SCIS'97-27F

SCIS'97 The 1997 Symposium on
Cryptography and Information Security
Fukuoka, Japan, January 29-February 1, 1997
The Institute of Electronics,
Information and Communication Engineers

(k,n)閾値匿名通信路とその応用

(k,n) threshold MIX net and its application

尾形 わかは[1] 黒沢 馨[2] 高谷 和伯[1]
Wakaha OGATA Kaoru KUROSAWA Kazunori TAKATANI

[1] 姫路工業大学 工学部 情報工学科
〒671-22 姫路市 書写 2167

Himeji Institute of Technology
2167 Shosha, Himeji-shi, Hyogo 671–22 Japan
wakaha@comp.eng.himeji-tech.ac.jp

[2] 東京工業大学大学院 情報理工学研究科 計算工学専攻
〒152 目黒区 大岡山 2–12–1

Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152 Japan
kurosawa@ss.titech.ac.jp

あらまし 匿名通信路 (MIX net) は，電子投票など多くの応用を有する。しかし、従来の方式では、１つのセンタが故障あるいは不正の発覚などによって停止した場合、匿名メッセージを復元することができなくなってしまう。本稿は，半数未満のセンタが停止したとしても匿名メッセージを復元することができる、新しい匿名通信路を提案するものである．

Abstract Anonymous channels have many applications, for example, to elections. Previouis anonymous channels, called MIX nets, cannot work if one or more centers are faulty. This paper shows a new anonymous channel which can still work even if less than a half of centers are faulty.

1　はじめに

匿名通信路は，電子投票方式など，多くの応用を有する．電子投票方式としては，票を分割する方式も提案されているが，この方式では 2 値の投票 (信任投票) しかできない．これに対し，匿名通信路を使った方式は，多値の投票をできるという利点を持つ．

Chaum[1] は，MIX net と呼ばれる匿名通信路を提案した．この方式は，以下のように動作する．

1. 複数の送信者はそれぞれのメッセージを RSA 暗号で暗号化し，MIX センタに送る．
2. MIX センタは，復号結果をランダムに並べかえて公開する．

Brigit Pfitzmann and Andrea Pfitzmann は，この方式に対し，匿名性を破壊する攻撃が可能であることを示した [3]．また，彼らは，RSA 暗号の代わりに能動攻撃に対し安全な公開鍵暗号を使えば，その攻撃を防ぐことができることも示した．

一方，MIX センタが一つだけだと，送信者とメッセージの対応関係が MIX センタにわかってしまう．そこで Chaum[1] は，n 個の MIX センタを直列に連結する方式を提案している．このようにすれば，たとえ $n-1$ 個の MIX センタが結託しても，送信者とメッセージの対応関係はわからない．

したがって，n 個の MIX センタを直列に連結し，能動攻撃に対し安全な公開鍵暗号を各 MIX センタの公開鍵暗号とする，というのが，現在，最も安全な方式であるといえる．

しかし，上記を方式においては，1 つのセンタが故障あるいは不正の発覚などによって停止した場合，匿名メッセージを復元することができなくなってしまう．本稿では，半数未満のセンタが停止したとしても匿名メッセージを復元することができる，新しい匿名通信路を提案する．

2　従来の匿名通信路

本章では，従来の匿名通信路およびそれに対する攻撃について述べる．

Chaum[1] の n 個の MIX センタを直列に連結する方式では，暗号文の長さが n に比例して大きくなってしまう．Park, Itoh and Kurosawa は，ElGamal 暗号を利用し，これを防ぐ方式を提案した．Sako and Kilian は，彼らの方式に ZKIP を組み込む方式を示している．最近，Michels らは，Sako and Kilian の方式に対し，匿名性を破壊する攻撃を示した．

一方，Brigit Pftzman は，Park, Itoh and Kurosawa の方式に対し，匿名性を破壊する攻撃を示した．この攻撃は，Sako and Kilian の方式にも適用可能である．これは，Elgamal 暗号が能動攻撃に対し安全でないからであると考えられる．

2.1　Chaum の方式

Chaum の方法では，送信者 P_j からのメッセージ m_j の匿名メッセージは，全ての MIX センタの公開鍵 E_i によって暗号化された暗号文：

$$E_1(r_1 \circ E_2(\cdots E_{n-1}(r_{n-1} \circ E_n(r_n \circ m_j))\cdots))$$

である．ただし$\circ$は文字列の連結を表わし，$r_1, \ldots, r_n$は乱数である．初めの MIX センタは複数の送信者から暗号文を受け取り，それぞれを自分の復号化鍵で復号化する．そして，その結果：

$$E_2(\cdots E_{n-1}(r_{n-1} \circ E_n(r_n \circ m_j))\cdots)$$

を次のセンタに送る．この際，複数の匿名メッセージをアルファベット順に並びかえ，元の暗号文との関係を隠す．他のセンタも同様に，暗号文を自分の復号化鍵で復号化し，アルファベット順に並びかえて次のセンタに送る．

