# CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public Key

Albrecht Petzoldt[1], Stanislav Bulygin[2], and Johannes Buchmann[1,2]

[1] Technische Universität Darmstadt, Department of Computer Science
Hochschulstraße 10, 64289 Darmstadt, Germany
{apetzoldt,buchmann}@cdc.informatik.tu-darmstadt.de

[2] Center for Advanced Security Research Darmstadt - CASED
Mornewegstraße 32, 64293 Darmstadt, Germany
{johannes.buchmann,Stanislav.Bulygin}@cased.de

**Abstrct.** Multivariate Cryptography is one of the alternatives to guarantee the security of communication in the post-quantum world. One major drawback of such schemes is the huge size of their keys. In [PB10] Petzoldt et al. proposed a way how to reduce the public key size of the UOV scheme by a large factor. In this paper we extend this idea to the Rainbow signature scheme of Ding and Schmidt [DS05]. By our construction it is possible to reduce the size of the public key by up to 62 %.

**Keywords:** Multivariate Cryptography, Rainbow Signature Scheme, Key Size Reduction.

## 1 Introduction

Besides lattice-, code- and hash-based cryptosystems, multivariate cryptography is one of the main alternatives to guarantee the security of communication in the post-quantum world [BB08]. Multivariate schemes are fast and efficient and seem especially suitable for signatures on low cost devices like RFIDs or smart cards.

Since the invention of multivariate cryptography in the 1980's, a huge variety of schemes both for encryption and signatures have been proposed. On the one hand, we have the so called BigField-Schemes like Matsumoto-Imai [MI88] and HFE [Pa96]. On the other hand, we have the SingleField-Schemes like UOV [KP99] and Rainbow [DS05]. In between, there are the so called MiddleField schemes like $\ell$-IC [DW07] and MFE [WY06]. For all of these schemes there exist many variations and improvements, like the minus variation [PG98] [PC01], Internal Perturbation [Di04] and Projection [DY07]. One common drawback of all multivariate schemes is the large size of their public and private keys. Therefore, the question of key size reduction for multivariate schemes is an important area of research.

In the last years, a lot of work was done to look at possibilities to reduce the key sizes. Most researchers hereby concentrated on the reduction of the private key. We mention here the proposals of Yang and Chen for creating schemes with

G. Gong and K.C. Gupta (Eds.): INDOCRYPT 2010, LNCS 6498, pp. 33–48, 2010.

sparse central maps [YC05] and approaches with so called equivalent keys of Hu et al. [HW05]. In [PB10] Petzoldt et al. presented an idea how to reduce the public key size of the UOV signature scheme by a large factor. The principle idea is, to compute the coefficients of the central map in such a way, that the corresponding public key gets a compact structure.

In this paper we show how to extend this idea to the Rainbow signature scheme, which was proposed by J. Ding and D. Schmidt in 2005 [DS05]. The result is a Rainbow scheme, whose public key belongs to a certain subset of the set of all valid Rainbow public keys. By doing so it is possible to reduce the size of the public key by up to 62 %. Furthermore, we can reduce the number of field multiplications needed during the verification process by 30 %.

The structure of this paper is as follows:

In Section 2 we describe the Rainbow signature scheme of Ding and Schmidt. Section 3 gives an overview on the approach of [PB10] to create a UOV scheme with partially cyclic public key. Section 4 deals with notations and definitions we need for our construction in Section 5. Section 6 looks at security aspects of the new scheme and Section 7 gives concrete parameter sets and compares it with other multivariate schemes of the UOV family. Finally, Section 8 concludes the paper.

## 2 Multivariate Public Key Cryptography

Multivariate Public Key Cryptography is one of the main approaches for secure communication in the post-quantum world. The principle idea is to choose a multivariate system $\mathcal{F}$ of quadratic polynomials which can be easily inverted (central map). After that one chooses two affine linear invertible maps $\mathcal{S}$ and $\mathcal{T}$ to hide the structure of the central map. The public key of the cryptosystem is the composed map $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ which is difficult to invert. The private key consists of $\mathcal{S}$, $\mathcal{F}$ and $\mathcal{T}$ and therefore allows to invert $\mathcal{P}$.

### 2.1 The Principle of Oil and Vinegar (OV)

One way to create easily invertible multivariate quadratic systems is the principle of Oil and Vinegar, which was first proposed by J. Patarin in [Pa97].

Let $K$ be a finite field. Let $o$ and $v$ be two integers and set $n = o + v$. Patarin suggested to choose $o = v$. After this original scheme was broken by Kipnis and Shamir in [KS98], it was recommended in [KP99] to choose $v > o$ (Unbalanced Oil and Vinegar (UOV)). In the following we describe the more general approach UOV.

We set $V' = \{1, \ldots, v\}$ and $O = \{v+1, \ldots, n\}$. Of the $n$ variables $x_1, \ldots, x_n$ we call $x_1, \ldots, x_v$ the Vinegar variables and $x_{v+1}, \ldots, x_n$ Oil variables. We define $o$ quadratic polynomials $f_k(\mathbf{x}) = f_k(x_1, \ldots, x_n)$ by

$$f_k(\mathbf{x}) = \sum_{i \in V',\ j \in O} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V',\ i \leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V' \cup O} \gamma_i^{(k)} x_i + \eta^{(k)} \ (k \in O)$$

Note that Oil and Vinegar variables are not fully mixed, just like oil and vinegar in a salad dressing.

