2008－CSEC－42（2）
2008 / 7 / 24

線形持駒方式の安全性に対する一考察

－ SCIS'07版 －

金子 敏信† 五十嵐保隆† 伊藤 大介† 早川 潔†

†

† 東京理科大学
〒 278-8510 千葉県野田市山崎 2641
E-mail: †kaneko@ee.noda.tus.ac.jp, ††yasutaka@rs.noda.tus.ac.jp

あらまし 持ち駒暗号方式は、多次多変数公開鍵暗号方式（原方式）の安全性強化を目的として、2003年に辻井らにより提案された暗号方式である。当初の提案では、順序解法型公開鍵方式を例に、それを強化する方式として説明され、その後、複数種類の改良版が示されている。ここでは、順序解法型公開鍵方式と持ち駒方式の組み合わせについて、SCIS'07版を取り上げ、その安全性を考察し、公開鍵から等価な秘密鍵を導出する解読アルゴリズムを示す。改良型順序解法と持ち駒方式の組み合わせは、実用的なパラメータサイズにおいては、安全性が不十分である。

キーワード 多次多変数公開鍵暗号方式、持ち駒暗号方式、順序解法型公開鍵方式、暗号解読

On the security of Piece In Hand Matrix Multivariate Public Key Cryptosystems

－ MPKC systems proposed in SCIS'07 －

Toshinobu KANEKO†, Yasutaka IGARASHI†, Daisuke ITOH†, and Kiyoshi HAYAKAWA†

†

† Tokyo University of Science
Yamazaki 2641, Noda City, Chiba, Japan
E-mail: †kaneko@ee.noda.tus.ac.jp, ††yasutaka@rs.noda.tus.ac.jp

Abstract MOCHIGOMA (Piece in Hand) system is an encryption algorithm proposed by Tujii et al. in 2003, for enhancing the security of multivariate type public key cryptosystems. They illustrate the effectiveness of MOCHIGOMA system by applying it to Sequential Solution Method public key cryptosystem (MOCHIGOMA+SSMPKC), which has been shown to be insecure. After the proposal of MOCHIGOMA system they have continuously proposed many variants of the system. In this paper, we analyze the security of MOCHIGOA+enhanced-SSMPKC cryptosystem, which is proposed by Tadaki et al. in SCIS 2007. We show an algorithm to derive equivalent private keys from the public key of the system. In a practical parameter size, the security of MOCHIGOMA+enhanced-SSMPKC is insufficient.

Key words multivariate type public key cryptosystems, MOCHIGOMA system, Piece in Hand system, Sequential Solution Method public key cryptosystem, cryptanalysis

1. はじめに

多次多変数公開鍵暗号方式は、高速な公開鍵暗号の実現を目指し、1980年代から研究が進められてきた。落とし戸の構造で分類するならば、一つは、拡大体上の特殊な関数を基礎体の多次多変数方程式と見なし利用する松本・今井方式（MI方式）[8]やその改良版のHFE方式[9]やPMI方式[1]、他方は、順序解法構造を落とし戸として利用する辻井らの順序解法方式や、類似の考えを利用した笠原らのRSSE方式[7]が上げられる。

順序解法方式の考えは、1986年に辻井らにより月文暗号と

して提案された[12]。公開鍵である多次多変数連立方程式に秘密鍵による（線形）変換を適用すると"簡単な式"が現れ、それを解いて、残りの式に代入する事により、次に解くべき"簡単な式"が順次現れるという構造を持つ。月文暗号の場合、"簡単な式"として、1次の有理式が使用されており、正当な受信者が最初に解く1次の有理式が平文及び暗号文の線形変換で導ける事に着目した公開鍵係数の比較により解読された[5]。辻井らは、月文暗号を改良し、この"簡単な式"として双1次変換の有理式を使用したものを1989年に提案している[10]。(注1)

