社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (41)
2007／7／20

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

辻井 重男† 只木孝太郎†† 藤田 亮†

† 情報セキュリティ大学院大学 〒221-0835 横浜市神奈川区鶴屋町 2-14-1
†† 中央大学研究開発機構 〒112-8551 東京都文京区春日 1-13-27
E-mail: †{tsujii,dgs063103}@iisec.ac.jp, ††tadaki@kc.chuo-u.ac.jp

あらまし 量子コンピュータに対する耐性を念頭において，多くの多変数公開鍵暗号方式が内外から提案されている．それ等の安全性を汎用的に強化する手法として，筆者等は持駒行列方式を提案してきた．持駒行列には，線形行列，及び非線形行列が考えられる．いずれの場合についても既に報告してきたが，非線形の場合，先に示した方式では，公開鍵多項式の次数が 3 次となり，鍵長が長くなるという欠点があった．今回，この次数を 2 次に抑える非線形持駒行列を考案したので発表する．

キーワード 公開鍵暗号，多変数多項式，多変数公開鍵暗号，持駒概念，非線形行列

A Construction Method of Nonlinear Piece In Hand Matrix for Universally Enhancing the Security of Various Multivariate Public Key Cryptosystems

Shigeo TSUJII†, Kohtaro TADAKI††, and Ryou FUJITA†

† Institute of Information Security Tsuruya-cho 2-14-1, Kanagawa-ku, Yokohama, 221-0835 Japan
†† Research and Development Initiative, Chuo University
Kasuga 1-13-27, Bunkyo-ku, Tokyo, 112-8551 Japan
E-mail: †{tsujii,dgs063103}@iisec.ac.jp, ††tadaki@kc.chuo-u.ac.jp

Abstract Considering invulnerability for a quantum computer, many multivariate public key cryptosystems have been proposed in Japan and abroad. As a universal method for enhancing the security of them, authors have proposed piece in hand matrix method. For piece in hand matrix, we could have two types of matrices: linear and nonlinear. We have already proposed on both cases. However, in the case of the nonlinear matrix, the degree of public key polynomials becomes three, which makes the key length longer. This time, we devised a nonlinear piece in hand matrix, where the degree of public key polynomials is kept two.

Key words public key cryptosystem, multivariate polynomial, multivariate public key cryptosystem, piece in hand concept, nonlinear matrix

1. まえがき

多変数公開鍵暗号研究は，1980 年代，今井・松本，辻井等によって始められた．辻井等は，1985 年，多変数公開鍵暗号の落とし戸として，順序解法と名付ける手法を考案したが，金子等の解析を受け，ある条件の場合，順序解法を用いた多変数公開鍵暗号が解読されることが示された [9], [22], [23]．これらの論文は，日本語でのみ発表したので国際的には知られていなかったのであるが，1993 年，Shamir は，順序解法と同様の手法を用いた署名方式を CRYPTO で発表し，同年，Coppersmith 等により解読されている [4], [21]．辻井等は，金子等の解析を受けて，順序解法に核変換と呼ぶ変換を導入することにより改良を施した一般化順序解法を提案した [24]．この暗号は，現在まで破られていないが，2004 年，本文のテーマである持駒方式を IACR の ePrint に掲載した折，付録として載せておいた英訳版に対する解析を現在，Ding 等が進めている [7]．

松本・今井等は，有限体 $\mathbf{F}_q$ の n 次拡大体 $\mathbf{K}$ の元とそのベクトル表現の関係を巧に利用した MI (Matsumoto-Imai) 暗号を 1983 年に提案し，1988 年，EUROCRYPT で発表した [17], [18]．1995 年，Patarin は，これを解析し，翌 1996 年には，MI 暗号を拡張した HFE (Hidden Field Equation) 暗号を提案している [20]．この頃から多変数公開鍵暗号研究が国際的に

活発化し様々な方式が提案され始めたが [5], [6], [16], [19], [32], MI 暗号はその世界的源流となっている．我が国でも，笠原・境，秋山等が，この分野で活発な活動を続けている [2], [3], [10]〜[15].