The map $\mathcal{F} = (f_{v+1}(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ can be easily inverted. First, we choose the values of the $v$ Vinegar variables $x_1, \ldots, x_v$ at random. Therewith we get a system of $o$ linear equations in the $o$ variables $x_{v+1}, \ldots, x_n$ which can be solved by Gaussian Elimination. (If the system doesn't have a solution, choose other values of $x_1, \ldots, x_v$ and try again).

### 2.2 The Rainbow Signature Scheme

In [DS05] J. Ding and D. Schmidt proposed a signature scheme called Rainbow, which is based on the idea of (Unbalanced) Oil and Vinegar [KP99].

Let $K$ be a finite field and $V$ be the set $\{1, \ldots, n\}$. Let $v_1, \ldots, v_{u+1}, u \geq 1$ be integers such that $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$ and define the sets of integers $V_i = \{1, \ldots, v_i\}$ for $i = 1, \ldots, u$. We set $o_i = v_{i+1} - v_i$ and $O_i = \{v_i + 1, \ldots, v_{i+1}\}$ $(i = 1, \ldots, u)$. The number of elements in $V_i$ is $v_i$ and we have $|O_i| = o_i$. For $k = v_1 + 1, \ldots, n$ we define multivariate quadratic polynomials in the $n$ variables $x_1, \ldots, x_n$ by

$$f_k(\mathbf{x}) = \sum_{i \in O_l,\ j \in V_l} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i,j \in V_l,\ i \leq j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in V_l \cup O_l} \gamma_i^{(k)} x_i + \eta^{(k)},$$

where $l$ is the only integer such that $k \in O_l$. Note that these are Oil and Vinegar polynomials with $x_i,\ i \in V_l$ being the Vinegar variables and $x_j,\ j \in O_l$ being the Oil variables.

The map $\mathcal{F}(\mathbf{x}) = (f_{v_1+1}(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ can be inverted as follows. First, we choose $x_1, \ldots, x_{v_1}$ at random. Hence we get a system of $o_1$ linear equations (given by the polynomials $f_k$ $(k \in O_1)$) in the $o_1$ unknowns $x_{v_1+1}, \ldots, x_{v_2}$, which can be solved by Gaussian Elimination. The so computed values of $x_i$ $(i \in O_1)$ are plugged into the polynomials $f_k(\mathbf{x})$ $(k > v_2)$ and a system of $o_2$ linear equations (given by the polynomials $f_k$ $(k \in O_2)$) in the $o_2$ unknowns $x_i$ $(i \in O_2)$ is obtained. By repeating this process we can get values for all the variables $x_i$ $(i = 1, \ldots, n)$[1].

The Rainbow signature scheme is defined as follows:

*Key Generation.* The private key consists of two invertible affine maps $\mathcal{S} : K^m \to K^m$ and $\mathcal{T} : K^n \to K^n$ and the map $\mathcal{F}(\mathbf{x}) = (f_{v_1+1}(\mathbf{x}), \ldots, f_n(\mathbf{x})) : K^n \to K^m$. Here, $m = n - v_1$ is the number of components of $\mathcal{F}$.

The public key consists of the field $K$ and the composed map $\mathcal{P}(\mathbf{x}) = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}(\mathbf{x}) : K^n \to K^m$.

*Signature Generation.* To sign a document $d$, we use a hash function $\mathbf{h} : K^* \to K^m$ to compute the value $\mathbf{h} = \mathbf{h}(d) \in K^m$. Then we compute recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h})$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x})$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. The signature of the document is $\mathbf{z} \in K^n$. Here, $\mathcal{F}^{-1}(\mathbf{x})$ means finding one (of the possibly many) pre-image of $\mathbf{x}$.

[1] It may happen, that one of the linear systems does not have a solution. If so, one has to choose other values of $x_1, \ldots x_{v_1}$ and try again.

*Verification.* To verify the authenticity of a signature, one simply computes $\mathbf{h}' = P(\mathbf{z})$ and the hashvalue $\mathbf{h} = \mathbf{h}(d)$ of the document. If $\mathbf{h}' = \mathbf{h}$ holds, the signature is accepted, otherwise rejected.

The size of the public key is

$$m \cdot \left( \frac{n \cdot (n+1)}{2} + n + 1 \right) = m \cdot \frac{(n+1) \cdot (n+2)}{2} \text{ field elements,} \tag{1}$$

the size of the private key

$$m \cdot (m+1) + n \cdot (n+1) + \sum_{l=1}^{u} o_l \cdot \left( v_l \cdot o_l + \frac{v_l \cdot (v_l+1)}{2} + v_{l+1} + 1 \right) \text{ field elements.} \tag{2}$$

The length of the needed hash value is $m$ field elements, the length of the signature is $n$ field elements.

The scheme is denoted by Rainbow$(v_1, o_1, \ldots, o_u)$. For $u = 1$ we get the original UOV scheme.

Rainbow over $GF(2^8)$ is commonly believed to be secure for at least 26 equations [BF09], [PB1a]. The actual design of the Rainbow layers is thereby not so important, as long as the following four items are taken into consideration [PB1a]:

- to defend the scheme against the Rainbow-Band-Separation attack (see subsection 6.2) one must have $n \geq \lceil \frac{5}{3} \cdot (m-1) \rceil$.
- to defend the scheme against the MinRank attack (see subsection 6.3) one must have $v_1 \geq 9$.
- to defend the scheme against the HighRank attack (see subsection 6.4) one must have $o_u \geq 10$.
- to defend the scheme against the UOV attack (see subsection 6.5) one must have $n - 2 \cdot o_u \geq 11$.

In particular, $(v_1, o_1, o_2) = (17, 13, 13)$ is a good choice for the parameters of Rainbow over $GF(2^8)$.