辻井らは、2004年に持ち駒方式と呼ばれる暗号方式を提案した[11]。これは、持ち駒行列と呼ばれる秘密鍵行列を使い、任意の多次多変数型公開鍵暗号を、強化する事を目的とする手法である。この持ち駒行列は定数行列であり線形持駒方式と呼ばれる。2006年には、持ち駒行列が平文に依存する関数で構成される非線形持駒方式[14]を強化版として示している。これらにおいて、強化される対象の多次多変数型公開鍵暗号（以下、原方式）の例として、順序解法型が使われている。この原方式は、前述の"簡単な式"として、1次多項式を使ったものである。以下、この原方式を順序解法型暗号と呼ぶ。(注2)持ち駒暗号方式の安全性について、辻井らは、多次多変数連立方程式の一般的な解法であるグレブナー基底を用いた数式処理ソフトによる解読結果を中心に議論している。

筆者らは、暗号アルゴリズムの構造に着目した考察を行う事により、正確な安全性評価や弱点の発見が出来ると考え、これらの持ち駒方式の評価を行った。結果として、原方式が順序解法型暗号の持ち駒方式の場合、線形持ち駒方式[11]、非線形持ち駒方式[14]何れも、解読が可能であることを示している[2],[6]。解読手法は、順序解法型暗号で最初に解く方程式は1次式である事、順序解法型暗号は再帰的構造を持つ事に着目し、公開鍵係数の掃き出し処理で、公開鍵から等価な秘密鍵を導出する手法である。

2007年に只木、辻井は、最初に解く方程式が1次式の順序解法型暗号は、文献[2],[6]の公開鍵係数掃き出し処理で必ず解読が可能であることを証明すると共に、この解読法に対抗する為に、最初に解く方程式を2次式の順序解法型（以下、改良型順序解法）にする事を提案した[13]。

持ち駒方式は、持ち駒行列により原方式の公開鍵係数にランダム項を紛れ込ませる事により、攻撃者の目をくらます(注3)方法である。これを、外乱数法と呼ぶ。ランダム項は、平文の関数でも、乱数変数でも良いとされている。これ以外、原方式の平文変数の一部をランダム項で置き換える手法も提案されている[15]。これを、内乱数法という。

筆者らは、これらの暗号方式について解析を行い、改良型順序解法[13]に対し、最初に解く方程式が中間変数に対し、1変数2次方程式で有ることに着目した解読法を示した[4]。本稿は、この解読法の詳細をまとめたものである。なお、文献[15]の内乱数法の持ち駒暗号方式を順序解法型公開鍵暗号に適用した場合も同様に、最初に解く方程式が1次方程式で有ることに着目して同様に解読が可能である[4]。

辻井らは、その後、平文依存のランダム値を重畳する新しい非線形持ち駒方式を提案している[3],[16]。正当な受信者は、ランダム値を復元するための値を、暗号文から求め、その値を使って計算されるランダム値を取り除くと、原方式が現れる仕掛けである。その、安全性に関する検討が今後、期待される。

2. 順序解法構造と持駒暗号方式

2.1 順序解法構造

$GF(q)$ 上の非線形連立方程式を適切な中間変数 $\mathbf{u} = (u_1, u_2, \cdots, u_k)$、$\mathbf{w} = (w_1, w_2, \cdots, w_k)$ を使い書き直し、次式に整理でき、これらの式を u_k から $u_{k-1}, \ldots, u_1$ の順に解くことにより簡単に解ける場合、元の非線形連立方程式を、順序解法構造を持つ非線形連立方程式という.

$$\begin{aligned} w_1 &= h_1(u_1, u_2, \cdots, u_k) \\ w_2 &= h_2(u_2, u_3, \cdots, u_k) \\ &\vdots \\ w_{k-1} &= h_{k-1}(u_{k-1}, u_k) \\ w_k &= h_k(u_k) \end{aligned} \tag{1}$$

文献[14]における原方式としての順序解法型暗号は、"簡単な式"として1次方程式を採用している。すなわち、$h_k, h_{k-1}, \cdots, h_1$ が、それぞれ $u_k, u_{k-1}, \cdots, u_1$ に関し1次方程式である。1次方程式 $w_k = h_k(u_k)$ を解いて得られた u_k を、$w_{k-1} = h_{k-1}(u_{k-1}, u_k)$ に代入すれば、u_{k-1} についての1次方程式が得られ、それを解いて次の式に代入し、...、の繰り返しで、全体を k 回の1次方程式の解法の計算量で解くことができる。

