Singular points of UOV and VOX

Pierre Pébereau

Singular points of UOV and VOX

Pierre Pébereau

Sorbonne Université, LIP6, CNRS
Thales SIX
pierre.pebereau@lip6.fr

Abstract. In this work, we study the singular locus of the varieties defined by the public keys of UOV and VOX, two multivariate signature schemes submitted to the additional NIST call for post-quantum signature schemes. We give a new attack for UOV$\hat{+}$ and VOX targeting singular points of the underlying UOV key. Our attack lowers the security of the schemes, both asymptotically and in number of gates, showing in particular that the parameter sets proposed for these schemes do not meet the NIST security requirements. More precisely, we show that the security of VOX/UOV$\hat{+}$ was overestimated by factors $2^2, 2^{18}, 2^{37}$ for security levels I, III, V respectively.
As an essential element of the attack on VOX, we introduce a polynomial time algorithm performing a key recovery from one vector, with an implementation requiring only 15 seconds at security level V.

Keywords: Multivariate cryptography · Cryptanalysis · Singular points · Bihomogeneous polynomial system

1 Introduction

Unbalanced Oil and Vinegar (UOV) is a multivariate signature scheme introduced in 1999 by Kipnis, Patarin and Goubin [21] to counter the Kipnis-Shamir attack [22] on the Oil and Vinegar signature scheme [27]. Since then, UOV has suffered no major attack and has been used as a basis for many multivariate signature schemes. The design is straightforward: the public key is a quadratic homogeneous polynomial system of m equations in $n > 2m$ variables over a finite field $\mathbb{F}_q$, and the secret key is an $m-$dimensional linear subspace of $\mathbb{F}_q^n$ that cancels the public key.

There is a strong belief that polynomial system solving remains a hard task for quantum computers, and this motivated the submission of UOV-based schemes to post-quantum standardisation contests. Among them, the NIST competition for post-quantum cryptography has garnered the most attention from the cryptographic community. Many multivariate signature schemes were submitted, in particular Rainbow [13] was a finalist in the third round. The cryptanalysis of Rainbow [5] renewed the interest in UOV and its variants, and among the 10 multivariate schemes submitted to the additional signature round, 7 are closely related to UOV (either special cases or using modified UOV keys). These

submissions are MAYO [4], PROV [9], QR-UOV [19], SNOVA [34], TUOV [12], (plain) UOV [6] and VOX [10].

The main appeal of these schemes, compared with the NIST PQC standards based on lattices, is the significantly shorter signature size they achieve: at NIST security level I, UOV achieves signatures as short as 96 bytes, as opposed to Falcon requiring 666 bytes. The drawback of these schemes is the very large key size: at NIST security level I, a UOV public key requires at least 278 kilobytes where Falcon uses an 897 bytes public key. This is mitigated by considering additional structure. For instance, the MAYO submission achieves at the same security level a signature of 321 bytes for a key size of 1168 bytes.

We follow a geometric approach to study the security of these schemes. In particular, we study the existence of *singular points* of the solution sets of the polynomial systems defined by the public key of UOV-based schemes. A singular point is a solution of the system at which the tangent space is too large. These points do not exist for random polynomial systems, therefore their existence yields attacks on these schemes.

Contributions and main results Denote $\mathbb{V}(I)$ the set of solutions of the polynomial system defined by a UOV public key $(p_1, \dots, p_m)$. We provide an algebraic variant of the Kipnis-Shamir attack described in [21] by studying the set of singular points of $\mathbb{V}(I)$. Our first result, Theorem 3.1, gives a lower bound on the dimension of the singular locus.

We also show that these are the only singular points of a generic (in the Zariski sense) UOV variety if the characteristic of the field is large enough in Theorem 3.2.

This has several consequences: we are able to identify some heuristics used in the Kipnis-Shamir attack, and our attacks do not suffer from the field size, as opposed to the Kipnis-Shamir attack which is enumerative by nature. In particular, the existence of singular points in the base field and an estimation of their number enables one to carry out the Kipnis-Shamir attack, whereas our attacks do not fail when there exists singular points only in a field extension.

We apply this work to UOV$\hat{+}$, a UOV variant which adds random quadratic equations to the public key. In Theorem 4.1, we prove that the $\hat{+}$ structure does not prevent the attacker from targeting the singular points of the underlying UOV key.

We provide a polynomial time algorithm recovering the full VOX private key from a single oil vector, generalizing a result of [28]. Combined with the dimension computation of Theorem 4.1, we obtain a key recovery attack against VOX/UOV$\hat{+}$ with an exponential coefficient smaller by a factor q^t in Theorem 4.3. We obtain cheaper attack costs than the estimates found in [16] and [10]. We propose alternative UOV$\hat{+}$ parameters defeating this attack.

We provide implementations of the attacks and experimental results with the code used to obtain them, to study the practical behavior of the different attacks and in particular compare the theoretical bounds with practical results on small instances.

Related work The Kipnis-Shamir attack [21] is an enumerative attack that repeatedly computes eigenvectors of some linear maps related to the public key of a UOV instance. It has been observed that this attack computes singular points in the intersection of two quadrics that share a large linear subspace. This observation is due to Luyten [24] in the context of Oil and Vinegar, and has been generalized to the case of UOV by Beullens and Castryck (private communication, July 2023). The difference in our approach is the focus on the properties of the singular locus, in particular its dimension, and proposing an alternative algebraic modeling of this computation.

VOX is a signature scheme based on UOV$\hat{+}$ and utilizing the QR structure introduced by [19]. The QR transform consists in using block matrices in the key pair. Each block, of size $\ell \times \ell$, represents an element of a field extension of degree ℓ, allowing for smaller public keys but introducing a new security assumption. Based on [18], Furue and Ikematsu attacked the parameters of the QR transform used in VOX. In response, alternative parameters were suggested for VOX [25], but the QR transform used in this case was shown to be insecure by Guo and Ding [20].

Neither of these attacks targeted the UOV$\hat{+}$ scheme. In contrast, we show that the unstructured security assumption, namely the security of the UOV$\hat{+}$ scheme, is overestimated by the VOX specification.

Organisation of the paper In Section 2, we define the UOV signature scheme and recall some classical results. In Section 3, we prove the non-vacuity of the singular locus of the UOV variety, and give the dimension of its intersection with $\mathcal{O}$. We then exploit this structure to introduce key recovery attacks against UOV. In Section 4, we apply the results of the previous sections to introduce key recovery attacks against UOV$\hat{+}$ bypassing the $\hat{+}$ structure. To obtain a full key recovery attack, we generalize the key recovery from one vector of [28] to the case of UOV$\hat{+}$. These results directly apply to VOX. In Section 5, we present experimental results supporting the theory presented throughout the paper.

2 Preliminaries

2.1 Notations

Let $q = p^e$ for p prime and $e \in \mathbb{N}_{>0}$. Let $\mathbb{F}_q$ denote the finite field with q elements. The prime p is the characteristic of $\mathbb{F}_q$. Vectors are assumed to be column vectors and are denoted by bold letters: $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{o}, \ldots$. Matrices are denoted by capital letters, and transposition of a matrix is written A^T. For a matrix F_k, the coefficient at position i, j is noted $f_{i,j}^{(k)}$. The kernel of a matrix A is denoted by $\ker(A)$ and is a right kernel: $\boldsymbol{x} \in \ker(A) \iff A\boldsymbol{x} = 0$. Given a field $\mathbb{F}$ and an integer n, we denote by $\mathbb{F}[x_1, \ldots, x_n]$ or $\mathbb{F}[\boldsymbol{x}]$ the polynomial ring of $\mathbb{F}$ in n indeterminates. If I is an ideal of $\mathbb{F}[\boldsymbol{x}]$, the variety defined by this ideal is noted $\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}^n, \forall p \in I, p(\boldsymbol{x}) = 0\}$. The restriction of a function f to a set E is denoted by $f_{|E}$. The canonical basis of the vector space $\mathbb{F}_q^n$ is noted $(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$.

For a given monomial ordering $\prec$, the leading term of a polynomial p is noted $\mathsf{LT}_\prec(p)$.

2.2 Unbalanced Oil and Vinegar

A UOV key pair for parameters (n, m, q) is composed of a secret key $(A, \mathcal{F})$ and a public key $\mathcal{P}$, with:

- $A \in GL_n(\mathbb{F}_q)$ an invertible matrix,
- $\mathcal{F} = (F_1, \dots, F_m) \in \mathbb{F}_q^{(n\times n)m}$ with $f_{i,j}^{(k)} = 0$ for $1 \leq i, j, k \leq m$
- $\mathcal{P} = (P_1, \dots, P_m) := (A^T F_1 A, \dots, A^T F_m A)$.

These matrices represent homogeneous quadratic maps (there are no constant and linear terms). The corresponding quadratic maps are defined by:

$$\mathcal{F}(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{F}_q^n \mapsto (\boldsymbol{x}^T F_1 \boldsymbol{x}, \dots, \boldsymbol{x}^T F_m \boldsymbol{x}) \tag{1}$$

$$\mathcal{P}(\boldsymbol{x}) : \boldsymbol{x} \in \mathbb{F}_q^n \mapsto (\boldsymbol{x}^T P_1 \boldsymbol{x}, \dots, \boldsymbol{x}^T P_m \boldsymbol{x}) \tag{2}$$

$$\mathcal{P} = \mathcal{F} \circ A \tag{3}$$

Given a hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{F}_q^m$, a signature for a message $\mathcal{M}$ is a vector $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$\mathcal{P}(\boldsymbol{x}) = \mathcal{H}(\mathcal{M}) \in \mathbb{F}_q^m.$$

The idea was introduced by Patarin in [27] and the motivation was that the secret system $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{t}$ is linear in $x_1, \dots, x_m$:

$$\mathcal{F}(\boldsymbol{x}) = \boldsymbol{t} \iff \begin{cases} \boldsymbol{x}^T F_1 \boldsymbol{x} = t_1 \\ \quad \vdots \\ \boldsymbol{x}^T F_m \boldsymbol{x} = t_m \end{cases} \tag{4}$$

The $x_1, \dots, x_m$ variables are distinguished from the other variables and are named "oil variables". The variables $x_{m+1}, \dots, x_n$ are "vinegar variables". The knowledge of A allows the signer to efficiently solve $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}$ using this property. Define the ideal generated by the public key $I = \langle p_1, \dots, p_m \rangle$. The set of accepted signatures for a message $\boldsymbol{t} \in \mathbb{F}_q^m$ is the set of $\mathbb{F}_q-$rational points of an algebraic variety of dimension $n - m$ generically. We distinguish the case $\boldsymbol{t} = (0, \dots, 0)$ and define the *UOV variety*

$$\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, \mathcal{P}(\boldsymbol{x}) = (0, \dots, 0)\}.$$

An insight from the cryptanalysis of Oil and Vinegar [22] and Rainbow [3] is the interest of having a geometric perspective on the equations defining the scheme. More precisely, these papers reformulate the UOV trapdoor in terms of subspaces, which yields a better understanding of the relationship between the public and private keys.

