Selecting Parameters for the Rainbow Signature Scheme - Extended Version -

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

Abstract. Multivariate public key cryptography is one of the main approaches to guarantee the security of communication in a post-quantum world. One of the most promising candidates in this area is the Rainbow signature scheme, which was first proposed by J. Ding and D. Schmidt in 2005. In this paper we develop a model of security for the Rainbow signature scheme. We use this model to find parameters for Rainbow over GF(16), GF(31) and GF(256) which, under certain assumptions, guarantee the security of the scheme for now and the near future.

Keywords: Multivariate cryptography, Rainbow signature scheme, parameters

1 Introduction

To guarantee the security of communication it is important to have fast and secure signature schemes. One major field of application for them is the authenticity of data and information, for example software updates.
One of the most promising candidates in this area is the Rainbow signature scheme, which was presented by J. Ding and D. Schmidt in [DS05]. Similarly to other multivariate schemes like $3iC^-p$ [DW07] and Projected Flash [PC01], [DY07] it is very efficient and provides fast signature generation and verification. In opposite to classical schemes, e.g. RSA or ECDSA, Rainbow is believed to be secure against attacks with quantum computers [BB08].

In the last years a lot of work has been done to study the security of multivariate schemes and many attacks were proposed. Among these are direct attacks on which a lot of work was done [YC07], [Fa99] as well as rank attacks which were introduced in [CS94] by Coppersmith and Stern to attack the Birational Permutation Scheme and later improved by a number of other researchers [YC05], [BG06]. A good overview of these attacks can be found in [GC00]. Special attacks on Rainbow-like schemes were proposed by Ding and Yang in [DY08]. There have also been some attempts to derive appropriate parameters from the complexities of these attacks [CC08]. However, it is still an open problem how we have to adapt the parameters of multivariate schemes to future developments in cryptanalysis and computing power.

In this paper we try to answer this question for the Rainbow signature scheme. We start with the security model of Lenstra and Verheul [LV00] to compute necessary security levels for the years 2010 to 2050. After that we look at the known attacks against the Rainbow signature scheme. Here, we concentrate mainly on two attacks, namely the direct attack and the Rainbow-Band-Separation attack. To study the complexity of these two attacks, we carried out a large number of own experiments, for which we used MAGMA [BC06], which contains an efficient implementation

of Faugeres F_4 [Fa99] algorithm for computing Gröbner bases. We use the results of these experiments to find appropriate parameters for Rainbow over the underlying fields $GF(16)$, $GF(31)$ and $GF(256)$. Finally, we compare Rainbow schemes over the different fields in terms of key sizes and signature lengths. One of our main results here is, that we get the smallest keys for Rainbow schemes over $GF(31)$, whereas we get the shortest signatures when using Rainbow over $GF(16)$.

The structure of the paper is as follows: In Section 2 we describe the Rainbow signature scheme. Section 3 describes our model of security for the Rainbow scheme. In Section 4 we take a closer look at the complexities of the direct and the Rainbow-Band-Separation attack and give concrete parameter sets for Rainbow over the fields $GF(16)$, $GF(31)$ and $GF(256)$. Section 5 summarizes our results and compares the Rainbow schemes over the different ground fields in terms of key sizes and signature length. Finally, Section 6 concludes the paper.

2 Multivariate Public Key Cryptography

Multivariate Public Key Cryptography is one of the main approaches for secure communication in a post-quantum world. The principle idea is to choose a multivariate system F of quadratic polynomials which can be easily inverted (central map). After that one chooses two affine linear invertible maps S and T to hide the structure of the central map. The public key of the cryptosystem is the composed map $P = S \circ F \circ T$ which is difficult to invert. The private key consists of S, F and T and therefore allows to invert P.
There are several ways to build the central map F. One approach are the so called BigField-Schemes like Matsumoto-Imai [MI88] and HFE [Pa96] with many variations and improvements [BB08], [Di04], [PC01]. On the other hand, we have the so called SingleField family with schemes like UOV [KP99] and Rainbow [DS05]. Recently, a third family called MediumField has been proposed which contains schemes like ℓ-iC [DW07].

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 (e.g. $K = GF(2^8)$). 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 this Section 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 $F = (f_{v+1}(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ can be easily inverted. First, we choose the values of the v Vinegar variables $x_1, \ldots, x_v$ at random. Such 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 new signature scheme called Rainbow, which is based on the idea of Oil and Vinegar.

Let K be a finite field (e.g. $K = GF(2^8)$) and S 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 $S_i = \{1, \ldots, v_i\}$ 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 S_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

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

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

The map $F(\mathbf{x}) = (f_{v_1+1}(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ 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 put 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 $(i = 1, \ldots, n)$ [3].

The Rainbow signature scheme is defined as follows:

Key Generation The private key consists of two invertible affine maps $L_1 : K^m \to K^m$ and $L_2 : K^n \to K^n$ and the map $F = (f_{v_1+1}(\mathbf{x}), \ldots, f_n(\mathbf{x}))$. Here, $m = n - v_1$ is the number of components of F.
The public key consists of the field K and the composed map $P(\mathbf{x}) = L_1 \circ F \circ L_2(\mathbf{x}) : K^n \to K^m$.

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 $\mathbf{x} = L_1^{-1}(\mathbf{h})$, $\mathbf{y} = F^{-1}(\mathbf{x})$ and $\mathbf{z} = L_2^{-1}(\mathbf{y})$. The signature of the document is $\mathbf{z} \in K^n$. Here, $F^{-1}(\mathbf{x})$ means finding one (of the possibly many) pre-image of $\mathbf{x}$.

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 (for $K = GF(2^8)$)

$$\text{size(public key)} = m \cdot \left(\frac{n \cdot (n+1)}{2} + n + 1 \right) = m \cdot \frac{(n+1) \cdot (n+2)}{2} \text{ bytes}, \tag{1}$$

the size of the private key

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

The length of the needed hash value is m bytes, the length of the signature is n bytes.
The scheme is denoted by Rainbow$(v_1, o_1, \ldots, o_u)$. For $u = 1$ we get the original UOV scheme.

[3] 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.

3 Our Model of Security

In this Section we describe the model underlying our parameter choices below. We base on the approach of Lenstra and Verheul [LV00].

3.1 The model

In [LV00] Lenstra and Verheul developed a security model, which they used to find appropriate parameters for symmetric cryptography and some asymmetric schemes. The main points of their model are:
1. Security margin: a definition of the term "adequate security".
2. Computing environment: the expected change in computational resources available to attackers.
3. Cryptanalytic development: the expected development in cryptanalysis.

In the following we take a closer look at these items.

Security margin To decide, whether a given scheme offers adequate security, one has to define the term "adequate security". [LV00] defines it by the security offered by DES in 1982. That is, in 1982 a computational effort of $5 \cdot 10^5$ MIPS years provided an adequate security. We follow this definition.

Computing environment Here [LV00] use a slightly modified version of Moore's law, which states that the amount of computing power and random access memory one gets for 1 dollar doubles every t months. Our default setting of t is 18, see [LV00]
Another thing we have to take into account, is the budget of an attacker, which might increase over time. The variable $b > 0$ is defined as the number of years it takes on average for an expected two-fold increase of a budget. Statistical data says, that the US Gross National product (in today's prices) doubles about every ten years. So our default setting for b is 10.

Cryptanalytic Development The number $r > 0$ is defined to be the number of months it is expected to take on average for cryptanalytic developments affecting Multivariate Public Key Cryptosystems to become twice as effective.
Under the assumption, that the pace of cryptanalytic findings in the area of multivariate cryptography will not vary dramatically from those in the field of classical cryptosystems, our default setting for r is $r = 18$.

