Fault Tolerant Anonymous Channel

Wakaha OGATA[1], Kaoru KUROSAWA[2],
Kazue SAKO[3], Kazunori TAKATANI[1]

[1] Himeji Institute of Technology,
wakaha@comp.eng.himeji-tech.ac.jp
http://wwwj2.comp.eng.himeji-tech.ac.jp/home/wakaha/
[2] Tokyo Institute of Technology,
kurosawa@ss.titech.ac.jp, http://tsk-www.ss.titech.ac.jp/~kurosawa/
[3] NEC Corporation, sako@sbl.cl.nec.co.jp

Abstract. Previous anonymous channels, called MIX nets, do not work if one center stops. This paper shows new anonymous channels which allow less than a half of faulty centers. A *fault tolerant* multivalued election scheme is obtained automatically. A very efficient ZKIP for the centers is also presented.

1 Introduction

Chaum considered an anonymous channel which hides the correspondences between the senders and the messages [Ch81]. Suppose that there are l senders $P_1, \ldots, P_l$ such that each P_i has a message m_i. Assume a center called MIX which publicizes his RSA public key E. Each sender P_i sends $c_i = E(m_i)$ to the MIX. The MIX decrypts them and publicizes $m_1, \ldots, m_l$ in the lexicographical order. The MIX, however, knows who sent what message. Finally, Chaum proposed a *MIX net* in which n MIXes are sequentially connected [Ch81]. Anonymity is protected if at least one MIX is honest.

The *MIX net*, however, does not work if one MIX (center) stops. This paper shows new anonymous channels which allow less than a half of faulty centers, where faulty centers can stop or deviate from the protocol arbitrarily. *Fault tolerant* multivalued election schemes are obtained automatically. (Cohen and Fischer type election scheme realizes only yes/no votes [CF85, Be86].) A very efficient zero knowledge interactive proof system (ZKIP) for MIX is also presented.

2 Fault tolerant anonymous channels

This section presents two robust anonymous channels which allow less than a half of faulty centers. One is based on the hardness of factorization and the other is based on the difficulty of the discrete log problem. In both schemes, even if less than a half of centers are faulty, (1) randomly shuffled messages are output and (2) anonymity is protected.

2.1 Proposed scheme based on factoring

The r-th residue public key cryptosystem is defined as follows [CF85]. Let r be a prime.
Secret key: Two large prime numbers p, q such that $r|p-1$ and $r \not| q-1$.
Public key: $N(\stackrel{\triangle}{=} pq)$ and y such that $y \neq x^r \bmod N$ for $\forall x$.
Plaintext: m such that $0 \leq m < r$.
Encryption: $E(m,x) \stackrel{\triangle}{=} y^m x^r \bmod n$, where x is a random number.
Decryption: Let $c = E(m,x)$. Then $m = j_0$ if

$$c^{(p-1)/r} = (y^{(p-1)/p})^{j_0} \bmod p$$

This cryptosystem satisfies a homomorphic property such that

$$E(m_1,x_1)E(m_1,x_2) = E(m_1+m_2 \bmod r, x_0), \text{ for some } x_0. \tag{1}$$

Then our scheme is described as follows. Suppose that there are l senders $P_1,\ldots,P_l$ such that each P_i has a message m_i. Assume n centers $MIX_1,\ldots,MIX_n$ such that each MIX_j has a public key E_j of the r-th residue cryptosystem. Let

$$k \stackrel{\triangle}{=} \lfloor (n-1)/2 \rfloor + 1.$$

Definition 1. For a plaintext m, choose a random polynomial $R(x)$ of degree $k-1$ such that $R(0) = m$. Let

$$B(m,R) \stackrel{\triangle}{=} [E_1(R(1),x_1),\cdots,E_n(R(n),x_n)],$$

where $x_1,\cdots,x_n$ are random numbers. We say that $B(m,R)$ is an encrypted shares of m.

Definition 2. For $B(m,R)$, choose a random polynomial $U(x)$ of degree $k-1$ such that $U(0) = 0$. Let

$$\hat{B}(m) \stackrel{\triangle}{=} [E_1(R(1),x_1)E_1(U(1),w_1),\cdots,E_n(R(n),x_n)E_n(U(n),w_n)],$$

where $w_1,\cdots,w_n$ are random numbers. We say that $\hat{B}(m)$ is a reencryption of $B(m)$. ($\hat{B}(m)$ is again an encrypted shares of m because $\hat{B}(m) = B(m,R+U)$.)

(Sender's protocol)
Each P_i computes $B(m_i,R_i)$, an encrypted shares of his message m_i, and publicizes $B(m_i,R_i)$. He proves that he knows $R_i(x)$ by using a ZKIP of knowledge. He is then proving two things:

1. He knows $R_i(0)$ which is his message itself. This proof prevents the Pfitzmann's attack against Chaum's MIX net [PP89].
2. He indeed distributed the message correctly (verifiable secret sharing scheme).

