Computer Security Symposium 2012
30 October – 1 November 2012

# 非可換環を用いた多変数多項式署名方式に対するランク攻撃に関する考察

安田貴徳 †　　高木剛 ‡　　櫻井幸一 ∗

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

‡ 九州大学 マス・フォア・インダストリ研究所
819-0395 福岡県福岡市西区元岡 744 番地
takagi@imi.kyushu-u.ac.jp

∗ 九州先端科学技術研究所　　九州大学 大学院システム情報科学研究院
814-0001 福岡県福岡市早良区百道浜 2-1-22　　819-0395 福岡県福岡市西区元岡 744 番地
kouichi@csce.kyushu-u.ac.jp

**あらまし** 多変数多項式公開鍵暗号 (MPKC) は量子コンピュータを用いても解読困難と考えられている公開鍵暗号である。我々は CT-RSA 2011 において非可換環を用いた MPKC の署名方式を提案した。それに対し、Enrico Thomae は非可換環の特性を用いて、ランク攻撃の計算量が軽減できると主張した。本稿では、この攻撃について考察し、提案時に解析した我々の方式の安全性に比べて、総合的な安全性は軽減していないことを説明する。

# On the Rank attacks against multivariate signature scheme using non-commutative rings

Takanori Yasuda†　　Tsuyoshi Takagi‡　　∗ Kouichi Sakurai

†Institute of Systems, Information Technologies and Nanotechnologies
Momochihama 2–1–22, Sawara-ku, Fukuoka-shi, Fukuoka, 814-0001, Japan
yasuda@isit.or.jp

‡Institute of Mathematics for Industry, Kyushu University
Motooka 744, Nishi-ku, Fukuoka-shi, Fukuoka, 819-0395, Japan
takagi@imi.kyushu-u.ac.jp

∗ Institute of Systems, Information Technologies and Nanotechnologies
Momochihama 2–1–22, Sawara-ku, Fukuoka-shi, Fukuoka, 814-0001, Japan,

Department of Informatics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka-shi, Fukuoka, 819-0395, Japan
sakurai@csce.kyushu-u.ac.jp

**Abstract** Multivariate Public Key Cryptosystems (MPKC) are candidates for post-quantum cryptography. We proposed a new signature scheme in MPKC which uses non-commutative rings in CT-RSA 2011. Enrico Thomae insisted that the complexity of Rank attacks against our scheme could be reduced because of some properties of non-commutative. In this paper, we analyze the attacks of Thomae, and then conclude that our scheme yet has equivalent security to that estimated in the original paper that our scheme was proposed.

# 1　はじめに

多項式公開鍵暗号（MPKC）[5] はポスト量子暗号の候補の一つである。MPKC の安全性は多変数方程式の求解の困難性に基づいており、安全面から多変数方程式の変数の個数をある程度増やす必要がある。この多変数方程式の係数集合が秘密鍵や公開鍵に使用されるため鍵長は大きくなる傾向にある。実際、1024 ビット RSA 署名方式と同等の安全性を持つと見られている MPKC の電子署名 Rainbow の場合 [13]、秘密鍵長は RSA の約 150 倍、公開鍵長は約 200 倍となる。

公開鍵暗号において鍵長の削減は重要な研究テーマである。RSA 暗号の場合は鍵長が小さいと格子攻撃が効果的であり [19, 3]、離散対数ベース暗号の場合は Pollard の $\lambda$ 法 [17, 11] が効果的となる [8]。MPKC の場合、前述のように鍵長の削減は実用性から求められる自然な要請であり、解決すべき大きな問題の一つとなっている。実際、様々な方式に対して、その鍵長の削減方法が提案されている [20, 23, 14, 16]。我々が CT-RSA 2012 で提案した NC-Rainbow [24] もその一つである。

秘密鍵長を削減しようと考えた場合、最も単純な方法は秘密鍵を制限することである。既に提案されている秘密鍵長の削減技術も広い意味では秘密鍵を制限していると見なせる。秘密鍵を制限する場合、最も懸念されることは安全性の低下であろう。秘密鍵長と安全性にトレードオフの関係があると考えられるからである。しかし、秘密鍵長の制限にも様々な方法があり、それによって安全性への影響も変わってくる。例えば、ある秘密鍵の制限方法があり、それは攻撃 A に対する安全性を低下させるが、攻撃 B に対しては、全く安全性を低下させないということが起こり得る。この場合、攻撃 A と攻撃 B のどちらが脅威であるかによって、安全性への影響が変わってくる。攻撃 A の方が脅威であれば、安全性の低下は免れないが、他方であれば、総合的な安全性は低下しない可能性がある。安全性の低下が少ない、或いは総合的な安全性を低下させない鍵長の削減が望ましいが、そのような方法についてはまだよく分かっていない。今後の研究課題の一つである。

