Cryptanalysis for 2-Layer TriRainbow

Taku Kato[1] and Shuhei Nakamura[2]

[1] Chigasaki-shi, Kanagawa, Japan
katotaku243@gmail.com
[2] Department of Computer and Information Sciences, Ibaraki University, Japan
shuhei.nakamura.fs71@vc.ibaraki.ac.jp

Abstract. TriRainbow is proposed by Ganguly and Saxena as a variant of the multi-layered scheme Rainbow. They show that TriRainbow is as efficient as Rainbow, but resistants to known attacks breaking Rainbow. In this paper, we propose efficient attacks against 2-layer TriRainbow by combining two known attacks against Rainbow. As a result, the complexity of our attack against SL1 TriRainbow is only 2^{32} for version 1, and 2^{70} for version 2. Moreover, our experiment shows that an equivalent key of TriRainbow version 1 with the parameter $(q, v, o, t) = (16, 36, 32, 32)$ is computed in a few minutes with a laptop.

Keywords: Post-quantum cryptography · Multivariate public key cryptography · Rainbow · TriRainbow

1 Introduction

Standard RSA and EC cryptosystems are designed based on difficult mathematical problems such as prime factorization and discrete logarithm problems. However, these mathematical problems are known to be solved in polynomial time using a large-scale quantum computer [9]. It is therefore necessary to construct cryptography based on new mathematical problems resistant to quantum computers. Such cryptography is referred to as post-quantum cryptography. In 2015, the National Security Agency announced a plan for a transition to post-quantum cryptography, and the National Institute of Standards and Technology (NIST) started public recruitment of such cryptography candidates in 2016.

Multivariate public key cryptography is based on an NP-hard problem of solving a system of quadratic equations, called the MQ problem [8], and is one of candidates in the NIST PQC standardization project [10]. UOV is a multivariate digital signature scheme proposed by Kipnis et al. [7], and has essentially not been broken over 20 years. Based on UOV, Ding et al. [4] proposed Rainbow as its multi-layered version and show that it can be simply and efficiently implemented using linear algebra methods over a small finite field. It is one of the finalists for the 3rd round of the NIST PQC standardization project [11]. In 2022, Beullens

Corresponding author: Taku Kato (katotaku243@gmail.com) proposed Simple attack and Combined attack against Rainbow and shows SL3 and SL5 Rainbow parameters satisfy only SL1 and SL3, respectively [2].

Recently, there are many studies on modifying UOV or Rainbow. For example, Beullens proposed MAYO and Furue et al. proposed QR-UOV. In 2023, Ganguly and Saxena [6] proposed TriRainbow as such a scheme, which replaces some of the oil variables in Rainbow with triangular variables. They show that it is more efficient than Rainbow but resistant to known attacks such as the Simple attack [2]. Moreover, for known attacks against Rainbow, they proposed the 2-layer TriRainbow parameter sets which satisfy the security levels of the NIST PQC standardization project.

In this paper, we propose attacks against 2-layer TriRainbow. Our attacks combine two known attacks against Rainbow. Namely, for 2-layer TriRainbow version 1, our attack is combined the HighRank attack and the Direct attack, and for 2-layer TriRainbow version 2, is combined the HighRank attack and the Simple attack. The complexity of our attack is about 2^{32} for SL1 TriRainbow version 1, and about 2^{70} for SL1 TriRainbow version 2. Moreover, our experiment shows that an equivalent key of TriRainbow version 1 with the parameter $(q, v, o, t) = (16, 36, 32, 32)$ is computed within a few minutes.

The reminder of this paper is organized as follows. In Section 2, we explain the construction of Rainbow and some known attacks against Rainbow. In Section 3, we review TriRainbow and describe two versions of 2-layer TriRainbow. In Section 4, we propose attacks for 2-layer TriRainbow. In Section 5, for our attack, we provide a complexity estimation for the proposed 2-layer TriRainbow parameters. We conclude this paper in Section 6.

2 Cryptanalysis against Rainbow

In this section, we present the notations used in this paper. Then we explain the construction of Rainbow and some known attacks against Rainbow.

2.1 Notations

Let $\mathbb{N}$ be the set of natural numbers. We denote by $\mathbb{F}_q$ a finite field with q elements. Let $\mathbb{F}_q^n$ be the set of n-dimensional vectors over $\mathbb{F}_q$ for $n \in \mathbb{N}$. For $m, n \in \mathbb{N}$, we write $\mathbb{F}_q^{m \times n}$ as the set of $(m \times n)$-matrices over $\mathbb{F}_q$. We write $A^\top$ as the transposed matrix of A.

2.2 Rainbow

In this section, we review Rainbow [4], which is a multi-layer version of UOV [7].

First, we define the notation used for Rainbow. The parameters of Rainbow are (q, v, o_1, o_2). The number of variables is given by $n = v + o_1 + o_2$ and the number of equations is given by $m = o_1 + o_2$. The indices of variables are divided into $V := \{1, \dots, v\}$, $O_1 := \{v + 1, \dots, v + o_1\}$ and $O_2 := \{v + o_1 + 1, \dots, n\}$.

Let $\mathcal{O}_1 := \{x \in \mathbb{F}_q^n \mid x_i = 0, i \in V\}$, $\mathcal{O}_2 := \{x \in \mathbb{F}_q^n \mid x_i = 0, i \in V \cup O_1\}$, $\mathcal{W} := \{(x_{v+1}, \ldots, x_n) \in \mathbb{F}_q^m \mid x_i = 0, i \in O_1\}$.

Next, we explain the public key and the secret key of Rainbow. Two invertible linear maps $\mathcal{S} \in \mathbb{F}_q^{m\times m}, \mathcal{T} \in \mathbb{F}_q^{n\times n}$ are chosen randomly. We choose a central map $\mathcal{F} = (\mathcal{F}^{(v+1)}, \ldots, \mathcal{F}^{(n)})^\top : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The first o_1 polynomials $\mathcal{F}^{(v+1)}, \ldots, \mathcal{F}^{(v+o_1)}$ are of the form

$$\mathcal{F}^{(k)}(x) = \sum_{i\in O_1, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1} \gamma_i^{(k)} x_i + \eta^{(k)}, \tag{1}$$

where $k \in O_1$, and the last o_2 polynomials $\mathcal{F}^{(v+o_1+1)}, \ldots, \mathcal{F}^{(n)}$ are of the form

$$\mathcal{F}^{(k)}(x) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{2}$$

where $k \in O_2$. Then, the public key of Rainbow is $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$, and the secret key of Rainbow is $(\mathcal{S}, \mathcal{F}, \mathcal{T})$. The representation matrices of $\mathcal{S}$ and $\mathcal{T}$ are denoted by S and T, respectively. Let $F^{(k)}$ be the representation matrix of a quadratic map $\mathcal{F}^{(k)}$.

