General public key residue cryptosystems and mental poker protocols

Kaoru KUROSAWA Yutaka KATAYAMA Wakaha OGATA

Shigeo TSUJII

Department of Electrical and Electronic Engineering

Faculty of Engineering

Tokyo Institute of Technology

2-12-1, Ookayama, Meguro-ku, Tokyo 152, JAPAN

Tel. +81-3-726-1111(Ext. 2577)

Fax +81-3-729-0685

E-mail kkurosaw@ss.titech.ac.jp or

kkurosaw%ss.titech.ac.jp@relay.cs.net

Abstract

This paper presents a general method how to construct public key cryptosystems based on the r-th residue problem. Based on the proposed method, we present the first mental poker protocol which can shuffle any set of cards. Its fault tolerant version is given, too. An efficient zero knowledge interactive proof system for quadratic non-residuosity is also shown.

1 Introduction

Goldwasser and Micali presented a probabilistic encryption scheme based on the quadratic residue problem[GM]. Cohen generalized this binary system to r valued systems for prime r, and applied it to a secret voting system [CF][BY]. Zheng showed a sufficient condition which the parameters must satisfy for odd r[ZMI]. Since such cryptosystems have a nice additive homomorphic property, they have many cryptographic applications.

This paper shows a general method how to construct a public key cryptosystem based on the r-th residue problem for any r (both odd and even). The necessary and sufficient conditions are presented which the parameters must satisfy.

We apply our result to mental poker protocols (Note that the number of cards is 52, which is even.) Previous mental poker protocols[C][MUS] are not that realistic. They cannot shuffle only discarded cards, for example. We propose the first mental poker protocol which can shuffle any set of cards. The difference is in the way of card expression. In the previous protocols, the k-th card is given by the composition of each player's secret permutation. In our protocol, card k is given by the sum of each player's secret random

number. Its fault tolerant version is given, too.

The related zero knowledge interactive proof systems are also shown.

2 Preliminaries

2.1 Public key residue cryptosystems

(Secret key) two large prime numbers, p and q.

(Public key) $N(=pq)$ and y

(Plaintext) $m(0 \leq m < r)$

(Encryption) $E(m) = y^m x^r \bmod N$, where x is a random number.

This cryptosystem has the following homomorphic property.

$E(m+n) = E(m)E(n)z^r \bmod N$ for some z.

Under what condition, is any element of Z_n^* uniquely deciphered ?

The condition for $r = 2$ is [GM]

$(y/p) = (y/q) = -1$

The condition for prime r is [CF][BY]

(1) $r|p-1, r \not| q-1$

(2) y is an r-th non-residue.

2.2 Some known lemmas

Let G be an abelian multiplicative group and H be a subgroup of G.

(Lemma A)[P]

Two elements g and g' of G are in the same coset of H if and only if $g^{-1}g'$ is an element of H.

(Lemma B)[P]

Every elememt of G is in one and only one coset of H.

(Lemma C)[P]

(Order of H)(index of G over H)=(order of G)

(Lemma D)[K]

In GF(p), the number of r-th roots of unity is $gcd(r, p-1)$, where p is a prime number.

2.3 Notations

$Z_N^* = \{x | 0 < x < N, gcd(x, N) = 1\}$

$Z_N^*(+1) = \{x | x \in Z_N^*, (x/N) = 1\}$

$B_N(r) = \{w | w = x^r \bmod N, x \in Z_N^*\}$

p, q : two prime numbers.

3 How to construct residue cryptosystems

3.1 Conditions of the parameters

[Theorem 1]

In the public key residue cryptosystem in 2.1, any element of Z_n^* is uniquely deci-

phered if and only if eq.(1)~(6) are satisfied.

$$y^j \notin B_N(r) \quad 1 \leq j < r \tag{1}$$

$$gcd(p-1, r) = e_1 \tag{2}$$

$$gcd(q-1, r) = e_2 \tag{3}$$

$$r = \begin{cases} e_1 e_2 & \text{if } r \text{ is odd.} \\ (e_1 e_2)/2 & \text{if } r \text{ is even.} \end{cases} \tag{4}$$

$$gcd(e_1, e_2) = \begin{cases} 1 & \text{if } r \text{ is odd.} \\ 2 & \text{if } r \text{ is even.} \end{cases} \tag{5}$$

$$(y/N) = 1 \text{ if } r \text{ is even.} \tag{6}$$

(Definition)

We call y which satisfies the above conditions "a basic element".