Let f be a quadratic form on a vector space $\mathbb{F}_q^n$. The *polar form* associated to f is $f^\star : (\boldsymbol{x}, \boldsymbol{y}) \mapsto f(\boldsymbol{x}+\boldsymbol{y}) - f(\boldsymbol{x}) - f(\boldsymbol{y})$. A subspace $V \subset \mathbb{F}_q^n$ is *totally isotropic* for f if for all $\boldsymbol{x} \in V, f(\boldsymbol{x}) = 0$. The secret key of UOV may be characterized in terms of isotropic subspaces:

Lemma 2.1. *The linear subspace $\mathcal{O}$ is a totally isotropic subspace of a quadratic form f if and only if for all $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, f^\star(\boldsymbol{x}, \boldsymbol{y}) = 0$.*

Let $(\boldsymbol{o}_1, \ldots, \boldsymbol{o}_m)$ be a basis of $\mathcal{O}$, a totally isotropic subspace of f. Complete $(\boldsymbol{o}_1, \ldots, \boldsymbol{o}_m)$ into a basis of $\mathbb{F}_q^n$ denoted B. Then a symmetric matrix[1] representing f in basis B has the secret UOV shape:

$$\mathsf{Mat}_B(f) = \begin{pmatrix} 0 & F^{(1)} \\ F^{(2)} & F^{(3)} \end{pmatrix}.$$

This shows that the secret key of UOV is a totally isotropic subspace $\mathcal{O}$ of dimension m shared by each of the public key quadratic forms. Therefore:

$$\mathcal{O} \subset \mathbb{V}(I).$$

This observation is due to Kipnis and Shamir in their attack against OV in 1998 [22], and this secret subspace was called "oil space".

2.3 Cryptanalysis of UOV and its variants

Consider an instance of UOV with parameters (q, n, m) with a public key $\mathcal{P}$.

The Kipnis-Shamir attack [21, 22] The Kipnis-Shamir attack on Oil and Vinegar [22, Theorem 7] is a polynomial time algorithm (polynomial in n and $\log(q)$) retrieving a basis of $\mathcal{O}$ when $n = 2m$. It motivated the "unbalanced" property of UOV introduced in [21]. The attack has been generalized to UOV by [21, Theorem 4.2], in which case it is no longer polynomial. We detail the attack on UOV below.

Let $(\alpha_i)_{1 \leq i \leq m-1} \in \mathbb{F}_q^{m-1}$ and define $M = \sum_{i=1}^{m-1} \alpha_i P_i$. Then $P_m^{-1} M$ has an invariant subspace included in $\mathcal{O}$ with probability greater than $p = \frac{q^{3m-n}-1}{q^m-1}$. The attacks consists in computing eigenvectors using the characteristic polynomial of M. It is computed in time $O(n^\omega)$ and factored in time $O(n \log(n))$ Therefore, after an expected q^{n-2m} draws of eigenvectors of such linear maps, each with a cost n^ω, an attacker expects to have found a vector in $\mathcal{O}$.

Key recovery from one vector [1, 3, 14, 28] Once one or more vectors of the secret key have been obtained, one obtains linear equations characterizing the remaining vectors. This is the reconciliation attack [3, 14], and it yields a polynomial time key recovery from two vectors by solving a linear system.

In fact, one vector suffices for this task with the following observation:

$$\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset \ker \begin{pmatrix} \boldsymbol{x}^T (P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T (P_m + P_m^T) \end{pmatrix}.$$

[1] If the matrix is not symmetric, then the block of zeros is replaced by any skew-symmetric matrix

This kernel has dimension $n-m$ generically. Therefore, the restriction of the UOV public key to this linear subspace is a UOV instance with fewer variables. If $n-m < 2m$, by [28, Lemma 2] the matrices composing the public key of this new UOV instance are singular. The kernels of these matrices are linear subspaces included in $\mathcal{O}$ that generically span $\mathcal{O}$.

3 Key recovery attack against UOV: Singular points

As seen in the previous section, finding one vector in the secret subspace $\mathcal{O}$ is enough to break UOV. This task is challenging, and motivates the search for distinguished points in $\mathcal{O}$. If such points exist, one may hope to compute them more efficiently than random points in $\mathcal{O}$. This section focuses on this question, proving that there exists a large number of singular points of the UOV variety in the secret subspace $\mathcal{O}$. This leads to new key recovery attacks on UOV.

3.1 Singular points of $\mathbb{V}(I)$

The goal of this subsection is to study the singular locus of the UOV variety, in particular its dimension. We start by defining singular points of an algebraic variety:

The main algebraic object we consider is the Jacobian matrix of a system of m equations in n variables defined by $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = (\frac{\partial p_i}{\partial x_j})_{1\leq i\leq m, 1\leq j\leq n}$.
Notice that for square matrices $P_1,\dots,P_m$, the Jacobian of the system $\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x},\dots,\boldsymbol{x}^T P_m \boldsymbol{x})$ has a simple description:

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \begin{pmatrix} \boldsymbol{x}^T(P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T(P_m + P_m^T) \end{pmatrix} \tag{5}$$

Definition 3.1. *Let $(p_1,\dots,p_m)$ be a collection of homogeneous polynomials over $\mathbb{K}[\boldsymbol{x}]$ defining a radical ideal $I = \langle p_1,\dots,p_m\rangle$. We say that $\boldsymbol{x} \in \mathbb{V}(I)\setminus\{0\}$ is a* singular point *of $\mathbb{V}(I)$ if the rank of the Jacobian matrix $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}]^{m\times n}$ is less than $\mathsf{codim}(I)$. The set of singular points of $\mathbb{V}(I)$ is noted $\mathsf{Sing}(\mathbb{V}(I))$.*

The singular locus is defined for the vanishing ideal $I(\mathbb{V}(I))$, therefore if the ideal I is not radical the polynomials $p_1,\dots,p_m$ must be chosen in $\sqrt{I}$. In the rest of the paper, we assume that $n > m$ and that the system $(p_1,\dots,p_m)$ forms a regular sequence, therefore $\mathsf{codim}(I) = m$. This is a natural assumption since the p_i are chosen uniformly at random among the quadrics that vanish on $\mathcal{O}$. In this case, a point $\boldsymbol{x}$ in the variety is singular if the Jacobian evaluated at $\boldsymbol{x}$ is not full rank. For generic polynomial systems, there are no singular points.

In the following theorem, we make a distinction between the values m and $o = \dim(\mathcal{O})$, even though they are equal for UOV. There are two reasons for this:

- There are schemes, such as MAYO [4] and PROV [9], based on the same core ideas as UOV but where $o \neq m$.
- This allows us to consider subsystems to compute singular points by leveraging the positive dimension of the full singular locus.

Theorem 3.1 (Homogeneous singularities)**.** *Let $p_1, \ldots, p_m$ be quadratic forms defining an ideal $I = \langle p_1, \ldots, p_m \rangle$ of $\mathbb{F}_q[x_1, \ldots, x_n]$ such that $\mathbb{V}(I)$ contains an $o-$dimensional linear subspace $\mathcal{O}$. Let $d = 2o+m-n-1$ and assume $n > m+o$.*

If $d \geq 0$, then the singular locus of $\mathbb{V}(I)$ is non-empty and its intersection with $\mathcal{O}$ has dimension at least d.

Proof. Let $\mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$. Let $B = (b_1, \ldots, b_n)$ be a basis of $\mathbb{F}_q^n$ such that $b_1, \ldots, b_o$ is a basis of $\mathcal{O}$. Let $\mathcal{F}(\boldsymbol{x}) = \mathcal{P}(B\boldsymbol{x})$. This system has the shape of a UOV secret key by Lemma 2.1: the equations depend linearly on $x_1, \ldots, x_o$. This implies that the partial derivatives with respect to any "oil" variable $1 \leq j \leq o$ are linear forms in the "vinegar" variables $x_{o+1}, \ldots, x_n$. Therefore, the Jacobian of the system has a special shape: $x_1, \ldots, x_o$ do not appear in the first o columns of the Jacobian. Thus, for all $\boldsymbol{x} \in \mathbb{F}_q^o \times \{0\}^{n-o}$ (an "oil vector"), we have:

$$\mathsf{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{matrix} 1 & \ldots & o & o+1 & \ldots & n \end{matrix} \\ \begin{bmatrix} 0 & \ldots & 0 & & & \\ \vdots & & \vdots & & J'(\boldsymbol{x}) & \\ 0 & \ldots & 0 & & & \end{bmatrix} \end{array} \begin{matrix} 1 \\ \vdots \\ m \end{matrix}$$

where $J'(\boldsymbol{x}) \in \mathbb{F}_q[x_1, \ldots, x_o]^{m \times (n-o)}$ with entries that are linear forms. Since $n > m$, notice that $\mathsf{Jac}_{\mathcal{F}}(\boldsymbol{x})$ is not full rank if and only if $J'(\boldsymbol{x})$ is not full rank since any minor containing one of the first o columns is zero. Thus, $\mathsf{Jac}_{\mathcal{F}}(\boldsymbol{x})$ is not full rank if and only if $\boldsymbol{x}$ lies in the variety of the determinantal ideal $\mathcal{J}_{m-1}$ generated by the $m-$minors of J'. As $n - o > m$, by [7, Theorem 2.1], this ideal has dimension at least $d = o - (n - o - (m-1))(m - (m-1))$ if $d \geq 0$, namely:

$$d = 2o + m - n - 1.$$

By the chain rule, there is a one-to-one mapping from singular points of the system $\mathcal{F}$ to singular points of the system $\mathcal{P}$:

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \mathsf{Jac}_{\mathcal{F}}(B^{-1}\boldsymbol{x})B^{-1}.$$

Therefore $\dim \mathsf{Sing}(\mathbb{V}(I)) \geq d$. □

By restricting to a subset of r equations from the public key, we may consider a zero-dimensional system:

$$2o + r - n - 1 \geq 0 \iff r \geq n - 2o + 1 \tag{6}$$

In particular, for $r_0 = n - 2o + 2$, the singular locus is expected to be (affine) 1-dimensional, enabling us to solve a 0-dimensional system after dehomogenizing (adding an affine constraint on the variables, such as $x_1 = 1$). In practice, the lower bound computed in Theorem 3.1 is achieved (see Section 5).

3.2 Generic smoothness

Smoothness - the absence of singularities - is a generic property of varieties in fields of characteristic 0 or sufficiently large [15, Corollary 16.23]. This fact also yields a tool to prove that for a generic UOV variety (informally, the variety of a key chosen uniformly at random), all the singularities are expected to lie in $\mathcal{O}$. The main caveat is that the field sizes used in practice are too small to hope to apply the results directly. Therefore, we will heuristically consider that the failure of the result in small characteristic will only yield low dimensional components of the singular locus, that will disappear when intersecting with generic hyperplanes.

The main ingredient is an algebraic version of Thom's weak transversality theorem due to Safey El Din and Schost [30, Proposition B.3], which itself relies on an algebraic version Sard's lemma. The methodology is to consider the coefficients in a UOV key (or more generally in a polynomial mapping) as indeterminates.

Let n, m, d be positive integers. Let $\mathbb{F}$ be a field of characteristic 0. Let $\boldsymbol{\Phi} : \mathbb{F}^n \times \mathbb{F}^d \to \mathbb{F}^m$ be a polynomial mapping. For $\theta \in \mathbb{F}^d$, denote by $\boldsymbol{\Phi}_\theta : \mathbb{F}^n \to \mathbb{F}^m$ the induced mapping $\boldsymbol{x} \mapsto \boldsymbol{\Phi}(\boldsymbol{x}, \theta)$. We say that $\boldsymbol{t} \in \mathbb{F}^m$ is a *regular value* of $\boldsymbol{\Phi}$ if $\boldsymbol{\Phi}$ is non-singular on $\boldsymbol{\Phi}^{-1}(\{\boldsymbol{t}\})$.