2.3 Key recovery attack against Rainbow

In this subsection, we review the key recovery attack against Rainbow.

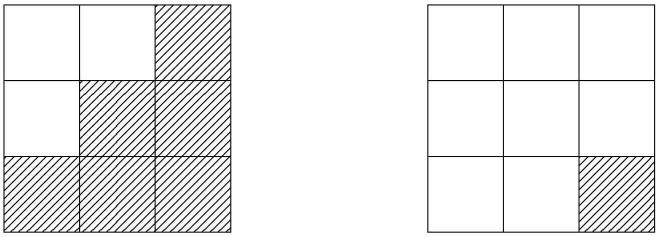
First, we recall the definition of an equivalent key, which is used some key recovery attacks on Rainbow [2,5].

Definition 1 (Equivalent key) *Fix $I = \{I^{(k)}\}_{k=v+1}^n$ ($I^{(k)} \subseteq \{(i,j) : 1 \leq i \leq j \leq n\}$). Let $\mathcal{S}, \mathcal{S}' : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{T}, \mathcal{T}' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be linear maps, and $\mathcal{F}, \mathcal{F}' : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be quadratic map. Then, $(\mathcal{S}', \mathcal{F}', \mathcal{T}')$ is* **an equivalent key** *of $(\mathcal{S}, \mathcal{F}, \mathcal{T})$ with respect to I if*

$$\mathcal{S}' \circ \mathcal{F}' \circ \mathcal{T}' = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$$

and $F'^{(k)}_{i,j} = F^{(k)}_{i,j}$ for $(i,j) \in I^{(k)}$ and $k \in \{v+1, \ldots, n\}$.

For Rainbow, the set $I^{(k)}$ is defined as the set of an index corresponding a monomial with zero coefficient in $\mathcal{F}^{(k)}$. Namely, for $k \in O_1$, $I^{(k)} = \{(i,j) : 1 \leq i \leq v, v + o_1 + 1 \leq j \leq n\} \cup \{(i,j) : v+1 \leq i \leq n, i \leq j \leq n\}$, and for $k \in O_2$, $I^{(k)} = \{(i,j) : v + o_1 + 1 \leq i \leq j \leq n\}$.



$I^{(k)}$ $(k \in O_1)$ $I^{(k)}$ $(k \in O_2)$

Fig. 1. $I = \{I^{(k)}\}_{k \in O_1 \bigcup O_2}$ (Rainbow)

With invertible linear maps $\Sigma : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\Omega : \mathbb{F}_q^n \to \mathbb{F}_q^n$, the equivalent key of Rainbow is constructed as follows:

$$\begin{aligned} \mathcal{S}' &:= \mathcal{S} \circ \Sigma, \\ \mathcal{F}' &:= \Sigma^{-1} \circ \mathcal{F} \circ \Omega^{-1}, \\ \mathcal{T}' &:= \Omega \circ \mathcal{T}. \end{aligned}$$

By the condition on the coefficient in I, two linear maps Σ and Ω have the following form:

$$\Omega = \begin{array}{|c|c|c|}\hline \Omega_1 & 0 & 0 \\ \hline \Omega_2 & \Omega_3 & 0 \\ \hline \Omega_4 & \Omega_5 & \Omega_6 \\ \hline \end{array} \qquad \Sigma = \begin{array}{|c|c|}\hline \Sigma_1 & 0 \\ \hline \Sigma_2 & \Sigma_3 \\ \hline \end{array}$$

Fig. 2. Linear maps Σ, Ω (Rainbow)

By setting $\Omega_1, \dots, \Omega_6, \Sigma_1, \Sigma_2, \Sigma_3$ appropriately, equivalent keys T', S' can take the following forms:

$$T' = \begin{array}{|c|c|c|}\hline I & T_1' & T_2' \\ \hline 0 & I & T_3 \\ \hline 0 & 0 & I \\ \hline \end{array} \qquad S' = \begin{array}{|c|c|}\hline I & S_1' \\ \hline 0 & I \\ \hline \end{array}$$

Fig. 3. Equivalent keys T', S' (Rainbow)

Next, we recall the key recovery attack against Rainbow and in particular, we explain the Simple attack [2]. For a quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, we define the **polar form** $\mathcal{P}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^m$ as follows:

$$\mathcal{P}'(x, y) := \mathcal{P}(x + y) - \mathcal{P}(x) - \mathcal{P}(y) + \mathcal{P}(0).$$

When fixing $y \in \mathbb{F}_q^n$, we denote by $\mathcal{P}'_y$ the map $x \mapsto \mathcal{P}'(x, y)$. By the structure I of Rainbow, we obtain the following properties:

- $\mathcal{P}(x) = 0$ for $x \in \mathcal{T}^{-1}\mathcal{O}_2$,
- $\mathcal{P}'(x, y) \in S\mathcal{W}$ for $x \in \mathcal{T}^{-1}\mathcal{O}_2$, $y \in \mathbb{F}_q^n$, and
- $\mathcal{P}(x) \in S\mathcal{W}$ for $x \in \mathcal{T}^{-1}\mathcal{O}_1$.

Then, these properties are represented as the diagram in Figure 4.

