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

2008－CSEC－42（3）
2008/7/24

多変数公開鍵暗号の設計指針
－持駒概念を中心にして－

辻井 重男† 金子 敏信†† 只木 孝太郎††† 五太子 政史††††

†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
††東京理科大学理工学部電気電子情報工学科 〒278-8510 千葉県野田市山崎 2641
†††，††††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@iisec.ac.jp, ††kaneko@ee.noda.tus.ac.jp †††tadaki@kc.chuo-u.ac.jp
††††gotaishi@tamacc.chuo-u.ac.jp

あらまし 多変数公開鍵暗号（MPKC）に対して，軽量性・高速性を主眼とするのではなく，量子コンピュータ時代が到来した場合の安全性を重視する立場から持駒概念による設計指針について考察し，続いて，2層構造の非線形持駒方式の構成法を提案し，更に，その安全性について検討している．

キーワード 公開鍵暗号，多変数公開鍵暗号，持駒概念，量子コンピュータ

Design Policy of MPKC based on Piece in Hand Concept

Shigeo TSUJII†, Toshinobu KANEKO††, Kohtaro TADAKI†††, and Masahito GOTAISHI††††

† Institute of Information Security 2-14-1, Tsuruya-cho, Kanagawa-ku, Yokohama, 221-0835 Japan
†† Tokyo University of Science 2641 Yamazaki, Noda-shi, Chiba, 278-8510 Japan
†††, ††††Research and Development Initiative, Chuo University
Kasuga 1-13-27, Bunkyo-ku, Tokyo, 112-8551 Japan

E-mail: †tsujii@iisec.ac.jp, ††kaneko@ee.noda.tus.ac.jp †††tadaki@kc.chuo-u.ac.jp,
††††gotaishi@tamacc.chuo-u.ac.jp

Abstract Design policy of multivariate public key cryptosystem based on Piece In Hand concept is proposed with focus on quantum computer age. Nonlinear Piece In Hand System with 2 layer structure is also proposed considering security against various known attacks.

Keyword Public key cryptosystem, Multivariate public key cryptosystem, Piece In Hand concept, Quantum computer

1. まえがき—多変数公開鍵暗号方式(MPKC)の誕生と発展

現在，欧米を中心に，MPKCの名の下に活発な研究が展開されている多変数公開鍵暗号方式(Multivariate Public Key Cryptosystems)は日本生まれの暗号である．

先ず，1983年，横浜国大の今井研究室において研究が開始され[27, 30]，今日，MI(Matsumoto-Imai)暗号として，多くの論文に引用されている方式が，1988年のEUROCRYPTにおいて発表された[29, 30]．これは拡大体に対するベクトル表現と多項式表現を巧みに使い分けた方式である．Patarinは，1995年，MI暗号を解読し，翌1996年，MI方式を一般化したHFE(Hidden Field Equation)方式を提案した[32]．

辻井等は，1985年から86年にかけて，回路解析における順序解法に着想を得て，順序解法方式を提案した[37, 38]．これは，秘密鍵となる多項式ベクトルを，1変数，2変数，・・・，n変数と1つずつ増加するように構成することにより，復号者が順次解ける形としておき，この多項式変換を，両側から線形変換して攪拌した多項式ベクトルを公開鍵とする方式である．順序解法方式は，金子等によって解読され[12]，辻井等は，1989年，順序解法の脆弱な要素を核変換と呼ぶ変換を置き換えた方式を提案した[39]．

これらの順序解法方式は，日本語でのみ発表していたため，海外に知られることはなく，1993年，A. Shamirは，順序解法と同様の方式を署名方式として提案した[33]．2004年，持駒方式をIACRのe-Printに掲載した際，参考のため，核変換を用いた方式も付録として掲載しておいた[37]．これをDingが読み，解読法を発表している[9]．

1990年に入り，笠原等は，順序解法を多段・多層化した構成を基本とし，これに様々な工夫を凝らした

MPKCを相次いで発表してきた[15-25]. その基本形は，後に述べるランク攻撃と呼ばれる攻撃法により解析されている[35, 36].

