多変数多項式署名方式の暗号方式への応用 *

安田貴徳 †　　櫻井幸一 †‡

† 九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22
yasuda@isit.or.jp

‡ 九州大学数理情報システム情報科学府
819-0395 福岡市西区元岡 744

あらまし　多変数多項式公開鍵暗号は耐量子暗号の候補である。署名方式として Rainbow が提案され、効率的攻撃法は未だに知られていない。本論文では、この Rainbow を暗号方式に応用する方法を提案する。Rainbow では全射多項式写像を用いるのに対し、暗号方式では単射多項式写像が必要となる。どのように Rainbow を単射写像に変えるかを説明する。

Application of a signature scheme in multivariate cryptosystem to encryption scheme

Takanori Yasuda†　　Kouichi Sakurai†‡

†Institute of Systems, Information Technologies and Nanotechonologies.
2-1-22 Fukuoka SRP Center Building 7F, Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN

‡Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819-0395 , JAPAN

Abstract　Multivariate public key cryptsystem (MPKC) is one candidate for post-quantum cryptosystem. For signature scheme Rainbow in MPKC, efficient attacks are yet reported now. In this paper, we propose an application of Rainbow to encryption scheme in MPKC.

1　はじめに

現在、公開鍵暗号の基盤となっている技術は RSA 暗号と楕円曲線暗号である。しかしながら、この 2 つの暗号は量子コンピュータに耐性を持たないため、量子コンピュータが普及する前に量子コンピュータに耐性を持つ公開鍵暗号（耐量子暗号）[1] に公開鍵暗号基盤を移行する必要がある。耐量子暗号の候補としては、格子ベース暗号、コードベース暗号、多変数多項式公開鍵暗号、ハッシュベース暗号が知られている。これらは安全性の数学的根拠の違いによる分類である。格子ベース暗号では NTRU 暗号方式 [10]、コードベース暗号では McEliece 暗号 [12] がその代表である。多変数多項式公開鍵暗号（MPKC）[6] では、ZHFE 方式 [17] と ABC 方式 [18] が暗号方式として知られている。但し、ZHFE 方式と ABC 方式は安全性の解析が乏しく、さらに処理効率も悪い。それゆえ、多変数多項式公開鍵暗号に属する安全で、かつ処理効率の良い暗号方式の開発が課題となっている。

一方、MPKC の署名方式として、Rainbow（方式）[8] が知られている。Rainbow 方式は 2005 年に Ding と Schmidt によって提案され、数々の安全性解析が行われてきた。しかし、未だ致命的な攻撃法が見つかっておらず、また、

*この研究は総務省戦略的情報通信研究開発推進事業（SCOPE）平成 27 年度イノベーション創出型研究開発フェーズ II（no. 0159-0016）の委託の一環である。

署名生成や検証の処理効率も良い。我々は、この署名方式 Rainbow を暗号方式に応用する方法を提案する。MPKC の暗号方式と署名方式では使用する多変数多項式写像が異なる。暗号方式では単射写像を用い、署名方式では全射写像を用いる。Rainbow は署名方式なので全射写像を用いている。これをいかにして単射写像に変換するかが提案方式のポイントである。

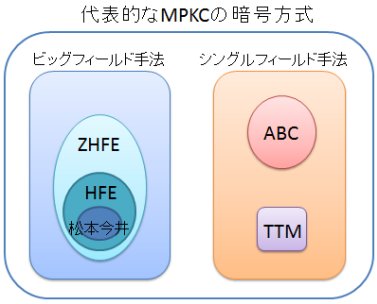
Rainbow の署名生成で必要となる多変数多項式写像の逆写像計算では、数回の線型方程式の解読が行われる。この線型方程式が全て単独解を持つことが保証できれば、Rainbow を暗号方式に転用できる。我々は各線型方程式の方程式数を増やすことで、それを達成した。

Rainbow を暗号方式で利用する場合、もう一つ注意すべき点がある。小さいサイズの別の暗号方式が必要になるという点である。我々は今回 Square[3] と呼ばれる暗号方式を利用した。実際に実装を行い、効率性や鍵長など実験を行っている。