Thom's weak transversality theorem ([30, Proposition B.3]). *Let $\mathcal{S} \subset \mathbb{F}^n$ be a Zariski open set and suppose that 0 is a regular value of $\boldsymbol{\Phi}$ on $\mathcal{S} \times \mathbb{F}^d$. Then there exists a non-empty Zariski open set $\mathcal{U} \subset \mathbb{F}^d$ such that for all $\theta \in \mathcal{U}$, 0 is a regular value of $\boldsymbol{\Phi}_\theta$ on $\mathcal{S}$.*

We apply this to the case of UOV to prove that for a generic UOV key and a large enough field, the only singularities lie in $\mathcal{O}$. Notice here that we define the keys in $\mathbb{Q}$ instead of $\mathbb{F}_p$: this will allow us to apply the previous result since $\mathsf{char}(\mathbb{Q}) = 0$. We then obtain the result in $\mathbb{F}_p$ for p a sufficiently large prime by reducing the equations modulo p. In the rest of this section, we will assume that p is a prime.

Definition 3.2. *Let n, m, o be positive integers with $n \geq 2o$.*

Let $d = m\left(o(n-o) + \frac{(n-o)(n-o+1)}{2}\right)$. Let $O = [1, \ldots, o], V = [o+1, \ldots, n]$ the indices of oil (resp. vinegar) variables in the UOV secret key. Let $\boldsymbol{\Phi} : \mathbb{Q}^n \times \mathbb{Q}^d \to \mathbb{Q}^m$ induced by $\boldsymbol{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta}) \mapsto (\Phi_1(\boldsymbol{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta})), \ldots, \Phi_k(\boldsymbol{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta})))$ where for $1 \leq k \leq m$,

$$\Phi_k(\boldsymbol{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta})) = \sum_{i \in O, j \in V} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i \in V, j \in V} \beta_{i,j}^{(k)} x_i x_j \tag{7}$$

Let $\mathcal{O}_x = \mathbb{Q}^o \times \{0\}^{n-o}$. Let $\mathcal{S} = \mathbb{Q}^n \setminus \mathcal{O}_x$

Notice that if $F = (f_1, \ldots, f_m) \in \mathbb{F}_p^{m(n \times n)}$ is the secret quadratic map of a UOV key in a prime field $\mathbb{F}_p$, then there exists coefficients $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{Z}^d \subset \mathbb{Q}^d$, such that $F = \boldsymbol{\Phi}_\theta \bmod p$.

Theorem 3.2. *Using the notations of Definition 3.2, and for p large enough, there exists a non-empty Zariski open set $\mathcal{U} \subset \mathbb{F}_p^d$ such that for all $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathcal{U}$, 0 is a regular value of Φ_θ on $\mathbb{F}_p^n \setminus (\mathbb{F}_p^o \times \{0\}^{n-o})$.*

In other words, consider the set of all UOV keys in sufficiently large characteristic p. It admits a non-empty Zariski open set $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, the only singularities of $V = \{\boldsymbol{x} \in \mathbb{F}_p^n, \mathcal{P}(\boldsymbol{x}) = (0, \ldots, 0)\}$ belong to the corresponding oil space.

Proof. First, notice that $\mathcal{O}_x = \mathbb{Q}^o \times \{0\}^{n-o}$ is a Zariski closed set, therefore $\mathcal{S} = \mathbb{Q}^n \setminus \mathcal{O}_x$ is a Zariski open set.

Next, we prove that the Jacobian matrix $\mathsf{Jac}_\Phi(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ is full rank on $\mathcal{S} \times \mathbb{Q}^d$. To do so, we will prove that it contains an identity submatrix. Recall that

$$\mathsf{Jac}_\Phi(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \begin{bmatrix} \nabla(\Phi_1(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})) \\ \vdots \\ \nabla(\Phi_m(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})) \end{bmatrix} \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}]^{m \times (n+d)} \tag{8}$$

To ease the description, we decompose the indeterminates in smaller subsets.

Let $\boldsymbol{x}_O = (x_1, \ldots, x_o), \boldsymbol{x}_V = (x_{o+1}, \ldots, x_n)$. For all $1 \leq k \leq m$, let $\boldsymbol{\alpha}^{(k)} = (\alpha_{1,o+1}^{(k)}, \ldots, \alpha_{o,n}^{(k)})$ and $\boldsymbol{\beta}^{(k)} = (\beta_{o+1,o+1}^{(k)}, \ldots, \beta_{n,n}^{(k)})$.

We can detail the Jacobian matrix based on the definition of Φ in Equation (7). The partial derivatives with respect to the $\boldsymbol{x}$ variables are not relevant in this proof but are included for completeness. Let $1 \leq k \leq m$.

a) For $\ell \in O$, $\frac{\partial}{\partial x_\ell} \Phi_k =: L_k^{(1)}(\boldsymbol{x}_V, \boldsymbol{\alpha})$ does not depend on $\boldsymbol{x}_O$.
b) For $\ell \in V$, $\frac{\partial}{\partial x_\ell} \Phi_k = \sum_{i \in O} \alpha_{i,\ell}^{(k)} x_i + \sum_{i \in V, i \neq \ell} \beta_{i,l}^{(k)} x_i + 2\beta_{\ell,\ell}^{(k)} x_\ell =: L_k^{(2)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})$.
c) For $i, j \in O \times V$, we have $\frac{\partial}{\partial \alpha_{i,j}^{(k)}} \Phi_k = x_i x_j$.
d) If $\ell \neq k$ and $i, j \in O \times V$ then $\frac{\partial}{\partial \alpha_{i,j}^{(k)}} \Phi_\ell = 0$.
e) Similarly, for $i, j \in V \times V$, we have $\frac{\partial}{\partial \beta_{i,j}^{(k)}} \Phi_k = x_i x_j$.
f) For $\ell \neq k$ and $i, j \in V \times V$, $\frac{\partial}{\partial \beta_{i,j}^{(k)}} \Phi_\ell = 0$.

This is summarized in Equation (9):

$$\mathsf{Jac}_\Phi(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \begin{array}{c} \begin{matrix} \boldsymbol{x}_O & \boldsymbol{x}_V & \boldsymbol{\alpha}^{(1)} & \boldsymbol{\beta}^{(1)} & \ldots & \boldsymbol{\alpha}^{(m)} & \boldsymbol{\beta}^{(m)} \end{matrix} \\ \begin{bmatrix} L_1^{(1)}(\boldsymbol{x}_V, \boldsymbol{\alpha}) & L_1^{(2)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) & x_i x_j & x_i x_j & \ldots & 0 & 0 \\ \vdots & & & & & & \vdots \\ L_m^{(1)}(\boldsymbol{x}_V, \boldsymbol{\alpha}) & L_m^{(2)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) & 0 & 0 & \ldots & x_i x_j & x_i x_j \end{bmatrix} \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \end{array} \tag{9}$$

We now restrict $\boldsymbol{x}$ to $\mathcal{S} = \mathbb{Q}^n \setminus \mathcal{O}_x$. As $\boldsymbol{x} \notin \mathcal{O}_x$, there exists $i \in V$ such that $x_i \neq 0$. Therefore, for all $1 \leq k \leq m$, we have:

$$\frac{\partial}{\partial \beta_{i,i}^{(k)}} \Phi_k = x_i^2 \text{ and } \forall \ell \neq k, \frac{\partial}{\partial \beta_{i,i}^{(k)}} \Phi_\ell = \frac{\partial}{\partial \beta_{i,i}^{(\ell)}} \Phi_k = 0.$$

In other words, the following submatrix of $\mathsf{Jac}_{\Phi}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ is x_i^2 times the identity matrix:

$$\mathsf{Jac}_{\Phi}(\boldsymbol{\beta}_{i,i}) = \begin{bmatrix} \nabla_{\boldsymbol{\beta}_{i,i}} \Phi_1 \\ \nabla_{\boldsymbol{\beta}_{i,i}} \Phi_2 \\ \vdots \\ \nabla_{\boldsymbol{\beta}_{i,i}} \Phi_m \end{bmatrix} = \begin{array}{c} \begin{matrix} \beta_{i,i}^{(1)} & \beta_{i,i}^{(2)} & \dots & \beta_{i,i}^{(m)} \end{matrix} \\ \begin{bmatrix} x_i^2 & 0 & \dots & 0 \\ 0 & x_i^2 & \dots & 0 \\ & & \vdots & \\ 0 & 0 & \dots & x_i^2 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ \vdots \\ m \end{matrix} \end{array}.$$

Since $x_i \neq 0$, then $x_i^2 \cdot I_m$ is invertible, therefore $\mathsf{Jac}_{\Phi}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ is full rank, and therefore $0 \in \mathbb{Q}^m$ is a regular value of Φ on $\mathcal{S}$.

By Thom's weak transversality theorem [30, Proposition B.3], there exists a non-empty Zariski open set $\mathcal{U} \subset \mathbb{Q}^d$ such that for all $\theta \in \mathcal{U}$, 0 is a regular value of Φ_θ on $\mathcal{S}$.

By definition of a non-empty Zariski open set, there exists a non-zero ideal $I \subset \mathbb{Q}[\theta]$ such that

$$\mathcal{U} = \mathbb{Q}^d \setminus \mathbb{V}(I).$$

There exists a non-constant polynomial $u \in I$ since I is non-zero. Let D be the least common multiple of the denominators of the coefficients of u. Then $v = Du \in \mathbb{Z}[\theta]$. Since $u \neq 0 \in \mathbb{Q}[\theta]$ we have $v \neq 0 \in \mathbb{Z}[\theta]$. Let p_0 be a prime greater than the largest prime dividing D. Then, for all $p \geq p_0$, $v \neq 0 \bmod p$.

Let $p \geq p_0$. Define $\mathcal{U}_{\mathbb{F}_p}$, the complement of the Zariski closed set defined by the vanishing of $I_p = \{u \bmod p, u \in I\}$ which is an ideal of $\mathbb{F}_p[\theta]$:

$$\mathcal{U}_{\mathbb{F}_p} = \mathbb{F}_p^d \setminus \mathbb{V}(I_p).$$

Since $v \bmod p \neq 0$ and $v \in I_p$, then $I_p \neq \{0\}$. This yields:

$$\mathbb{V}(I_p) \neq \mathbb{F}_p^d.$$

Therefore, $\mathcal{U}_{\mathbb{F}_p}$ is a non-empty Zariski open set of $\mathbb{F}_p^d$. For all $\theta \in \mathcal{U}_{\mathbb{F}_p}$, 0 is a regular value of $\Phi_\theta \bmod p$ on $\mathcal{S} \bmod p$.

□

Notice that Theorem 3.2 also yields a proof that a generic polynomial map does not admit singularities. Since the field sizes in UOV are typically very small (around 2^8), this does not yield a proof for the practical parameter sets.

The heuristic expectation is that the cases of failures of the result (the existence of singularities outside of $\mathcal{O}$ in small characteristic) yield only low dimensional components of the singular locus, which therefore does not affect the computations described in the next sections of the paper. This is verified experimentally in Section 5 by computing Gröbner bases of the ideal of the singular locus for various parameter sets.

3.3 Gröbner bases of the singular locus

The original Kipnis-Shamir attack of [21] implicitly relied on two ingredients: the fact that all singular points are elements of $\mathcal{O}$, which generically holds for large

enough fields by Theorem 3.2, and the existence of $\mathbb{F}_q$-rational singular points, which are singular points that are defined over $\mathbb{F}_q$ as opposed to an extension of $\mathbb{F}_q$. This hypothesis allows us to perform an algebraic attack even in the absence of rational singular points.

