Revisiting the Security of VDOO

Siyu Li[1], Hao Guo[1], Peigen Li[2], and Siyong Tao[1]

[1] Department of Mathematical Sciences, Tsinghua University
guoh22@mails.tsinghua.edu.cn, lisiyu22@mails.tsinghua.edu.cn,
taosy22@mails.tsinghua.edu.cn
[2] Beijing Institute of Mathematical Sciences and Applications
lpg22@bimsa.cn

Abstract. VDOO is a multivariate signature scheme submitted to the Next-generation Commercial Cryptographic Algorithms Program (NGCC). We study the security of its submitted parameter sets. In this paper, VDOO is described as a multilayer Rainbow construction. By retaining only its last oil space, we obtain a generalized UOV instance and apply existing wedge attacks.
For the parameter set targeting 512-bit security, we estimate costs of 2^{432} and 2^{379} gates for the reconciliation and intersection variants, respectively. These estimates rely on the assumptions of the attack model and are below both the claimed security level and the attack costs reported in the specification.
Our analysis uses only the generalized UOV structure. The additional information in the multilayer structure may allow further improvements. Our results also motivate further study of parameter choices that balance resistance to known attacks with signing efficiency.

Keywords: Post-quantum cryptography · Multivariate cryptography · Cryptanalysis · VDOO · Wedge attacks

1 Introduction

Widely deployed public-key cryptosystems, including RSA and elliptic curve cryptosystems, rely on the hardness of integer factorization or discrete logarithms. Shor's algorithm solves these problems in polynomial time on a sufficiently large quantum computer [16], motivating the development of post-quantum cryptography. Proposed alternatives draw on several mathematical problems, including those arising from lattices, error-correcting codes, multivariate polynomial systems, and isogenies. Diversity among these foundations is important for avoiding dependence on a single family of hardness assumptions. As part of its standardization effort, NIST issued a call for additional digital signature schemes in September 2022 [12]. In 2023, it received 50 submissions, of which 40 satisfied the submission requirements [13]. In China, the Institute of Commercial Cryptography Standards (ICCS) launched the Next-generation Commercial Cryptographic Algorithms Program (NGCC) in 2025 to solicit algorithms addressing the threat of quantum computing [8]. The call for public-key algorithm proposals opened in October 2025 [9].

Multivariate public-key cryptosystems are of particular interest for their potential to offer short signatures and efficient arithmetic over finite fields. Their public keys typically consist of quadratic polynomials, and signature verification amounts to evaluating the corresponding polynomial map. The associated multivariate quadratic (MQ) decision problem is NP-complete in general [7]. However, this worst-case hardness does not by itself establish the security of a cryptographic construction: efficient signing requires a hidden trapdoor, whose structure may also be exploited by an attacker. The security analysis must therefore consider both generic equation solving and attacks against the particular trapdoor.

The unbalanced oil-and-vinegar (UOV) construction is a central example of this approach [11]. Its quadratic map vanishes on a hidden oil subspace, and fixing the vinegar variables makes the equations linear in the oil variables. Rainbow extends this principle to several layers [4], with the variables of preceding layers serving as vinegar variables for the next layer. Although Rainbow reached the third round of the NIST PQC process, subsequent attacks demonstrated that its nested structure could be exploited for efficient key recovery [2]. These results motivate a careful distinction between the security of an underlying UOV instance and the additional information exposed by a layered construction.

VDOO (Vinegar-Diagonal-Oil-Oil) is a first-round digital signature candidate in NGCC [10]. It introduces a diagonal layer followed by two oil-and-vinegar layers [6, 1]. For parameters (v, d, o_1, o_2, q), the diagonal part consists of d successive equations, each introducing one new variable linearly once the preceding variables are fixed. The remaining two layers introduce o_1 and o_2 oil variables, respectively. Thus VDOO can be viewed as a multilayer oil-and-vinegar construction. This design reduces the linear algebra required by the diagonal part, while retaining a nested trapdoor structure that warrants separate cryptanalytic study.

More specifically, the VDOO central map is precisely that of a $(d+2)$-layer Rainbow scheme with layer sizes $(1, \ldots, 1, o_1, o_2)$ [4]. The first d layers each have one oil variable and one equation, followed by two layers with o_1 and o_2 oil variables, respectively.

On the day after the NGCC first-round candidate list was published, the authors of this paper announced an attack on the submitted VDOO parameters on the PQC Forum [14]. The present paper provides a detailed explanation of that claim, including the attack method and its complexity estimates. Subsequently, Cartor et al. [3] also presented attacks on VDOO using Simple and MinRank-based methods. Their analysis concerns the earlier VDOO parameter sets and does not provide attack estimates for the parameter sets in the NGCC submission specification [1]. Our analysis focuses on those submission parameter sets.

