Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-Commutative Rings

Enrico Thomae

Horst Görtz Institute for IT-security Faculty of Mathematics Ruhr-University of Bochum, 44780 Bochum, Germany enrico.thomae@rub.de

Abstract. The Rainbow Signature Scheme is a non-trivial generalization of the well known Unbalanced Oil and Vinegar Signature Scheme (Eurocrypt '99) minimizing the length of the signatures. Recently a new variant based on non-commutative rings, called NC-Rainbow, was introduced at CT-RSA 2012 to further minimize the secret key size. We disprove the claim that NC-Rainbow is as secure as Rainbow in general and show how to reduce the complexity of MinRank attacks from 2^{288} to 2^{192} and of HighRank attacks from 2^{128} to 2^{96} for the proposed instantiation over the ring of Quaternions. We further reveal some facts about Quaternions that increase the complexity of the signing algorithm. We show that NC-Rainbow is just a special case of introducing further structure to the secret key in order to decrease the key size. As the results are comparable with the ones achieved by equivalent keys, which provably do not decrease security, and far worse than just using a PRNG, we recommend not to use NC-Rainbow.

Key words: Multivariate Cryptography, Algebraic Cryptanalysis, Rainbow, MinRank, HighRank, Non-commutative Rings, Quaternions

1 Introduction

Rainbow was proposed in 2005 [4] and is a layer-based variant of the well known multivariate quadratic (\mathcal{MQ}) signature scheme Unbalanced Oil and Vinegar (UOV). UOV itself was proposed by Patarin et al. [8] at Eurocrypt 1999 and is one of the oldest \mathcal{MQ} -schemes still unbroken. The downside of UOV is a comparably large signature expansion by a factor of 3 for current parameters (m = 28, n = 84) [16]. Rainbow improves this to signatures of length n = 42 for messages of length m = 24, also for current parameters ($2^8, 18, 12, 12$) [5]. \mathcal{MQ} -schemes in general suffer from comparably large key sizes. The Rainbow scheme over non-commutative rings proposed at CT-RSA 2012, also called NC-

scheme over non-commutative rings proposed at CT-RSA 2012, also called NC-Rainbow [17], claims to reduce the secret key size by 75% while obtaining the same level of security.

Related Work. The parameter set $(2^8, 6, 6, 5, 5, 11)$ proposed for Rainbow in the original paper [4] was broken by Billet and Gilbert [2] in 2006 using a *Min-Rank* attack. The idea of those attacks was known since 2000 and first proposed in [7]. At Crypto 2008 Faugère *et al.* [6] refined the technique of Billet and Gilbert using Gröbner Bases. Ding *et al.* took this attack into account and proposed new parameters of Rainbow in [5]. For a comprehensive comparison of all known attacks on Rainbow and proposals for secure parameters we refer to [12]. So far there are two different techniques known to reduce the secret key size of Rainbow. On the one hand we can introduce a special structure, such like a cyclic coefficient matrix [11] and on the other hand we can use equivalent keys [13]. The latter exploits that large parts of the key are redundant and do not provide any security, whereas for the first variant it is an open problem to quantify the loss of security.

Achievement and Organization. Section 2 introduces the NC-Rainbow signature scheme as proposed in [17]. For readers unfamiliar with multivariate quadratic schemes, we start by briefly describing the Unbalanced Oil and Vinegar scheme and its layer-based variant Rainbow. Section 3 explains the algebraic structure of the ring of Quaternions and show how these seriously speed up MinRank and HighRank attacks.

2 Basics

In this section we explain the Rainbow signature scheme over non-commutative rings as proposed in [17] and introduce the necessary notation. For a better understanding we first briefly introduce the Unbalanced Oil and Vinegar as well as the Rainbow Signature Scheme.

The general idea of \mathcal{MQ} -signature schemes is to use a public multivariate quadratic map $\mathcal{P}: \mathbb{F}_q^n \to \mathbb{F}_q^m$ with

$$\mathcal{P} = \begin{pmatrix} p^{(1)}(x_1, \dots, x_n) \\ \vdots \\ p^{(m)}(x_1, \dots, x_n) \end{pmatrix}$$

and

$$p^{(k)}(x_1,\ldots,x_n) := \sum_{1 \le i \le j \le n} \widetilde{\gamma}_{ij}^{(k)} x_i x_j = x^{\mathsf{T}} \mathfrak{P}^{(k)} x,$$

where $\widetilde{\gamma}_{ij}^{(k)} \in \mathbb{F}_q$ are some coefficients, $\mathfrak{P}^{(k)}$ is the $(n \times n)$ matrix describing the quadratic form of $p^{(k)}$ and $x = (x_1, \ldots, x_n)^{\intercal}$. Note that we can neglect linear and constant terms as they never mix with quadratic terms and thus have no positive effects on security.