文献[13]の順序解法構造

本稿で、解読対象とする文献[13]の改良型順序解法型暗号では、最初に解く式 $w_k = h_k(u_k)$ を、u_k の2次方程式としている。これにより、全ての方程式の全次数が2次となり最初に解く式を他の式から区別できないとしている。最初に解く式を小規模な連立2次方程式で置き換える事も可能であるが、本稿では、最初に解く式を1変数2次方程式として攻撃アルゴリズムを述べる(注4)。

2.2 順序解法型公開鍵暗号

式(1)の $\mathbf{u}$ と $\mathbf{w}$ の関係を

$$\mathbf{w} = H(\mathbf{u}) \tag{2}$$

と表す。中間変数 $\mathbf{u}$ を平文ベクトル $\mathbf{x}^T = (x_1, x_2, \cdots, x_k)$(注5)の線形変換

(注1)：攻撃者に許される条件を論文から明確に読み取ることが、筆者には出来なかったので文献[5]に類する係数比較法が適用出来るか否かは、未検討である。
(注2)：月文暗号や双1次変換の有理式を用い、式を展開した形で公開鍵とする場合、公開鍵係数の爆発的増加を招くので、この様な順序解法型暗号を用いたと推察される
(注3)：グレブナー基底攻撃であれば、計算量を増加させる

(注4)：最初に解く式が複数変数の小規模連立2次方程式でも基本的には、本稿のアルゴリズムが適用可能である
(注5)：^{T} は転置を表す

$$\mathbf{u} = A\mathbf{x} \tag{3}$$

とし、暗号文ベクトル $\mathbf{y}^T = (y_1, y_2, \cdots, y_k)$ として、中間変数 $\mathbf{w}$ を線形変換したもの

$$\mathbf{y} = B\mathbf{w} \tag{4}$$

を使う暗号化変換を順序解法型公開鍵暗号という。ここで、公開鍵は、合成関数

$$\mathbf{y} = BH(A\mathbf{x}) \tag{5}$$

を展開して得られる2次式の係数及び演算規則である体 $GF(q)$ である。ここで、行列 A、B は正則行列であり、順序解法構造を持つ関数 $H()$ と共に、秘密鍵となる。

2.3 持ち駒暗号方式

持ち駒暗号方式は、順序解法型公開鍵暗号のような多次多変数公開鍵暗号を強化する事を目的に考案されている。文献[13]で示されている持ち駒暗号方式を示す。強化対象の暗号を原方式と呼び、式(5)に示されるような暗号化変換を関数 $G()$ とし、持ち駒暗号方式の暗号化変換は、次式で表される。

$$\mathbf{y} = E(\mathbf{x}) = SG(A\mathbf{x}) + R\bar{\mathbf{X}} \tag{6}$$

ここで、ベクトル $\mathbf{X}$ は、変数 $x_1, \cdots, x_N$ の2次以下の単項式を並べた $t = {}_NC_2 + 2N + 1 = (N^2 + 3N + 2)/2$ 次元縦ベクトルである。この変数の頭の k ディジットが平文ディジット $x_1, \cdots, x_k$ であり、残りの $m = N - k$ ディジットが雑音ディジットである。暗号化変換において、雑音ディジットには、送信者が任意の値を入れることが出来るが、その値は受信側で、復元される必要はない。

$$\bar{\mathbf{X}} = (x_1^2, x_1x_2, x_1x_3, \cdots, x_N^2, x_1, \cdots, x_N, 1) \tag{7}$$