1980年代から90年代初頭にかけての我が国におけるMPKCの研究動機は，量子コンピュータの出現に備えるためというより，RSA暗号の万一の危殆化，あるいはRSA暗号より高速性などの面で勝る方式を探求しようという点にあった．また，フランスなどを中心に，1990年代後半に活発化するMPKCの研究も，MI暗号の署名方式としてのICカードへの実装を考慮して，「軽い・速い」を開発目標としてきた面も強い．

他方，1994年，量子コンピュータにより，素因数分解，及び離散対数問題が解けることが明らかになったことを受けて，量子コンピュータの出現という公開鍵暗号への危機対応，引いては電子社会のEmergency Responseという意識による研究も欧米を中心に，2000年前後から活発になり，2006年には，量子コンピュータ時代の暗号方式に関する国際会議として第1回PQCrypto (Post-Quantum Cryptography)がベルギーで開催され[1]，来る2008年10月には，Ding教授等の主催により第2回PQCryptoが米国で開催される予定である(秋山，辻井がプログラム委員を務めている)．

尚，MPKCに関する解説書がDing等により出版されている[7]．また，Ding等は文献[5]において，MPKCを表1に示すように，4つのタイプに分類している．

表1：MPKCの分類[5]

方式		提案者・論文等
Mixed-Field (or "Big Field")	MIA	MI Scheme A or C* 松本・今井
	HFE	Hidden Field Equation Patarin MIAの一般化
Single-Field (or "True")	UOV	Unbalanced Oil and Vinegar [26] Patarin等
	STS	Stepwise Triangular System 辻井他 Shamir これらの方式は後に現在の形に一般化された

表1以外に、最近はℓ-Invertible Cycle (ℓ-IC)方式[5]やRainbow方式等の混合型方式[7]が提案されている。

2. 安全性の現状を踏まえた設計指針の提案

多変数多項式の解を求める計算はNP完全であることが知られている．しかし，その一方向性に着目してMPKCを構成する場合，落し戸を組み込むため，一般に解読計算量は低下する．MPKCに対する攻撃法としては：

a) 平文を直接求める攻撃法

MPKCにおいては，公開鍵は，平文を変数とする多変数多項式ベクトルで表される．落とし戸構造を解明することなく，公開鍵と暗号文から平文を直接求める方法として，グレブナ基底法，再線形化法，XL法などが知られている[3, 10, 34].

グレブナ基底アルゴリズムは1965年，Buchbergerにより，イデアル所属判定問題を解くためのアルゴリズムとして考案されたものであるが，暗号解析において注目されるようになったのは，Faugereによる F4アルゴリズムが考案された1999年前後からである[10]. このことが，多様な暗号方式の提案と相まって，MPKC研究を活発化したと見ることも出来る．また，多変数からなる単項式を1つの変数で置き換えることなどにより多変数多項式を直接解く手法として，再線形化法，XL法などが提案され[3, 34]，両者の性能比較に関する研究も続けられている[11, 50].

b) ランク攻撃法

MPKCでは，何らかの落とし戸を組み込んだ多変数多項式ベクトルを最後に線形変換した多項式ベクトルを公開鍵とする場合が多い．笠原等による方式の基本形や，T. T. Mohによる TTM方式[31]などの，中間変数を多層的に且つ多段階的に増加させる落とし戸構造を持つ方式(辻井，Shamir等の方式はその特殊な場合と見做せる)をWolf等はSTS構造(Stepwise Triangular Structure)と名づけて，上に述べた線形変換を中間変数多項式ベクトルのランクという観点から，等価的に割り出す方法を提案している[51, 53]. これをランク攻撃と呼んでいる．

c) 差分攻撃

これは，2次の公開鍵多項式の差分をとって得られる1次多項式に隠された構造を利用する攻撃法[36]であり，MI方式を内部的に摂動化した PMI(Perturbed Matsumoto Imai)方式[4]に適用された．Ding(PMI方式の提案者)等はこれを避けるため，いくつかのランダム多項式を付加する方式を提案し，PMI+と名づけている[6]. PMI方式は，復号時間が指数関数的に増加することと引き換えにグレブナ基底攻撃等に対する解読強度を上げる方式である．

d) その他の攻撃法

Gaussian Eliminationや係数等値法などを組み合わせた方法(金子等により，順序解法，及び，順序解法を原方式とする線形持駒方式に適用された攻撃法等[13, 14])，ランク攻撃法と差分攻撃法を組み合わせた攻撃法[8]等が知られている．