2 MPKC の暗号方式

MPKC の暗号方式として最初に提案されたのは松本・今井方式 [13] である。しかし、これに対し Patarin によって効率的攻撃法が提案された [15]。その後、Patarin は松本・今井方式の拡張として HFE 方式を提案した [16] が、Kipnis, Shamir によって効率的攻撃法が提案された [11]。HFE 方式の変形方式はいくつか提案されたが、それらのほとんどが安全性に問題を抱えていることが分かった。但し、2014 年に提案された HFE 方式の変形方式 ZHFE 方式 [17] に関してはまだ致命的な攻撃法は見つかっていない。

松本今井方式や HFE 方式やその変形方式などは多項式写像の構成に基礎体より十分大きい拡大体を利用している。このような構成法をビッグフィールド手法と言う。一方で、拡大体の力を借りずに方式を構成する方法をシングルフィールド手法と言う。シングルフィールド手法を用いた暗号方式としては TTM 方式 [14] が提案されたが、Rank 攻撃が効率的となることが示されている [9]。シングルフィールド手法としては ABC 方式 [18] が 2013 年に、これの 3 次版である Cubic ABC 方式 [7] が 2014 年に提案され、未だ致命的な攻撃法は見つかっていない。



3 署名方式 Rainbow

3.1 数学的準備

q を素数の冪とするとき、位数 q を持つ可換体が同型を除いてただ一つ存在する。それを $GF(q)$ と表す。ベクトル空間 $GF(q)^{l_1}$ からベクトル空間 $GF(q)^{l_2}$ への写像 ψ がアファイン写像であるとは、$GF(q)$ 上のある l_2 行 l_1 列の線形行列 A と $GF(q)^{l_2}$ 内のあるベクトル v が存在し、ψ が

$$GF(q)^{l_1} \ni \mathbf{c} \mapsto \mathbf{c}.A + v \in GF(q)^{l_2}$$

の形で表されるときを言う。また、アファイン写像が単射写像であるとき、アファイン埋め込み写像と言い、全単射写像であるとき、アファイン変換（同型写像）と言う。

3.2 逆写像が計算可能な 2 次多項式写像

原型の Rainbow[8] による署名方式を説明する。K を位数 q の有限体とし、n を自然数とする。自然数 $t, v_1, \ldots, v_{t+1}$ を

$$0 < v_1 < v_2 < \cdots < v_t < v_{t+1} = n$$

なるものとする。$i = 1, \ldots, t$ に対し、以下のようにおく。

- $S_i = \{1, \ldots, v_i\}, \quad O_i = \{v_i + 1, \ldots, v_{i+1}\},$

- $o_i = v_{i+1} - v_i$.

S_i の個数は v_i で、O_i の個数は o_i である。t をレイヤ数と呼び、$x_1, \ldots, x_{v_1}$ をヴィネガ変数、各 $i = 1, \ldots, t$ に対し、$x_{v_i+1}, \ldots, x_{v_{i+1}}$ を第 i レイヤのオイル変数と呼ぶことにする。よって、変数 $x_1, \ldots, x_n$ はヴィネガ変数と各レイヤのオイル変数に分割されることになる。2 次多項式からなる写像

$$G = (g_{v_1+1}, \ldots, g_n) : K^n \to K^m$$

(但し、$m = n - v_1$) を次の形で与える：

$$g_k(x_1, \ldots, x_n) = \sum_{i \in O_h, j \in S_h} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i,j \in S_h,\, i \le j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in S_{h+1}} \gamma_i^{(k)} x_i + \eta^{(k)} \quad (k = v_1+1, \ldots, n). \tag{1}$$

但し、h は k が属するレイヤ番号、すなわち、“$k \in O_h$” で定まる自然数 $1 \le h \le n$ であり、$\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k)}, \eta^{(k)} \in K$ である。この写像は逆写像を効率的に計算することができる。順番としては、ヴィネガ変数、第 1 レイヤのオイル変数、… 第 t レイヤのオイル変数の順に決定していく。具体的には、任意の $A = (a_i)_{i=v_1+1,\ldots,n} \in K^m$ に対し、$B = G^{-1}(A)$（の一つ）を計算するアルゴリズムは以下のようになる。

Step 1 ヴィネガ変数の値 $b_1, \ldots, b_{v_1}$ はランダムにとる。

Step 2 $h = 1$ から順に t まで、第 h レイヤのオイル変数の値 $b_{v_h+1}, \ldots, b_{v_{h+1}}$ を次のように計算する。