(Center's protocol) Now

$$[B(m_1, R_1), \cdots, B(m_l, R_l)] \tag{2}$$

are publicized. MIX_1 randomly computes a reencryption of each $B(m_i, R_i)$ such that $B(m_i, R_i + U_i)$. MIX_1 chooses a random permutation π on $\{1, 2, \ldots, l\}$ and publicizes

$$[B(m_{\pi(1)}, R_{\pi(1)} + U_{\pi(1)}), \cdots, B(m_{\pi(l)}, R_{\pi(l)} + U_{\pi(l)})).] \tag{3}$$

MIX_1 further proves that eq.(3) is computed from eq.(2) correctly by using a ZKIP. For $2 \leq j \leq n$, MIX_j executes the same process sequentially.

(Decryption)

At the end, MIX_n publicizes

$$[B(m_{\varphi(1)}, \tilde{R}_{\varphi(1)}), \cdots, B(m_{\varphi(l)}, \tilde{R}_{\varphi(l)})]$$

for some permutation φ, where $B(m_{\varphi(i)}, \tilde{R}_{\varphi(i)})$ is an encrypted shares of $m_{\varphi(i)}$. Let

$$B(m_{\varphi(i)}, \tilde{R}_{\varphi(i)}) = [c_{i,1}, \ldots, c_{i,n}]$$

Each MIX_j decrypts $c_{i,j}$ and publicizes its plaintext $v_{i,j}$ for $i = 1, \ldots, l$. Then everybody can recover $m_{\varphi(i)}$ from k or more $v_{i,j}$. Each MIX_j proves that he behaved correctly by using a ZKIP.

If some P_i or MIX_j is detected to be faulty, he is ignored from that time on.

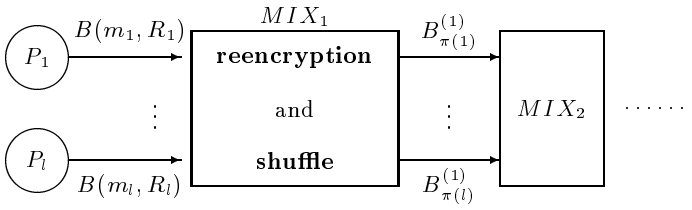

Fig. 1. Reencryption and shuffle, where $B^{(1)}_{\pi(i)} \triangleq B(m_{\pi(i)}, R_{\pi(i)} + U_{\pi(i)})$.

2.2 Proposed scheme based on DLOG

This anonymous channel makes use of the scheme shown in Sec. 5.1 of [PIK93], which uses ElGamal public key cryptosystem. (It is called type 2 channel in [Pf94].)

Each MIX_j distributes his secret key x_j to all MIXes by using Shamir's (k, n)-threshold secret sharing scheme. Each sender proves that he knows his message by using a ZKIP to avoid the attack of [PP89]. Each MIX_j proves that he behaved correctly by using a ZKIP so that the attack of Sec.5.1 in [Pf94] does

not work. Further, the attack of Sec.5.2 in [Pf94] does not work because x_j of a faulty MIX_j is revealed by using the (k, n)-threshold secret sharing scheme.

Let p and q be primes such that $q \mid p-1$. Let $g \in Z_p$ be a q th root of unity. Each MIX_j chooses a secret key $x_j \in Z_q^*$ and publicizes $y_j = g^{x_j} \bmod p$ as his public key. Further, he distributes x_j to all MIXes by using Shamir's (k, n)-threshold secret sharing scheme. He executes Feldman's non-interactive Verifiable Secret Sharing [Fe87].

(Sender's protocol) Each sender P_i encrypts his message m_i as

$$(G_i, M_i) = (g^r \bmod p, (y_1 y_2 \cdots y_n)^r m_i \bmod p)$$

He publicies (G_i, M_i) and proves that he knows m_i by using a ZKIP.

(Center's protocol) For $1 \leq j \leq n$, MIX_j reencrypts and shuffles $(G_1, M_1), \cdots, (G_l, M_l)$ sequentially. He proves that he behaved correctly by using a ZKIP.

(Decryption) At the end, suppose that MIX_n publicized $(\hat{G}_1, \hat{M}_1), \cdots, (\hat{G}_l, \hat{M}_l)$. For each $(\hat{G}, \hat{M})$, each MIX_j computes

$$G_j = \hat{G}^{x_j} \bmod p$$

and publicizes G_j. He proves the validity of G_j by using a ZKIP. Then the plaintext m is obtained by

$$m = \hat{M}/(G_1 \cdots G_n)$$

If there are some faulty MIXes and some G_j is not opend, the remained honest MIXes reveal the corresponding secret key x_j by using Shamir's (k, n)-threshold serect sharing scheme.