After having developed concrete security levels based on these three items, Lenstra and Verheul analyzed known attacks against several schemes to get concrete parameter sets.
Analogous to [LV00], we will use "Infeasible number of MIPS years" (IMY) to define security requirements for the Rainbow signature scheme. Given that breaking DES takes $5 \cdot 10^5$ MIPS years, which was infeasible to do in year 1982, we get the number of MIPS years that are infeasible to break in the year y by the formula

$$IMY(y) = 5 \cdot 10^5 \cdot 2^{12(y-1982)/t} \cdot 2^{(y-1982)/b} \quad \text{MIPS years.} \tag{3}$$

With our default settings we get

$$IMY(y) = 2^{\frac{23}{30} \cdot y - 1500.6} \text{ MIPS years} \tag{4}$$

So far, we have not considered the possible advances in cryptanalysis. To cover these, we have to adapt the upper formula slightly. So, a cryptosystem, which shall be secure in the year y, must reach the security level

$$\text{Security level}(y) \geq IMY(y) \cdot 2^{12(y-2009)/r} \text{ MIPS years} \overset{r=18}{=} 2^{\frac{43}{30} \cdot y - 2839.9} \text{ MIPS years} \tag{5}$$

To translate this security bound into the corresponding number of field multiplications, we use a data-point computed by J. Ding et al. in [DY08]. There the authors solve a system of 37 quadratic equations in 22 variables over $GF(2^8)$ in about $1.06 \cdot 10^6$ seconds on a single 2.2 GHz Opteron machine by XL-Wiedemann. This corresponds to approximately 329.7 MIPS years [4]. Since the complexity of the system is about $2^{46.7}$ m, we get

$$1 \text{ MIPS year} = 3.49 \cdot 10^{11} \text{ m} \tag{6}$$

Such we get

$$\text{Security level}(y) \geq 2^{\frac{43}{30} \cdot y - 2801.5} \text{ m} \tag{7}$$

For our experiments (see next section) we use a single core Opteron 2.7 GHz CPU with 128 GB RAM. Since this CPU achieves about 10200 MIPS, we get

$$\text{Security level}(y) \geq 2^{\frac{43}{30} \cdot y - 2853.2} \text{ s} \tag{8}$$

3.2 Security level of Rainbow

In this subsection we look at the known attacks against the Rainbow signature scheme. We will find, that the security of the scheme is mainly given by the complexities of two attacks, namely the direct and the Rainbow-Band-Separation attack and therefore can be said to be the minimum of those two complexities.

The known attacks against the Rainbow Signature Scheme are:

1. direct attacks [BB08], [Ya07]: Direct attacks use equation solvers like XL and its derivatives as well as Gröbner Basis algorithms: Buchberger, F_4, and F_5. The complexity is approximately given as
$$C_{\text{direct}}(q, m, n) = C_{MQ(q,m,n)}, \tag{9}$$
where $C_{MQ(q,m,n)}$ denotes the complexity of solving a "generic" system of m quadratic equations in n variables over a field with q elements.
2. Rainbow-Band-Separation attack [DY08]
$$C_{\text{RBS}}(q, m, n) = C_{MQ(q,m+n-1,n)} \tag{10}$$
3. MinRank attack [GC00], [YC05]
$$C_{\text{MR}}(q, m, n, v_1) = [q^{v_1+1} \cdot m \cdot (n^2/2 - m^2/6)] \text{ m} \tag{11}$$
4. HighRank attack [GC00], [DY08]
$$C_{\text{HR}}(q, n, o_u) = [q^{o_u} \cdot n^3/6] \text{ m} \tag{12}$$
5. UOV attack [KP99]
$$C_{\text{UOV}}(q, n, o_u) = [q^{n-2 \cdot o_u - 1} \cdot o_u^4] \text{ m} \tag{13}$$
6. UOV-Reconciliation attack [BB08], [DY08]
$$C_{\text{UOVR}}(q, m, n, o_u) = C_{MQ(q,m,n-o_u)} \tag{14}$$
7. Attacks against the hashfunction

Here, m stands for the number of field multiplications needed during the attack.

[4] The given processor achieves about 9800 MIPS (SiSoft Sandra)

Defending a Rainbow scheme against the attacks from the items 3 to 7 is relatively easy:

Proposition 1: A Rainbow instance over $GF(q)$ with parameters $v_1, o_1, \ldots, o_u$ (see Section 2.2) , for which the items

1. $v_1 \geq \frac{\ell}{\lg_2(q)} - 1$
2. $o_u \geq \frac{\ell}{\lg_2(q)}$
3. $n - 2 \cdot o_u \geq \frac{\ell}{\lg_2(q)} + 1$

hold, has a security level of ℓ bits against the MinRank, the HighRank and the UOV attack.

Proof.

$$C_{\mathrm{MR}}(q, m, n, v_1) = [q^{v_1+1} \cdot m \cdot (n^2/2 - m^2/6)] \text{ m} \overset{1.}{\geq} [2^{a \cdot \ell/a} \cdot m \cdot (n^2/2 - m^2/6)] \text{ m} > 2^\ell \text{ m}$$

$$C_{\mathrm{HR}}(q, n, o_u) = [q^{o_u} n^3/6] \text{ m} \overset{2.}{\geq} [2^{a \cdot \ell/a} \cdot n^3/6] \text{ m} > 2^\ell \text{ m}$$

$$C_{\mathrm{UOV}}(q, n, o_u) = [q^{n-2o_u-1} \cdot o_u^4] \text{ m} \overset{3.}{\geq} [2^{a \cdot \ell/a} \cdot o_u^4] \text{ m} > 2^\ell \text{ m} \quad \square$$

Together, the complexities of the HighRank- and the UOV-attack give us a lower bound for the number of variables we need in a secure Rainbow Scheme. Namely, we get

$$n \geq \frac{3 \cdot \ell}{\lg_2(q)} + 1 \tag{15}$$

To defend the scheme against the UOV-Reconciliation attack, we need $v_1 \geq o_u$. Then, the algebraic part of the attack leads to an underdetermined system of quadratic equations which is as difficult to solve as a direct attack against the original scheme.

In order to prevent attacks on the hashfunction, one has to choose the number m of equations in the system large enough such that a birthday attack against a hashfunction with $\lg_2(q^m)$ bit is infeasible.

In opposite to this, how one has to choose the parameters of Rainbow in order to defend the scheme against the direct and the Rainbow-Band-Separation attack, it not quite as clear and depends closely on the cardinality of the underlying field.
In the next section, we will take a closer look at these two complexities for the underlying fields $GF(16)$, $GF(31)$ and $GF(256)$ and try to find appropriate parameter sets for Rainbow over these fields.

4 Parameter choice

In this section we want to find appropriate parameter sets for the Rainbow Signature Scheme over the underlying fields $GF(16)$, $GF(31)$ and $GF(256)$.

The number of equations we need in our Rainbow Scheme is mainly determined by

- The complexity of a direct attack and
- Attacks against the hashfunction

Then number of variables in the scheme is mainly determined by

- The complexity of the RBS-attack
- The complexity of the UOV-attack and HighRank attack

In the following three subsections we look at Rainbow Schemes over $GF(16)$, $GF(31)$ and $GF(256)$.

