コンピュータセキュリティ 10−10
(2000. 7. 25)

合成数を法とする離散対数問題と暗号への応用

松川公一　早田孝博　小林邦勝

山形大学工学部情報科学科
〒992-8510 米沢市城南 4-3-16
Tel : 0238-26-3345　E-mail : kobayash@ee5.yz.yamagata-u.ac.jp

あらまし　合成数を法とする離散対数問題に落し戸を作り、これを暗号に応用する。位数の小さい元を底とする離散対数の計算は容易に行うことができるが、位数の大きい元を底とする離散対数を計算することは難しい。この違いを利用して合成数を法とする離散対数問題に落し戸を作る。幾つかの異なる素数の積からなる大きな合成数の素因数分解が困難であれば、この合成数を法として位数の大きい元を底とする離散対数を計算することは難しいが、素因数を知っている場合には、これらの素数を法として位数の小さい元を底とする離散対数を容易に計算することができる。この合成数を法とする離散対数問題を公開鍵暗号とディジタル署名に応用する。

キーワード　合成数を法とする離散対数問題、位数、落し戸、公開鍵暗号、ディジタル署名

Discrete Logarithm Problem over Composite Modulus and Its Application to Cryptography

Koichi MATSUKAWA　Takahiro HAYATA　Kunikatsu KOBAYASHI

Faculty of Engineering, Yamagata University
4-3-16, Jyonan, Yonezawa, 992-8510 Japan
Tel : 0238-26-3345　E-mail : kobayash@ee5.yz.yamagata-u.ac.jp

Abstract

We propose a discrete logarithm problem over composite modulus with the trapdoor , and apply it to cryptography. It is easy to calculate a discrete logarithm problem with the base g having a small order, but it is hard to calculate a discrete logarithm problem with the base g having a large order. By using these differences, we can make the trapdoor in the discrete logarithm problem over composite modulus.

key words　discrete logarithm problem over composite modulus, order, trapdoor, public key cryptosystem, digital signature

1. まえがき

公開鍵暗号の代表的なものに，離散対数問題の難しさに安全性の根拠を置く ElGamal 暗号 [1] があり，最近は，この概念を楕円曲線上に適用した楕円曲線暗号 [2], [3] の研究が活発に行われている．素数を法とする離散対数問題には現時点では落し戸が作られておらず，ElGamal 暗号の場合には復号をするために暗号文の他に乱数に基づく余分な情報も受信者に送る必要がある．一方，離散対数問題をより一般化することや離散対数問題に落し戸を作ること等を目的に，合成数を法とする離散対数問題の研究 [4], [5] が行われており，離散対数問題に落し戸を作ることができれば伝送効率を高めることができると考えられる．

本文では，離散対数問題に落し戸を作ることを目的として，合成数を法とする離散対数問題について考察する．位数の小さい元を法とする離散対数の計算は容易に行うことができるが，位数の大きい元を底とする離散対数を計算することは難しい．この違いを利用して，合成数の素因数分解が困難であるという条件のもとで，合成数を法とする離散対数問題に落し戸を作り，この落し戸を用いた公開鍵暗号とディジタル署名のアルゴリズムを提案する．初めに，合成数 $n=\prod_{i=1}^{l} p_i$ を法とする離散対数問題を解くアルゴリズムを示す．このアルゴリズムは，公開鍵 a, n と与えられた $y \equiv a^x (\mathrm{mod} n)$ から各素因数 p_i のもとでの離散対数 $x_i \equiv x (\mathrm{mod} p_i)$ を求め，それらを中国人の剰余定理を用いて組み合わせることにより，離散対数 x を求めるものである．次に，合成数を法として位数の大きい元を底とする離散対数問題を公開鍵暗号に応用する．位数の小さい元のみを用いて離散対数の底になる公開鍵を定めると，この元をその位数乗することにより秘密鍵が求まり，暗号が解読される問題が生じる．この問題を避けるために，本文では，位数の小さい元の他に位数の大きい元も用いて，両者の位数の積を位数とする元を用いて公開鍵を生成し，これを底とする離散対数問題を扱う．このとき，Fermat の小定理を用いて小さい位数と大きい位数に関係を与える．次に，この暗号の安全性について検討し，公開鍵から秘密鍵を求めること，暗号文から平文を求めること，暗号文から平文の部分情報を求めることは，いずれも計算量的に難しいことを示す．最後に，この合成数を法とする離散対数問題をディジタル署名に応用し，鍵生成，署名手順，検証手順を示す．また，この署名を偽造することは計算量的に困難であることを示す．

