素因数分解の困難性を利用した紛失通信プロトコルについて

知識情報処理研究　　3603R057-0　藤原 亮介
指　　導　松嶋 敏泰 教授

On 1-out-of-n Oblivous Trasnfer Protocols based on Prime Factoring Problem

by Ryosuke Fujiwara

1　序論

近年更なる広がりをみせる情報化社会において，情報セキュリティの重要性は年々高まりをみせている．その情報セキュリティに関係する要素技術の中でも，特に重要とされるのが暗号技術である．暗号は公開鍵暗号と秘密鍵暗号に分類され，公開鍵暗号はある仮定を置いた時に，暗号の安全性を数学的に証明することができる．ある決められた手順で暗号を用いることで，メッセージ秘匿以外にもディジタル署名や個人認証，そして電子現金や電子投票等，様々な機能を実現する技術を暗号プロトコルという．

２者間で互いの所有情報を相手に秘匿しつつ，一部の情報のみの受け渡しを可能にする暗号プロトコルが，紛失通信プロトコルである．紛失通信にはまず，利用者の所有情報が他者に漏洩しないこと，つまり利用者の安全性を保証することが求められる．公開鍵暗号を利用した紛失通信プロトコルは，離散対数問題の困難性を安全性の根拠にした方式 [1] と，素因数分解問題の困難性を根拠にした方式 [2] に大きく分類される．これらの従来研究では，さらに理想的なランダム関数の存在を仮定して，プロトコルを構成しその安全性を証明している．ただし理想的なランダム関数は現実に存在しないので，実用時にはそれに近い性質を持つ関数で置き換えなくてはならず，その結果証明した安全性と実用時の安全性に差異が生じてしまう [5].

一方 Tzeng らは，理想的なランダム関数の存在を仮定しない紛失通信プロトコルを提案している [3]．このプロトコルは理想的なランダム関数を利用せず，離散対数問題の困難性のみを利用して安全性が証明されている．しかし理想的なランダム関数を利用せず，素因数分解の困難性のみを利用した紛失通信プロトコルはいまだ提案されていない．

そこで本研究では，理想的なランダム関数を利用せず，素因数分解の困難性のみを利用して紛失通信プロトコルを構成する．そして，その安全性を証明することを目的とする．

2　準備

確率的多項式時間アルゴリズムの集合を POLY，整数上の正多項式の集合を poly とする．自然数の集合 $\mathbb{N}$ から選択した k を，安全性の尺度として取り扱う．X_k は k-bit 空間上の確率変数であり，R_k は一様分布に従う k-bit 空間上の確率変数である．

2.1　計算量的識別不可能性

D は入力に対し独立な乱数 $r \in R_k$ を内部で生成し，確率的に {0,1} を出力する識別器である．本研究では，確率変数を入力とした D が出力 1 を導く確率を取り扱う為，集合 $A = \{(x,r) \mid D(x,r) = 1\}$ を与えて (1) 式のように定義する．

$$\mathrm{P}(D(X_k) = 1) \stackrel{\mathrm{def}}{=} \sum_{(x,r)\in A} \sum \Pr\{X_k = x, R_k = r\}. \quad (1)$$

定義 1. 計算量的識別不可能性

X_k, Y_k を k-bit 空間上の確率変数とし，X_k, Y_k の族を $\{X_k\}_{k\in\mathbb{N}}, \{Y_k\}_{k\in\mathbb{N}}$ とする．(2) 式を満たす時，確率変数族 $\{X_k\}_{k\in\mathbb{N}}, \{Y_k\}_{k\in\mathbb{N}}$ は計算量的に識別不可能である．

$$\forall D \in \mathrm{POLY} \ \ \forall F \in \mathrm{poly} \ \ \exists k_0 \ \ \forall k > k_0$$
$$\mid \mathrm{P}(D(X_k) = 1) - \mathrm{P}(D(Y_k) = 1) \mid < \frac{1}{F(k)}. \quad (2)$$

2.2　安全性の根拠となる仮定

公開鍵暗号を利用した紛失通信は，ある問題を解くことが困難であるという仮定の下に構成される．用いられる問題は大別すると２種類，離散対数問題と素因数分解問題である．ここで，$\mathbb{PRIME}_k$ は k-bit 空間上の素数の集合で，p, q は $\mathbb{PRIME}_k$ 上の素数である．$\mathbb{Z}_q$ は q を法とする剰余系であり，$\mathbb{Z}_q^*$ は $\mathbb{Z}_q$ かつ q と互い