A は $k \times k$ 正則行列、S は、$rank(S) = k$ の $n \times k$ 行列、但し $(n > k)$、R は $n \times t$ 行列であり、$k \times n$ の行列 M と以下の関係にある。この M を持ち駒行列という。

$$\begin{cases} MS &= I_k \\ MR &= \mathbf{0} \end{cases} \tag{8}$$

ここで、I_k は $k \times k$ の単位行列、$\mathbf{0}$ は、全零行列を表す。

公開鍵と暗号化変換

式(6)を展開した l 番目の式の2次項 x_ix_j の係数 s_{lij}、1次項 x_i の係数 s_{li}、0次項係数 s_{lt} を並べた $n \times t$ 係数行列 E_k

$$E_k = \begin{pmatrix} s_{111} & s_{112} & \cdots & s_{1kk} & s_{11} & \cdots & s_{1k} & s_{1t} \\ s_{211} & \ddots & & s_{2kk} & s_{21} & \ddots & & s_{2t} \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ s_{n11} & \cdots & \cdots & s_{nkk} & s_{n1} & \cdots & & s_{nt} \end{pmatrix} \tag{9}$$

及び体 $GF(q)$ が公開鍵となる。

平文 $\mathbf{x}$ の暗号化変換は、$\mathbf{x}$ と雑音ディジットから単項式ベクトル $\bar{\mathbf{X}}$ を求め、行列 E_k を乗ずる事で行われる。

$$\mathbf{y} = E_k\bar{\mathbf{X}} \tag{10}$$

秘密鍵と復号変換

秘密鍵は、行列 A、S、R、及び原方式 $G(\mathbf{x})$ である。正当な受信者が、暗号文 $\mathbf{y}$ を復号する際は、式(6)に、左から持ち駒行列 M を掛ける。式(8)の条件より

$$M\mathbf{y} = G(A\mathbf{x}) \tag{11}$$

が得られるので、原方式 G を復号した後、行列 A の逆行列 A^{-1} を作用させれば平文 $\mathbf{x}$ が得られる。原方式の多次多変数公開鍵暗号に、行列 R で重畳したランダム項が、秘密鍵である持ち駒行列 M で取り除かれる事が本方式のミソである。

以下において、説明を簡単化する為、文献[13]と同じく、原方式である順序解法型暗号の秘密鍵行列 B 及び A は単位行列とする。即ち、$G = H$ と考え、順序解法型公開鍵暗号を持ち駒方式に適用した暗号の暗号化変換を

$$\mathbf{y} = E(\mathbf{x}) = SH(A\mathbf{x}) + R\bar{\mathbf{X}} \tag{12}$$

として、解読方法の説明を行う。即ち、持ち駒方式の秘密鍵行列 S 及び A の中に、順序解法型暗号の秘密鍵行列 B 及び A が組み込まれていると考えて、議論を展開する。これは、行列 S、A、M および、関数 G を

$$\begin{cases} S & \rightarrow & SB \\ A & \rightarrow & AA \\ M & \rightarrow & B^{-1}M \\ G & \rightarrow & H \end{cases} \tag{13}$$

で置き換えたと考えれば、一般性を失うものではない。この場合、正当な受信者は、式(11)の操作で $\mathbf{w} = M\mathbf{y}$ を手に入れ、順序解法構造の連立方程式 $\mathbf{w} = H(\mathbf{u})$ を k 番目の式から順次解くことになる。

3. 改良型順序解法暗号を原方式とする持ち駒方式の解読

3.1 文献[6]の解読法のまとめ

本稿で対象とする改良型順序解法+持ち駒方式公開鍵暗号は、順序解法構造で最初に解く式 $w_k = h_k(u_k)$ を除けば、順序解法+線形持ち駒方式であるので、文献[6]の解読法の概要をまとめる。そこでは、正当な受信者の復号作業をシミュレートする戦略で、解読が行われる。即ち公開鍵行列の式(9)の E_k から、復号に必要な等価な秘密鍵を導出し解読を行う。

順序解法構造における"簡単な式"が1次式で有ることに着目し、正当な受信者の復号手順で、秘密鍵 M が果たしている役割及び、順序解法の再帰構造を考えれば、順序解法+線形持ち駒方式の公開鍵暗号は、次の2つの性質を持つことが判る。