2. 準　　備

互いに異なる l 個の素数を $q_i (1 \leqq i \leqq l)$，任意の正整数を e_i とし，

$$m = \prod_{i=1}^{l} q_i^{e_i} \tag{1}$$

$$m_i = \frac{m}{q_i^{e_i}} (1 \leqq i \leqq l) \tag{2}$$

とおく．次に，

$$p_i \equiv 1 (\mathrm{mod} q_i^{e_i}) (1 \leqq i \leqq l) \tag{3}$$

を満たす素数 p_i を求め

$$n = \prod_{i=1}^{l} p_i \tag{4}$$

$$n_i = \frac{n}{p_i} (1 \leqq i \leqq l) \tag{5}$$

とおく．ここで，l 個の素数 p_i は互いに異なるとする．このとき，Euler 関数より，法 p_i に対する 1 の原始 $q_i^{e_i}$ 乗根は $(q_i-1)q_i^{e_i-1}$ 個存在する．つまり，

$$a_i^{q_i^{e_i}} \equiv 1 (\mathrm{mod} p_i) (1 \leqq i \leqq l) \tag{6}$$

を満たす，位数が $q_i^{e_i}$ である $GF(p_i)$ の元 a_i は $(q_i-1)q_i^{e_i-1}$ 個存在する．
次に，この a_i を用いて

$$a \equiv \sum_{i=1}^{l} a_i n_i \left(n_i^{-1} \bmod p_i \right) (\mathrm{mod} n) \tag{7}$$

を求める．このとき，

$$a^{q_i^{e_i}} \equiv 1 (\mathrm{mod} p_i) \tag{8}$$

より，

$$GCD\left(a^{q_i^{e_i}} - 1, n\right) = p_i \tag{9}$$

となる．

平文 x の範囲を $0 < x < m$ とするとき，合成数 n を法とし，式 (7) の a を底とする離散対数問題は

$$y \equiv a^x (\mathrm{mod} n) \tag{10}$$

の y, a, n が与えられたときに x を求める問題であり，次の手順で離散対数 x は得られる．
手順 1．合成数 n の l 個の素因数 p_i を用いて

$$\begin{aligned} y_i &\equiv y(\mathrm{mod}p_i) \\ &\equiv (a_1 n_1 n_1^{-1} + \cdots + a_l n_l n_l^{-1})^x (\mathrm{mod}p_i) \\ &\equiv a_i^x (\mathrm{mod}p_i) \\ &\equiv a_i^{x_i} \end{aligned} \quad (11)$$

を，各々，求める．

手順２．この $a_i^{x_i}$ の値は

$$y_i \equiv y(\mathrm{mod}p_i) \equiv \begin{cases} a_i^0 \\ a_i^1 \\ \vdots \\ a_i^{q_i^{e_i}-1} \end{cases} \quad (12)$$

の右辺の $q_i^{e_i}$ 個の中のいずれかの値と等しくなるから，式 (12) の左辺と右辺を比べることにより，x_i が得られる．

手順３．式 (3) より，x と x_i の間には

$$x_i \equiv x(\mathrm{mod}q_i^{e_i}) \quad (13)$$

の関係が成り立つから，式 (10) の離散対数 x の値は中国人の剰余定理を用いて

$$x \equiv \sum_{i=1}^{l} x_i m_i \left(m_i^{-1} \bmod q_i^{e_i} \right) (\mathrm{mod}m) \quad (14)$$

と求まる．

3. 公開鍵暗号への応用

次の２つの条件を満たすとき，この合成数を法とする離散対数問題は公開鍵暗号に応用することができる．

(条件１) 式 (6) を満たす元 a_i の位数 $q_i^{e_i}$ は離散対数が計算できる程度に小さいこと，つまり，a_i^0 から $a_i^{q_i^{e_i}-1}$ までの $q_i^{e_i}$ 個の値をソートして，表に表わすことができる程度に $q_i^{e_i}$ の値が小さいこと．例えば，$q_i^{e_i}$ は 10^7 以下など．