我々が CT-RSA 2012 で提案した NC-Rainbow は MPKC の電子署名方式の一つ Rainbow[6] の変形方式である。Rainbow は暗号化および復号化の処理が効率的であることが知られているが [4]、他の MPKC の方式同様、秘密鍵長が大きいという問題点を持つ。そこで、我々は Rainbow において有限体 $K$ が用いられている部分を非可換環 $R$ で置き換えることによりこの問題点を克服した [24]。また、同時に我々は Rainbow に対して知られている攻撃に対して、我々の鍵長削減方法を用いたとき安全性が低下するかどうかを検証し、低下しないという結論を得た。一方で、Enrico Thomae は NC-Rainbow に対して、Rainbow への攻撃法であるランク攻撃の計算量を解析し、非可換環の特性により、ランク攻撃の計算量は Raibow に対するそれより、軽減されると主張した [18]。

本稿では Thomae のランク攻撃について考察し、その計算量は Thomae の主張する値よりも大きくなることを説明する。また、例えランク攻撃の計算量が Thomae の主張する通りであったとしても、ランク攻撃よりも直接攻撃などの方が脅威であり、総合的な安全性は NC-Rainbow の提案時に我々が解析した安全性と比較して、軽減していないことを説明する。

# 2　非可換環を用いた MPKC の署名方式

我々が CT-RSA 2012 で提案した NC-Rainbow は Rainbow [6] の変形方式である。その基本アイデアは Rainbow において（可換）有限体を用いた部分を非可換環に置き換えるというものである。逆に、NC-Rainbow の非可換環を有限体に変えれば Rainbow になる。そこで、この節では、NC-Rainbow の方式の記述し、その特別な場合として Rainbow を説明する。

## 2.1　MPKC の署名方式

Rainbow, NC-Rainbow に限らず、MPKC の署名（および暗号）方式は共通の枠組みに沿っ

て構成される。具体的な方式の記述の前にこのことについて簡単に説明する。

MPKC の安全性は有限体 $K$ 上の多変数２次方程式の求解の困難性に基づいている。すなわち、

$$\begin{aligned}\sum_{1\le i\le j\le n} a_{i,j}^{(1)}x_ix_j + \sum_{1\le i\le n} b_i^{(1)}x_i + c^{(1)} &= d_1\\ \sum_{1\le i\le j\le n} a_{i,j}^{(2)}x_ix_j + \sum_{1\le i\le n} b_i^{(2)}x_i + c^{(2)} &= d_2\\ &\vdots\\ \sum_{1\le i\le j\le n} a_{i,j}^{(m)}x_ix_j + \sum_{1\le i\le n} b_i^{(m)}x_i + c^{(m)} &= d_m\end{aligned}$$

なる方程式は一般に求解が難しいという仮定である。これを $\mathbf{F}: K^n \to K^m$ を用いて

$$\mathbf{F}(\mathbf{x}) = \mathbf{d} \tag{1}$$

と書くとしよう。ここで注意すべきは、この (1) の求解が難しいのは、あくまで $\mathbf{F}$ がランダムに選ばれた場合であり、自由に選べるのであれば求解が簡単な $\mathbf{F}$ は構成できるということである。例えば、$\mathbf{F}$ の変数が $x_1,\dots,x_s,y_1,\dots,y_t$ からなり、$y_iy_j$ の形の２次単項式がどの方程式にも表れないと仮定しよう。このとき、$x_1,\dots,x_s$ に適当な値を代入すれば、(1) は $y_1,\dots,y_t$ に関する１次方程式に形を変える。ここからの求解は簡単である。

一般に MPKC の署名（および暗号）方式の秘密鍵としてこのような求解が簡単な多変数２次方程式系が使われる。このとき、公開鍵はこれを基底変換や平行移動を用いて撹乱した多変数２次方程式系で与えられる。公開鍵がランダムに与えられた $\mathbf{F}$ と区別がつかない場合、多変数２次方程式の求解の困難性の仮定から、その方式の安全性が保障される。なお、上で例として与えた求解が簡単な多変数２次方程式系（の拡張）を秘密鍵として用いたものが、Rainbow、および NC-Rainbow である。

### 2.2 非可換環

$K$ を位数 $q$ の有限体とする。$R$ を環とし、次の条件を満たすとする。

(1) $R$ は $K$ 上有限次元のベクトル空間。

(2) $\alpha(vw) = (\alpha v)w = v(\alpha w)$
$(\forall\alpha \in K, \forall v, \forall w \in R)$.