に素となる数の集合である．また，$\mathbb{N}$ の一様分布に従って出力される r を $r \in_R \mathbb{N}$ と表記する．

2.2.1 離散対数問題に属する問題

離散対数問題とは，$g^a \bmod q$ が与えられた時に a を求める問題である．そして Decision Diffie-Hellman Problem(DDH) は，離散対数問題において２種の値を識別する問題である．

仮定 2. DDH 仮定

以下によって確率変数 X_k, Y_k を定めた時，確率変数族 $\{X_k\}_{k\in\mathbb{N}}, \{Y_k\}_{k\in\mathbb{N}}$ が計算量的識別不可能性を満たすと仮定する．

$$\begin{aligned} X_k &= \{(g, g^a, g^b, g^{ab})\},\ g \in_R \mathbb{Z}_q,\ (a,b) \in_R \mathbb{Z}_q^*, \\ Y_k &= \{(g, g^a, g^b, g^c)\},\ g \in_R \mathbb{Z}_q,\ (a,b,c) \in_R \mathbb{Z}_q^*. \end{aligned}$$

離散対数問題を解くアルゴリズムが存在する時，DDH が解かれるのは明らか (逆は成立しない)．

2.2.2 素因数分解問題に属する問題

素数 p, q を選択して $N = pq$ とし，N の Carhmichael 関数 $\lambda(N)$ の値を $\lambda = lcm(p-1, q-1)$ とする．

素因数分解問題とは N が与えられた時，N の素因数 p, q を求める問題である．そして Decision Composite Residuosity Class Problem(DCR) は，素因数分解問題において２種の値を識別する問題である [4]．

仮定 3. DCR 仮定

以下によって確率変数 X_k, Y_k を定めた時，確率変数族 $\{X_k\}_{k\in\mathbb{N}}, \{Y_k\}_{k\in\mathbb{N}}$ が計算量的識別不可能性を満たすと仮定する．

$$\begin{aligned} X_k &= \{(N, g, x, z) \mid z = g^x r^N \bmod N^2\}, \\ &\qquad x \in_R \mathbb{Z}_N,\ (g,r) \in_R \mathbb{Z}_{N^2}^*, \\ Y_k &= \{(N, g, x, z)\},\quad x \in_R \mathbb{Z}_N,\ (g,z) \in_R \mathbb{Z}_{N^2}^*. \end{aligned}$$

素因数分解問題を解くアルゴリズムが存在する時，$\lambda(N)$ が計算可能なのは明らか．さらに

$$r^{\lambda} = 1 \bmod N, \tag{3}$$
$$r^{N\lambda} = 1 \bmod N^2, \tag{4}$$

より DCR が解かれるのは明らか (逆は成立しない)．

3 紛失通信

3.1 紛失通信の問題設定

1-out-of-n 紛失通信とは，送信者が持つ n 個の情報 $m_1, ..., m_n$ のうち，受信者が選択した $\alpha \in \{1, ..., n\}$ に対応する情報 m_α を，受信者が取得する暗号プロトコルである．送信者が $m_1, ..., m_n$ を $c_1, ..., c_n$ に暗号化し，受信者に全て送信．受信者は α に対応する c_α を選択，復号して m_α を取得する．この時，(1) 受信者は選択した α を送信者に知られない，(2) 送信者は保有する n 個の情報の内，m_α 以外の情報を受信者に知られない，という形で各利用者の安全性を保証する．

3.2 紛失通信の安全性

定義 4. 受信者の安全性

受信者 R は選択した α_0, α_1 から y_0, y_1 を作成する．任意の α_0, α_1 に対し，送信者 S が得られる y_0, y_1 が確率変数となる．その族が計算量的に識別不可能ならば，送信者は受信者の選択 α に関するいかなる情報も得ることができない．