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[d, "\mathcal{P}"] & \mathcal{T}^{-1}\mathcal{O}_1 \arrow[l, hook] \arrow[d, "\mathcal{P}"] & \mathcal{T}^{-1}\mathcal{O}_2 \arrow[l, hook] \arrow[d, "\mathcal{P}"] \arrow[dl, "\mathcal{P}'_y"] \\
\mathbb{F}_q^m & \mathcal{S}^{-1}\mathcal{W} \arrow[l, hook] & \{0\} \arrow[l, hook]
\end{tikzcd}$$

Fig. 4. Quadratic map $\mathcal{P}$ and linear map $\mathcal{P}'_y$ (Rainbow)

The Simple attack recovers $x \in \mathcal{T}^{-1}\mathcal{O}_2$ in the kernel of $\mathcal{P}'_y$ using the relationship in Figure 4. Note that, since the dimension of $\mathcal{T}^{-1}\mathcal{O}_2$ and $S^{-1}\mathcal{W}$ are o_2, the dimension of the kernel of $\mathcal{P}'_y|_{\mathcal{T}^{-1}\mathcal{O}_2}$ for a random chosen $y \in \mathbb{F}_q^n$ is at least 1 with probability

$$1 - \prod_{i=0}^{o_2-1} (1 - q^{i-o_2}) \fallingdotseq \frac{1}{q}.$$

The outline of the Simple attack is as follows. First, $y \in \mathbb{F}_q^n$ is chosen uniformly randomly. By using linear equations $\mathcal{P}'_y(x) = 0$, we eliminate m variables in x and substitute x into the equation $\mathcal{P}(x) = 0$ in Figure 4. By solving the quadratic equations, we compute $x \in \mathcal{T}^{-1}\mathcal{O}_2$. Then, the equivalent key $(\mathcal{S}', \mathcal{F}', \mathcal{T}')$ will be recovered efficiently.

3 2-layer TriRainbow

In this section, we review TriRainbow [6] and describe two versions of 2-layer TriRainbow.

3.1 TriRainbow

In this subsection, we recall a digital signature scheme TriRainbow proposed by Ganguly and Saxena [6] as an efficient modified Rainbow.

TriRainbow has a multi-layer form similar to Rainbow but each layer uses not only a UOV form but also the triangular form. More precisely, the layers of TriRainbow consist of alternating triangular forms and UOV forms although the layers of Rainbow consist only of UOV forms.

Rainbow is originally proposed as a multi-layer version of UOV but its two layer case is mainly used for efficiency [4]. The authors also focus on two layer case of TriRainbow in order to obtain the same efficiency as Rainbow. In [6], they give the security analysis of TriRainbow for the known attacks against Rainbow including the Simple attack and the Combined attack, which lead to totally break Rainbow in [2]. As a result, for such an attack, they provide the parameters of TriRainbow with two layers for satisfying the security levels in the NIST PQC standardization project.

2-layer TriRainbow is the scheme which one of the two layers of Rainbow is replaced by the triangular form, and it has the parameters (q, v, o, t). The number of variables is given by $n = v + o + t$ and the number of equations is given by $m = o + t$. There are two different versions in 2-layer TriRainbow depending on the position of a triangular form.

3.2 2-layer TriRainbow version 1

The indices of variables are divided into $V := \{1, \ldots, v\}$, $O := \{v+1, \ldots, v+o\}$, $Tri := \{v+o+1, \ldots, n\}$. Let $\mathcal{O} := \{x \in \mathbb{F}_q^n \mid \ x_i = 0, i \in V\}$, $\mathcal{T}_{ri} := \{x \in \mathbb{F}_q^n \mid x_i = 0, i \in V \cup O\}$, $\mathcal{W} := \{(x_{v+1}, \ldots, x_n) \in \mathbb{F}_q^m \mid x_i = 0, i \in O\}$.

We explain the public key and the secret key of 2-layer TriRainbow version 1. Two invertible linear maps $\mathcal{S} \in \mathbb{F}_q^{m \times m}, \mathcal{T} \in \mathbb{F}_q^{n \times n}$ are chosen randomly. We choose a central map $\mathcal{F} = (\mathcal{F}^{(v+1)}, \ldots, \mathcal{F}^{(n)})^\top : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The first o polynomials $(\mathcal{F}^{(v+1)}, \ldots, \mathcal{F}^{(v+o)})$ are of the form

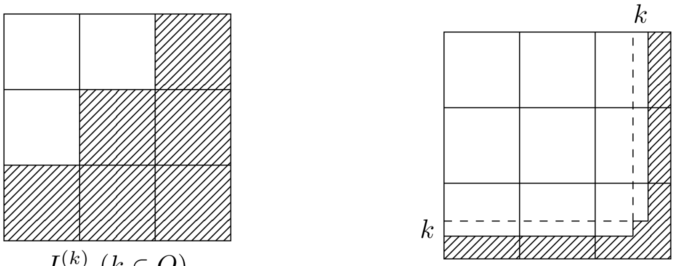
$$\mathcal{F}^{(k)}(x) = \sum_{i,j \in V, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in O, j \in V} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup Tri} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{3}$$

where $k \in O$, and the last t polynomials $\mathcal{F}^{(v+o+1)}, \ldots, \mathcal{F}^{(n)}$ are of the form

$$\mathcal{F}^{(k)}(x) = \sum_{1 \le i \le k-1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \le k-1} \beta_{ij}^{(k)} x_i x_k + \sum_{1 \le i \le k} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{4}$$

where $k \in Tri$. Then, the public key is $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$, and the secret key is $(\mathcal{S}, \mathcal{F}, \mathcal{T})$. The representation matrices of $\mathcal{S}, \mathcal{T}$ are denoted by S, T. Let $F^{(k)}$ be the representation matrix of a quadratic map $\mathcal{F}^{(k)}$.

An equivalent key of 2-layer TriRainbow version 1 is as follows. For 2-layer TriRainbow version 1, the set $I^{(k)}$ corresponds to the monomials with zero coefficient in $\mathcal{F}^{(k)}$. Namely, $I^{(k)} = \{(i,j) : 1 \le i \le v, v+o+1 \le j \le n\} \cup \{(i,j) : v+1 \le i \le n, i \le j \le n\}$ for $k \in O$, and $I^{(k)} = \{(i,j) : 1 \le i \le k-1, k+1 \le j \le n\} \cup \{(i,j) : k \le i \le j \le n\}$ for $k \in Tri$.