4.1 Rainbow Schemes over GF(16)

Rank- and UOV attacks Table 1 gives the parameter restrictions set by Rank and UOV attacks. To prevent attacks with the UOV-Reconciliation attack, one should also have $v_1 \geq o_u$.

years	MinRank $v_1 \geq$	HighRank $o_u \geq$	UOV-Attack $n - 2o_u \geq$	HR+UOV $n \geq$
2010	19	20	21	61
2011-2013	20	21	22	64
2014-2015	21	22	23	67
2016-2018	22	23	24	70
2019-2021	23	24	25	73
2022-2024	24	25	26	76
2025-2027	25	26	27	79
2028-2029	26	27	28	82
2030-2032	27	28	29	85
2033-2035	28	29	30	88
2036-2038	29	30	31	91
2039-2041	30	31	32	94
2042-2043	31	32	33	97
2044-2046	32	33	34	100
2047-2049	33	34	35	103
2050-2052	34	35	36	106

Table 1. Parameter restrictions for Rainbow over GF(16) according to Proposition 1

Direct attacks We carried out a large number of experiments of solving Rainbow systems over $GF(16)$ with MAGMA's F_4 algorithm. Before we could apply the MAGMA function `GroebnerBasis`, we had to convert the underdetermined Rainbow systems into determined ones by guessing at some of the variables. Since an underdetermined system with m equations in $n > m$ variables has approximately $16^{(n-m)}$ solutions, it can be expected that our determined systems have a solution. By guessing at additional variables we created overdetermined systems to see whether this reduces the time needed to compute a Gröbner Basis. When doing so, one has to run the algorithm several times to find a solution of the original system.
Figure 1 shows the results of these experiments. As the figure shows, for more than 35 equations we get the best results by guessing at ten additional variables. The time MAGMA needs to solve 16^{10} of these overdetermined systems can be estimated as

$$RT_{F_4}(16, m) = 2^{1.67 \cdot m + 3.4} \ s \ (m \geq 35) \tag{16}$$

The number of equations we need to reach our security level, is therefore given as

$$m \geq \frac{\log_2(\text{Security level}(y)) - 3.4}{1.67} \tag{17}$$

Note that the numbers m we get by this formula would lead to hash lengths which are not secure. So the number of equations in our schemes is determined by the hash length.

RBS-attack Due to the complexity of the UOV-attack we get an impression how many variables we need in our Rainbow scheme (see Table 1). To see whether this number is big enough to defend the scheme against the Rainbow-Band-Separation (RBS) attack, we carried out some experiments to estimate the running time of this attack. In the first step of the RBS attack one has to solve

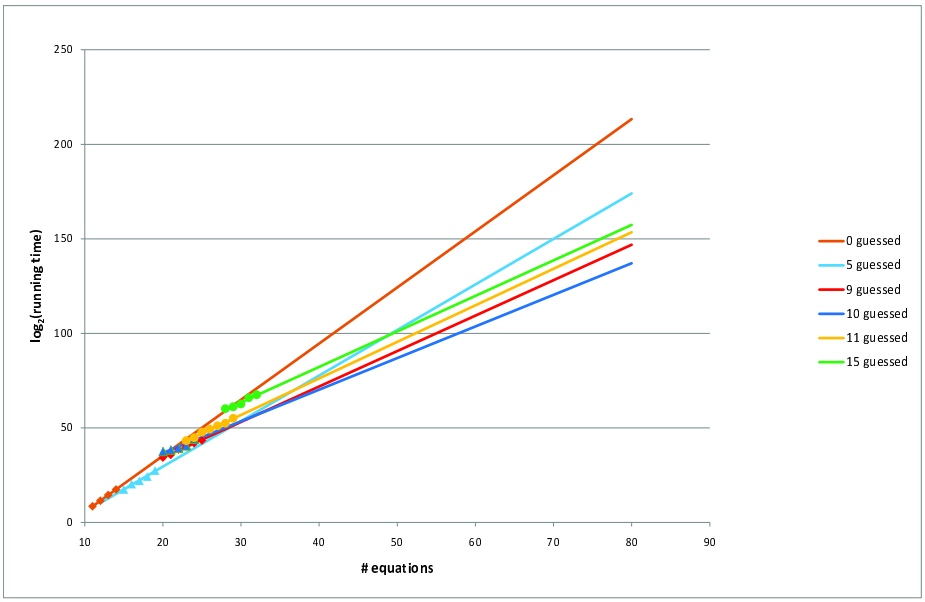

Fig. 1. Running time of the direct attack against Rainbow schemes over GF(16) with guessing

an overdetermined system of $m' = m + n - 1$ equations in n variables. The running time of the RBS attack is mainly given by the time needed to solve this system.
For different values of m and n we carried out experiments to find the time MAGMA needs to solve this initial system. Table 2 shows the results.

As figure 2 shows, for a Rainbow scheme over GF(16) with m equations and $n = \frac{3}{2} \cdot (m-1)$ variables the running time of the RBS attack is as least as high as the running time of the direct attack (dotted line in the figure). Therefore, the values of n shown in table 1 are high enough. Table 3 shows the proposed parameters for Rainbow Schemes over GF(16).

4.2 Rainbow Schemes over GF(31)

In [CC09] Chen et al. suggested to define multivariate schemes over the field GF(31). Using this field seems to be especially appropriate on PC's with modern CPU's supporting the SSE vector instruction set extensions. In this Section we want to find the optimal parameters for the Rainbow Signature Scheme over GF(31).

Table 4 gives the parameter restrictions set by Rank and UOV attacks. To prevent attacks with the UOV-Reconciliation attack, one should also have $v_1 \geq o_u$.

Direct attacks We carried out some experiments of solving Rainbow systems over $GF(31)$ with MAGMA's F_4 algorithm. Again, we had to convert the underdetermined Rainbow systems into determined ones by guessing at some of the variables, before we could apply the MAGMA function `GroebnerBasis`. Since an underdetermined system with m equations in n variables has approximately $31^{(n-m)}$ solutions, it can be expected that our determined systems have a solution. By

$n = 2 \cdot (m-1)$	m	8	9	10	11
	n	14	16	18	20
		35.2 s 28 MB	798 s 209 MB	9527 s 753 MB	161738 s 2763 MB
$n = \frac{5}{3} \cdot (m-1)$	m	7	10	13	
	n	10	15	20	
		0.15 s 6.6 MB	53.2 s 35 MB	30127 s 2032 MB	
$n = \frac{3}{2} \cdot (m-1)$	m	9	11	13	15
	n	12	15	18	21
		0.8 s 8.5 MB	49.8 s 32.2 MB	1172 s 170.0 MB	72298 s 2916 MB

Table 2. Running time of the RBS attack against Rainbow Schemes over GF(16)

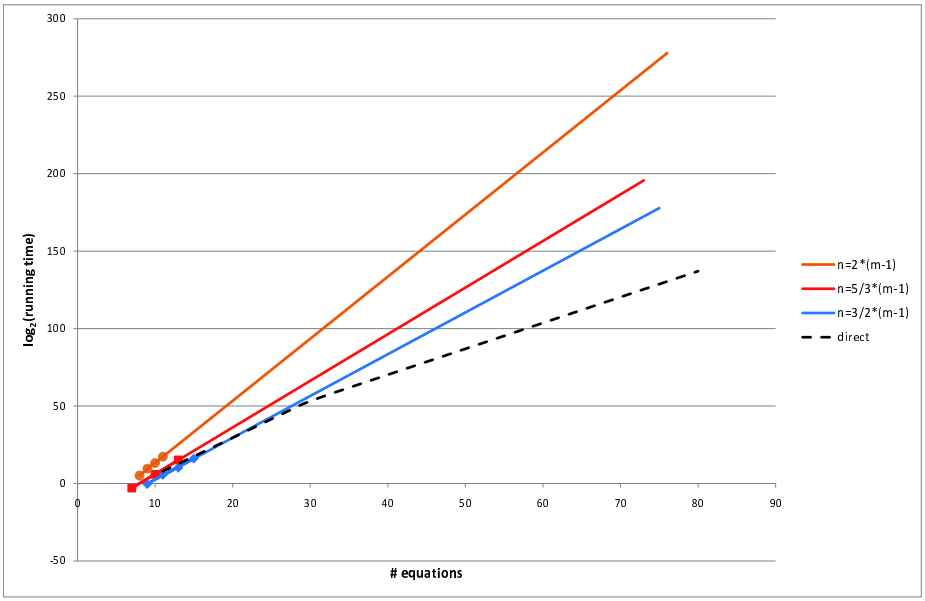

Fig. 2. Running time of the RBS attack against Rainbow over GF(16) for different ratios of m and n