定義 5. 送信者の安全性

通常のプロトコルと，不正を行わない第三者 T が存在する理想的なプロトコルを比較する．受信者 R は送信者 S とプロトコルを実行し，$m_1, ..., m_n$ を暗号化した $c_1, ..., c_n$ と補助情報，そして m_α を得る．受信者 R' は R と S をシミュレートし，$m_1, ..., m_n$ とは独立に定められた乱数 $c'_1, ..., c'_n$ と補助情報を得た上で，第三者機関 T と通信を行う．T は R' から得られた α に対し，m_α と c_α を R' に与える．

任意の $m_1, ..., m_n$ に対し，R と R' が取得した情報が確率変数となる．その族が計算量的に識別不可能ならば，受信者は送信者が所有する情報 $m_1, ..., m_n$ に関するいかなる情報も得ることができない．

4 紛失通信の従来研究

4.1 ランダム関数仮定下で安全な方式

理想的なランダム関数の存在を仮定して紛失通信を構成し，その安全性を証明している従来研究として，離散対数問題に属する問題を用いる [1] と，素因数分解問題に属する問題を用いる [2] が挙げられる．

4.2 DDH 仮定下で安全な方式 [3]

[3] では，理想的なランダム関数の存在を仮定せず，離散対数問題に属する DDH の困難性のみを仮定して，

紛失通信を構成しその安全性を証明している．

Step0. 初期設定
公開情報：$g,\ h,\ \mathbb{Z}_q$　　…受信者に $\log_g h$ は未知
送信者　：$m_1, ..., m_n \in \mathbb{Z}_q$
受信者　：$\alpha \in \{1, ..., n\}$

Step1. 受信者 → 送信者
$t \in_R \mathbb{Z}_q^*$ を選択し，y を計算．

$$y \stackrel{\text{def}}{=} g^t h^\alpha. \tag{5}$$

y を送信者へ．

Step2. 送信者 → 受信者
for $1 \leq i \leq n$
$r_i \in_R \mathbb{Z}_q^*$ を選択し，c_i, PK_i を計算．

$$c_i \stackrel{\text{def}}{=} m_i(\frac{y}{h^i})^{r_i} \quad = m_\alpha(\frac{g^t h^\alpha}{h^\alpha})^{r_\alpha} = m_\alpha g^{tr_\alpha}. \tag{6}$$

$$\mathrm{PK}_i \stackrel{\text{def}}{=} g^{r_i}. \tag{7}$$

$c_1, ..., c_n,\ \mathrm{PK}_1, ..., \mathrm{PK}_n$ を受信者へ．

Step3. 受信者
受信者は $c_\alpha, \mathrm{PK}_\alpha$ を選択して，m_α を計算．

$$(\mathrm{PK}_\alpha)^t = g^{tr_\alpha}. \tag{8}$$

$$\frac{c_\alpha}{(\mathrm{PK}_\alpha)^t} = \frac{m_\alpha g^{tr_\alpha}}{g^{tr_\alpha}} = m_\alpha. \tag{9}$$

受信者は α に対応する m_α を取得．

5　提案法

5.1　素因数分解の困難性を利用した紛失通信

紛失通信の安全性の定義から，理想的なランダム関数の存在を仮定しなくても，計算量的識別不可能性を満たす数論の問題があれば，安全な紛失通信が構成できると考えられる．

[3] は理想的なランダム関数の存在を仮定せず，計算量的識別不可能性を満たす問題，つまり離散対数問題に属する DDH の困難性のみを仮定して，紛失通信を構成しその安全性を証明している．

そこで本研究では，理想的なランダム関数の存在を仮定せず，計算量的識別不可能性を満たす問題，つまり素因数分解問題に属する DCR の困難性のみを仮定して，紛失通信を構成しその安全性を証明する．

5.2　DCR 仮定下で安全な方式 (提案法)

Step0. 初期設定
公開情報：$N,\ \mathbb{Z}_N,\ \mathbb{Z}_{N^2}$
送信者　：$\lambda,\ \ m_1, ..., m_n \in \mathbb{Z}_N$
受信者　：$\alpha \in \{1, ..., n\}$