これらの方式提案に呼応するかのように，多変数暗号解析の正攻法である多変数多項式の零点問題の解法においても，1999 年，Kipnis と Shamir は，HFE 暗号を攻撃する目的で，Relinearization と呼ぶ方法を提案し，2000 年，Courtois 等は，その改良版である XL 法を提案した．また，本来，イデアル所属判定問題を解く際の生成系であるグレブナ基底は，「与えられた多変数多項式と同じ共通零点を持つ，解きやすい形の多項式集合」とも看做せることから，公開鍵暗号のみならず，共通鍵暗号まで含めて安全性解析に適用されている．グレブナ基底を求める効率的アルゴリズムとして，Faugère により，1999 年には F_4 が，2002 年には F_5 が提案された．そして，2003 年，Faugère と Joux は，F_5 グレブナ基底計算により，Patarin によって提案された first HFE challenge（80bits）を解読している．

1980 年代の多変数公開鍵暗号研究は，RSA 暗号より高速な暗号方式の追求が大きな動機であったが，その後，RSA 暗号や楕円曲線暗号が依拠する素因数分解や離散対数問題が量子コンピュータにより原理的には多項式時間で解かれることが明らかになったため，最近の研究活発化の背景には，量子コンピュータ時代の到来に備えるという意識の高まりがこれに加わった．2006 年 5 月，ベルギーで，初めて，量子コンピュータ時代の暗号に関するワークショップ，PQCrypto（Post-Quantum Cryptography）が開催され，多数の論文が発表された [1].

多変数多項式は，ランダム多変数多項式，すなわち，その係数をランダムに定めた多項式の場合，その零点問題は NP 困難であるが，公開鍵暗号として，多変数多項式を利用する場合，落とし戸を組み込まねばならないため，NP 困難性が損なわれ易い点が問題となる．

これまで，順序解法（辻井他），MI（松本・今井），HFE (Patarin)，RSSE（笠原・境），代数曲面（秋山他）… など多くの多変数公開鍵暗号方式が提案されてきたが，それらの殆どは，多変数多項式の零点問題に対する一般的解法であるグレブナ基底計算アルゴリズムによって，ランダム多変数多項式に比較して，小さな計算量で解読されてしまうことが予想され，また，これは，小さな例に関するシミュレーションでも確かめることができる．

そこで，従来，提案されてきた様々な多変数公開鍵暗号方式をランダム多変数多項式に近づけることにより，これらの安全性を汎用的に向上させる概念あるいは手法として，筆者等は，持駒方式を提案してきた．持駒方式とは，秘匿通信において，様々な多変数公開鍵暗号方式（原方式）に対し，

- 鍵生成：原方式の公開鍵（多項式列ベクトル）にランダム部（多項式列ベクトル）を付加したベクトルを持駒方式の公開鍵（多項式列ベクトル）とする．
- 暗号化：送信者は，持駒方式の公開鍵（多項式列ベクトル）を用いて平文を暗号化し，持駒方式の暗号文を得，これを送信する．
- 復号； 正当な受信者が有する秘密鍵である持駒行列と呼ぶ非正則行列を，受信された暗号文に乗ずることにより，ランダム部を消去し，原方式の暗号文を得，それを，原方式の復号アルゴリズムによって復号する．

という手法である．

持駒行列には，線形行列と非線形行列が考えられる．線形行列は，予め定められた定数を要素とする行列であるのに対して，非線形行列は，平文の一部を要素として含む行列であり，復号時に，受信した暗号文から情報を取り出して，持駒行列を構成する．

持駒方式においては，ランダム部を付加し，復号の際，それを除去するような構成とするため，平文変数より，式の数が多くなり（overdefined），グレブナ基底攻撃等に対する耐性が劣化することも考えられるので，乱数変数を付加して，変数の数を式数より大きくする手法 [29]〜[31] も組み合わせる．

この手法において，乱数変数を付加することにより，原方式部に乱数変数が含まれるため，ランダム部に相当する部分を除去することができる正当な受信者でさえ，乱数変数の値を一意に復号することはできない．しかしながら，持駒行列を用いることにより，持駒方式の暗号文から原方式の暗号文（に相当するベクトル）を得，さらに，原方式の復号アルゴリズムにより，原方式の平文（に相当するベクトル）を得られたならば，持駒方式の平文を得ることは可能である．

一方，平文変数と乱数変数の区別がわかっていても，持駒行列を知らずに，攻撃者が，ランダム部を除去することは困難である．平文を得ようとする一般的な攻撃としては，公開鍵多項式と暗号文から構成したイデアルについてグレブナ基底を計算し，これをもとにしてイデアルを分解することが考えられる．この計算量はイデアルの零点の構造に依存し，構造が複雑になるにつれて，計算量が増大する．乱数変数を付加した持駒方式の場合について考えると，平文変数の値が一意であり，その構造がもっとも単純な場合でさえ，乱数変数の値が（適当な変数変換を施したとしても）一意と限らないため，イデアルの零点の構造は総体的に複雑となる．それゆえ，持駒方式の平文を得るために要する，攻撃者と正当な受信者の計算量の間に差が生じ，これにより，暗号の安全性が向上する．

