Vol.2016-DPS-166 No.7
Vol.2016-CSEC-72 No.7
2016/3/3

3乗写像を用いた多変数多項式暗号の提案

安田 貴徳[1,a)]　櫻井 幸一[1,2]

概要：多変数多項式公開鍵暗号は耐量子暗号の候補である．効率的な暗号化・復号化アルゴリズムを持つ多変数多項式公開鍵暗号の暗号方式として SQUARE と呼ばれる方式が提案されていたが，既に微分攻撃が効果的に適用できることが指摘されている．SQUARE では有限体の 2 乗写像を用いているが，本論文ではこれを 3 乗写像に変えた類似の暗号方式 CUBE を提案する．SQUARE のように 2 次多項式を用いた方式は CUBE のように 3 次多項式を用いた方式より安全性は低いが，鍵長は小さくなる．本論文では同じ安全性において 2 次と 3 次の場合で鍵長を比較した．

Proposal of Multivariate Encryption Scheme Using Cubic Map

Takanori Yasuda[1,a)]　Kouichi Sakurai[1,2]

Abstract: Multivariate Public Key Cryptosystems are candidate of post-quantum cryptography. As an encryption scheme in Multivariate Public Key Cryptosystems, SQUARE was proposed, but can be applied the differential attack effectively to. SQUARE employs squaring map over a finite field, whereas we propose an encryption scheme CUBE which employs cubing map in this paper. In general, multivariate encryption scheme using quadratic polynomials is more insecure than that using cubic polynomials, but its key size is less than that for cubic polynomials. In this paper, we compare these key sizes under the same security level.

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）[2] 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 [18]，コードベース暗号では McEliece 暗号 [20] がその代表である．

多変数多項式公開鍵暗号（MPKC）[11] では，多くの暗号方式が提案されてきた．C^* 方式 [21] や HFE 方式 [25]，ABC 方式 [28] などが挙げられる．これら暗号方式の共通の性質として，（多変数）2 次多項式を用いて構成している点がある．しかし，これら 2 次多項式を用いた暗号方式の多くが安全性に問題を持っていることが指摘されている．そこで最近では（多変数）3 次多項式を用いた方式が提案されている．

Cubic ABC 方式 [12] は ABC 方式を 3 次多項式を用いたものに拡張して安全性を強化したものである．また，ZHFE 方式 [26] も 3 次多項式で方式が構成されるが，それを 2 次多項式で表示することによって鍵長を削減している．署名方式では UOV 方式を 3 次に変更した方式も提案されている [23]．但し，3 次多項式を用いた暗号方式の不利な点として，安全性レベルに関する鍵長の増大度が 2 次の場合よりも大きいということが挙げられる．低い安全性レベルでは 3 次多項式を用いた暗号方式の方が鍵長は小さくて済むが，あるレベルを境に 2 次多項式を用いた方が鍵長が小さくなってしまう．

ここでは，最も基本的な 3 次多項式である 3 乗写像を用

[1] 公益財団法人九州先端科学技術研究所 (Institute of Systems, Information Technologies and Nanotechnologies)
[2] 九州大学 (Kyushu Uniersity)
[a)] yasuda@isit.or.jp
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．

いた多変数多項式暗号方式 (CUBE) を提案する．2 次多項式を用いた多変数多項式暗号方式に SQUARE と呼ばれる 2 乗写像を用いた方式があるが，提案方式はその 3 乗版である．SQUARE は既に微分攻撃と呼ばれる攻撃が効果的に適用できることが分かっているが，一方で（多くの場合）SQUARE に付随する多変数多項式方程式系が「正則」と呼ばれる性質を持ち，グレブナー基底計算などを用いた攻撃に強い耐性を持つことが知られている [10].

