2020

Choosing subfields for LUOV and lifting fields for rainbow

Dung Hoang Duong
University of Wollongong, hduong@uow.edu.au

Le van Luyen

Ha Tran

Choosing subfields for LUOV and lifting fields for rainbow

Abstract

© The Institution of Engineering and Technology 2019 Multivariate public key cryptography is one of the main candidates for post-quantum cryptography. Rainbow, an improved (multi-layer) version of unbalanced oil and vinegar (UOV), is one of the most famous multivariate signature schemes that is a promising candidate for NIST standardisation. At INDOCRYPT 2017, Beullens and Preneel introduced a new variant LUOV of UOV. Their idea is to generate a UOV scheme over the binary field L = F2 and then lift it into a bigger field K = F2r and hence dramatically reduce the public key size. In this study, the authors first theoretically deduce the choice for the subfield L (which is different from F2) which results in smaller signature sizes (up to 40%). Moreover, they extend the idea to Rainbow and theoretically yield the optimal choice for the subfield L over which a Rainbow is generated before being lifted to K. As a result, they can reduce the public key size of the obtained Rainbow scheme up to at least 36%.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Duong, H., van Luyen, L. & Tran, H. (2020). Choosing subfields for LUOV and lifting fields for rainbow. IET Information Security, 14 (2), 196-201.

Choosing Subfields for LUOV and Field Lifting for Rainbow

Dung Hoang Duong[1], Le Van Luyen[2], and Ha Thanh Nguyen Tran[3]

[1] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong
Northfields Avenue, Wollongong NSW 2522, Australia
{hduong}@uow.edu.au

[2] Faculty of Mathematics and Computer Science, University of Science, VNU-HCMC, Vietnam
lvluyen@hcmus.edu.vn

[3] Department of Mathematics and Statistics, University of Calgary, Canada
hatran1104@gmail.com

Abstract. Multivariate public key cryptography (MPKC) is one of the main candidates for post-quantum cryptography. Rainbow, an improved (multi-layer) version of Unbalanced Oil and Vinegar (UOV), is one of the most famous multivariate signature schemes that is a promising candidate for NIST standardization. At INDOCRYPT 2017, Beullens and Preneel [2] introduced a new variant LUOV of UOV. Their idea is to generate a UOV scheme over the binary field $L = \mathbb{F}_2$ and then lift it into a bigger field $K = \mathbb{F}_{2^r}$ and hence dramatically reduces the public key size. In this paper, we first theoretically deduce the choice for the subfield L (which is different from $\mathbb{F}_2$) which results in smaller signature sizes (up to 40%). Moreover, we extend the idea to Rainbow and theoretically yield the optimal choice for the subfield L over which a Rainbow is generated before being lifted to K. As a result, we can deduce the public key size of the obtained Rainbow scheme up to 37.5%.

1 Introduction

Post-quantum cryptography is a new direction in the last two decades after the thread of polynomial quantum algorithms of Shor [23] which totally break currently most widely used public key cryptosystems RSA [22], DSA [13] and ECC [12]. It takes much more attention recently after the call of NIST [15] for proposals of post-quantum cryptosystems to be standardized in near future. There have been a number of submissions for the first round [16] and the first NIST conference has been recently held for discussions [17].

Multivariate cryptography is one of the main candidates for this standardization [15,16]. Multivariate schemes are in general very fast and require only modest computational resources, which can be used on low cost devices like smart cards and RFID chips [4,5]. Multivariate schemes were first proposed by Matsumoto and Imai in the mid 1980s [14]. Since then there have been a rich

development of designing multivariate schemes into several directions, e.g. Big-Field or SingleField schemes. The first SingleField signature scheme was the Oil and Vinegar (OV) signature scheme, introduced by Patarin after he broke the Matsumoto-Imai scheme [18]. Soon after, Patarin broke the OV schemes and introduced a variant [11], which is called Unbalanced Oil and Vinegar (UOV) scheme. After around two decades, UOV schemes are still secure up to choices of parameters. While the signature generation of UOV is very efficient, it has a very large public key. To deal with this, several improvements have been suggested. The first improvement was made by Ding and Schmidt [7], who proposed the Rainbow signature scheme, which can be seen as a multi-layer version of UOV with smaller keys and shorter signatures. The Rainbow signature scheme is still secure for around Other important improvements were made by Petzoldt [19] to dramatically reduce the public key sizes of UOV schemes.

