素因数分解問題に基づく公開鍵暗号系

八木沢 正博†

素因数分解問題に基づく落とし戸一方向関数を利用した公開鍵暗号系の具体的な実現方法を提案する．本方法では演算量が極めて少なくなる．また，平文の範囲を拡張することにより，任意の暗号文 $0 \leq w < n$ に対応する平文が存在し，ディジタル署名が可能となる．系の構成は，次のようになる．十分に大きな素数 p, q から成る $n = pq$ を法とする有限環上で，整数 a, b を係数，w を暗号文，$0 \leq x, y, z \leq R$ を平文とする暗号化式 $w = x + ay + bz \pmod{n}$ を構築する．ここで，$o(p) = o(q^2)$, $a = e^{-1}c \pmod{n}$, $b = e^{-1}d \pmod{n}$, $c = c_1k_1q + c_2k_2p \pmod{n}$, $d = d_1k_1q + d_2k_2p \pmod{n}$, $e = e_1k_1q + e_2k_2p \pmod{n}$, $1 = k_1q + k_2p \pmod{n}$, $R(e_1 + c_1 + d_1) < p$, $R < d_1$, $o(c_1) = o(e_1) = o(q^{0.9})$, $o(d_1) = o(q)$, $d_1c_2 - c_1d_2 \pmod{q} = 0$.「係数 a, b が与えられたとき，n の素因数分解に必要な計算量と，本暗号を解読する困難さとは等価である」ことを示すことができる．

A Public-key Cryptosystem Based on Prime Factorization Problem

MASAHIRO YAGISAWA†

This paper presents a public-key cryptosystem based on prime factorization problem. This system requires only $o(10)$ operations in ciphering and deciphering. Deciphering this cryptosystem has complexity as great as that required for factoring $n = pq$ on condition that the value of coefficients a, b mentioned below is given. The cryptosystem is constructed as follows. With large primes p, q, $o(p) = o(q^2)$, we get a cipher-text w such that $w = x + ay + bz \pmod{n}$ where $n = pq$, $a = e^{-1}c \pmod{n}$, $b = e^{-1}d \pmod{n}$, $c = c_1k_1q + c_2k_2p \pmod{n}$, $d = d_1k_1q + d_2k_2p \pmod{n}$, $e = e_1k_1q + e_2k_2p \pmod{n}$, $1 = k_1q + k_2p \pmod{n}$, $o(c_1) = o(e_1) = o(q^{0.9})$, $o(d_1) = o(q)$, $d_1c_2 - c_1d_2 \pmod{q} = 0$. x, y and z are plain-texts, and $0 \leq x, y, z \leq R$, $R(e_1 + c_1 + d_1) < p$, $R < d_1$. Deciphering operations are as follows. From $w_1 = e_1w \pmod{p} = e_1x + c_1y + d_1z \pmod{p}$, and $0 \leq e_1x + c_1y + d_1z < p$, we obtain $e_1x + c_1y + d_1z = w_1$. So $x = (w_1c_2 - e_2wc_1)(e_1c_2 - e_2c_1)^{-1} \pmod{q}$, and we obtain $y = (w_1 - e_1x)c_1^{-1} \pmod{d_1}$, $z = (w_1 - e_1x - c_1y)/d_1$.

1. はじめに

素因数分解問題に基づく落とし戸一方向関数[1]を利用した公開鍵暗号系の具体的な実現方法を提案する．本方法では演算量が極めて少なくなる．本論文の構成は，次のようになる．2章で，今回採用する落とし戸一方向関数を説明し，具体的に構築する方法について述べる．3章でこの落とし戸一方向関数を用いた公開鍵暗号系を構築し，4章で本暗号系の解読法と素因数分解問題の解法が計算量の上で同程度の困難度を有するか否かを論議する．5章でディジタル署名が可能であることを述べる．6章では，今後の課題について述べる．