(Decryption)

In mod p,

$$\begin{aligned} \{E(m)\}^{(p-1)/e_1} &= (y^m x^r) y^{(p-1)/e_1} \\ &= (y^{(p-1)/e_1})^m (x^{r/e_1})^{(p-1)} \\ &= (y^{(p-1)/e_1})^m \end{aligned}$$

Similarly,

$$\{E(m)\}^{(q-1)/e_2} = (y^{(q-1)/e_2})^m \bmod q$$

Therefore, for $0 \leq i < r$, just compare

$$\{E(m)\}^{(p-1)/e_1} \bmod p \quad \text{and} \quad \{E(m)\}^{(q-1)/e_2} \bmod q.$$

with

$$(y^{(p-1)/e_1})^i \mod p \quad \text{and} \quad (y^{(q-1)/e_2})^i \mod q.$$

(Sketch of proof of Theorem 1)

Observe that

$$E\{0\} = 1, 2^r, \cdots$$

$$E\{m\} = y, y2^r, \cdots, \quad (1 \leq m < r)$$

Notice that $\{E(0)\}$ is a multiplicative group and $\{E(m)\}$ is a coset. Therefore, any element of Z_n^* is uniquely deciphered if and only if

(1) y^m is the coset leader $(1 \leq m < r)$.

(2) $\bigcup_{m=0}^{r-1} \{E(m)\} = Z_n^*$

Eq.(1) is the necessary and sufficient condition for (1) from Lemma A. It can be proved that Eq.(2)~(6) are the necessary and sufficient conditions for (2). Q.E.D.

3.2 Proof of Theorem 1

Theorem 1 is based on the following lemmas, which are derived from lemma A~D in 2.2. We discuss only the case of $r = odd$ for the simplicity. The case of $r = even$ is similar.

[Lemma 1]

(1) Let w be an r-th residue mod p. Then, the number of r-th roots of w is e_1.

(2) Let $w \in B_N(r)$. Then, the number of r-th roots of w is $e_1 e_2$.

(3) Z_n^* is a multiplicative group and its order is $(p-1)(q-1)$.

(4) $B_N(r)$ is a subgroup of Z_n^* and its order is $(p-1)(q-1)/e_1 e_2$.

(5) The index of Z_n^* over $B_N(r)$ is e_1e_2.

[Lemma 2]

(1) $x^{e_1} \in B_p(r)$ for any x.

(2) Let g be a primitive element of GF(p). Then,

$$g^j \notin B_p(r) \quad 1 \leq j < e_1$$

[Lemma 3]

Let $s = lcm(e_1, e_2)$. Then,

(1) $x^s \in B_N(r)$ for any x

(2) Let y be an integer which is a primitive element of GF(p) and GF(q). Then,

$$y^j \notin B_p(r) \quad 1 \leq j < s$$

(3) Let $r = e_1e_2$. Then, there exists y such that eq.(1) holds if and only if eq.(5) holds.

(4) If $r \neq e_1e_2$, there is no y such that any element of Z_n^* is uniquely deciphered.

3.3 Existency of basic elements

[Theorem 2]

(number of basic elements)/$|Z_N^*| = \phi(r)/r$ if r is odd.

(number of basic elements)/$|Z_N^*(+1)| = \phi(r)/r$ if r is even.

It is known that [HW]

$$r/\phi(r) = O(loglogr).$$

Therefore, the expected number of trials to choose a basic element is $O(loglogr)$.

[Theorem 3]

Let $r = \prod_{i=1}^{k} p_i^{j_i}$, where p_i is prime for $1 \leq i < k$. Then,

$$y^i \notin B_N(r) \quad 1 \leq i < r$$

if and only if

$$y^{(r/p_i)} \notin B_N(r) \quad 1 \leq i < k$$

[Lemma 4]

$w \in B_N(r)$ if and only if

$$w^{(p-1)/e_1} = 1 \mod p \quad \text{and} \quad w^{(q-1/)e_2} = 1 \mod q$$

4 Proposed mental poker protocols

We propose the first mental poker protocols which can shuffle any set of cards. In Poker 1, a distributed sum scheme is introduced for the card representation. Poker 2 is a fault tolerant version.