years	hash size (bit)	(m,n)	public key size (kB)	example scheme (v_1, o_1, o_2)	private key size (kB)	signature size (bit)	IMY
1982							$5.00 \cdot 10^5$
2010	160	(40,61)	38.1	(21,20,20)	26.4	244	$1.45 \cdot 10^{12}$
2011	168	(42,64)	44.0	(22,21,21)	30.3	256	$2.47 \cdot 10^{12}$
2012	168	(42,64)	44.0	(22,21,21)	30.3	256	$4.19 \cdot 10^{12}$
2013	168	(42,64)	44.0	(22,21,21)	30.3	256	$7.14 \cdot 10^{12}$
2014	176	(44,67)	50.4	(23,22,22)	34.6	268	$1.21 \cdot 10^{13}$
2015	176	(44,67)	50.4	(23,22,22)	34.6	268	$2.07 \cdot 10^{13}$
2016	184	(46,70)	57.4	(24,23,23)	39.2	280	$3.52 \cdot 10^{13}$
2017	184	(46,70)	57.4	(24,23,23)	39.2	280	$5.98 \cdot 10^{13}$
2018	184	(46,70)	57.4	(24,23,23)	39.2	280	$1.02 \cdot 10^{14}$
2019	192	(48,73)	65.0	(25,24,24)	44.2	292	$1.73 \cdot 10^{14}$
2020	192	(48,73)	65.0	(25,24,24)	44.2	292	$2.94 \cdot 10^{14}$
2021	192	(48,73)	65.0	(25,24,24)	44.2	292	$5.01 \cdot 10^{14}$
2022	200	(50,76)	73.3	(26,25,25)	49.6	304	$8.52 \cdot 10^{14}$
2023	200	(50,76)	73.3	(26,25,25)	49.6	304	$1.45 \cdot 10^{15}$
2024	200	(50,76)	73.3	(26,25,25)	49.6	304	$2.47 \cdot 10^{15}$
2025	208	(52,79)	82.3	(27,26,26)	55.5	316	$4.20 \cdot 10^{15}$
2026	208	(52,79)	82.3	(27,26,26)	55.5	316	$7.14 \cdot 10^{15}$
2027	208	(52,79)	82.3	(27,26,26)	55.5	316	$1.21 \cdot 10^{16}$
2028	216	(54,82)	91.9	(28,27,27)	61.8	328	$2.07 \cdot 10^{16}$
2029	216	(54,82)	91.9	(28,27,27)	61.8	328	$3.52 \cdot 10^{16}$
2030	224	(56,85)	102.3	(29,28,28)	68.6	340	$5.98 \cdot 10^{16}$
2031	224	(56,85)	102.3	(29,28,28)	68.6	340	$1.02 \cdot 10^{17}$
2032	224	(56,85)	102.3	(29,28,28)	68.6	340	$1.73 \cdot 10^{17}$
2033	232	(58,88)	113.4	(30,29,29)	75.8	352	$2.95 \cdot 10^{17}$
2034	232	(58,88)	113.4	(30,29,29)	75.8	352	$5.01 \cdot 10^{17}$
2935	232	(58,88)	113.4	(30,29,29)	75.8	352	$8.53 \cdot 10^{17}$
2036	240	(60,91)	125.3	(31,30,30)	83.5	364	$1.45 \cdot 10^{18}$
2037	240	(60,91)	125.3	(31,30,30)	83.5	364	$2.47 \cdot 10^{18}$
2038	240	(60,91)	125.3	(31,30,30)	83.5	364	$4.20 \cdot 10^{18}$
2039	248	(62,94)	138.0	(32,31,31)	91.8	376	$7.14 \cdot 10^{18}$
2040	248	(62,94)	138.0	(32,31,31)	91.8	376	$1.22 \cdot 10^{19}$
2041	248	(62,94)	138.0	(32,31,31)	91.8	376	$2.07 \cdot 10^{19}$
2042	256	(64,97)	151.6	(33,32,32)	100.5	388	$3.52 \cdot 10^{19}$
3043	256	(64,97)	151.6	(33,32,32)	100.5	388	$5.99 \cdot 10^{19}$
2044	264	(66,100)	166.0	(34,33,33)	109.9	400	$1.02 \cdot 10^{20}$
2045	264	(66,100)	166.0	(34,33,33)	109.9	400	$1.73 \cdot 10^{20}$
2046	264	(66,100)	166.0	(34,33,33)	109.9	400	$2.95 \cdot 10^{20}$
2047	272	(68,103)	181.3	(35,34,34)	119.7	412	$5.02 \cdot 10^{20}$
2048	272	(68,103)	181.3	(35,34,34)	119.7	412	$8.53 \cdot 10^{20}$
2049	272	(68,103)	181.3	(35,34,34)	119.7	412	$1.45 \cdot 10^{21}$
2050	280	(70,106)	197.5	(36,35,35)	130.1	424	$2.47 \cdot 10^{21}$

Table 3. Proposed Parameters for Rainbow over GF(16)

years	MinRank $v_1 \geq$	HighRank $o_u \geq$	UOV-Attack $n - 2o_u \geq$	HR+UOV $n \geq$
2010-2013	16	17	18	52
2014-2016	17	18	19	55
2017-2020	18	19	20	58
2021-2023	19	20	21	61
2024-2027	20	21	22	64
2028-2030	21	22	23	67
2031-2034	22	23	24	70
2035-2037	23	24	25	73
2038-2041	24	25	26	76
2042-2044	25	26	27	79
2045-2047	26	27	28	82
2048-2051	27	28	29	85

Table 4. Parameter restrictions for Rainbow over GF(31) according to Proposition 1

further guessing at 1, 2, 3 or 4 additional variables we created overdetermined systems to see whether this reduces the time needed to compute a Gröbner Basis. When doing so, one has to run the algorithm several times to find a solution of the original system.

As table 5 shows, for more than 12 equations we get the best results when guessing at two

# equations	11	12	13	14	15	16	17	18
no guessing	7.8 m 517 MB	58.3 m 1283 MB	7.7 h 7601 MB	52.3 h 53728 MB	 ooM			
1 guessed	3.1 m 13.3 MB	18.9 m 29.5 MB	2.6 h 82.4 MB	15.8 h 285 MB	124.9 h 979 MB	846.5 h 3872 MB		
2 guessed	3.7 m 8.7 MB	25.7 m 12.3 MB	2.4 h 17.3 MB	14.4 h 43.7 MB	77.9 h 108 MB	428.8 h 312 MB	178.8 d 1278 MB	
3 guessed			6.2 h 9.3 MB	38.2 h 15 MB	176.8 h 26 MB	726.5 h 53 MB	283.1 d 219 MB	1644.5 d 587 MB
4 guessed				70.8 h 8.9 MB	344.4 h 10.8 MB	1906.7 h 18 MB	556.4 d 43 MB	2994.5 d 97 MB

Table 5. Solving Rainbow systems over GF(31) by F_4 with guessing

variables. Furthermore, our extrapolation (see figure 3) shows that for $m \geq 25$ equations it is even better to guess at three variables. So, for the parameters currently used in multivariate schemes it is the optimal strategy to guess at three variables. Such we get

$$RT_{F4}(31, m) = 2^{2.50 \cdot m - 18.2} sec \ (25 \leq m \leq 52) \tag{18}$$

To have a secure Rainbow Scheme, this running time has to be greater or equal to our Security level, or

$$m \geq \frac{log_2(\text{Security level}(y)) + 18.2}{2.50} \tag{19}$$

Note that in some cases the number m given by formula (19) would lead to hash lengths which are not secure. In these cases the number of equations in our schemes is determined by the hash length.