2.2 Park, Itoh and Kurosawa の方式

Chaum の方式では，暗号文と復号した文の関係を分からなくするため，メッセージの前に乱数 r_j を連結させている．このため，センタの数を増やすと暗号文が長くなってしまう．Park, Itoh and Kurosawa は，ElGamal 暗号を利用し，暗号文の長さがセンタの数によらないという方式を示した．

共通公開情報　　：素数 p，$\bmod p$ における原始根 g
MIX センタ C_j の公開鍵 ：$y_j = g^{x_j} \bmod p$

簡単のため，

$$w_i \triangleq \prod_{j=i+1}^{n} y_j (\bmod p)$$

とする．まず，各送信者は乱数 r_0 を選び，匿名メッセージとして

$$Z_1 = (G_1, M_1) = (g^{r_0} \bmod p, w_0^{r_0} m \bmod p)$$

を MIX センタ C_1 に送る．

PIK の方式 (1)
(**MIX**j+復号化 j) MIX センタ $C_j (1 \leq j < n)$ は，

$$(G_j, M_j)$$

のリストを受け取り，それぞれに対して

$$H_j \triangleq G_j^{x_j}, \quad (G_{j+1}, M_{j+1}) \triangleq (G_j^{r_j} \bmod p, M_j w_j^{r_j} / H_j \bmod p)$$

を作り，送信者数分の (G_{j+1}, M_{j+1}) を順番を入れ替えて次の MIX センタ C_{j+1} に送る．
(復号化 n) C_n は

$$H_n \triangleq G_n^{x_n}, \quad m' \triangleq M_n / H_n \bmod p$$

を作り，m' を公開する．

PIK の方式 (2)
(**MIX**j) MIX センタ $C_j (1 \leq j \leq n)$ は，

$$(G_j, M_j)$$

のリストを受け取り，それぞれに対して

$$(G_{j+1}, M_{j+1}) \triangleq (G_j^{r_j} \bmod p, M_j w_j^{r_j} \bmod p)$$

を作り，送信者数分の (G_{j+1}, M_{j+1}) を順番を入れ替えて次の MIX センタ C_{j+1} に送る．最終センタは (G_{n+1}, M_{n+1}) を公開ボードに公開する．
(復号化) $C_j (1 \leq j \leq n)$ は公開された各 (G_{n+1}, M_{n+1}) に対し，

$$H_j \triangleq G_j^{x_j}$$

を作り，公開ボードに加える．公開ボードに公開されたリストから，

$$m' \triangleq M_{n+1} (\prod_{j=1}^{n} H_j) \bmod p$$

を計算することができる．

全ての MIX センタが正しく動作している場合，m' の集合は匿名メッセージ m の集合と同じである．

2.3 Sako and Kilian の方式

Sako and Kilian は，PIK の方式 (1) の各処理のあとに，処理を正しく行ったことを示す ZKIP を行う方式を示した [6]．

各 MIX センタは

- すべての H_iを公開
- (G_i, M_i) から正しく H_iを作っていることを証明する ZKIP
- $(G_i, M_i), H_i$から正しく (G_{i+1}, M_{i+1}) を作っていることを証明する ZKIP

を行う．

2.4 Michels らの攻撃

Michels らは，Sako and Kilian の方式に対し以下のような攻撃を示した [7]．

受動的な攻撃：C_jを除く全ての MIX センタが結託したとする．C_1から C_{j-1}は送信者の送った匿名メッセージ (G_1, M_1) を正しく処理し，C_jに (G_j, M_j) を送る．このとき，不正者らは (G_j, M_j) が特定の送信者の匿名メッセージであることを知っている．C_jは (G_j, M_j) から H_jを作り公開する．すると，C_{j+1}から C_nの秘密鍵から，特定の送信者のメッセージ m を以下のようにして計算することができる．

$$m \stackrel{\triangle}{=} M_j / (H_j \prod_{t=j+1}^{n} G_j^{x_t})$$

2.5 Pfitzmann のアタック

Pfizmann は PIK の方式に対し，次のような攻撃が可能であることを示した [5]．

受動的な攻撃：メッセージの集合 Z_p^*は，部分群 $U_2 \stackrel{\triangle}{=} \{a \in Z_p^* \mid a = (g^2)^x \text{ for some } x \in Z_p^*\}$ を持つ．ある送信者の送信した暗号文を

$$C = (t, u) = (g^r, w_0^r m)$$

とすると，確率 $1/2$ で $t \in U_2$である．このとき $u \in U_2 \Leftrightarrow m \in U_2$となり，$C$に m の情報の一部が漏れてしまう．また，任意の $p-1$ を割り切る整数 lについても同様に U_lを考えることができ，匿名メッセージの特定を助ける．