Hypothesis 1 (Kipnis-Patarin-Goubin)**.** *Let* $\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, p_1(\boldsymbol{x}) = \ldots = p_m(\boldsymbol{x}) = 0\}$ *be the variety defined by a collection of quadrics with a common totally isotropic subspace* $\mathcal{O}$*. Then* $\mathsf{Sing}(\mathbb{V}(I)) \subset \mathcal{O}$*.*

Hypothesis 1 is used in [21, "How to find O?"] implicitly, as the invariant subspace H computed by the attack is one-dimensional, and one cannot use [21, Lemma 3] to distinguish lines in the variety from lines in $\mathcal{O}$. To apply [21, Lemma 3], one requires a two-dimensional subspace of $\mathbb{F}_q^n$ at least. The relationship between these invariant subspaces and singular points is clarified in Section 3.6.

Note however that if the hypothesis does not hold, the attack is not prevented, but it may return false positives. This does not significantly affect the complexity, as these can be efficiently recognized as such using a test "$\boldsymbol{x} \in \mathcal{O}$?" [1, 28].

As opposed to the Kipnis-Shamir approach, we obtain an attack without computing solutions of the system and only through a grevlex Gröbner basis computation.

Lemma 3.1. *Let* I *be a proper ideal of* $\mathbb{K}[\boldsymbol{x}]$*. Assume there exists linear polynomials in* I*, and let* $\prec$ *be a graded ordering.*

a) A Gröbner basis of I *with respect to* $\prec$ *contains at least one linear polynomial.*
b) If $\ell_1 \ldots, \ell_s$ *are the linear polynomials contained in a Gröbner basis with respect to* $\prec$*, then* $\bigcap_{1 \leq i \leq s} \mathbb{V}(\ell_i) = \bigcap_{f \in I, \deg(f)=1} \mathbb{V}(f)$*.*

Proof. a) Let $G = (g_1, \ldots, g_t)$ be a Gröbner basis of I with respect to $\prec$. Since I is proper, $G \neq (1)$. By definition of a Gröbner basis, for all $f \in I$, $\mathsf{LT}_\prec(f)$ must be divisible by the leading term of an element of G. The order $\prec$ is graded, therefore the degree of the leading term of a polynomial must be the total degree of this polynomial.

Let $f \in I$ be a linear polynomial. There exists $i \in [1, t]$ such that:

$$\mathsf{LT}_\prec(g_i) | \mathsf{LT}_\prec(f).$$

Since $\deg(\mathsf{LT}_\prec(f)) = 1$, $\mathsf{LT}_\prec(g_i)$ is of degree 1 and therefore g_i is of degree 1.

b) By *a)*, let $g_1, \ldots, g_s$ be the linear polynomials in a Gröbner basis $G = (g_1, \ldots, g_t)$ for I with respect to $\prec$ (assuming without loss of generality that they are indexed by $(1, \ldots, s)$). Let f be a linear polynomial in I. By definition of a Gröbner basis, $\mathsf{LT}_\prec(f)$ must be divisible by the leading term of an element of G. We have observed in *a)* that only a degree 1 polynomial in the Gröbner basis may perform this division, and the quotient of a linear polynomial by another linear polynomial is a constant polynomial (an element of the field).

This implies that every degree 1 polynomial in I can be written as a linear combination $f = \sum_{i=1}^{s} a_i g_i$ of the degree 1 elements of the Gröbner basis.

Therefore,

$$\bigcap_{1\leq i\leq s} \mathbb{V}(g_i) \subset \bigcap_{f\in I, \deg(f)=1} \mathbb{V}(f).$$

The reverse inclusion comes from the fact that for all $i \in [1, s]$, $g_i \in I$. Therefore, the subspaces $\bigcap_{1\leq i\leq s} \mathbb{V}(g_i)$ and $\bigcap_{f\in I, \deg(f)=1} \mathbb{V}(f)$ are equal. □

If the Gröbner basis is reduced, the same argument shows that the linear polynomials in the Gröbner basis must define distinct hyperplanes.

In the UOV case, using Theorem 3.2 or Hypothesis 1 combined with Lemma 3.1, one hopes to find exactly $n - o$ linear polynomials in a reduced grevlex Gröbner basis for the ideal defining $\mathsf{Sing}(\mathbb{V}(I))$. This behavior is observed in practice in Section 5. Note that a geometric property on a variety (here the singular locus) yields an algebraic property on the radical of the ideal defining it, therefore we make a (slightly weaker) statement that applies to the radical of the ideal defining the singular locus.

Let $\mathcal{P} \in \mathbb{F}_q[x_1, \ldots, x_n]^m$ be a set of m homogeneous quadratic equations vanishing on a proper $o-$dimensional linear subspace $\mathcal{O}$ with $d = 2o+m-n-1 > 0$ and let $I = \langle p_1, \ldots, p_m\rangle$. Let $H_1, \ldots, H_{d-1}$ be generic linear polynomials. We define an ideal that vanishes on a subset of the singular locus of $\mathbb{V}(I)$:

$$J = \langle p_1, \ldots, p_m\rangle + \langle \mathsf{Minors}_m(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))\rangle + \langle x_1 - 1, H_1(\boldsymbol{x}), \ldots, H_{d-1}(\boldsymbol{x})\rangle.$$

Note that by Theorem 3.1 J is zero-dimensional generically. We dehomogenize the system with $x_1 - 1$.

In the next result, we assume that when the conclusions of Theorem 3.2 do not hold (because of a small characteristic), then the singularities that lie outside of $\mathcal{O}$ form a low dimensional subvariety of the singular locus of a generic UOV key. This is a weaker assumption than $\mathsf{Sing}(\mathbb{V}(I)) \subset \mathcal{O}$.

Proposition 1. *Assume that* $\dim(\mathsf{Sing}(\mathbb{V}(I)) \setminus \mathcal{O}) < 2o - m - n - 1$. *Then a Gröbner basis of* $\sqrt{J}$ *with respect to a graded order contains linear polynomials, and the variety defined by these linear polynomials is a subspace of* $\mathcal{O}$.

Proof. First, notice that $\dim(\mathsf{Sing}(\mathbb{V}(I)) \setminus \mathcal{O}) < d \implies \mathbb{V}(J) \subset \mathcal{O}$. Indeed, $(\mathsf{Sing}(\mathbb{V}(I)) \setminus \mathcal{O}) \cap \mathbb{V}(H_1) \cap \ldots \cap \mathbb{V}(H_{d-1}) \cap \mathbb{V}(x_1 - 1) = \emptyset$ by definition of the dimension of a variety.

Since $\emptyset \subsetneq \mathcal{O} \subsetneq \mathbb{F}_q^n$, there exists a non-trivial linear polynomial h such that $\mathcal{O} \subset \mathbb{V}(h)$. Since $\mathbb{V}(J) \subset \mathcal{O}$, $\forall \boldsymbol{x} \in \mathbb{V}(J), h(\boldsymbol{x}) = 0$. By the Nullstellensatz [35, Theorem 14, p. 164], this implies $h \in \sqrt{J}$. By Lemma 3.1, this implies that a Gröbner basis of $\sqrt{J}$ with respect to a graded order contains linear polynomials, and the intersection of the varieties they define is a subspace of $\mathcal{O}$. □

Note that in experiments (Section 5) J was always found to be radical.

3.4 Modeling singularities

We use Theorem 3.1 to obtain key recovery attacks against UOV by computing a grevlex Gröbner basis for the ideal describing the singular locus of the variety defined by subsets of equations of the UOV public key. By Proposition 1 we expect such a Gröbner basis to contain linear polynomials that characterize $\mathcal{O}$ when the ideal is radical. In particular, one does not require the singular points to be $\mathbb{F}_q$-rational to complete the attack.

We consider two different modelings that are folklore, the minors modeling and a bihomogeneous modeling based on the "Lagrange multiplier" method as it is known in optimization (this is closely related to the Kipnis-Shamir approach to the MinRank problem). Both modelisations are highly structured (the former defines a determinantal ideal and the latter is bihomogeneous of bidegree (2,1)). Informally, the intuition is the following:

- **Minors modeling**: The Jacobian is not full rank if all its maximal minors vanish.
- **Lagrange multipliers**: The Jacobian is not full rank if there is a non-zero vector in its left-kernel.

In practice, we enforce the constraint $\boldsymbol{x} \neq \mathbf{0}$ by dehomogenizing the system using for instance the equation $x_1 - 1 = 0$.

Definition 3.3. *Let $\mathcal{P}(\boldsymbol{x})$ be a UOV system of m equations in n variables. We denote by $\mathsf{Jac}_{\mathcal{P},r}$ the Jacobian matrix of the system $\mathcal{P}(\boldsymbol{x})$ truncated to the first r lines.*

1. *Minors modeling:*

$$\mathcal{M}(\mathcal{P}, r) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{x} \neq \mathbf{0} \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathsf{Minors}_r(\mathsf{Jac}_{\mathcal{P},r}(\boldsymbol{x})) = 0 \end{cases} \tag{10}$$

2. *Bihomogeneous modeling:*

$$\mathcal{B}(\mathcal{P}, r) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^r, \boldsymbol{x} \neq \mathbf{0}, \boldsymbol{y} \neq \mathbf{0} \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P},r}(\boldsymbol{x}) = 0 \end{cases} \tag{11}$$

The solutions $\boldsymbol{x}$ of either of these systems, if any, are singular points of the variety defined by $\langle p_1, \ldots, p_m \rangle$ by construction.

In the case of Oil and Vinegar, Luyten [24] observed that solving the minors modeling system for $r = 2$ is a polynomial task in practice. However, the minors modeling does not scale well in the case of UOV, due to the cost of computing maximal minors (there are $\binom{n}{r}$ maximal minors). This is why we introduce the bihomogeneous system.

Equations (10) and (11) define the singular points of a subset of r equations from a UOV public key. The value chosen for r is the one such that the ideal $\langle p_1(\boldsymbol{x}), \ldots, p_r(\boldsymbol{x})\rangle + \langle \mathsf{Minors}_r(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))\rangle$ defines a one-dimensional variety by Theorem 3.1 and (6). By intersecting it with an arbitrary hyperplane to dehomogenize (for instance the one defined by $x_1 - 1$), we obtain a zero-dimensional variety.

Notice that a priori, Theorem 3.1 gives a bound on the dimension of the singular locus of the variety defined by a system of r UOV equations and some equations describing the rank defect of the Jacobian of these equations. Though, in (10) and (11), the quadratic equations include all m public key equations. This is because Theorem 3.1 gives the dimension of the intersection of the singular locus with the secret subspace $\mathcal{O}$: any point in this intersection is an element of $\mathcal{O}$, and it therefore cancels all the public key equations.

Even ignoring the large cost of computing the $\binom{n}{r}$ minors of degree r in the minors modeling case, the degree of regularity of the ideal suggests a slightly worse complexity than the bihomogeneous modeling. Therefore, we focus on the analysis of complexity results associated with the bihomogeneous modeling.

Note that any r lines of the Jacobian may be chosen to build $\mathsf{Jac}_{\mathcal{P},r}$, the choice of the first r ones is arbitrary.

3.5 Computing singular points using the bihomogeneous modeling

In this section, we are interested in the complexity of obtaining a grevlex Gröbner basis for the system described in Equation (11). The system is bihomogeneous and we rely on results presented first in [33], and their application to computer algebra in [17, 31] and in cryptography in [29].