† 昭和エンジニアリング（株）
Showa Engineering Corporation

2. 落とし戸一方向関数の構築

p, q を二つの十分に大きい素数，a, b を整数係数，w を暗号文，(x, y, z) を平文とした暗号化式

$$w = x + ay + bz \pmod{n} \tag{1a}$$

$$n = pq \tag{1b}$$

$$o(p) = o(q^2) \tag{1c}$$

$$o(a) = o(b) = o(n) \tag{1d}$$

を考える．ここで，モジュラ演算（$Y = X \pmod{M}$）を施した結果 Y は，$0 \leq Y < M$ の範囲をとることと定義する．(x, y, z) から w を計算するのは容易であるが，w が与えられたとき，(x, y, z) を求めるのは，n の素因数 p, q を知らないかぎり，適当なアルゴリズムがないため，計算量の上から困難であると思われる．これが，本論文で採用しようとしている一方向関数である．合成数 n が，$n = pq$ と素因数分解さ

れること，および係数 a，b 等が以下のように与えられることを落とし戸として，復号化アルゴリズムを構築する．

係数 a，b は次のような c，d と e から与えられる．

$$a = e^{-1}c \pmod n \tag{2a}$$
$$b = e^{-1}d \pmod n \tag{2b}$$
$$c = c_1k_1q + c_2k_2p \pmod n \tag{2c}$$
$$d = d_1k_1q + d_2k_2p \pmod n \tag{2d}$$
$$e = e_1k_1q + e_2k_2p \pmod n \tag{2e}$$
$$l = k_1q + k_2p \pmod n \tag{2f}$$

このとき，各パラメータの大きさは，

$$o(e_1) = o(c_1) = o(q^{0.9}) \tag{2g}$$
$$o(d_1) = o(c_2) = o(d_2) = o(q) \tag{2h}$$

さらに，

$$d_1 \text{ は素数} \tag{2i}$$
$$gcd(e_1c_2 - e_2c_1,\ q) = 1 \tag{2j}$$
$$d_1c_2 - c_1d_2 \pmod q = 0 \tag{2k}$$

を満たす．x，y，z 等は，

$$0 \le x, y, z \le R \tag{2l}$$
$$R(e_1 + c_1 + d_1) < p \tag{2m}$$
$$R < d_1, \quad R < q \tag{2n}$$

を満たす．

（復号化手順） (1a) の両辺に e_1 をかけると，

$$e_1w \equiv e_1x + e_1ay + e_1bz \pmod n \tag{3}$$

この両辺に mod p を施すと，(2a)〜(2e) より，

$$w_1 = e_1w \pmod p$$
$$= e_1x + c_1y + d_1z \pmod p \tag{4}$$

(2l)，(2m) より，

$$w_1 = e_1x + c_1y + d_1z \tag{5}$$

が得られる．このとき，

$$R^3 < R^2(e_1 + c_1 + d_1) < pq = n \tag{6}$$

が成立している．

（(5) 式 $\times e_1a -$ (3) 式 $\times c_1$）を作り，mod q を施すと

$$w_1e_1a - e_1wc_1 \equiv (e_1a - c_1)e_1x + e_1e_2^{-1}(d_1c - c_1d)z \pmod q \tag{7}$$

を得る．ここで，(2k) より，

$$d_1c - c_1d \pmod q$$
$$= d_1c_2 - c_1d_2 \pmod q = 0 \tag{8}$$

だから，(2j) 式に注意して，

$$x = (w_1c_2 - e_2wc_1)(e_1c_2 - e_2c_1)^{-1} \pmod q \tag{9}$$

(5) 式に x を代入して，mod d_1 を施すと，

$$y = (w_1 - e_1x)c_1^{-1} \pmod{d_1} \tag{10}$$

(9) 式，(10) 式を (5) 式に代入して，

$$z = (w_1 - e_1x - c_1y)/d_1 \tag{11}$$

が得られる．（復号化手順 終わり）

つまり，n の素因数 p，q を知るものは上記の落とし戸を利用できるので復号化が可能となる．また，任意の暗号文 w に対して，平文 (x, y, z) が一意に復号化されることが容易に示せる．

暗号文 w に対して，二つの平文 (x, y, z)，(x', y', z') が対応すると仮定すると，

$$w = x + ay + bz \pmod n \cdots\cdots ①$$
$$w = x' + ay' + bz' \pmod n \cdots\cdots ②$$