$g_{v_h+1}, \ldots, g_{v_{h+1}}$ は変数 $x_1, \ldots, x_{v_{h+1}}$ に関する 2 次の多項式系である。これに $x_1 = b_1, \ldots, x_{v_h} = b_{v_h}$ なる代入を施すことにより、$x_{v_h+1}, \ldots, x_{v_{h+1}}$ に関する 1 次の多項式系 $\bar{g}_{v_h+1}, \ldots, \bar{g}_{v_{h+1}}$ が作れる。1 次方程式

$$\begin{cases} \bar{g}_{v_h+1}(x_{v_h+1}, \ldots, x_{v_{h+1}}) = a_{v_h+1} \\ \vdots \\ \bar{g}_{v_{h+1}}(x_{v_h+1}, \ldots, x_{v_{h+1}}) = a_{v_{h+1}} \end{cases}$$

の解を計算し、それを $b_{v_h+1}, \ldots, b_{v_{h+1}}$ と置く。（もし解がなければ Step 1 に戻る。）

出力 $B = (b_1, \ldots, b_n)$.

3.3 方式の記述

上の G を両側からランダムなアフィン変換で合成することにより、（G とアフィン変換の情報を知らない者にとって）逆写像が計算困難な 2 次多項式写像が得られると信じられている。このトラップドア付一方向関数を用いて、Rainbow の方式は以下のように記述される。

鍵生成

秘密鍵: G と 2 つのアフィン同型写像 $L : K^m \to K^m,\ R : K^n \to K^n$.

公開鍵: $F = L \circ G \circ R$.

署名生成 メッセージを $\mathbf{M} \in K^m$ とする。$\mathbf{A} = L^{-1}(\mathbf{M})$, $\mathbf{B} = G^{-1}(\mathbf{A})$ (の一つ), $\mathbf{C} = R^{-1}(\mathbf{B})$ の順に $\mathbf{A}, \mathbf{B}, \mathbf{C}$ を計算する。（$\mathbf{A}, \mathbf{C}$ は L, R がアフィン変換なので容易に計算できる。$\mathbf{B}$ は上で説明したアルゴリズムで計算する。）$\mathbf{C}$ が署名である。

検証 $F(\mathbf{C}) = \mathbf{M}$ ならば署名は有効。

この方式を Rainbow$(K; v_1, o_1, \ldots, o_t)$ と表し、$v_1, \ldots, o_t$ を Rainbow のパラメータと呼ぶ。また、G をこの Rainbow の中心写像と呼ぶ。

4 提案方式の概要

提案の暗号方式は以下の 3 つの部分からなる。（1）核となる暗号方式部分、（2）Rainbow 部分、（3）Plus 部分。オリジナルの Rainbow の署名生成では、Step 1 でヴィネガ変数にランダムな値を代入する。これが許されるのは署名方式の場合、1 つの文書に対応する署名の候補が複数存在しても良いからである。しかし、暗号方式の場合、復号化で元の平文に一意的に戻らなければならない。よって、Rainbow を暗号方

式に応用する場合、ヴィネガ変数にランダムな値を代入する部分は別の暗号方式による復号操作に置き換えなければならない。

Rainbow 部分は線型方程式の解読を複数回行う。署名方式の Rainbow ではオイル変数の個数と方程式数を同じものを使用する。しかし、それでは解が複数存在する可能性があるので、方程式数をオイル変数の個数より大きくしたものを使用する。

Plus 部分で Rainbow 部分の安全性を強化する。UOV-Reconciliation 攻撃や RBS 攻撃など、Rainbow に対して提案されている攻撃の効力をなくす目的がある。

5 提案方式の一般的構成

提案方式では以下のパラメータを最初に選択する。

- $K = GF(q)$: 奇標数の有限体（$q \equiv 3 \bmod 4$）
- $S : K^d \to K^d$: 核となる多変数多項式暗号方式の中心写像
- h: 層数
- $o_1, \ldots, o_h$: 各層のオイル変数の個数
- r: 復号成功確率を決める整数
- s: Plus 部分の方程式数
- l: embedding 手法で減らす変数の個数
- $\phi : GF(q^d) \to K^d$: K 上の線形同型写像