Our Contribution We provide a detailed account of the wedge-based attack on the VDOO submission parameter sets [1]. We view VDOO as a generalized UOV instance and directly apply the recent wedge attacks [15, 5]. Specifically, retaining

only the last oil space gives an instance with $n = v + d + o_1 + o_2$ variables, oil-space dimension o_2, and $m = d + o_1 + o_2$ equations. This approach uses the UOV structure without exploiting the additional information in VDOO's multilayer flag, which we describe through its input and output subspaces.

For the submission parameter set targeting 512-bit security, $(q, v, d, o_1, o_2) = (256, 260, 10, 10, 175)$, we estimate gate-count exponents of 432 and 379 for the reconciliation and intersection variants of the wedge attack, respectively. Both are lower than the exponents 526 and 642 reported for the attacks in the specification. Thus, even this direct application of wedge attacks gives lower complexity estimates for the 512-bit parameter set, as summarized in Table 1.

Table 1: VDOO parameters and attack estimates. All attack complexities are expressed as $\log_2(\#\,\text{gates})$. The first three columns reproduce the values in the VDOO specification [1]. For each wedge attack, the second line gives (k, D, ℓ) defined in Sect. 4.

Security level	Parameters (q, v, d, o_1, o_2)	[1] (SA, RA)	Wedge attacks	
			Reconciliation	Intersection
128-bit	$(16, 67, 16, 14, 40)$	$(166, 162)$	172 $(19, 21, 1)$	–
256-bit	$(256, 205, 10, 17, 68)$	$(278, 281)$	948 $(2, 198, 2)$	–
512-bit	$(256, 260, 10, 10, 175)$	$(526, 642)$	432 $(123, 52, 1)$	**379** $(33, 37, 1)$

Outline Section 2 reviews UOV and Rainbow. Section 3 describes VDOO and its hidden subspace structure. Section 4 presents the wedge-attack complexity estimates. Section 5 concludes with directions for future work.

2 Preliminaries

In this section, we introduce the notation and review the UOV and Rainbow signature schemes.

Notation Let p be a prime power, and let $\mathbb{F}_q$ be a finite field with q elements and characteristic p. We use bold lowercase letters, such as $\mathbf{x}$, for column vectors and $\mathbf{x}^\top$ for their transposes. Calligraphic letters, such as $\mathcal{F}$ and $\mathcal{O}$, denote maps and spaces, while uppercase letters, such as F, denote matrices.

2.1 UOV Scheme

The UOV signature scheme was introduced by Kipnis, Patarin, and Goubin in 1999 [11]. Let $n = v + o$ with $v > o$. In the standard signature scheme, $m = o$. Partition the variables into vinegar and oil blocks:

$$\mathbf{x} = \begin{pmatrix} \mathbf{x}_V \\ \mathbf{x}_O \end{pmatrix}, \qquad \mathbf{x}_V \in \mathbb{F}_q^v, \quad \mathbf{x}_O \in \mathbb{F}_q^o. \tag{2.1}$$

Central map. Consider the homogeneous quadratic map

$$\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m, \qquad f_i(\mathbf{x}) = \mathbf{x}^\top F_i \, \mathbf{x}. \tag{2.2}$$

With respect to the block sizes (v, o), the coefficient matrices have the zero pattern

$$F_i = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}, \qquad 1 \le i \le m. \tag{2.3}$$

Here $*$ denotes a potentially nonzero block; no symmetry of F_i is assumed. The zero oil–oil block excludes all quadratic terms involving only oil variables. Thus the polynomials may contain vinegar–vinegar and vinegar–oil terms, and fixing $\mathbf{x}_V$ makes them affine linear in $\mathbf{x}_O$. In central coordinates, the oil space is

$$\mathcal{O} := \left\{ \begin{pmatrix} \mathbf{0} \\ \mathbf{o} \end{pmatrix} : \mathbf{o} \in \mathbb{F}_q^o \right\}, \qquad \mathcal{F}(\mathcal{O}) = \{0\}.$$

Inversion of the central map. Given a target $\mathbf{z} \in \mathbb{F}_q^m$, choose $\mathbf{x}_V$ uniformly at random. With these vinegar variables fixed, the equations

$$f_i(\mathbf{x}_V, \mathbf{x}_O) = z_i, \qquad 1 \le i \le m, \tag{2.4}$$

form a linear system in the o oil variables. Since $m = o$, a nonsingular coefficient matrix gives a unique solution. If the system is inconsistent, choose new vinegar variables and retry. A solution yields $\mathbf{x}$ satisfying $\mathcal{F}(\mathbf{x}) = \mathbf{z}$.