$I^{(k)}$ $(k \in O)$ $I^{(k)}$ $(k \in Tri)$

Fig. 5. Structure $I = \{I^{(k)}\}_{k \in O \bigcup Tri}$

With invertible linear maps $\Sigma : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\Omega : \mathbb{F}_q^n \to \mathbb{F}_q^n$, the equivalent key of 2-layer TriRainbow version 1 is constructed as follows:

$$\begin{aligned}
\mathcal{S}' &:= \mathcal{S} \circ \Sigma \\
\mathcal{F}' &:= \Sigma^{-1} \circ \mathcal{F} \circ \Omega^{-1} \\
\mathcal{T}' &:= \Omega \circ \mathcal{T}.
\end{aligned}$$

By the condition on the coefficient in I, two linear maps Σ and Ω have the following form:

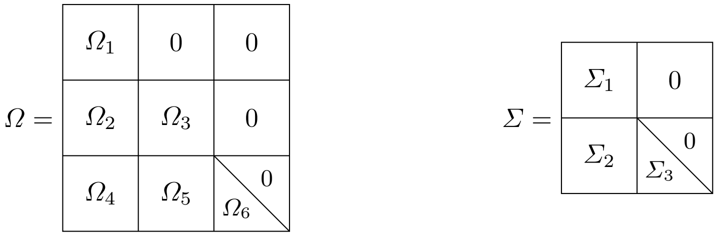


Fig. 6. Linear maps Σ, Ω (2-layer TriRainbow version 1)

By setting $\Omega_1, \ldots, \Omega_6, \Sigma_1, \Sigma_2, \Sigma_3$ appropriately, equivalent keys T' and S' can take the following forms:

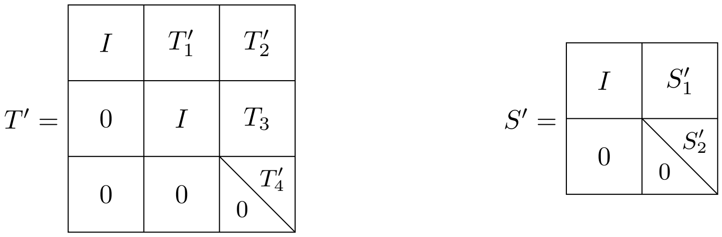


Fig. 7. Equivalent keys T', S' (2-layer TriRainbow version 1)

3.3 2-layer TriRainbow version 2

The indices of variables are divided into $V := \{1, \dots, v\}$, $Tri := \{v+1, \dots, v+t\}$, $O := \{v+t+1, \dots, n\}$. Let $\mathcal{T}_{ri} := \{x \in \mathbb{F}_q^n \mid x_i = 0, i \in V\}$, $\mathcal{O} := \{x \in \mathbb{F}_q^n \mid x_i = 0, i \in V \cup Tri\}$, $\mathcal{W} := \{(x_{v+1}, \dots, x_n) \in \mathbb{F}_q^m \mid x_i = 0, i \in Tri\}$.

We explain the public key and the secret key of 2-layer TriRainbow version 2. Two invertible linear maps $\mathcal{S} \in \mathbb{F}_q^{m \times m}, \mathcal{T} \in \mathbb{F}_q^{n \times n}$ are chosen randomly. We choose a central map $\mathcal{F} = (\mathcal{F}^{(v+1)}, \dots, \mathcal{F}^{(n)})^\top : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The first t polynomials $(\mathcal{F}^{(v+1)}, \dots, \mathcal{F}^{(v+o)})$ are of the form

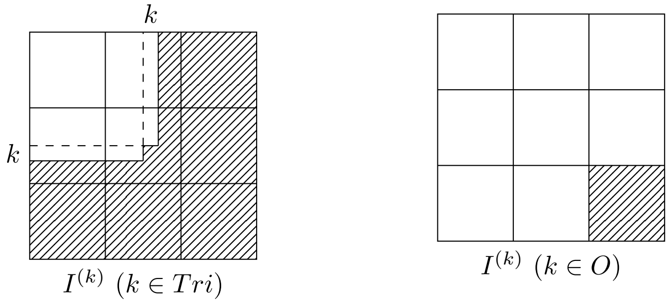
$$\mathcal{F}^{(k)}(x) = \sum_{1 \le i \le k-1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \le k-1} \beta_{ij}^{(k)} x_i x_k + \sum_{1 \le i \le k} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{5}$$

where $k \in Tri$, and the last o polynomials $\mathcal{F}^{(v+t+1)}, \dots, \mathcal{F}^{(n)}$ are of the form

$$\mathcal{F}^{(k)}(x) = \sum_{i,j \in V \cup Tri, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in O, j \in V \cup Tri} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup Tri \cup O} \gamma_i^{(k)} x_i + \eta^{(k)} \tag{6}$$

where $k \in O$. Then, the public key is $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$, and the secret key is $(\mathcal{S}, \mathcal{F}, \mathcal{T})$. The representation matrices of $\mathcal{S}, \mathcal{T}$ are denoted by S, T. Let $F^{(k)}$ be the representation matrix of a quadratic map $\mathcal{F}^{(k)}$.

An equivalent key of 2-layer TriRainbow version 2 is as follows. For 2-layer TriRainbow version 2, the set $I^{(k)}$ corresponds to the monomials with zero coefficient in $\mathcal{F}^{(k)}$. Namely, for $k \in Tri$, $I^{(k)} = \{(i,j) : 1 \le i \le k-1, k+1 \le j \le n\} \cup \{(i,j) : k \le i \le j \le n\}$, and, for $k \in O$, $I^{(k)} = \{(i,j) : v+t+1 \le i \le j \le n\}$.



$I^{(k)}$ $(k \in Tri)$

$I^{(k)}$ $(k \in O)$

Fig. 8. Structure $I = \{I^{(k)}\}_{k \in Tri \bigcup O}$

With invertible linear maps $\Sigma : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\Omega : \mathbb{F}_q^n \to \mathbb{F}_q^n$, the equivalent key of 2-layer TriRainbow version 2 is constructed as follows:

$$
\begin{aligned}
\mathcal{S}' &:= \mathcal{S} \circ \Sigma \\
\mathcal{F}' &:= \Sigma^{-1} \circ \mathcal{F} \circ \Omega^{-1} \\
\mathcal{T}' &:= \Omega \circ \mathcal{T}.
\end{aligned}
$$

By the condition on the coefficient in I, two linear maps Σ and Ω have the following forms:

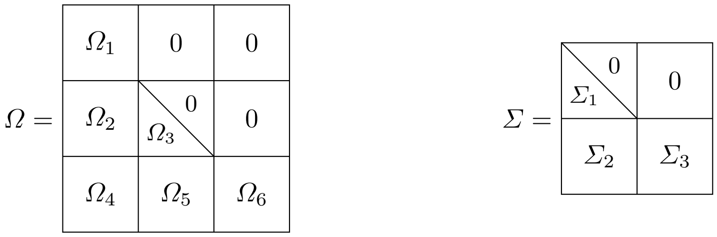


Fig. 9. Linear maps Σ, Ω (2-layer TriRainbow version 2)