性質1　公開鍵係数行列 E_k に2次項以上を消去するような適切な行基本操作を行えば，簡単な式の係数行列が少なくとも1本出てくる。

性質2　順序解法型の構造より，簡単な式の解を他の式に代入し，適切な行基本操作を行えば次に解くべき簡単な式が順次現れる。

この性質を使い解読アルゴリズムは以下となる。

Step. 1　$i=k$ とおく。

Step. 2　公開鍵係数行列 E_k に行基本操作を加え梯形型とし，1 次項のみの行を探す．その際に行った行基本操作は，基本行列の積として記録しておく。

Step. 3　得られた簡単な式（例えば $x_{i1}+x_{i2}+\cdots$）が順序解法で最初に解くべき式である。その式の値を既知の中間変数 w_k と考え，式に含まれる 1 つの平文要素 x_{il} を w_i 使い消去し，変数の 1 つ少ない公開鍵係数行列 E_{i-1} を作る．すでに得られた簡単な式の本数が k 本未満の場合は $i=i-1$ として Step.2 へ

Step. 4　行基本操作に用いた基本行列の積から等価な持駒行列 M が得られる。得られた k 本の簡単な式を並べて等価な秘密鍵行列 A が求まる。

文献[6] では、この解読アルゴリズムが破綻無く実行可能であることを証明したが、性質 1 で"簡単な式"が複数本出てくる場合に得られる秘密鍵の等価性について厳密な証明はしていない。"簡単な式"が複数本出る場合(注6)を含め、このアルゴリズムで必ず解読が可能である事を示したのが文献[13] である。

3.2　解読法の着眼点

改良型順序解法＋持ち駒暗号方式においても正当な受信者の復号手順をシミュレートする戦略で解読を行う。改良型においては、最初に解く式 $w_k=h_k(u_k)$ が

$$w_k=\alpha u_k^2+\beta u_k+\gamma \tag{14}$$

このような 2 次式に変更になり、それ以降で正当な受信者が解く式は、従来と同じ 1 次式である。従って、最初に解く k 番目の式を推定できれば、残りの多次多変数連立方程式は、従来の公開鍵行列の掃き出し法による梯形型変形で解読が可能である。

ここで、式 (14) 右辺の中間変数 u_k は、$\mathbf{u}=A\mathbf{x}$ より、平文 $\mathbf{x}$ の線形結合であり、左辺の中間変数 w_k は、$\mathbf{w}=M\mathbf{y}$ より暗号文の線形結合である。従って、その線形結合定数を推定できれば、十分である。

中間変数 u_k は、行列 A の要素 a_{ij} を線形結合定数として、次式となる。

$$u_k=a_{k1}x_1+a_{k2}x_2+\cdots+a_{kk}x_k \tag{15}$$

行列 A は正則行列であり、a_{k1} から a_{kk} の内の少なくとも 1 つは、非零である事に注意する。ここで a_{k1} が非零であったと仮定する。この時、$a_{k1}=1$ としても、順序解法構造を損なうものではない。なぜならば $\tilde{u}_k=a_{k1}^{-1}u_k$ とおけば、

$$\tilde{u}_k=x_1+\tilde{a}_{k2}x_2+\cdots+\tilde{a}_{kk}x_k \tag{16}$$

に対し、$\tilde{u}_k$ に関する 2 次方程式

$$w_k=\alpha a_{k1}^2\tilde{u}_k^2+\beta a_{k1}\tilde{u}_k+\gamma \tag{17}$$

を解くことにより、順序解法の実行が、可能である。もし、$a_{k1}=0$ であれば、線形結合定数の推定に失敗するので、そのときは、$a_{k1},\cdots$ が非零であると仮定して、再度定数の推定を行えばよい。それ故、ここでは、中間変数 u_k が

$$u_k=x_1+a_{k2}x_2+\cdots+a_{kk}x_k \tag{18}$$

と書けると仮定し、定数 $a_{k2},\ldots,a_{kk}$ を推定する。

従って、

$$x_1=u_1-a_{k2}x_2-\cdots-a_{kk}x_k \tag{19}$$

とおいて、公開鍵による暗号化変換の式 (12) に代入し、適切な線形結合

$$T=c_1y_1+c_2y_2+\cdots+c_ny_n \tag{20}$$

をとれば、最初に解く 2 次式 (14) が得られ、u_k 及び定数以外の項は消えるはずである。等価な線形結合定数が満たす条件は、この式において x_i、u_kx_i、x_ix_j の項の係数が 0 となる事である。その条件を満たす線形結合係数 $a_{k2},\ldots,a_{kk}$ 及び $c_1,\cdots,c_n$ が等価な行列 A と持ち駒行列 M の k 行目を与える事になる。