一般に，署名方式の方が，暗号(秘匿)方式より安全な方式を構築しやすいが，両者を含めて，安全性の保証された方式は知られていない．

J. Ding等は，文献[5]の Conclusionsにおいて，下記のように述べている：

"We stress that it is still an original sin that no list of possible attacks can be exhaustive"

この表現は，ゲーデルの不完全性定理を連想させる．この定理を物理学者オッペンハイマーは「人間の理性の限界を示すもの」と評したが，むしろ，「自然の摂理を人間の理性が解き明かしたもの」と解釈すべきであろう．その意味で，上記の原罪という表現は実感が籠っている．いずれにしても，総当たり法以外に解のないMPKCを構築するための道のりは遠く，今後多くの研究を重ねる必要があろう．

既に述べたように，MPKCの目指すところは，

① 軽くて速い公開鍵暗号の追求

② 量子コンピュータの出現に対抗し得る公開鍵暗号の探求

という2つがある．両者を満たすことができれば申し分ないが，現在の研究段階ではこれは難しい．

Shamir 等は，文献[35]の結言において，

Multivariate cryptographic schemes are very efficient but have a lot of exploitable mathematical structure. Their security is not fully understood, and new attacks against them are found on a regular basis. It would thus be prudent not to use them in any security-critical applications.

と述べているが，著者の一人（辻井）も全く同感であり，2003 年以来，②の立場から持駒概念を提案し，具体的な方式を考案してきた．即ち，鍵長，暗号文長(伝送効率)等の面での実装性能を，現在のデバイス・LSI のレベルから見て，多少落としたとしても，量子コンピュータ時代を念頭において，安全性を重視すると言う観点から，研究を進めている．

3. 持駒方式の研究経緯

図1:持駒方式の概念

上に述べたように，持駒方式は，こうした研究状況を踏まえて，多様な MPKC の安全性を，例外を除き，可能な限り汎用的に強化することを目的とする方式として，辻井，只木，藤田等によって 2003 年以降，提案されてきたものであり，様々な実現方式を含む概念的方式である[40-49](図 2).

持駒と言う名称は，全ての情報が公開鍵に含まれていない秘密鍵を用意あるいは構成して，復号することを意味しており，線形持駒と非線形持駒に大別される．

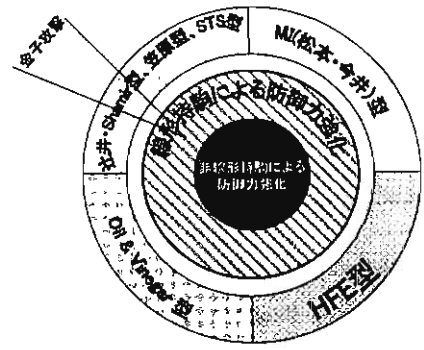


図2: 持駒方式による原方式強化の現状

線形持駒方式は，図 3 に示すような構成であり，原方式として順序解法方式を用いる場合は金子等により解読されている[13].