$(① - ②) \times e_1 \pmod p$ を計算すると，

$$0 = e_1(x - x') + c_1(y - y') + d_1(z - z') \pmod p \cdots\cdots ③$$

$-R \le (x - x'), (y - y'), (z - z') \le R$ だから，(2m) より $-p <$（③の右辺）$< p$ となり，

$$0 = e_1(x - x') + c_1(y - y') + d_1(z - z') \cdots ④$$

が得られる．④ に (7) 式から (9) 式と同様な復号化手順を施すと，

$$x - x' = 0 \pmod q \cdots\cdots ⑤$$

$0 \le x,\ x' \le R$ より $-q < -R \le x - x' \le R < q$ だから，

$$x - x' = 0 \cdots\cdots ⑥$$

$y - y'$ も同様にして，

$$y - y' = 0 \cdots\cdots ⑦$$

よって，

$z - z' = 0$ つまり $(x, y, z) = (x', y', z')$ となる．

3. 公開鍵暗号系の構築

2 章の落とし戸一方向関数を用いて，公開鍵暗号系を構築する．変数，係数の定義は 2 章に同じとする．a，b を整数係数，w を暗号文，(x, y, z) を平文とした暗号化式

$$w = x + ay + bz \pmod n \tag{12a}$$
$$0 \le x, y, z \le R \tag{12b}$$

を考える．

パラメータのサイズとして，次のサイズを推奨する．

$$o(q) = 10^{150} \tag{13a}$$
$$o(p) = 10^{300} \tag{13b}$$
$$o(a) = o(b) = o(n) = 10^{450} \tag{13c}$$
$$o(d_1) = 10^{150} - 3 \cdot 10^{135} \tag{13d}$$
$$o(c_2) = o(d_2) = 10^{150} \tag{13e}$$
$$o(R) = 10^{150} \tag{13f}$$
$$o(c_1) = o(e_1) = 10^{135} \tag{13g}$$
$$R(e_1 + c_1 + d_1) < p \tag{13h}$$

「1994 年，Rivest らが懸賞問題とした 129 桁の整

数の64桁，65桁の素数をLenstraが読み解いた[11)]」との報告があることから q のサイズとして上記を選んだ．

公開する暗号化鍵（公開鍵）K_E は，次のようである．

$$K_E = [a, b, n, R] \tag{14}$$

［暗号化］ 公開されている a，b，n と平文 (x, y, z) から

$$w = x + ay + bz \pmod{n} \tag{15}$$

を計算し，暗号文 w を送信する．

これに要する計算量は，2個の乗算と2個の加算のみである．K_E が必要とする容量は約5kbitとなる．

ここで，$X = (x, y, z)$，$w = E(X)$ とおくと E は一方向関数である．つまり，X から w を計算することは極めて容易であるが，w から X を求めることは，計算量の上からみて非常に困難である．

［復号化］ 正規の受信者が w を受信すると，

$$w = x + ay + bz \pmod{n} \tag{16}$$

および，a，b 等が(2a)～(2n)式で与えられていることから，

$$\begin{aligned} w_1 &= e_1 w \pmod{p} \\ &= e_1 x + c_1 y + d_1 z \pmod{p} \end{aligned} \tag{17}$$

が得られ，以下，2章で述べた（復号化手順）により，x，y，z を求める．復号化鍵（秘密鍵）K_D は，

$$K_D = [p, q, e_1] \tag{18}$$

である．

復号化に必要な計算量は，乗除算11個，加減算3個，(13a)～(13h)式のパラメータを採用すると，K_D が必要とする容量は約2kbitである．

本暗号方式と他の代表的な方式（RSA暗号[2)]，Rabin暗号[9)]，Williams暗号[10)]，逆数暗号[3)]）と比較し，$m =$（平文のビット長）として，暗号化・復号化に必要な計算量を順に示すと，

本暗号 $o(m^2), o(m^2)$; RSA $o(m^3), o(m^3)$
Rabin $o(m^2), o(m^3)$; Williams $o(m^2), o(m^3)$
逆数 $o(m^2), o(m^3)$

となり，本暗号方式の計算量が少ないことが分かる．本暗号系の理解を深めるために簡単な数値例を示す．

$p = 12345678901234567891$，$q = 3514560899$
$n = pq = 43389640337888295136869494009$
$k_1 = 6269978530800504231$，$k_2 = 1729626951$
$d_1 = 3514209481$（素数），$d_2 = 3415890089$
$c_1 = 389197037$，$c_2 = 3476745377$
$e_1 = 390097037$，$e_2 = 3314560727$