The trapdoor is given by a structured central map $\mathcal{F}:\mathbb{F}_q^n\to\mathbb{F}_q^m$ with

$$\mathcal{F} = \begin{pmatrix} f^{(1)}(u_1, \dots, u_n) \\ \vdots \\ f^{(m)}(u_1, \dots, u_n) \end{pmatrix}$$

and

$$f^{(k)}(u_1,\ldots,u_n) := \sum_{1 \le i \le j \le n} \gamma_{ij}^{(k)} u_i u_j = u^{\mathsf{T}} \mathfrak{F}^{(k)} u.$$

In order to hide this trapdoor we choose two secret linear transformations S, T and define $\mathcal{P} := T \circ \mathcal{F} \circ S$. See figure 1 for illustration.



Fig. 1. \mathcal{MQ} -Scheme in general.

For the **Unbalanced Oil and Vinegar (UOV)** signature scheme the variables u_i with $i \in V := \{1, \ldots, v\}$ are called *vinegar variables* and the remaining variables u_i with $i \in O := \{v + 1, \ldots, n\}$ are called *oil variables*. The central map $f^{(k)}$ is given by

$$f^{(k)}(u_1, \dots, u_n) := \sum_{i \in V, j \in V} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(k)} u_i u_j.$$

The corresponding matrix $\mathfrak{F}^{(k)}$ is depicted in figure 2.



Fig. 2. Central map $\mathfrak{F}^{(k)}$ of UOV. White parts denote zero entries while gray parts denote arbitrary entries.

As we have m equations in m+v variables, fixing v variables will yield a solution with high probability. Due to the structure of $\mathfrak{F}^{(k)}$, *i.e.* there are no quadratic terms of two oil variables, we can fix the vinegar variables at random to obtain a system of linear equations in the oil variables, which is easy to solve. This procedure is not possible for the public key, as the transformation S of variables fully mixes the variables (like oil and vinegar in a salad). Note that for UOV we can discard the transformation T of equations, as the trapdoor is invariant under this linear transformation.

Rainbow uses the same idea as UOV but in different layers. A current choice of parameters is given by $(q, v_1, o_1, o_2) = (2^8, 18, 12, 12)$. In particular the field size $q = 2^8$ and the number of layers is two. Note, two layers seems to be the best choice in order to prevent MinRank attacks and preserve short signatures at the same time. The central map \mathcal{F} of Rainbow is divided into two layers $\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(12)}$ and $\mathfrak{F}^{(13)}, \ldots, \mathfrak{F}^{(24)}$ of form given in figure 3. Let $V_1 := \{1, \ldots, v_1\}, O_1 := \{v_1 + 1, \ldots, v_1 + o_1\}$ and $O_2 := \{v_1 + o_1 + 1, \ldots, v_1 + o_1 + o_2\}$. A formal description of \mathcal{F} is given by the following formula.

$$f^{(k)}(u_1, \dots, u_n) := \sum_{i \in V_1, j \in V_1} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V_1, j \in O_1} \gamma_{ij}^{(k)} u_i u_j$$

for $k = 1, \dots, o_1$
$$f^{(k)}(u_1, \dots, u_n) := \sum_{i \in V_1 \cup O_1, j \in V_1 \cup O_1} \gamma_{ij}^{(k)} u_i u_j + \sum_{i \in V_1 \cup O_1, j \in O_2} \gamma_{ij}^{(k)} u_i u_j$$

for $k = o_1 + 1, \dots, o_1 + o_2$



Fig. 3. Central map of Rainbow $(2^8, 18, 12, 12)$. White parts denote zero entries while gray parts denote arbitrary entries.

To use the trapdoor we first solve the small UOV system $\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(o_1)}$ by fixing the v_1 vinegar variables at random. The solution $u_1, \ldots, u_{v_1+o_1}$ is now used as vinegar variables of the second layer. Solving the obtained linear system yields $u_{v_1+o_1+1}, \ldots, u_{v_1+o_1+o_2}$. The NC-Rainbow signature scheme proposed at CT-RSA 2012 [17] uses some non-commutative ring \mathbb{Q}_q with dimension r over \mathbb{F}_q to further decrease the secret key size. Due to the existence of a \mathbb{F}_q -linear isomorphism $\phi^{\widetilde{n}} : \mathbb{F}_q^{\widetilde{n}r} \to \mathbb{Q}_q^{\widetilde{n}}$ with $\widetilde{n}r := n$ and $\widetilde{m}r := m$, the central map \mathcal{F} can be replaced by $\phi^{-\widetilde{m}} \circ \widetilde{\mathcal{F}} \circ \phi^{\widetilde{n}}$ for $\widetilde{\mathcal{F}} : \mathbb{Q}_q^{\widetilde{n}} \to \mathbb{Q}_q^{\widetilde{m}}$. Let $\widetilde{V}_1 := \{1, \ldots, \widetilde{v}_1\}, \widetilde{O}_1 := \{\widetilde{v}_1 + 1, \ldots, \widetilde{v}_1 + \widetilde{o}_1\}$ and $\widetilde{O}_2 := \{\widetilde{v}_1 + \widetilde{o}_1 + 1, \ldots, \widetilde{v}_1 + \widetilde{o}_1 + \widetilde{o}_2\}$ with $r\widetilde{v}_1 := v_1, r\widetilde{o}_1 := o_1$ and $r\widetilde{o}_2 := o_2$. The central map $\widetilde{\mathcal{F}}$, as defined in [17], is given by the following polynomials.