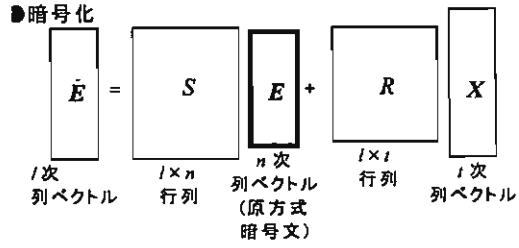


図 3:線形持駒方式

非線形持駒方式は，復号に必要な秘密鍵を構成するための補助情報を，公開鍵に含ませておく方式である．これまで，図 5，6 に示すように，4 層式，及び 3 層式が提案されてきた[47, 48]．いずれの方式も：

① 原方式の公開鍵多項式毎にランダム性の強い多項式（擾乱多項式と呼ぶこととする）を加算して，ランダム性を強め，原方式の持つ構造を弱めることにより，グレブナ基底攻撃や XL 攻撃などの汎用的攻撃に対する耐性を強化する．

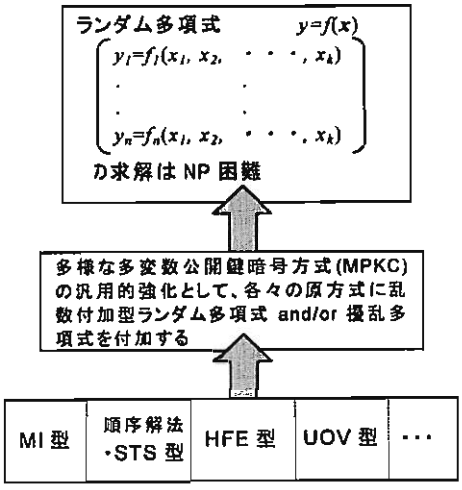
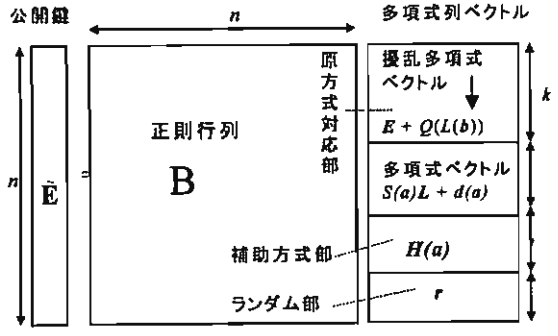


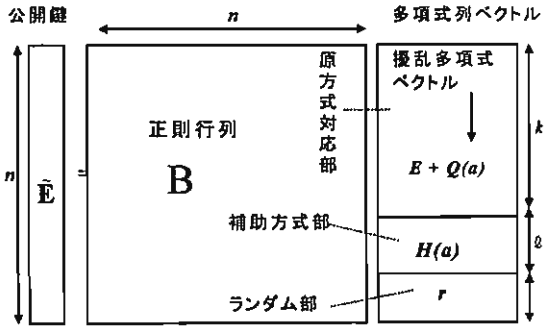
図 4:持駒方式の目標

② 復号のプロセスにおいて，擾乱多項式を除去しなければならないが，そのために，擾乱多項式を構成するための補助情報を暗号文に含ませておく必要がある．補助情報を含ませるための方式を補助方式と呼ぶこととする．



復号手順
①補助方式部より a を得る
②$d(a)$を削除
③$N(a)S(a)= E$(単位行列)となる $N(a)$を構成して $L(b)$を得
④擾乱多項式ベクトル $Q(L(b))$を構成して削除
⑤原方式 E を復号して平文を得る

図 5:非線形持駒方式の発展:4 層構造



復号手順
①補助方式部より a を得る
②擾乱多項式ベクトル $Q(a)$を構成して削除
③原方式 E を復号して平文を得る

図 6:非線形持駒方式の発展:3 層構造

ランダム多項式とは言え，これを原方式に並列に加えることは，グレブナ基底攻撃などの正面攻撃に対する情報をそれだけ余分に与える点では，好ましくはない．しかし，ランダム多項式は復号過程で除去されるので，乱数をふんだんに付加して，変数の数を式数よりかなり大きくして，グレブナ基底攻撃などに対する安全性を逆に高めることが出来る．そこで，線形持駒方式，及び 4 層構成・3 層構成の非線形持駒方式においては，ランダム多項式群に，原方式には含まれない多くの乱数を付加することにより，変数の数を式数より大きくして，グレブナ基底攻撃などに対する安全性を高めている(乱数が含まれているのがランダム多項式だという目印を攻撃者に与えないように，ランダム多項式に含ませる乱数の内，総当り法に耐えられる程度の数の乱数を原方式部にも含ませている)．

