マルチメディア通信と分散処理 30－6
（1986. 7. 25）

有理関数の順序解法による公開鍵暗号方式

辻井重男* 松本 勉** 黒沢 馨* 伊東利哉* 藤岡 淳*

* 東京工業大学 ** 横浜国立大学

情報化社会の到来により、物理的に転送されていたデータ等が、回線上を伝送されることになり、秘密保持に対する要求が高まってくる。このネットワーク・セキュリティにおいて、中心的役割を担うのが暗号である。本稿では、非線形連立方程式の順序解法に基づく公開鍵暗号方式を提案する。本暗号系は、①暗号化、及び、復号化の計算量は、平文長の2乗に比例する。②ディジタル署名が可能である、等の利点を有する。また、本方式においては、公開鍵は有理関数で記述される。まず、有理関数を導入した非線形連立方程式の順序解法を利用する公開鍵暗号方式を提案し、それに対する解読法について考察を行い、信頼性を保証するための本暗号系の満たすべき条件を導出する。最後に、暗号化・復号化計算量、公開鍵・秘密鍵記述量、及び、ディジタル署名について考察する。

A Public-Key Cryptosystem based on the Difficulty of Solving a System of Nonlinear Simultaneous Equations

Shigeo TSUJII* Tsutomu MATSUMOTO** Kaoru KUROSAWA* Toshiya ITOH* Atsushi FUJIOKA*

* Tokyo Institute of Technology ** Yokohoma National University

This paper propose a new public-key cryptosystem based on the difficulty of a system of non-linear equations. The proposed cryptosystem has the following features ;

1) The public-key is non-linear transform from plaintext to a ciphertext in the form of rational functions.
2) The complexity of both encryption and decryption is $O(m^2)$.
3) Digital signature is possible.

The trap-door of the cryptosystem is that the public-key is composed of linear and non-linear transforms from plaintext to ciphertext and the non-linear transform is chosen to be solved easily by receivers.

1．まえがき

公開鍵暗号方式[1]は、秘密通信において鍵の配送が不要であること、ディジタル署名[2]が可能であること等の優れた特徴を有する反面、従来の暗号方式、即ち、慣用鍵暗号方式に比べて、暗号化・復号化の計算量が大きく、高速伝送路を実時間で利用する場合に不利となる欠点をもっている。

現在、最も著名であり、また、信頼感を得ている公開鍵暗号方式は、ＲＳＡ方式[3]であると思われるが、暗号化、及び、復号化の計算量は、通常の計算法では平文長の３乗に比例する。

著者等は、先に暗号化、及び、復号化に要する計算量が平文長の２乗に比例する暗号系として、非線形連立方程式の順序解法による公開鍵暗号方式を提案している[4]，[5]。非線形連立方程式の順序解法とは、k変数$(x_1, x_2, \cdots, x_k)$の非線形連立方程式において、x_1がまず求められ、x_2はx_1が分かれば求められ、x_3はx_1とx_2が知られれば求められ、以下同様にx_kが求められるような解法を言う。

以下、本稿では、２．において、非線形連立方程式の順序解法について述べ、３．では、有理関数を用いた非線形連立方程式の順序解法による暗号方式を提案する。また、４．にて、その信頼性を検討し、５．では、本方式の処理量、及び、鍵記述量について、６．では、ディジタル署名について述べる。最後に７．において、まとめとして、本方式の諸特性を述べるとともに、今後の課題等について言及する。

2．非線形連立方程式の順序解法

簡単のために、平文ｘ、暗号文ｙが４次元ベクトルの場合について述べる。即ち、

$$x = (x_1, x_2, x_3, x_4)^T$$
$$y = (y_1, y_2, y_3, y_4)^T$$

で表す。但し、Ｔはベクトルの転置を示す。

今、関数$f_{ij}(x)$を要素とする上三角行列を、

$$F(x) = \begin{bmatrix} f_{11}(x_2, x_3, x_4) & f_{14}(x_2, x_3, x_4) & f_{14}(x_2, x_3, x_4) & f_{14}(x_2, x_3, x_4) \\ 0 & f_{22}(x_3, x_4) & f_{24}(x_3, x_4) & f_{24}(x_3, x_4) \\ 0 & 0 & f_{33}(x_4) & f_{34}(x_4) \\ 0 & 0 & 0 & f_{44} \end{bmatrix}$$