線形持駒方式 [25]〜[31] における秘密鍵である線形持駒行列が，攻撃者によって，等価的にでも偽造される一般的方法はないと考えられるが，偽造されないということを，証明することも難しい．非線形行列を偽造することは，線形的手法では不可能であり，非線形的手法によって偽造することは，暗号解読により平文を得ることと同義となる．

そこで，持駒行列を非線形行列とする非線形持駒方式を構築しておくことも意味があると考え，既に，文献 [27], [28] 等で，その構成法を示したが，公開鍵多項式の次数が上がるという欠点があった．本文では，この次数を上げない非線形持駒行列の構成法を提案する．要約すれば，本方式は

（1） 公開鍵多項式の次数を上げない非線形持駒行列の導入
（2） 乱数付加（線形・非線形を問わず適用可能）

という 2 つの着想を柱に，非線形持駒方式を構成する．

2. 準　　備

2.1 記号の説明

正整数 $q \geq 2$ に対し，$\mathbf{F}_q$ を位数 q の有限体とする．$\mathbf{F}_q[x_1,\ldots,x_k]$ を係数を $\mathbf{F}_q$ にもち，$x_1,x_2,\ldots,x_k$ を変数とするすべての多項式の集合とする．任意の空でない集合 S と，任意の正整数 n,l に対し，$S^{n\times l}$ を要素を S にもつすべての $n\times l$ 行列の集合とし，S^n を n 個の S の要素からなるすべての列ベクトルの集合とする．列ベクトルを $\boldsymbol{p},\boldsymbol{E},\boldsymbol{X}$ のようにボールド体によって表記する．任意の行列 $A\in S^{n\times l}$ に対し，$A^T\in S^{l\times n}$ をその転置行列とする．$O_{n,l}\in S^{n\times l}$, $\mathbf{0}_n\in S^n$ をそれぞれ，すべての要素が 0 である $n\times l$ 行列，n 次元列ベクトルとする．$\mathbf{F}_q[x_1,\ldots,x_k]^n, \mathbf{F}_q[x_1,\ldots,x_m]^k$ の多項式列ベクトルをそれぞれ

$$\boldsymbol{f}=\begin{pmatrix} f_1\\ \vdots\\ f_n\end{pmatrix}, \boldsymbol{g}=\begin{pmatrix} g_1\\ \vdots\\ g_k\end{pmatrix}$$

とする．ここに $f_1,\ldots,f_n\in\mathbf{F}_q[x_1,\ldots,x_k], g_1,\ldots,g_k\in\mathbf{F}_q[x_1,\ldots,x_m]$ である．$\boldsymbol{f}$ に対する $\boldsymbol{g}$ の代入 $\boldsymbol{f}(\boldsymbol{g})\in\mathbf{F}_q[x_1,\ldots,x_m]^n$ を

$$\boldsymbol{f}(\boldsymbol{g})\equiv\begin{pmatrix} h_1\\ \vdots\\ h_n\end{pmatrix}$$

と定義する．ここに，各 h_i は $\mathbf{F}_q[x_1,\ldots,x_m]$ の要素であり，各 f_i の変数 $x_1,\ldots,x_k$ にそれぞれ $g_1,\ldots,g_k$ を代入して得られたものである．任意の $\boldsymbol{f}\in\mathbf{F}_q[x_1,\ldots,x_k]^n, \boldsymbol{p}\in\mathbf{F}_q^k$ に対し，$\boldsymbol{f}(\boldsymbol{p})$ を，$\boldsymbol{f}$ の変数 $x_1,\ldots,x_k$ にそれぞれ $p_1,\ldots,p_k$ を代入して得られた結果である $\mathbf{F}_q^n$ のベクトルとする．ここに $\boldsymbol{p}=(p_1,\ldots,p_k)^T$, $p_1,\ldots,p_k\in\mathbf{F}_q$ である．任意の多項式行列 $N\in\mathbf{F}_q[x_1,\ldots,x_k]^{n\times l}$ と任意の多項式列ベクトル $\boldsymbol{g}\in\mathbf{F}_q[x_1,\ldots,x_m]^k$ に対し，$N(\boldsymbol{g})\in\mathbf{F}_q[x_1,\ldots,x_m]^{n\times l}$ を，N に対する $\boldsymbol{g}$ の代入と定義する．