Step1. 受信者 → 送信者
$t \in_R \mathbb{Z}_N$ を選択して，y を計算．

$$y \stackrel{\text{def}}{=} \alpha t. \tag{10}$$

y を送信者へ．

Step2. 送信者 → 受信者
for $1 \leq i \leq n$
$r_i \in_R \mathbb{Z}_{N^2}^*$ を選択して，c_i を計算．

$$c_i \stackrel{\text{def}}{=} (1+N)^{m_i} r_i^N \bmod N^2. \tag{11}$$

$s_i \in_R \mathbb{Z}_N$ を選択して，$\mathrm{PK}_i, \mathrm{PK}'_i$ を計算．

$$\mathrm{PK}_i \stackrel{\text{def}}{=} \lambda + s_i y \quad = \lambda + s_\alpha \alpha t. \tag{12}$$

$$\mathrm{PK}'_i \stackrel{\text{def}}{=} r_i^{s_i i} \quad = r_\alpha^{s_\alpha \alpha}. \tag{13}$$

$c_1, ..., c_n,\ \mathrm{PK}_1, ..., \mathrm{PK}_n,\ \mathrm{PK}'_1, ..., \mathrm{PK}'_n$ を受信者へ．

Step3. 受信者
受信者は $c_\alpha, \mathrm{PK}_\alpha, \mathrm{PK}'_\alpha,$ を選択して，m_α を計算．

$$(\mathrm{PK}'_\alpha)^{Nt} = r_\alpha^{s_\alpha \alpha N t}. \tag{14}$$

$$c_\alpha^{\mathrm{PK}_\alpha} = \{(1+N)^{m_\alpha} r_\alpha^N\}^{(\lambda + s_\alpha \alpha t)}. \tag{15}$$

$$\frac{c_\alpha^{\mathrm{PK}_\alpha}}{(\mathrm{PK}'_\alpha)^{Nt}} = \frac{\{(1+N)^{m_\alpha} r_\alpha^N\}^{(\lambda + s_\alpha \alpha t)}}{r_\alpha^{s_\alpha \alpha N t}}, \tag{16}$$

$$= (1+N)^{m_\alpha(\lambda + s_\alpha \alpha t)} r_\alpha^{N\lambda}, \tag{17}$$

$r_i^{N\lambda} = 1 \bmod N^2$ より，

$$= (1+N)^{m_\alpha(\lambda + s_\alpha \alpha t)}, \tag{18}$$

$(1+N)^a = 1 + aN \bmod N^2$ より，

$$= 1 + (\lambda + s_\alpha \alpha t) N m_\alpha. \tag{19}$$

$$(1+N)^{\mathrm{PK}_\alpha} = (1+N)^{\lambda + s_\alpha \alpha t}, \tag{20}$$

$$= 1 + (\lambda + s_\alpha \alpha t) N. \tag{21}$$

$$\frac{\frac{c_\alpha^{\mathrm{PK}_\alpha}}{(\mathrm{PK}'_\alpha)^{Nt}} - 1}{(1+N)^{\mathrm{PK}_\alpha} - 1} = \frac{(\lambda + s_\alpha \alpha t) N m_\alpha}{(\lambda + s_\alpha \alpha t) N}, \tag{22}$$

$$= m_\alpha. \tag{23}$$

受信者は α に対応する m_α を取得．

5.3 提案プロトコルの安全性証明

定理 6. 提案プロトコルは受信者の安全性を満たす.

証明. 受信者 R は選択した α に対し独立に乱数 t を定め，$y = \alpha t$ を作成する．y の分布は t に従うので，確率変数 y_0, y_1 は共に一様分布に従う．よって y_0, y_1 の族が計算量的に識別不可能なので，提案プロトコルは受信者の安全性を満たす.

定理 7. DCR 仮定下において，提案プロトコルは送信者の安全性を満たす.

証明. 提案プロトコルにおいて，送信者の安全性を侵害するアルゴリズム (R と R' の出力を識別可能な D') が存在すると仮定．D' が存在する時，DCR を解く D が存在することを示す.

(1)D は入力 (N, g, x, z) に対し，提案プロトコルを $g = 1 + N,\ x = s_\beta,\ z = c_\beta$ という値で実行する.

(2)D は提案プロトコルから得られた出力から，$(c_\beta, \mathrm{PK}_\beta, \mathrm{PK}'_\beta)$ を選択し，$\frac{c_\beta^{\mathrm{PK}_\beta}}{(\mathrm{PK}'_\beta)^{Nt}}$ を計算する.