このとき、$R$ を有限次元 $K$ 代数と呼ぶ。さらに、$R$ の元 $v, w$ で $vw \neq wv$ なるものが存在するとき、$R$ は非可換であるという。本稿では有限次元（非可換）$K$ 代数のことを単に（非可換）環と呼ぶことにする。

**例 2.1** (四元数環). $K'$ を $K$ の *2* 次拡大とする。$b \in K^\times$ に対し、非可換環 $Q_q(b)$ が次のようにして定まる。:

$$\begin{aligned}&(\text{集合})\quad Q_q(b) = K'\cdot 1 \oplus K'\cdot e,\\ &(\text{積})\quad e^2 = b,\ \alpha e = e\bar{\alpha}\quad (\forall\alpha \in K').\end{aligned}$$

$Q_q(b)$ は $K$ 上 *4* 次元 *(*$r = 4$*)* である。これを四元数環と呼ぶ。後に、$K = GF(256), b = -1$ の場合の四元数環を用いる。これを $Q_{256}$ と書くことにする。すなわち、$Q_{256} = Q_{256}(-1)$.

以降、非可換環を $R$ を一つ固定し、$r$ で $R$ の $K$ ベクトル空間としての次元を表すことにする。また、$K$ 線形同型写像 $\phi: K^r \xrightarrow{\sim} R$ を固定する。

### 2.3 NC-Rainbow

NC-Rainbow の方式の記述をする。$R$ を 2.2 節でとった ($r$ 次元) 非可換環とする。$n$ を自然数とし、$s, v_1, v_2, \dots, v_{s+1}$ を

$$0 < v_1 < v_2 < \cdots < v_s < v_{s+1} = n$$

なる自然数とする。$i = 1,\dots,s$ に対し、以下のようにおく。

- $S_i = \{1,\dots,v_i\},\quad O_i = \{v_i+1,\dots,v_{i+1}\}$,
- $o_i = v_{i+1} - v_i$.

$S_i$ 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、$x_1,\dots,x_{v_1}$ をヴィネガ変数、各 $i = 1,\dots,t$ に対し、$x_{v_i+1},\dots,x_{v_{i+1}}$ 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 $x_1,\dots,x_n$ 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。

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

を次の非可換多項式の形で表わされるものとする。

$$g_k(x_1,\dots,x_n) = \sum_{i\in O_h, j\in S_h} (x_i\alpha_{i,j}^{(k)}x_j + x_j\alpha_{i,j}^{(k)}x_i) + \sum_{i,j\in S_h} x_i\beta_{i,j}^{(k)}x_j + \sum_{i\in S_{h+1}} (\gamma_i^{(k,1)}x_i + x_i\gamma_i^{(k,2)}) + \eta^{(k)} \quad (k = v_1+1,\dots,n). \tag{2}$$

ここで、$h$ は $k\in O_h$ で定まる自然数 $1\le h\le n$ であり、$\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k,1)}, \gamma_i^{(k,2)}, \eta^{(k)} \in R$ である。

鍵生成、署名生成、検証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 $A_1 : K^m \to K^m,\ A_2 : K^n \to K^n$.（さらに安全にするなら非可換環 $R$ と同型写像 $\phi$ も秘密にする。）

**公開鍵** $F = A_1\circ\phi^{-m}\circ G\circ\phi^n\circ A_2 : K^n \to K^m$.（ここで $\phi^{-m} = (\phi^{-1})^m$ である。）

**署名生成** メッセージを $\mathbf{M}\in K^m$ とする。$\mathbf{a} = (\phi^m\circ A_1^{-1})(\mathbf{M}),\ \mathbf{b} = G^{-1}(\mathbf{a})$（の一つ）, $\mathbf{c} = (A_2^{-1}\circ\phi^{-n})(\mathbf{b})$ の順に $\mathbf{a},\mathbf{b},\mathbf{c}$ を計算する。$\mathbf{c}$ が署名となる。但し、$\mathbf{b} = G^{-1}(\mathbf{a})$ の計算手順は次のとおり。:

**Step 1** $b_1,\dots,b_{v_1}\in R$ をランダムに取る。

**Step 2** $h = 1,\dots,s$ に対して、逐次以下（これを第 $h$ レイヤと呼ぶ）を行う。

$\{g_{v_h+1},\dots,g_{v_{h+1}}\}$ は変数 $x_1,\dots,x_{v_{h+1}}$ に関する非可換多項式系と見れる。この多項式系への $x_1 = b_1,\ \dots,\ x_{v_h} = b_{v_h}$ なる代入により、$x_{v_h+1},\dots,x_{v_{h+1}}$ に関する以下の形の 1 次の非可換多項式系が作れる。

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

の解 $b_{v_h+1},\dots,b_{v_{h+1}}\in R$ を計算する。（解がなければ Step 1 に戻る。）

**Step 3** $\mathbf{b} = (b_1,\dots,b_n)$ と取る。

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

これを NC-Rainbow$(R;\ v_1,o_1,\dots,o_s)$ と表し、$v_1,\dots,o_s$ を NC-Rainbow のパラメータと呼ぶ。

### 2.4 Rainbow と NC-Rainbow の関係

Rainbow は NC-Rainbow で用いた $R$ を（非可換性の条件を外して）有限体 $K$ で取ったものである。Rainbow の場合、$K$ の可換性により、(2) は次のように簡潔に書くことができる。

$$g_k(x_1,\dots,x_n) = \sum_{i\in O_h, j\in V_h} \alpha_{i,j}^{(k)}x_ix_j + \sum_{i,j\in V_h,\, i\le j} \beta_{i,j}^{(k)}x_ix_j + \sum_{i\in V_{h+1}} \gamma_i^{(k)}x_i + \eta^{(k)}. \tag{3}$$

但し、$\alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)}, \gamma_i^{(k)}, \eta^{(k)} \in K$. これ以外は鍵生成、署名生成、検証、いずれも NC-Rainbow と同じである。この Rainbow を（すなわち、$R = K$, パラメータ $v_1,o_1,\dots,o_s$ の NC-Rainbow を）Rainbow$(v_1,o_1,\dots,o_s)$ と表すことにする。

NC-Rainbow を用いることの利点は Rainbow に比べて秘密鍵長が小さいことである。実際、秘密鍵長はそれぞれ次のように書け（体 $K$ の元の個数で勘定）、NC-Rainbow の方が秘密鍵長が小さいことが分かる。

NC-Rainbow$(R;\ v_1,o_1,\dots,o_t)$ **の秘密鍵長**

$$m(m+1) + n(n+1) + \sum_{h=1}^{s} ro_h\left(2v_ho_h + v_h^2 + 2v_{h+1} + 1\right),$$

Rainbow$(rv_1,ro_1,\dots,ro_t)$ **の秘密鍵長**

$$m(m+1) + n(n+1) + \sum_{h=1}^{t} ro_h\left(r^2v_ho_h + \frac{rv_h(rv_h+1)}{2} + rv_{h+1} + 1\right).$$

ここで、比較する NC-Rainbow と Rainbow のパラメータが異なるのは、変数の個数 $n$ と方程式数 $m$ をそろえるためである。実際、上のパラメータを持つ NC-Rainbow は下のパラメータを持つ Rainbow に書き換えることが可能で、この対応は自然である。

非可換環を用いることで秘密鍵長が削減できる理由を簡単に述べておく。非可換環 $R$ の次元を $r$ とすると、“環の正則表現”と言われるものを用いて、$R$ の任意の元は $r \times r$ の正方行列を用いて表すことができる。通常、$r \times r$ の正方行列を表すには $r^2$ 個の体の元が必要であり、一方、非可換環の元は $r$ 個の体の元で表すことができる。すなわち、$K^r$ の元で $K^{r^2}$ の元を表すことが可能である。Rainbow の秘密鍵の記述に正方行列が複数現れるが、それを表すのに非可換環を用いれば、通常より秘密鍵の長さが小さくて済むことになる。