2.2 多変数公開鍵暗号の一般形

多変数公開鍵暗号の一般形を以下に記述する．平文，暗号文をそれぞれ列ベクトル $\boldsymbol{p}=(p_1,\ldots,p_k)^T\in\mathbf{F}_q^k, \boldsymbol{c}=(c_1,\ldots,c_n)^T\in\mathbf{F}_q^n$ と表す．公開鍵は，パラメータ q,k と多項式列ベクトル $\boldsymbol{E}\in\mathbf{F}_q[x_1,\ldots,x_k]^n$ である．暗号化は，$\boldsymbol{p}$ から $\boldsymbol{c}$ への以下の変換である：

$$\boldsymbol{c}=\boldsymbol{E}(\boldsymbol{p}).$$

秘密鍵を用いることにより，与えられた $\boldsymbol{c}\in\mathbf{F}_q^n$ に対し，$(x_1,\ldots,x_k)$ を変数とする方程式系 $\boldsymbol{E}=\boldsymbol{c}$ を効率的に解くことができる．それゆえ，この公開鍵暗号が安全であるためには，秘密鍵を知らずに，任意の $\boldsymbol{c}$ から $\boldsymbol{p}$ を多項式時間で求められないように，$\boldsymbol{E}$ を構成しなければならない．

以下では，正当な受信者 Bob が秘密鍵を保有し，送信者 Alice が暗号文 $\boldsymbol{c}=\boldsymbol{E}(\boldsymbol{p})$ を Bob に送信する場合を考える．Bob は秘密鍵を用いて，Alice が送信した暗号文 $\boldsymbol{c}$ から，容易に平文 $\boldsymbol{p}$ を得ることができる．一方で，秘密鍵を知らない盗聴者 Catherine に対し，$\boldsymbol{c}$ から $\boldsymbol{p}$ を得ることが困難でなければならない．

多くの多変数公開鍵暗号系について，その公開鍵多項式列ベクトル $\boldsymbol{E}\in\mathbf{F}_q[x_1,\ldots,x_k]^n$ は以下のような形をなす：

$$\boldsymbol{E}=B_0\boldsymbol{G}(A_0\boldsymbol{x}). \tag{1}$$

ここで，$\boldsymbol{x}=(x_1,\ldots,x_k)^T\in\mathbf{F}_q[x_1,\ldots,x_k]^k$ である．A_0,B_0 は，正則行列であり，それぞれ $\mathbf{F}_q^{k\times k}, \mathbf{F}_q^{n\times n}$ の要素である．$\boldsymbol{G}$ は $\mathbf{F}_q[x_1,\ldots,x_k]^n$ の多項式列ベクトルであり，$\boldsymbol{G}$ の変数 $x_1,\ldots,x_k$ に多項式列ベクトル $A_0\boldsymbol{x}\in\mathbf{F}_q[x_1,\ldots,x_k]^k$ を代入したものである．Bob は A_0,B_0 を秘密にし，（ある暗号系では，$\boldsymbol{G}$ も秘密とする）式 (1) の右辺を整頓した結果を公開鍵 $\boldsymbol{E}$ として公開する．$\boldsymbol{E}$ のサイズが大きくならないようにするため，$\boldsymbol{G}$ の次数は 2 以下であるのが普通である．このような暗号系を 2 次多変数公開鍵暗号系と呼ぶ．

3. 持駒行列による多変数公開鍵暗号の汎用的安全性向上手法の基本形

$\mathcal{K}$ を，公開鍵多項式が $\boldsymbol{E}\in\mathbf{F}_q[x_1,\ldots,x_k]^n$ である，任意の 2 次多変数公開鍵暗号系とする．$\mathcal{K}$ の安全性を強化するため，$\tilde{\mathcal{K}}$ の公開鍵 $\tilde{\boldsymbol{E}}\in\mathbf{F}_q[x_1,\ldots,x_k]^t$ を，$\mathcal{K}$ の公開鍵 $\boldsymbol{E}$ から，以下のように構成する：

$$\tilde{\boldsymbol{E}}\equiv S\boldsymbol{E}+R\boldsymbol{X}. \tag{2}$$

ここで $\boldsymbol{X}$ を，$\mathbf{F}_q[x_1,\ldots,x_k]$ の次数 2 以下のすべての単項式をある順序に従って並べたものからなるベクトルとする．すなわち，一つの例として，以下のようになる：

$$\boldsymbol{X}\equiv(x_1x_1,x_1x_2,\ldots,x_{k-1}x_k,x_kx_k,x_1,x_2,\ldots,x_k,1)^T.$$