4. 2 層式非線形持駒方式の提案

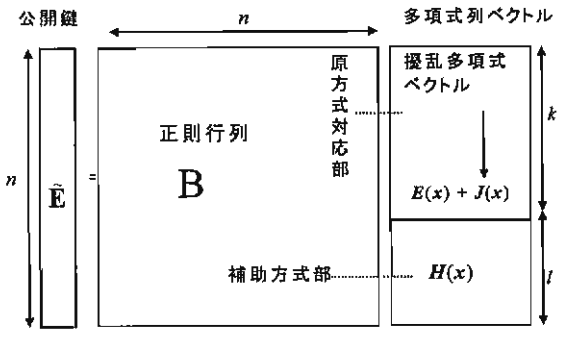
本文では，補助方式部の役割とランダム多項式の差分攻撃への耐性という役割をある多項式群で兼用させることにより，伝送効率(平文長対暗号文長の比率)を向上させることは出来ないだろうかという観点から着想した，図 7 に示すような 2 層構成の非線形持駒方式の一構成法を提案する．本方式では

① 2 次ランダム多項式，即ち「k 個の変数から成る 2 次の多変数多項式における全ての単項式の各係数をランダムに定めた多項式」の代わりに，「ℓ 個のランダムな 1 次の多変数多項式の積」を ℓ 個定めて補助方式とする．

② 復号過程では，上記の 2 次多変数多項式を分解して，ランダムな 1 次多変数多項式を得，これらの組み合わせから得られる k 個($=l(l-1)/2$)の多項式を原方式に対する擾乱多項式として利用する．

尚，補助方式部，及び擾乱多項式部に，多くの乱数を付加することにより安全性を高めることは，4 層，3 層構造の場合と同様に可能であるが，記述を簡単にす

るため，乱数付加をしない場合について述べる．



復号手順
①補助方式部より $H(x)$を得る
②擾乱多項式ベクトル $J(x)$を構成して削除
③原方式 E を復号して平文を得る

図 7:非線形持駒方式の発展:2 層構造

(1) 鍵生成

平文変数 k 次元ベクトル $\boldsymbol{x}$

$$\boldsymbol{x}=(x_1, x_2, \cdots, x_k) \qquad (1)$$

$$x_i \in \mathrm{F}_q \quad i=1, 2, \cdots, k$$

A を k 次正則行列とし，

$$\boldsymbol{v} = A\boldsymbol{x} \qquad (2)$$

とおく．$\boldsymbol{v}$ は k 次元中間変数ベクトルである．

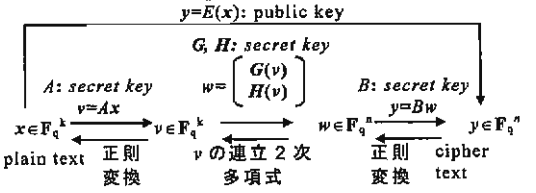


図 8: 二層式非線形持駒方式

図 8 の二層式非線形持駒方式において中間変数領域において，持駒方式を導入しない場合を

$$w_0=E(v) \qquad (3)$$

で表し，これを原方式相当部と呼ぶこととする．

$E(v)$は k 次元多項式ベクトルであるが，これに加える k 次元擾乱多項式ベクトルを $J(v)$で表し，

$$G(v) \underset{def}{=} E(v) + J(v) \qquad (4)$$

と定義する．

$J(v)$は，次のような補助方式部 $H(v)$から非線形操作によって構成され，復号時に除去される．

$$H(v)=\begin{pmatrix} h_1(v)h_l(v)+h_{l-2}(v)h_{l-1}(v)+\alpha_l \\ \vdots \\ h_1(v)h_6(v)+h_4(v)h_5(v)+\alpha_6 \\ h_1(v)h_5(v)+h_3(v)h_4(v)+\alpha_5 \\ h_1(v)h_4(v)+\alpha_4 \\ h_2(v)h_3(v)+\alpha_3 \\ h_1(v)h_3(v)+\alpha_2 \\ h_1(v)h_2(v)+\alpha_1 \end{pmatrix} \qquad (5)$$