3.3　等価な行列 A、M の推定

公開鍵による暗号化変換の式 (12) の第 l 番目 ($l=1,\ldots,n$) の式を書けば式 (9) の E_k の要素を使い

$$y_l(\mathbf{x})=\sum_{i=1}^{N}s_{li}x_i+\sum_{i=1,j=1}^{N}s_{lij}x_ix_j+s_{lt} \tag{21}$$

である。x_1 を消去する式 (19) を使い、式 (20) が、最初に解く u_k のみの 2 次式になる為の係数条件式は、以下である。

[x_i の係数条件]

$$a_i\sum_{l=1}^{n}c_ls_{l1}+\sum_{l=1}^{n}c_ls_{li}=0 \tag{22}$$

[ux_i の係数条件]

$$a_i(2\sum_{l=1}^{n}c_ls_{l11})+\sum_{l=1}^{n}c_ls_{l1i}=0 \tag{23}$$

[x_i^2 の係数条件]

$$a_i^2\sum_{l=1}^{n}c_ls_{l11}+a_i\sum_{l=1}^{n}c_ls_{l1i}+\sum_{l=1}^{n}c_ls_{lii}=0 \tag{24}$$

[x_ix_j の係数条件 ($i\neq j$)]

$$a_ia_j(2\sum_{l=1}^{n}c_ls_{l11})+a_j\sum_{l=1}^{n}c_ls_{l1i}+a_i\sum_{l=1}^{n}c_ls_{l1j}+\sum_{l=1}^{n}c_ls_{lij}=0 \tag{25}$$

これらの式において i,j は $i=2,\cdots,N, j=i,\cdots,N$ の範囲を取り得る。この係数を決める条件式の最後の 2 つは、a_i と c_l の 3 次式であり、もとの多次多変数連立方程式を解く問題より、見かけ上難しそうに見えるが、以下の方法で簡単に解くことが出来る。

(注6)：これはある意味で弱い順序解法型暗号である。

基本の2次条件式

式 (22)、(23) 以外は、a_i,c_l の3次式である。これら式の適切な差を取ることにより残りの式も2次式に整理できる。ポイントは、ux_i の係数条件から導かれる式 (23) の2次項 (第1項の $\sum$) の a_i 倍又は a_j 倍が、最後の2つの式の3次項と一致していることにある。式 (24) を2倍した式から、式 (23) を差し引けば、3次項を消去した式

$$a_i \sum_{l=1}^{n} c_l s_{l1i} + 2 \sum_{l=1}^{n} c_l s_{lii} = 0 \qquad (26)$$

が得られる。同様の操作を式 (23) と式 (25) に対して行えば

$$a_i \sum_{l=1}^{n} c_l s_{l1j} + 2 \sum_{l=1}^{n} c_l s_{lij} = 0 \qquad (27)$$

が得られる。この2種類の式と式 (22)、(23) を合わせて、基本の2次条件式と呼ぶ。式の数は式 (22)、(23)、(26) が、それぞれ $N-1$ 通り、式 (27) が ${}_{N-1}C_2$ 通りである。

XL 型の条件式増殖と解読

これら基本の条件式に未知数である a_i を適切に掛け算し、式を整理する事により使える条件式を増やす。これは、XL 型解読法として知られている技術である。式 (22) の第1項の $\sum$ は、x_i に対する条件式と x_j に対する条件式で同一なので、一方を a_j 倍、他方を a_i 倍して差をとれば

$$a_i \sum_{l=1}^{n} c_l s_{lj} + a_j \sum_{l=1}^{n} c_l s_{li} = 0 \qquad (28)$$

の式が得られる。これで得られる式の数は、${}_{N-1}C_2$ 通りである。さらに、式 (26)、(27) でも同様の操作を行えば、2次式が同じく ${}_{N-1}C_2$ 通り得られる。以上を合計するならば、得られる条件式は、$3(N-1)+3{}_{N-1}C_2 = 3N(N-1)/2$ となる。これらの条件式の自明な解として $c_l = 0,(l = 1,\ldots,n)$ があるので、条件式を満たす非自明な解が求める係数 a_i,c_l を与える。