S,R はそれぞれ $\mathbf{F}_q^{l\times n}, \mathbf{F}_q^{l\times t}$ の行列である．また，t は $\boldsymbol{X}$ の要素数であり，$q\geq 3$ に対して $t=\binom{k+2}{2}=(k^2+3k+2)/2$ である(注1)．項 $R\boldsymbol{X}$ は $\tilde{\boldsymbol{E}}$ を乱雑化する役割を果たす．それゆえ，攻撃者によって，$\tilde{\boldsymbol{E}}$ から $\boldsymbol{E}$ あるいは，$\boldsymbol{E}$ と等価な，すなわち Alice の平文を得るのに十分な多項式列ベクトルを切り分けられないように，R を構成する必要がある．$\tilde{\mathcal{K}}$ の平文は $\mathcal{K}$ と同じく $\mathbf{F}_q^k$ のベクトルである．$\tilde{\mathcal{K}}$ の任意の平文 $\boldsymbol{p}\in\mathbf{F}_q^k$ に対応する暗号文を $\tilde{\boldsymbol{c}}=\tilde{\boldsymbol{E}}(\boldsymbol{p})\in\mathbf{F}_q^l$ とする．

行列 S,R に加えて，$\tilde{\mathcal{K}}$ の秘密鍵として持駒行列 $M\in\mathbf{F}_q^{n\times l}$ を導入する．鍵生成においては，行列 R,M,S を順に，以下の 3 つの条件をみたすように生成する．

[条件 1]　$l\geq n+\operatorname{rank}R$. □

[条件 2]　$MR=0$ かつ $\operatorname{rank}M=n$. □

[条件 3]　$MS=I_n$，ここに I_n は $\mathbf{F}_q^{n\times n}$ の単位行列. □

(注1)：$q=2$ の場合，いわゆる field equation $x_i^2=x_i (i=1,\ldots,k)$ を用いて，$\boldsymbol{X}$ から単項式 $x_1^2,\ldots,x_k^2$ を取り除くことができる．このとき $t=(k^2+k+2)/2$ となる．

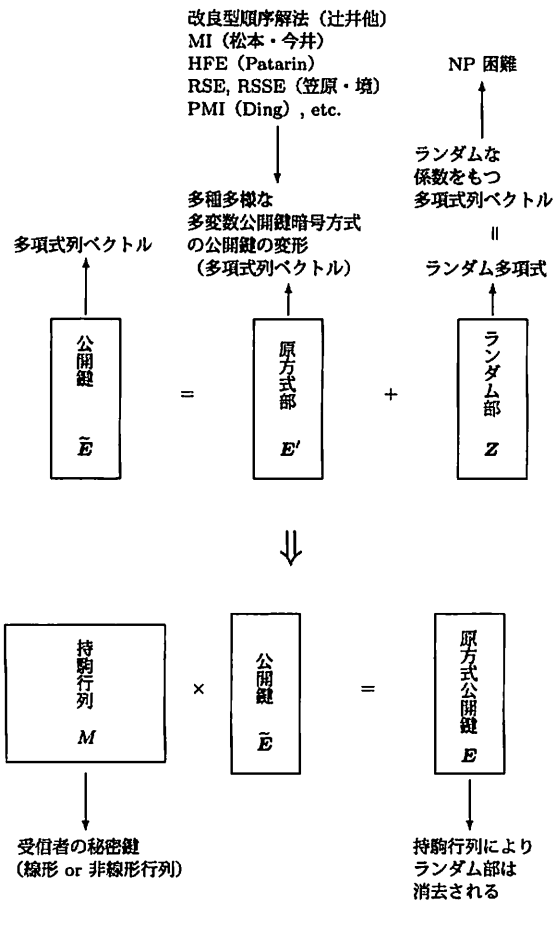

図 1　持駒行列の概念

これらの条件により，$\tilde{E}$ の左から持駒行列 M を乗じた結果が，原方式の公開鍵 E となる：

$$M\tilde{E} = E \tag{3}$$

これは，持駒方式全般に対する必要条件である．

$\tilde{\mathcal{K}}$ の公開鍵は $(q, k, \tilde{E})$ の組であり，秘密鍵は持駒行列 M および原方式 $\mathcal{K}$ の秘密鍵である．$\tilde{\mathcal{K}}$ の復号は，以下のように行う．式 (3) より，まず，平文 p に対する暗号文 $\tilde{c}$ の左から M を乗じて，$c \equiv E(p) = M\tilde{c}$ を得る．次に，$\mathcal{K}$ の秘密鍵を用いて，平文 p を得る．