5.1 鍵生成

$n = d + o_1 + \cdots + o_h - l$, $m = d + o_1 + \cdots + o_h + hr + s$ とおく。提案方式の公開鍵となるベクトル値多変数多項式写像の変数の個数が n、方程式数が m となる。$n' = d + o_1 + \cdots + o_h$ とおき、$K^{n'}$ 上定義される 3 種類のベクトル値多変数 2 次多項式写像 G_S, G_R, G_P を次のように構成する。

(1) $G_S : K^{n'} \to K^d$ の構成
G_S を S の自然な拡張として、すなわち

$$G_S : K^{d+o_1+\cdots+o_h} \xrightarrow{\text{射影}} K^d \xrightarrow{S} K^d$$

と定義する。

(2) $G_R : K^{n'} \to K^{o_1+\cdots+o_h+hr}$ の構成
まず、各層 $k = 1, \ldots, h$ に対して、ベクトル値多変数 2 次多項式写像 $G_{R,k} : K^{d+o_1+\cdots+o_h} \to K^{o_k+r}$ を構成する : $v_k = d + o_1 + \cdots + o_{k-1}$ とし、$V_k = \{1, 2, \ldots, v_k\}$, $O_k = \{v_k + 1, \ldots, v_k + o_k\}$ とおく。$G_{R,k}$ は $o_k + r$ 個の多変数 2 次多項式成分を持つが、各成分は

$$g(x_1, \ldots, x_{n'}) = \sum_{i \in O_k, j \in V_k} \alpha_{i,j} x_i x_j + \sum_{i,j \in V_k, i \le j} \beta_{i,j} x_i x_j + \sum_{i \in V_k \cup O_k} \gamma_i x_i + \eta$$

の形で選択する。但し、$\alpha_{i,j}, \beta_{i,j}, \gamma_i, \eta$ は K の元であり、$G_{R,k}$ の成分ごとにランダムに選択される。G_R を $G_R = G_{R,1} \| \ldots \| G_{R,h}$ と定義する。

(3) $G_P : K^{n'} \to K^s$ の構成
ランダムな係数を持つ以下の形の多変数 2 次多項式

$$g(x_1, \ldots, x_{n'}) = \sum_{1 \le i \le j \le n'} \alpha_{i,j} x_i x_j + \sum_{1 \le i \le n'} \beta_i x_i + \gamma \quad (\alpha_{i,j}, \beta_i, \gamma \in K)$$

を s 個選択し、それらを並べてベクトル値写像にしたものが G_P である。

上記の (1), (2), (3) を用いて、ベクトル値多変数 2 次多項式写像 $G : K^{n'} \to K^m$ を $G = G_S \| G_R \| G_P$ で定義する。

次に、以下の 2 つをランダムに構成する。

(1) アファイン埋め込み写像 $A_1 : K^n \to K^{n'}$,

(2) アファイン同型写像 $A_2 : K^m \to K^m$.

$F = A_2 \circ G \circ A_1$ とおくとこれは K^n から K^m への多変数 2 次多項式写像となる。

このとき、G, A_1, A_2 を秘密鍵とし、F を公開鍵とする。

5.2 暗号化

平文 M は K^n の元と同一視する。M に対する暗号文 C は以下で得られる。

$$C = F(M) \in K^m.$$

5.3 復号化

$C = (c_1, \ldots, c_m) \in K^m$ を暗号文とする。

Step 1 $B = (b_1, \ldots, b_m) = A_2^{-1}(C)$ を計算。

Step 2 B の一部 $B_S = (b_1, \ldots, b_d)$ に対し、$D_0 = S^{-1}(B_S)$ を計算。

Step 3 k は 1 から h まで順に動き、以下を実行：

(4-1) $B_k = (b_{m_{k-1}+1}, \ldots, b_{m_k})$（但し、$m_t := d + o_1 + \cdots + o_t + tr$ $(t = 1, 2, \ldots)$）に対し、$X_k = (x_{v_{k-1}+1}, \ldots, x_{v_k})$ に関する線型方程式 $G_k(D_{k-1}, X_k) = B_i$ を立てる。