ここで $h_i(v)$は

$$h_i(v)=\sum_{j=1}^{k} a_{ij}x_j \quad i=1, 2,,, l \qquad (6)$$

$$a_{ij} \in_R \mathrm{F}_q \qquad (7)$$

で定められるランダムな多変数 1 次多項式である．また，

$$\alpha_i \in_R \mathrm{F}_q \qquad (8)$$

式(3)より，式(3)の $J(v)$を次のように構成する．

$$J(v)=S\begin{pmatrix} h_{l-1}(v)h_l(v)+\beta_k \\ \vdots \\ h_2(v)h_4(v)+\beta_{l+3} \\ h_2(v)h_3(v)+\beta_{l+2} \\ h_1(v)h_l(v)+\beta_l \\ \vdots \\ h_1(v)h_3(v)+\beta_2 \\ h_1(v)h_2(v)+\beta_1 \end{pmatrix} \qquad (9)$$

$$k=\frac{l(l-1)}{2} \qquad (10)$$

S は k 行 k 列の非正則行列である．

$$\boldsymbol{w} \underset{def}{=} \begin{pmatrix} G(v) \\ H(v) \end{pmatrix} = \begin{pmatrix} E(v)+J(v) \\ H(v) \end{pmatrix}$$

は $n(=k+l)$次元多項式ベクトルである．

B を n 次元正則行列とするとき，公開鍵は平文 $\boldsymbol{x}$ に関する n 次元の 2 次多項式ベクトル

$$y = \tilde{E}(x) = Bw$$
$$= B\begin{pmatrix} E(Ax) + J(Ax) \\ H(Ax) \end{pmatrix} \qquad (12)$$

で表される.

公開鍵

q：有限体 F_q の位数
k：平文ベクトルの次元
$\tilde{E}(x)$：n 次元 2 次多項式ベクトル

秘密鍵

A：k 次元正則行列
B：n 次元正則行列 $(n=k+l)$
S：k 次非正則行列
$E(v)$：原方式対応部（k 次元多項式ベクトル）
$J(v)$：k 次元擾乱多項式ベクトル
$H(v)$：l 次元補助多項式ベクトル

(2) 暗号化

k 次元の平文ベクトル p に対して暗号文ベクトル

$$c=\tilde{E}(p) \qquad (13)$$

を得る.

(3) 復号

(i) $w=B^{-1}c$
(ii) w より $H(v)$を求める.
(iii) $H(v)$より $J(v)$を構成する.
(iv) $G(v)$より $J(v)$を除去（減算）して $E(v)$を得る.
(v) 原方式部の復号手順に従って $E(v)$より中間変数ベクトル v の値を求める.
(vi) $p=A^{-1}v$ より平文を得る.

5. 2 層構造の非線形持駒方式の安全性に関する考察

(1) グレブナ基底攻撃等により公開多変数方程式を直接解く攻撃に対する安全性

持駒方式は，もともと，公開鍵に内蔵されている秘密構造を利用せず，公開多変数方程式を，グレブナ基底アルゴリズムや XL 法などにより直接解いて，平文を求める攻撃に対する汎用的安全性強化法として提案されたのである．3 層構造，4 層構造の場合

① ランダム部により多くの乱数を付加する.
② 原方式の各多項式に擾乱多項式を加算する.

の 2 つの対策により，安全性を向上させている.

2 層構造の場合も，上に述べた方式によって，②を実現した．先に述べたように，①についても，3 層構造，4 層構造の場合と同様に，補助方式部，及び擾乱多項式部に，多くの乱数を付加することにより，安全性を向上させることが可能である．但し，2 層構造の場合も 3 節に述べた注意が必要である.