By setting $\Omega_1, \ldots, \Omega_6, \Sigma_1, \Sigma_2, \Sigma_3$ appropriately, equivalent keys T' and S' can take the following form:

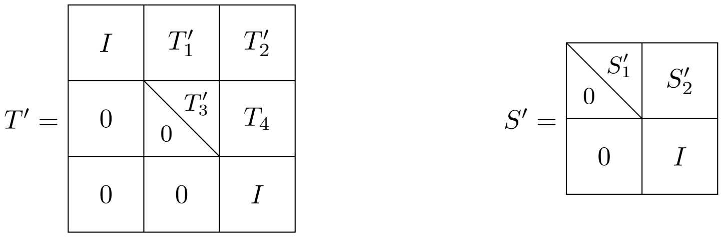


Fig. 10. Equivalent keys T', S' (2-layer TriRainbow version 2)

4 Proposed Attacks against 2-layer TriRainbow

In this section, we propose an attacks for 2-layer TriRainbow. First, we introduce our attack for 2-layer TriRainbow version 1 and then describe our attack for 2-layer TriRainbow version 2.

4.1 Our attack against 2-layer TriRainbow version 1

In this subsection, we propose an attack combining the HighRank attack and the Direct attack against 2-layer TriRainbow version 1.

First, we randomly choose a vector $\mathbf{a}$ from $\mathbb{F}_q^{o+t}$ and check that the kernel of $\sum_{i=v+1}^{n} a_i P^{(i)}$ is of dimension one. For such a vector $\mathbf{a}$, we define the vector $\mathbf{v}$ as $\mathrm{Ker}(\sum_{i=v+1}^{n} a_i P^{(i)}) = \langle \mathbf{v} \rangle$. If the solutions of $(\sum_{i=v+1}^{n} \lambda_i P^{(i)})\mathbf{v} = \mathbf{0}$ forms the subspace of dimension $o + t - 1$, then the basis of the subspace give the vector $\mathbf{s}_n$ of $\mathcal{S}'^{-1}$.

For $i \in \{v+1, \dots, n-1\}$ and $j \in \{1, \dots, n\}$, comparing the (j, n)-th coordinate of the representing matrices with respect to the first $o + t - 1$ components of $\mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1} = \mathcal{F}'$, we have

$$\mathbf{e}_j^\top \{P^{(i)} + s_{i,n} P^{(n)}\} \mathbf{t}_n = 0. \tag{7}$$

Since the equations (7) are $(o + t - 1)n$ linear equations in $n - 1$ variables, the vector $\mathbf{t}_n$ can be computed by Gaussian elimination.

Thus we can obtain the matrix $\mathcal{T}'_{(1)}$ such that the n-th column is $\mathbf{t}_n$ and the other columns are $\mathbf{e}_1, \dots, \mathbf{e}_{n-1}$, and the matrix $\mathcal{S}'_{(1)}$ such that the n-th column is $\mathbf{s}_n$ and the other rows are $\mathbf{e}_{v+1}, \dots, \mathbf{e}_{n-1}$. Define $\mathcal{P}_{(1)} = \mathcal{S}'_{(1)} \circ \mathcal{P} \circ \mathcal{T}'_{(1)}$. Then, for the first $o + t - 1$ components of $\mathcal{P}_{(1)}$, the n-th column and the n-th row are zero.

Next, we will define $\mathcal{S}'_{(2)}, \dots, \mathcal{S}'_{(o+t)}$ and $\mathcal{T}'_{(2)}, \dots, \mathcal{T}'_{(o+t)}$ and obtain $\mathcal{P}_{(2)}, \dots, \mathcal{P}_{(o+t)}$ such that for the first $m - i$ components of $\mathcal{P}_{(i)}$, the last i columns and the last i rows are zero. We perform this procedure by induction with respect to

$\ell \in \{2, \ldots, o+t\}$ and assume that we obtain $\mathcal{S}'_{(2)}, \ldots, \mathcal{S}'_{(\ell-1)}, \mathcal{T}'_{(2)}, \ldots, \mathcal{T}'_{(\ell-1)}$, and $\mathcal{P}_{(2)}, \ldots, \mathcal{P}_{(\ell-1)}$.

We randomly choose a vector $\mathbf{a}$ from $\mathbb{F}_q^{o+t-\ell}$ and check that the kernel of $\sum_{i=v+1}^{n-\ell} a_i P^{(i)}$ is of dimension ℓ. For such a vector $\mathbf{a}$, we define the vector $\mathbf{v}_1, \ldots, \mathbf{v}_\ell$ as $\mathrm{Ker}(\sum_{i=v+1}^{n-\ell} a_i P^{(i)}) = \langle \mathbf{v}_1, \ldots, \mathbf{v}_\ell \rangle$. If the solutions of $\{(\sum_{i=v+1}^{n-\ell} \lambda_i P^{(i)})\mathbf{v}_j = \mathbf{0}\}_j$ forms the subspace of dimension $o+t-\ell$, then the basis of the subspace give the vector $\mathbf{s}_{n-\ell+1}$ of $\mathcal{S}'^{-1}$.

For $i \in \{v+1, \ldots, n-\ell\}$ and $j \in \{1, \ldots, n\}$, comparing the $(j, n-\ell+1)$-th coordinate of the representing matrices with respect to the first $o+t-\ell$ components of $\mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1} = \mathcal{F}'$, we have

$$\mathbf{e}_j^\top \{P^{(i)} + s_{i,n-\ell+1} P^{(n-\ell+1)}\} \mathbf{t}_{n-\ell+1} = 0. \tag{8}$$

Since the equations (8) are $(o+t-\ell)n$ linear equations in $n-\ell-1$ variables, the vector $\mathbf{t}_{n-\ell+1}$ can be computed by Gaussian elimination.