4. 非線形持駒行列の構成法

- パラメータ：

（1） 原方式に関するパラメータ

- q: 原方式を構成する有限体の位数
- k: 原方式の平文変数の個数
- n: 原方式の公開鍵多項式の数

（2） 非線形持駒方式に関するパラメータ

- n_0: 多項式列ベクトル L_0 の次元 $(n_0 \leq n)$
- l_d: ランダム項ベクトル d の次元，非線形持駒行列 N の列サイズ $(l_d \geq n_0)$
- m: 補助情報ベクトル a の次元
- h: ランダム項ベクトル r の次元
- $g = l_d + n + m + h$: 公開鍵多項式の数

n, n_0 について，$0 < \alpha \leq 1$ に対し，$n_0 = \alpha n$ とする．l_d に関する条件より $l_d \geq n_0 = \alpha n$ となり，$g = l_d + n + m + h \geq (\alpha+1)n + m + h$ から $n/g < 1/(\alpha+1)$ となる．$k = n$ の原方式を考えると，いわゆる伝送効率 $k/g < 1/(\alpha+1)$ となる．特に $n_0 = n$ すなわち $\alpha = 1$ とした場合，$k/g < 1/2$ となり，伝送効率が悪くなる．

- 秘密鍵：

（1） 原方式の秘密鍵

（2） $B \in \mathbf{F}_q^{g \times g}$

（3） $\boldsymbol{a} \in \mathbf{F}_q[x_1, \ldots, x_k]^m$

（4） $\boldsymbol{H} \in \mathbf{F}_q[x_1, \ldots, x_m]^m$

（5） $\boldsymbol{d} \in \mathbf{F}_q[x_1, \ldots, x_m]^{l_d}$

（6） $\boldsymbol{r} \in \mathbf{F}_q[x_1, \ldots, x_k]^h$

（7） $S_0 \in \mathbf{F}_q[x_1, \ldots, x_m]^{l_d \times n_0}$

（8） $\boldsymbol{L}_0 \in \mathbf{F}_q[x_1, \ldots, x_k]^{n_0}$

（9） $\boldsymbol{Q} \in \mathbf{F}_q[x_1, \ldots, x_{n_0}]^n$

ここで各記号の意味は次の通りである．

- B: 正則行列．
- $\boldsymbol{a}$: 非線形持駒行列（平文に依存する要素を含む）を正当な受信者が構成する際に必要な平文（実際には乱数）情報を代入するための m 次元多項式列ベクトル（各要素（多項式）の次数は 1 以下）．
- $\boldsymbol{H}$: 逆変換が容易な 2 次変換（MI 暗号の公開鍵多項式を用いた変換など）を表す多項式列ベクトル
- $\boldsymbol{d}$: $S(\boldsymbol{a})\boldsymbol{L}$ を保護し，かつ公開鍵多項式を総体的にランダム化するための 2 次多項式列ベクトル
- $\boldsymbol{r}$: 公開鍵多項式を総体的にランダム化するための 2 次多項式列ベクトル
- S_0: ランダムな 1 次多項式を要素とする $l_d \times n_0$ 非線形行列
- $\boldsymbol{L}_0$: ランダムな 1 次多項式列ベクトル
- $\boldsymbol{Q}$: $\boldsymbol{E} + \boldsymbol{Q}$ という形で $\boldsymbol{E}$ を直接ランダム化し，公開鍵多項式を総体的にランダム化するための 2 次多項式列ベクトル

以上のようなパラメータ設定により，$\boldsymbol{H}(\boldsymbol{a})$ ベクトルのみが構造を有し，$\boldsymbol{E} + \boldsymbol{Q}(\boldsymbol{L}_0)$ は単ランダム多項式列ベクトルであり，$\boldsymbol{r}$ 及び $S(\boldsymbol{a})\boldsymbol{L} + \boldsymbol{d}(\boldsymbol{a})$ はランダム多項式列ベクトルである．このような工夫により，公開鍵多項式列ベクトルの次数を 2 次に抑えると共に，ランダム性を増大させている．