$$\widetilde{f}^{(k)}(u_1,\ldots,u_n) := \sum_{i\in\widetilde{V}_1,j\in\widetilde{V}_1} u_i\gamma_{ij}^{(k)}u_j + \sum_{i\in\widetilde{V}_1,j\in\widetilde{O}_1} u_i\gamma_{ij}^{(k)}u_j + u_j\gamma_{ji}^{(k)}u_i$$

for $k = 1,\ldots,\widetilde{O}_1$
$$\widetilde{f}^{(k)}(u_1,\ldots,u_n) := \sum_{i\in\widetilde{V}_1\cup\widetilde{O}_1,j\in\widetilde{V}_1\cup\widetilde{O}_1} u_i\gamma_{ij}^{(k)}u_j + \sum_{i\in\widetilde{V}_1\cup\widetilde{O}_1,j\in\widetilde{O}_2} u_i\gamma_{ij}^{(k)}u_j + u_j\gamma_{ji}^{(k)}u_i$$

for $k = \widetilde{O}_1 + 1,\ldots,\widetilde{O}_1 + \widetilde{O}_2$

Note that in contrast to [17] we neglect linear and constant terms. As not all coefficients of those terms are chosen uniformly at random over \mathbb{F}_q (cf. section 3) they would provide further equations to speed up the Reconciliation attack (cf. Sec. 5, Eq. 4 in [15]). As we will not investigate Reconciliation attacks, we just forget about this flaw of NC-Rainbow.

3 Cryptanalysis of NC-Rainbow

The authors of [17] claimed that NC-Rainbow is as secure as the original Rainbow scheme, as every instance $(\mathbb{Q}_q, \tilde{v}_1, \tilde{o}_1, \tilde{o}_2)$ of the former can be transformed to an instance $(\mathbb{F}_q, v_1, o_1, o_2)$ of the latter, due to the \mathbb{F}_q -linear isomorphism ϕ . Well, as we will see below, this only provides an upper bound on the security.

First, we need the other direction to prove security, which does not hold due to the special choice of $\tilde{\mathcal{F}}$. More precisely, we will see in lemma 2 that the size of $\tilde{\mathcal{F}}$ must be at least as large as the size of \mathcal{F} to obtain exactly the same level of security.

Second, ϕ is not \mathbb{F}_q^r -linear. So even if the size of $\widetilde{\mathcal{F}}$ is large enough, it is not clear at all, if the additional structure of \mathbb{Q}_q can be used to attack the scheme. We will later use the structure of Quaternions to speed up MinRank and HighRank attacks.

Third, the ring used by the authors of [17] is commutative. But we do not restrict our cryptanalysis to this case and also investigate non-commutative rings (cf. remark 1).

In the sequel we explain and attack NC-Rainbow over the ring of Quaternions (cf. definition 1), as proposed by the authors of [17]. Note that the amount of additional structure introduced by $\tilde{\mathcal{F}}$ is independent of the encoding of the

non-commutative ring and thus NC-Rainbow is not equally secure to Rainbow for every non-commutative ring (cf. lemma 2). But there might be smarter encodings than Quaternions, which speed up known attacks a little less. We still do not think it is worthwhile to search for those non-commutative rings, as the whole construction is just a special case of reducing key size by introducing some structure to the secret key. Compare [11, 13] for the state of the art.

Definition 1 (Ring of Quaternions). The non-commutative ring of Quaternions $(\mathbb{Q}_q, +, \odot)$ of dimension r = 4 is defined by

$$\mathbb{Q}_q := \{(a, b, c, d)^\mathsf{T} \mid a, b, c, d \in \mathbb{F}_q\}$$

with

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix} := \begin{pmatrix} a_1 + a_2 \\ b_1 + b_2 \\ c_1 + c_2 \\ d_1 + d_2 \end{pmatrix}$$

and

$$\begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix} \odot \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix} := \begin{pmatrix} a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\ a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2 \\ a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 \\ a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2 \end{pmatrix}$$

The authors of [17] suggested to use the finite field \mathbb{F}_{2^8} . Note there exists a \mathbb{F}_{2^8} -linear map given by $\phi : \mathbb{F}_{2^8}^4 \to \mathbb{Q}_{256} : (a, b, c, d)^\intercal \mapsto (a, b, c, d)^\intercal$.

Remark 1. The ring of Quaternions is commutative over fields of *even* characteristic, by definition of multiplication \odot [14]. Thus we will distinguish between *odd* and *even* characteristic for every single attack in the sequel.