Thus we can obtain the matrix $\mathcal{T}'_{(\ell)}$ such that the $(n-\ell+1)$-th column is $\mathbf{t}_{n-\ell+1}$ and the other columns are $\mathbf{e}_1, \ldots, \mathbf{e}_{n-\ell}, \mathbf{e}_{n-\ell+2}, \ldots, \mathbf{e}_n$, and the matrix $\mathcal{S}'_{(\ell)}$ such that the ℓ-th column is $\mathbf{s}_\ell$ and the other columns are $\mathbf{e}_{v+1}, \ldots, \mathbf{e}_{\ell-1}, \mathbf{e}_{\ell+1}, \ldots, \mathbf{e}_n$. Define $\mathcal{P}_{(\ell)} = \mathcal{S}'_{(\ell)} \circ \mathcal{P}_{(\ell-1)} \circ \mathcal{T}'_{(\ell)}$. Then, for the first $o+t-\ell$ components of $\mathcal{P}_{(\ell)}$, its last ℓ columns and its last ℓ rows are zero.

By repeating the above operation recursively, $\mathbf{t}_{v+o+1}, \ldots \mathbf{t}_n$ will be computed.

Finally, $\mathcal{T}'^{-1}$ will be computed. As shown in Figure 11, define $\overline{T}' = \mathcal{T}_{(1)} \circ \cdots \circ \mathcal{T}_{(m)}$ and $\overline{T}''$ such that $\mathcal{T}'^{-1} = \overline{T}'\overline{T}''$. Then, we have

$$\mathcal{S}'^{-1} \circ \mathcal{P} \circ \overline{T}' = \mathcal{F}' \circ \overline{T}''^{-1}. \tag{9}$$

The left hand of equation (9) is revealed in this point. The first o quadratic maps of (9) is a public key of UOV with parameter (q, v, o) when restricting the domain to $\{(x_1, \ldots, x_{v+o}, 0, \ldots, 0) \mid x_i \in \mathbb{F}_q\}$.

Therefore, we can compute a pre-image of $\mathcal{P}$ by the Direct attack against UOV of the form (9). Alternatively, applying a key recovery attack against UOV, we can recover $\overline{T}''^{-1}$. Then, our attack becomes a key recovery attack. This is the outline of our attack against 2-layer TriRainbow version 1.

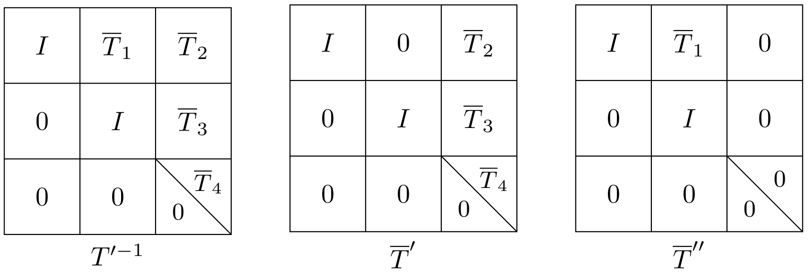


Fig. 11. A decompositon of equivalent key T'

Remark 1 Let (q, v, o, t) be a 2-layer TriRainbow version 1 parameter and put $n = v + o + t$ and $m = o + t$. For $d \in \mathbb{N}$ and $v + o + 1 \leq \ell \leq n$, we can add d dummy layers to the triangular layers of 2-layer TriRainbow in the ℓ-th position as follows. The central map of 2-layer TriRainbow with d dummy layers is

$$(\mathcal{F}^{(v+1)}, \ldots, \mathcal{F}^{(\ell-1)}, \mathcal{F}^{(\ell+d)}, \ldots, \mathcal{F}^{(n+d)}),$$

and other secret keys are two invertible linear maps $\mathcal{T} : \mathbb{F}^{n+d} \to \mathbb{F}^{n+d}$ and $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ (see Section 3.2). Moreover, the public key is $\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$. Then, our attack is still valid for 2-layer TriRainbow with such a dummy modifier. Indeed, after our attack recovers quadratic maps $\mathcal{F}^{(\ell+d)}, \ldots, \mathcal{F}^{(n+d)}$ as the same way above, we find $\mathbf{a} \in \mathbb{F}_q^{\ell-v-1}$ such that $V := \mathrm{Ker}(\sum_{i=v+1}^{\ell-1} a_i P^{(i)})$ is of dimension $n - \ell + d + 1$ and the solution space of $\{(\sum_{i=v+1}^{n-\ell} \lambda_i P^{(i)})\mathbf{v}_j = \mathbf{0}\}_j$ is of dimension $\ell - v - 1$ where $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_{n-\ell+d+1} \rangle$. Then, we obtain the vector $\mathbf{s}_{\ell-1}$ and solve linear equations (8) for the vectors $\mathbf{t}_\ell, \ldots, \mathbf{t}_{\ell+d-1}$ in succession. The remaining process is also the way in this subsection.

4.2 Our key recovery attack against 2-layer TriRainbow version 2

In this subsection, we propose a key recovery attack for 2-layer TriRainbow version 2. In our attack, the second UOV layer will be computed by the Simple attack. Then, the first triangular layer will be recovered in a similar way as the attack against the second layer of 2-layer TriRainbow version 1.

By the structure of central map $\mathcal{F}$ of 2-layer TriRainbow version 2, we have the following properties:

- $\mathcal{P}(x) = 0$ for $x \in \mathcal{T}^{-1}\mathcal{O}$ and
- $\mathcal{P}'(x, y) \in \mathcal{SW}$ for $x \in \mathcal{T}^{-1}\mathcal{O}$, $y \in \mathbb{F}_q^n$.

Then, these properties are represented as the diagram in Figure 12.

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[d, "\mathcal{P}"] & \mathcal{T}^{-1}\mathcal{T}_{ri} \arrow[l, hook'] \arrow[dl, "\mathcal{P}"] & \mathcal{T}^{-1}\mathcal{O} \arrow[l, hook'] \arrow[dl, "\mathcal{P}'_y"'] \arrow[d, "\mathcal{P}"] \\
\mathbb{F}_q^m & \mathcal{S}^{-1}\mathcal{W} \arrow[l, hook'] & \{0\} \arrow[l, hook']
\end{tikzcd}$$

Fig. 12. The diagram of $\mathcal{P}$ and $\mathcal{P}'_y$ of 2-layer TriRainbow version 2

Figure 12 is the same as Figure 4 in the place used for the Simple attack. Therefore, we can apply the Simple attack to 2-layer TriRainbow version 2 and $x \in \mathcal{T}^{-1}\mathcal{O}$ is recovered. The outline of the algorithm is as follows:

1. Choose $y \in \mathbb{F}_q^n$ uniformly randomly.
2. By using $\mathcal{P}'_y(x) = 0$, eliminate m variables in x.

3. Solve quadratic equations $\mathcal{P}(x) = 0$.
4. If there is no solution in the equations, return to 1.

Next, we recover S' by using $x \in \mathcal{T}^{-1}\mathcal{O}$ as follows. Let the first t vectors of $(S'^{-1})^\top$ be $\mathbf{s}_1, \dots, \mathbf{s}_t$. By the definition of equivalent key S' and $\mathcal{W}$, the space $(S\mathcal{W})^\perp$ is spanned by $\mathbf{s}_1, \dots, \mathbf{s}_t$. Then, by Figure 12, we have $\mathbf{s}_i^\top \mathcal{P}'(x, y) = 0$ for $i \in \{1, \dots, t\}$ and $y \in \mathbb{F}_q^n$. Especially, for $i \in \{1, \dots, t\}$ and $j \in \{1, \dots, n\}$, we have

$$\mathbf{s}_i^\top \mathcal{P}'(x, \mathbf{e}_j) = 0. \tag{10}$$

For $i \in \{1, \dots, t\}$, equations (10) are linear equations in the variables $\mathbf{s}_i$. By solving the equations for all $i \in \{1, \dots, t\}$, the secret key S' will be recovered.

The last o vectors of T'^{-1} be computed using S' as follows. For $i \in \{1, \dots, t\}$, $j \in \{1, \dots, n\}$ and $x' \in \mathbb{F}_q^n$, we have

$$\mathbf{s}_i^\top \mathcal{P}'(x', \mathbf{e}_j) = 0. \tag{11}$$

The equations 11 are linear equations in the variables x'. By solving the equations, a basis of $\mathcal{T}^{-1}\mathcal{O}$ is obtained. Applying Gaussian elimination, the last o vectors of T'^{-1} can be computed.

Finally, we compute $\mathbf{t}_{v+1}, \dots \mathbf{t}_{v+t}$ from $\mathbf{t}_{v+t}$ to $\mathbf{t}_{v+1}$ inductively.

First, we compute $\mathbf{t}_{v+t}$ as follows. For $k \in \{v+1, \dots, v+t-1\}$, $i \in V$, $j = v+t$, comparing the (i,j)-th coordinate of the representing matrix of the k-th quadratic map of $\mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1} = \mathcal{F}'$, we have

$$\mathbf{e}_i^\top \{P^{(k)} + \sum_{h \in Tri} s_{k,h} P^{(h)}\} \mathbf{t}_{v+t} = 0. \tag{12}$$

For all $k \in \{v+1, \dots, v+t-1\}$, $i \in V$, solving equations (12), the vector $\mathbf{t}_{v+t}$ is obtained.

We assume that $\mathbf{t}_{v+t}, \dots \mathbf{t}_{v+t-l+1}$ are recovered and we show the way to compute $\mathbf{t}_{v+t-l}$ from these vectors. For $k \in \{v+1, \dots, v+t-l\}$, $i \in V$, $j = v+t-l+1$, comparing the (i,j)-th coordinate of the representing matrix of the k-th quadratic map of $\mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1} = \mathcal{F}'$, we have

$$\mathbf{e}_i^\top \{P^{(k)} + \sum_{h \in Tri} s_{k,h} P^{(h)}\} \mathbf{t}_{v+t-l+1} = 0. \tag{13}$$

In addition, for $k \in \{v+t-l+1, \dots, v+t-1\}$, $i \in \{k+1, \dots, v+t\}$, $j = v+t-l+1$, comparing the (i,j)-th coordinate of the representing matrix of the k-th quadratic map of $\mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1} = \mathcal{F}'$, we have

$$\mathbf{e}_i^\top \{P^{(k)} + \sum_{h \in Tri} s_{k,h} P^{(h)}\} \mathbf{t}_{v+t-l+1} = 0. \tag{14}$$

The equations (13) and (14) are $(t-l)v + \sum_{k=v+t-l+1}^{v+t-1} (v+t-k) = (t-l)v + l(l-1)/2$ linear equations in $v+t-l$ variables $\mathbf{t}_{v+t-l+1}$. Since we have $(t-l)v + l(l-1)/2 \geq v+t-l$ for all $2 \leq l \leq t$ in the parameter proposed by [6], the vector $\mathbf{t}_{v+t-l+1}$ can be computed by Gaussian elimination.

By repeating the above operation recursively, $\mathbf{t}_{v+1}, \dots \mathbf{t}_{v+t}$ will be computed.

In the above procedure, the equivalent key $\mathcal{S}', \mathcal{T}'$ are computed. By computing $\mathcal{F}' = \mathcal{S}'^{-1} \circ \mathcal{P} \circ \mathcal{T}'^{-1}$, the quadratic map $\mathcal{F}'$ is also recovered. This is the outline of our attack for 2-layer TriRainbow version 2.

Remark 2 By the same argument as Remark 1, our attack is still valid for 2-layer TriRainbow version with a dummy modifier in Remark 1 to the triangular layer.

5 Cryptanalysis

In this section, for our attack presented in the previous section, we provide a complexity estimation for the 2-layer TriRainbow parameters proposed in [6]

5.1 Complexity estimation for 2-layer TriRainbow version 1

We estimate the complexity of our attack against 2-layer TriRainbow version 1.

In our attack against the second layer, the dominant part is to find the vector $\mathbf{v}$ such that the solution space of $(\sum_{i=v+1}^{n} \lambda_i P^{(i)})\mathbf{v} = \mathbf{0}$ is of dimension $o+t-1$ and is estimated by $\mathrm{O}((n^2 + n^3/6)q)$ in [5]. Our attack against the first layer is an attack against UOV of the form (9). The other parts are at most $\mathrm{O}(n^4)$ since only linear equations are solved.

When we use the Direct attack as an attack against UOV with a parameter (q, v, o), the complexity is estimated by

$$\mathrm{O}\left(\binom{o-1+D}{D}^2 \binom{o+1}{2}\right). \tag{15}$$

Here, $D \in \mathbb{N}$ is the minimal degree of terms whose coefficient is non-positive in the series $(1-t^2)^o(1-t)^{-o}$.