At Indocrypt 2017, Beullens and Preneel [2] proposed a new variant of UOV, called LUOV. Their idea is to first generate a UOV scheme over the binary field $\mathbb{F}_2$, and then lift into the bigger field $\mathbb{F}_{2^r}$ to get a UOV scheme over $\mathbb{F}_{2^r}$. Associated to Petzoldt's methods [19], their schemes have small public key sizes and are efficient in verification[4]. However, for security reason, LUOV is a large system of large number of variables, which result in large signature sizes and blow up the ratio between the vinegar and oil variables.

In this paper we revisit the LUOV scheme [2] and theoretically derive the choice of subfields $L = \mathbb{F}_{2^t}$ over which the UOV is first generated before being lifted to the big field $\mathbb{F}_{2^r}$. As a result, we can reduce the number of variables and equations which imply to deduce up to 40% of the signature sizes, compared to those of LUOV. As a trade-off, since using non-binary field L, the public key sizes of our schemes increase around 30% to those of LUOV[5].

In addition, we extend the idea of field lifting to Rainbow signature schemes. We use our method to theoretically deduce the choice of the subfield L and construct the new LRainbow scheme based on the aforementioned technique for LUOV. As a result, we can reduce the public key size up to 37.5%.

2 Preliminaries

In this section, we recall some basic concepts of multivariate public key cryptography. The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials over a finite field K. The security of multivariate schemes is based on the *MQ-Problem* which asks for a solution of a given system of multivariate quadratic polynomials over the field K. The MQ-Problem is proven to be NP-hard even for quadratic polynomials over the field $\mathbb{F}_2$ [10].

To build a multivariate public key cryptosystem, one starts with an easily invertible quadratic map $\mathcal{F} : K^n \to K^m$ (*central map*). To hide the structure

[4] LUOV has been submitted to NIST [17] with some optimizations. In this paper, we just compare our work with the original LUOV.

[5] for 120, 196 and 256 bit security, but it is approximately the same in 100 bit security; see Table 3 for details.

of $\mathcal{F}$ in the public key, one composes it with two invertible affine (or linear) maps $\mathcal{T} : K^m \to K^m$ and $\mathcal{S} : K^n \to K^n$. The *public key* is therefore given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^m$. The *private key* consists of $\mathcal{T}, \mathcal{F}$ and $\mathcal{S}$.

In this paper we consider multivariate signature schemes. For these schemes, we require $n \geq m$, which ensures that every message has a signature.

Signature Generation: To generate a signature for a message (or its hash value) $\mathbf{d} \in K^m$, one computes recursively $\mathbf{w} = \mathcal{T}^{-1}(\mathbf{d}) \in K^m$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{w}) \in K^n$ and $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$. $\mathbf{z} \in K^n$ is the signature of the message $\mathbf{d}$. Here, $\mathcal{F}^{-1}(\mathbf{w})$ means finding one (of possibly many) pre-image of $\mathbf{w}$ under the central map $\mathcal{F}$.

Signature Verification: To check the authenticity of a signature $\mathbf{z} \in K^n$, the verifier simply computes $\mathbf{d}' = \mathcal{P}(\mathbf{z})$. If the result is equal to the message $\mathbf{d}$, the signature is accepted, otherwise rejected.

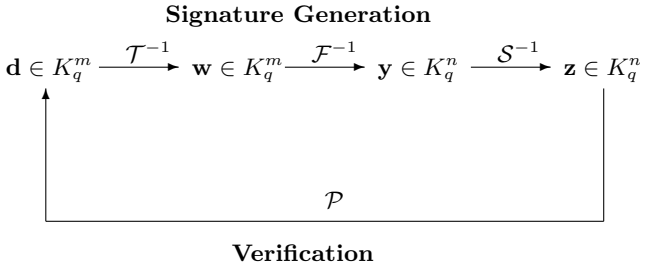

Fig. 1. Two processes of multivariate signature schemes

3 Unbalanced Oil and Vinegar signature scheme

In this section, we first recall the construction of Unbalanced Oil and Vinegar (UOV) signature scheme in Section 3.1 and a method of Petzoldt [19] to reduce the public key of UOV in Section 3.2. Lastly, the LUOV scheme by Beullens and Preneel [2] is described in Section 3.3

3.1 UOV Signature Schemes

Let $K = \mathbb{F}_q$ be the finite field with q elements and let $n = v + o$ with v, o positive integers. An oil-vinegar quadratic polynomial over K is of the form

$$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq v}} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c,$$

with coefficients $a_{ij}, b_i, c \in K$. The variables $x_1, \ldots, x_v$ are called vinegar variables, and $x_{v+1}, \ldots, x_n$ the oil variables. Note that in an oil-vinegar polynomial, the oil and vinegar variables are not fully mixed, i.e., there are no quadratic terms x^2 for oil variables x. A UOV scheme is constructed as the following.