Public map and signing. Hide the central coordinates using invertible linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The public map is

$$\mathcal{P} : \mathbb{F}_q^n \xrightarrow{\mathcal{S}} \mathbb{F}_q^n \xrightarrow{\mathcal{F}} \mathbb{F}_q^m. \tag{2.5}$$

To sign a target $\mathbf{t} \in \mathbb{F}_q^m$ obtained by hashing the message, invert the central map as above. For a preimage $\mathbf{x}$, output $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{x})$. Verification checks $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.

2.2 Rainbow Scheme

We describe the central map of a two-layer Rainbow [4] construction. Let v, o_1, o_2 be positive integers, and set $n = v + o_1 + o_2$ and $m = o_1 + o_2$. Partition the variables as

$$\mathbf{x} = (\mathbf{x}_V, \mathbf{x}_{O_1}, \mathbf{x}_{O_2}) \in \mathbb{F}_q^v \times \mathbb{F}_q^{o_1} \times \mathbb{F}_q^{o_2}, \tag{2.6}$$

where $\mathbf{x}_V$ consists of the initial vinegar variables and $\mathbf{x}_{O_1}, \mathbf{x}_{O_2}$ are the oil variables of the two layers.

Central map. Consider the homogeneous quadratic map

$$\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m, \qquad f_i(\mathbf{x}) = \mathbf{x}^\top F_i \, \mathbf{x} \, . \tag{2.7}$$

With respect to the block sizes (v, o_1, o_2), the coefficient matrices have the following zero patterns:

$$\begin{aligned} F_i &= \begin{pmatrix} * & * & 0 \\ * & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad 1 \le i \le o_1, \\ F_i &= \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & 0 \end{pmatrix}, \qquad o_1 < i \le m. \end{aligned} \tag{2.8}$$

Here $*$ denotes a potentially nonzero block; no symmetry of F_i is assumed. The first-layer polynomials involve only $\mathbf{x}_V$ and $\mathbf{x}_{O_1}$, with no quadratic terms in $\mathbf{x}_{O_1}$. For the second layer, $(\mathbf{x}_V, \mathbf{x}_{O_1})$ act as vinegar variables, and there are no quadratic terms in $\mathbf{x}_{O_2}$.

Layer-by-layer inversion. Given a target $\mathbf{z} = (\mathbf{z}^{(1)}, \mathbf{z}^{(2)}) \in \mathbb{F}_q^{o_1} \times \mathbb{F}_q^{o_2}$, we seek $\mathbf{x}$ such that $\mathcal{F}(\mathbf{x}) = \mathbf{z}$. The block structure allows us to proceed in two steps:

1. Choose $\mathbf{x}_V$ uniformly at random. With $\mathbf{x}_V$ fixed, the first o_1 equations form a linear system in $\mathbf{x}_{O_1}$; solve this system with target $\mathbf{z}^{(1)}$.
2. Fix the resulting $(\mathbf{x}_V, \mathbf{x}_{O_1})$. The remaining o_2 equations form a linear system in $\mathbf{x}_{O_2}$; solve this system with target $\mathbf{z}^{(2)}$.

If either system is inconsistent, restart with a new choice of $\mathbf{x}_V$. Whenever both systems are solvable, the resulting $\mathbf{x} = (\mathbf{x}_V, \mathbf{x}_{O_1}, \mathbf{x}_{O_2})$ satisfies $\mathcal{F}(\mathbf{x}) = \mathbf{z}$.

Public map.

$$\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \xrightarrow{\mathcal{S}} \mathbb{F}_q^n \xrightarrow{\mathcal{F}} \mathbb{F}_q^m \xrightarrow{\mathcal{T}} \mathbb{F}_q^m, \tag{2.9}$$

Here $\mathcal{S}$ and $\mathcal{T}$ are invertible linear maps, and $\mathcal{F}$ is the central map defined above.

Remark 2.1. The inversion procedure extends to more than two layers by treating the variables of all preceding layers as vinegar variables for the current layer.

3 VDOO

In this section, we describe the VDOO signature scheme and its underlying mathematical structure.

3.1 Central Map

The parameters $n, m, v, d, o_1, o_2 \in \mathbb{N}^+$ satisfy

$$n = v + d + o_1 + o_2, m = d + o_1 + o_2.$$

We partition the variables as

$$\mathbf{x}^\top = (\mathbf{r}^\top, \mathbf{s}^\top, \mathbf{a}^\top, \mathbf{b}^\top) \in \mathbb{F}_q^n, \mathbf{r} \in \mathbb{F}_q^v, \mathbf{s} \in \mathbb{F}_q^d, \mathbf{a} \in \mathbb{F}_q^{o_1}, \mathbf{b} \in \mathbb{F}_q^{o_2}.$$

The central polynomial map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is divided into three layers: the diagonal layer, the first oil layer, and the second oil layer.