Remark 2. The ring of Quaternions over finite fields is not a division ring (skew field) [1]. This can be easily followed by a theorem of Wedderburn, who proved in 1905 that every finite skew field is a field (cf. theorem 2.55, page 70 in [10]). The authors of [17] did not address the impact of this fact to the signing algorithm. For example the element $(1, 1, 1, 1) \in \mathbb{Q}_{2^k}$ does not have an inverse and thus it might become much harder to find a solution of the linear system of oil variables. Note that the probability of a random element in \mathbb{Q}_q to have no inverse is 1/q. For the proposed parameters $(\tilde{v}_1, \tilde{o}_1, \tilde{o}_2) = (5, 4, 4)$ we need 12 inversions to perform the Gaussian elimination in both layers and additional 8 inversions to obtain the solution. Hence the probability of finding a solution is $0.996^{20} \approx 0.923$ in \mathbb{Q}_{2^8} and $0.937^{20} \approx 0.272$ in \mathbb{Q}_{2^4} . Note that NC-Rainbow over \mathbb{Q}_2 has probability 2^{-20} and thus would hardly work in practice.

Hidden Structure of NC-Rainbow. Before we continue to improve MinRank and HighRank attacks, we want to determine the hidden structure of NC-Rainbow over Quaternions in general. Example 1 gives a first impression. Example 1. To illustrate special structures over \mathbb{F}_q introduced by NC-Rainbow, we use the following example throughout the paper. Let $v_1 = 8$, $o_1 = 4$, $o_2 = 4$ and thus $\tilde{v}_1 = 2$, $\tilde{o}_1 = 1$, $\tilde{o}_2 = 1$. In figure 4 the central polynomials $\mathfrak{F}_1, \ldots, \mathfrak{F}_8$ of Rainbow are compared to the central polynomials $\mathfrak{F}_1, \ldots, \mathfrak{F}_8$ over fields of *odd* characteristic obtained by NC-Rainbow. Thereby crosses denote arbitrary values and empty squares denote systematical zeros. Later we will see that even the crosses of different maps are connected in some way. Further figure 5 shows that the structure is even stronger over fields of *even* characteristic.



Fig. 4. Central map of Rainbow compared to NC-Rainbow over fields of odd characteristic.

To determine all the structure over \mathbb{F}_q , we have a closer look at $u_i\gamma_{ij}u_j + u_j\gamma_{ji}u_i$ over \mathbb{Q} for $i \neq j$. Let $u_1 := (u_{11}, u_{12}, u_{13}, u_{14})^{\mathsf{T}}$, $u_2 := (u_{21}, u_{22}, u_{23}, u_{24})^{\mathsf{T}}$, $\gamma_{12} := (t_1, t_2, t_3, t_4)^{\mathsf{T}}$ and $\gamma_{21} := (t_5, t_6, t_7, t_8)^{\mathsf{T}}$. Due to remark 1 we only have to consider $u_i\gamma_{ij}u_j$ in fields of *even* characteristic.



Fig. 5. Central map of NC-Rainbow over fields of even characteristic.

We obtain $\phi^{-1} \circ (u_1 \gamma_{12} u_2) \circ \phi = u_1^{\mathsf{T}} (M_1, M_2, M_3, M_4) u_2$ with M_i given below.

$$\begin{split} M_1 &= \begin{pmatrix} t_1 & t_2 & t_3 & t_4 \\ t_2 & t_1 & t_4 & t_3 \\ t_3 & t_4 & t_1 & t_2 \\ t_4 & t_3 & t_2 & t_1 \end{pmatrix}, M_2 = \begin{pmatrix} t_2 & t_1 & t_4 & t_3 \\ t_1 & t_2 & t_3 & t_4 \\ t_4 & t_3 & t_2 & t_1 \\ t_3 & t_4 & t_1 & t_2 \end{pmatrix} \\ M_3 &= \begin{pmatrix} t_3 & t_4 & t_1 & t_2 \\ t_4 & t_3 & t_2 & t_1 \\ t_1 & t_2 & t_3 & t_4 \\ t_2 & t_1 & t_4 & t_3 \end{pmatrix}, M_4 = \begin{pmatrix} t_4 & t_3 & t_2 & t_1 \\ t_3 & t_4 & t_1 & t_2 \\ t_2 & t_1 & t_4 & t_3 \\ t_1 & t_2 & t_3 & t_4 \end{pmatrix} \end{split}$$

Note that $\phi^{-1} \circ u_i \gamma_{ij} u_j \circ \phi$ produces 4 polynomials over \mathbb{F}_q with 16 monomials $u_{1i}u_{2j}$, i, j = 1, 2, 3, 4. Further for the original Rainbow scheme, all these 64 coefficients of $u_{1i}u_{2j}$ for $1 \leq i, j \leq 4$ in the secret polynomials $f^{(1)}, \ldots, f^{(4)}$ of \mathcal{F} are chosen independently, uniformly at random. But due to the special choice of the central map of NC-Rainbow, now only 4 coefficients t_i are chosen uniformly at random. Clearly this introduce additional structure to the secret key \mathcal{F} that can be used for algebraic attacks (cf. [15]). In order to be as secure as the original scheme, we need at least as many coefficients in the central map of NC-Rainbow as in the original. This is not possible for dimensions r > 2 due to lemma 1.