The central map $\mathcal{F} : K^n \to K^o, (x_1, \ldots, x_n) \mapsto (f^{(1)}, \ldots, f^{(o)})$ consists of o oil-vinegar polynomials

$$f^{(1)} = \sum_{\substack{1 \le i \le n \\ 1 \le j \le v}} a_{ij}^{(1)} x_i x_j + \sum_{i=1}^{n} b_i^{(1)} x_i + c^{(1)},$$

$$\cdots\cdots\cdots$$

$$f^{(o)} = \sum_{\substack{1 \le i \le n \\ 1 \le j \le v}} a_{ij}^{(o)} x_i x_j + \sum_{i=1}^{n} b_i^{(o)} x_i + c^{(o_1)},$$

where the coefficients $a_{ij}^{(k)}, b_{ij}^{(k)}, c^{(k)}$ are in K. Choose randomly two invertible affine maps $\mathcal{S} : K^n \to K^n$ and $\mathcal{T} : K^o \to K^o$. The public key is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^o$, and the private key consists of $\mathcal{T}$, $\mathcal{F}$ and $\mathcal{S}$.

To sign a message $\mathbf{m} = (m_1, \ldots, m_o) \in K^o$, we first compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{m}) = (y_1, \ldots, y_o)$ and do the following.

(1) Randomly choose vinegar values $a = (a_1, \ldots, a_v) \in K^v$ and plug into the polynomials in the central map to obtain $\bar{f}^{(1)}, \ldots, \bar{f}^{(o)}$.
(2) Solving the linear system $\bar{f}^{(i)} = y_i$ with $i = 1, \ldots, o$ yields solution $(b_1, \ldots, b_o)$. If there is no solution then come back to Step (1).
(3) Set $\mathbf{x} = (a_1, \ldots, a_v, b_1, \ldots, b_o)$. A signature is computed by $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$. A signature $\mathbf{s}$ is accepted if $\mathcal{P}(\mathbf{s}) = \mathbf{m}$, otherwise it is rejected.

The public key of the scheme consists of o quadratic equations in n variables, and hence the public key has size

$$o \cdot \frac{(n+1)(n+2)}{2} \quad \text{field elements}$$

and the size of the private key is

$$o \cdot (o+1) + n(n+1) + o \cdot \left(\frac{v(v+1)}{2} + v \cdot o + n + 1 \right)$$

field elements.

3.2 Reducing public key size of UOV

Petzoldt [19] proposed a method to reduce the public key size of UOV with the main idea as follows.

Set

$$D = \frac{v(v+1)}{2} + ov$$

be the number of quadratic terms of each oil-vinegar polynomial in the central map. One should arrange the public polynomials in lexicographic order and set up the corresponding matrix consisting of the coefficients. Let B be its $o \times D$ sub-matrix consisting of the coefficients of the quadratic terms on the public polynomials. Then Petzoldt choose the B to be circular, i.e., choose the first row randomly and other rows are just rotations of the first one. Other entries are randomly chosen. Using the structure of UOV, the chosen public key can be used to generate the corresponding private key. One important point is that generating such the public key has not found any risk to the security of the scheme. By that method, the CyclicUOV scheme now has public key size

$$D + o \cdot \left(\frac{o(o+1)}{2} + n + 1 \right) \quad \text{field elements.}$$

One can associate with the cyclic structure of UOV a Pseudo-Random-Number Generator (PRNG) or a Linear Feedback Shift Register (LFSR) for generating and storing the matrix B to reduce the public key significantly [19], as used in Beullens and Preneel [2]. In this paper, we just apply only the cyclic method and compute the corresponding public key size by above formula.

3.3 LUOV Signature Scheme

At INDOCRYPT 2017, Beullens and Preneel [2] introduced another method to reduce the public key size of UOV. Their idea is to first generate the UOV scheme over $\mathbb{F}_2$, i.e., the secret key $\mathcal{F}, \mathcal{S}, \mathcal{T}$ (and hence the public key $\mathcal{P}$) are chosen to be over $\mathbb{F}_2$. The keys are then lifted to the bigger field $\mathbb{F}_{2^r}$ to obtain a UOV scheme over $\mathbb{F}_{2^r}$. The public key of LUOV scheme now is

$$o \cdot \frac{(n+1)(n+2)}{2} \quad \text{bits.}$$

One then can apply a method of Petzoldt [19] mentioned in Section 3.2 to reduce the public key to

$$\frac{v(v+1)}{2} + o \cdot v + o \cdot \left(\frac{o(o+1)}{2} + n + 1 \right) \quad \text{bits.}$$

A signature consists of n elements of $\mathbb{F}_{2^r}$, hence it has size nr bits.