## 3 ランク攻撃

Rainbow の攻撃法の一種にランク攻撃と呼ばれるものがある。公開鍵の 2 次多項式部分の係数を行列で表したとき、特定のランクを持つものを探して、秘密鍵を決定する攻撃方法である。ランク攻撃には最小のランクを利用する MinRank 攻撃とフルランクでない最大ランクを利用する HighRank 攻撃の 2 種類がある。

### 3.1 MinRank 攻撃 ([9, 21, 2])

MinRank 攻撃はヴィネガ変数と第 1 レイヤのオイル変数の張る部分空間を決定する攻撃である。これにより、よりレイヤ数の小さい Rainbow に攻撃を帰着させることができる。以下、(HighRank 攻撃の場合も) Rainbow$(v_1, o_1, \ldots, o_t)$ を考える。中心写像 $G = (g_{v_1+1}, \ldots, g_n)$ に対し、その 2 次部分をそれぞれ $g^{(2)}_{v_1+1}, \ldots, g^{(2)}_n$ と書く。各 $g^{(2)}_i$ はサイズ $n$ の三角行列 $T_i$ を用いて

$$g^{(2)}_i(\mathbf{x}) = \mathbf{x}.T_i.\mathbf{x}^T, \quad (\mathbf{x} = (x_1, \ldots, x_n))$$

のように表すことができる。対称行列 $S_i$ $(i = v_1 + 1, \ldots, n)$ を $S_i = T_i + T_i^T$ により定義し、$\mathcal{A} = \mathrm{Span}_K\{S_{v_1+1}, \ldots, S_n\}$ と置く。MinRank 攻撃では $\mathcal{A}$ の(0 でない)最小ランクを持つ行列を探索する。Rainbow の構成方法から、この最小ランクは $v_1 + o_1$ と一致するとしてよく、この最小ランクを持つ行列の核を計算することにより、ヴィネガ変数と第 1 レイヤのオイル変数の張る部分空間(の補空間)が計算できる。

MinRank 攻撃の大部分は最小ランクを持つ行列を探索する過程に費やされる。この過程の計算は次のようなステップで行われる。

**Step 1** $v \in K^n$ をランダムにとる。
**Step 2** $(\sum_{i=v_1+1}^{n} x_i S_i)v = 0$ なる $\lambda_{v_1+1}, \ldots, \lambda_n$ に関する方程式を解いて、解 $\lambda_{v_1+1}, \ldots, \lambda_n$ を得る。解がなければ Step 1 に戻る。
**出力** $S = \sum_{i=v_1+1}^{n} \lambda_i S_i$.

上のアルゴリズム Step 2 で解が見つかるためには $v$ がヴィネガ変数と第 1 レイヤのオイル変数の張る部分空間の補空間(を $R^{-1}$ で移した空間)に属さなければならない。ヴィネガ変数と第 1 レイヤのオイル変数の張る部分空間の次元は $v_1 + o_1$ であるから、任意の $v \in K^n$ がその補空間に入る確率は $1/q^{v_1+o_1}$ である。方程式を解くための計算も含めると、MinRank 攻撃の計算量は以下のように見積もられる ([21],[13])。

$$q^{v_1+o_1} m(n^2/2 - m^2/6) \text{ 回の積計算.} \tag{4}$$

### 3.2 HighRank 攻撃 ([9, 7, 14])

HighRank 攻撃では MinRank 攻撃とは逆に最後のレイヤのオイル変数の張る空間を特定する。これにより、よりレイヤ数の小さい Rainbow に攻撃を帰着させることができる。行列のなすベクトル空間 $\mathcal{A}$ を MinRank 攻撃の説明で定義したものとする。HighRank 攻撃では $\mathcal{A}$ の(フルランクでない)最大ランクを持つ行列を探索する。Rainbow の構成方法から、この最大ランクは $v_t$ と一致するとしてよく、この最大ランクを持つ行列の核を計算することにより、最後のレイヤのオイル変数の張る部分空間が計算できる。