このグレブナー基底計算などを用いた攻撃は直接攻撃と呼ばれ，あらゆる多変数多項式公開鍵暗号の方式に適用できる攻撃で，安全性レベルを決定するうえで最も基本的な攻撃方法となる．「正則」と呼ばれる性質を持つ多変数多項式方程式系が付随する方式の場合，このグレブナー基底計算攻撃の計算量を最大とすることが知られているが，残念ながら SQUARE を除くほとんどの 2 次多項式を用いた多変数多項式暗号方式は正則ではなく，それが安全性を低下させる要因の一つとなっていた.

提案方式 CUBE が正則かどうかは，まだ調査途中であるが，SQUARE に適用できた微分攻撃は少なくとも自然には拡張できない．本稿では正則な 3 次多項式を用いた多変数多項式暗号方式と正則な 2 次多項式を用いた多変数多項式暗号方式に対して，同じ安全性の下，鍵長の比較を行った.

2. 暗号方式 SQUARE

q を（2 でない）素数べき, n を正の整数で, $q^n \equiv 3 \bmod 4$ とする．（すなわち, $q \equiv 3 \bmod 4$ かつ n は奇数.）$K = GF(q)$ とし，K-線形同型写像

$$\phi : GF(q^n) \xrightarrow{\sim} GF(q)^n$$

を一つ固定する．多変数 2 次多項式写像 $G : K^n \to K^n$ を

$$G : K^n \xrightarrow{\phi^{-1}} GF(q^n) \ni X \mapsto X^2 \in GF(q^n) \xrightarrow{\phi} K^n$$

で定義する．以下をランダムに選ぶ.

- $A_1, A_2 : K^n \to K^n$, アファイン同型写像.

このとき，秘密鍵は A_1, A_2，公開鍵は $F = A_2 \circ G \circ A_1 : K^n \to K^n$.

2.1 暗号化

平文 $M \in K^n$ に対し,

$$C = F(M) \in K^n$$

が暗号文.

2.2 復号化

$B = A_2^{-1}(C)$, $B' = G^{-1}(B)$, $B'' = A_1^{-1}(B')$ の順に計算．B'' が平文と一致する．

2.2.1 $B' = G^{-1}(B)$ の計算方法

$B = A_2^{-1}(C)$, $B'' = A_1^{-1}(B')$ はアファイン同型写像の逆写像なので, $O(n^2)$ で計算可能である．あとは $B' = G^{-1}(B)$ が多項式時間で計算可能であれば，復号計算も多項式時間で可能となる.

$$G^{-1} : K^n \xrightarrow{\phi^{-1}} GF(q^n) \ni X \mapsto X^{1/2} \in GF(q^n) \xrightarrow{\phi} K^n$$

の ϕ^{-1}, ϕ は線形写像なので，平方根（の一つ）$X^{1/2}$ の計算が効率的にできればよい．$D^{1/2}$ $(D \in GF(q^n))$ は以下のベキ乗算で計算できる.

$$D^{1/2} = D^{\frac{q^n+1}{4}}.$$

3. 暗号方式 CUBE

q を（3 でない）素数べきとし，q^n は 9 を法として 1 でないとする．SQUARE の 3 次への自然な拡張として CUBE を定義する.

3.1 鍵生成

$K = GF(q)$ とし，K-線形同型写像

$$\phi : GF(q^n) \xrightarrow{\sim} GF(q)^n$$

を SQUARE の場合と同様に一つ固定する．多変数 3 次多項式写像 $G : K^d \to K^d$ を

$$G : K^n \xrightarrow{\phi^{-1}} GF(q^n) \ni X \mapsto X^3 \in GF(q^n) \xrightarrow{\phi} K^n$$

で定義する．以下を SQUARE の場合と同様にランダムに選ぶ.

- $A_1, A_2 : K^n \to K^n$, アファイン同型写像.

このとき，秘密鍵は A_1, A_2，公開鍵は $F = A_2 \circ G \circ A_1 : K^n \to K^n$.