4 Choosing subfields for LUOV

In this section, we first revisit known attacks against UOV and from that derive the parameter choices for LUOV. To be precise, in order to generate LUOV over $\mathbb{F}_{2^r}$, we give a choice for a subfield $\mathbb{F}_{2^t}$ over which a UOV scheme is generated before being lifted to obtain a UOV scheme over $\mathbb{F}_{2^r}$. In LUOV, the authors chose $t = 1$, i.e., first generate a UOV scheme over $\mathbb{F}_2$. In Section 4.2, we show that our choice $t = 2$ yields a scheme with a slightly larger public key but much smaller signature size (around 40% reduced).

4.1 Security Analysis

In this section, we look at currently known attacks against UOV.

Direct Attacks The direct attack is the most straightforward attack to forge a signature by simply solving the equation $\mathcal{P}(\mathbf{x}) = \mathbf{d}$ given the message $\mathbf{d}$. One then can use a solver such as Gröbner basis techniques F_4 [9] and F_5 [1]. Since UOV is a underdetermined system, the most efficient technique to solve $\mathcal{P}(\mathbf{x}) = \mathbf{d}$ is the Hybrid method F_5 which fixes k variables and solve the system of m equations with $n - k$ variables. The complexity can be estimated as

$$\min_{k \geq 0} q^k \cdot \mathcal{O}\left(m \cdot \binom{n-k+d_{\text{reg}}-1}{d_{\text{reg}}}\right)^{\omega},$$

where $2 < \omega \leq 3$ is the linear algebra constant of solving a linear system and d_{reg} is the degree of regularity of the system.

It has been well known that general UOV schemes under direct attacks behave similar to random systems. It holds also for LUOV with $L = \mathbb{F}_2$, as in experiments in [2]. In such case, we can estimate the degree of regularity of LUOV to be the smallest d for which the coefficient of x^d in the expression

$$\frac{(1-x^2)^m}{(1-x)^{m-k}}$$

is non-positive.

UOV Attack The UOV attack tries to find an equivalent key to forge a signature. This was introduced by Paratin to break Balanced Oil and Vinegar scheme [11]. The attack can be generalized to the unbalanced case. The goal of this attack is to find the pre-image of the so called Oil subspace $\mathcal{O}$ under the affine transformation $\mathcal{S}$ where $\mathcal{O} = \{x \in K \mid x_1 = x_2 = \cdots = x_v = 0\}$. Finding this space allows us to separate the oil from the vinegar variables and recover the private key. The complexity of this attack is estimated as

$$q^{v-o-1} \cdot o^4.$$

4.2 Choosing subfields

We now consider the field $K = \mathbb{F}_{2^r}$ and would like to choose a subfield $L = \mathbb{F}_{2^t}$ with $t < r$ over which we generate a UOV scheme. We follow [2] to choose the fields K to be $\mathbb{F}_{2^{32}}, \mathbb{F}_{2^{48}}, \mathbb{F}_{2^{64}}$ and $\mathbb{F}_{2^{80}}$. In order to be secure against the direct attack, the public key should contain at least $27, 34, 50$ and 66 polynomials respectively for security level of 100 bits, 128 bits, 192 bits and 256 bits respectively. For a l bits security level, we require

$$2^{t(v-o-1)} \cdot o^4 > 2^l$$

which is equivalent to

$$t(v - o - 1) + 4\log(o) > l. \tag{1}$$

Since we generate UOV schemes over a subfield, it must be that $v > 2o$, compared to $v = 2o$ in usual UOV schemes. For the purpose of reducing the signature size, optimally choose $v \cong 2.5{\cdot}o$. Plugging each pair $(o, l) = (27, 100), (34, 128), (50, 192)$ and $(66, 256)$ into Equation (1), one obtains that $t = 2$ for all cases. This yields our variant for LUOV, which we call LUOV2.

We do experiments for LUOV2 against direct attack, and the results are recorded in Table 1. The Table 1 shows that our LUOV2 scheme behaves similar to the corresponding random system. Hence, we can use the analysis in Section 4.1 for evaluating the degree of regularity of our LUOV2 scheme and hence estimating the complexity of direct attack against LUOV2.