(4-2) 線型方程式を解き、その解を D_k と置く。

Step 4 $D = D_0 \| D_1 \| \cdots \| D_h$ と置く。

Step 5 $M' = A_1^{-1}(D)$ を計算。（M' が復号文）

6 核となる暗号方式の選択

前節では、暗号方式 S を一般的な多変数多項式暗号方式として説明した。ここではその一つとして暗号方式 Square を選択し、暗号方式の一例を構成する。

暗号方式 Square は松本今井方式 [13] の特別な場合で、それ自体は微分攻撃と呼ばれる攻撃が効果的に働くことが既に知られている [2]。しかし、これを提案方式内の暗号方式 S として用いると、Rainbow 方式が微分攻撃に耐性を持つことより、安全性を強化することができる。そこで、以下では S を Square で選択し、固定することにする。

6.1 Square の中心写像と逆写像計算

d を奇数とする。$K = GF(q)$ の d 次拡大体 $GF(q^d)$ は K 上 d 次元のベクトル空間と見なすことができる。よって K-線形同型

$$\phi : GF(q^d) \to GF(q)^d$$

を一つ選び固定する。このとき以下のように写像 G'_S を定義する。

$$G'_S : K^d \xrightarrow{\phi^{-1}} GF(q^d) \ni X \to X^2 \in GF(q^d) \xrightarrow{\phi} K^d.$$

これは K 上 d 変数の d 多項式からなる 2 次斉次多項式写像となることが分かる。暗号方式 Square は中心写像をこの G'_S で定義した方式である。

G'_S の逆写像計算は以下のように行うことができる。

Step 1 G'_S の値 Y_0 に対して、$B_0 = \phi^{-1}(Y_0)$ を計算。

Step 2 $A_0 = \pm B_0^{(q^d+1)/4}$ を計算。

Step 3 $X_0 = \phi(A)$ を計算。

この X_0 は $G'_S(X_0) = Y_0$ を満たす。

注意 1 *Step 2* の計算はバイナリ法あるいはその変形方式で計算量は、$\mathcal{O}(d\log_2(q))\mathbf{M}$（$\mathbf{M}$ は $GF(q^d)$ での 1 回の積を表す。）であるが、$(q^d+1)/4$ を q 進展開し、*GLS*法や *GLV*法、ペアリング計算などで見られる *multi-exponentiation* の技術を用いて計算すると計算量は、$\mathcal{O}(\log_2(q))\mathbf{M}$ に軽減することができる。

6.2 安全性

提案方式の安全性を解析する。考慮すべき攻撃は以下である。

1) 直接攻撃
2) 微分攻撃
3) ランク攻撃
4) Rainbow に対する攻撃（RBS 攻撃、UOV 攻撃、UOV-R 攻撃）

6.2.1 直接攻撃

直接攻撃は公開鍵と暗号文から作られる多変数多項式方程式システムを解読することで平文を求める攻撃である。直接攻撃で最も効率的な

ものはグレブナー基底攻撃である。多変数多項式方程式システムには degree of regularity（正則性の次元）と呼ばれる不変量が定義される。degree of regularity には理論的上限が知られていて、その上限と一致する degree of regularity を持つ多変数多項式方程式システムは、“（半）正則”であるという。（方程式数が変数の個数を上回る場合、“半”が付く。）グレブナー基底計算の計算量は degree of regularity に依存することが知られており、同じ方程式数と変数の個数を持つ多変数多項式方程式システムでは degree of regularity が大きい方が計算量が大きくなる。特に（半）正則な場合、同じ方程式数と変数の個数を持つ多変数多項式方程式システムの中で最も計算量が大きい。以下はいくつかのパラメータに対する degree of regularity の実験結果（の一部）である。（層数 h は全て 1 としている。時間 2 は同じ方程式数と変数の個数を持つランダムシステムの計算時間、DoR=Degree of Regularity.）

- $(q, d, o_1, r, s, l) = (31, 15, 11, 3, 2, 6)$ の場合

時間 (s)	時間 2(s)	DoR	DoR 上限値
9331	8840	6	6

- $(q, d, o_1, r, s, l) = (31, 15, 12, 3, 2, 8)$ の場合

時間 (s)	時間 2(s)	DoR	DoR 上限値
206	204	5	5

- $(q, d, o_1, r, s, l) = (31, 15, 12, 3, 2, 6)$ の場合

時間 (s)	時間 2(s)	DoR	DoR 上限値
34080	41647	6	6

6.2.2 微分攻撃

Square 単体に対しては微分攻撃が効果的であったため、提案方式についても微分攻撃を考察する必要がある。微分攻撃の詳しい説明はしないが、以下の性質を利用した攻撃である。