## 3 The Approach of [PB10]

In this section we describe briefly the approach of [PB10] to create a UOV-based scheme with a partially cyclic public key.

For SingleField schemes, both the public key $\mathcal{P}$ and the central map $\mathcal{F}$ are quadratic maps from $K^n$ to $K^o$ and therefore can be written as

$$\mathcal{P}(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)} \quad \text{resp.}$$

$$\mathcal{F}(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=i}^{n} f_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} f_i^{(k)} x_i + f_0^{(k)} \ (k = 1, \ldots, o)$$

In the special case of the unbalanced Oil and Vinegar Signature Scheme [KP99] $\mathcal{P}$ is given as a concatenation of the central UOV-map $\mathcal{F}$ and an affine invertible map $\mathcal{T} = ((t_{ij})_{i,j=1}^{n}, c_T)$, i.e. $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$.

The authors of [PB10] observed, that this equation leads (after fixing the affine map $\mathcal{T}$) to a linear relation between the coefficients of $\mathcal{P}$ and those of $\mathcal{F}$ of the form

$$p_{ij}^{(k)} = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ij}^{rs} \cdot f_{rs}^{(k)}, \tag{3}$$

where the coefficients $\alpha_{ij}^{rs}$ are given as

$$\alpha_{ij}^{rs} = \begin{cases} t_{ri} \cdot t_{si} & (i = j) \\ t_{ri} \cdot t_{sj} + t_{rj} \cdot t_{si} & \text{otherwise} \end{cases}. \tag{4}$$

The relation (3) can be written in the form

$$\mathbf{p}^{(k)} = A' \cdot \mathbf{f}^{(k)}, \tag{5}$$

with two vectors containing the coefficients of the quadratic monomials of the $k$-th components of $\mathcal{P}$ resp. $\mathcal{F}$ and a matrix

$$A' = \left(\alpha_{ij}^{rs}\right) \ (1 \leq i \leq v,\ i \leq j \leq n \text{ for the rows},\ 1 \leq r \leq v,\ r \leq s \leq n \text{ for the columns}). \tag{6}$$

By fixing the vectors $\mathbf{p}^{(i)}$ $i = 1, \ldots, o$ and inverting this relation, the authors of [PB10] were able to compute the central map $\mathcal{F}$ of a UOV scheme (with invertible affine map $\mathcal{T}$), whose public key has a coefficient matrix $M_P$ of the form

$$M_P = (B|C),$$

where the rows of $B$ are given by the vectors $\mathbf{p}^{(i)}$ $i = 1, \ldots, o$ and $C$ is a matrix without apparent structure. By choosing the matrix $B$ as a partially circulant matrix, they were able to reduce the public key size of the UOV scheme by a large factor.

## 4 Preliminaries

In this section we introduce some notations and definitions we need for the construction of our scheme in the next section. We restrict ourselves to the case of two Rainbow layers.

### 4.1 Notations

We denote
$D_1 = \frac{v_1 \cdot (v_1+1)}{2} + v_1 \cdot o_1$ the number of quadratic terms in the central polynomials of the first layer.

$D_2 = \frac{v_2 \cdot (v_2+1)}{2} + v_2 \cdot o_2$ the number of quadratic terms in the central polynomials of the second layer.
$D = \frac{n \cdot (n+1)}{2}$ the number of quadratic terms in the public polynomials.
For the invertible affine map $\mathcal{S} = (S, c_S)$ we divide the $m \times m$ matrix $S$ into four parts:
$S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix}$, where $S_{11}$ is the upper left $o_1 \times o_1$ submatrix of $S$.

### 4.2 The Monomial Ordering

To make the description of our construction easier, we use a special "blockwise" ordering of monomials:

- The first block (consisting of $D_1$ monomials) contains the monomials which appear in the first Rainbow layer (i.e. the monomials $x_i x_j$ $(1 \leq i \leq v_1,\ i \leq j \leq v_2)$).
- The second block (consisting of $D_2 - D_1$ monomials) contains the monomials which appear in the second but not in the first Rainbow layer (i.e. the monomials $x_i x_j$ $((1 \leq i \leq v_1,\ v_2+1 \leq j \leq n) \vee (v_1+1 \leq i \leq v_2,\ i \leq j \leq n))$.
- The third block contains the remaining quadratic monomials (i.e. the monomials $x_i x_j$ $(v_2 + 1 \leq i \leq j \leq n)$).
- The fourth and last block consists of the linear and constant monomials.

Inside the blocks we use the lexicographical ordering.

**Example.** For $(v_1, v_2, n) = (2, 4, 6)$ we get the following ordering of monomials $x_1^2 > x_1x_2 > x_1x_3 > x_1x_4 > x_2^2 > x_2x_3 > x_2x_4 > x_1x_5 > x_1x_6 > x_2x_5 > x_2x_6 > x_3^2 > x_3x_4 > x_3x_5 > x_3x_6 > x_4^2 > x_4x_5 > x_4x_6 > x_5^2 > x_5x_6 > x_6^2 > x_1 > x_2 > x_3 > x_4 > x_5 > x_6 > 1$.

## 5 The Scheme

In this section we describe how to construct a Rainbow scheme with a partially cyclic key. We restrict here to the case of two Rainbow layers.[2]

### 5.1 Properties of the Rainbow Public Key

For the Rainbow signature scheme the public key is given as a the concatenation of three maps

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}.$$

We denote the concatenated map $\mathcal{F} \circ \mathcal{T}$ by $\mathcal{Q}$ and get

$$\mathcal{P} = \mathcal{S} \circ \mathcal{Q}.$$

[2] With a similar idea it is possible to create a partially cyclic public key for a Rainbow scheme with $u$ layers. We don't handle it here.