3 Efficient ZKIP for shuffle

In this section, we show a very efficient ZKIP for the center's protocol of Sec. 2.1. The communication complexity is $1/l$ of the standard ZKIP. A similar ZKIP can be obtained for that of Sec.2.2.

MIX_1 wants to prove that eq.(3) is computed from eq.(2) correctly in zero knowledge. In eq.(2) and eq.(3), let

$$B(m_i, R_i) = [a_{i,1}, \cdots, a_{i,n}]$$
$$B(m_{\pi(i)}, R_{\pi(i)} + U_{\pi(i)}) = [b_{i,1}, \cdots, b_{i,n}]$$

Let P denote a prover and V denote a verifier. Repeat the steps $1 \sim 4$ below $\log_2 N$ times.

(Step 1) P randomly computes a reencryption of each $B(m_i, R_i)$ such that $B(m_i, R_i + \hat{U}_i)$. Then P chooses a random permutation τ on $\{1, 2, \ldots, l\}$ and sends to V

$$[B(m_{\tau(1)}, R_{\tau(1)} + \hat{U}_{\tau(1)}), \cdots, B(m_{\tau(l)}, R_{\tau(l)} + \hat{U}_{\tau(l)})).] \tag{4}$$

Let

$$B(m_{\tau(i)}, R_{\tau(i)} + \hat{U}_{\tau(i)}) = [d_{i,1}, \cdots, d_{i,n}].$$

P also bit commits τ and $\phi \stackrel{\triangle}{=} \tau\pi^{-1}$. He sends the commitals to V.

(Step 2) V sends to P a random bit e and random numbers t_i $(1 \leq i \leq l)$ such that $0 \leq t_i < r$.

(Step 3) P computes

$$U' \stackrel{\triangle}{=} \begin{cases} \sum_{i=1}^{l} t_i \hat{U}_{\pi(i)} & \text{if } e = 0, \\ \sum_{i=1}^{l} t_i (\hat{U}_{\tau(i)} - U_{\phi(i)}) & \text{if } e = 1 \end{cases}$$

Let w_j $(1 \leq j \leq n)$ be the random number which satisfies

$$E_j(U'(j), w_j) = \begin{cases} \prod_{i=1}^{l} (d_{i,j}/a_{\tau(i),j})^{t_i} & \text{if } e = 0 \\ \prod_{i=1}^{l} (d_{i,j}/b_{\phi(i),j})^{t_i} & \text{if } e = 1 \end{cases} \tag{5}$$

- If $e = 0$, P sends $U', w_1, \cdots, w_n$ and the decommmital of τ to V.
- If $e = 1$, P sends $U', w_1, \cdots, w_n$ and the decommmital of ϕ to V.

(Step 4) V accepts if

1. U' is a polynomial of degree at most $(k-1)$ such that $U'(0) = 0$.
2. Eq.(5) is satisfied for $1 \leq j \leq n$.

Theorem 3. *If eq.(3) is not computed from eq.(2) correctly, then*

$$\Pr(V \textit{ accepts in each round}) \leq 1/2 + 1/2r$$

for any (possibly cheating) prover.

References

[Be86] J. Benaloh, Secret sharing homomorphisms: Keeping a secret secret , in: *Proc. of Eurocrypt'86*, 251–260 (1986).

[CF85] J.D. Cohen and M.J. Fischer, A Robust and Verifiable Cryptographically Secure Election Scheme, in: *Proc. of 26th IEEE Symp. on Foundations of Computer Science*, 372–382 (1985).

[Ch81] D.L. Chaum, Untraceable Electronic Mail, Return Address, and Digital Pseudonyms, in: *Communications of the ACM, Vol.24, No.2*, 84-88 (1981).

[Fe87] P. Feldman, A Practical Scheme for Non-Interactive Verifiable Secret Sharing, in: *Proc. of 28th IEEE symposium on Foundations of Computer Science*, 427–437 (1987).

[MH96] M. Michels and P. Horster, Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme, in: *Proc. of Asiacrypt '96*, 125–132 (1996).

[Pf94] B. Pfitzmann, Breaking an Efficient Anonymous Channel, in: *Proc. of Eurocrypt '94*, 339–348 (1994).

[PIK93] C. Park, K. Itoh and K. Kurosawa, All/Nothing Election Scheme and Anonymous Channel, in: *Proc. of Eurocrypt '93*, (1993).

[PP89] B. Pfitzmann and A. Pfitzmann, How to Break the Direct RSA-implementation of Mixes, in: *Proc. of Eurocrypt '89*, 373-381 (1989).

This article was processed using the LaTeX macro package with LLNCS style