Table 1. Comparison of degree of regularity of LUOV2 and random system with several parameters over $\mathbb{F}_{2^{32}}$

(v,o)	(13,5)	(15,6)	(18, 7)	(20,8)	(23,9)	(25,10)
LUOV2	7	8	9	10	11	12
Random System	7	8	9	10	11	12

4.3 Parameters and Implementation

Table 3 shows our choice of parameters and comparison with LUOV [2] schemes. Here, each scheme is a UOV generated over $L = \mathbb{F}_{2^t}$ and then lifted into $K = \mathbb{F}_{2^r}$. The main difference of our scheme LUOV2 with LUOV scheme is that we choose $L = \mathbb{F}_{2^2}$ instead of $\mathbb{F}_2$ in [2]. As can be seen from Table 3, with our choice of $L = \mathbb{F}_{2^2}$, the public key size is almost similar to that of LUOV for 100-bit security, and approximately 30% larger for other security levels. However, our numbers of oil and vinegar variables are reduced, which decrease the signature sizes 40% compared to those of LUOV.

Table 2. Parametersand keysizes of LUOV [2] and LUOV2

Sec. Level	Scheme(r, t, o, v)	Public Key (kB)	Signature (kB)
100 bits	LUOV$(32, 1, 31, 134)$	4.21	0.6
	LUOV2$(\mathbf{32}, \mathbf{2}, \mathbf{27}, \mathbf{69})$	**4.27**	**0.36**
128 bits	LUOV$(48, 1, 38, 171)$	7.16	1.2
	LUOV2$(\mathbf{48}, \mathbf{2}, \mathbf{36}, \mathbf{91})$	**9.0**	**0.76**
192 bits	LUOV$(64, 1, 54, 256)$	17.96	2.4
	LUOV2$(\mathbf{64}, \mathbf{2}, \mathbf{50}, \mathbf{136})$	**22.3**	**1.49**
256 bits	LUOV$(80, 1, 70, 341)$	35.62	4.0
	LUOV2$(\mathbf{80}, \mathbf{2}, \mathbf{66}, \mathbf{183})$	**47.8**	**2.49**

5 LRainbow: Field Lifting for Rainbow

In this Section, we extend the idea of Beullens and Preneel [2] and Section 4 for Rainbow scheme [7]. We first recall the construction of Rainbow in Section 5.1, Petzoldt's method for reducing the public key size in Section 5.2 and attacks in Section 5.3. Then we introduce the field lifting version LRainbow of Rainbow (cf. Section 5.4) and the choice of subfield together with parameters and key sizes in Section 5.5.

5.1 Rainbow Signature Scheme

Rainbow signature schemes are multi-layer versions of UOV schemes. For convenience we introduce two layered Rainbow scheme (in design, there is no advantage of using more than two layers). Let $K = \mathbb{F}_q$ be the finite field with q elements $n = v + o_1 + o_2$ with v, o_1, o_2 positive integers. Set $m = o_1 + o_2$, $v_2 = o_1 + v_1$. The Rainbow central map $\mathcal{F} : K^n \to K^{o_1+o_2}, (x_1, \ldots, x_n) \mapsto (f_1, \ldots, f_{o_1+o_2})$ consists of $m = o_1 + o_2$ following polynomials

$$
\begin{aligned}
f^{(1)} &= \sum_{\substack{1\le i\le v_1+o_1\\ 1\le j\le v_1}} a_{ij}^{(1)} x_i x_j + \sum_{i=1}^{v_1+o_1} b_i^{(1)} x_i + c^{(1)},\\
&\cdots\cdots\cdots\\
f^{(o_1)} &= \sum_{\substack{1\le i\le v_1+o_1\\ 1\le j\le v_1}} a_{ij}^{(o_1)} x_i x_j + \sum_{i=1}^{v_1+o_1} b_i^{(o_1)} x_i + c^{(o_1)},\\
f^{(o_1+1)} &= \sum_{\substack{1\le i\le n\\ 1\le j\le v_1+o_1}} a_{ij}^{(o_1+1)} x_i x_j + \sum_{i=1}^{n} b_i^{(o_1+1)} x_i + c^{(o_1+1)},\\
&\cdots\cdots\cdots\\
f^{(o_1+o_2)} &= \sum_{\substack{1\le i\le n\\ 1\le j\le v_1+o_1}} a_{ij}^{(o_1+o_2)} x_i x_j + \sum_{i=1}^{n} b_i^{(o_1+o_2)} x_i + c^{(o_1+o_2)},
\end{aligned}
$$

where the coefficients $a_{ij}^{(k)}, b_{ij}^{(k)}, c^{(k)}$ are in K. Choose randomly two invertible affine maps $\mathcal{S} : K^n \to K^n$ and $\mathcal{T} : K^{o_1+o_2} \to K^{o_1+o_2}$. The public key is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^{o_1+o_2}$, and the private key consists of $\mathcal{T}$, $\mathcal{F}$ and $\mathcal{S}$.