と選ぶ．このとき

$$d_1 c_2 - c_1 d_2 \pmod{q} = 0$$

となっている．

$$\begin{aligned} c &= c_1 k_1 q + c_2 k_2 p \pmod{n} \\ &= 309837621779362613203826703 06 \\ d &= d_1 k_1 q + d_2 k_2 p \pmod{n} \\ &= 375362731189636623497035364 6 \\ e &= e_1 k_1 q + e_2 k_2 p \pmod{n} \\ &= 216791822740231602328425083 5 \\ a &= e^{-1} c \pmod{n} \\ &= 169950449015255417864257860 31 \\ b &= e^{-1} d \pmod{n} \\ &= 272198324694673660311173526 10 \end{aligned}$$

$0 \le x, y, z \le R = 2840290229 < d_1$
$w = x + ay + bz \pmod{n}$

この係数 a，b を R，n とともに公開する．

① ケース1

［暗号化］

$x = 1111111111$，$y = 2222222222$，$z = 2333333333$ のとき

$$\begin{aligned} w &= x + ay + bz \pmod{n} \\ &= 260131463029125499248924419 43 \end{aligned}$$

となる．

［復号化］

$$\begin{aligned} w_1 &= e_1 w \pmod{p} = 9498145577698764494 \\ x &= (w_1 c_2 - e_2 w c_1)(e_1 c_2 - e_2 c_1)^{-1} \pmod{q} \\ &= 1111111111 \\ y &= (w_1 - e_1 x) c_1^{-1} \pmod{d_1} \\ &= 2222222222 \\ z &= (w_1 - e_1 x - c_1 y)/d_1 = 2333333333 \end{aligned}$$

が得られる．

② ケース2

$w = 111111111111111111111111111111$ が与えられたとき

［復号化］

$$\begin{aligned} w_1 &= e_1 w \pmod{p} \\ &= 5297847579279651159 \end{aligned}$$

$x = 3201122198$，$y = 2138544653$，
$z = 915364912$

検算すると，

$$\begin{aligned} x + ay + bz &\pmod{n} \\ &= 111111111111111111111111111111 = w \end{aligned}$$

（数値例終わり）

$x > R$ となっているが，このように x，y，z の範囲を拡大することにより，任意の暗号文に平文を対応させることができる．詳細は5章参照．

4. 安 全 性

n の素因数 p, qを求めることを考えると，p, qは，

$$o(p)=10^{300},\ o(q)=10^{150},\ o(n)=10^{450} \tag{19}$$

の大きさであるため，素因数分解に要する時間は，$k\fallingdotseq 1$ として，

$$o\left(\exp\left(k(\log n\log\log n)^{1/2}\right)\right)=6.87\times 10^{36} \tag{20}$$

であり，容易には分解できない．ただし，本方法では，p, q の大きさが (19) で与えられているので，計算時間は (20) より，小さくなる可能性があるが，

$$o\left(\exp\left(k(\log q\log\log q)^{1/2}\right)\right)=3.26\times 10^{19} \tag{21}$$

以上の大きさと思われる．定数 c, d は，

$$c \pmod p = c_1,\ o(c_1)=o(q^{0.9})=o(n^{0.3})$$
$$d \pmod p = d_1,\ o(d_1)=o(q)=o(n^{1/3})$$

であり，n に関連した特異性をもつが，係数 a, b は

$$\begin{aligned} a &= e^{-1}c \pmod n \\ &= (e^{-1}c_1 \pmod p)k_1q \\ &\quad +(e^{-1}c_2 \pmod q)k_2p \pmod n \end{aligned}$$

等，少なくとも，$o(a \pmod p)=o(p)=(n^{2/3})$ の大きさに関しては，c, d のような特異性はない．また，c, d には (2k) 式で与えられる制約があるが，「係数 a, b が与えられたとき，n の素因数 p, q を求める計算量を PAL（n; a, b）とおくと，本暗号系の暗号解読と PAL（n; a, b）の困難さが等価である」ことを示すことができる．

その前に，次の lemma 1 を証明する．

［Lemma 1］ $q\le A<p/e_1$ なる任意の暗号文 A に対応する平文を (x,y,z) とすると，$(A-x)$ は q の倍数である．

（証明）

$q\le A<p/e_1$ ……①

の範囲の任意の暗号文 A に対応する平文 (x,y,z) を復号化アルゴリズムを用いて求める．

$A=x+ay+bz \pmod n$ ……②

この両辺に e_1 をかけて，

$e_1A=e_1x+e_1ay+e_1bz \pmod n$ ……③

$$\begin{aligned} w_1 &= e_1A \pmod p = e_1A \\ &= e_1x+c_1y+d_1z \cdots ④ \end{aligned}$$