- 公開鍵：

$$\tilde{\boldsymbol{E}} = B \begin{pmatrix} S(\boldsymbol{a})\boldsymbol{L} + \boldsymbol{d}(\boldsymbol{a}) \\ \boldsymbol{E} + \boldsymbol{Q}(\boldsymbol{L}_0) \\ \boldsymbol{H}(\boldsymbol{a}) \\ \boldsymbol{r} \end{pmatrix}$$

ここに，$S = \begin{pmatrix} S_0 & O_{l_d, n-n_0} \end{pmatrix}$, $\boldsymbol{L} = \begin{pmatrix} \boldsymbol{L}_0 \\ \boldsymbol{0}_{n-n_0} \end{pmatrix}$

- 平文：$\boldsymbol{p} = (p_1, \ldots, p_k)^T \in \mathbf{F}_q^k$
- 暗号文：$\widetilde{\boldsymbol{c}} = (\widetilde{c}_1, \ldots, \widetilde{c}_g)^T \in \mathbf{F}_q^g$
- 暗号化：$\widetilde{\boldsymbol{c}} = \widetilde{\boldsymbol{E}}(\boldsymbol{p})$
- 復号：

(1) $\boldsymbol{w} = (w_1, \ldots, w_g)^T = B^{-1}\widetilde{\boldsymbol{c}}$.

- $\boldsymbol{w}_1 = (w_1, \ldots, w_{l_d})^T$.
- $\boldsymbol{w}_2 = (w_{l_d+1}, \ldots, w_{l_d+n})^T$.
- $\boldsymbol{w}_3 = (w_{l_d+n+1}, \ldots, w_{l_d+n+m})^T$.
- $\boldsymbol{w}_4 = (w_{l_d+n+m+1}, \ldots, w_g)^T$.

(2) $\boldsymbol{a}(\boldsymbol{p}) = \boldsymbol{H}^{-1}(\boldsymbol{w}_3)$.

(3) $N(\boldsymbol{p})S(\boldsymbol{a}(\boldsymbol{p})) = \begin{pmatrix} I_{n_0} & O_{n_0,n-n_0} \\ O_{n-n_0,n_0} & O_{n-n_0,n-n_0} \end{pmatrix}$ となる $N(\boldsymbol{p}) \in \mathbf{F}_q^{n \times l_d}$（非線形持駒行列）を求める.

(4) $\boldsymbol{L}(\boldsymbol{p}) = N(\boldsymbol{p})(\boldsymbol{w}_1 - \boldsymbol{d}(\boldsymbol{a}(\boldsymbol{p}))) = \begin{pmatrix} \boldsymbol{L}_0(\boldsymbol{p}) \\ \boldsymbol{0}_{n-n_0} \end{pmatrix}$.

(5) $\boldsymbol{c} = \boldsymbol{w}_2 - \boldsymbol{Q}(\boldsymbol{L}_0(\boldsymbol{p}))$.

(6) 原方式の秘密鍵を用いて $\boldsymbol{c}$ から $\boldsymbol{p}$ を得る.

なお，この方式において，線形持駒方式と同様に，乱数変数を付加することができる[29]〜[31]．これにより，平文変数の個数が，もとの k から p ($p \leq k$) となり，$(v-p)$ 個の乱数変数が新たに導入され，変数の総数は v となる.

5. むすび

本文では，公開鍵多項式の次数を 2 次に抑える非線形持駒行列の構成法について述べた．現在，いくつかの原方式に対応した持駒方式における乱数効果，及び非線形効果に着目して，グレブナ基底攻撃への耐性について計算実験と考察を進めている．未だ，プリミティブな方式検討の段階であり，IND-CCA レベルの安全性評価は今後の課題である.

文　献

[1] International Workshop on Post-Quantum Cryptography, PQCrypto 2006, Katholieke Universiteit Leuven, Belgium, May 2006. http://postquantum.cr.yp.to

[2] K. Akiyama and Y. Goto, "An algebraic surface public-key cryptosystem," IEICE Technical Report, ISEC2004-80 (2004-11), Nov. 2004.

[3] K. Akiyama and Y. Goto, "A public-key cryptosystem using algebraic surfaces," Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.119-138, May 2006.

[4] D. Coppersmith, J. Stern, and S. Vaudenay, "Attacks on the birational permutation signature schemes," *Proc. CRYPTO '93*, Lecture Notes in Computer Science, vol.773, pp.435-443, Springer, 1993.

[5] 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.