命題 2 $GF(q^d)$ の任意の元の積と可換な $GF(q^d)$ 上の $GF(q)$ 線形写像は $GF(q^d)$ の元による積写像のみである。

Square 単体の場合、上の命題を用いて $GF(q^d)$ の積写像を多項式時間で構成することができる。それが微分攻撃が効率的となる理由であった。しかし、提案方式の場合、$GF(q^d)$ の元と無関係な変数が存在するため、上の命題を用いて $GF(q^d)$ の積写像を構成することができない。それゆえ、微分攻撃は効果的でない。

6.2.3 ランク攻撃

ランク攻撃とは提案方式のように層構造を持つ方式の各層を行列ランクの違いを利用して決定する攻撃法である。Square の変形方式 Double-Layer Square に対して、ランク攻撃が適用できた [19] ように提案方式にも適用できる。しかし、Double-Layer Square へのランク攻撃の計算量 $\mathcal{O}(q^{l+1})$ であるから l の値を大きく取ることで、ランク攻撃に対する安全性を強化することが可能である。

6.2.4 Rainbow に対する攻撃

RBS 攻撃、UOV 攻撃、UOV-R 攻撃などがあるが、s を 1 以上で取ることで、これらの攻撃に対する安全性を強化することができる。

6.3 Toy Example

以下のパラメータの場合を考える。

- $K = GF(31)$: 奇標数の有限体
- $d = 3$: Square 方式で用いる拡大体の次元
- $h = 2$: 層数
- $(o_1, o_2) = (3, 2)$: 各層のオイル変数の個数
- $r = 1$: 復号成功確率を決める整数
- $s = 1$: Plus 部分の方程式数
- $l = 3$: embedding 手法で減らす変数の個数

このとき、公開鍵 F は K^5 から K^{11} へのベクトル値多変数 2 次多項式写像となる。すなわち、F の成分 F_k $(k = 1, 2, \ldots, 11)$ は

$$F_k(x_1, \ldots, x_5) = \sum_{1 \le i \le j \le 5} \alpha_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le 5} \beta_i^{(k)} x_i + \gamma^{(k)} \quad (\alpha_{i,j}^{(k)}, \beta_i^{(k)}, \gamma^{(k)} \in K)$$

のように表される。次は公開鍵 $F = (F_1, \ldots, F_{11})$ の一例である。

(1) $F_1 = 9x_1^2+2x_1x_2+7x_1x_3+6x_1x_4+18x_1x_5+28x_2^2+21x_2x_3+6x_2x_4+21x_2x_5+4x_3^2+17x_3x_4+11x_4^2+16x_4x_5+2x_5^2+2x_1+28x_2+1x_3+30x_4+12x_5+11$,

(2) $F_2 = 20x_1^2+24x_1x_2+24x_1x_3+14x_1x_4+17x_1x_5+16x_2^2+15x_2x_3+24x_2x_4+14x_3^2+1x_3x_4+21x_3x_5+14x_4^2+6x_4x_5+18x_5^2+10x_1+23x_2+11x_3+24x_4+22x_5+9$,

(3) $F_3 = 9x_1^2+15x_1x_2+19x_1x_3+20x_1x_4+1x_1x_5+3x_2^2+13x_2x_3+15x_2x_4+14x_2x_5+15x_3^2+25x_3x_4+4x_3x_5+24x_4^2+30x_4x_5+19x_1+18x_2+19x_3+4x_4+7x_5+29$,

(4) $F_4 = 14x_1^2+9x_1x_2+6x_1x_3+25x_1x_4+14x_2^2+29x_2x_3+4x_2x_4+8x_2x_5+13x_3^2+19x_3x_4+16x_3x_5+16x_4^2+24x_4x_5+4x_5^2+16x_1+22x_2+2x_3+24x_4+5x_5+12$,

(5) $F_5 = 19x_1^2+16x_1x_2+7x_1x_3+13x_1x_4+3x_1x_5+6x_2^2+15x_2x_3+27x_2x_4+3x_2x_5+6x_3^2+18x_3x_4+10x_3x_5+1x_4^2+1x_4x_5+19x_5^2+20x_1+15x_2+26x_3+25x_4+4x_5+16$,