3.2 暗号化

平文 $M \in K^n$ に対し，暗号文は

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

3.3 復号化

$B = A_2^{-1}(C)$, $B' = G^{-1}(B)$, $B'' = A_1^{-1}(B')$ の順に計算．B'' が平文と一致する.

3.3.1 $B' = G^{-1}(B)$ の計算方法

$B = A_2^{-1}(C)$, $B'' = A_1^{-1}(B')$ はやはりアファイン同型写像の逆写像なので，$O(n^2)$ で計算可能である．あとは $B' = G^{-1}(B)$ が多項式時間で計算可能であれば，復号計算も多項式時間で可能となる．（この詳しい説明は appendix を参照.）

$$G^{-1}: K^n \xrightarrow{\phi^{-1}} GF(q^n) \ni X \mapsto X^{1/3} \in GF(q^n) \xrightarrow{\phi} K^n$$

の ϕ^{-1}, ϕ は線形写像なので，3 乗根（の一つ）$X^{1/3}$ の計算が効率的にできればよい．$D^{1/3}$ $(D \in GF(q^n))$ は以下のベキ乗算で計算できる．

$$D^{1/3} = D^s,$$

$$\begin{cases} s \equiv 1/3 \bmod q^n - 1 & \text{if } q^n \not\equiv 1 \bmod 3, \\ s = \frac{q^n+2}{9} & \text{if } q^n \equiv 7 \bmod 9, \\ s = \frac{q^n+5}{9} & \text{if } q^n \equiv 4 \bmod 9. \end{cases}$$

4. SQUARE および CUBE の鍵長

SQUARE および CUBE の秘密鍵，公開鍵はいずれも体 F 上の多項式写像で表される．すなわち，鍵はその係数の集合となる．体の元の個数による秘密鍵長，公開鍵長は以下のようになる：

SQUARE:

秘密鍵長

$$2n^2 + 2n \text{ 個.}$$

公開鍵長

$$\begin{aligned} &\binom{n+1}{2} + \binom{n}{1} + 1 = \frac{(n+1)n}{2} + n + 1 \\ &= \frac{1}{2}n^2 + \frac{3}{2}n + 1 \text{ 個.} \end{aligned}$$

CUBE:

秘密鍵長

$$2n^2 + 2n \text{ 個.}$$

公開鍵長

$$\begin{aligned} &\binom{n+2}{3} + \binom{n+1}{2} + \binom{n}{1} + 1 \\ &= \frac{(n+2)(n+1)n}{6} + \frac{(n+1)n}{2} + n + 1 \\ &= \frac{1}{6}n^3 + n^2 + \frac{11}{6}n + 1 \text{ 個.} \end{aligned}$$

5. 多変数多項式方程式系を解読する攻撃

MPKC の安全性は多変数多項式方程式系の解読と関係がある．その関係と攻撃計算量について説明する．

5.1 MP 問題

K を位数 q の有限体とする．**MP(Multivariate Polynomial) 問題**は以下のような K 係数多変数多項式方程式系の解読問題を表す．

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0, \\ f_2(x_1, x_2, \ldots, x_n) = 0, \\ \quad \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{cases} \tag{1}$$

特に全ての f_i が 2 次多項式からなるとき，**MQ(Multivariate Quadratic Polynomial) 問題**と呼ぶ．MPKC の安全性は主にこの MP 問題の解読困難性に依存している．以下，MPKC の解読と MP 問題の解読の関係について説明する．

$G = (g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) : \mathbb{F}^n \to K^m$ を多変数多項式からなる写像で**逆写像 G^{-1} の計算が多項式時間で可能**なものとする．（SQUARE や CUBE の G がその例である．）$A_1 : K^m \to K^m$, $A_2 : K^n \to K^n$ をアフィン同型写像とする．$F = (f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) : K^n \to K^m$ を $F = A_1 \circ G \circ A_2$ で定まる多変数多項式写像とする．このとき，G, A_1, A_2 を秘密鍵，F を公開鍵として MPKC の方式が作れる．SQUARE も CUBE もこの基本構造を持っている．G をその方式の**中心写像**という．G が単射の場合，暗号方式となり，平文 P を K^n の元で取り，暗号文 C を $C = F(P)$ で計算する．復号するときは，$F^{-1}(C)$ を計算することになる．