HighRank 攻撃の大部分は最大ランクを持つ行列を探索する過程に費やされる。この過程の計算は次のようなステップで行われる。

**Step 1** $M \in \mathcal{A}$ をランダムにとる。
**Step 2** $M$ が正則でないかどうか調べる。正則であれば Step 1 に戻る。
**出力** $M$.

一般に $M \in \mathcal{A}$ は $g_k^{(2)} \circ R$ $(k = v_1+1, \ldots, n)$ の線形和で表されるが、$M$ がフルランクでない最大ランクを持つ行列となる場合、この線形和において $g_{v_t+1}^{(2)} \circ R, \ldots, g_n^{(2)} \circ R$ の項は含まれないと仮定してよい。この仮定は $g_k^{(2)}$ の記述（(3) の２次部分）の $\alpha_{i,j}^{(k)}$ 達がランダムに選ばれていることによるものである。$M$ がこのような線形和で表される確率は $1/q^{o_t}$ である。この確率も $\alpha_{i,j}^{(k)}$ 達がランダムに選ばれていることから得られる。

上のアルゴリズムでは、正則かどうかの計算も必要になるので、HighRank 攻撃の計算量は以下のように見積もられる [7, 13]。

$$q^{o_t} n^3/6 \text{ 回の積計算.}$$

# 4 Thomae のランク攻撃の解析

Thomae は NC-Rainbow に対して、さらに詳しくランク攻撃の計算量を解析した [18]。Thomae の解析は $R = Q_q$（$Q_q$ は四元数環 § 2.2）の場合に制限されており、ここでもこの場合のみを扱う。まず、$R$ の $K$-基底 $\{u_1, u_2, u_3, u_4\}$ を固定する。これにより $R$ は４次元空間 $K^4$ と同一視できる。特に、$u_i \gamma u_j$ $(1 \le i, j \le 4, \gamma \in R)$ の形の（非可換）２次多項式は４つの $K^4$ 上の（可換）２次多項式で表すことができる。この４つの２次多項式を $f_1, f_2, f_3, f_4$ としよう。これらの多項式に対して、$x_i x_j$ の係数を $(i, j)$-成分とした行列を $A_1, A_2, A_3, A_4$ と表す。これらは $K$ 係数の $(4 \times 4)$ 正方行列である。Thomae は次のことを示した。

**補題 4.1.** *$A_1, A_2, A_3, A_4$ の張る $K$-ベクトル空間の次元は $q$ が 2 冪のときは 1、それ以外は、3 である。特に、$A_1, A_2, A_3, A_4$ は線形独立ではない。*

この $A_1, A_2, A_3, A_4$ は線形独立ではないという性質はランク攻撃に影響が出る。実際、MinRank 攻撃で説明した最小ランクを持つ行列を探索するアルゴリズムの **Step 2** の方程式の解空間が広がり、解を見つけるための探索回数が削減される。上の補題を使うと、このアルゴリズムの計算量が分かり、以下が言える。

**命題 4.1.** *NC-Rainbow$(R; v_1, o_1, \ldots, o_t)$ を考える。MinRank 攻撃において最小ランクを持つ行列を探索するアルゴリズムの計算量は我々の解析 [24] では、*

$$q^{4v_1+4o_1} m(n^2/2 - m^2/6) \text{ 回の積計算}$$

*であったが、Thomae の解析 [18] では、これが以下に削減される。:*

$$\begin{cases} q^{4v_1+o_1} m(n^2/2 - m^2/6) \text{ 回の積計算} & 2|q \text{ のとき}, \\ q^{4v_1+3o_1} m(n^2/2 - m^2/6) \text{ 回の積計算} & \text{それ以外}. \end{cases}$$

同様にして、HighRank 攻撃に対しても最大ランクを持つ行列を探索するアルゴリズムの **Step 2** に影響が出て、次が言える。

**命題 4.2.** *NC-Rainbow$(R; v_1, o_1, \ldots, o_t)$ を考える。HighRank 攻撃において最大ランクを持つ行列を探索するアルゴリズムの計算量は我々の解析 [24] では、*

$$q^{4o_t} n^3/6 \text{ 回の積計算}$$

*であったが、Thomae の解析 [18] では、これが以下に削減される。:*

$$q^{3o_t} n^3/6 \text{ 回の積計算}$$

これら２つの命題から、Thomae は次の２つを主張している [18]。

**主張 4.1.** *NC-Rainbow$(R; v_1, o_1, \ldots, o_t)$ に対し、MinRank 攻撃の計算量は以下になる。:*

$$\begin{cases} q^{4v_1+o_1} m(n^2/2 - m^2/6) \text{ 回の積計算} & 2|q \text{ のとき}, \\ q^{4v_1+3o_1} m(n^2/2 - m^2/6) \text{ 回の積計算} & \text{それ以外}. \end{cases}$$