Lemma 1. Let \mathbb{F}_q be any finite field and R a non-commutative ring of dimension r > 2 over \mathbb{F}_q . Then NC-Rainbow over R with any secret map $\widetilde{\mathcal{F}}$ can never be as secure as Rainbow.

Proof. The maximal number of quadratic monomials containing variables u_1 and u_2 in R is 6, namely $\gamma_1 u_1 u_2$, $\gamma_2 u_2 u_1$, $u_1 \gamma_3 u_2$, $u_2 \gamma_4 u_1$, $u_1 u_2 \gamma_5$, $u_2 u_1 \gamma_6$ for some coefficients $\gamma_i \in R$. Every element $\gamma_i \in R$ encodes r elements of \mathbb{F}_q and thus the maximal number of coefficients we can choose uniformly at random over \mathbb{F}_q is 6r. On the other hand there are r^2 monomials over \mathbb{F}_q produced by u_1 and u_2 . All those monomials occur in r different polynomials and thus are represented by r^3 coefficients in \mathbb{F}_q . In the case of Rainbow all these coefficients are chosen independently, uniformly at random. While $r^3 > 6r$ for r > 2 this is not possible for NC-Rainbow.

Next we observe that the matrices M_i are heavily structured. A simple addition $M_1 + M_2 + M_3 + M_4$ provides a matrix with the same value in every entry and

thus with rank 1 instead of 4. We will use this fact later on to improve MinRank attacks.

The following matrices produced by $u_i \gamma_{ii} u_i$ provide even more structure (cf. figure 5).

$$M_{1} = \begin{pmatrix} t_{1} & 0 & 0 & 0 \\ 0 & t_{1} & 0 & 0 \\ 0 & 0 & t_{1} & 0 \\ 0 & 0 & 0 & t_{1} \end{pmatrix}, M_{2} = \begin{pmatrix} t_{2} & 0 & 0 & 0 \\ 0 & t_{2} & 0 & 0 \\ 0 & 0 & t_{2} & 0 \\ 0 & 0 & 0 & t_{2} \end{pmatrix},$$
$$M_{3} = \begin{pmatrix} t_{3} & 0 & 0 & 0 \\ 0 & t_{3} & 0 & 0 \\ 0 & 0 & t_{3} & 0 \\ 0 & 0 & 0 & t_{3} \end{pmatrix}, M_{4} = \begin{pmatrix} t_{4} & 0 & 0 & 0 \\ 0 & t_{4} & 0 & 0 \\ 0 & 0 & t_{4} & 0 \\ 0 & 0 & 0 & t_{4} \end{pmatrix}.$$

For fields of *odd* characteristic the structure of M_i produced by $u_i \gamma_{ij} u_j + u_j \gamma_{ji} u_i$ becomes slightly more difficult.

$$M_{1} = \begin{pmatrix} t_{1} + t_{5} & -t_{2} - t_{6} & -t_{3} - t_{7} & -t_{4} - t_{8} \\ -t_{2} - t_{6} & -t_{1} - t_{5} & t_{4} - t_{8} & -t_{3} + t_{7} \\ -t_{3} - t_{7} & -t_{4} + t_{8} & -t_{1} - t_{5} & t_{2} - t_{6} \\ -t_{4} - t_{8} & t_{3} - t_{7} & -t_{2} + t_{6} & -t_{1} - t_{5} \end{pmatrix},$$

$$M_{2} = \begin{pmatrix} t_{2} + t_{6} & t_{1} + t_{5} & -t_{4} + t_{8} & t_{3} - t_{7} \\ t_{1} + t_{5} & -t_{2} - t_{6} & -t_{3} - t_{7} & -t_{4} - t_{8} \\ t_{4} - t_{8} & -t_{3} - t_{7} & t_{2} + t_{6} & t_{1} - t_{5} \\ -t_{3} + t_{7} & -t_{4} - t_{8} & -t_{1} + t_{5} & t_{2} + t_{6} \end{pmatrix},$$

$$M_{3} = \begin{pmatrix} t_{3} + t_{7} & t_{4} - t_{8} & t_{1} + t_{5} & -t_{2} + t_{6} \\ -t_{4} + t_{8} & t_{3} + t_{7} & -t_{2} - t_{6} & -t_{1} + t_{5} \\ t_{1} + t_{5} & -t_{2} - t_{6} & -t_{3} - t_{7} & -t_{4} - t_{8} \\ t_{2} - t_{6} & t_{1} - t_{5} & -t_{4} - t_{8} & t_{3} + t_{7} \end{pmatrix},$$

$$M_{4} = \begin{pmatrix} t_{4} + t_{8} & -t_{3} + t_{7} & t_{2} - t_{6} & t_{1} + t_{5} \\ t_{3} - t_{7} & t_{4} + t_{8} & t_{1} - t_{5} & -t_{2} - t_{6} \\ -t_{2} + t_{6} & -t_{1} + t_{5} & t_{4} + t_{8} & -t_{3} - t_{7} \\ t_{1} + t_{5} & -t_{2} - t_{6} & -t_{3} - t_{7} & -t_{4} - t_{8} \end{pmatrix}.$$