(条件２) 式 (4) で与えられる合成数 n の素因数分解が困難となる程度に素数 p_i が大きいこと．例えば，p_i は 10^{150} 以上など．

3.1 鍵 生 成

互いに異なる l 個の小さな素数 q_i を定め，

$$q_i^{e_i} \leqq 10^7 (1 \leqq i \leqq l) \quad (15)$$

を満たす最大の正整数 e_i を求める．

これらを用いて，式 (1),(2) の m と m_i を計算する．

次に，k_i を適当な正整数とし，次の２つの関係を満たす素数 p_i を定める．

$$q_i^{e_i} \mid p_i - 1 \quad (16)$$

$$k_i q_i^{e_i} + 1 \mid p_i - 1 \quad (17)$$

ここで，位数 $q_i^{e_i}$ は離散対数が計算できる程度に小さい値であるのに対して，位数 $k_i q_i^{e_i} + 1$ は離散対数の計算が困難である大きな値とする．

また，位数が $k_i q_i^{e_i} + 1$ である $GF(p_i)$ の元 b_i

$$b_i^{k_i q_i^{e_i}+1} \equiv 1 (\mathrm{mod}p_i) \quad (18)$$

を求め，この b_i と式 (6) の a_i を用いて

$$e \equiv \sum_{i=1}^{l} a_i b_i n_i (n_i^{-1} \bmod p_i) (\mathrm{mod}n) \quad (19)$$

を計算する．ここで，

$$e^{q_i^{e_i}(k_i q_i^{e_i}+1)} \equiv 1 (\mathrm{mod}p_i) \quad (20)$$

より

$$GCD\left(e^{q_i^{e_i}(k_i q_i^{e_i}+1)} - 1, n \right) = p_i \quad (21)$$

となるが，

$$\begin{aligned} e^{q_i^{e_i}} &\not\equiv 1 (\mathrm{mod}p_i) \\ e^{k_i q_i^{e_i+1}} &\not\equiv 1 (\mathrm{mod}p_i) \end{aligned} \quad (22)$$

より

$$\begin{aligned} GCD\left(e^{q_i^{e_i}} - 1, n \right) &\neq p_i \\ GCD\left(e^{k_i q_i^{e_i}+1} - 1, n \right) &\neq p_i \end{aligned} \quad (23)$$

である．公開鍵は式 (4) の n と式 (19) の e であり，秘密鍵は $q_i, e_i, p_i, a_i, b_i, k_i (1 \leqq i \leqq l)$ である．

3.2 暗 号 化

式 (1) の m より小さい適当な正整数 M を公開し，平文 x のとり得る範囲を

$$0 < x \leqq M \quad (24)$$

とし，暗号文 y を

$$y \equiv e^x (\mathrm{mod}n) \quad (25)$$

で定める．

3.3 復 号 化

まず，秘密鍵 p_i を用いて

$$\begin{aligned} y_i &\equiv y(\mathrm{mod}p_i) \\ &\equiv \left(\sum_{i=1}^{l} a_i b_i n_i (n_i^{-1} \bmod p_i) \right)^x (\mathrm{mod}p_i) \\ &\equiv (a_i b_i)^x (\mathrm{mod}p_i) \end{aligned} \quad (26)$$

を求め，次に，式 (18) の関係を満たす秘密鍵 $k_i q_i^{e_i} + 1$ を用いて

$$
\begin{aligned}
z_i &\equiv y_i^{k_i q_i^{e_i}+1} (\mathrm{mod} p_i) \\
&\equiv ((a_i b_i)^x)^{k_i q_i^{e_i}+1} \\
&\equiv \left(a_i^{k_i q_i^{e_i}+1} \cdot b_i^{k_i q_i^{e_i}+1} \right)^x \\
&\equiv \left(\left(a_i^{q_i^{e_i}} \right)^{k_i} \cdot a_i \cdot b_i^{k_i q_i^{e_i}+1} \right)^x \\
&\equiv a_i^x
\end{aligned} \tag{27}
$$

を計算する．この z_i は式 (12) の右辺のいずれかの値と等しいから，これら $q_i^{e_i}$ 個の値をソートした表などを用いて，式 (13) の x_i を求める．最後に，式 (14) を用いて平文 x を求める．簡単な数値例を以下に示す．

(例 1) $q_1 = 5, e_1 = 1, k_1 = 3, q_2 = 7, e_2 = 1, k_2 = 2, q_3 = 2, e_3 = 3, k_3 = 2$ とすると

$$
\begin{aligned}
q_1^{e_1} &= 5, k_1 q_1^{e_1} + 1 = 16 \\
q_2^{e_2} &= 7, k_2 q_2^{e_2} + 1 = 15 \\
q_3^{e_3} &= 8, k_3 q_3^{e_3} + 1 = 17
\end{aligned} \tag{28}
$$