(6) $F_6 = +18x_1x_2+2x_1x_3+26x_1x_4+8x_1x_5+12x_2^2+10x_2x_3+14x_2x_4+11x_2x_5+16x_3^2+22x_3x_4+18x_3x_5+2x_4^2+14x_4x_5+19x_5^2+2x_1+26x_2+24x_3+16x_4+28x_5+14$,

(7) $F_7 = 1x_1^2+2x_1x_2+13x_1x_3+18x_1x_4+18x_1x_5+8x_2^2+24x_2x_3+16x_2x_4+27x_2x_5+7x_3^2+10x_3x_4+22x_3x_5+27x_4^2+14x_4x_5+30x_5^2+13x_1+28x_2+28x_3+18x_4+3x_5+10$,

(8) $F_8 = 21x_1^2+1x_1x_2+29x_1x_3+7x_1x_4+25x_1x_5+25x_2^2+20x_2x_3+11x_2x_4+9x_2x_5+23x_3^2+28x_3x_4+24x_3x_5+18x_4^2+6x_4x_5+9x_5^2+17x_1+27x_2+21x_3+19x_4+28x_5+22$,

(9) $F_9 = 8x_1^2+6x_1x_2+17x_1x_3+1x_1x_4+29x_1x_5+23x_2^2+15x_2x_3+15x_2x_4+19x_2x_5+5x_3^2+5x_3x_4+22x_3x_5+23x_4^2+8x_4x_5+19x_5^2+28x_1+25x_2+5x_3+6x_4+22x_5+3$,

(10) $F_{10} = 5x_1^2+2x_1x_2+17x_1x_3+12x_1x_4+16x_1x_5+1x_2^2+18x_2x_3+7x_2x_4+21x_2x_5+14x_3^2+9x_3x_4+4x_3x_5+3x_4^2+12x_4x_5+30x_5^2+26x_1+18x_2+25x_3+23x_4+10$,

(11) $F_{11} = 22x_1^2+28x_1x_2+20x_1x_3+1x_1x_4+18x_1x_5+8x_2^2+3x_2x_3+23x_2x_4+8x_2x_5+2x_3^2+15x_3x_4+9x_3x_5+17x_4^2+10x_4x_5+7x_1+2x_2+3x_3+12x_4+27x_5+7$.

この公開鍵を用いた平文 M と暗号文 C の一例は

$$M = (25, 29, 17, 21, 29) \in K^5,$$
$$C = (10, 13, 11, 30, 27, 4, 4, 1, 25, 5, 21) \in K^{11}$$

である。

6.4 実用的パラメータの実行時間

以下のパラメータ（80 ビット安全相当）を考える。

- $K = GF(31)$: 奇標数の有限体
- $d = 33$: Square 方式で用いる拡大体の次元
- $h = 1$: 層数
- $o_1 = 32$: 各層のオイル変数の個数
- $r = 16$: 復号成功確率を決める整数
- $s = 5$: Plus 部分の方程式数
- $l = 16$: embedding 手法で減らす変数の個数

このとき、$(n, m) = (49, 86)$ となる。復号失敗確率は $31^{-16} \simeq 2^{-79}$ となる。異なる平文に対する暗号化と復号化を 100 回行ったときの実行時間の平均は以下のようになった。

暗号化平均時間	0.75 ミリ秒
復号化平均時間	1.06 ミリ秒
秘密鍵長	57103Byte
公開鍵長	69875Byte

実行環境は以下の通り。

OS Microsoft Windows 7 Professional 64bit
CPU Intel(R) Xeon CPU E31270 @ 3.40GHz
メモリ 16.0GB
Compiler Cygwin + gcc version 3.4.4
Language C

6.5 他の暗号方式との比較

ZHFE 方式の暗号化、復号化の平均時間が [17] で見積もられている。

q	n	D_0	暗号化（ms）	復号化（ms）
7	35	57	6	89
11	35	33	3	43

ここで q, n, D_0 は ZHFE 方式を定めるパラメータである。これは数式処理ソフト Magma を用いて実装されたものであるが、復号化が暗号化の 10 倍以上必要となることが分かる。一方、提案方式の復号化は暗号化の 2 倍未満となる。