Obtaining a generic, *i.e.* independent of the choice of coefficients t_i , linear combination $a_1M_1 + a_2M_2 + a_3M_3 + a_4M_4 =: N$ with rank less than 4 becomes a little more involved. We now want to show that there always exists a matrix N with rank 3, *i.e.* we can find a linear combination of columns such that $b_1N_{.1} + b_2N_{.2} + b_3N_{.3} + N_{.4} = 0$. Collecting the coefficients of t_1, \ldots, t_8 in every of the 4 components and setting them to zero provides 32 quadratic equations in the unknowns a_1, a_2, a_3, a_4 and b_1, b_2, b_3 . We obtain the following solution by computing the Gröbner Basis of this system.

$$a_1 = 1, a_2 = b_1, a_3 = b_2, a_4 = b_3 \text{ and } b_1^2 + b_2^2 + b_3^2 = -1$$

Lemma 2 proves that $b_1^2 + b_2^2 + b_3^2 = -1$ with $b_1 = 0$ always has a solution over \mathbb{F}_p with p > 2 prime. Note that this implies the existence of a solution also over extension fields.

Lemma 2. Let p > 2 be prime. Then there exists a, b such that

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

Proof. This lemma, as well as its proof, is well-known in literature. As the proof itself is very elegant, we give a brief description for readers who are unfamilar with this topic. Consider the two sets

$$A = \left\{ 0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2 \right\} \text{ and } B = \left\{ -0^2 - 1, -1^2 - 1, \dots, -\left(\frac{p-1}{2}\right)^2 - 1 \right\}.$$

Obviously all elements of A as well as of B are pairwise distinct. Due to $|A| = |B| = \frac{p+1}{2}$ we obtain a total amount of |A| + |B| = p + 1 elements. As $|\mathbb{F}_p| = p$ there must be one element contained in both sets and thus $a^2 \equiv -b^2 - 1 \pmod{p}$.

To conclude the preparation of our MinRank attack, we give the matrices produced by $u_i \gamma_{ii} u_i$ over fields of *odd* characteristic.

$$M_{1} = \begin{pmatrix} 2t_{1} - 2t_{2} - 2t_{3} & -2t_{4} \\ -2t_{2} - 2t_{1} & 0 & 0 \\ -2t_{3} & 0 - 2t_{1} & 0 \\ -2t_{4} & 0 & 0 - 2t_{1} \end{pmatrix}, M_{2} = \begin{pmatrix} 2t_{2} & 2t_{1} & 0 & 0 \\ 2t_{1} - 2t_{2} - 2t_{3} & -2t_{4} \\ 0 - 2t_{3} & 2t_{2} & 0 \\ 0 - 2t_{4} & 0 & 2t_{2} \end{pmatrix},$$
$$M_{3} = \begin{pmatrix} 2t_{3} & 0 & 2t_{1} & 0 \\ 0 & 2t_{3} - 2t_{2} & 0 \\ 2t_{1} - 2t_{2} - 2t_{3} & -2t_{4} \\ 0 & 0 & -2t_{4} & 2t_{3} \end{pmatrix}, M_{4} = \begin{pmatrix} 2t_{4} & 0 & 0 & 2t_{1} \\ 0 & 2t_{4} & 0 & -2t_{2} \\ 0 & 0 & 2t_{4} - 2t_{3} \\ 2t_{1} - 2t_{2} - 2t_{3} - 2t_{4} \end{pmatrix}.$$

MinRank attack. The main idea of rank attacks is that the rank of $\mathfrak{F}^{(k)}$ is invariant under the bijective transformation of variables S but not under the transformation of equations T. Thus we can use the rank as distinguisher to recover T. Note that once T is known, S is also recovered comparably fast by UOV attacks like the one of Kipnis and Shamir [9] due to the special choice of parameters.

A naive way of performing a MinRank attack [2] is to sample a vector $\omega \in_R \mathbb{F}_q^n$ and hope that it lies in the kernel of a linear combination of low-rank matrices. If this is true, solving the linear system of equations

$$\sum_{i=1}^{m} \lambda_i \mathfrak{P}^{(i)} \omega = 0 \text{ for } \omega \in_R \mathbb{F}_q^n, \lambda_i \in \mathbb{F}_q, \mathfrak{P}^{(i)} \in \mathbb{F}_q^{n \times n}$$

reveals a part of the secret transformation T. The complexity of sampling $\omega \in \ker(\mathfrak{F})$ is q^{n-d} with n the number of variables and $d = \dim(\ker(\mathfrak{F}))$. Note $n-d = \operatorname{rank}(\mathfrak{F})$.