RBS-attack To determine the number n of variables needed in our Rainbow Schemes we carried out some experiments to estimate the running time of the Rainbow-Band-Separation (RBS) attack.

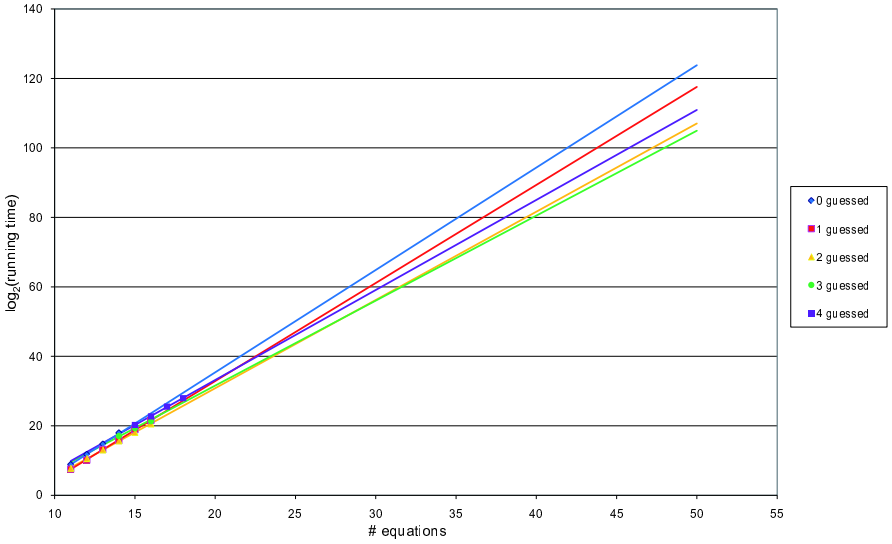

Fig. 3. Running time of the direct attack against Rainbow schemes over GF(31)

In the first step of this attack one has to solve an overdetermined system of $m' = m+n-1$ equations in n variables. The running time of the RBS attack is mainly given by the time needed to solve this system.
For different values of m and n we carried out experiments to find the time MAGMA needs to solve this initial system. Table 6 shows the results. As figure 4 shows, the running time of the RBS attack against a Rainbow Scheme with m equations and $n = \frac{3}{2} \cdot (m-1)$ variables is almost the same as the running time of the direct attack against such a system (dotted line in the figure). Therefore, to create secure Rainbow Schemes over GF(31), we need

$$n \geq \frac{3}{2} \cdot (m-1) \tag{20}$$

Note that due to the UOV-attack we need often more variables than stated by this formula. So, in most cases the RBS-attack does not give a restriction to our parameter choice.

Data Conversion between $GF(31)$ and $GF(2)^\star$ Since both hashvalues and signatures are usually given as bit strings, one needs to convert elements of $GF(2)^\star$ into elements of $GF(31)$ and vice versa. To store the keys, it is necessary to convert elements of $GF(31)$ into bitstrings, too. Like in [CC09] we use the following data conversion between $GF(31)$ and $GF(2)^\star$:

- 3 elements of GF(31) fit into a 2-byte block
- an 8-byte block fits into 13 elements of GF(31)

$n = 2 \cdot (m-1)$	m	8	9	10	11
	n	14	16	18	20
		34.1 s 30 MB	777 s 214 MB	9321 s 765 MB	153864 s 2890 MB
$n = \frac{5}{3} \cdot (m-1)$	m	7	10	13	
	n	10	15	20	
		0.14 s 0.7 MB	50.4 s 37 MB	28921 s 2081 MB	
$n = \frac{3}{2} \cdot (m-1)$	m	9	11	13	15
	n	12	15	18	21
		0.8 s 9.2 MB	40.5 s 36 MB	954 s 231 MB	56881 s 3291 MB

Table 6. Running time of the RBS attack against Rainbow schemes over GF(31)

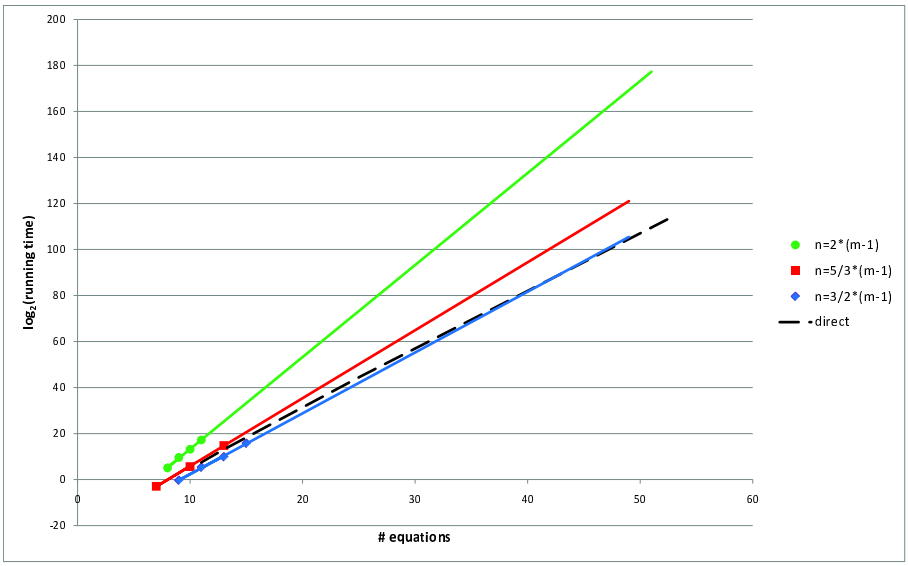

Fig. 4. Running time of the RBS attack against Rainbow schemes over GF(31) for different ratios of m and n