(③ $\times c_1$ − ④ $\times e_1a$) を求め，mod q を施すと，

$$\begin{aligned} & e_1bc_1-d_1e_1a \\ &\equiv e_1e_2^{-1}(d_2c_1-d_1c_2) \pmod q = 0 \end{aligned}$$

に注意して，

$$\begin{aligned} & e_1Ac_1-e_1Ae_1a\equiv e_1A(c_1-e_1a) \\ &\equiv e_1(c_1-e_1a)x \pmod q \cdots ⑤ \end{aligned}$$

(2j) 式より，$gcd(c_1-e_1a,\ q)=1$ だから，変形して，

$x=A \pmod q$ ……⑥

$y=e_1(A-x)\cdot c_1^{-1} \pmod{d_1}$ ……⑦

$z=(w_1-e_1x-c_1y)/d_1$ ……⑧

また，

$A\ge q$ つまり，$A-x\neq 0$ ……⑨

ここで，⑨と⑥より，

$gcd(A-x,\ n)=q$ ……⑩

つまり，$(A-x)$ は 0 でない q の倍数となる．

（証明終わり）

［定理 1］

暗号化式

$w=x+ay+bz \pmod n$ ……①

において，任意の一つの暗号文に対応する平文 (x,y,z) を求めるアルゴリズムを AL とする．平文が存在するときはいつでもこのアルゴリズム AL の計算量は $F(n)$ であるとする．このとき，「係数 a, b が与えられたとき，n を素因数分解するアルゴリズムの計算量 PAL（n; a, b）」は $(12/5)F(n)+\log_2 n$ 以下である．

（証明）

$0\le x_0,\ y_0,\ z_0\le R$ の範囲の任意の平文 (x_0,y_0,z_0) を選び，対応する暗号文を w_0 として，

$w_0=x_0+ay_0+bz_0 \pmod n$ ……②

次に，

$q\le|m|<p/e_1-R$ ……③

の範囲の整数 m を任意に選ぶ．しかし，q, p は公開されていないので，

$o(n^{1/3})<|m|<o(n^{0.366})-R$ ……④

の範囲の値を選ぶ．暗号文 w_0+m に対する平文 (x,y,z) を AL により求める．平文集合の位数は $R^3\fallingdotseq n$ であり，暗号文 w の定義域は $[0,n)$ であるから，任意の暗号文に対する平文の存在する確率は，ほぼ 1 である．暗号文 w_0+m に対する平文 (x,y,z) が存在すると，

$w_0+m\equiv x+ay+bz \pmod n$ ……⑤

⑤から②の辺々を引いて，

$$\begin{aligned} m &\equiv (x-x_0)+a(y-y_0)+b(z-z_0) \\ &\pmod n \cdots ⑥ \end{aligned}$$

となるが，このとき，Lemma 1 を適用するために，$(y-y_0)$, $(z-z_0)$ と m の符号が一致するように m を選ぶ．つまり，y, z の値は 0 から R の範囲

をランダムにとるから，$(y_0+z_0)/R>1$ のとき，$o(n^{1/3})<-m<o(n^{0.366})-R$，$(y_0+z_0)/R\leq 1$ のとき，$o(n^{1/3})<m<o(n^{0.366})-R$ と m を選ぶことにより，$(y-y_0)$，$(z-z_0)$ と m の符号が一致する確率 Pr は平均すると 5/12 になる．なぜなら，$g=y/R$，$h=z/R$ とおき，g，h は $0\leq g$，$h\leq 1$ の範囲の連続した値をとると仮定して，Pr は，

$$Pr=\int_0^1 dg\left\{\int_0^{1-g}(1-g)(1-h)dh+\int_{1-g}^1(gh)dh\right\}=5/12$$

で与えられる．Lemma 1 が適用できると，

$$gcd(m-(x-x_0),\ n)=q\cdots\cdots\cdots\cdots\cdots\textcircled{7}$$

から，n が素因数分解される．⑦の最大公約数の計算量は高々 $\log_2 n$ である．したがって，平均的な計算量は $(12/5)F(n)+log_2 n$ 以下である．（証明終わり）