となり，式 (16),(17) を満たす素数 p_i を $p_1 = 241, p_2 = 211, p_3 = 137$ と定める．これらの素数を法として，位数が $q_i^{e_i}$ の元 a_i と位数が $k_i q_i^{e_i} + 1$ の元 b_i を求めると

$$
\begin{aligned}
a_1 &= 87, b_1 = 44 \\
a_2 &= 58, b_2 = 19 \\
a_3 &= 10, b_3 = 16
\end{aligned} \tag{29}
$$

が得られる．因みに，法 p_i のもとでの元 $a_i b_i$ の位数は，各々，80,105,136 となる．また，他の値は

$$
\begin{aligned}
n &= p_1 p_2 p_3 = 6966587 \\
n_1 &= n/p_1 = 28907, n_1^{-1} \equiv 37 (\mathrm{mod} p_1) \\
n_2 &= n/p_2 = 33017, n_2^{-1} \equiv 117 (\mathrm{mod} p_2) \\
n_3 &= n/p_3 = 50851, n_3^{-1} \equiv 40 (\mathrm{mod} p_3)
\end{aligned} \tag{30}
$$

$$
\begin{aligned}
m &= q_1^{e_1} q_2^{e_2} q_3^{e_3} = 280 \\
m_1 &= m/q_1^{e_1} = 56, m_1^{-1} \equiv 1 (\mathrm{mod} q_1^{e_1}) \\
m_2 &= m/q_2^{e_2} = 40, m_2^{-1} \equiv 3 (\mathrm{mod} q_2^{e_2}) \\
m_3 &= m/q_3^{e_3} = 35, m_3^{-1} \equiv 3 (\mathrm{mod} q_3^{e_3})
\end{aligned} \tag{31}
$$

となり，式 (19) で定める公開鍵 e は $e = 3331315$ となる．

次に，平文 x の上限 M を $M = 256$ と定め，n, e, M の 3 つを公開する．$x = 234$ のとき，暗号文 y は式 (25) より $y = 1906357$ となる．復号は，まず，秘密鍵 p_i を用いて

$$
\begin{aligned}
y_1 &= y (\mathrm{mod} p_1) \equiv 47 \\
y_2 &= y (\mathrm{mod} p_2) \equiv 183 \\
y_3 &= y (\mathrm{mod} p_3) \equiv 2
\end{aligned} \tag{32}
$$

を求め，次に，これらを法 p_i のもとで $(k_i q_i^{e_i} + 1)$ 乗して

$$
\begin{aligned}
y_1^{16} &= 205 \equiv 87^{x_1} (\mathrm{mod} p_1) \\
y_2^{15} &= 148 \equiv 58^{x_2} (\mathrm{mod} p_2) \\
y_3^{17} &= 100 \equiv 10^{x_3} (\mathrm{mod} p_3)
\end{aligned} \tag{33}
$$

を求め，あらかじめソートして表などに求めている離散対数とこれらを比較することにより，平文の部分情報 x_i は

$$
x_1 = 4, x_2 = 3, x_3 = 2 \tag{34}
$$

と得られる．従って，平文 x は式 (14) より $x = 234$ と求まる．

3.4 安全性の検討

まず，本暗号の要点をまとめると次のようになる．

(1) 各素数 p_i のもとで，離散対数が計算できる程度に小さい位数 $q_i^{e_i}$ の元 a_i を用いる．

(2) これら a_i と離散対数の計算が困難な大きい位数 $k_i q_i^{e_i} + 1$ の元 b_i を用いて，中国人の剰余定理で公開鍵 e を定める．この e は

$$
e^{q_i^{e_i}} \not\equiv 1 (\mathrm{mod} p_i) \tag{35}
$$

$$
e^{q_i^{e_i}(k_i q_i^{e_i}+1)} \equiv 1 (\mathrm{mod} p_i) \tag{36}
$$

を満たす．つまり，$q_i^{e_i} (k_i q_i^{e_i} + 1)$ の値を特定することが計算量的に難しいように k_i を大きく定め，公開鍵 e と n から秘密鍵 p_i を求めることが計算量的に難しいようにする．