Suppose that $P_1, \cdots, P_n$ want to play poker. Each palyer constructs the r-th residue cryptosystem, where $r = 52$ in Poker 1 and $r = 53$ in Poker 2.

(1) P_i publicizes his public key (N_i, y_i).

(2) P_i proves that (N_i, y_i) satisfies the conditions in 3.1 by a zero knowledge proof system.

4.1 Poker 1

A DECK of cards is $\{0, \cdots, 51\}$. In Poker 1, card k in DECK is expressed by

$$\{E_1(f_1(k)), \cdots, E_n(f_n(k))\}$$

where $f_i(k)$ is P_i's secret random number such that

$$k = f_1(k) + \cdots + f_n(k) \bmod 52$$

We show how to assign such random numbers to each player in a distributed and trusted way.

(Putting cards upside down)

P_1 choose randomly $\{r_{i,j}\}$ such that

$$k = r_{1,k} + \cdots + r_{n,k} \bmod 52,\ 0 \leq k \leq 51$$

and publicizes them. At this stage, every card is open. P_1 then encrypts each $r_{i,k}$ by P_i's public key. He publicizes the result and the related random numbers which were used in the encryptions. Let

$$C_k = (t_{1,k}, \cdots, t_{n,k}), \quad 0 \leq k \leq 51$$

where $t_{i,k} = E_i(r_{i,k})$.

At this stage, each card has become the backside. However, everyone knows, for each card, what the front side is. So, next, each player shuffles the cards in turn.

(Shuffling cards in DECK)

Do the following for $h = 1, \cdots, n$.

P_h chooses random numbers $\{s_{i,j}\}$ such that

$$0 = s_{1,k} + \cdots + s_{n,k} \mod 52, \quad 0 \leq k \leq 51$$

He then chooses a random permutaion π and computes

$$t'_{1,k} = t_{1,\pi(k)} \times E_i(s_{i,k}) \mod N_i$$

Note that, for some π',

$$E_1^{-1}(t_{1,k})' + \cdots + E_n^{-1}(t'_{n,k}) = \pi'(k) \bmod 52, \quad 0 \leq k \leq 51$$

because of the homomorphic property of E_i and eq.(4.1). He sets $t_{1,k} = t'_{1,k}$ and publicizes

$$C_k = (t_{1,k}, \cdots, t_{n,k}), \quad 0 \leq k \leq 51$$

By a zero knowledge interactive proof system, he proves that he computed C_k according to the protocol.

Now, we have made a DECK.

(Getting a card from the DECK)

When P_i gets a card from the DECK, the other players open their plaintexts of $\{t_{i,k}\}$ and the related random numbers. Only P_i can obtain the card by computing

$$\pi'(k) = E_1^{-1}(t_{1,k}) + \cdots + E_n^{-1}(t_{n,k}) \bmod 52$$

The other players can compute the back side of this card as follows.

$$E_i(\pi'(k)) = t_{1,k} \times y_i^{E_1^{-1}(t_{1,k})+\cdots,\overset{i}{\vee},\cdots+E_n^{-1}(t_{n,k})}$$

(Shuffling Hand)

Let the cards in the hand of P_i be $E_i(c_1), \cdots, E_i(c_m)$. P_i shuffles them before he opens or discards one of them. For the suffling, he chooses a random permutaion π and publicizes

$$E_i(c_{\pi(1)})E_i(0), \cdots, E_i(c_{\pi(m)})E_i(0)$$

He proves that he followed the protocol by a zero knowledge interactive proof system.

(Openning a card)

When P_i opens $E_i(\pi'(k))$, he just opens $\pi'(k)$ and the related random number.

(Discarding a card)

When P_i discards $E_i(\pi'(k))$, he just declares that he discards $E_i(\pi'(k))$.

(Giving a card)

When P_i gives $E_i(\pi'(k))$ to P_j, he publicizes $E_j(\pi'(k))$. By a zero knowledge interactive proof system, P_i proves that the plaintexts of $E_i(\pi'(k))$ and $E_j(\pi'(k))$ are the same.