Note that the relation between the maps $\mathcal{Q}$ and $\mathcal{F}$ has the same form as the relation between public key and central map in the UOV case. Therefore we get exactly the same equations as in section 3.

$$q_{ij}^{(k)} = \sum_{r=1}^{n} \sum_{s=i}^{n} \alpha_{ij}^{rs} \cdot f_{rs}^{(k)} \ (1 \leq k \leq m), \tag{7}$$

where the coefficients $\alpha_{ij}^{rs}$ are given as

$$\alpha_{ij}^{rs} = \begin{cases} t_{ri} \cdot t_{si} & (i = j) \\ t_{ri} \cdot t_{sj} + t_{rj} \cdot t_{si} \text{ otherwise} \end{cases}. \tag{8}$$

Due to the special structure of the central map $\mathcal{F}$, we can reduce the number of terms in equation (7). We get

$$\begin{aligned} q_{ij}^{(k)} &= \sum_{r=1}^{v_1} \sum_{s=r}^{v_2} \alpha_{ij}^{rs} \cdot f_{rs}^{(k)} \ (1 \leq k \leq o_1) \\ q_{ij}^{(k)} &= \sum_{r=1}^{v_2} \sum_{s=r}^{n} \alpha_{ij}^{rs} \cdot f_{rs}^{(k)} \ (o_1 + 1 \leq k \leq m), \end{aligned} \tag{9}$$

Analogous to the case of the UOV we want to write equation (9) in a compact form. To do this, we define a quadratic $D_2 \times D_2$ matrix $A$ containing the coefficients $\alpha_{ij}^{rs}$

$$A = \left(a_{ij}^{rs}\right) \ (1 \leq i \leq v_2,\ i \leq j \leq n \text{ for the rows}, 1 \leq r \leq v_2,\ r \leq s \leq n \text{ for the columns}). \tag{10}$$

The order in which the $\alpha_{ij}^{rs}$ appear in the matrix, is thereby given by the monomial ordering defined in subsection 4.2 (for both rows and columns). We divide the matrix $A$ into the four parts

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix},$$

where $A_{11}$ is the upper left $D_1 \times D_1$ submatrix of $A$.

We write down the coefficients of $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{F}$ (according to the monomial ordering defined above) into three matrices $P'$, $Q'$ and $F'$ and divide these matrices as follows

We define the matrices $P$, $Q$ and $F$ to be the matrices consisting of the first $D_2$ columns of $P'$, $Q'$, resp. $F'$. With these definitions we get the following relations between the three matrices $P$, $Q$ and $F$:

$$P = S \cdot Q \text{ or } \begin{pmatrix} B_1 & C_1 \\ & B_2 \end{pmatrix} = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} \cdot \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} \tag{11}$$

$$Q = F \cdot A^T \text{ or } \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} = \begin{pmatrix} F_1 & 0 \\ & F_2 \end{pmatrix} = \begin{pmatrix} A_{11}^T & A_{21}^T \\ A_{12}^T & A_{22}^T \end{pmatrix} \tag{12}$$

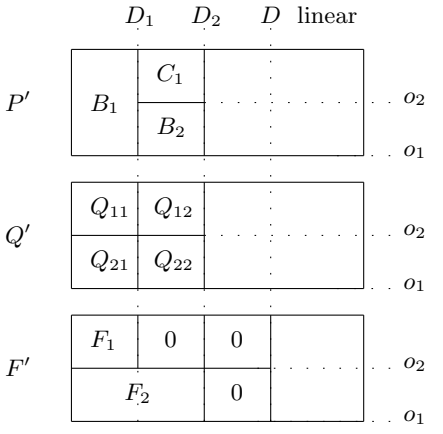


**Fig. 1.** Layout of the matrices $P'$, $Q'$ and $F'$

### 5.2 Construction

Additionally to the requirement that $S$ and $T$ are invertible, which is needed for the correctness of the scheme, we need the following assumptions to be true:

- The lower right $o_2 \times o_2$ submatrix $S_{22}$ of $S$ must be invertible.
- The transformation matrix $A$ must be invertible.
- The upper left $D_1 \times D_1$ submatrix $A_{11}$ of $A$ must be invertible.

To justify these assumptions we carried out a number of experiments. For each of the values of $(v_1, o_1, o_2)$ listed in Table 1 we created 1000 matrices $S$ and $A$ and observed how many of them were invertible.

**Table 1.** Percentage of invertible (sub-)matrices

| Rainbow$(256, v_1, o_1, o_2)$ | (4,2,2) | (9,6,6) | (11,9,9) | (14,11,11) | (17,13,13) |
|---|---|---|---|---|---|
| invertible matrices $S_{22}$ | 99.6 | 99.8 | 99.5 | 99.4 | 99.6 |
| invertible matrices $A$ | 99.8 | 99.7 | 99.6 | 99.8 | 99.7 |
| invertible matrices $A_{11}$ | 99.5 | 99.6 | 99.4 | 99.5 | 99.4 |

At the beginning of our construction we assign the elements of $B_1$ and $B_2$ elements of $K$, so that they get a compact structure.

For this we choose two vectors $\mathbf{a}^{(1)} = (a_1^{(1)}, \ldots, a_{D_1}^{(1)}) \in K^{D_1}$ and $\mathbf{a}^{(2)} = (a_1^{(2)}, \ldots, a_{D_2-D_1}^{(2)}) \in K^{D_2-D_1}$ at random. Then we set

$$b_{ij}^{(1)} = a_{((j-i) \bmod D_1)+1}^{(1)} \tag{13}$$

for the elements of the $m \times D_1$ matrix $B_1$ and

$$b_{ij}^{(2)} = a_{((j-i) \bmod (D_2-D_1))+1}^{(2)} \tag{14}$$

for the elements of the $o_2 \times (D_2 - D_1)$ matrix $B_2$.