本暗号系では，暗号文 w の値が p/e_1 より小さく q 以上の場合は，暗号文 w と平文 x の差 $(w-x)$ が q の倍数となるため n が素因数分解されるという欠点をもつ．が，暗号文が q 以上 p/e_1 以下の範囲に入る確率はおおよそ $p/(e_1 n)\fallingdotseq 10^{-285}$ と非常に小さい．黒沢等の逆数暗号[3]においては，平文 M と法 n が $gcd(M,n)=p$ or q であれば p，q がわかってしまうが，本方法では，その欠点はないといえる．その理由として，逆数暗号では平文から暗号文を求める過程で，逆数を求める必要があり，このとき逆数が存在せず共通因数である p または q が必然的に求まるが，本暗号系では，$x+ay+bz \pmod n$ を計算するだけであるから，その恐れはないといえる．

5. ディジタル署名[4]

暗号文 w，平文 $M=(x,y,z)$ として，2 章の暗号化 E，復号化 D の順序を交換できる本暗号系では秘匿の機能を備えたディジタル署名が可能である．

本暗号系で，平文集合を拡張することにより，

$$E(D(w))=w \tag{22}$$

が成立することを示す．暗号文集合 C，平文集合 H を

$$C=\{w|\ 0\leq w<n-1\} \tag{23}$$

$$H=\{(x,y,z)|\ 0\leq x,y,z\leq R\} \tag{24}$$

と表す．(6) 式より，$R^3<n$ だから，w と (x,y,z) は一対一対応していないが，(x,y,z) の範囲を，

$$H'=\{(x,y,z)|\ 0\leq x\leq q-1,\ 0\leq y\leq d_1-1,\ z\min\leq z\leq z\max\} \tag{25}$$

$$z\min=[(-(q-1)e_1-c_1(d_1-1))/d_1] \tag{26}$$

$$z\max=[(p-1)/d_1] \tag{27}$$

ここで，$[\cdot]$ は・を越えない最大整数を表す，と拡張することにより，

$$q\cdot d_1\cdot[(p+(q-1)e_1+c_1(d_1-1))/d_1]>n \tag{28}$$

となり，C 内の任意の w に対応する (x,y,z) が存在しうる．

なぜなら，2 章の復号化手順を考慮すれば，(x,y,z) が存在することは容易に分かる．つまり，(x,y,z) の範囲を H' に拡張することにより，任意の w に対応する $D(w)$ が存在する．

［定理 2］

任意の $w\in C$ に対して，$E(D(w))=w$ が成立する．

（証明）

$$D(w)=(x,y,z)\cdots\cdots\cdots\cdots\cdots\cdots\textcircled{1}$$

とおくと，(x,y,z) は復号化アルゴリズムから次のようにして与えられる．

$$w_1=e_1 w \pmod p\cdots\cdots\cdots\cdots\cdots\textcircled{2}$$

$$x=(w_1c_2-e_2wc_1)(e_1c_2-e_2c_1)^{-1} \pmod q\cdots\cdots\textcircled{3}$$

$$y=(w_1-e_1x)c_1^{-1} \pmod{d_1}\cdots\cdots\cdots\cdots\textcircled{4}$$

$$z=(w_1-e_1x-c_1y)/d_1\cdots\cdots\cdots\cdots\cdots\textcircled{5}$$

で与えられる．この (x,y,z) に 2 章の暗号化アルゴリズムを施す．

$$w_1=e_1x+c_1y+d_1z\cdots\cdots\cdots\cdots\cdots\textcircled{6}$$

だから，$B=x+ay+bz$ とおいて，

$$\begin{aligned}B &\pmod p\\ &=e_1^{-1}(e_1B) \pmod p\\ &=e_1^{-1}(e_1x+c_1y+d_1z) \pmod p\\ &=e_1^{-1}w_1 \pmod p=w \pmod p\cdots\cdots\textcircled{7}\end{aligned}$$

つぎに，

$$\begin{aligned}B &\pmod q\\ &=e^{-1}(ex+c_2y+d_2z) \pmod q\\ &=e_2^{-1}c_1^{-1}(c_1e_2x+c_2(c_1y)+c_1d_2z) \pmod q\end{aligned}$$