Diagonal Layer Each polynomial in the diagonal layer is constructed as follows:

$$f_{k-v}(\mathbf{x}) = \sum_{i=1}^{k-1} \alpha_{i,k}^{(k)} x_i x_k + \sum_{1 \le i \le j \le k-1} \beta_{i,j}^{(k)} x_i x_j = \mathbf{x}^\top F^{(k)} \mathbf{x},$$

where

$$k \in [v+1, \ldots, v+d], \alpha_{i,k}^{(k)}, \beta_{i,j}^{(k)} \in \mathbb{F}_q$$

and $F^{(k)}$ has the block form

$$\begin{pmatrix} A_k & \alpha_k & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_k \in \mathbb{F}_q^{(k-1)\times(k-1)}, \alpha_k \in \mathbb{F}_q^{k-1}.$$

First Oil Layer Each polynomial in the first oil layer is constructed as follows:

$$f_{k-v}(\mathbf{x}) = \sum_{1 \le i \le j \le v+d} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i=1}^{v+d} \sum_{j=v+d+1}^{v+d+o_1} \beta_{i,j}^{(k)} x_i x_j = \mathbf{x}^\top F^{(k)} \mathbf{x},$$

where

$$k \in [v+d+1, \ldots, v+d+o_1], \alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)} \in \mathbb{F}_q$$

and $F^{(k)}$ has the block form

$$\begin{pmatrix} B_k & C_k & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, B_k \in \mathbb{F}_q^{(v+d)\times(v+d)}, C_k \in \mathbb{F}_q^{(v+d)\times o_1}.$$

Second Oil Layer Each polynomial in the second oil layer is constructed as follows:

$$f_{k-v}(\mathbf{x}) = \sum_{1 \le i \le j \le v+d+o_1} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i=1}^{v+d+o_1} \sum_{j=v+d+o_1+1}^{v+d+o_1+o_2} \beta_{i,j}^{(k)} x_i x_j = \mathbf{x}^\top F^{(k)} \mathbf{x},$$

where

$$k \in [v+d+o_1+1, \ldots, v+d+o_1+o_2], \alpha_{i,j}^{(k)}, \beta_{i,j}^{(k)} \in \mathbb{F}_q$$

and $F^{(k)}$ has the block form

$$\begin{pmatrix} D_k & E_k \\ 0 & 0 \end{pmatrix}, D_k \in \mathbb{F}_q^{(v+d+o_1)\times(v+d+o_1)}, E_k \in \mathbb{F}_q^{(v+d+o_1)\times o_2}.$$

To find a solution $\mathbf{x}$ satisfying $\mathcal{F}(\mathbf{x}) = \mathbf{y}$, first choose the initial v vinegar variables $x_1, \ldots, x_v \xleftarrow{\$} \mathbb{F}_q$ uniformly at random. Solve the diagonal equations sequentially: for $1 \le i \le d$, obtain x_{v+i} from the known values $x_1, \ldots, x_{v+i-1}, y_i$ by solving the equation $f_i(x_1, \ldots, x_{v+i}) = y_i$ in one variable. Once $x_1, \ldots, x_{v+d}$ are fixed, solve the first oil layer, which has o_1 variables $x_{v+d+1}, \ldots, x_{v+d+o_1}$ and o_1 linear equations $f_{d+1}, \ldots, f_{d+o_1}$, using Gaussian elimination. The procedure may fail; in this case, restart by sampling $x_1, \ldots, x_v \xleftarrow{\$} \mathbb{F}_q$ again. Solve the second oil layer in the same way to obtain $\mathbf{x}$ satisfying $\mathcal{F}(\mathbf{x}) = \mathbf{y}$.

3.2 Key Generation

Key generation samples the central map $\mathcal{F}$ with the three-layer structure described above and two invertible affine maps

$$\mathcal{T}(\mathbf{x}) = T\mathbf{x} + \mathbf{b}, \qquad \mathcal{S}(\mathbf{y}) = S\mathbf{y} + \mathbf{a},$$

where $\mathbf{b} \in \mathbb{F}_q^n$ and $\mathbf{a} \in \mathbb{F}_q^m$ are sampled uniformly at random. The secret key is $(\mathcal{F}, \mathcal{T}, \mathcal{S})$, and the public key consists of the coefficients of

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

For efficient key generation, the linear parts are chosen to be block upper-triangular matrices:

$$T = \begin{bmatrix} I_v & T_1 & T_2 & T_3 \\ 0 & I_d & T_4 & T_5 \\ 0 & 0 & I_{o_1} & T_6 \\ 0 & 0 & 0 & I_{o_2} \end{bmatrix}, \qquad S = \begin{bmatrix} I_d & S_1' & S_2' \\ 0 & I_{o_1} & S_3' \\ 0 & 0 & I_{o_2} \end{bmatrix}.$$

The block sizes are (v, d, o_1, o_2) for T and (d, o_1, o_2) for S. All entries in the off-diagonal blocks are sampled independently and uniformly from $\mathbb{F}_q$. The identity diagonal blocks ensure $\det(T) = \det(S) = 1$, so both inverses can be computed by block back-substitution.