Our goal is to compute the coefficients of the central map $F$ in such a way that $B_1$ and $B_2$ appear in the matrix $P$ representing the public key as shown in figure 1. From equations (11) and (12) we get

$$\begin{pmatrix} Q_{11} \\ Q_{21} \end{pmatrix} = S^{-1} \cdot B_1 \tag{15}$$

$$F_1 = Q_{11} \cdot (A_{11}^{-1})^T \tag{16}$$

$$Q_{12} = F_1 \cdot A_{21}^T \tag{17}$$

$$Q_{22} = S_{22}^{-1} \cdot (B_2 - S_{21} \cdot Q_{12}) \tag{18}$$

$$F_2 = (Q_{21}||Q_{22}) \cdot (A^{-1})^T \tag{19}$$

### 5.3 Key Generation and Key Sizes

*Key Generation*

1. Choose randomly two vectors $\mathbf{a}^{(1)} \in K^{D_1}$ and $\mathbf{a}^{(2)} \in K^{D_2-D_1}$. Compute the entries of the matrices $B_1$ and $B_2$ by formulas (9) and (10).
2. Choose randomly two affine invertible maps $\mathcal{S} = (S, c_S) : K^m \to K^m$ and $\mathcal{T} = (T, c_T) : K^n \to K^n$. If the matrix $S_{22}$ (see subsection 4.1) is not invertible, choose another map $\mathcal{S}$.
3. Compute for $\mathcal{T}$ the corresponding transformation matrix $A$ using (10) and (8). Both $A$ and its upper left $D_1 \times D_1$ submatrix $A_{11}$ have to be invertible. If this is not the case, choose another map $\mathcal{T}$.
4. Compute the matrix $\begin{pmatrix} Q_{11} Q_{21} \end{pmatrix}$ using (15) .
5. Compute the quadratic coefficients of the central polynomials of the first layer by formula (16).
6. Compute the entries of the matrices $Q_{12}$ and $Q_{22}$ by formulas (17) and (18).
7. Compute the quadratic coefficients of the central polynomials of the second Rainbow layer by formula (19).
8. Choose the coefficients of the linear and constant terms of the central polynomials at random.
9. Compute the public key of the scheme by $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$.

The resulting public key has the form shown in figure 1.

The *public key* consists of the vectors $\mathbf{a}^{(1)}$ and $\mathbf{a}^{(2)}$, the matrix $C_1 = S_{11} \cdot Q_{12} + S_{12} \cdot Q_{22}$ and the last $\frac{(n+1)\cdot(n+2)}{2} - D_2$ columns of the matrix $P$.

The *private key* consists of the maps $\mathcal{S}$, $\mathcal{Q}$ and $\mathcal{T}$.

Note that both public and private keys of our scheme are from a subset of all valid Rainbow public resp. private keys. So, each instance of our scheme can be seen as a Rainbow scheme.

The *size of the public key* is

$$D_1+(D_2-D_1)+o_1\cdot(D_2-D_1)+m\cdot\left(\frac{(n+1)\cdot(n+2)}{2}-D_2\right)=m\cdot\frac{(n+1)\cdot(n+2)}{2}-o_1\cdot D_1-(o_2-1)\cdot D_2 \tag{20}$$

field elements, the *size of the private key*

$$m\cdot(m+1)+n\cdot(n+1)+\sum_{l=1}^{2}o_l\cdot\left(v_l\cdot o_l+\frac{v_l\cdot(v_l+1)}{2}+v_{l+1}+1\right)\text{ field elements.} \tag{21}$$

*Signature generation* and *verification* work as for the standard Rainbow scheme.

### 5.4 Efficiency of the Verification Process

Besides the considerable reduction of the public key size, the number of multiplications needed in the verification process is decreased by about 30 %.

This can be seen as follows: To evaluate an arbitrary public key, for every quadratic term two $K$-multiplications are needed. Together with the $n$ multiplications for the linear terms, one needs $n\cdot(n+2)$ multiplications for each polynomial. Hence, to evaluate the whole public key, one needs

$$m\cdot n\cdot(n+2)\ K-\text{multiplications} \tag{22}$$

When evaluating our partially cyclic public key, some of the multiplications can be used several times (For example, $a_1^{(1)}\times x_1$ appears in every of the $m$ public polynomials.) Thus, we do not have to carry out all the multiplications one by one. A close analysis shows, that by using this strategy we can reduce the number of K-multiplications needed in the verification process to

$$m\cdot n\cdot(n+2)-\left(\frac{m}{2}\cdot(2\cdot v_1\cdot v_2-v_1^2-v_1)+\frac{o_2}{2}\cdot(v_1^2-2v_1v_2-v_1+2v_2v_3-v_2^2-v_2)\right), \tag{23}$$

which, for $(v_1,o_1,o_2)=(17,13,13)$, leads to a reduction of 30 %.

## 6 Security

In this section we look at known attacks against the Rainbow signature scheme and study their effects against our scheme.

### 6.1 Direct Attacks [BB08], [YC07]

The most straightforward way for an attacker to forge a signature for a message $h$ is to solve the public system $P(\mathbf{x})=h$ by an algorithm like XL or a Gröbner Basis method. To study the security of our scheme against direct attacks, we carried out experiments with MAGMA [BC97], which contains an

efficient implementation of Faugeres $F_4$-algorithm [Fa99] for computing Gröbner Bases. Table 2 shows the results of our experiments against random systems, the standard Rainbow scheme and our partially cyclic version.