When we use the Intersection attack [1] as an attack against UOV with a parameter (q, v, o), we solve $M := \binom{k+1}{2}o - 2\binom{k}{2}$ quadratic equations in $N := k(v+o) - (2k-1)o$ variables where $k \in \mathbb{N}$ such that $(k-1)(v+o) - (2k-1)o > 0$. Then, the complexity is estimated by

$$\mathrm{O}\left(\binom{N-1+D}{D}^2 \binom{N+1}{2}\right). \tag{16}$$

Here, $D \in \mathbb{N}$ is the minimal degree of terms whose coefficient is non-positive in the series $(1-t^2)^M(1-t)^{-N}$.

Table 1 shows the complexity of our attack for 2-layer TriRainbow version 1 and the security level asserted in [6]. Therefore, 2-layer TriRainbow version 1 does not satisfy the security level asserted in [6] for known attacks against Rainbow.

Table 1. Comparing the complexity of our attack for 2-layer TriRainbow version 1 and the security level (SL) in [6]

SL	q	v	o	t	Complexity of our attack	Asserted SL in [6]
1	16	36	32	34	2^{32}	2^{145}
3	256	68	32	50	2^{109}	2^{207}
5	256	96	36	66	2^{118}	2^{272}

5.2 Complexity estimation for 2-layer TriRainbow version 2

We estimate the complexity of our attack for 2-layer TriRainbow version 2.

In our attack against the second layer, the dominant part is the complexity of computing $x \in \mathcal{T}^{-1}\mathcal{O}$. Then, we solve m quadratic equations in v variables and the complexity is estimated by

$$\mathrm{O}\left(\binom{v-1+D}{D}^2\binom{v+1}{2}\right). \tag{17}$$

Here, $D \in \mathbb{N}$ is the minimal degree of terms whose coefficient is non-positive in the series $(1-t^2)^m(1-t)^{-v}$.

In our attack against the first layer, the dominant part is to find the vector $\mathbf{v}$ such that the solution space of $(\sum_{i=v+1}^{v+o} \lambda_i P^{(i)})\mathbf{v} = \mathbf{0}$ is of dimension $o+t-1$ and is estimated by $\mathrm{O}(((v+o)^2 + (v+o)^3/6)q)$ in [5]. The other parts are at most $\mathrm{O}(n^4)$ since only linear equations are solved.

Table 2 shows the complexity of our attack for 2-layer TriRainbow version 2 and the security level asserted in [6]. Therefore, 2-layer TriRainbow version 2 does not satisfy the security level asserted in [6].

Table 2. Comparing the complexity of our attack for 2-layer TriRainbow version 2 and the security level (SL) in [6]

SL	q	v	t	o	Complexity of our attack	Asserted SL in [6]
1	16	36	34	32	2^{70}	2^{145}
3	256	68	34	48	2^{157}	2^{207}
5	256	96	38	64	2^{248}	2^{272}

5.3 Experiments

In this subsection, we perform an experiment on our attack against SL1 TriRainbow version 1. The experiments were performed by using Magma V2.24-5[3] on a 2.3 GHz Intel Core i7 CPU.

In the paper [6], Ganguly and Saxena provide cryptanalysis against their scheme and propose some parameters for satisfying the security level in the NIST PQC standardization project. They first take the parameter as the same as Rainbow and add some dummy layers to it for mitigating a partial key recovery against the upper layer as an option. For example, they add two dummy layers to the SL1 Rainbow parameter $(q, v, o, t) = (16, 36, 32, 32)$ and give $(q, v, o, t) = (16, 36, 32, 34)$ as their SL1 TriRainbow parameter. Then, their discussion for the complexity estimation does not need such a dummy modifier and the security of their parameters essentially depends on a parameter set based on Rainbow (see also Remark 1 and 2). Therefore we consider the security of their scheme without the dummy modifier.

Table 3 shows an experimental result for our key recovery attack against 2-layer TriRainbow version 1 with $(q, v, o, t) = (16, 36, 32, 32)$. Our experiment is the average timing of 20 experiments for the parameter. In the complexity estimation [6], the parameter attains the 128 bits security. However, Table 3 shows that our attack breaks the parameter in a few minutes. Note that we confirm our attack also breaks SL1 TriRainbow version 1 with two dummy layers as in Remark 1 in almost the same time as in Table 3.

Table 3. The average, the maximum, and the minimum of 20 experiments on our attack against 2-layer TriRainbow version 1 with $(q, v, o, t) = (16, 36, 32, 32)$.

Our attack	2nd Layer (sec)	1st Layer (sec)	Total (sec)
Average	72.1	220.8	292.9
Maximum	81.4	235.8	307.0
Minimum	64.9	205.0	276.5

6 Conclusion

In this paper, we propose new efficient attacks against 2-layer TriRainbow. Our attack uses the High rank attack for the triangular layer, and the Direct attack, the Intersection attack or the Simple attack for the UOV layer. Then, the complexities of the TriRainbow version 1 parameters $(q, v, o, t) = (16, 36, 32, 34), (256, 68, 32, 50)$ and $(256, 96, 36, 66)$ proposed by Ganguly and Saxena for satisfying $145, 207$ and 272 bits security are about $32, 109$ and 118 bits, respectively. Moreover, the complexities of the TriRainbow version 2 parameters $(q, v, t, o) = (16, 36, 34, 32), (256, 68, 34, 48)$ and $(256, 96, 38, 64)$ proposed by Ganguly and Saxena for satisfying $145, 207$ and 272 bits security are about $70, 157$ and 275 bits, respectively.

As future work, we will investigate the multi-layer TriRainbow for both versions.

References

1. Beullens, W.: Improved Cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021. LNCS, vol. 12696, pp. 348–373. Springer International Publishing, Cham (2021)
2. Beullens, W.: Breaking Rainbow Takes a Weekend on a Laptop. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022. LNCS, vol. 13508, pp. 464–479. Springer Nature Switzerland, Cham (2022)
3. Bosma, W., C.J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997)
4. Ding, J., Schmidt, D.: Rainbow, A New Multivariable Polynomial Signature Scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
5. 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., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
6. Ganguly, A., Saxena, N.: A new multivariate digital-signature scheme by mixing oil-vinegar with triangles (accessed 21 April 2023), `https://www.cse.iitk.ac.in/users/nitin/papers/TriRainbow.pdf`
7. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)
8. Michael R. Garey, D.S.J.: Computers and Intractability; A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York, NY, USA (1979)
9. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
10. National Institute of Standards and Technology: Post-Quantum Cryptography, `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization`
11. National Institute of Standards and Technology: Post-Quantum Cryptography, Round 3 Submissions, `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`