⑥より，

$$\begin{aligned}&=e_2^{-1}c_1^{-1}(c_1e_2x+c_2(w_1-e_1x-d_1z)+c_1d_2z) \pmod q\\ &=e_2^{-1}c_1^{-1}((c_1e_2-c_2e_1)x+c_2w_1+(-c_2d_1+c_1d_2)z) \pmod q\end{aligned}$$

$c_2d_1-d_2c_1 \pmod q=0$ だから，

$$=e_2^{-1}c_1^{-1}((c_1e_2-c_2e_1)x+c_2w_1) \pmod q$$

③より，$(c_1e_2-c_2e_1)x\equiv -w_1c_2+e_2wc_1 \pmod q$ だから

$$\begin{aligned}&=e_2^{-1}c_1^{-1}(-w_1c_2+e_2wc_1+c_2w_1) \pmod q\\ &=e_2^{-1}c_1^{-1}(e_2wc_1) \pmod q\end{aligned}$$

$\equiv w \pmod{q}$ ……⑧

したがって，⑦，⑧から，

$B = w \pmod{n}$

となる．つまり，$E(D(w)) = w$ が成立している．

（証明終わり）

本署名法では署名文に相当するのは，$D(w) = (x, y, z)$ である．

また，本方法は，暗号化・復号化の計算量が極めて少ないことから，高速署名方式ESIGN[5),6)] に比較して，より高速な署名法といえる．

6. 終わりに

素因数分解問題に基づく公開鍵暗号系を提案した．本暗号系が必要とする計算量は，暗号化・復号化ともに極めて小さいことが特徴である．計算量について，本暗号系の解読と素因数分解の同等性に関して議論することができた．今後は，PAL(n; a, b) と「係数 a, b が与えられていないとき，n を素因数分解するのに必要な計算量PAL(n)」とに差があるか否かを見極めたい．また，PAL(n; a, b) の計算量が小さい場合，係数 a, b の特異性，つまり $a \pmod{p}$, $b \pmod{p} \ll p$ であることを利用して n を素因数分解する新たなアルゴリズムの発見につながる可能性を秘めている．今後は本暗号系を用いて，ゼロ知識対話証明[7)] やマルチパーティプロトコル[8)] を実現する手法を確立していきたい．

参考文献

1) 渡辺　治：一方向関数のお話，情報処理，Vol.32, No.6, pp.704–713 (1991).
2) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
3) 黒沢，伊東，竹内：素因数分解の困難さと同等の強さを有する逆数を利用した公開鍵暗号，信学論，Vol.J70-A, No.11, pp.1632–1636 (1987).
4) 辻井，笠原：暗号と情報セキュリティ，p.132，昭晃堂，東京 (1990).
5) Okamoto, T.: A Fast Signature Scheme Based on Congruential Polynomial Operations, *IEEE Transaction on Information Theory*, Vol.IT-36, No.1, pp.47–53 (1990).
6) Fujioka, A., Okamoto, T. and Miyaguchi, S.:ESIGN: An Efficient Digital Signature Implementation on Smart Card, in Advances in Cryptology-EURO-CRYPT'91, Lecture Notes in Computer Science 547, pp.446–457, Springer-Verlag (1991).
7) 小山謙二：ゼロ知識対話証明の原理と課題，情報処理，Vol.32, No.6, pp.643–653 (1991).
8) 黒沢　馨，岡本龍明：ゼロ知識証明とマルチパーティプロトコル，情報処理，Vol.32, No.6, pp.663–672 (1991).
9) Rabin, M.O.: Digitalized Signatures and Public-Key Functions as Instractable as Factorization, Technical Report, LOS/TR-212 (1979).
10) Williams, H.C.: A Modification of the RSA Public Key Encryption Procedure, *IEEE Trans.*, IT-26, No.6, pp.726–729 (1980).
11) 太田，黒沢，渡辺：情報セキュリティの科学，p.141，講談社，東京 (1995).

(平成7年1月24日受付)
(平成7年7月 7 日採録)

八木沢正博（正会員）

昭和25年生．昭和49年東京大学工学部計数工学科卒業．昭和51年同大学院修士課程修了．同年昭和電工（株）入社，川崎工場勤務．昭和61年昭和エンジニアリング（株）に出向，現在に至る．化学プラントの計装エンジニアとして，プラントの設計，保全に従事．現在，素因数分解問題に興味を持つ．