공학사)
1978년 2월 성균관 대학교 대학원 전자공학과 졸업 (공학석사)
1988년 2월 성균관 대학교 대학원 전자공학과 졸업 (공학박사)
1978년 4월 - 1980년 3월 한국전자통신연구소 연구원
1985년 9월 - 1986년 8월 일본 동경공대 객원연구원
1982년 3월 - 현재 성균관대학교 공과대학 정보공학과 교수
1991년 - 현재 한국통신정보보호학회 편집이사

※ 주관심분야 : 암호이론, 정보이론