秘密鍵を持たない者にとって，F^{-1} の計算が困難であることが，安全性を確保するために必要となる．すなわち，$D = (d_1, d_2, \ldots, d_m) \in K^m$ に対し，

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = d_1, \\ f_2(x_1, x_2, \ldots, x_n) = d_2, \\ \quad \vdots \\ f_m(x_1, x_2, \ldots, x_n) = d_m \end{cases} \tag{2}$$

の解を求めることが困難である必要がある．(2) は $F - D = \mathbf{0}$ という MP 問題に変形でき，この MP 問題の解読が困難でなければならない．

5.2 MP 問題の解読と正則性

MP 問題を解読する一般的解法として，総当たり法以外ではグレブナー基底計算 [14], [15] と XL 法 [30] が知られている．特に標数が 2 でない MP 問題に対してはグレブナー基底計算が効果的であることが実験的に知られている．グレブナー基底計算アルゴリズムとして，Faugére によって提案された $F4/F5$ アルゴリズム [14], [15] が効率的として知られている．さらに，グレブナー基底計算アルゴリズムの計算量は「正則性」と言う概念と密接に関係している事が知られている．以下で，この正則性について説明する．

大雑把に（かつ幾何学的に）説明すると，多変数多項式列 $(f_1, \ldots, f_m)$ が正則であるとは，アフィン空間 K^n においてイデアル $\langle f_1, \ldots, f_m \rangle$ で定義される部分多様体の次元が $n - m$ になるということである．すなわち，$f_1, \ldots, f_m$ が最小個数の無駄のない定義方程式となっていることを表している．正確な（代数的な）定義は以下のようになる．

Definition5.1 (1) 斉次多項式の列 $(f_1, f_2, \ldots, f_m)$ が正則（regular）であるとは，全ての $i = 1, \ldots, m$ に対し，g

が

$$gf_i \in \langle f_1, \ldots, f_{i-1} \rangle$$

を満たすならば，$g \in \langle f_1, f_2, \ldots, f_{i-1} \rangle$ となるときを言う．(2) 任意の多項式の列 $(f_1, f_2, \ldots, f_m)$ が正則であるとは，$(f_1^h, \ldots, f_m^h)$ が正則になるときを言う．但し，f_i^h は f_i の最高次の斉次部分である．

5.3 正則性の次数

MP 問題に対して「正則性の次数」という不変量が以下のように定義される．

Definition5.2 ([3]) 斉次イデアル $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ の正則性の次数は以下で定義される．

$$d_{\mathrm{reg}} = \min\left\{ d \geq 0 \;\middle|\; \dim_K(\{f \in \mathcal{I} \,|\, \deg(f) = d\}) = \binom{n+d-1}{d} \right\}.$$

Proposition5.3 MP 問題が n 変数，n 多項式で定義され，対応する斉次イデアルが 0 次元となる場合，F_5 アルゴリズムによる体の算術の総個数は以下で抑えられる．

$$O\left(\binom{n+d_{\mathrm{reg}}}{n}^{\omega}\right).$$

ここで $2 < \omega < 3$ である．

正則な MQ 問題に対する正則性の次数は以下のように表されることが知られている [27].

$$[\text{Macaulay bound}] \quad 1 + \sum_{i=1}^{n} (d_i - 1). \qquad (3)$$

ここで，d_i は MQ 問題を定める各多項式 f_i の総次数である．一般に，この (3) は正則性の次数の理論的上限であることが知られている．よって，命題 5.3 より，正則な場合が最も F_5 アルゴリズムの計算量を大きくすることになる．