As the table shows, $F_4$ cannot solve our systems significantly faster than those of the standard Rainbow scheme.

**Definition 1.** *Let* $p(\mathbf{x}) = p(x_1, \ldots, x_n)$ *be a quadratic multivariate polynomial and*

$$dp(\mathbf{x}, \mathbf{c}) = p(\mathbf{x} + \mathbf{c}) - p(\mathbf{x}) - p(\mathbf{c}) + p(\mathbf{0})$$

*its discrete differential. For* $p$ *we define a matrix* $H_p$ *by*

$$dp = \mathbf{x}^T \cdot H_p \cdot \mathbf{c}$$

*For the matrix* $H_{p_i}$ *representing the quadratic part of the* $i$*-th public polynomial we write in short* $H_i$*.*

### 6.2 Rainbow-Band-Separation [DY08]

The goal of this attack is to find an equivalent private key by which one can forge signatures for arbitrary messages. One tries to find a basis change of variables which transforms the matrices $H_i$ into "Rainbow form" (see figure 2)

To achieve this, one has to solve several overdetermined systems of quadratic equations. The complexity of the attack is determined by the complexity of its first step, which consists of solving an overdetermined system of $m + n - 1$ quadratic equations in $n$ variables. Table 3 shows the results of our experiments with the Rainbow Band Separation attack. The quadratic systems were again solved with MAGMA. As the table shows, the RBS attack can not take an advantage out of the special structure of our public key.

**Table 2.** Results of the experiments with direct attacks

| $(v_1, o_1, o_2)$ | (8,5,6) | (9,6,6) | (10,6,7) | (11,7,7) |
|---|---|---|---|---|
| cyclicRainbow | 406 s | 3135 s | 23528 s | 220372 s |
| Rainbow | 405 s | 3158 s | 23560 s | 222533 s |
| random system | 408 s | 3178 s | 23621 s | 221372 s |

| | | |
|---|---|---|
| $*_{v_1 \times v_1}$ | $*_{v_1 \times o_1}$ | $0_{v_1 \times o_2}$ |
| $*_{o_1 \times v_1}$ | $0_{o_1 \times o_1}$ | $0_{o_1 \times o_2}$ |
| $0_{o_2 \times v_1}$ | $0_{o_2 \times o_1}$ | $0_{o_2 \times o_2}$ |

$1 \leq i \leq o_1$

| | | |
|---|---|---|
| $*_{v_1 \times v_1}$ | $*_{v_1 \times o_1}$ | $*_{v_1 \times o_2}$ |
| $*_{o_1 \times v_1}$ | $*_{o_1 \times o_1}$ | $*_{o_1 \times o_2}$ |
| $*_{o_2 \times v_1}$ | $*_{o_2 \times o_1}$ | $0_{o_2 \times o_2}$ |

$o_1 + 1 \leq i \leq m$

**Fig. 2.** Matrices $H_i$ in the Rainbow form

**Table 3.** Results of our experiments with the Rainbow Band Separation attack

| $(256, v_1, o_1, o_2)$ | (8,5,6) | (9,6,6) | (10,6,7) | (11,7,7) |
|---|---|---|---|---|
| cyclicRainbow | 403 s | 3163 s | 23583 s | 223726 s |
| Rainbow | 412 s | 3152 s | 23652 s | 224273 s |

### 6.3 MinRank Attack [GC00], [BG06]

In the MinRank attack one tries to find linear combinations $H = \sum_{i=1}^{m} \alpha_i H_i$ of the matrices representing the homogeneous quadratic parts of the public polynomials such that $\text{rank}(H) \leq v_2$. This linear combination are with high probability linear combinations of the central polynomials of the first Rainbow layer.

These linear combinations can be found by choosing randomly a vector $\mathbf{v} \in K^n$ and trying to solve the system $(\sum_{i=1}^{m} \alpha_i H_i) \cdot \mathbf{v} = \mathbf{0}$ for the $\alpha_i$ $(i = 1, \ldots, m)$. After having found $o_1$ linear combinations of this form, the attacker is able to extract the first Rainbow layer. After that, it is possible to recover the other layers one by one and therefore to find an equivalent private key. The complexity of the MinRank attack is determined by the complexity of finding the linear combinations, which is about $o_1 \cdot q^{v_1+1} \cdot m^3$.

Table 4 shows the results of our experiments with the MinRank attack. For every parameter set listed in the table we created 100 Rainbow schemes and attacked each of these schemes by the MinRank attack. The table shows the average number of vectors $\mathbf{v}$ we had to test until finding $o_1$ linear combinations of rank $\leq v_2$.

As the table shows, linear combinations with rank $\leq v_2$ can not be found easier for our scheme than for the standard Rainbow scheme. Furthermore, for our scheme these linear combinations do not show any visible structure. Note that the parameters listed in the table are far below those actually used for Rainbow. For the parameters proposed in subsection 2.2 the complexity of the attack is much higher than $2^{80}$.

### 6.4 HighRank Attack [GC00], [DY08]

In the HighRank attack one tries to identify the variables appearing the lowest number of times in the central equations. These are the variables of the last Rainbow layer.