Definition 3.4. *Let $\mathbb{K}$ be a field, let $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_m)$ be two sets of variables. Let p be a polynomial in $\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$. We say that p is bihomogeneous of bidegree (d_1, d_2) with respect to $\boldsymbol{x}, \boldsymbol{y}$ if*

$$\forall (\lambda, \mu) \in \overline{\mathbb{K}}^2, p(\lambda \boldsymbol{x}, \mu \boldsymbol{y}) = \lambda^{d_1} \mu^{d_2} p(\boldsymbol{x}, \boldsymbol{y}).$$

Recall that $\boldsymbol{y}$ is any non-zero element of the left kernel of the Jacobian evaluated on a singular point. This kernel must be of dimension at least one by definition of a singular point, and expected to be of dimension no greater than one if the formula for the dimension of the determinantal ideal $\mathcal{J}_{m-2}$ of the $m-1$ minors of the Jacobian from [7, Theorem 2.1] is negative. Thus, for each $\boldsymbol{x} \in \mathsf{Sing}(\mathbb{V}(I))$, there exists q choices of $\boldsymbol{y}$ in $(\mathbb{F}_q)^r$. We dehomogenize with $y_1 - 1 = 0$ to obtain a unique solution with high probability.

We may choose r such that the system $\mathcal{B}(\mathcal{P}, r)$ defines a 1-dimensional (affine) variety. We dehomogenize this system by adding the equation $x_1 - 1 = 0$ to the system, yielding a zero-dimensional system.

Ignoring for a moment the $m-r$ polynomials of the public key not involved in the Jacobian matrix, we still consider a zero-dimensional system:

$$\begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^r \\ P_1(\boldsymbol{x}) = \ldots = P_r(\boldsymbol{x}) = 0 \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P},r}(\boldsymbol{x}) = 0 \\ x_1 - 1 = 0 \end{cases}$$

Notice that the n Lagrange multiplier equations $\boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^n$ are bilinear of bidegree (1,1) and the "public equations" $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^m$ only involve $(x_1, \ldots, x_n)$ and therefore have bidegree (2,0).

Following [31, Lemma 7], under the assumption that this system forms a regular sequence, we obtain the following bivariate Hilbert series:

$$\frac{(1-t_1t_2)^n(1-t_1)(1-t_2)(1-t_1^2)^r}{(1-t_1)^{n+1}(1-t_2)^{r+1}}$$

We are interested in the first term with a non-positive coefficient of least total degree. Note that it is not clear that this approach can be extended to the overdetermined case, therefore we consider the zero-dimensional case as an upper bound.

$$O\left(\binom{n+r+d_{reg}}{d_{reg}}^{\omega}\right).$$

We give in Table 1 the estimated number of arithmetic operations required to solve the bihomogeneous system (11) using a generic Gröbner basis algorithm.

Parameter set (n, m, q)	uov-Is $(160, 64, 16)$	uov-Ip $(112, 44, 256)$	uov-III $(184, 72, 256)$	uov-V $(244, 96, 256)$
$\log_2$ ops	421	314	516	671

Table 1: Maximal degree in a grevlex Gröbner basis computation of singular points for UOV

This suggests that the approach is not competitive with the state of the art of key recovery attacks against UOV.

3.6 Revisiting the Kipnis-Shamir attack [22], [21]

In this section, we combine the dimension computation of Theorem 3.1 along with an estimate of the number of $\mathbb{F}_q$-rational singular points of the UOV variety to give a complexity estimate for an enumerative algorithm computing singular points, which turns out to be entirely equivalent to the Kipnis-Shamir attack [21].

Bihomogeneous modeling - $\boldsymbol{y}-$Enumeration. Consider a hybrid approach to the bihomogeneous system defined in Equation (11), where we enumerate over all possible values of $\boldsymbol{y}$. In this case, we have n linear equations in $\boldsymbol{x}$, having evaluated all the $\boldsymbol{y}$ variables in $\mathbb{F}_q$. Let us consider this case more carefully, by rewriting the modeling:

$$\exists \boldsymbol{x}, \boldsymbol{y}, \quad \begin{cases} \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \\ \mathcal{P}(\boldsymbol{x}) = 0 \end{cases} \iff \exists \boldsymbol{x}, \boldsymbol{y}, \quad \begin{cases} \left(\sum_{i=1}^{m} y_i (P_i + P_i^T) \right) \boldsymbol{x} = 0 \\ \mathcal{P}(\boldsymbol{x}) = 0 \end{cases} \tag{12}$$

Instead of using a Gröbner basis algorithm, observe that the linear equations entirely determine $\boldsymbol{x}$, and there are no $\boldsymbol{x}$ solutions to $\left(\sum_{i=1}^{m} y_i (P_i + P_i^T) \right) \boldsymbol{x} = 0$ unless the linear combination $\sum_{i=1}^{m} y_i (P_i + P_i^T)$ is singular. If $\boldsymbol{x}$ is a solution of the linear system, we check whether it is a solution of the quadratic system simply by evaluating $\mathcal{P}(\boldsymbol{x})$. Such a point will be singular for the system $\{p_1(\boldsymbol{x}), \dots, p_m(\boldsymbol{x})\}$ by (12).

Since the quadratic system is homogeneous, it does not matter which solution of the linear system we choose, as we expect only a dimension 1 kernel. Denote $M(\boldsymbol{y}) = \sum_{i=1}^{m} y_i (P_i + P_i^T)$.

Since the matrices are square, and the target rank is $n-1$, we may consider Equation (12) as a MinRank instance where the only equation is the determinant of the matrix $M(\boldsymbol{y})$. Guessing all the $\boldsymbol{y}$ variables is an enumerative method for this MinRank instance.

To estimate the complexity of this approach, we count the number of choices of $\boldsymbol{y}$ corresponding to singular points. To avoid counting the same vectors multiple times, we count projective points instead of affine ones. For each projective singular point $\boldsymbol{x}$, there exists a single projective point $\boldsymbol{y} \in \ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$ as the rank of the Jacobian is $n-1$. Let S be the number of projective rational singular points of the UOV variety. This yields S valid choices of $\boldsymbol{y}$ out of q^{m-1} possibilities (recall that we impose $y_1 = 0$).

Before estimating S, we focus on the cost of finding a valid value of $\boldsymbol{y}$: we can reduce the number of possible $\boldsymbol{y}$ to q^{m-2}.

We can improve the previous approach by noticing that we did not use the equation defined by the determinant of $M(\boldsymbol{y})$: we only checked whether it was vanished. If we only guess $m-2$ variables, then we can consider the determinant as a univariate polynomial in the remaining variable (for example, y_m). We may solve this univariate equation with a fast finite field algorithm [8] to find the values of y_m such that the determinant vanishes. Computing the determinant of a univariate matrix is a polynomial task with efficient algorithms in practice[1] [26]. To summarize, for each guess of the $m-2$ variables $(y_2, \dots, y_{m-1})$, we proceed as follows:

- Compute $M(y)$ a sum of m $n \times n$ matrices in $\mathbb{F}_q[y]_{\leq 1}$ (amortized[2]) $O(n^2)$

[1] Precomputing this determinant as a multivariate polynomial in $\boldsymbol{y}$ is not a good idea because of its very large size - even evaluating it will be costly with $\binom{n}{m-1}$ monomials.

[2] We avoid recomputing the full sum and instead update it at each step.

- Compute $\det(M(y))$, a determinant in $\mathbb{F}_q[y]$ $O(n^\omega)$
- Solve $\det(M(y)) = 0$ in $\mathbb{F}_q$. $O(n \log n)$
- For each of the ℓ roots, solve an $n \times n$ linear system $O(\ell n^\omega)$
- Check if any solution cancels the quadratic system (amortized[3]) $O(\ell n^2)$

The expected number of rational roots of a univariate polynomial in $\mathbb{F}_q$ is 1.

Assuming S is non-zero, the expected complexity of computing singular points enumeratively is:

$$C(n, m, q) = O\left(\frac{q^{m-2}}{S} n^\omega\right) \tag{13}$$

Kipnis-Shamir attack. The Kipnis-Shamir attack computes singular points in the intersection of two quadrics that share a large isotropic subspace. This observation is due to Luyten [24], and Beullens and Castryck (private communication, July 2023). We can derive the same result with the tools introduced earlier.

The Kipnis-Shamir attack studies the characteristic polynomial of the matrix $P_m^{-1}M$, where M is a random linear combination of public key matrices $M = \sum_{i=1}^{m-1} y_i P_i$. Using Coppersmith's trick [22, Remark above Definition 5.], the matrices P_i and $P_i + P_i^T$ both have the (U)OV property, namely that they are congruent to a matrix with an $m \times m$ block of zeros on the diagonal, with the same change of variables. This implies that we may replace P_i by $P_i + P_i^T$ in the attack, matching the formulation of (12).

Lemma 3.2. *For $1 \leq i \leq m$, let $P_i^\star = P_i + P_i^T$. Assume $P_m^\star$ is invertible.*

If $\boldsymbol{x}$ is an eigenvector of $(P_m^\star)^{-1} \sum_{i=1}^{m-1} y_i P_i^\star$, then $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})$ has a rank defect.

Proof. Let $M = \sum_{i=1}^{m-1} y_i P_i^\star$ and let χ be the characteristic polynomial of $(P_m^\star)^{-1}M$.

$$\chi(\lambda) = \det\left((P_m^\star)^{-1}M - \lambda I\right).$$

Therefore:

$$\det(P_m^\star) \cdot \chi(\lambda) = \det(M - \lambda P_m^\star) \tag{14}$$

In Equation (12), we solved $\det(M - \lambda P_m^\star)(y) = 0$ to compute y_m.

This shows that eigenvectors of $(P_m^\star)^{-1}M$ associated to an eigenvalue λ_0 induce a rank defect in $\mathsf{Jac}_{\mathcal{P}}$ by Equation (12), and an associated element of the left kernel of $\mathsf{Jac}_{\mathcal{P}}$ is $(y_1, \ldots, y_{m-1}, -\lambda_0)$. □

In particular, this shows that if an eigenvector of $(P_m^\star)^{-1}M$ lies in the variety $\mathbb{V}(I)$, then by Hypothesis 1, it must lie in $\mathcal{O}$.

To obtain the cost of the Kipnis-Shamir attack, the following heuristic is used in [21, Note above Theorem 4.2].

[3] Any solution that does not belong to $\mathcal{O}$ will vanish any indivual equation only with probability $1/q$, therefore it is on average sufficient to check $O(1)$ equations

Hypothesis 2. *Let $P_1, \dots, P_m$ be matrices from a UOV public key for parameters n, m, q. Among a collection of q^{n-2m} distinct linear maps of the form $P_j^{-1}M$, the expected number of eigenspaces of dimension 1 that lie in $\mathcal{O}$ is at least 1.*

Since each eigenspace included in $\mathcal{O}$ corresponds exactly to a single singular point of the variety, this result allows for an estimate of S. Another heuristic but more standard approach is the Lang-Weil bound [23, Lemma 1], which states that there are roughly q^d $\mathbb{F}_q$-rational points in a projective variety of dimension d. This yields $S \approx q^{\dim(\mathsf{Sing}(V(I)))-1} = q^{3m+n-2}$. In both cases, we obtain:

$$C(n, m, q) = O(q^{n-2m} n^\omega) \tag{15}$$

In conclusion, an enumerative approach to the computation of singular points provides an algebraic interpretation of the Kipnis-Shamir attack from [21]. Furthermore, we highlight a hypothesis (Hypothesis 1) used in the original Kipnis-Shamir attack of [21], and prove it generically in large enough fields. We reproduce the experiments of [21] in low dimension in a new algebraic framework.