6. 正則な場合の 2 次と 3 次の方式の鍵長比較

SQUARE に付随する MP 問題は（体の標数を大きくすると）正則となることが知られている [10] よって，正則性の次数は以下のようになる．

$$d_{reg} = 1 + n.$$

一方で，CUBE に付随する MP 問題が正則になるかどうかはまだ分からない（今後の課題）．もし正則となるならば正則性の次数は以下のようになる．

$$d_{reg} = 1 + 2n.$$

この考察は SQUARE や CUBE に制限する必要はない．

一般に次のことが言える．

(1) n 変数，n 個の 2 次多項式から構成される多変数多項式暗号方式で，それに付随する MP 問題が正則となる場合，その正則性の次数は次のようになる．

$$d_{reg} = 1 + n.$$

(2) n 変数，n 個の 3 次多項式から構成される多変数多項式暗号方式で，それに付随する MP 問題が正則となる場合，その正則性の次数は次のようになる．

$$d_{reg} = 1 + 2n.$$

(1) の方式を $\mathcal{S}_2$ と表し，(2) の方式を $\mathcal{S}_3$ と表すことにしよう．今，$\mathcal{S}_2, \mathcal{S}_3$ の安全性が付随する MP 問題の F_5 アルゴリズムによる計算量で決定されると仮定する．このときの n と安全性レベルの関係は表 1 のようになる．表 1 を基に

表 1 $\mathcal{S}_2, \mathcal{S}_3$ のサイズと安全性レベルの関係

安全性レベル	$\mathcal{S}_2$ の n	$\mathcal{S}_3$ の n
80 ビット	21	16
112 ビット	29	22
128 ビット	33	25
160 ビット	42	30
192 ビット	50	36

同じ安全性レベルでの $\mathcal{S}_2, \mathcal{S}_3$ の鍵長の比較を行ったのが表 2, 表 3 である．

表 2 安全性レベルと $\mathcal{S}_2, \mathcal{S}_3$ の秘密鍵長の関係

安全性レベル	$\mathcal{S}_2$ の秘密鍵長	$\mathcal{S}_3$ の秘密鍵長	比（$\mathcal{S}_3/\mathcal{S}_2$）
80 ビット	925 個	544 個	0.59
112 ビット	1740 個	1012 個	0.58
128 ビット	2244 個	1300 個	0.58
160 ビット	3612 個	1860 個	0.51
192 ビット	5100 個	2664 個	0.52

表 3 安全性レベルと $\mathcal{S}_2, \mathcal{S}_3$ の公開鍵長の関係

安全性レベル	$\mathcal{S}_2$ の秘密鍵長	$\mathcal{S}_3$ の秘密鍵長	比（$\mathcal{S}_3/\mathcal{S}_2$）
80 ビット	1265 個	969 個	0.77
112 ビット	2325 個	2300 個	0.99
128 ビット	2975 個	3276 個	1.10
160 ビット	4730 個	5456 個	1.15
192 ビット	6630 個	9139 個	1.39

7. まとめ

3 乗写像を利用した多変数多項式暗号方式 CUBE を提案した．これは 2 乗写像を利用した多変数多項式暗号方式 SQUARE の拡張であり，効率的な復号化アルゴリズムが存在する．また，正則と呼ばれる性質を持つ 2 次多項式からなる多変数多項式暗号方式と 3 次多項式からなる多変数多項式暗号方式を同じ安全性にしたとき，鍵長の比較を理論的に行った．秘密鍵長に関しては安全性レベルを変えても，3 次多項式の場合，2 次多項式の場合に比べて約半分のサイズであった．一方，公開鍵長に関しては，低い安全性レベルの場合は 3 次多項式の場合の方が鍵サイズが小さかったが，大きくなると逆転し，192 ビットでは 3 次多項式の場合は 2 次多項式の場合の約 1.4 倍となった．