To do this, one forms random linear combinations $H$ of the matrices $H_i$. If $H$ has nontrivial kernel, one checks if the solution set of $(\sum_{i=1}^{m} \lambda_i H_i) \cdot \ker H = \mathbf{0}$ has dimension $n - o_2$. Then, with probability $q^{-o_2}$, we have

$$\ker(H) \subseteq \mathcal{T}(\mathcal{O}) \text{ with } \mathcal{O} = \{\mathbf{x} \in K^n | x_1 = \cdots = x_{n-o_2} = 0\}.$$

**Table 4.** Results of experiments with the MinRank attack

| $(q, v_1, o_1, o_2)$ | (8,3,2,2) | (8,4,3,3) | (16,3,2,2) | (16,4,3,3) |
|---|---|---|---|---|
| cyclicRainbow | 7635 | 83534 | 124174 | 2982618 |
| Rainbow | 7724 | 84676 | 125463 | 3028357 |

After having found a basis of $\mathcal{T}^{-1}(\mathcal{O})$, one extends this basis to a basis of the whole space $K^n$. This enables an attacker to forge signatures the same way as a legitimate user. The complexity of the attack is determined by the complexity of finding a basis of $\mathcal{T}^{-1}(\mathcal{O})$, which is about $q^{o_u} \cdot m^3$.

For each of the parameter sets listed in Table 5 we created 100 Rainbow schemes. The table shows the average number of linear combinations we had to test until finding a basis of $\mathcal{T}^{-1}(\mathcal{O})$.

**Table 5.** Results of our experiments with the HighRank attack

| $(q, v_1, o_1, o_2)$ | (8,3,2,2) | (8,4,3,3) | (16,3,2,2) | (16,4,3,3) |
|---|---|---|---|---|
| cyclicRainbow | 64.2 | 511.5 | 257.3 | 4093.7 |
| Rainbow | 65.1 | 512.3 | 256.8 | 4097.8 |

As the table shows, for both the Rainbow and the cyclic Rainbow scheme we have to test nearly the same number of linear combinations to find a basis of $\mathcal{T}^{-1}(\mathcal{O})$. Note that the parameters listed in the table are far below those actually used for Rainbow. For the parameters proposed in subsection 2.2 the complexity of the attack is much higher than $2^{80}$.

### 6.5 UOV Attack [KP99]

Since a Rainbow scheme can be seen as a UOV scheme with $v_u$ vinegar and $o_u$ oil variables, it can be attacked by the UOV attack of Kipnis and Shamir [KP99]. The goal of this attack is to find the pre-image $\mathcal{T}^{-1}(\mathcal{O})$ of the Oil-subspace $\mathcal{O} = \{\mathbf{x} \in K^n | x_1 = \cdots = x_{n-o_2} = 0\}$ under the affine invertible map $\mathcal{T}$. One chooses randomly a linear combination $H$ of the matrices $H_1, \ldots, H_m$ and sets $G := H \cdot H_j^{-1}$ for some $j \in \{1, \ldots, m\}$. After that, one computes all the minimal invariant subspaces of $G$. With high probability, these invariant subspaces are also subspaces of $\mathcal{T}^{-1}(\mathcal{O})$. After having found a basis of $\mathcal{T}^{-1}(\mathcal{O})$, one extends this basis to a basis of the whole space $K^n$. This enables an attacker to forge signatures for arbitrary messages. The complexity of the attack is determined by the complexity of finding a basis of $\mathcal{T}^{-1}(\mathcal{O})$, which is about $q^{n-2 \cdot o_u} \cdot m^3$.

For each of the parameter sets listed in the table we created 100 instances of both schemes. Then we attacked these instances by the UOV-attack. Table 6 shows the average number of matrices $G$ we had to test until finding a basis of $\mathcal{T}^{-1}(\mathcal{O})$.

**Table 6.** Results of the experiments with the UOV attack

| $(16, v_1, o_1, o_2)$ | (3,2,2) | (5,3,3) | (9,6,6) | (12,10,10) |
|---|---|---|---|---|
| cyclicRainbow | 1734 | 531768 | 852738 | 1183621 |
| Rainbow | 1728 | 532614 | 847362 | 1146382 |

As the table shows, for both schemes we have to test nearly the same number of matrices $G$ to find a basis of $\mathcal{T}^{-1}(\mathcal{O})$. Note that the parameters listed in the table are far below those actually used for Rainbow. For the parameters proposed in subsection 2.2 the complexity of the attack is much higher than $2^{80}$.

### 6.6 Summary

As the previous five subsections showed, known attacks against the Rainbow signature scheme do not work significantly better in our case, which means that they can not use the special structure of our public key. So, in this sense our scheme seems to be secure and we do not have to increase our parameter sets.

However, in the future we are going to study the security of our scheme under other attacks, e.g. decomposition attacks [FP09]. It might also be possible that some dedicated attacks against our scheme exist.

## 7 Parameters

Based on the security analysis in the previous section we propose for our scheme the same parameters as suggested for the standard Rainbow Scheme (see section 2), namely

$$(q, v_1, o_1, o_2) = (256, 17, 13, 13).$$

Table 7 compares our scheme with others from the UOV family. Additionally to the parameters proposed above, the table contains key- and signature sizes for a more conservative parameter set for $m = 28$.

For 26 equations, we get a key size reduction of $\frac{25.9-10.2}{25.9} = 62\%$, for 28 equations $\frac{32.2-12.9}{32.2} = 60\%$.