**主張 4.2.** *NC-Rainbow$(R; v_1, o_1, \ldots, o_t)$ に対し、HighRank 攻撃の計算量は以下になる。:*

$$q^{3o_t} n^3/6 \text{ 回の積計算}$$

# 5 Thomae のランク攻撃の計算量に関する我々の考察

## 5.1 考察１

Thomae は命題 4.1、4.2 から、主張 4.1、4.2 を結論付けているが、ここにはギャップがある。

なぜなら、命題 4.1、4.2 で計算量を見積もったアルゴリズムは MinRank 攻撃、HighRank 攻撃で必要な計算の一部にすぎないからである。MinRank 攻撃の場合だと、次のようなステップが続く。:

1. 最小ランクを持つ行列を探索するアルゴリズムを使って、行列 $S$ を得る。(これは Thomae の主張した計算量で得ることができる。)
2. $S$ の核を計算することにより、オイル変数 $x_{v_2+1}, \ldots, x_n$ の張る空間を計算する。
3. $v'_1 = v_1 + o_1, o'_1 = o_2, \ldots, o'_{t-1} = o_t$ として、レイヤ数の１つ小さい Rainbow が構成される。(帰着完了)

通常の MinRank 攻撃の場合、$S$ のランクは高い確率で $v_1+o_1$ になるので、オイル変数 $x_{v_2+1}, \ldots, x_n$ の張る空間が正確に計算できる。しかし、NC-Rainbow の場合、補題 4.1 により、$S$ のランクは必ず $v_1+o_1$ より真に小さくなるので、オイル変数 $x_{v_1+o_1+1}, \ldots, x_n$ の張る空間が正確には計算できないことになる。すなわち、Thomae が証明した補題 4.1 が逆に障害となり、MinRank 攻撃が完了しないことになる。HighRank 攻撃も同様のことが言える。

### 5.2 考察２

上の考察で、Thomae の方法だけでは MinRank 攻撃と HighRank 攻撃は完了しないことを説明した。もし、(計算量が無視可能な) 新たなアルゴリズムを追加することにより、命題 4.1、4.2 と、主張 4.1、4.2 のギャップが取り除けたと仮定しよう。すなわち、Thomae の主張する計算量で MinRank 攻撃と HighRank 攻撃が完了すると仮定する。このとき、他の攻撃法との計算量の比較を行うと表 1 のようになる。この表は２レイヤを持つ NC-Rainbow に対して、我々が NC-Rainbow の提案時に解析した安全性レベルと Thomae の（主張する）ランク攻撃の安全性レベルを比較したものである。この表を見て分かるように、Thomae の主張する計算量を認めたとしても、我々が NC-Rainbow の提案時に解析した安全性レベルの方が低く、よって、総合的な安全性は軽減していない。これは、Rainbow において、ランク攻撃より、直接攻撃 [1, 22] や UOV-Reconciliation 攻撃 [7, 13]、Rainbow-Band-Separation 攻撃 [7, 13] の方が脅威であり、計算量にも開きがあることが原因である。

表 1: NC-Rainbow($Q_{256}$; $v_1, o_1, o_2$) の安全性レベルの比較

| | $(5,4,4)$ | $(7,5,5)$ | $(9,6,6)$ |
|---|---|---|---|
| 我々の解析 (bits) | 83 | 96 | 107 |
| MinRank (bits) | 112 | 160 | 208 |
| HighRank (bits) | 96 | 120 | 144 |

## 6 まとめ

我々が CT-RSA2012 において提案した NC-Rainbow に対して、Thomae が行ったランク攻撃の計算量見積もりに関する考察を行った。Thomae の攻撃法だとランク攻撃は完了しないことが分かり、また、何らかの追加アルゴリズムにより完了したとしても、総合的な安全性レベルは軽減されていないことが分かった。今後は、NC-Rainbow を含む鍵長削減技術と安全性との関係を明らかにしていきたい。

**謝辞**　本研究は科研費 若手研究 B（課題番号：24740078）の助成を受けている。また、本研究の一部は、JST 日印研究交流プロジェクト「情報通信と他の分野を結合した複合領域」の支援を受けている。

## 参考文献

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

[2] Billet, O. and Gilbert, H., “Cryptanalysis of Rainbow”, SCN’06, Springer LNCS vol. 4116, pp. 336–347, 2006.