能動的な攻撃：一人の送信者 Sが別の送信者の匿名メッセージの平文を特定する不正を考える．Sは見たい匿名メッセージ (t, u) を盗聴し，自分の匿名メッセージとして $(t', u') = (t^x, u^x)$ を匿名通信路に送る．最終 MIX センタ C_nが復元したメッセージには，$m' = m^x$となる組 (m, m') が必ずあり，m が見たいメッセージである．

また Pfizmann は，以下の修正を加えれば，これらの攻撃に対し安全となることを示した．

受動的な攻撃に対して：素数 p を，十分大きな素数 qに対して $q|p-1$ となるように選ぶ．メッセージの集合として部分群 U_qを使い，gは U_qの原始根を用いる．

能動的な攻撃に対して：メッセージの後ろに幾つかの 0 を加えるなどして冗長性をもたせ，最後に復元されたメッセージが規定された冗長性を持っているかチェックする．

Pfizmann は，しかし，それでもなお，次のような攻撃が可能であることも示している．ある送信者 Sと最終 MIX センタ C_nが結託することを考える．Sは自分の匿名メッセージとして $(t', u') = (t^x, u^x)$ を匿名通信路に送る．C_nは復号化したメッセージの中から $(m, m' = m^x)$ を見つけ，m を知る．そして冗長性のチェックで引っかかる m'をもっともらしい m''に入れ替え公開する．

この攻撃は，PIK の方式のみならず，Chaum の方式に RSA 暗号を適用した方式に対しても有効である．また，ZKIP を導入した Sako and Kilian の方式でも，C_nの不正はチェックできるがターゲットにされたメッセージのプライバシーは守られていない．

3　センタの故障を許す新しい匿名通信路

2章で述べた従来の方式は全て，1つのMIXセンタが故障や不正の発覚などによって停止した場合，匿名メッセージを復元することができない．本章では，半数未満のセンタが停止したとしても匿名メッセージを復元することができる，新しい匿名通信路を提案する．

本方式は，多値の確率的暗号系とShamirの(k,n)閾値秘密分散共有法を組合せをベースに構成される．(Benalohの票分割型の選挙プロトコルも，多値の確率的暗号系とShamirの(k,n)閾値秘密分散共有法を組合せをもとに構成されている．) 多値の確率的暗号系は，能動攻撃に対し安全ではない．そこで，送信者は知識のZKIPを行なうことにより，Pfizmannの攻撃を防いでいる．

3.1　r値の確率的暗号系

rは素数であるとする．

確率的暗号系

(平文) $0 \leq m < r$．

(秘密鍵) $r|p-1, r \not| q-1$を満たす二つの大きな素数p,q

(公開鍵) pとqの積nと，全てのxについて$y \neq x^r \bmod n$であるy

(暗号化) $c = E(m,x) = y^m x^r \bmod n$．ただし，$x$は$Z_n^*$から選んだ乱数．

(復号化) 全てのjに対して$c^{(p-1)/r} \bmod p$を$(y^{(p-1)/p})^j \bmod p$と比べる．

この確率的暗号系は，

$$E(m_1,x_1)E(m_1,x_2) = E(m_1+m_2 \bmod r, x_0)$$

を満たす．

3.2　提案方式

(公開情報の公開) 送信者S_iの匿名メッセージの内容m_iを，$0 \leq m_i < r$とする．各MIXセンタは，r値の確率的暗号系を公開しておく．

(匿名メッセージの送信) 各送信者S_iは$R_i(0) = m_i$であるような$k-1$次の多項式$R_i(x)$をランダムに選び，匿名メッセージとして，

$$B_i^{(0)} \triangleq [b_{i,1}^{(0)}, \ldots, b_{i,n}^{(0)}], \text{ ただし } b_{i,j}^{(0)} \triangleq E_j(R_i(j), x_{i,j})$$

を作り，$B_i^{(0)}$を公開ボードに公開する．また，B_iに含まれる暗号文に対する平文が，$k-1$次の多項式から作られていることを，検証センタに対しZKIPを用いて証明する．