(2) ランク攻撃に対する安全性

2 層構造の場合，補助方式部から擾乱多項式を構成する際，除算を要するので，圧倒的確率で，除算が可能なように，有限体の位数が大きい（例えば，10 進数 100 桁）場合に適用分野を限定している．従って，ランク攻撃は不可能である.

(3) 差分攻撃に対する安全性

補助方式部がランダム性を有しているので，PMI+ 方式と同様，差分攻撃を回避できると考えられるが今後，検討が必要である.

(4) その他の攻撃に対する安全性

補助方式の構成法に脆弱性があると，金子等の攻撃が可能となるので，今後，本文に示した構成法も含めて，補助方式の構成法とその安全性の検討を進める必要がある.

尚，k 次行列 S を非正則としたのは，具体的な攻撃法を想定しているわけではないが，この行列 S が，行列 B に等価的に吸収されることがないようにするためである.

6. 今後の課題

現在のところ，持駒方式全般を通して，解読が報告されているのは，線形持駒方式において，原方式として順序解法を用いた場合のみである．辻井・Shamir 等の方式を含む STS 方式を原方式とする線形持駒方式に対して、一般にランク攻撃が適用し得るか否か、現在検討を進めている。

非線形持駒方式については，解読法は報告されていない.

非線形持駒方式では，原方式は各多項式毎に擾乱を受けているので，持駒による安全性強化の原方式依存度は弱いと考えているが，今後，補助方式部の構成法と併せて，更に考察を深めたい.

具体的には，補助方式部に l-IC Cryptosystem[5]のアイディアを導入した補助方式部の構成法について，検討すると共に，計算機実験を進める予定である.

2 層構成は、4，3 層構成に比べて、伝送効率（暗号文対平文長）の点では優れているが、補助方式部に差分攻撃への耐性を兼用させている点で、劣るか否かが問題である。今後、4，3，2 層構成の比較検討を進めたい。

また、補助方式部の 2 次多項式をランダムな 1 次多項式の積として構成しているので、2 次多項式としてはランダムではないが、このような構造を有するいわば準ランダム多項式のグレブナ基底の計算量が完全な 2 次ランダム多項式に比べて、どのように異なるのかという問題は、本提案方式に止まらず、一般的に興味深い課題である。

終わりに，本研究は，総務省の SCOPE による研究「量子コンピュータの出現に対抗し得る公開鍵暗号の研究」の成果の一つであることを記し，謝意を表しておく．また，文献調査等に協力してくれた藤田亮君（情

報セキュリティ大学院大学博士課程学生)に感謝する.

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, "A public-key cryptosystem using algebraic surfaces," Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.119-138, May 2006.

[3] N. Courtois, A. Klimov, J. Patarin, A. Shamir, "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations," *Proc. EUROCRYPT 2000*, Lecture Notes in Computer Science, vol 1807, pp 392-407

[4] 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.

[5] J. Ding, C. Wolf, and B. Y. 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.

[6] J. Ding and J.E. Gower, "Inoculating multivariate schemes against differential attacks," *Proc. PKC* 2006, Lecture Notes in Computer Science, vol 3958, pp 290-301, Springer, 2006

[7] J. Ding, J. E. Gower, and D. S. Schmidt, Multivariate Public Key Cryptosystems, Springer, 2006.

[8] J. Ding, B. Y. Yang, C. H. Owen Chen, M. S. Chen, and C. M. Cheng, "New differential-algebraic attacks and reparametrization of Rainbow," *Proc. ACNS* 2008, Lecture Notes in Computer Science, vol 5037, pp 242-257, Springer, 2008

[9] J. Ding and J. Wagner, "Cryptanalysis of rational multivariate public key cryptosystems," Proc. SCC 2008, pp.165-178, 2008.

[10]J. C. Faugere, "A new efficient algorithm for computing Grobner bases(F4)," J. Pure Appl. Algebra, vol. 139, pp 61-88, 1999

[11]G. Ars, J. C. Faugere, H. Imai, M. Kawazoe, and M. Sugita, "Comparison between XL and Grobner basis algorithms," *Proc. ASIACRYPT 2004*, Lecture Notes in Computer Science, vol. 3329, pp 338-353, Springer, 2004.