で定義する。

ここで、

$$y = F(x) \cdot x$$

のような非線形連立方程式を考えた場合に、第４行目の式

$$y_4 = f_{44} \cdot x_4$$

より、

$$\therefore \quad x_4 = \frac{1}{f_{44}} \cdot y_4$$

が求まり、つづいて、第３行目の式、

$$y_3 = f_{33}(x_4) \cdot x_3 + f_{34}(x_4) \cdot x_4$$

より、

$$\therefore\ x_3 = \frac{1}{f_{34}(x_4)}\ (y_3 - f_{34}(x_4)\cdot x_4)$$

というように、x_4より順次、x_3, x_2, x_1を容易に求めることができる。

3．順序解法を利用した暗号系

本章では、以下に示す形式の暗号系について考察する。

平文ベクトルは、暗号化・復号化計算量を考慮して、$GF(2^t)$上のk次元ベクトルとし、また、行列A，Bの要素、及び、F(v)の係数は、公開鍵・秘密鍵記述量を考慮して、$GF(2^s)$の元とする（但し、$GF(2^s)$は、$GF(2^t)$の部分体とする）。

このとき、暗号系は下のように構成される。

$$v = A\cdot x$$
$$w = F(v)\cdot v \qquad (*)$$
$$y = B\cdot w$$

但し、

$$F(v) = \begin{bmatrix} f_{11}(v) & f_{12}(v) & \cdots\cdots & f_{1k}(v) \\ 0 & f_{22}(v) & \cdots\cdots & f_{2k}(v) \\ 0 & 0 & \cdots\cdots & \\ 0 & 0 & \cdots\ 0 & f_{kk}(v) \end{bmatrix}$$

$$f_{ii}(v) = \frac{c_i v_i + d_i}{v_i(a_i v_i + b_i)} \qquad (i=1\sim k)$$

$$a_i, b_i, c_i, d_i \in GF(2^s)$$

$$f_{ij}(v) = \frac{\sum_{n=i+1}^{k} c^n_{ij} v_n + d_{ij}}{v_j\left(\sum_{n=i+1}^{k} a^n_{ij} v_n + b_{ij}\right)} \qquad \begin{matrix}(i=1\sim k)\\(j=i+1\sim k)\end{matrix}$$

$$a^n_{ij}, b_{ij}, c^n_{ij}, d_{ij} \in GF(2^s)$$

$$x = (x_1, x_2, \cdots, x_k)^T$$
$$v = (v_1, v_2, \cdots, v_k)^T$$
$$w = (w_1, w_2, \cdots, w_k)^T$$
$$y = (y_1, y_2, \cdots, y_k)^T$$

$$x_i, v_i, w_i, y_i \in GF(2^t)$$

とする。

ここで、行列F(v)の要素である有理関数の個数mは、F(v)が上三角行列であることから、

$$m = \frac{1}{2}k(k+1)$$

となる。これらの有理関数の線形結合をとり、変数をvによる表現からxによる関数に表現を変えたものが、公開鍵となる。

《公開鍵》

以上より、ベクトルyを、変数$x_1, \cdots, x_k$によって表現し、

$$y_1 = \sum_{i=1}^{m} \frac{g_{1i}(x_1, x_2, \cdots, x_k)}{g_{Di}(x_1, x_2, \cdots, x_k)}$$

$$y_2 = \sum_{i=1}^{n} \frac{g_{2i}(x_1, x_2, \cdots, x_k)}{g_{Di}(x_1, x_2, \cdots, x_k)}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_k = \sum_{i=1}^{n} \frac{g_{ki}(x_1, x_2, \cdots, x_k)}{g_{Di}(x_1, x_2, \cdots, x_k)}$$

を、公開鍵とする。

但し、

g_{ij}, g_{Di} : $x_1, x_2, \cdots, x_k$の１次式

とする。

ここで、公開鍵中の有理関数の個数は、nとなることに注意する。

《秘密鍵》

A，B、及び、F(v)を秘密鍵とする。

【暗号化】

平文xを公開鍵に代入し、暗号文yを得る。

【復号化】

まず、

$$w = B^{-1} \cdot y$$

を求め、これに対して順序解法を適用してvを得、最後に、

$$x = A^{-1} \cdot v$$

としてxを求める。

解読については、後に論ずるが、極めて困難にすることが可能であると考えられる。

本構造はObscure表現[6]によるアルゴリズム合成の典型である。

4．本方式の信頼性

4.1 攻撃法．1

本方式では行列F(v)中の非線形関数として有理関数を用いているが、これは、非線形性を多項式とした場合の暗号系については、解読が可能であることが指摘されている[5]ことによる。この解読法の方針は、行列F(v)の形状に着目して、秘密鍵であるA，Bを求めようとするものであり、例えば、順序解法を開始するためには、変数についての線形な式が必ず存在しなければならない、といった事実に基づいている。逆に、行列F(v)中の非線形関数を有理関数とすることにより、この解読法は適用できないこととなる。即ち、線形な式は存在せず、行列A，Bを定める手がかりが得られないことになる。