(3) 平文 x を 1 から順に変えて，暗号文 $y \equiv e^x (\mathrm{mod} n)$ と一致する x を求めることが計算量的に困難となるように，平文 x の上限 M の値を大きく定める．M はおおよそ

$$
M \approx \prod_{i=1}^{l} q_i^{e_i} \tag{37}
$$

で与えられるから，この値が十分大きくなるように l を定める．

(4) 合成数 $n = \prod_{i=1}^{l} p_i$ の素因数分解が計算量的に難しいように，素数 p_i を大きく定める．

これらの条件のもとで本暗号の安全性の検討を行う．

(1) 公開鍵 e と n から秘密鍵 p_i を求める困難さ．

式 (36) より

$$
GCD \left(e^{q_i^{e_i}(k_i q_i^{e_i}+1)} - 1, n \right) = p_i \tag{38}
$$

となる．法 p_i のもとでの元 $a_i b_i$ の位数 $q_i^{e_i} (k_i q_i^{e_i} + 1)$ が大きく，(例えば，256bit) 全数探索でこの値を特定することが計算量的に難しい場合には，公開鍵か

ら秘密鍵を求めることは難しい，

(2) 暗号文 y から平文 x を求める困難さ．

式 (25) の暗号文 y から平文 x を求めることは，合成数を法とする離散対数問題を計算することになるが，現時点では，素因数分解の難しい合成数を法とする離散対数問題を効率的に解くアルゴリズムは知られていない．つまり，式 (25) の暗号文 y から平文 x を直接求めることは難しい．

(3) 暗号文 y から平文の部分情報 x_i を求める困難さ．

合成数 n の素因数分解は難しいと仮定しているので，暗号文 y から式 (26) の暗号文の部分情報 y_i を求めることは難しい．従って，この y_i から得られる平文の部分情報 x_i を求めることも難しい．

4. ディジタル署名への応用

4.1 鍵 生 成

2つの大きな素数 q_1 と q_2 を選び，

$$p_i \equiv 1(\mathrm{mod} q_i)(i=1,2) \tag{39}$$

を満たす互いに異なる素数 p_1 と p_2 を定める．これらの積を

$$n = p_1 p_2, \quad m = q_1 q_2 \tag{40}$$

とし，法 p_i に対する 1 の原始 q_i 乗根の一つを $a_i(i=1,2)$ とする．ここで，p_1 と p_2 は大きく，合成数 n の素因数分解は難しいと仮定する．次に，

$$\begin{aligned} a \equiv\ & a_1 p_2 \left(p_2^{-1} \bmod p_1\right) \\ & + a_2 p_1 \left(p_1^{-1} \bmod p_2\right) (\mathrm{mod} n) \end{aligned} \tag{41}$$

を求め，この a と n を公開する．

4.2 署 名 法

文書 M のとり得る範囲を

$$0 < M < m \tag{42}$$

とし，次の M_i

$$M_i \equiv M(\mathrm{mod} q_i)(i=1,2) \tag{43}$$

を用いて

$$\begin{aligned} S_1 &\equiv M_1 q_2 \left(q_2^{-1} \bmod q_1\right) (\mathrm{mod} m) \\ S_2 &\equiv M_2 q_1 \left(q_1^{-1} \bmod q_2\right) (\mathrm{mod} m) \end{aligned} \tag{44}$$

を求め，署名文 S を

$$S = S_1 + S_2 \tag{45}$$

と定める．このとき

$$M \equiv S_1 + S_2 = S(\mathrm{mod} m) \tag{46}$$

を満たす．もし，

$$M \equiv S(\mathrm{mod} n) \tag{47}$$

となる場合には，素数 $q_i(i=1,2)$ を選び直し，

$$M \not\equiv S(\mathrm{mod} n) \tag{48}$$

となる q_i を求め，文書 M と式 (48) を満たす署名文 S を送る．

4.3 署 名 検 証

公開鍵 a, n と送られてきた M, S を用いて

$$a^M \equiv a^S(\mathrm{mod} n) \tag{49}$$

が成立するかどうかを確かめ，成立するときは署名文 S は正しいと認証する．

簡単な数値例を次に示す．

（例 2） $q_1 = 83, q_2 = 89, p_1 = 167, p_2 = 179$ とすると，$m = 7387, n = 29893$ となり，$q_1^{-1} = 74(\mathrm{mod} q_2), q_2^{-1} = 14(\mathrm{mod} q_1), p_1^{-1} = 164(\mathrm{mod} p_2), p_2^{-1} = 14(\mathrm{mod} p_1)$ となる．法 p_i に対する 1 の原始 q_i 乗根 $(i=1,2)$ を，各々，$a_1 = 2, a_2 = 3$ と定めると，公開鍵 a は $a = 27390$ となる．公開鍵は a と n である．文書 M が $M = 2345$ のとき，$M_1 \equiv 21(\mathrm{mod} q_1), M_2 \equiv 31(\mathrm{mod} q_2)$ となり，$S_1 = 4005, S_2 = 5727$ より，署名文 S は $S = 9732$ と求まる．この M と S を送る．署名検証を行うと $a^M \equiv 9986(\mathrm{mod} n), a^S \equiv 9986(\mathrm{mod} n)$ となり，署名文 S は正しいことが確認される．