4 Application to UOV$\hat{+}$ and VOX

4.1 Definition of UOV$\hat{+}$

VOX [10] is a signature scheme submitted to the first round of the NIST call for additional signatures. It relies on the same core principles as UOV, but adds random homogeneous quadratic equations to the public key. These equations are used to hide the structure of the UOV trapdoor in the form of "noise" by mixing them with the UOV public key equations. This is the "hat plus" (noted $\hat{+}$) transform [16]. This allows the signer to use smaller parameters at the cost of solving a polynomial system for each signature instead of a linear system. VOX also relies on an additional structure, the Quotient Ring (QR) transform [19], which is akin to the construction of structured lattices.

We dismiss the additional structure of the QR transform and work in the general case: we consider that the VOX secret matrices are dense and random instead of structured. This is equivalent to working directly on UOV$\hat{+}$ or Full-VOX (FOX, introduced in the same specification), by multiplying the parameters o, v by the "QR factor" c. Note that VOX uses prime fields with $q > 2$.

A UOV$\hat{+}$ key pair for parameters (q, o, v, t) is composed of a secret key $(S, A, \mathcal{F})$ and a public key $\mathcal{P}$, with:

- $A \in GL_{o+v}(\mathbb{F}_q)$
- $\mathcal{S} = \begin{pmatrix} I_t & S' \\ 0 & I_{o-t} \end{pmatrix}, \quad S' \in \mathbb{F}_q^{(o-t)\times t}, \mathcal{S} \in GL_o(\mathbb{F}_q)$
- $\mathcal{F} = (F_1, \dots, F_o) \in \mathbb{F}_q^{(n\times n)o}$ with $f_{i,j}^{(k)} = 0$ for $1 \le i, j \le o, t < k \le o$
- $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A$ a quadratic map

Let $n = o + v$ and let $\hat{\mathcal{F}} = (F_{t+1}, \dots, F_o)$ be the underlying UOV secret key. The (truncated) UOV key pair underlying the UOV$\hat{+}$ key is $(\hat{\mathcal{F}}, A), \hat{\mathcal{P}} = \hat{\mathcal{F}} \circ A$.

The polynomials $p_1, \ldots, p_t = f_1, \ldots, f_t$ are uniformly random (they are called "vinegar polynomials" in [10]) and they define the variety $V_t = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, p_1(\boldsymbol{x}) = \ldots = p_t(\boldsymbol{x}) = 0\}$ of dimension $n - t$. To avoid confusion with vinegar variables, we will refer to them as the random polynomials of the public key.

4.2 Singular points of the UOV$\hat{+}$ variety

We now apply the results of Section 3 to UOV$\hat{+}$. The core idea is to study, as previously done for UOV, how singular points of the secret key are mapped by the secret change of variables, and in turn deduce non-generic properties of the public key. In the case of UOV, all singular points of the secret key were mapped to singular points of the public key by the one-to-one map A.

In the case of UOV$\hat{+}$, the singular locus of the underlying UOV key is intersected by the variety defined by the random polynomials to obtain singular values of the public key. Still, singular values of the public system are elements of $\mathcal{O}$, the UOV secret of the UOV$\hat{+}$ key.

Theorem 4.1. *Let $\mathcal{P} = (p_1, \ldots, p_o)$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t), with $n > 2o$. Let $d = 3o - n - 2t - 1$.*
If $d \geq 0$, the UOV$\hat{+}$ variety $\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, p_1(\boldsymbol{x}) = \ldots = p_r(\boldsymbol{x}) = 0\}$ has a singular locus of dimension at least d.

Proof. Assume d is non-negative. Consider the underlying UOV public key defined by $\hat{\mathcal{P}}(\boldsymbol{x}) = \hat{\mathcal{F}} \circ A(\boldsymbol{x}) = (\hat{p}_{t+1}(\boldsymbol{x}), \ldots, \hat{p}_o(\boldsymbol{x}))$. By Theorem 3.1, it defines a variety $\mathbb{V}(\hat{I}) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, \hat{\mathcal{P}}(\boldsymbol{x}) = \boldsymbol{0}\}$ with a singular locus of dimension at least $d + t$. The UOV$\hat{+}$ variety $\mathbb{V}(I)$ is obtained by intersecting $\mathbb{V}(\hat{I})$ with t random quadric hypersurfaces defined by the equations $p_1(\boldsymbol{x}) = 0, \ldots, p_t(\boldsymbol{x}) = 0$.

The Jacobian of the system $\mathcal{P}'(\boldsymbol{x}) : (p_1 = 0, \ldots, p_t = 0, \hat{p}_{t+1} = 0, \ldots, \hat{p}_o = 0)$ contains the Jacobian of $\hat{\mathcal{P}}(\boldsymbol{x})$ as a submatrix. The UOV$\hat{+}$ public key is obtained by linear combination of equations from $\mathcal{P}'(\boldsymbol{x})$:

$$\mathcal{P}(\boldsymbol{x}) = \mathcal{S} \circ \mathcal{P}'(\boldsymbol{x}).$$

The chain rule implies that

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \mathcal{S} \cdot \mathsf{Jac}_{\mathcal{P}'}(\boldsymbol{x}).$$

Therefore, if $\boldsymbol{x} \in \mathbb{V}(I)$ is a singular point of $\mathbb{V}(\hat{I})$, then $\boldsymbol{x}$ must be a singular point of $\mathbb{V}(I)$. This implies that the singular locus of $\mathbb{V}(I)$ contains the intersection of the singular locus of $\mathbb{V}(\hat{I})$ with V_t, the variety defined by the random equations.

By [11, Chapter 9, Section 4, Theorem 3 (page 499)], this intersection has dimension at least d, which yields the result. □

The UOV$\hat{+}$ (and VOX) security estimates rely on the idea that one cannot attack the partial UOV key without first guessing the coefficients of the $\mathcal{S}$ map on at least two equations, therefore multiplying the cost of any attack on the partial key by a factor q^{2t}.

Theorem 4.1 shows that we can target the partial UOV key by computing singular points of the UOV$\hat{+}$ key without guessing $\mathcal{S}$, since the singular locus of the partial key intersects the variety V_t if d is non-negative. In light of Section 3.6, this proves that the Kipnis-Shamir attack directly works on the UOV$\hat{+}$ public key since it computes rational singular points of the variety generated by a collection of quadratic equations.

Applying once again the Lang-Weil bound [23, Lemma 1], we use Equation (13) to predict the cost of the Kipnis-Shamir attack interpreted as an enumerative singular point computation. We have $\dim \mathsf{Sing}\mathbb{V}(I) = 3o - n - 1 - 2t$. This yields the following expected cost for the Kipnis-Shamir attack against UOV$\hat{+}$:

$$C(q, n, o, t) = O\left(\frac{q^{o-1}}{|\mathsf{Sing}\mathbb{V}(I)|} n^\omega\right) = O(q^{n-2o+2t} n^\omega) \tag{16}$$

This cost is identical to the estimations in [16] and [10].

We propose in the next section to adapt the Kipnis-Shamir attack to the case of UOV$\hat{+}$ by computing the singular points of the underlying UOV key instead of those of the public key, improving the complexity by an exponential factor.

4.3 Key recovery from one vector against UOV$\hat{+}$

The main tool we need to adapt the Kipnis-Shamir attack to UOV$\hat{+}$ is an algorithm to distinguish elements of $\mathcal{O}$ from random elements of $\mathbb{F}_q^n$. In UOV, this task is much easier because elements of $\mathcal{O}$ cancel the public key polynomials.

A polynomial-time key recovery from one vector against UOV is introduced both in [1] and [28].

We focus on the second approach, which proceeds by studying the kernel of the Jacobian of the system evaluated on an element of the secret subspace $\mathcal{O}$. In [28, Section 4], these tools are applied to VOX, interpreted as UOV$\hat{+}$: the underlying UOV public key is targeted once the map $\mathcal{S}$ is inverted. Using t vectors of the UOV secret key, one inverts the map by solving a linear system. The author concludes that the method does not apply out of the box, and instead requires t vectors of $\mathcal{O}$ to break the scheme.

In this section, we show that [28, Theorem 7] may be generalized to UOV$\hat{+}$ without inverting $\mathcal{S}$, and thus show how to perform a key recovery against UOV$\hat{+}$ and VOX using a single oil vector. Furthermore, for fixed t and for $n - 2o = t$, the parameter regime chosen in VOX [10], we achieve a complexity polynomial in n and o.

The next lemma enables us to restrict a UOV$\hat{+}$ public key to a smaller subspace containing an unusually large intersection with the underlying UOV secret subspace $\mathcal{O}$.

Lemma 4.1. *Let $\mathcal{P} = (P_1, \dots, P_o)$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t), let $\mathcal{O}$ be the associated UOV secret subspace.*

If $\boldsymbol{x} \in \mathcal{O}$, then $\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \cap \mathcal{O}$ has dimension at least $o - t$ as a linear subspace.

Proof. Recall that

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \begin{pmatrix} \boldsymbol{x}^T(P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T(P_o + P_o^T) \end{pmatrix}.$$

Furthermore, by definition of $\mathcal{S}$ the chain rule yields:

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \mathcal{S} \cdot \mathsf{Jac}_{\hat{\mathcal{P}}}(\boldsymbol{x}) \tag{17}$$

Since $\mathcal{S}$ is injective, the right kernels of $\mathsf{Jac}_{\hat{\mathcal{P}}}(\boldsymbol{x})$ and $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})$ are equal. The observation of [28] is that

$$\mathcal{O} \subset \ker \begin{pmatrix} \boldsymbol{x}^T(\hat{P}_{t+1} + \hat{P}_{t+1}^T) \\ \vdots \\ \boldsymbol{x}^T(\hat{P}_o + P_o^T) \end{pmatrix}.$$

Notice that by Equation (17) we have:

$$\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) = \ker \begin{pmatrix} \boldsymbol{x}^T(P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T(P_t + P_t^T) \end{pmatrix} \cap \ker \begin{pmatrix} \boldsymbol{x}^T(\hat{P}_{t+1} + \hat{P}_{t+1}^T) \\ \vdots \\ \boldsymbol{x}^T(\hat{P}_o + \hat{P}_o^T) \end{pmatrix}.$$

Therefore in our case

$$\mathcal{O} \cap \ker \begin{pmatrix} \boldsymbol{x}^T(P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T(P_t + P_t^T) \end{pmatrix} \subset \ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})).$$

This intersection has dimension at least $o - t$ and is contained in $\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$, therefore

$$\dim\left(\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \cap \mathcal{O}\right) \geq o - t.$$

This concludes the proof. □

By genericity of $P_1, \ldots, P_t$, we expect this to be an equality, which is verified in practice. We obtain a key recovery from one vector by restricting the UOV$\hat{+}$ public key to this kernel, and by considering the properties of this new UOV$\hat{+}$ instance. In the parameters of the NIST submission, t is bounded by 8. In theory this value can be increased, but this could signficantly increase the time required to sign a message.