全ての未知項を独立未知数として線形方程式として高次方程式を解く線形化手法で解くとすると未知項の種類数は、a_i が $N-1$ 通り c_l が n 通り、a_ic_l が $(N-1)n$ 通りであり、その数は合計 $N-1+n+(N-1)n = Nn+N-1$ である。通常、持ち駒暗号方式では、安全性の為 $n \leqq N$ に取られる事を考えると、未知項の数に比べ、得られた線形方程式の数が 1.5 倍程度となり、高い確率で未知数 a_i,c_l を定める事ができる。Tiny model で実験しそれを確認している。これにより、改良型順序解法で解く最初の2次方程式が見いだせたので、残りは、文献[6] の手法で解読すれば十分である。

4. 考　　察

4.1 ランダム項によるダミー解

前節の XL 型手法で得られる方程式は、真の秘密鍵に対し成立するので、自明でない解は必ず存在する。しかし、持ち駒暗号方式で導入されたランダム項の影響で、偽の解が、得られる可能性を考察する。

$GF(q)$ 上の N 変数2次式がランダムに n 本与えられたとする。N 変数の2次以下の項の種類数は、$M = {}_NC_2+N+N+1 = (N^2+3N+2)/2$ である。n 本の式の線形結合で2次項を消去して1つの式にまとめても依然としてその式の中には、項の数が $M-n+1$ 項ある。そのような式は q^{M-n+1} 通りある。即ち、式 (6) における行列 R の影響で、公開鍵係数行列がランダムになったとすると最初に解く式は $M-n+1$ 種類の高次項を持ち、その式の候補は、q^{M-n+1} 通りある。

しかし、改良型順序解法において最初に解く式は、式 (14) のような1変数2次式である。この式で、自由に設定出来るのは α/γ、β/γ、及び線形結合係数 a_i の $N+2$ 変数であり、式の種類数は、q^{N+2} 通りである。従って、ランダムな $GF(q)$ 上の N 変数2次式 n 本の線形結合を取って、(偽の) 1変数2次式が出てくる確率は

$$\frac{q^{N+2}}{q^{M-n+1}} = q^{-\frac{N^2+N-2n}{2}} \qquad (29)$$

であり、十分小さい。

4.2 解読計算量および改良型順序解法の安全性

本稿で述べた解読計算量の見積もりを行う。最初に解く1変数2次方程式を与える等価な線形結合係数の計算が最も時間がかかる。XL 型の解読を素朴に実行したとして、その計算量は、$Nn+N-1 \approx Nn$ 変数の線形連立方程式を解く時間であり、ほぼ $(Nn)^3$ である。一方、正当な受信者の復号計算量で多いのは、式 (11) の持ち駒行列 M の乗算であろう。M は、k 行 n 列であり、計算量は、ほぼ kn である。正当な受信者がストレス無く復号計算が行え、攻撃者の解読計算が不可能であるためには、この計算量格差が十分大きいことが必要である。どの程度の計算量格差があれば、安心して使える暗号となるかの絶対的基準は無いが、共通鍵暗号の世界では、128 ビット鍵の安全な暗号が安心して使える暗号であると考えられており、その場合攻撃計算量は正当な受信者の計算量の 2^{128} 倍である事が要求されている。これを改良型順序解法暗号に適用するならば、$(Nn)^3/kn = (N^3n^2)/k > 2^{128}$ である。おおざっぱに $N \approx n \approx k$ と考えれば、平文未知数の数 $k \approx 2^{32}$ 以上で、2^{32} 本以上の連立2次方程式で記述されるような改良型順序解法+持ち駒暗号方式であれば安心して使える暗号となる。しかしながら、このパラメータサイズは実用的なものでは無く、その意味で、この暗号の安全性は不十分であると判断される。