(3)D は入力 $(N,\ 1+N,\ \mathrm{PK}_\beta, \frac{c_\beta^{\mathrm{PK}_\beta}}{(\mathrm{PK}'_\beta)^{Nt}})$ に対し，D' を用いて値の識別を試みる.

(3a) $z = g^x r^N \bmod N^2$ の時，入力は (24) 式に従う.

$$\frac{c_\beta^{\mathrm{PK}_\beta}}{(\mathrm{PK}'_\beta)^{Nt}} = \{(1+N)^{m_\beta}\}^{(\lambda + s_\beta \alpha t)} r^{NS_\beta t(\alpha-\beta)}. \quad (24)$$

入力は提案プロトコルに従うので，D' は入力を R からの出力と判定し，1 を出力する.

(3b) $z \in \mathbb{Z}^*_{N^2}$ の時，入力は (25) 式に従う.

$$\frac{c_\beta^{\mathrm{PK}_\beta}}{(\mathrm{PK}'_\beta)^{Nt}} = \frac{c_\beta^{\lambda + s_\beta \alpha t}}{r^{s_\beta \beta N t}}. \quad (25)$$

入力は提案プロトコルに従わないので，D' は入力を R' からの出力と判定し，0 を出力する.

(4)D は D' の識別結果を用いて，DCR を識別する.
$D' = 1$ ならば，D は入力を $(N, g, x, z) \in X_k$ と判定.
$D' = 0$ ならば，D は入力を $(N, g, x, z) \in Y_k$ と判定.

以上より，送信者の安全性を侵害する D' が存在する時，DCR を識別可能な D が存在する．ただし，DCR 仮定により DCR を解くアルゴリズム D は存在しない．よって矛盾となり D' も存在しないことになり，R と R' が取得する情報を確率変数とした時，その族は計算量的識別不可能性を満たす．よって提案プロトコルは送信者の安全性を満たす.

6 考察

提案法の証明より，計算量的識別不可能性をもつ DCR 仮定のみでも，紛失通信の安全性を証明することができた．[3] で離散対数問題に属する DDH，本研究で素因数分解問題に属する DCR について，同じ結果が得られたことになる．この 2 種類の問題においては，理想的なランダム関数の存在を仮定して証明された紛失通信の安全性を，計算量的識別不可能性をもつ問題のみによっても証明できることが解った.

また，紛失通信の評価基準として計算量 (べき乗計算の回数) が挙げられるが，[3] が (6) 式で m_i の暗号化時に y を用いるのに対し，提案法は (11) 式で m_i の暗号化時に y を用いていない．よって提案法では受信者の計算量は増大しているものの，送信者はプロトコル開始前の計算が可能になり，全体としてプロトコル開始後の計算量は削減されている.

7 結論

本研究では，理想的なランダム関数の存在を仮定せず，素因数分解問題に属する DCR の困難性のみを仮定して，紛失通信を構成し安全性の証明を与えた.

今後の課題として，より解くのが困難な問題を用いて安全性を証明することで，紛失通信の安全性を向上させていくことが挙げられる.

参考文献

[1] M.Naor and B.Pinkas,“ Efficient Oblivious Trasnfer Protocols, ”*Proc. 12th Ann. Symp. Discrete Algorithms*, pp.448-457, 2001.

[2] K.Kurosawa and Q.V.Duong,“ How to Design Efficient Multiple-Use 1-out-of-n Oblivious Trasnfer, ”*IEICE Transaction Fundamentals*, Vol.E87-A, No.1, pp.141-146, January 2004.

[3] W.G.Tzeng,“ Efficient 1 out of n Ovlivious Trasnfer Schemes with Universally Usable Parameters, ”*IEEE Transaction on Computers*, Vol.53, No.2, pp.232-240, February 2004.

[4] P.Paillier,“ Public-Key Cryptosystems Based on Composite Degree Residuosity Class, ”*Advances in Cryptology - EUROCRYPTO'99*, Vol.1592 of LNCS, Springer-Verlag, pp.223-238, 1999.

[5] Ran Canetti, Oded Goldreich and Shai Halevi, “ Random Oracle Methodology, ”*In Proc. of 30th Annual ACM Symposium on the Theory of Computing*, pp.209-218, May 1998.