Theorem 4.2. *Let $\mathcal{P}$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t) with $t \leq 8$, let $\mathcal{O}$ be the associated UOV secret subspace, let $\boldsymbol{x} \in \mathcal{O}$ and assume $n = 2o + t$ and $3t + 1 < o$.*

There exists a probabilistic algorithm taking as input $\boldsymbol{x}$ and $\mathcal{P}$ and outputting a basis of $\mathcal{O}$, using $O\left(\binom{n-2o+2t+5}{4}^2 \binom{n-2o+2t+1}{2}\right)$ arithmetic operations in $\mathbb{F}_q$.

Proof. Notice that $\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$ has dimension $n-o$ for regular points, and dimension $n-o+1$ for singular points of the underlying UOV key. We assume the latter. Indeed, when $\boldsymbol{x}$ is not singular, the dimension of the kernel is smaller and the problem is easier to solve. Let B be a basis of $\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$.

Following [28], we restrict the UOV$\hat{+}$ public key to this kernel.

$$P_{i|B} := B^T \cdot P_i \cdot B \text{ for } 1 \leq i \leq o.$$

The collection $P_{|B} = (P_{1|B}, \ldots, P_{o|B})$ is a public key of a generalized[4] UOV$\hat{+}$ instance with the same number of equations o, in dimension $n' = n-o+1$, and with an UOV trapdoor of dimension $o-t$ by Lemma 4.1.

Let

$$\mathcal{O}' = \mathcal{O} \cap \ker \begin{pmatrix} \boldsymbol{x}^T(P_1 + P_1^T) \\ \vdots \\ \boldsymbol{x}^T(P_t + P_t^T) \end{pmatrix}$$

be the oil space associated to this key. Define the following ideals: $I = \langle P_{1|B}, \ldots, P_{o|B} \rangle$ and $I_t = \langle P_{1|B}, \ldots, P_{t|B} \rangle$.

Notice that if $\boldsymbol{x} \in \mathbb{V}(I_t)$ then $P_{1|B}(\boldsymbol{x}) = ... = P_{t|B}(\boldsymbol{x}) = 0$ by definition. Recall that $\hat{P}$ is the underlying truncated UOV public key: if $\boldsymbol{x} \in \mathcal{O}'$, then $\hat{P}_{t+1|B}(\boldsymbol{x}) = ... = \hat{P}_{o|B}(\boldsymbol{x}) = 0$. Finally, if $\boldsymbol{x} \in \mathcal{O}' \cap \mathbb{V}(I_t)$, for $t+1 \leq i \leq o$:

$$P_{i|B}(\boldsymbol{x}) = (S \circ F)_{i|B}(x) = \hat{P}_{i|B}(\boldsymbol{x}) + \sum_{1 \leq j \leq t} s_{i,j} P_{j|B}(\boldsymbol{x}) = 0.$$

Therefore $x \in \mathcal{O}' \cap \mathbb{V}(I_t)$ implies $\boldsymbol{x} \in \mathbb{V}(I)$:

$$\mathbb{V}(I_t) \cap \mathcal{O}' \subseteq \mathbb{V}(I).$$

Recall that $\dim(\mathcal{O}') = o-t$ therefore $\dim(\mathbb{V}(I_t) \cap \mathcal{O}') \geq o-t-t$ and therefore $\dim \mathbb{V}(I) \geq o-2t$. On the other hand, the expected dimension of a variety defined by a generic collection of o equations in $n-o+1$ variables is $n-2o+1 = t+1$. Therefore, if $n-2o+1 < o-2t$, then the variety $\mathbb{V}(I)$ is in general strictly larger if $\boldsymbol{x} \in \mathcal{O}$ than if $\boldsymbol{x} \notin \mathcal{O}$, as in the second case the system $\mathcal{P}_{|B}$ admits no UOV trapdoor.

This property yields a distinguisher by computing a grevlex Gröbner basis for the ideal $J = I + \langle h_1, \ldots, h_{o-2t} \rangle$, where $h_1, \ldots, h_{o-2t}$ are generic linear polynomials that we add to the system to reach dimension 0. As always, we dehomogenize the system by making sure that (at least) one of the h_i is inhomogeneous: for example, $h_1 = x_1 - 1$. Note that $\mathbb{V}(J) \subset \mathcal{O}'$. Therefore by Lemma 3.1, the grevlex Gröbner basis contains $o-2t$ (the number of h_i) $+ 2t$ (the number of hyperplanes defining $\mathcal{O}'$) $= o$ linear polynomials.

Notice that this system is (heavily) overdetermined as $n-2o+2t+1 = 3t+1 < o$: the number of variables[5] depends only on t, which is bounded by

[4] In the sense that the number of equations and the dimension of the oil-space differ.
[5] Each hyperplane eliminates one variable.

8. Assuming semi-regularity, the cost of the linear algebra step for computing a Gröbner basis is understood by studying the Hilbert series

$$H(z) = \frac{(1-z^2)^o}{(1-t)^{n-2o+2t+1}} = (1+t)^o(1-t)^{o-3t-1}.$$

The degree of regularity is the index of the first non-positive coefficient in this series (which is a polynomial). The coefficient of degree d of this series is a polynomial in o and t of degree at most d:

$$c_t^{(d)}(o) = \sum_{i=0}^{d} \binom{o-3t-1}{i}(-1)^i \binom{o}{d-i}(1)^{d-i}.$$

We study this coefficient case by case:

- For $d = 4$ and $t = 6$, this polynomial is negative for $o \in [44, 337]$.
- For $d = 3$ and $t = 6$, this polynomial is negative for $o \geq 70$
- For $d = 4$ and $t = 7$, this polynomial is negative for $o \in [57, 450]$.
- For $d = 3$ and $t = 7$, this polynomial is negative for $o \geq 92$
- For $d = 4$ and $t = 8$, this polynomial is negative for $o \in [71, 580]$.
- For $d = 3$ and $t = 8$, this polynomial is negative for $o \geq 117$.

The interest of this computation is two-fold:

1. For the parameters used in VOX, the degree of regularity is 4.
2. When o grows, the degree of regularity is less than 4 for fixed t.

We use the complexity estimate for solving a quadratic polynomial system in [10, Section 7.1]:

$$O\left(\binom{n_{vars}+d}{d}^2 \binom{n_{vars}}{2}\right) \tag{18}$$

Which yields the following upper bound on the number of arithmetic operations required for the computation of a grevlex Gröbner basis:

$$O\left(\binom{n-2o+2t+5}{4}^2 \binom{n-2o+2t+1}{2}\right) \tag{19}$$

This is a polynomial in n and o. To summarize, given $\boldsymbol{x}$, the algorithm computes a grevlex Gröbner basis for the ideal J, and returns the linear terms in the grevlex Gröbner basis if $\boldsymbol{x} \in \mathcal{O}$. If $\boldsymbol{x} \notin \mathcal{O}$, the ideal is $\langle 1 \rangle$ and the grevlex Gröbner basis is the singleton $\{1\}$.

To fully recover the key, one computes $\mathcal{O}'$ from the linear terms, and then solves a linear system for each equation to determine the coefficients of $\mathcal{S}$. Once $\mathcal{S}$ is known, the attacker performs a one vector key recovery attack against the underlying UOV key which is now known, using for example [28]. The cost of these last steps is $O(on^\omega)$, and is dominated by the Gröbner basis computation. □

Notice that this yields a test "$\boldsymbol{x} \in \mathcal{O}$?" with the same complexity by checking whether the Gröbner basis is different from $\{1\}$.

We verify experimentally the degree of regularity prediction and the complexity of the algorithm in Section 5.2.

4.4 Key recovery on VOX by computing underlying singular points

We combine the study of the singular points from Section 4.2 with the one vector key recovery from Section 4.3 and introduce a novel attack on UOV$\hat{+}$ and VOX.

The Kipnis-Shamir attack on UOV computes vectors that drop the rank of the Jacobian of a UOV public key among eigenvectors of some linear maps. For each such vector $\boldsymbol{x}$, it checks whether $\mathcal{P}(\boldsymbol{x}) = \mathbf{0}$, in which case the attacker concludes that they have computed a point of $\mathcal{O}$. For UOV$\hat{+}$ and VOX, a simple generalization of the attack computes singular points of the VOX public key with identical computations.

We proceed differently: for points that drop the rank of the Jacobian, instead of checking $\mathcal{P}(\boldsymbol{x}) = 0$, check "$\boldsymbol{x} \in \mathcal{O}$?" using Section 4.3. This means that we will compute points in the singular locus of the underlying UOV key which has dimension at least $d + t$ by (the proof of) Theorem 4.1.

Theorem 4.3 (Key recovery attack on VOX)**.** *Let $\mathcal{P}$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t). Let $n = o + v$ and assume $n = 2o + t$ and $3t + 1 < o$.*

There exists an algorithm computing an equivalent secret key for $\mathcal{P}$ using an expected number of arithmetic operations:

$$O\left(q^{n-2o+t}\binom{n-2o+2t-3}{4}^2\binom{n-2o+2t+1}{2}\right).$$

Proof. As seen in the proof of Theorem 4.1, the singular points of the underlying UOV key $\hat{\mathcal{P}}$ drop the rank of the Jacobian. Since the dimension of the singular locus of $\hat{\mathcal{P}}$ is $3o - t - n - 1$, following the methodology of Section 3.6, we expect to find an element of $\mathcal{O}$ among the points that drop the rank of the Jacobian after q^{n-2o+t} trials. With the notations of Section 3.6, each trial costs:

- Computing $\boldsymbol{x} \in \ker(P_o^{-1}M)$ $\qquad O(n^\omega)$
- Testing $\boldsymbol{x} \in \mathcal{O}$? using Theorem 4.2 $\qquad O\left(\binom{n-2o+2t-3}{4}^2\binom{n-2o+2t+1}{2}\right)$

The second step dominates the cost of each trial, yielding an expected number of arithmetic operations:

$$O\left(q^{n-2o+t}\binom{n-2o+2t-3}{4}^2\binom{n-2o+2t+1}{2}\right).$$

□

Following NIST methodology, we consider that one arithmetic operation requires $\log(q)^2 + 2\log(q)$ gates, which gives bit complexities for VOX in Figure 1.

$q, o \cdot c, v \cdot c, t$	Bit complexity	Previous [10]	Target
$251, 48, 54, 6$	**140**	142	143
$1021, 70, 77, 7$	**188**	206	207
$4093, 96, 104, 8$	**243**	280	272

Fig. 1: Complexity of the key recovery attack against VOX [10].

4.5 Defeating the attack

The attack presented in Theorem 4.3 is exponential, therefore patching the scheme is straightforward: increase any of the exponential quantities sufficiently to reach the security levels. The two main levers are t and $v = n - o$. The parameter t exponentially affects the signing time, therefore it cannot be significantly increased or it would make VOX dramatically slower than other signature schemes.

We focus on the second option: increasing the number of vinegar variables, while leaving o, q, t untouched. Theorem 4.2 achieves a polynomial complexity in n and $\log(q)$ when $n - 2o = O(1)$, but the degree of this polynomial is given by the cost of solving an overdetermined polynomial system:

$$O\left(\binom{n-2o+2t+1+d}{d}^2 \binom{n-2o+2t+1}{2}\right)$$

where d is the first non-positive index in the Hilbert series of the ideal:

$$H(z) = \frac{(1-z^2)^o}{(1-t)^{n-2o+2t+1}}.$$

By increasing v, we hit two birds with one stone in Theorem 4.3: we increase both the cost of enumeration q^{n-2o+t} and the cost of testing each candidate. Therefore, small increases in this parameter will yield a scheme that can withstand this attack. We give in Figure 2 a set of parameters defeating our attack.