3.3 Structure of VDOO

The layered structure of VDOO can be expressed by nested subspaces of $\mathbb{F}_q^n$ and $\mathbb{F}_q^m$. We first work in the central coordinates, with input blocks $(\mathbf{r}, \mathbf{s}, \mathbf{a}, \mathbf{b})$ and output blocks of sizes (d, o_1, o_2). Define

$$\mathcal{O}_2 := \{(0,0,0,\mathbf{b})^\top\} \subseteq \mathcal{O}_1 := \{(0,0,\mathbf{a},\mathbf{b})^\top\} \subset \mathbb{F}_q^n,$$
$$W_2 := \{(0,0,\mathbf{y}_2)^\top\} \subseteq W_1 := \{(0,\mathbf{y}_1,\mathbf{y}_2)^\top\} \subset \mathbb{F}_q^m.$$

Here the free blocks range over their corresponding coordinate spaces. Thus $\dim \mathcal{O}_1 = \dim W_1 = o_1 + o_2$ and $\dim \mathcal{O}_2 = \dim W_2 = o_2$. Let

$$\mathcal{F}'(\mathbf{x}, \mathbf{y}) = \mathcal{F}(\mathbf{x}+\mathbf{y}) - \mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{y})$$

be the bilinear polar map. The two oil layers satisfy

$$\begin{aligned} \mathcal{F}(\mathcal{O}_1) \subseteq W_2, \qquad & \mathcal{F}(\mathcal{O}_2) = \{0\}, \\ \mathcal{F}'(\mathbb{F}_q^n, \mathcal{O}_1) \subseteq W_1, \qquad & \mathcal{F}'(\mathbb{F}_q^n, \mathcal{O}_2) \subseteq W_2. \end{aligned}$$

The following diagram shows both the restrictions of $\mathcal{F}$ and, for every fixed $\mathbf{x} \in \mathbb{F}_q^n$, the polar maps $\mathcal{F}'(\mathbf{x}, -)$. The horizontal arrows are inclusions; the arrows labelled by $\mathcal{F}$ and its restrictions commute with these inclusions. The dashed arrow shows the polar-map inclusion separately from the commuting solid arrows.

$$\begin{array}{ccccccc} \mathcal{O}_2 & \hookrightarrow & \mathcal{O}_1 & & \hookrightarrow & & \mathbb{F}_q^n \\ \downarrow{\scriptstyle 0} & \swarrow_{\mathcal{F}'(\mathbf{x},-)} & \downarrow{\scriptstyle \mathcal{F}|_{\mathcal{O}_1}} & \swarrow_{\mathcal{F}'(\mathbf{x},-)} & & & \downarrow{\scriptstyle \mathcal{F}} \\ \{0\} & \hookrightarrow & W_2 & & \hookrightarrow & W_1 & \hookrightarrow \mathbb{F}_q^m . \end{array}$$

The diagonal layer refines these relations into a flag. For $1 \le i \le d$, set

$$\begin{aligned} D_i &= \{\mathbf{x} \in \mathbb{F}_q^n : x_1 = \cdots = x_{v+i-1} = 0\}, \\ Z_i &= \{\mathbf{y} \in \mathbb{F}_q^m : y_1 = \cdots = y_{i-1} = 0\}. \end{aligned}$$

Also set $D_{d+1} = \mathcal{O}_1$ and $Z_{d+1} = W_1$. The full flag is summarized below. The solid vertical arrows are restrictions of $\mathcal{F}$.

$$\begin{array}{ccccccccc} \mathcal{O}_2 & \hookrightarrow & \mathcal{O}_1 & \hookrightarrow & D_d & \hookrightarrow \cdots \hookrightarrow & D_1 & \hookrightarrow & \mathbb{F}_q^n \\ \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \mathcal{F}} & & \downarrow{\scriptstyle \mathcal{F}} & & \downarrow{\scriptstyle \mathcal{F}} & & \downarrow{\scriptstyle \mathcal{F}} \\ \{0\} & \hookrightarrow & W_2 & \hookrightarrow & W_1 & \hookrightarrow \cdots \hookrightarrow & Z_2 & \hookrightarrow & Z_1 = \mathbb{F}_q^m . \end{array}$$