To sign a message $\mathbf{m} = (m_1, \ldots, m_{o_1+o_2}) \in K^{o_1+o_2}$, we first compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{m}) = (y_1, \ldots, y_{o_1+o_2})$ and do the following.

(1) Choose $a = (a_1, \ldots, a_{v_1}) \in K^{v_1}$ and plug into the polynomials in the central map to obtain $\bar{f}^{(1)}, \ldots, \bar{f}^{(o_1+o_2)}$.
(2) Solving the linear system $\bar{f}^{(i)} = y_i$ with $i = 1, \ldots, o_1$ yields solution $(b_1, \ldots, b_{o_1})$. If there is no solution then come back to Step (1).

(3) Plug $(b_1, \ldots, b_{o_1})$ into $\bar{f}^{(o_1+1)}, \ldots, \bar{f}^{(o_1+o_2)}$ and solve the linear system $\bar{f}^{(i)} = y_i$ with $i = o_1 + 1, \ldots, o_1 + o_2$ to get a solution $(b_{o_1+1}, \ldots, b_{o_1+o_2})$. If there is no solution then come back to Step (1).
(4) Set $\mathbf{x} = (a_1, \ldots, a_{v_1}, b_1, \ldots, b_{o_1+o_2})$. A signature is computed by $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$.

A signature $\mathbf{s}$ is accepted if $\mathcal{P}(\mathbf{s}) = \mathbf{m}$, otherwise it is rejected.

The public key of the scheme consists of m quadratic equations in n variables, and hence the public key has size

$$m \cdot \frac{(n+1)(n+2)}{2} \quad \text{field elements}$$

and the size of the private key is

$$m \cdot (n+1) + n(n+1) + \sum_{i=1}^{2} o_i \left(\frac{v_i(v_i+1)}{2} + v_i \cdot o_i + v_{i+1} + 1 \right)$$

field elements.

5.2 CyclicRainbow

Petzoldt [20] proposed a way to reduce the public key size of Rainbow as follows. For $i = 1, 2$, set

$$D_i = \frac{v_i(v_i+1)}{2} + o_i v_i$$

to be the number of quadratic terms in the i-th layer of the Rainbow scheme. Assume that the matrix representing the public key is of the form:

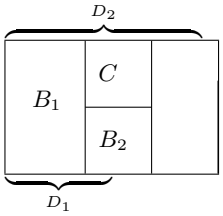

Fig. 2. Structure of the public key $\mathcal{P}$

Then Petzoldt choose the matrices B_1 and B_2 to be circular, i.e., choose the first row randomly and other rows are just rotations of the first one. Other entries are randomly chosen. Using the structure of Rainbow, the chosen public key can be used to generate the corresponding private key. One important point is that

making the public key has not found any risk to the security of the scheme. By that method, the CyclicRainbow scheme now has public key size

$$D_2 + \sum_{i=1}^{2} o_i \left(\frac{(n+1)(n+2)}{2} - D_i \right) =$$
$$D_2 + m \cdot \frac{(n+1)(n+2)}{2} - \sum_{i=1}^{2} o_i \cdot D_i$$

field elements.

5.3 Attacks

In this section, we review all currently known (classical) attacks against Rainbow.

Direct Attacks It is also well-known that Rainbow schemes behave similarly to random systems and therefore we can estimate the complexity of direct attack against Rainbow as in the case of UOV (cf. Section 5.3. The complexity can be estimated as

$$\min_{k \geq 0} q^k \cdot \mathcal{O}\left(m \cdot \binom{n-k+d_{\text{reg}}-1}{d_{\text{reg}}} \right)^{\omega},$$

where $2 < \omega \leq 3$ is the linear algebra constant of solving a linear system and d_{reg} is the degree of regularity of the system, which can be estimated as the smallest d for which the coefficient of x^d in the expression

$$\frac{(1-x^2)^m}{(1-x)^{m-k}}.$$

is non-positive.