(シャフル) MIXセンタC_1は，ランダム置換πと，$U_i(0) = 0$である$k-1$次の多項式$U_i(x)(0 \leq i \leq l)$を用意し，

$$B_1^{(1)} \triangleq [d_{i,1}, \ldots, d_{i,n}], \text{ ただし } d_{i,j} \triangleq b_{\pi(i),j}^{(0)} E_j(U_i(j), w_{i,j})$$

を作る．ただし$w_{i,j}$は乱数である．C_1は

$$(B_1^{(1)}, \ldots, B_l^{(1)})$$

を公開ボードに公開する．また，正しい処理をしていることを，検証センタに対しZKIPを用いて証明する．

他の MIX センタ C_j も，C_1 と同様の操作を順にし，結果：

$$(B_1^{(j)}, \ldots, B_l^{(j)})$$

を公開ボード に公開する．また，正しい処理をしていることを，検証センタに対し ZKIP を用いて証明する．

(復号化) 最後の MIX センタ C_n の公開値を

$$(B_1^{(n)}, \ldots, B_l^{(n)}), \text{ ただし } B_i^{(n)} = [b_{i,1}^{(n)}, \ldots, b_{i,n}^{(n)}]$$

とする．各 MIX センタ C_j は，$b_{i,j}^{(n)}(i = 1, \ldots, l)$ を復号化し，平文 $m_{i,j}$ を公開する．また，平文が正しいことを検証センタに対し ZKIP を用いて証明する．

(匿名メッセージの復元) 公開された k 個以上の $m_{i,j}(j = 1, \ldots, n)$ から，(k, n) 閾値法を用いてもとのメッセージ m_i' を求める．

匿名メッセージのシャフルをする時点で故障や不正を行った MIX センタがあった場合には，そのセンタのシャフルは飛ばして続ければよい．

4 効率的なシャフルの ZKIP

Standard な ZKIP に比べ通信量が $1/l$ になる，正しくシャフルしていることを示す ZKIP を示す．ここでは，C_1 の行うプロトコルを挙げる．他のセンタの行う ZKIP も全く同じように構成される．
証明すること：公開値

$$(A_1, \ldots, A_l), \quad \text{ただし} \quad A_i = [a_{i,1}, \ldots, a_{i,n}]$$
$$(B_1, \ldots, B_l), \quad \text{ただし} \quad B_i = [b_{i,1}, \ldots, b_{i,n}]$$

に対して，$U_i(0) = 0$ である $k-1$ 次の多項式 $U_i(1 \le i \le l)$，乱数 $w_{i,j}(1 \le i \le l, 1 \le j \le n)$ および置換 π が存在して，

$$b_{i,j} = a_{\pi(i),j} E_j(U_i(j), w_{i,j}) \tag{1}$$

が成り立つこと．

Protocol 1

(Step 1) MIX センタ C_1 は $\hat{U}_i(0) = 0$ である $k-1$ 次の多項式 $\hat{U}_i(1 \le i \le l)$，乱数 $\hat{w}_{i,j}(1 \le i \le l, 1 \le j \le n)$ および置換 τ をランダムに選び，

$$\hat{b}_{i,j} \triangleq a_{\tau(i),j} E_j(\hat{U}_i(j), \hat{w}_{i,j})$$

を計算し，

$$(\hat{B}_1, \ldots, \hat{B}_l), \quad \hat{B}_i = [\hat{b}_{i,1}, \ldots, \hat{b}_{i,n}]$$

を検証センタに送る．また，τ および $\tau\pi^{-1}$ のコミットメントを検証センタに送る．

(Step 2) 検証センタはランダムビット e および乱数 $c_i(1 \le i \le l)$ を C_1 に送る．

(Step 3) $e=0$ ならば，C_1は

$$\begin{aligned} U' &\triangleq \sum_{i=1}^{l} c_i \hat{U}_i, \\ w'_j &\triangleq \prod_{i=1}^{l} (\hat{w}_{i,j})^{c_i} \quad (1 \le j \le n), \end{aligned}$$

およびτを検証者に送る．$e=1$ ならば，C_1は

$$\begin{aligned} U'' &\triangleq \sum_{i=1}^{l} c_i (\hat{U}_i - U_{\phi(i)}), \\ w''_j &\triangleq \prod_{i=1}^{l} (\hat{w}_{i,j} / w_{\phi(i),j})^{c_i} \quad (1 \le j \le n), \\ \phi &\triangleq \pi^{-1}\tau \end{aligned}$$