ところが、秘密鍵F(v)中の有理関数の分母を、すべて当てることによりこの解読法を応用しようとすることが考えられる。公開されている有理関数の分母は、秘密鍵F(v)の成分である有理関数の分母を、中間変数ベクトルvによる表現から、平文ベクトルxによる表現に変換したものである。これは、線形変換Aは、有理関数の変数をxからvへ変換するだけであり、また、線形変換Bは、有理関数の線形結合をとるだけであることより明らかである。

よって、F(v)のどの成分に、公開されているどの有理関数の分母が相当するかが、公開鍵よりすべて既知になってしまうと、暗号系を多項式により構成していることと同値になってしまい、先に述べた解読法が適用でき、信頼性が保証されないことになる（分母が既知になると、ある平文xを代入したときの分母の値は定数と見なしてよい）。

しかし、公開されている有理関数の分母が、上三角行列F(v)のどの成分の有理関数の分母となるかを、すべて一致させることをしらみ潰しにより考えてみると、その場合の数としては、有理関数の数mの階乗通りの組合せが存在する。これらの関係を表1に示す。

この結果より、kを6以上とすれば、場合の数は、5×10^{19} 以上になるので、しらみ潰しにより分母を当てようとすることは、事実上不可能になる。

表1 変数ベクトルの次元と場合の数

k	m	m !
4	10	4×10^{6}
5	15	1×10^{12}
6	21	5×10^{19}
7	28	3×10^{29}

4.2 攻撃法．2

続いては、岡本・中村による解読法[7]について考察してみる。この解読法は、暗号化の構造に着目して暗号文yから平文xへの変換を求めるものである。

3．の形式で公開鍵暗号系を構成すると、式(*)のk番目の成分から、

$$w_k = f_{kk}\cdot v_k = \frac{c_k v_k + d_k}{a_k v_k + b_k}$$

となり、これを、v_kについて解くと、

$$v_k = -\frac{b_k w_k - d_k}{a_k w_k - c_k}$$

となる。この式は分母・分子ともにw_kの1次式である。次に、式(*)のk－1番目の成分は、

$$w_{k-1} = f_{k-1\,k-1}\cdot v_{k-1} + f_{k-1\,k}\cdot v_k = \frac{c_{k-1} v_{k-1} + d_{k-1}}{a_{k-1} v_{k-1} + b_{k-1}} + \frac{c_{k-1}^{k-1}{}_{k} v_k + d_{k-1\,k}}{a_{k-1}^{k-1}{}_{k} v_k + b_{k-1\,k}}$$

となる。これを、v_{k-1}について解いてみると、w_{k-1}, v_kについての式となり、ここでv_kに先の式を代入すると、

$$v_{k-1} = \frac{N_{k-1}(w_{k-1}, w_k)}{D_{k-1}(w_{k-1}, w_k)}$$

を得る。ここで、$N_{k-1}(w_{k-1}, w_k)$、$D_{k-1}(w_{k-1}, w_k)$は、w_{k-1}, w_kの2次式である。以下同様に、v_iをwによって表現してみると、wについての有理関数となり分子多項式$N_i(w)$、及び、分母多項式$D_i(w)$の最高次数dv_iは

$$dv_i = 1 + (k-i)\sum_{j=1}^{k} dv_j$$

$$\therefore \quad (k-1-i)dv_i = (k-i)^2 dv_{i+1} - 1 \qquad (\text{但し、} dv_k = 1, dv_{k-1} = 2)$$