Here $\mathcal{O}_1 = D_{d+1}$ and $W_1 = Z_{d+1}$. For each $1 \le i \le d$ and every fixed $\mathbf{x} \in \mathbb{F}_q^n$, the individual diagonal step has the following form. The dashed arrows show the polar-map relations:

$$\begin{array}{ccccc} D_i & & \hookrightarrow & & \mathbb{F}_q^n \\ \downarrow{\scriptstyle \mathcal{F}|_{D_i}} & \swarrow_{\mathcal{F}'(\mathbf{x},-)} & & & \downarrow{\scriptstyle \mathcal{F}} \\ Z_{i+1} & \hookrightarrow & Z_i & \hookrightarrow & \mathbb{F}_q^m . \end{array}$$

Each successive diagonal quotient D_i/D_{i+1} and Z_i/Z_{i+1} is one-dimensional, and

$$\mathcal{F}(D_i) \subseteq Z_{i+1}, \qquad \mathcal{F}'(\mathbb{F}_q^n, D_i) \subseteq Z_i \quad (1 \le i \le d).$$

Indeed, on D_i the first i central polynomials vanish, while their polar forms with an arbitrary input vanish in the first $i-1$ output coordinates.

To pass to public coordinates, let $\mathcal{P}_2$ denote the homogeneous quadratic part of $\mathcal{P}$. Then with invertible transform S and T it has

$$\mathcal{P}_2(\mathbf{x}) = S\mathcal{F}(T\,\mathbf{x}).$$

Every input subspace $U \subseteq \mathbb{F}_q^n$ above becomes $T^{-1}U$, and every output subspace $W \subseteq \mathbb{F}_q^m$ becomes SW. All the stated inclusions and mapping relations therefore hold for $\mathcal{P}_2$ and its polar map with these transformed subspaces. This gives a coordinate-independent description of the hidden VDOO flag.

Remark 3.1. 1. VDOO(q, v, d, o_1, o_2) has a $(d+2)$-layer oil-and-vinegar structure with layer sizes $(\underbrace{1, \ldots, 1}_{d \text{ layers}}, o_1, o_2)$. Each diagonal layer contributes one new oil variable and one equation; the last two layers contribute o_1 and o_2 oil variables and equations, respectively. Thus there are $m = d+o_1+o_2$ equations in total. The layer sizes are the dimensions of successive quotients in the input flag, rather than the dimensions of the nested subspaces themselves. In this sense, VDOO is a structured multilayer Rainbow-type construction.

2. If only the last oil space $\mathcal{O}_2$ is retained, the homogeneous quadratic public map satisfies $\mathcal{P}_2(T^{-1}\mathcal{O}_2) = \{0\}$ with $\dim \mathcal{O}_2 = o_2$. Hence VDOO defines a structured UOV(n, o_2, m, q) instance, where the parameters denote the number of variables, the oil-space dimension, the number of equations, and the field size. In central coordinates, the first $n - o_2 = v + d + o_1$ variables act as vinegar variables. This is the generalized UOV setting with m equations; here $m = d + o_1 + o_2 > o_2$, whereas standard UOV signing uses $m = o_2$. The finer VDOO flag supplies additional structure.

4 Attack

In this section, we review the wedge attack. As a result, we can apply it to analyze the security of VDOO if we regard it as a UOV instance with a hidden oil space.

4.1 Wedge Attack

Ran introduced the wedge attack against UOV(n, o, m, q) in [15]. Furue and Ikematsu [5] subsequently extended this approach to p^ℓ-truncated polynomial algebras and incorporated it into the intersection attack on UOV. They consider the Macaulay matrix of the public equations over the p^ℓ-truncated ring $\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \cdots, x_n^{p^\ell} \rangle$. Their recovery criterion compares the dimension

of the Macaulay-matrix kernel with that of the subspace induced by the oil space. Define

$$h(z) = \frac{1 - z^{p^\ell}}{1 - z}.$$

Note that the Hilbert series of the p^ℓ-truncated ring

$$\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \cdots, x_n^{p^\ell} \rangle$$

is

$$H(z) = h(z)^n = (1 + z + \cdots + z^{p^\ell - 1})^n.$$

Under the assumption that the public quadratic polynomials $p_1, \cdots, p_m$ are semi-regular in the p^ℓ-truncated ring, the Hilbert series of the quotient ring

$$\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \cdots, x_n^{p^\ell}, p_1, \cdots, p_m \rangle$$

is

$$H_1(z) = \Big[\frac{h(z)^n}{h(z^2)^m}\Big]_+ = \Big[\frac{(1 + z + \cdots + z^{p^\ell - 1})^n}{(1 + z^2 + \cdots + z^{2(p^\ell - 1)})^m}\Big]_+,$$

Here $[\cdot]_+$ denotes truncation at the first nonpositive coefficient: that coefficient and all subsequent coefficients are set to zero.