years	hash size (bit)	(m,n)	public key size GF(31)-elements	kB	example scheme (v_1, o_1, o_2)	private key size GF(31)-elements	kB	signature size (bit)	IMY
1982									$5.00 \cdot 10^5$
2010	160	(33,52)	47223	30.7	(19,16,17)	34084	22.2	280	$1.45 \cdot 10^{12}$
2011	168	(35,52)	50085	32.6	(17,18,17)	34652	22.2	280	$2.47 \cdot 10^{12}$
2012	168	(35,52)	50085	32.6	(17,18,17)	34652	22.6	280	$4.19 \cdot 10^{12}$
2013	168	(35,55)	55860	36.4	(20,18,17)	39833	26.0	296	$7.14 \cdot 10^{12}$
2014	176	(36,55)	57456	37.4	(19,18,18)	40322	26.3	296	$1.21 \cdot 10^{13}$
2015	176	(36,55)	57456	37.4	(19,18,18)	40322	26.3	296	$2.07 \cdot 10^{13}$
2016	184	(38,58)	67260	43.8	(20,19,19)	46498	30.5	312	$3.51 \cdot 10^{13}$
2017	184	(38,58)	67260	43.8	(20,19,19)	46498	30.5	312	$5.98 \cdot 10^{13}$
2018	184	(38,58)	67260	43.8	(20,19,19)	46498	30.5	312	$1.02 \cdot 10^{14}$
2019	192	(39,58)	69030	44.9	(19,20,19)	47202	30.7	312	$1.73 \cdot 10^{14}$
2020	192	(39,58)	69030	44.9	(19,20,19)	47202	30.7	312	$2.94 \cdot 10^{14}$
2021	192	(39,61)	76167	44.5	(22,19,20)	53749	35.0	328	$5.01 \cdot 10^{14}$
2022	200	(41,61)	80073	45.8	(20,21,20)	54476	35.5	328	$8.52 \cdot 10^{14}$
2023	200	(41,61)	80073	45.8	(20,21,20)	54476	35.5	328	$1.45 \cdot 10^{15}$
2024	200	(41,64)	87945	51.7	(23,20,21)	61676	40.2	344	$2.47 \cdot 10^{15}$
2025	208	(43,64)	92235	51.7	(21,22,21)	62460	40.7	344	$4.20 \cdot 10^{15}$
2026	208	(43,64)	92235	53.1	(21,22,21)	62460	40.7	344	$7.14 \cdot 10^{15}$
2027	208	(43,64)	92235	54.5	(21,22,21)	62460	40.7	344	$1.21 \cdot 10^{16}$
2028	216	(44,67)	103224	59.6	(23,22,22)	70798	46.1	360	$2.07 \cdot 10^{16}$
2029	216	(44,67)	103224	61.1	(23,22,22)	70798	46.1	360	$3.52 \cdot 10^{16}$
2030	224	(46,67)	103224	61.1	(21,24,22)	71508	46.6	360	$5.98 \cdot 10^{16}$
2031	224	(46,70)	117576	68.2	(24,23,23)	80272	52.3	376	$1.02 \cdot 10^{17}$
2032	224	(46,70)	117576	68.2	(24,23,23)	80272	52.3	376	$1.73 \cdot 10^{17}$
2033	232	(48,70)	122688	69.9	(22,25,23)	81037	52.8	376	$2.95 \cdot 10^{17}$
2034	232	(48,70)	122688	71.6	(22,25,23)	81037	52.8	376	$5.01 \cdot 10^{17}$
2935	232	(48,73)	133200	77.7	(25,24,24)	90554	59.0	392	$8.53 \cdot 10^{17}$
2036	240	(49,73)	135975	79.5	(24,25,24)	91002	59.2	392	$1.45 \cdot 10^{18}$
2037	240	(49,73)	135975	79.5	(24,25,24)	91002	59.2	392	$2.47 \cdot 10^{18}$
2038	240	(49,76)	147147	95.8	(27,24,25)	101124	65.8	408	$4.20 \cdot 10^{18}$
2039	248	(51,76)	153153	88.0	(25,26,25)	102156	66.5	408	$7.14 \cdot 10^{18}$
2040	248	(51,76)	153153	89.9	(25,26,25)	102156	66.5	408	$1.22 \cdot 10^{19}$
2041	248	(51,76)	153153	91.9	(25,26,25)	102156	66.5	408	$2.07 \cdot 10^{19}$
2042	256	(52,79)	168480	99.1	(27,26,26)	113674	74.0	424	$3.52 \cdot 10^{19}$
3043	256	(52,79)	168480	101.3	(27,26,26)	113674	74.0	424	$5.99 \cdot 10^{19}$
2044	264	(54,79)	174960	101.3	(25,28,26)	114616	74.6	424	$1.02 \cdot 10^{20}$
2045	264	(54,82)	188244	111.2	(28,27,27)	126578	82.4	440	$1.73 \cdot 10^{20}$
2046	264	(54,82)	188244	113.9	(28,27,27)	126578	82.4	440	$2.95 \cdot 10^{20}$
2047	272	(56,82)	195216	127.1	(26,29,27)	127583	83.1	440	$5.02 \cdot 10^{20}$
2048	272	(56,85)	209496	136.4	(29,28,28)	140422	91.4	456	$8.53 \cdot 10^{20}$
2049	272	(56,85)	209496	136.4	(29,28,28)	140422	91.4	456	$1.45 \cdot 10^{21}$
2050	280	(57,85)	213237	138.8	(28,29,28)	141000	91.8	456	$2.47 \cdot 10^{21}$

Table 7. Proposed Parameters for Rainbow over GF(31)

4.3 Rainbow Schemes over GF(256)

In this Section we want to find the optimal parameters for the Rainbow Signature Scheme over GF(256).

Table 8 gives the parameter restrictions set by Rank and UOV attacks. To prevent attacks with the UOV-Reconciliation attack, one should also have $v_1 \geq o_u$.

years	MinRank $v_1 \geq$	HighRank $o_u \geq$	UOV-Attack $n - 2o_u \geq$	HR+UOV $n \geq$
2010	9	10	11	31
2011-2015	10	11	12	34
2016-2021	11	12	13	37
2022-2027	12	13	14	40
2028-2032	13	14	15	43
2033-2038	14	15	16	46
2039-2043	15	16	17	49
2044-2049	16	17	18	52
2050-2055	17	18	19	55

Table 8. Parameter restrictions for Rainbow over GF(256) according to Proposition 1

Direct attacks We carried out some experiments of solving Rainbow systems over $GF(256)$ with MAGMA's F_4 algorithm. Before we could apply the MAGMA function `GroebnerBasis`, we had to convert the underdetermined Rainbow systems into determined ones by guessing at some of the variables. By further guessing at 1, 2, 3 or 4 additional variables we created overdetermined systems to see whether this reduces the time needed to compute a Gröbner Basis. When doing so, one has to run the algorithm several times to find a solution of the original system. Table 9 shows the results of these experiments.

# equations	11	12	13	14	15	16
no guessing	6.4 m 342 MB	0.8 h 1236 MB	6.6 h 7426 MB	47.2 h 35182 MB	- ooM	-
guessing 1 variable	29 m 11 MB	2.8 h 23 MB	23 h 76 MB	134 h 285 MB	48 d 997 MB	257 d 3953 MB
guessing 2 variables	264 m 8.6 MB	30 h 10.7 MB	170 h 14.5 MB	1214 h 42 MB	230 d 118 MB	1259 d 335 MB
guessing 3 variables	5880 m 8.3 MB	715 h 9.0 MB	3830 h 11.2 MB	23597 h 14.8 MB	4449 d 24.8 MB	18443 d 51.7 MB
guessing 4 variables	93807 m 7.9 MB	8126 h 8.6 MB	43465 h 10.6 MB	22652 h 11.8 MB	67129 d 12.9 MB	382986 d 18.0 MB

Table 9. Solving Rainbow systems over GF(256) with F4 with guessing

So, in our examples, we get the best results without guessing. But, as our extrapolation shows, for $m \geq 22$ equations it will be better to guess at one variable, and for $m \geq 29$ to guess at two variables before applying F4 (see figure 5). The time MAGMA needs for solving a determined