となる。

以上より、中間変数wから中間変数vへの変換となる有理関数を求めることが

できる。

次に、変数wによる表現の有理関数を変数yによる表現に変形したとしても、ベクトルwからベクトルyへの変換は線形変換のため、有理関数の最高次数に変化はない。

$$v_i = \frac{N_i(w)}{D_i(w)} = \frac{\hat{N}_i(y)}{\hat{D}_i(y)}$$

$$deg[N_i(w)] = deg[\hat{N}_i(y)] \quad deg[D_i(w)] = deg[\hat{D}_i(y)]$$

しかし、最終的に暗号文yから平文xへの有理関数を求めるためには、ベクトルvからベクトルxへの線形変換A^{-1}を経るために、v_iについての線形結合をとることが必要であり、結果として分母多項式$\hat{D}_i(y)$をすべてのiについて通分することとなる。

$$x = A^{-1}v$$

$$x_i = \sum_{j=1}^{k} \hat{a}_{ij} v_j = \sum_{j=1}^{k} \hat{a}_{ij} \frac{\hat{N}_j(y)}{\hat{D}_j(y)} = \frac{\tilde{N}_i(y)}{\tilde{D}_i(y)}$$

但し、

$$A^{-1} = (\hat{a}_{ij})$$

とする。

よって、$\tilde{N}_i(y)$, $\tilde{D}_i(y)$の最高次数dx_iは、

$$dx_i = \sum_{j=1}^{k} dv_j$$

となる。一般に、k変数d次多項式の項数tは、

$$t = \sum_{i=0}^{d} {}_{i+k-1}C_{k-1}$$

で表現できる。ここで、

$$\sum_{r=n}^{n} {}_rC_n = {}_{n+1}C_{n+1}$$

を用いれば、$\tilde{N}_i(y)$, $\tilde{D}_i(y)$の項の数tx_iは、それぞれ、

$$tx_i = {}_{d+k}C_k \qquad (d = dx_i)$$

となる。よって、

$$x_i = \frac{\tilde{N}_i(y)}{\tilde{D}_i(y)}$$

より、

$$\tilde{D}_i(y)x_i = \tilde{N}_i(y)$$

として、任意の平文xを代入し暗号文yを得ることによって、多項式$\tilde{D}_i(y)$, $\tilde{N}_i(y)$の未知係数に対する連立方程式を立て、これを定めることが理論的には可能になる。

ここで、$\tilde{D}_i(y)$, $\tilde{N}_i(y)$の未知係数の個数である項の数tx_i

表2 変数ベクトルの次元と未知係数の個数

k	$2tx_i$
4	3×10^5
5	7×10^9
6	1×10^{16}
7	1×10^{24}

を、実際に計算してみると、表２のようになる。

現在、最も速い逆行列の計算法[8]を用いても、n次正方行列の逆行列の計算に必要な計算量は、$O(n^{2.5})$である。よって、kを５以上とすれば、この方法による解読は、不可能であると結論付けることができる。

以上のことから、有理関数に基づく順序解法により構成される暗号系は、$k \geq 6$とすれば、充分高い信頼性をもつものと考えられる。従って、以下の議論においては、$k = 6$とする。

５．本方式の処理量、及び、記述量

３．で示した構成において、g_{ij}, g_{Di}は、$x_1 \sim x_6$の１次式となる。６変数の１次多項式は、７個の項をもつ。

従って、暗号化・復号化に要する処理量は、表３に示す通りとなる。

表３　必要な演算の種類と回数（k＝6 の場合）

演算	暗号化変換	復号化変換
a × b	８８２	１９４
a ÷ b	１２６	２１
a ＋ b	１００２	１９７

一方、本暗号系は、公開鍵記述量を削減するために、有理関数の係数、及び、正則行列の成分はGF(2^s)の要素とし、平文・暗号文ベクトルの要素は、その拡大体GF(2^t)上の元としている。ここで、GF(2^{65})上においては、除算を高速に行うことができる[9]ので、

$t = 65$　　$s = 13$　　（$t = 5s$）

とする。

よって、公開鍵・秘密鍵記述量は、表４のようになる。

表４　公開鍵・秘密鍵記述量（k＝6 の場合）

公開鍵記述量	1764s bits
	22.9 kbits　(s＝13)
秘密鍵記述量	236s bits
	3.1 kbits　(s＝13)

６．ディジタル署名

本方式は、公開鍵が有理関数で与えられているので、分母＝０となるような平文が存在し、これがディジタル署名を実現する際に問題となる。以下本章では、このような平文の存在する割合が極めて小さく、実用上問題とならないことを示す。