**Table 7.** Comparison of different UOV-based signature schemes

| Scheme | public key size (kB) | private key size (kB) | hash size (bit) | signature size (bit) |
|---|---|---|---|---|
| UOV(256,26,52) | 80.2 | 76.1 | 208 | 624 |
| cyclicUOV(256,26,52) | 14.5 | 76.1 | 208 | 624 |
| Rainbow(256,17,13,13) | 25.9 | 19.1 | 208 | 344 |
| cyclicRainbow(256,17,13,13) | 10.2 | 19.1 | 208 | 344 |
| UOV(256,28,56) | 99.9 | 92.8 | 224 | 672 |
| cyclicUOV(256,28,56) | 16.5 | 92.8 | 224 | 672 |
| Rainbow(256,19,14,14) | 32.2 | 24.3 | 224 | 376 |
| cyclicRainbow(256,19,14,14) | 12.9 | 24.3 | 224 | 376 |

## 8 Conclusion

In this paper we showed a way how to extend the approach of [PB10] to the Rainbow signature scheme. The result is a Rainbow-like scheme, which reduces the size of the public key by 62 % and the number of field multiplications needed during the verification process by 30 %. We believe that our idea might be a good approach for implementing the Rainbow scheme on low cost devices, e.g. smartcards. Furthermore, it's a quite general idea, which should be applicable to a number of other SingleField Scheme, for example enSTS [TG10].

Points of research for the future are in particular security issues of the scheme as well as the use of PRNG's to construct the public key.

## Acknowledgements

We thank Enrico Thomae and Christopher Wolf for fruitful discussions and helpful comments. Furthermore we want to thank the anonymous reviewers for their valuable comments which helped to improve the paper.

## References

[BB08] Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post Quantum Cryptography. Springer, Heidelberg (2009)

[BC97] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24(3-4), 235–265 (1997)

[BF09] Bettale, L., Faugere, J.-C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Math. Cryptology, 177–197 (2009)

[BG06] Billet, O., Gilbert, H.: Cryptanalysis of Rainbow. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 336–347. Springer, Heidelberg (2006)

[DS05] Ding, J., Schmidt, D.: Rainbow, a new multivariate polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005)

[Di04] Ding, J.: A new variant of the Matsumoto-Imai cryptosystem through perturbation. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 266–281. Springer, Heidelberg (2004)

[DY08] Ding, J., Yang, B.-Y., Chen, C.-H.O., Chen, M.-S., Cheng, C.M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257. Springer, Heidelberg (2008)

[DW07] Ding, J., Wolf, C., Yang, B.-Y.: $\ell$-invertible Cycles for Multivariate Quadratic Public Key Cryptography. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 266–281. Springer, Heidelberg (2007)

[DY07] Ding, J., Yang, B.-Y., Cheng, C.-M., Chen, O., Dubois, V.: Breaking the symmetry: a Way to Resist the new Differential Attack, eprint 366/2007

[Fa99] Faugére, J.C.: A new efficient algorithm for computing Groebner bases (F4). Journal of Pure and Applied Algebra 139, 61–88 (1999)

[FP09] Faugére, J.C., Perret, L.: An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. Journal of Symbolic Computation 44(12), 1676–1689 (2009)

[GC00] Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 44–57. Springer, Heidelberg (2000)

[HW05] Hu, Y.-H., Wang, L.-C., Chou, C.-P., Lai, F.: Similar Keys of Multivariate Public Key Cryptosystems. In: Desmedt, Y.G., Wang, H., Mu, Y., Li, Y. (eds.) CANS 2005. LNCS, vol. 3810, pp. 211–222. Springer, Heidelberg (2005)

[KP99] Kipnis, A., Patarin, L., Goubin, L.: Unbalanced Oil and Vinegar Schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)

[KS98] Kipnis, A., Shamir, A.: Cryptanalysis of the Oil and Vinegar Signature scheme. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 257–266. Springer, Heidelberg (1998)

[MI88] Matsumoto, T., Imai, H.: Public Quadratic Polynomial-Tuples for efficient Signature-Verification and Message-Encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)

[Pa96] Patarin, J.: Hidden Field equations (HFE) and Isomorphisms of Polynomials (IP). In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 38–48. Springer, Heidelberg (1996)

[Pa97] Patarin, J.: The oil and vinegar signature scheme, presented at the Dagstuhl Workshop on Cryptography (September 1997)

[PB10] Petzoldt, A., Bulygin, S., Buchmann, J.: A Multivariate Signature Scheme with a partially cyclic public key. In: Proceedings of SCC 2010, pp. 229–235 (2010)

[PB1a] Petzoldt, A., Bulygin, S., Buchmann, J.: Selecting Parameters for the Rainbow Signature Scheme. In: Sendrier, N. (ed.) Post-Quantum Cryptography. LNCS, vol. 6061, pp. 218–240. Springer, Heidelberg (2010)

[PC01] Patarin, J., Courtois, N., Goubin, L.: Flash, a fast multivariate signature algorithm. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 298–307. Springer, Heidelberg (2001)

[PG98] Patarin, J., Goubin, L., Courtois, N.: C*-+ and HM: Variations around two schemes of T. Matsumoto and H. Imai. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 35–50. Springer, Heidelberg (1998)

[TG10] Tsuji, S., Gotaishi, M., Tadaki, K., Fujita, R.: Proposal of a Signature Scheme based on STS Trapdoor. In: Sendrier, N. (ed.) Post-Quantum Cryptography. LNCS, vol. 6061, pp. 201–217. Springer, Heidelberg (2010)

[WY06] Wang, L.C., Yang, B.Y., Hu, Y.H., Lai, F.: A medium field multivariate public-key encryption scheme. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 132–149. Springer, Heidelberg (2006)

[YC05] Yang, B.-Y., Chen, J.-M.: Building secure tame like multivariate public-key cryptosystems: The new TTS. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 518–531. Springer, Heidelberg (2005)

[YC07] Yang, B.-Y., Chen, J.-M.: All in the XL family: Theory and practice. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005)