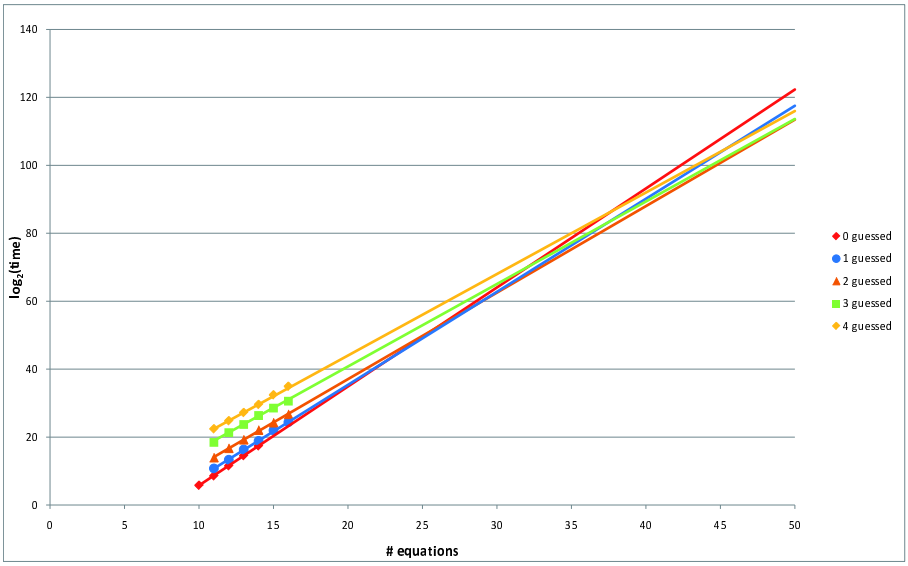

Fig. 5. Running time of the direct attack against Rainbow schemes over GF(256) with guessing

system with m equations can then be estimated by the formula

$$\begin{aligned} \mathrm{RT}_{\mathrm{F4}}(2^8, \mathrm{m}) &= 2^{2.74 \cdot m - 19.4} \text{ sec} \quad (22 \leq m \leq 28) \\ \mathrm{RT}_{\mathrm{F4}}(2^8, m) &= 2^{2.55 \cdot m - 13.9} \text{ sec} \quad (29 \leq m \leq 50) \end{aligned} \tag{21}$$

To have a secure Rainbow Scheme, this running time has to be greater or equal to our Security level, or

$$m \geq \frac{log_2(\text{Security level}(y)) + 13.9}{2.55} \tag{22}$$

RBS-attack To determine the number n of variables needed in our Rainbow Schemes we carried out some experiments to estimate the running time of the Rainbow-Band-Separation (RBS) attack. In the first step of this attack one has to solve an overdetermined system of $m' = m+n-1$ equations in n variables. The running time of the RBS attack is mainly given by the time needed to solve this system.
For different values of m and n we carried out experiments to find the time MAGMA needs to solve this initial system. Table 10 shows the results.

As Figure 6 shows, the running time of the RBS attack against a Rainbow Scheme over GF(256) with m equations and $n = \frac{5}{3} \cdot (m-1)$ variables is almost the same as the running time of the direct attack against such a system (dotted line in the figure). Therefore, to create secure Rainbow Schemes over GF(256), we need

$$n \geq \frac{5}{3} \cdot (m-1) \tag{23}$$

Table 11 shows the proposed parameters for Rainbow over $GF(256)$.

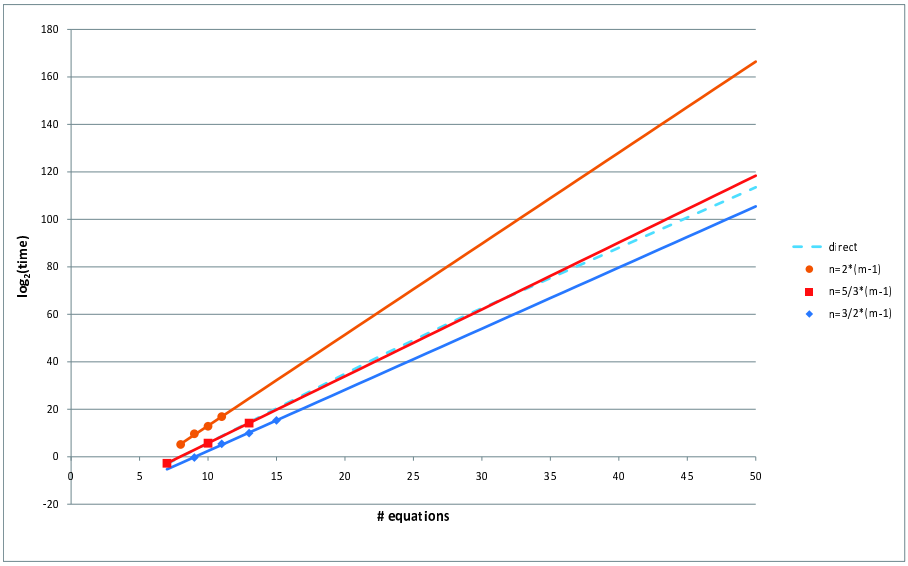

Fig. 6. Running time of the RBS attack against Rainbow schemes over GF(31) for different ratios of m and n

$m = \frac{3}{2} \cdot n$	# equations	21	24	27	30
	# variables	14	16	18	20
		36 s 30 MB	804 s 214 MB	7293 s 765 MB	120831 s 2890 MB
$m = \frac{8}{5} \cdot n$	# equations	16	24	32	
	# variables	10	15	20	
		0.15 s 0.7 MB	52.5 s 37 MB	18263 s 2081 MB	
$m = \frac{5}{3} \cdot n$	# equations	20	25	30	35
	# variables	12	15	18	21
		0.8 s 1.2 MB	42,7 s 36 MB	985 s 231 MB	40298 s 3291 MB

Table 10. Running time of the RBS attack against Rainbow over GF(256)

Year	$(m,\ n)$	public key size (kB)	example scheme (v_1, o_1, o_2)	private key size (kB)	hash size (bit)	signature size(bit)	IMY
1982							$5.00 \cdot 10^5$
2010	(26,43)	25.7	(17,13,13)	19.1	208	344	$1.45 \cdot 10^{12}$
2011	(27,45)	29.2	(18,13,14)	21.7	216	360	$2.47 \cdot 10^{12}$
2012	(27,45)	29.2	(18,13,14)	21.7	216	360	$4.19 \cdot 10^{12}$
2013	(28,46)	31.6	(18,14,14)	23.1	224	368	$7.14 \cdot 10^{12}$
2014	(29,47)	34.1	(18,14,15)	24.8	232	376	$1.21 \cdot 10^{13}$
2015	(29,47)	34.1	(18,14,15)	24.8	232	376	$2.07 \cdot 10^{13}$
2016	(30,49)	38.3	(19,15,15)	27.7	240	392	$3.51 \cdot 10^{13}$
2017	(30,51)	41.3	(21,15,15)	30.5	240	408	$5.98 \cdot 10^{13}$
2018	(31,52)	44.4	(21,15,16)	32.4	248	416	$1.02 \cdot 10^{14}$
2019	(31,52)	44.4	(21,15,16)	32.4	248	416	$1.73 \cdot 10^{14}$
2020	(32,53)	47.3	(21,16,16)	34.4	256	424	$2.94 \cdot 10^{14}$
2021	(33,54)	50.8	(21,16,17)	36.5	264	432	$5.01 \cdot 10^{14}$
2022	(33,55)	52.7	(22,16,17)	38.1	264	440	$8.52 \cdot 10^{14}$
2023	(34,57)	58.2	(23,17,17)	42.0	272	456	$1.45 \cdot 10^{15}$
2024	(34,58)	60.2	(24,17,17)	43.8	272	464	$2.47 \cdot 10^{15}$
2025	(35,59)	64.1	(24,17,18)	46.3	280	472	$4.20 \cdot 10^{15}$
2026	(35,59)	64.1	(24,17,18)	46.3	280	472	$7.14 \cdot 10^{15}$
2027	(36,60)	68.1	(24,18,18)	48.7	288	480	$1.21 \cdot 10^{16}$
2028	(37,61)	72.3	(24,18,19)	51.4	296	488	$2.07 \cdot 10^{16}$
2029	(37,63)	77.0	(26,18,19)	55.6	296	504	$3.52 \cdot 10^{16}$
2030	(38,65)	84.0	(27,19,19)	60.5	304	520	$5.98 \cdot 10^{16}$
2031	(38,65)	84.0	(27,19,19)	60.5	304	520	$1.02 \cdot 10^{17}$
2032	(39,66)	88.8	(27,19,20)	63.6	312	528	$1.73 \cdot 10^{17}$
2033	(39,66)	88.8	(27,19,20)	63.6	312	528	$2.95 \cdot 10^{17}$
2034	(40,68)	96.7	(28,20,20)	69.1	320	544	$5.01 \cdot 10^{17}$
2035	(40,69)	99.4	(29,20,20)	71.6	320	552	$8.53 \cdot 10^{17}$
2036	(41,72)	110.7	(31,20,21)	80.3	328	576	$1.45 \cdot 10^{18}$
2037	(42,73)	116.6	(31,21,21)	83.8	336	584	$2.47 \cdot 10^{18}$
2038	(42,73)	116.6	(31,21,21)	83.8	336	584	$4.20 \cdot 10^{18}$
2039	(43,74)	122.6	(31,21,22)	87.7	344	592	$7.14 \cdot 10^{18}$
2040	(43,74)	122.6	(31,21,22)	87.7	344	592	$1.22 \cdot 10^{19}$
2041	(44,76)	132.1	(32,22,22)	94.4	352	608	$2.07 \cdot 10^{19}$
2042	(44,78)	139.0	(32,22,22)	94.4	352	624	$3.52 \cdot 10^{19}$
2043	(45,79)	145.8	(34,22,23)	104.8	360	632	$5.99 \cdot 10^{19}$
2044	(46,80)	152.8	(34,23,23)	109.1	368	640	$1.02 \cdot 10^{20}$
2045	(46,80)	152.8	(34,23,23)	109.1	368	640	$1.73 \cdot 10^{20}$
2046	(47,81)	159.9	(34,23,24)	113.6	376	648	$2.95 \cdot 10^{20}$
2047	(47,82)	163.8	(35,23,24)	117.1	376	656	$5.02 \cdot 10^{20}$
2048	(48,84)	175.4	(36,24,24)	125.2	384	672	$8.53 \cdot 10^{20}$
2049	(48,85)	179.6	(37,24,24)	128.8	384	680	$1.45 \cdot 10^{21}$
2050	(49,85)	183.3	(36,24,25)	130.2	392	680	$2.47 \cdot 10^{21}$