[12]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.

[13]伊藤大介, 福島啓友, 金子敏信," 順序解法を原方式にもつ線形持駒方式の安全性に関する一考察," 信学技報, ISEC2006-30, SITE2006-27(2006-7), July 2006.

[14]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 19 北陸連大, E-36, 2007.

[15]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.

[16]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.

[17]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.

[18]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.

[19]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.

[20]M. Kasahara, "Constructions of 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.

[21]M. Kasahara, "A new class of public Key cryptosystem constructed on the basis of multivariate polynomials randomly generated," IEICE Technical Report, ISEC2007-81 (2007-09), Sep. 2007.

[22]M. Kasahara, "New classes of public key cryptosystem constructed on the basis of multivariate polynomials," Proc. SITA 2007, 12-3, Nov. 2007.

[23]M. Kasahara, "New classes of public key cryptosystem constructed on the basis of multivariate polynomials and random coding," IEICE Technical Report, ISEC2007-118 (2007-12), Dec. 2007.

[24]M. Kasahara, "New classes of public key cryptosystem constructed on the basis of multivariate polynomials and random coding – Another class of K(III)RSE(g)PKC –," IEICE Technical Report, ISEC2007-154 (2008-02), Feb. 2008.

[25]M. Kasahara, "New classes of public key cryptosystem constructed on the basis of multivariate polynomials and error control coding," IEICE Technical Report, ISEC2008-13 (2008-05), May 2008.

[26]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.

[27]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.

[28]H. Imai and T. Matsumoto, "Algebraic methods for constructing asymmetric cryptosystems," Proc. AAECC-3, Lecture Notes in Computer Science, vol.229, pp.108-119, Springer, 1985.

[29]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.

[30]松本勉, 今井秀樹, "署名機能と機密保持機能を効率よく実現する多変数多項式タプル非対称暗号系の構成," 信学論(A), vol.J71-A, no.7, pp.1441-1452, July 1988.

[31]T. T. Moh, "A public key system with signature and

master key functions," Communications in Algebra, 27(5), pp.2207-2222, 1999.

[32]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.

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

[34]A. Kipnis and A. Shamir, "Cryptanalysis of the HFE public key cryptosystem by relinearization," Proc. CRYPTO '99, Lecture Notes in Computer Science, vol.1666, pp.19-30, Springer, 1999.

[35]V. Dubois, P. A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," *Proc. CRYPTO* 2007, Lecture Notes in Computer Science, vol 4622, pp 1-12, Springer, 2007.

[36]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

[37]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.

[38]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.

[39]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.

[40]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.

[41]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.

[42]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/

[43]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.

[44]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.

[45]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.

[46]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.

[47]S. Tsujii, K. Tadaki, and R. Fujita, "Nonlinear piece in hand matrix method for enhancing security of multivariate public key cryptosystems," Proc. SCC 2008, pp. 124-144, 2008

[48]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, IEICE Technical Report ISEC2007-56 (2007-07) Jul. 2007.

[49]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," *Proc. SCIS2008*, 1F1-1, Jan. 2008.

[50]五太子政史, 辻井重男, "有限体上の多変数連立二次方程式に関する新しい求解法の提案," *Proc. SCIS2008*, 3B1-3, Jan. 2008.

[51]C. Wolf, A. Braeken, and B. Preneel, "Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC," *Proc. SCN 2004*, vol. 3352, Lecture Notes in Computer Science, pp 294-309, Springer, 2004

[52]C. Wolf and B. Preneel, "Taxonomy of public key schemes based on the problem of Multivariate Quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005. http://eprint.iacr.org/

[53]C. Wolf, A. Braeken, and B. Preneel, "On the security of stepwise triangular systems," Designs, Codes and Cryptography, vol.40, no.3, pp.285-302, Sep. 2006.