Define

$$T(n, p^\ell, d) = [H(z)]_d, \quad T_1(n, m, p^\ell, d) = [H_1(z)]_d,$$

where $[\cdot]_d$ denotes the coefficient of z^d in the series expansion of the corresponding Hilbert series.

Define

$$D := \min\{2 \le d \le o(p^\ell - 1) : \ T_1(n, m, p^\ell, d) \le T(o, p^\ell, d)\}.$$

The complexity is estimated by

$$\mathrm{Comp}_{\mathrm{Wedge}}(n, o, m, \ell) = 3 \cdot \binom{n+1}{2} \cdot (T(n, p^\ell, D) - T(o, p^\ell, D) + 1)^2$$

field multiplications. In the following estimates, k denotes the codimension of a generic linear subspace to which we restrict the input. For a UOV(n, o, m, q) instance with $0 \le k < o$, this yields a UOV$(n - k, o - k, m, q)$ instance.

– **Wedge-reconciliation.** The reconciliation attack uses a UOV(n, o, m, q) instance. Its estimated complexity is

$$\min_{1 \le \ell \le e, 0 \le k < o} \mathrm{Comp}_{\mathrm{Wedge}}(n - k, o - k, m, \ell),$$

where e is the integer such that $q = p^e$.

– **Wedge-intersection.** We distinguish two cases. For $n < 3o$, the resulting problem is a UOV$(n, 3o-n, 3m-2, q)$ instance, with estimated complexity

$$\min_{1\le \ell \le e, 0 \le k < 3o-n} \mathrm{Comp}_{\mathrm{Wedge}}(n-k, 3o-n-k, 3m-2, \ell).$$

When $n \ge 3o$, the resulting problem is a UOV$(n, 1, 3m-2, q)$ instance with probability q^{3o-n-1}. The estimated complexity is

$$q^{n+1-3o} \cdot \mathrm{Comp}_{\mathrm{Wedge}}(n, 1, 3m-2, \ell).$$

To convert the above costs from field multiplications to gate counts, we use

$$\#\,\text{gates} = \#\,\text{field multiplications} \cdot \left(2 \cdot (\log_2 q)^2 + \log_2 q\right).$$

4.2 Application to VDOO

By Remark 3.1, retaining the last oil space identifies VDOO(q, v, d, o_1, o_2) with a generalized UOV(n, o_2, m, q) instance, where

$$n = v + d + o_1 + o_2, \qquad m = d + o_1 + o_2.$$

We apply the wedge-attack framework described above to estimate the cost of recovering the hidden input space $\widehat{\mathcal{O}}_2 := T^{-1}\mathcal{O}_2$; see [5] for the underlying framework. This step uses only the generalized UOV structure and does not exploit the finer VDOO flag.

Once $\widehat{\mathcal{O}}_2$ is known, form the output subspace

$$\widehat{W}_2 := \mathrm{span}_{\mathbb{F}_q} \mathcal{P}'_2(\mathbb{F}_q^n, \widehat{\mathcal{O}}_2) \subseteq SW_2.$$

Since the polar map is bilinear, this span can be computed by evaluating it on basis vectors of $\mathbb{F}_q^n$ and $\widehat{\mathcal{O}}_2$. If $\dim \widehat{W}_2 = o_2$, the inclusion is an equality, and the corresponding hidden output space SW_2 is recovered by linear algebra. For the round-one parameter sets, $\dim \widehat{\mathcal{O}}_2 = o_2$ is relatively large, providing many polar images from which to generate this output space. Under a generic-rank heuristic for the central-map coefficients, these images are expected to span SW_2, so the full-span condition is typically satisfied. Once $\widehat{\mathcal{O}}_2$ is known, this condition can be checked directly by computing the rank of the collected images.

Under this full-span condition, we can remove the last oil layer by passing to the input and output quotients $\mathbb{F}_q^n / \widehat{\mathcal{O}}_2$ and $\mathbb{F}_q^m / \widehat{W}_2$. In central coordinates, this amounts to discarding the last o_2 variables and output coordinates. The remaining central map is a $(d+1)$-layer Rainbow construction with layer sizes

$$(\underbrace{1, \ldots, 1}_{d \text{ layers}}, o_1),$$

with $n - o_2 = v + d + o_1$ variables and $m - o_2 = d + o_1$ equations.

For the round-one VDOO parameter sets specified in [1], the parameters of the residual Rainbow construction allow its trapdoor to be recovered in polynomial time. The subsequent reconstruction therefore contributes only polynomial overhead. Consequently, under the full-span condition above, the overall attack complexity is dominated by the wedge attack on the generalized UOV(n, o_2, m, q) instance. The corresponding estimates are reported in Table 1.