5. 結　　論

2007 年に只木らが SCIS で提案した改良型順序解法と持ち駒暗号方式の組みあわせに対し、安全性を検討した。それは、最初に解く "簡単な式" が1変数2次式の順序解法構造を持つ多次多変数公開鍵暗号である。この"簡単な式"が出てくるように暗号化変換の入出力ディジットの線形結合係数を公開鍵から定めれば、この暗号は解読ができる。本稿では、この原理に基づく効果的な解読アルゴリズムを提案しその攻撃計算量を明らかにした。この解読アルゴリズムを使うならば、改良型順序解法と持ち駒暗号方式の組あわせは、実用的なパラメータサイズでは安全性が不十分である。

文　献

[1] J. Ding, "A new variant of the Matsumoto-Imai cryptosystem through perturbation," Proc. PKC 2004, Lecture Notes in Computer Science, Vol.2947, pp.305-318, Springer, (2004.3)

[2] 福島 啓友, 伊藤 大介, 金子 敏信, "順序解法を原方式に持つ非線形持駒方式の安全性に関する一考察",FIT2006, pp.257-258, (2006.9)

[3] 藤田亮, 只木孝太郎, 辻井重男, "多様な多変数公開鍵暗号を汎用的に強化する非線形持駒摂動ベクトル方式",1F1-1, SCIS2008, (2008.1)

[4] 早川潔, 伊藤大介, 金子敏信: "線形持駒方式 (SCIS'07 版) の安全性に対する一考察", 平成 19 年度電気関係学会北陸支部連合大会, E-36, (2007.9)

[5] 長谷川栄, 金子敏信,"非線形連立方程式の順序解法による公開鍵暗号方式の攻撃法"、第１０回　情報理論とその応用シンポジウム、SITA'87,JA5-3, pp.113-118,(1987.11)

[6] 伊藤 大介, 福島 啓友, 金子敏信, "順序解法を原方式に持つ線形持駒方式の安全性に関する一考察", 信技報,ISEC 2006-30, pp.155-159, (2006.7)

[7] M. Kasahara and R. Sakai, "A construction of publickey cryptosystem based on singular simultaneous equations and its variants," 信学技法, ISEC2005-7 (2005-05)

[8] T. Matsumoto and H. Imai, "Public quadratic polynomialtuples for efficient signature-verification and messageencryption,"Proc. EUROCRYPT '88, Lecture Notes in Computer Science, Vol.330, pp.419-453, Springer, (1988.5)

[9] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms," Proc. EUROCRYPT '96, Lecture Notes in Computer Science, Vol.1070, pp.33-48, Springer, (1996.5)

[10] 辻井, 藤岡, 平山,"順序解法の一般化による公開鍵暗号系", 信学論 A, Vol.J72-A,No.2,pp.390-397,(1989.2)

[11] S. Tsujii, R. Fujita, and K. Tadaki, "Proposal of MOCHIGOMA (piece in hand) concept for multivariate type public key cryptosystem", 信学技法, ISEC2004-74, (2004-09)

[12] 辻井重男, 黒澤馨, 伊東利哉, 藤岡淳, 松本勉, "非線形連立方程式の順序解法による公開鍵暗号方式," 信学論 (D), vol.J69-D, no.12, pp.1963-1970, (1986.12)

[13] K.Tadaki and S.Tsujii."On the Enchancement of Security by Piece In Hand Matrix Method for Multivatariate Public Key Cryptrosystems",2C1-3, SCIS2007, (2007.1)

[14] 辻井重男, 只木孝太郎, 藤田亮, "持駒行列の提案その 2 -多変数多項式型公開鍵暗号の安全性強化のための汎用的手法-", SCIS2006, 2A4-1, (2006.1)

[15] Shigeo Tsujii, Kohtaro Tadaki, and Ryou Fujita, "Proposal for Peice in Hand Matrix: General Concept for Enhancing Security of Multivariate Public Key Cryptosystems", IEICE TRANS. FUNDAMENTALS VOL.E-90-A, NO.5, pp992-999, (2007.5)

[16] 辻井重男, 只木孝太郎, 藤田亮, "多様な多変数公開鍵暗号を汎用的に強化する非線形持駒行列の構成法", 信学技報, vol.107, no.141, ISEC2007-56, pp.75-80, (2007.1)