を検証者に送る．

(Step 4) $e=0$ ならば，検証センタはU'が高々$(k-1)$ 次の多項式かつ $U'(0)=0$ であることと

$$\prod_{i=1}^{l} (\hat{b}_{i,j} / a_{\tau(i),j})^{c_i} = E_j(U'(j), w'_j) \quad (1 \le j \le n) \tag{2}$$

が成り立つことをチェックする．$e=1$ ならば，検証センタは U''が高々$(k-1)$ 次の多項式かつ $U''(0)=0$ であることと

$$\prod_{i=1}^{l} (\hat{b}_{i,j} / b_{\phi(i),j})^{c_i} = E_j(U''(j), w''_j) \quad (1 \le j \le n) \tag{3}$$

が成り立つことをチェックする．

(Step 5) 以上を十分大きい回数繰り返す．

Protocol 1 が completeness を満たすことは明らかである．次に soundness について考える．公開値 $(A_1, \ldots, A_l), (B_1, \ldots, B_l)$ を与えたとき，任意の置換πに対して

$$b_{i,j} = a_{\pi(i),j} E_j(U_i(j), w_{i,j})$$

が成り立つ $U_i(j)$ は一意に求まる．従って，$(n-1)$ 次以下の多項式 U_iも一意に定まる．不正な公開値とは，すべての置換πに対し，少なくとも一つの i が存在し，上式を満足する多項式 U_iが $U_i \neq 0$ または U_i は k次以上となる場合である．

これから先は，公開値は不正であるとする．

Lemma 4.1 π, τを任意に固定し，$\phi = \pi^{-1}\tau$とする．全ての c_iに対し次式を考える．

$$\prod_{i=1}^{l} (b_{\phi(i),j} / a_{\tau(i),j})^{c_i} = E_j(U(j), w_j) \tag{4}$$

すると，

$$Pr(\text{式 } (4) \text{ を満たす多項式 } U \text{ が，} k-1 \text{ 次以下でかつ } U(0)=0 \text{ を満たす}) \le 1/r.$$

さて，c_iを変化させたとき，(Step 4) の全てのチェックを満足するU', w'_j, U'', w''_jの存在する確率を考えよう．式 (2)，(3) から$\hat{b}$を消去すると，

$$\prod_{i=1}^{l}(b_{\phi(i),j}/a_{\tau(i),j})^{c_i} = E_j(U'(j) - U''(j), w'_j/w''_j)$$

となる．ここで，$U = U' - U'', w_j = w'_j/w''_j$としよう (すると上式は式 (4) と同じになることに注意)．U', U''が (Step 4) の全てのチェックを満足するならば，Uは $(k-1)$ 次以下であり $U(0) = 0$ を満たす．したがって

$$\Pr(U', w'_j, U'', w''_j\text{が存在する}) \leq \Pr(\text{式 (4) を満たす } U\text{が，} k-1 \text{ 次以下でかつ } U(0) = 0 \text{ を満たす})$$

となり，lemma より

$$\Pr(U', w'_j, U'', w''_j\text{が存在する}) \leq 1/r$$

となる．したがって，確率 $(1 - 1/r)$ で (Step 4) の全てのチェックを満足するU', w'_j, U'', w''_j は同時に存在せず，少なくとも一方の e でチェックが成り立たない．したがって 1 回の (Step 1) から (Step 4) までで不正が発覚する確率は$\frac{1}{2}(1 - 1/r)$ 以上であり，十分多く繰り返すことによって不正確率を無視できるほど小さくできる．

ZK 性は，標準的な方法で証明できる．

5 投票プロトコルへの応用

前節で示した匿名通信路を用いれば，センタの故障，不正に強い電子投票システムを作ることができる．

<u>提案する投票プロトコル</u>

(公開情報の公開) 投票者 S_iの投票したい候補者の氏名または候補者番号 m_iを，$0 \leq m_i < r$とする．各 MIX センタは，r値の確率的暗号系を公開しておく．

(投票者の確認) 各投票者 S_iは，投票の前に有権者であることを証明する．

(投票) 各投票者 S_iは m_iを，提案した (k, n) 閾値匿名通信路よって送る．

(投票値の復元) MIX センタによって並びかえられた投票値を復元し，投票結果を計算する．

参考文献

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

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

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

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

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

[6] K. Sako and J. Killian, Reciept-Free Mix-Type Voting Scheme, in: *Proc. of Eurocrypt '95*, 393–403 (1995).

[7] M. Michels and P. Horster, Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme, in: *Proc. of Asiacrypt '96*,