4.4 署名文の偽造困難性

法 $n = p_1 p_2$ の素因数分解は難しいと仮定しているので，この n から式 (39) の関係を満たす素数 q_1 と q_2 を求めることは難しい．従って，それらの積 $m = q_1 q_2$ を n から求めることは難しく，文書 M から式 (46) の関係を満たす署名文 S を求めることは計算量的に困難である．すなわち，式 (46) には S と m の 2 つの未知数があるため文書 M に対する署名文 S の偽造を行うことは困難である．

5. む す び

合成数を法とする離散対数問題に落し戸を作り，これを公開鍵暗号に応用した．一般に，合成数を法として位数の大きい元を底とする離散対数問題を解くことは難しいが，Fermat の小定理を用いて小さい位数と大きい位数に関係を与え，両者の積を位数とする元を底に定めた離散対数問題は高速に解くことができる．位数の小さい元 a_i のみを用いて離散対数

の底である公開鍵 a を定めると，a を a_i の位数乗することにより秘密鍵 p_i が求まり，暗号が解読される問題が生じる．この問題を避けるために，本文では，小さな位数 $q_i^{e_i}$ の元 a_i と大きな位数 $k_iq_i^{e_i}+1$ の元 b_i を用いて，両者の積 $q_i^{e_i}(k_iq_i^{e_i}+1)$ を位数とする元 a_ib_i に対する離散対数問題を扱った．公開する法 n の素因数 p_i と元 b_i の位数 $k_iq_i^{e_i}+1$ を知っている場合には，合成数 n を法とする離散対数問題を高速に解くことができるため，合成数を法とする離散対数問題を公開鍵暗号に用いることができる．

離散対数問題を公開鍵暗号に応用する場合には，復号するときに離散対数の計算が必要になるが，これをディジタル署名に応用して署名文を作る場合には離散対数の計算を必要としないため，素数 p_i として $p_i=2q_i+1$（q_i ：素数）を満たす Sophie Germain 素数を用いることもできる．ただ，Sophie Germain 素数を用いた場合でも，本署名における文書 M のとり得る範囲は公開鍵 n の $\frac{1}{4}$ 以下に制限され，文書と署名文との比で定めた伝送効率は $\frac{1}{4}$ 以下と低くなる．

同様に，本暗号における平文 x のとり得る範囲 m と公開鍵 n との比，つまり，平文と暗号文とのレートは $\frac{m}{n}$ と非常に小さく，これを改善することが一つの課題である．

文　献

[1] T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inf. Theory, IT-31, 4, pp.469–472, 1985.

[2] N.Koblitz, "Elliptic Curve Cryptosystems," Math. Comp., 48, 177, pp.203–209, 1987.

[3] V.S.Miller, "Use of Elliptic Curves in Cryptography," Proc.of Crypto'85, LNCS 218, Springer-Verlag, pp.417–426, 1985.

[4] 村上恭通, 笠原正雄, "合成数を法とする離散対数問題," 信学論 (A) , Vol.J76-A, No.4, pp.649–655, 1993.

[5] S.Uchiyama and T.Okamoto, "A New Public-Key Cryptosystems as Secure as Factoring," Technical Report of IEICE, ISEC97-55, pp.25–31, 1997.

[6] S.C.Pohlig and M.E.Hellman, "An improved for computing logarithms over GF(p) and its cryptographic significance," IEEE Trans. Inf. Theory,, IT-24,pp.106–110, 1978.

[7] 池野信一, 小山謙二, "現代暗号理論," 電子情報通信学会, 1986.

[8] D.R.Stinson 著, 櫻井幸一監訳, "暗号理論の基礎," 共立出版, 1996.

[9] 岡本龍明, 山本博資, "現代暗号," 産業図書, 1997.

[10] 小林邦勝, "合成数を法とする離散対数問題を用いた公開鍵暗号," 信学技報, ISEC98-79, pp.55–59, March, 1999.

[11] 岡本龍明, 藤崎英一郎, 内山成憲, 森田光, "公開鍵暗号「ＥＰＯＣ」および「ＰＳＥＣ」," 信学技報, ISEC2000-9, pp.141–155, May, 2000.