Lemma 3. The complexity of MinRank attacks on NC-Rainbow over fields \mathbb{F}_q of even characteristic is at most $q^{4\widetilde{v}_1+\widetilde{o}_1}$ instead of $q^{4\widetilde{v}_1+4\widetilde{o}_1}$.

Proof. For fields of even characteristic we already showed that $M_1+M_2+M_3+M_4$ has rank 1 instead of 4. Remember that for $\mathfrak{F}^{(1)} + \mathfrak{F}^{(2)} + \mathfrak{F}^{(3)} + \mathfrak{F}^{(4)} =: \mathfrak{F}$ every (4×4) submatrix contains only equal elements, *i.e.* $\mathfrak{F}_{i,j} = \mathfrak{F}_{x,y}$ with $4k \leq i, x \leq 4(k+1), 4\ell \leq j, y \leq 4(\ell+1)$ for some $k \neq \ell$. Adding column $v_1 + 4k$ to the columns $v_1 + 4k - 1, v_1 + 4k - 2, v_1 + 4k - 3$ for $1 \leq k \leq \tilde{o}_1$ vanishes a total of $3\tilde{o}_1$ columns. Hence \mathfrak{F} has rank $4\tilde{v}_1 + \tilde{o}_1$. Compare example 1 for an illustration:



Lemma 4. The complexity of MinRank attacks on NC-Rainbow over fields \mathbb{F}_q of odd characteristic is at most $q^{4\widetilde{v}_1+3\widetilde{o}_1}$ instead of $q^{4\widetilde{v}_1+4\widetilde{o}_1}$.

Proof. Due to lemma 2 there exists a linear combination of every four columns $v_1+4k, v_1+4k-1, v_1+4k-2, v_1+4k-3$ with $1 \le k \le \tilde{o}_1$ of $\mathfrak{F}^{(1)}+\mathfrak{F}^{(2)}+\mathfrak{F}^{(3)}+\mathfrak{F}^{(4)}$, such that one column vanishes.

We implemented NC-Rainbow using the software system Magma V2.16-1 [3] and observed that the ranks are even smaller than given by lemma 3 and 4. Table 1 illustrate the ranks of the central polynomials and their linear combination for fields of even characteristic and different sets of parameters. The last two columns give the maximum of all minimal ranks that we brute-forced in several experiments.

\widetilde{v}_1	\widetilde{o}_1	\widetilde{o}_2	$ \begin{aligned} & \mathbf{\mathfrak{F}}_i \\ & 1 \leq i \leq o_1 \end{aligned} $	${igside{\mathfrak{F}}_i} o_1 < i \leq m$	$\sum_{i=1}^{4} \mathfrak{F}_i$	$\sum_{i=o_1+1}^{o_1+4} \mathfrak{F}_i$	$\left \sum_{i=1}^{o_1} \gamma_i \mathfrak{F}_i\right $	$\sum_{i=o_1+1}^{o_1+o_2} \gamma_i \mathfrak{F}_i$
5	1	1	24	28	20	24	16	20
5	1	2	24	32	20	24	16	18
5	2	1	28	32	20	28	14	24
5	2	2	28	36	20	28	14	20
5	3	3	32	44	20	32	14	22

Table 1. Ranks of NC-Rainbow over even characteristic, experimentally derived. The last two columns give the maximum of all minimal ranks that we brute-forced in several experiments.

Table 2. Ranks of NC-Rainbow over odd characteristic, experimentally derived. The last two columns give the maximum of all minimal ranks that we brute-forced in several experiments.

\widetilde{v}_1	\widetilde{o}_1	\widetilde{o}_2	$ \begin{aligned} & \widetilde{\mathfrak{F}}_i \\ & 1 \leq i \leq o_1 \end{aligned} $	$rac{\mathfrak{F}i}{o_1 < i \leq m}$	$\sum_{i=1}^{o_1} \gamma_i \mathfrak{F}_i$	$\sum_{i=o_1+1}^{o_1+o_2} \gamma_i \mathfrak{F}_i$
5	1	1	24	28	22	26
5	1	2	24	32	22	28
5	2	1	28	32	24	30
5	2	2	28	36	24	31
5	3	3	32	44	27	39

Heuristic: We have experimentally derived that $\mathfrak{F}^{(1)} + \mathfrak{F}^{(2)} + \mathfrak{F}^{(3)} + \mathfrak{F}^{(4)}$ has rank $4\tilde{v}_1$ instead of $4\tilde{v}_1 + \tilde{o}_1$ for even characteristic. Moreover, for $4\tilde{o}_1 > \tilde{v}_1$ there always exists a linear combination such that all (4×4) matrices on the diagonal are zero. Experiments suggest that this linear combination has rank $3\tilde{v}_1 - 1$.

Table 3. Log₂ complexity of MinRank attacks against NC-Rainbow over \mathbb{Q}_q with even characteristic.