5 Conclusions and Future Work

We have provided a detailed explanation of the attack announced on the PQC Forum [14], evaluating wedge attacks [15, 5] against the NGCC submission parameter sets of VDOO [1]. The submission specification already considers the algebraic attacks developed against Rainbow. Table 1 compares our estimates with those reported in the specification.

The original VDOO parameters use two oil layers of similar size [6] but the NGCC parameters are much less balanced. Their simple-attack estimates meet the target security levels according to the specification [1]. However, the large final oil space in the 512-bit parameter set favors wedge attacks. Our estimates for this set fall below its claimed security level.

This imbalance also affects signing efficiency. For a fixed o_1+o_2, less balanced oil layers require more work in the two Gaussian eliminations. How to choose parameters that balance signing efficiency and security against simple, MinRank, and wedge attacks remains to be a question.

Our application of wedge attacks uses only the generalized UOV structure of VDOO, retaining its last oil space without exploiting the finer multilayer structure. Whether this additional structure can yield more effective wedge attacks or other attacks remains an open question for future work. More generally, VDOO can be viewed as a $(d+2)$-layer Rainbow-type construction, with layer sizes $(\underbrace{1,\ldots,1}_{d \text{ layers}}, o_1, o_2)$. Understanding how wedge attacks interact with this nested structure, and what this implies for the security of Rainbow constructions more broadly, is another direction that we intend to pursue.

Acknowledgments This work was supported by the National Key R&D Program of China (No. 2023YFC3305501) and the National Natural Science Foundation of China (Grant No. 126011023). We also thank Jintai Ding for helpful discussions.

AI disclosure In preparing this paper, we used GPT-6 to edit the text for clarity and grammar. The authors take full responsibility for the content and any errors that may remain.

Bibliography

[1] Adhikary, S., Bravo, C., Coscojuela-Escanilla, P., Ganguly, A., Karmakar, A., Kundu, S., Pal, D., Perret, L., Saxena, N.: VDOO: Vinegar diagonal oil oil. https://sites.google.com/view/vdoo-sign, specification v1.1

[2] Beullens, W.: Breaking rainbow takes a weekend on a laptop. In: Annual International Cryptology Conference. pp. 464–479. Springer (2022)

[3] Cartor, M., Cartor, R., Pierrottet, A.: Breaking the spell: Cryptanalysis of VDOO. Cryptology ePrint Archive, Paper 2026/2178 (2026), https://eprint.iacr.org/2026/2178

[4] Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: International conference on applied cryptography and network security. pp. 164–175. Springer (2005)

[5] Furue, H., Ikematsu, Y.: Key recovery attacks on UOV using p^ℓ-truncated polynomial rings. In: Heninger, N., Rosulek, M. (eds.) Advances in Cryptology – CRYPTO 2026. Lecture Notes in Computer Science, vol. 16803, pp. 289–318. Springer, Cham (2026). https://doi.org/10.1007/978-3-032-35398-6_10

[6] Ganguly, A., Karmakar, A., Saxena, N.: VDOO: A short, fast, post-quantum multivariate digital signature scheme. arXiv:2312.09535 (2023). https://doi.org/10.48550/arXiv.2312.09535

[7] Garey, M.R., Johnson, D.S.: Computers and intractability, vol. 174. freeman San Francisco (1979)

[8] Institute of Commercial Cryptography Standards: Announcement on launching the next-generation commercial cryptographic algorithms program (NGCC) (Feb 2025), https://www.niccs.org.cn/niccs/Notice/pc/content/content_1937428197396713472.html

[9] Institute of Commercial Cryptography Standards: Call for proposals for the next-generation public-key cryptographic algorithms (Oct 2025), https://www.niccs.org.cn/niccs/Notice/pc/content/content_1975896137741635584.html

[10] Institute of Commercial Cryptography Standards: NGCC: Public-key cryptographic algorithms, round 1 candidates (2026), https://www.niccs.org.cn/niccs/Round1Additional/pc/list.html

[11] Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 206–222. Springer (1999)

[12] National Institute of Standards and Technology: Call for additional digital signature schemes for the post-quantum cryptography standardization process. NIST Web Page (2022), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

[13] National Institute of Standards and Technology: Additional PQC digital signature candidates announced. https://csrc.nist.gov/News/2023/additional-pqc-digital-signature-candidates (2023)

[14] Public announcement of the attack on VDOO. PQC Forum discussion (2026), https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/LA5Z--9hCTU
[15] Ran, L.: Wedges, oil, and vinegar: An analysis of uov in the exterior algebra. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 363–388. Springer (2026)
[16] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)