(Shuffling any set of cards)

Suppose that all players want to mix the cards in DECK with a discarded card, $E_i(\pi'(k))$, and reshuffle them. Note that

$$\pi'(k) = 0 + \cdots + \pi'(k) + \cdots + 0$$

and $E_i(\pi'(k))$ is given. Then, it is easy to see that we can use the same protocol as "shuffling cards in DECK".

(Remark)

The necessary zero knowledge interactive proof systems are easy to obtain from the homomorphic property of the cryptosystem.

4.2 Poker 2

This protocol is a fault tolerant version of Poker 1. When n=2t+1, at most t faulty players are allowed. Let g(x) be a random polynomial with degree t and with the constant term k. Card k is expressed as follows.

$$E_1(g(1)), \cdots, E_n(g(n))$$

The other part of the protocol is almost the same, except that P_j sends g(j) to P_i secretly, $j \neq i$, when P_i gets a card from the DECK.

5 ZKIP for public key residue cryptosystems

5.1 Knowledge of a plaintext

Suppose that z is given such that

$$z = y^m x^r \bmod N \tag{7}$$

A(lice) wants to convince B(ob) that she knows m and x.

(Protocol 1)

Repeat the following n times, where $n = |N|$.

(step 1) A chooses m' and x' randomly and computes

$$z' = y^{m'} x'^r \bmod N$$

She sends z' to B.

(step 2) B sends a random bit e to A.

(step 3) A sends m" and x" to B such that

$$z^e z' = y^{m"} x"^r \bmod N$$

(step 4) B checks the above equation.

5.2 On the basic element

Let

$$S = \begin{cases} Z_n^* & \text{if } r \text{ is odd.} \\ Z_n^*(+1) & \text{if } r \text{ is even.} \end{cases}$$

A wants to convince B that (N, y) satisfies the following two conditions.

(1) For any $z \in S$, there exists m and x such that eq.(7) holds, where $0 \leq m < r$.

(2) The above m is unique.

[ZKIP for (1)]

Repeat the following n times, where $n = |N|$.

(step 1) B chooses $z \in S$ at random and sends it to A.

(step 2) A shows that she knows the m and x by protocol 1.

[ZKIP for (2)]

Repeat the following n times, where $n = |N|$.

(step 1) B chooses m and x randomly and computes eq.(7). He sends the z to A.

(step 2) B shows that he knows m and x by protocol 1.

(step 3) A computes the plaintext of z, $\hat{m}$, and send it to B.

(step 4) B checks that $\hat{m} = m$.

(Remarks) When $r = 2$,

(1) ZKIP for (1) is also a ZKIP for

$$N = p^i q^j, \quad (y/p^i) = (y/q^j) = -1$$

(2) ZKIP for (2) is also a ZKIP for that y is a quadratic non-residue. The number of bits communicated is a half of [GMR].

Acknowledgement

We are grateful to Dr.Itoh and Mr.Kishimoto for useful advice.

References

[BY] Benaloh and Yung: "Distributing the power of a government to enhance the privacy of voters", Proc. 5th Annual Symp. on pronciples of distributed computing, ACM, pp.52-62 (1985)

[C] Crepeau: "A zero knowledge poker protocol that achieves confidentiality of players' strategy, or how to achieve an electronic poker face", CRYPTO'86, pp.239-247 (1986)

[CF] Cohen and Fischer: "A robust and verifiable cryptographically secure election scheme", Proc. 26th FOCS, pp.372-382 (1985)

[GM] Goldwasser and Micali: "Probabilistic encription and how to play mental poker, keeping secret all partial information", 14th STOC, pp.365-377 (1982)

[GMR] Goldwasser, Micali and Rackoff: "The knowledge complexity of interactive proof systems", SIAM J. on computing, vol.18, No.1, pp.186-208 (1989)

[HW] Hardy and Wright: "An introduction to the theory and numbers", 5th ed., Oxford Univ. Press (1979)

[K] Koblitz: "A course in number theory and cryptography", Springer-Verlag (1987)

[MUS] Miyama, Uyematsu and Sakaniwa: "A mental poker protocol without later verifications", (in Japanese) (1987)

[P] Peterson: "Error correcting codes", MIT Press (1961)

[ZMI] Zheng, Matsumoto and Imai: "Residuosity problem and its application to cryptography", Trans, IEICE, vol.E71, No.8, pp.759-767 (1988)