Table 11. Proposed parameters for Rainbow over GF(256)

5 Summary

In this section we summarize the results presented in the previous section. We compare Rainbow schemes over the three fields $GF(16)$, $GF(31)$ and $GF(256)$ in terms of key sizes and signature lengths.

5.1 Key Sizes

Table 12 shows the public key sizes of Rainbow schemes over $GF(16)$, $GF(31)$ and $GF(256)$.

year	GF(16)	GF(31)	GF(256)
2010	38.1	30.7	**25.7**
2020	65.0	**44.9**	47.5
2030	102.3	**72.3**	84.0
2040	138.0	**99.7**	122.6
2050	197.5	**138.8**	183.3

Table 12. Public key sizes of Rainbow over different fields (in kB)

At the moment, the key sizes are minimal for Rainbow Schemes over GF(256), but they increase much faster than the key sizes needed over GF(31). So, from the year 2018 on, the smallest keys are those of Rainbow schemes over GF(31).

5.2 Signature Lengths

Table 13 compares Rainbow schemes over $GF(16)$, $GF(31)$ and $GF(256)$ in terms of the signature length.

year	GF(16)	GF(31)	GF(256)
2010	**244**	280	344
2020	**292**	312	424
2030	**340**	360	520
2040	**376**	408	592
2050	**424**	456	680

Table 13. Signature sizes for Rainbow over different fields (in bit)

As the table shows, one gets the shortest signatures when using Rainbow over GF(16). These signatures are about 20 to 30 bit shorter than the ones you get with GF(31). The signatures of Rainbow over GF(256) are much longer and this difference in length will increase over time.

6 Conclusion

Although nobody can say, which cryptanalytic developments and developments in computing devices will take place in the next years, we hope that this paper will help people to choose 1) the field most suitable for their purpose and 2) appropriate parameters for the Rainbow signature scheme. The proposed parameter sets should give the reader an impression, which public key sizes are needed to achieve given levels of security.

7 Acknowledgements

We thank Jintai Ding, Bo-Yin Yang and Erik Dahmen for many helpful comments.

References

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

[BC06] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235-265, 1997

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

[CC08] Chen, A.I.-T., Chen, C.-H. O., Chen, M.-S., Cheng, C.M., and Yang, B.-Y.: Practical-Sized Instances for Multivariate PKCs: Rainbow, TTS and ℓIC- Derivatives. In: LNCS 5299 pp. 95–108, Springer Heidelberg (2008)

[CC09] Chen, A.I.-T., Chen, M.S., Chen T.R., Cheng, C.M., Ding, J., Kuo, E.L.H., Lee, F.Y.S., Yang B.-Y.: SSE-Implementation of Multivariate PKC's on Modern x86-CPUs. CHES 2009, pp. 33 -48

[CS94] Coppersmith, D., Stern, J., Vaudenay, S.: Attacks on the Birational Signature Scheme. In LNCS 773 pp. 435 to 443, Springer, Heidelberg (1994)

[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., and Cheng, C.M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: LNCS 5037, pp.242–257, Springer, Heidelberg (2005)

[DW07] Ding, J., Wolf, C., Yang, B.-Y.: ℓ-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., and Dubois, V.: Breaking the symmetry: A way to resist the new Differential attacks. Available at http://www.eprint.iacr.org/2007/366.pdf

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

[Fa02] Faugere, J.C.: A new efficient algorithm for computing Groebner bases without reduction to zero (F5). In International Symposium on Symbolic and Algebraic Computation ISSAC 2002, pp. 75–83. ACM Press (2002)

[FP08] J.-C. Faugere, L. Perret: On the security of UOV. In: Proceedings of the First International Conference on Symbolic Computation and Cryptology, Beijing, 2008

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

[GP09] G.-M. Greuel, G. Pfister and H. Schönemann: Singular 3.1.0 — A computer algebra system for polynomial computations, http://www.singular.uni-kl.de (2009)

[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: Krawzyck, H. (ed.) CRYPTO 1998, LNCS vol. 1462, pp. 257–266 Springer, Heidelberg (1998)

[LV00] Lenstra, A.K., Verheul E.R.: Selecting Cryptographic Key Sizes. PKC 2000, pp. 446–465, www.keylength.com

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

[Pa96] Patarin, J.: Hidden Field equations (HFE) and Isomorphisms of Polynomials (IP). In: Proceedings of EUROCRYPT'96, pp. 38–48, Springer, Heidelberg (1996)

[Pa97] Patarin, J,: The oil and vinegar signature scheme, presented at the Dagstuhl Workshop on Cryptography (September 97)

[PG98] Patarin, J., Goubin, L., Courtois, N.: C^*_+ and HM: Variations about two schemes of H. Matsumoto and T. Imai. In: Proceedings of ASIACRYPT'98, pp. 35–49, Springer, Heidelberg (1998)

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

[YC05] Yang, B.-Y., Chen J.-M.: Building secure tame like multivariate public-key cryptosystems: The new TTS. In: Boyd, C., Gonzales 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 LNCS 3506 pp. 67–86. Springer, Heidelberg (2007)

[Ya07] Yang, B.-Y., Chen, C.-H. O., Bernstein, D.J., and Chen, J.-M.: Analysis of QUAD. In: Biryukov, A. (ed.) FSE 2007, LNCS 4593 pp. 290–307. Springer, Heidelberg (2007)