[6] J. Ding, C. Wolf, and B. Yang, "ℓ-invertible cycles for multivariate quadratic public key cryptography," Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.47-66, May 2006.

[7] J. Ding, Private Communication, June 2007.

[8] P. A. Fouque, L. Granboulan, and J. Stern, "Differential cryptanalysis for multivariate schemes," *Proc. EUROCRYPT 2005*, Lecture Notes in Computer Science, vol.3494, pp.341-353, Springer, 2005.

[9] 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資料, JA5-3, Nov. 1987.

[10] 笠原正雄，境隆一，"新しい公開鍵暗号の原理とその一実現法，" 信学技報, ISEC2000-92 (2000-11), Nov. 2000.

[11] M. Kasahara and R. Sakai, "A construction of public key cryptosystem for realizing ciphertext of size 100 bit and digital signature scheme," IEICE Trans. Fundamentals, vol.E87-A, no.1, pp.102-109, Jan. 2004.

[12] M. Kasahara and R. Sakai, "A construction of public-key cryptosystem based on singular simultaneous equations," IEICE Trans. Fundamentals, vol.E88-A, no.1, pp.74-80, Jan. 2005.

[13] M. Kasahara and R. Sakai, "A construction of public-key cryptosystem based on singular simultaneous equations and its variants," IEICE Technical Report, ISEC2005-7 (2005-05), May 2005.

[14] M. Kasahara, "Construction of new classes of SE(g)PKC – Along with some notes on K-Matrix · PKC –," IEICE Technical Report, ISEC2006-4 (2006-05), May 2006.

[15] M. Kasahara, "Constructions of $\mathrm{K_{HLN}}$ · SE(g)PKC on the basis of K-Construction with hidden location noise(HLN)," IEICE Technical Report, ISEC2006-83 (2006-09), Sep. 2006.

[16] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," *Proc. EUROCRYPT '99*, Lecture Notes in Computer Science, vol.1592, pp.206-222, Springer, 1999.

[17] 松本勉，今井秀樹，原島博，宮川洋，"暗号化変換の自明でない表現を用いる非対称暗号系，" 昭 58 信学情報・システム全大, S8-5, Sep. 1983.

[18] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," *Proc. EUROCRYPT '88*, Lecture Notes in Computer Science, vol.330, pp.419-453, Springer, 1988.

[19] T.T. Moh, "A public key system with signature and master key functions," Communications in Algebra, 27(5), pp.2207-2222, 1999.

[20] 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.

[21] A. Shamir, "Efficient signature schemes based on birational permutations," *Proc. CRYPTO '93*, Lecture Notes in Computer Science, vol.773, pp.1-12, Springer, 1993.

[22] 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, Dec. 1985.

[23] 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, Dec. 1986.

[24] 辻井重男，藤岡淳，平山裕介，"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, Feb. 1989.

[25] S. Tsujii, "A new structure of primitive public key cryptosystem based on soldiers in hand matrix," Technical Report TRISE 02-03, Chuo University, Jul. 2003.

[26] S. Tsujii, R. Fujita, and K. Tadaki, "Proposal of MOCHIGOMA(Piece in Hand) concept for multivariate type public key cryptosystem," IEICE Technical Report, ISEC2004-74 (2004-09), Sep. 2004.

[27] S. Tsujii, K. Tadaki, and R. Fujita, "Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: public key without containing all the information of secret key," Cryptology ePrint Archive, Report 2004/366, Dec. 2004. http://eprint.iacr.org/

[28] S. Tsujii, K. Tadaki, and R. Fujita, "Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: public key without containing all the information of secret key," *Proc. SCIS2005*, 2E1-3, pp.487-492, Jan. 2005.

[29] 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—，" *Proc. SCIS2006*, 2A4-1, Jan. 2006.

[30] S. Tsujii, K. Tadaki, and R. Fujita, "Proposal for piece in hand matrix ver.2: general concept for enhancing security of multivariate public key cryptosystems," Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.103-117, May 2006.

[31] S. Tsujii, K. Tadaki, and R. Fujita, "Proposal for piece in hand matrix: general concept for enhancing security of multivariate public key cryptosystems," IEICE Trans. Fundamentals, vol.E90-A, no.5, pp.992-999, May 2007.

[32] L. Wang, B. Yang, Y. Hu, and F. Lai, "A "medium-field" multivariate public-key encryption scheme," *Proc. CT-RSA 2006*, Lecture Notes in Computer Science, vol.3860, pp.132-149, Springer, 2006.