今後の課題としては，CUBE の安全性解析が挙げられる．

参考文献

[1] G. Ars, J.-C. Faugère, H. Imai, M. Kawazoe, and M. Sugita, “Comparison Between XL and Gröbner Basis Algorithm”, Asiacrypt 2004, Springer LNCS, vol. 3329, pp. 338-353, (2004).
[2] Bernstein, D.J., Buchmann, J. and Dahmen, E., “Post Quantum Cryptography”, Springer, Heidelberg 2009.
[3] M. Bardet, J.-C. Faugere, and B. Salvy, B.-Y. Yang, “On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations”, MEGA2005, (2005).
[4] L. Bettale, J.-C. Faugère and L. Perret, “Hybrid approach for solving multivariate systems over finite fields”, J. Math. Crypt. vol. 3, pp. 177-197, (2009)
[5] L. Bettale, J.-C. Faugère and L. Perret, “Cryptanalysis of Multivariate and Odd-Characteristic HFE Variants”, PKC 2011, Springer LNCS vol. 6571, pp. 441-458, (2011).
[6] Billet O., Macario-Rat G., “Cryptanalysis of the SQUARE Cryptosystems”, Asiacrypt’09, Springer LNCS vol. 5912, pp. 451–468, 2009.
[7] 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.
[8] Clough C. and Ding J., “Secure Variants of SQUARE Encryption Scheme”, PQCrypto’10, Springer LNCS vol. 6061, pp. 154–164, 2010.
[9] Ding, J., “A New Variant of Matsumoto-Imai Cryptosystem through Perturbation”, PKC’04, Springer LNCS vol. 2947, pp. 305–318, 2004.
[10] J. Ding, C. Clough, and A. Araujo, “Inverting SQUARE Systems Algebraically is Exponential”, Finite Fields and Their Applications, vol. 26, pp. 32-48, (2014).
[11] Ding, J., Gower, J. E. and Schmidt, D. S., “Multivariate Public Key Cryptosystems”, Advances in Information Security 25, Springer, 2006.
[12] Ding J., Petzoldt A., Wang L.-C., “The Cubic Simple Matrix Encryption Scheme”, PQCrypto’14, Springer LNCS vol. 8772, pp. 76–87, 2014.
[13] Ding, J. and Schmidt, D., “Rainbow, a New Multivariable Polynomial Signature Scheme”, ACNS’05, Springer LNCS vol. 3531, pp. 164–175, 2005.
[14] J.-C. Faugère, “A new efficient algorithm for computing Gröbner bases (F_4), J. Pure Appl. Algebra, vol. 139 (1-3), pp. 61-88, (1999).
[15] J.-C. Faugère, “A new efficient algorithm for computing Gröbner bases without reduction to zero F_5, Proceedings of ISSAC, pp. 75-88, (2002).
[16] J.-C. Faugère, “Algebraic cryptanalysis of HFE using Gröbner bases”, Technical Report 4738, INRIA (2003).
[17] Goubin, L. and Courtois N., “Cryptanalysis of the TTM Cryptosystem”, Asiacrypt’00, Springer LNCS vol. 1976, pp. 44–57, 2000.
[18] 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.
[19] Kipnis A. and Shamir, “Cryptanalysis of the HFE Public Key Cryptosytem by Relinearlization”, Crypto’99, Springer LNCS vol. 1666, pp. 19–30, 1999.
[20] 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.
[21] 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.
[22] Moh, T.-T., “A Fast Public Key System with Signature ans Master Key functions”, CrypTEC’99, pp. 63–69.
[23] Nie X., Liu B., Lu G., “Cubic Unbalance Oil and Vinegar Signature Scheme”, Inscrypt’15, 2015.
[24] Patarin J., “Cryptanalysis of Matsumoto and Imai Public Key Scheme of Eurocrypt’88”, Crypto’95, Springer LNCS vol. 963, pp. 248–291, 1995.
[25] Patarin J., “Hidden Field Equations (HFE) and Isomorphism of Polynomials (IP)”, Eurocrypt’96, Springer LNCS vol. 1070, pp. 33–48, 1996.
[26] 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.
[27] P.-J.Spaenlehauer, PhD thesis.
[28] Tao C., Diene A., Tang S., Ding J., “Simple Matrix Scheme for Encryption”, PQCrypto 2013, Springer LNCS vol. 7932, pp. 231–242, 2013.
[29] 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.
[30] B.-Y. Yand and J.-M. Chen, “All in the XL Family: Theory and Practice”, ICISC 2004, Springer LNCS, vol. 3506, pp. 67-86, (2004).