The Rank Attacks There are Minrank [3] and Highrank [6] attacks. The Minrank [3] attack tries to find a linear combination of the public key polynomials of minimal rank. In case of Rainbow, such minimal rank is v_2 which corresponds to a linear combination of polynomials in the first layer of the central map. The complexity is estimated as

$$q^{v_1+1} \cdot m \cdot \left(\frac{n^3}{3} - \frac{m^2}{6} \right). \tag{2}$$

The Highrank [6] attack tries to identify variables that appear the lowest number of times in the polynomials of the central map. In case of Rainbow, those are the oil variables of the last layer. The complexity of the Highrank attack is estimated as

$$q^{o_2} \cdot \frac{n^3}{6}. \tag{3}$$

UOV Attack One can consider Rainbow as a UOV scheme with $v = v_1 + o_1$ and $o = o_2$ and hence it can be attacked by the UOV attack. Its goal is to find the pre-image of the Oil subspace $\{x \in K^n : x_1 = \cdots = x_v = 0\}$ under the affine transformation $\mathcal{S}$. The complexity of this attack is estimated as

$$q^{n-2o_2-1} \cdot o_2^4. \tag{4}$$

Rainbow-Band-Separation Attack The Rainbow-Band-Separation (RBS) attack [8] tries to find linear transformations $\mathcal{S}$ and $\mathcal{T}$ that transform the public polynomials into ones of the form of polynomials in the central map of Rainbow, and hence find an equivalent key to forge a signature. To do this, one has to solve $m + n - 1$ equations in n variables. In our paper, we use the field $K = \mathbb{F}_{2^8}$ and we follow [21] to choose $n \geq \frac{5}{3}(m-1)$ so that the complexity of the RBS attack against Rainbow is at least the complexity of the direct attack.

5.4 Lifting Rainbow to Extension Fields

In this section, we extend the idea of LUOV to Rainbow, i.e., we will work with Rainbow over the field $K = \mathbb{F}_{2^r}$. The idea is to generate the Rainbow a key pair over a subfield $L = \mathbb{F}_{2^t}$ (with $1 \leq t \leq r$), i.e., all coefficients of $\mathcal{F}, \mathcal{S}, \mathcal{T}$ and hence $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ are over L. Then we lift them up to $\mathbb{F}_{2^r}$ and consider the new scheme as a Rainbow scheme over $K = \mathbb{F}_{2^r}$. We follow .. to call this scheme *LRainbow*. As mentioned in, the choice of r is very important: if r is large than we can reduce the number of public equations; however for efficiency, r can not be too large. One must be care full in choosing parameters to balance the trade-off between whether r is large or small.

The public key of the LRainbow scheme now is

$$m \cdot \frac{(n+1)(n+2)}{2} \cdot t \quad \text{bits.}$$

A signature consists of n elements of $\mathbb{F}_{2^r}$, hence it has size nr bits.

5.5 Choice of subfield and parameters

We choose $K = \mathbb{F}_{2^8}$ to be the field with 256 elements. We follow [21] for choosing parameters. Let l be the desired security level, then the number of equations of the Rainbow scheme should be at least

$$m(l) = \lceil \frac{l - 12.1}{2.65} \rceil, \tag{5}$$

and the number of oil variables o_2 in the second layer is at least

$$o_2(l) = \lceil \frac{l - 3 \cdot \log(m) + \log(6)}{8} \rceil. \tag{6}$$

As mentioned in Section 5.3, the number of variables $n(l)$ should be at least

$$n(l) \geq \frac{5}{3}(m(l) - 1) \tag{7}$$

so that the complexity of the RBS attack against Rainbow scheme is at least the complexity of the direct attack.

Since we choose $K = \mathbb{F}_{2^8}$, and our target security levels are $l = 100, 128, 196$ and 256, it follows from (5) that the minimum number of public equations $m_{\min}$

Table 3. Parameters and key sizes of LRainbow scheme

Security level	(v_1, o_1, o_2)	Public key size (kB)	Signature size (B)
100	$(23, 16, 18)$	13.84	57
128	$(28, 21, 23)$	28.21	72
192	$(44, 32, 36)$	99.53	112
256	$(61, 46, 48)$	257.63	155

is at least $34, 44, 68$ and 94 respectively. We choose $o_2 \cong o_1$ (with o_2 is a bit slightly larger than o_1, and since we would like to also reduce the signature length, v_1 can not be too large. In order to be consistent with (7), we optimally choose $v_1 \leq 1.3 \cdot o_2$. Plugging each $m_{\min} = 34, 44, 68, 94$ into (2),(3), and (4) and requires that they are larger than $2^{100}, 2^{128}, 2^{192}$ and 2^{256} respectively, we optimally obtain $\log(q) = 5$.

So our LRainbow is constructed by first generating a CyclicRainbow (cf. Section 5.2) scheme over $L = \mathbb{F}_{2^5}$ and lifting it into $K = \mathbb{F}_{2^8}$ to obtain a Rainbow scheme over K. Table 3 shows our choice of parameters for target security level together with public key and signature size. By our choice of subfield L, the public key size of LRainbow is reduced 37.5% compared to that of corresponding CyclicRainbow over K.