$(\widetilde{v}_1,\widetilde{o}_1,\widetilde{o}_2)$	claimed	real	heuristic
(5, 4, 4)	288	192	112
(7, 5, 5)	384	264	160
(9, 6, 6)	480	336	208

HighRank attack. Our observation regarding HighRank attacks holds both for even and odd characteristic.

Lemma 5. The complexity of HighRank attacks on NC-Rainbow over \mathbb{Q}_q is at most $q^{o_2-\tilde{o}_2}$ instead of q^{o_2} .

Proof. We already mentioned that there exists a linear combination of high rank matrices such that the rank decrease. In particular for fields of even characteristic $M_1 + M_2 + M_3 + M_4$ has rank 1 instead of 4 and for fields of odd characteristic we showed in lemma 2 that there exists a generic linear combination of M_1, M_2, M_3, M_4 with rank 3. Thus we do not have to remove *all* polynomials \mathfrak{F}_i of high rank to observe a decrease of rank, but only 3 out of 4, *i.e.* in total we have to brute force $4\tilde{o}_2 - \tilde{o}_2 = o_2 - \tilde{o}_2$ linear combinations of public polynomials \mathfrak{P}_i .

Table 4. Log₂ complexity of HighRank attacks against NC-Rainbow over \mathbb{Q}_q .

$(\widetilde{v}_1,\widetilde{o}_1,\widetilde{o}_2)$	claimed	\mathbf{real}
(5, 4, 4)	128	96
(7, 5, 5)	160	120
(9, 6, 6)	192	144

Acknowledgments

The author wants to thank the anonymous reviewers of SCN 2012 for their helpful remarks and suggestions. He was supported by the German Science Foundation (DFG) through an Emmy Noether grant. Furthermore the author was in part supported by the European Commission through the IST Programme under contract ICT-2007-216676 Ecrypt II.

Bibliography

- M. Aristidou and A. Demetre. A Note on Quaternion Rings over Z_p. In International Journal of Algebra, volume 3, pages 725 - 728, 2009.
- [2] O. Billet and H. Gilbert. Cryptanalysis of Rainbow. In SCN, pages 336–347, 2006.
- [3] Computational Algebra Group, University of Sydney. The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry. http://magma.maths.usyd.edu.au/magma/.
- [4] J. Ding and D. Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. In Conference on Applied Cryptography and Network Security — ACNS 2005, volume 3531 of Lecture Notes in Computer Science, pages 164–175. Springer, 2005.
- [5] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng. New Differential-Algebraic Attacks and Reparametrization of Rainbow. In Proceedings of the 6th international conference on Applied cryptography and network security, ACNS'08, pages 242–257, Berlin, Heidelberg, 2008. Springer-Verlag.
- [6] J.-C. Faugère, F. L. dit Vehel, and L. Perret. Cryptanalysis of MinRank. In CRYPTO, pages 280–296, 2008.
- [7] L. Goubin and N. T. Courtois. Cryptanalysis of the TTM Cryptosystem. In Advances in Cryptology — ASIACRYPT 2000, volume 1976 of Lecture Notes in Computer Science, pages 44–57. Tatsuaki Okamoto, editor, Springer, 2000.
- [8] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced Oil and Vinegar Signature Schemes. In Advances in Cryptology — EUROCRYPT 1999, volume 1592 of Lecture Notes in Computer Science, pages 206–222. Jacques Stern, editor, Springer, 1999.
- [9] A. Kipnis and A. Shamir. Cryptanalysis of the Oil and Vinegar Signature Scheme. In Advances in Cryptology — CRYPTO 1998, volume 1462 of Lecture Notes in Computer Science, pages 257–266. Hugo Krawczyk, editor, Springer, 1998.
- [10] R. Lidl and H. Niederreiter. *Finite Fields*. Number 20 in EMA. CUP, Cambridge, UK, 2nd edition, 1997.
- [11] A. Petzoldt, S. Bulygin, and J. Buchmann. CyclicRainbow a Multivariate Signature Scheme with a Partially Cyclic Public Key. In *INDOCRYPT*, volume 6498 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2010.
- [12] A. Petzoldt, S. Bulygin, and J. Buchmann. Selecting Parameters for the Rainbow Signature Scheme. In PQCrypto, pages 218–240, 2010.
- [13] A. Petzoldt, E. Thomae, S. Bulygin, and C. Wolf. Small Public Keys and Fast Verification for Multivariate Quadratic Public Key Systems. In *CHES*, pages 475–490, 2011.
- [14] R. S. Pierce. In Associative Algebras, page 16. Springer, 1982.

- [15] E. Thomae. A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes. 2012. http://eprint.iacr.org/2012/223.
- [16] E. Thomae and C. Wolf. Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. In *Practice and Theory in Public Key Cryptography (PKC 2012).* Springer-Verlag, 2012.
- [17] T. Yasuda, K. Sakurai, and T. Takagi. Reducing the Key Size of Rainbow Using Non-Commutative Rings. In CT-RSA, volume 7178 of Lecture Notes in Computer Science, pages 68–83. Springer, 2012.