付　　録

A.1 3 乗根の計算方法について

$q'(=q^n)$ を素数べきとする．$q' \equiv 1 \bmod 9$ でない場合に，3 乗根をベキ乗算で計算する方法を 2 つの場合に分けて説明する．

A.1.1 $q' \not\equiv 1 \bmod 3$ の場合

LemmaA.1.1 $q' \not\equiv 1 \bmod 3$ のとき，任意の $\alpha \in GF(q')^\times$ に対し，3 乗根が一意的に存在する．実際，3 乗根 β は以下のようになる．

$$\beta = \alpha^s \quad \text{where} \quad s \equiv 1/3 \bmod q' - 1.$$

証明）$GF(q')^\times$ は位数が 3 で割れない巡回群である． □

A.1.2 $q' \equiv 1 \bmod 3$ かつ $q' \not\equiv 1 \bmod 9$ の場合

LemmaA.1.2 $q' \equiv 1 \bmod 3$ かつ $q' \not\equiv 1 \bmod 9$ ならば,

$$GF(q')^\times \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/((q'-1)/3)\mathbb{Z}. \qquad \text{(A.1)}$$

証明）$GF(q')^\times$ は巡回群で，$(q'-1)/3$ は 3 で割れないから（中国式剰余定理）． □

LemmaA.1.3 上と同じ q' とする．$GF(q') \ni \alpha$ に対し，上補題の同型の行先を $\phi(\alpha) = (c_\alpha, d_\alpha) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/((q'-1)/3)\mathbb{Z}$ とする．このとき,

$$\alpha \text{ が 3 乗元} \iff c_\alpha = 0.$$

証明）$\mathbb{Z}/3\mathbb{Z}$ の元は 3 倍するとどれも 0 であり，$\mathbb{Z}/((q'-1)/3)\mathbb{Z}$ の任意の元は 3 倍元である（$\because$ $(q'-1)/3$ は 3 で割れない）から． □

LemmaA.1.4 上と同じ q' とする．$\alpha \in GF(q')$ を 3 乗元とする．α の 3 乗根の一つ β は次のように計算できる．

$$\beta = \begin{cases} \alpha^{\frac{q'+2}{9}} & q' \equiv 7 \bmod 9, \\ \alpha^{\frac{q'+5}{9}} & q' \equiv 4 \bmod 9. \end{cases}$$

証明）$q' \bmod 9$ によって場合分けするのは，α に関する指数が整数となるようにするため．$q' \equiv 7 \bmod 9$ とし，(A.1) の右の群で考える．上の補題から，$\phi(\alpha) = (0, d_\alpha)$ である．よって，d_α の 1/3 倍元を計算すればよい．一方,

$$3 \cdot \left(\frac{q'+2}{9} \cdot d_\alpha\right) = \frac{q'+2}{3} \cdot d_\alpha = \left(\frac{q'-1}{3} + 1\right) \cdot d_\alpha = d_\alpha,$$

なので, $(q'+2)/9 \cdot d_\alpha$ は d_α の 1/3 倍元となる．$q' \equiv 4 \bmod 9$ の場合も同様である． □