[3] Boneh, D. and Durfee, G., “Cryptanalysis of RSA with Private Key $d$ Less Than $N^{0.292}$”, IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1339–1349, 2000.

[4] Chen, A. I.-T., Chen, M.-S., Chen, T.-R., Cheng, C.-M., Ding, J., Kuo, E. L.-H., Lee, F. Y.-S. and Yang, B. Y., “SSE Implementation of Multivariate PKCs on Modern x86 CPUs”, CHES’09, Springer LNCS vol. 5747, pp. 33–48, 2009.

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

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

[7] Ding, J. Yang, B.-Y., Chen, C.-H. O., Chen, M.-S. and Cheng, C. M., “New Differential-Algebraic Attacks and Reparametrization of Rainbow”, ACNS’08, Springer LNCS vol. 5037, pp. 242–257, 2008.

[8] Galbraith, S. D. and Ruprai, R. S., “Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval”, PKC’10, Springer LNCS vol. 6056, pp. 368–383, 2010.

[9] Goubin, L. and Courtois, N.T., “Cryptanalysis of the TTM Cryptosystem”, ASIACRYPT’00, Springer LNCS vol. 1976, pp. 44–57, 2000.

[10] Kipnis, A. and Shamir, A., “Cryptanalysis of the Oil and Vinegar Signature Scheme”, CRYPTO’98, Springer LNCS vol. 1462, pp. 257–266, 1998.

[11] van Oorschot, P.C. and Wiener, M.J., “Parallel Collision Search with Cryptanalytic Applications”, Journal of Cryptology, vol. 12, pp. 1–28, 1999.

[12] Petzoldt, A., Bulygin, S. and Buchmann, J., “A Multivariate Signature Scheme with a Partially Cyclic Public Key”, Proceedings of the Second International Conference on Symbolic Computation and Cryptography (SCC2010), pp. 229–235, 2010.

[13] Petzoldt, A., Bulygin, S. and Buchmann, J., “Selecting Parameters for the Rainbow Signature Scheme”, PQCrypto’10, Springer LNCS vol. 6061 pp. 218–240, 2010.

[14] Petzoldt, A., Bulygin, S. and Buchmann, J., “CyclicRainbow - A multivariate Signature Scheme with a Partially Cyclic Public Key based on Rainbow”, INDOCRYPT’10, Springer LNCS vol. 6498, pp. 33–48, 2010.

[15] Petzoldt, A., Bulygin, S. and Buchmann, J., “Linear Recurring Sequences for the UOV Key Generation”, PKC’11, Springer LNCS vol. 6571, pp. 335–350, 2011.

[16] Petzoldt, A., Thomae, E., Bulygin, S., and Wolf, C., “Small Public Keys and Fast Verification for Multivariate Quadratic Public Key Systems”, CHES’11, Springer LNCS vol. 6917, pp. 475–490, 2011.

[17] Pollard, J.M., “Monte Carlo Methods for Index Computation mod $p$”, Mathematics of Computation vol. 143, no. 32, pp. 918–924, 1978.

[18] Thomae, E., “Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-Commutative Rings”, SCN’12, *ePrint* http://eprint.iacr.org/2012/270.

[19] Wiener, M.J., “Cryptanalysis of Short RSA Secret Exponents”, IEEE Trans. Inform. Theory, vol. 36, no. 3, pp. 553–558, 1990.

[20] Wolf, C., Preneel, B., “Taxonomy of Public Key Schemes Based on the Problem of Multivariate Quadratic Equations”. Cryptology ePrint Archive, Report 2005/077, 64

[21] Yang, B.-Y. and Chen, J.-M., “Building Secure Tame like Multivariate Public-Key Cryptosystems: The new TTS”, ACISP’05, Springer LNCS vol. 3574, pp. 518–531, 2005.

[22] Yang, B.-Y. and Chen, J.-M., “All in the XL Family, Theory and Practice”, ICISC’04, Springer LNCS, vol. 3506, pp. 67–86, 2005.

[23] Yang, B.-Y., Chen, J.-M. and Chen Y.-H., “TTS: High-speed Signatures on a low-cost smart card”. CHES’04, Springer LNCS vol. 3156, pp. 371–385, 2004.

[24] Yasuda, T., Sakurai, K. and Takagi, T., “Reducing the Key Size of Rainbow using Non-commutative Rings”, CT-RSA’12, Springer LNCS vol. 7178, pp. 68–83, 2012.