Pezoldt らは Cubic ABC 方式の鍵長が見積もっている [7]。

q	s	n	秘密鍵長（kB）	公開鍵（kB）
2^8	7	49	72.7	2,115
2^{16}	7	49	145.4	4,230

ここで q, s, n は Cubic ABC 方式を定めるパラメータである。明らかに、提案方式より鍵長が大きくなることが分かる。

7 むすび

多変数多項式公開鍵暗号の処理効率の良い暗号方式を開発した。多変数多項式公開鍵暗号は量子コンピュータに耐性を持つため、次世代の公開鍵基盤の有力候補である。そのなかで、提案方式は秘匿通信などを効率よく実行する次世代暗号として期待できる。

参考文献

[1] Bernstein, D.J., Buchmann, J. and Dahmen, E., “Post Quantum Cryptography”, Springer, Heidelberg 2009.

[2] Billet O., Macario-Rat G., “Cryptanalysis of the Square Cryptosystems”, Asiacrypt’09, Springer LNCS vol. 5912, pp. 451–468, 2009.

[3] Clough C., Baena J., Ding J., Yang B.-Y., Chen M.-S., “Square, a New Multivariate Encryption Scheme”, CT-RSA’09, Springer LNCS vol. 5473, pp. 252–264, 2009.

[4] Clough C. and Ding J., “Secure Variants of Square Encryption Scheme”, PQCrypto’10, Springer LNCS vol. 6061, pp. 154–164, 2010.

[5] Ding, J., “A New Variant of Matsumoto-Imai Cryptosystem through Perturbation”, PKC’04, Springer LNCS vol. 2947, pp. 305–318, 2004.

[6] Ding, J., Gower, J. E. and Schmidt, D. S., “Multivariate Public Key Cryptosystems”, Advances in Information Security 25, Springer, 2006.

[7] Ding J., Petzoldt A., Wang L.-C., “The Cubic Simple Matrix Encryption Scheme”, PQCrypto’14, Springer LNCS vol. 8772, pp. 76–87, 2014.

[8] Ding, J. and Schmidt, D., “Rainbow, a New Multivariable Polynomial Signature Scheme”, ACNS’05, Springer LNCS vol. 3531, pp. 164–175, 2005.

[9] Goubin, L. and Courtois N., “Cryptanalysis of the TTM Cryptosystem”, Asiacrypt’00, Springer LNCS vol. 1976, pp. 44–57, 2000.

[10] J. Hoffstein, J. Pipher, and J.H. Silverman, “NTRU: a ring based public key cryptosystem”. ANTS-III, Springer LNCS vol. 1423, pp. 267–288, 1998.

[11] Kipnis A. and Shamir, “Cryptanalysis of the HFE Public Key Cryptosytem by Relinearlization”, Crypto’99, Springer LNCS vol. 1666, pp. 19–30, 1999.

[12] MacEliece R.J., “A public-key cryptosystem based on algebraic coding theory”, DSN Progress Report 42-44, pp.114-116.Jet Propulsion Lab., Pasadena, CA, 1978.

[13] Matsumoto T. and Imai H., “Public Quadratic Polynomial-tuples for Efficient Signature Verification and Message Encryption”, Eurocrypt’88, Springer LNCS vol. 330, pp. 419–453, 1988.

[14] Moh, T.-T., “A Fast Public Key System with Signature ans Master Key functions”, CrypTEC’99, pp. 63–69.

[15] Patarin J., “Cryptanalysis of Matsumoto and Imai Public Key Scheme of Eurocrypt’88”, Crypto’95, Springer LNCS vol. 963, pp. 248–291, 1995.

[16] Patarin J., “Hidden Field Equations (HFE) and Isomorphism of Polynomials (IP)”, Eurocrypt’96, Springer LNCS vol. 1070, pp. 33–48, 1996.

[17] Porras J., Baena J., and Ding J., “ZHFE, a New Multivariate Public Key Encryption Schem”, PQCrypto 2014, Springer LNCS vol. 8772, pp. 229–245, 2014.

[18] Tao C., Diene A., Tang S., Ding J., “Simple Matrix Scheme for Encryption”, PQCrypto 2013, Springer LNCS vol. 7932, pp. 231–242, 2013.

[19] Thomae E. and Wolf C., “Roots of Square: Cryptanalysis of Double-Layer Square and Square+”, PQCrypto 2011, Springer LNCS vol. 7071, pp. 83–97, 2011.