Remark 1. One can choose $L = \mathbb{F}_2$ as in the case of LUOV. However, in order to avoid attacks, one need to choose large numbers of oil and vinegar variables, which will result in large key and signature sizes.

6 Conclusion

In this paper, we revisit the construction of LUOV scheme [2] and theoretically deduce the choice of subfield over which the UOV scheme first generated before being lifted to the full field. As a result, our method can reduce the signature size up to 40%. Moreover, we also extend this idea to Rainbow signature scheme obtain a field lifting Rainbow scheme, called LRainbow. As a result, our LRainbow scheme can reduce up to 37.5% the public key size. One can again reduce the public key size by using the method in [24] with the cost of increasing the signature size, which will be addressed in our future work.

References

1. L. Bettale, J.-C. Faugére, L. Perret: Hybrid approach for solving multivariate systems over finite fields. CHES 2013, LNCS vol. 8086, pp. 250–272, Springer, 2013
2. Ward Beullens and Bart Preneel. “Field Lifting for Smaller UOV Public Keys”. INDOCRYPT 2017, LNCS vol. 10698, pp 227–246, Springer 2017
3. O. Billet, H. Gilbert: Cryptanalysis of Rainbow. SCN 2006, LNCS vol. 4116, pp. 336 - 347. Springer, 2006.

4. A. Bogdanov, T. Eisenbarth, A. Rupp, C. Wolf. Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves? CHES 2008, LNCS vol. 5154, pp. 45–61. Springer, 2008.
5. A.I.T. Chen, M.-S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E. L.-H. Kuo, F. Y.-S. Lee, B.-Y. Yang. SSE implementation of multivariate PKCs on modern x86 cpus. CHES 2009, LNCS vol. 5747, pp. 33 - 48. Springer, 2009.
6. D. Coppersmith, J. Stern, S. Vaudenay: Attacks on the birational permutation signature schemes. CRYPTO '93, LNCS vol. 773, pp. 435 - 443. Springer, 1993.
7. J. Ding, D. S. Schmidt: Rainbow, a new multivariate polynomial signature scheme. ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer 2005.
8. J. Ding, B.Y. Yang, C.H.O Chen, M.S. Chen, C.M. Cheng: New Differential-Algebraic attacks and Reparametrization of Rainbow. ACNS 2008, LNCS vol. 5037, pp. 242–257. Springer, 2008.
9. J.C. Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, pp. 61-88 (1999).
10. M.R. Garey and D.S. Johnson: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company 1979
11. A. Kipnis, L. Patarin, L. Goubin: Unbalanced Oil and Vinegar Schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206–222. Springer 1999.
12. N. Koblitz: Elliptic curve cryptosystems. Math. Comp. 48, 177 (1987), pp. 203 - 209.
13. D. Kravitz: Digital Signature Algorithm. US patent 5231668 (July 1991).
14. T. Matsumoto, H. Imai: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. EUROCRYPT 1988. LNCS vol. 330, pp. 419-453. Springer 1988.
15. National Institute of Standards and Technology: Report on Post Quantum Cryptography. NISTIR draft 8105, https://csrc.nist.gov/publications/detail/nistir/8105/final
16. National Institute of Standards and Technology: Post-Quantum Cryptography - Round 1 Submission, https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
17. National Institute of Standards and Technology: First PQC Standardization Conference https://csrc.nist.gov/events/2018/first-pqc-standardization-conference
18. J. Patarin: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. CRYPTO 1995, LNCS vol. 963, pp. 248-261. Springer, 1995.
19. A. Petzoldt, S. Bulygin, J. Buchmann: Linear recurring sequences for the UOV key generation. PKC 2011, LNCS vol. 6571, pp. 335–350. Springer, 2011.
20. A. Petzoldt, S. Bulygin, J. Buchmann: CyclicRainbow - a multivariate signature scheme with a partially cyclic public key. INDOCRYPT 2010, LNCS vol. 6498, pp. 33–48. Springer, 2010
21. A. Petzoldt, S. Bulygin and J. A. Buchmann: Selecting Parameters for the Rainbow Signature Scheme. PQCrypto 2010, LNCS vol. 6061, pp. 218–240
22. R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 21 (2), pp. 120-126 (1978).
23. P. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26 (5), pp. 1484 - 1509 (1997).
24. A. Szepieniec, W. Beullens and Bart Preneel: MQ Signatures for PKI. PQCrypto 2017: Post-Quantum Cryptography, LNCS vol. 10346, pp. 224–240, Springer 2017.