3．で述べたように暗号文yは、平文xの有理関数により、

$$y_1 = \sum_{i=1}^{2^{t-1}} \frac{g_{1i}(x_1, x_2, \cdots, x_6)}{g_{Di}(x_1, x_2, \cdots, x_6)}$$

$$y_2 = \sum_{i=1}^{2^{t-1}} \frac{g_{2i}(x_1, x_2, \cdots, x_6)}{g_{Di}(x_1, x_2, \cdots, x_6)}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_6 = \sum_{i=1}^{2^{t-1}} \frac{g_{6i}(x_1, x_2, \cdots, x_6)}{g_{Di}(x_1, x_2, \cdots, x_6)}$$

但し、

g_{ij}, g_{Di} : $x_1, x_2, \cdots, x_6$の１次式

で与えられる。今、$g_{Di}(x_1, x_2, \cdots, x_6) = 0$となる平文全体をＺとする。ところで、

$$g_{Di}(x_1, x_2, \cdots, x_6) = (\hat{a}_i x_1 + \hat{b}_i x_2 + \cdots + \hat{f}_i x_6 + \hat{g}_i)$$

であるから、$g_{Di}(x_1, x_2, \cdots, x_6) = 0$となる平文全体は、$2^{5t}$個存在する。すると、明らかに、有理関数の個数は２１個であるので、集合Ｚの要素数｜Ｚ｜は、

$$|Z| \leqq 21 \cdot 2^{5t}$$

となる。ディジタル署名不可能な暗号文の全体をＮＧとすると、これは、復号化操作により平文を導出できないものの全体と一致するので、

$$|Z| = |NG|$$

が成り立つ。一方、暗号文空間全体は2^{6t}個の要素をもつので、暗号文空間の中で、ディジタル署名不可能な暗号文の存在する割合ｒは、

$$r = \frac{|NG|}{2^{6t}} = \frac{|Z|}{2^{6t}} \leqq 21 \cdot 2^{-t}$$

となる。

ここで、t＝６５とすると、$r < 10^{-20}$となり、本方式においてディジタル署名が実現できない確率は実際上無視できると考えてよい。

以上をまとめて、表５に示す。

表５　本暗号系の諸特性

k=6		t=65 s=13
平文長	6t bits	390 bits
暗号文長	6t bits	390 bits
公開鍵記述量	1764s bits	22.9 kbits
秘密鍵記述量	236s bits	3.1 kbits
暗号化計算量	$O(t^2)$	——
復号化計算量	$O(t^2)$	——
ディジタル署名	可能	——

7．むすび

非線形連立方程式の順序解法に基づく公開鍵暗号系の一般化された方式を示し、非線形性を有理関数とした方式を提案した。続いて、考え得る解読法を想定して、それらに対して十分な信頼性を有することを確認した。また、公開鍵・秘密鍵記述量、暗号化・復号化変換計算量等について検討し、さらに、ディジタル署名が可能であることを示した。

本暗号系では、暗号文ベクトルxが与えられると、各項が独立に計算できるので、並列処理による高速な変換の実現が期待できる。今後、暗号化装置のハードウェア構成等について検討を進める予定である。

また、いかなる暗号系も絶対の信頼性を保証することは不可能であるが、今後、御批判を仰ぎつつ信頼性について考察を深めたいと考えている。

文献

[1] W.Diffie and M.E.Hellman : "New Directions in Cryptography", IEEE Trans. Inf. Theory, IT-22, pp.644-654 (Nov. 1976).

[2] D.W.Davis and W.L.Price（上園忠弘監訳）：“ネットワーク・セキュリティ”，日経マグロウヒル社 (1985).

[3] R.L.Rivest, A.Shamir and L.Adleman : "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Commun. ACM, 21, pp.120-126 (Feb. 1978).

[4] 辻井重男：“非線形連立方程式の順序解法を利用する公開鍵暗号方式”，情報理論とその応用研究会　第８回シンポジウム資料，pp.156-157 (1985-12).

[5] 辻井，松本，黒沢，伊東，藤岡：“非線形連立方程式の順序解法による公開鍵暗号方式”，信学技報，IT85-90 (1985-05).

[6] 松本，今井，原島，宮川：“Obscure表現による高速非対称暗号系”，信学技報，IT84-50，(1984-03).

[7] 岡本，中村：“最近提案された公開鍵暗号系の評価”，第３回ＣＩＳシンポジウム資料，(1986-02).

[8] D.Coppersmith and S.Winograd : "On the Asymptotic Complexity of Matrix Multiplication", SIAM J. Comput., 11, 3, (Aug. 1982).

[9] 伊東，オン，辻井：“正規基底を用いたＧＦ(2^t)における逆元の高速算法”，昭和６１年度電子通信学会通信部門全国大会，（投稿中）