We include the reduction in expanded public key size that these parameters achieve compared with plain UOV at a comparable security level: this is the main motivation to use VOX, as the compressed public key size only depends on m in UOV (see [6, Section 3.3, page 20]). The percentage is computed as $\frac{U-V}{U}$ where U (resp. V) is the expanded public key size in UOV (resp. in VOX).

Level	q, o, v, t	Complexity Th. 4.3 ($\log_2$)	epk (bytes)	epk gain vs UOV [6]
I	251, 48, 55, 6	148.8	177 566	36% / 57%
III	1021, 70, 79, 7	208.7	677 482	44%
V	4093, 96, 107, 8	279.8	2 066 429	28%

Fig. 2: Alternative VOX parameters defeating modified Kipnis-Shamir

5 Experimental results

We start with experimental computations of the dimension of Theorem 3.1, along with the property described in Lemma 3.1. Next, we present an implementation of the attacks of Section 4.3 and Section 4.4.

The degree of regularity and complexity claims of the algorithm of Theorem 4.2 are verified by the provided implementation. Based on this, the complexity of the algorithm in Theorem 4.3 depends on the expected number of trials before a vector in $\mathcal{O}$ is found. Checking this amounts to performing a Kipnis-Shamir attack on the underlying UOV key, and verifying that the number of trials is correct.

We detail our experiments in this section, and provide code in the additional files to replicate them.

5.1 Dimension of the singular locus of the UOV variety

To study the properties of the singular locus, we use the bihomogeneous modeling defined in Equation (11).

Let $\mathcal{P}$ be the public key of a UOV instance for parameters n, m, q, let $d = 3m - n - 1$ (as in Theorem 3.1), and choose f a collection of $d - 1$ linear maps uniformly at random. These linear maps define the hyperplanes with which we intersect our variety. The zero-dimensional system we solve to perform a key recovery attack (without a hybrid approach) is the following:

$$\boldsymbol{x} \in \mathbb{F}_q^n, x_1 = 1, \boldsymbol{y} \in \mathbb{F}_q^m, y_1 = 1 \begin{cases} \mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^m \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^n \\ f(\boldsymbol{x}) = 0 \in \mathbb{F}_q^d \end{cases} \tag{20}$$

We list in Figure 3 the results obtained on UOV systems. We provide code to reproduce our experiments.

We can compute experimentally the degree and dimension of a variety using the computation of a Gröbner basis. More precisely, the dimension is the degree of the denominator of the Hilbert series and the degree is the evaluation of the numerator of the series at 1.

In practice, all the systems were zero-dimensional, which implies that our experiment matches Theorem 3.1: if the dimensions had been overestimated, the Gröbner bases would be [1], while the fact that the systems are zero-dimensional show that we added the right number of linear equations to the system. In every case, the Gröbner basis contains exactly $n - m$ linear polynomials defining $\mathcal{O}$, which by Proposition 1 supports applying Theorem 3.2 even in a small field.

5.2 "$\boldsymbol{x} \in \mathcal{O}$?" for VOX/UOV$\hat{+}$

We give in Figure 4 the experimental results of the algorithm of Theorem 4.2 on all security levels for VOX. The experiments were ran on a laptop with

m,n	Dimension	Degree of the variety	Degree of regularity
4, 8	2	4	3
4, 9	1	10	4
4, 10	0	20	5
5, 10	3	5	4
5, 11	2	15	4
5, 12	1	35	5
5, 13	0	70	6
6, 12	4	6	4
6, 13	3	21	5
6, 14	2	56	6
6, 15	1	126	6
6, 16	0	252	7
7, 14	5	7	4
7, 15	4	28	5
7, 16	3	84	6
7, 17	2	210	7

Fig. 3: Experimental computation of Gröbner bases for bihomogeneous modelisations of the singularities of UOV systems in $\mathbb{F}_{251}$.

an Intel CPU i7-1165G7 running at 2.80GHz with 8GB of RAM, using the library msolve [2] with 8 threads (option -t8) after generating the equations using SageMath [32].

q, o, v, t	Bit complexity	Running time	d_{reg}
$251, 48, 54, 6$	38.6	1.8s	4
$1021, 70, 77, 7$	41.1	5.5s	4
$4093, 96, 104, 8$	43.4	15.4s	4

Fig. 4: "$\boldsymbol{x} \in \mathcal{O}$" for VOX in polynomial time.

Notice that in every case, the degree matches the prediction of Theorem 4.2, while the complexity growth (roughly a factor 5 for each security level) is a small overestimation of the running time.

Acknowledgements

The author would like to thank Simon Abelard and Mohab Safey El Din for their supervision and insightful discussions.

References

1. Aulbach, T., Campos, F., Krämer, J., Samardjiska, S., Stöttinger, M.: Separating oil and vinegar with a single trace side-channel assisted Kipnis-Shamir

attack on UOV. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2023**(3), 221–245 (2023). https://doi.org/10.46586/tches.v2023.i3.221-245, https://doi.org/10.46586/tches.v2023.i3.221-245

2. Berthomieu, J., Eder, C., Din, M.S.E.: msolve: A library for solving polynomial systems. In: Chyzak, F., Labahn, G. (eds.) ISSAC '21: International Symposium on Symbolic and Algebraic Computation, Virtual Event, Russia, July 18-23, 2021. pp. 51–58. ACM (2021). https://doi.org/10.1145/3452143.3465545, https://doi.org/10.1145/3452143.3465545
3. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 348–373. Springer (2021). https://doi.org/10.1007/978-3-030-77870-5_13, https://doi.org/10.1007/978-3-030-77870-5_13
4. Beullens, W.: MAYO: practical post-quantum signatures from oil-and-vinegar maps. In: AlTawy, R., Hülsing, A. (eds.) Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers. Lecture Notes in Computer Science, vol. 13203, pp. 355–376. Springer (2021). https://doi.org/10.1007/978-3-030-99277-4_17, https://doi.org/10.1007/978-3-030-99277-4_17
5. Beullens, W.: Breaking Rainbow takes a weekend on a laptop. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 464–479. Springer (2022). https://doi.org/10.1007/978-3-031-15979-4_16, https://doi.org/10.1007/978-3-031-15979-4_16
6. Beullens, W., Chen, M.S., Ding, J., Gong, B., Kannwischer, M.J., Patarin, J., Peng, B.Y., Schmidt, D., Shih, C.J., Tao, C., Yang, B.Y.: Uov (2023), uovsig.org, consulted 05/10/2023
7. Bruns, W., Vetter, U.: Determinantal Rings. Springer Berlin Heidelberg, Berlin, Heidelberg (1988). https://doi.org/10.1007/BFb0080379
8. Cantor, D.G., Zassenhaus, H.: A new algorithm for factoring polynomials over finite fields. Mathematics of Computation **36**(154), 587–592 (1981), http://www.jstor.org/stable/2007663
9. Cogliati, B., Faugère, J.C., Fouque, P.A., Goubin, L., Larrieu, R., Macario-Rat, G., Minaud, B., Patarin, J.: Provable unbalanced oil and vinegar (2023), http://prov-sign.github.io, consulted 05/10/2023
10. Cogliati, B., Faugère, J.C., Fouque, P.A., Goubin, L., Larrieu, R., Macario-Rat, G., Minaud, B., Patarin, J.: Vox-sign (2023), http://vox-sign.com/files/vox_nist.pdf, consulted 05/10/2023
11. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Publishing Company, Incorporated, 4th edn. (2015)
12. Ding, J., Gong, B., Guo, H., He, X., Jin, Y., Pan, Y., Schmidt, D., Tao, C., Xie, D., Yang, B.Y., Zhao, Z.: Triangular unbalanced oil and vinegar (2023), tuovsig.org, consulted 05/10/2023
13. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY,

USA, June 7-10, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3531, pp. 164–175 (2005). https://doi.org/10.1007/11496137_12, https://doi.org/10.1007/11496137_12
14. Ding, J., Yang, B., Chen, C.O., Chen, M., Cheng, C.: New differential-algebraic attacks and reparametrization of Rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5037, pp. 242–257 (2008). https://doi.org/10.1007/978-3-540-68914-0_15, https://doi.org/10.1007/978-3-540-68914-0_15
15. Einsenbud, D.: Commutative Algebra with a view toward Algebraic Geometry. Springer New York (1995)
16. Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L.: A new perturbation for multivariate public key schemes such as HFE andUOV. Cryptology ePrint Archive, Paper 2022/203 (2022), https://eprint.iacr.org/2022/203
17. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. Journal of Symbolic Computation **46**(4), 406–437 (2011). https://doi.org/https://doi.org/10.1016/j.jsc.2010.10.014
18. Furue, H., Ikematsu, Y.: A new security analysis against mayo and QR-UOV using rectangular minrank attack. In: Advances in Information and Computer Security: 18th International Workshop on Security, IWSEC 2023, Yokohama, Japan, August 29–31, 2023, Proceedings. p. 101–116. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-41326-1_6, https://doi.org/10.1007/978-3-031-41326-1_6
19. Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T.: A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021. pp. 187–217. Springer International Publishing, Cham (2021)
20. Guo, H., Ding, J.: A practical minrank attack against vox. Cryptology ePrint Archive, Paper 2024/166 (2024), https://eprint.iacr.org/2024/166
21. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 206–222. Springer (1999). https://doi.org/10.1007/3-540-48910-X_15, https://doi.org/10.1007/3-540-48910-X_15
22. Kipnis, A., Shamir, A.: Cryptanalysis of the oil & vinegar signature scheme. In: Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 257–266. Springer (1998). https://doi.org/10.1007/BFb0055733, https://doi.org/10.1007/BFb0055733
23. Lang, S., Weil, A.: Number of points of varieties in finite fields. American Journal of Mathematics **76**(4), 819–827 (1954), http://www.jstor.org/stable/2372655
24. Luyten, P.: Understanding Kipnis Shamir with two quadrics (2023), Master thesis, KU Leuven
25. Macario-Rat, G., Patarin, J., Cogliati, B., Faugère, J.C., Fouque, P.A., Gouin, L., Larrieu, R., Minaud, B.: Rectangular attack on VOX. Cryptology ePrint Archive, Paper 2023/1822 (2023), https://eprint.iacr.org/2023/1822

26. Neiger, V., Pernet, C.: Deterministic computation of the characteristic polynomial in the time of matrix multiplication. Journal of Complexity **67**, 101572 (Dec 2021). https://doi.org/10.1016/j.jco.2021.101572, https://unilim.hal.science/hal-02963147
27. Patarin, J.: The oil and vinegar signature scheme. In: Dagstuhl Workshop on Cryptography September, 1997 (1997)
28. Pébereau, P.: One vector to rule them all: Key recovery from one vector in UOV schemes. In: Post-Quantum Cryptography: 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings, Part II. pp. 92–108. Springer-Verlag, Berlin, Heidelberg (2024). https://doi.org/10.1007/978-3-031-62746-0_5, https://doi.org/10.1007/978-3-031-62746-0_5
29. Perlner, R., Smith-Tone, D.: Rainbow band separation is better than we thought. Cryptology ePrint Archive, Paper 2020/702 (2020), https://eprint.iacr.org/2020/702
30. Safey El Din, M., Schost, E.: A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. J. ACM **63**(6) (jan 2017). https://doi.org/10.1145/2996450, https://doi.org/10.1145/2996450
31. Safey El Din, M., Trebuchet, P.: Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. Research Report RR-6001, INRIA (2006), https://inria.hal.science/inria-00105204
32. The Sage Developers: SageMath, the Sage Mathematics Software System (2022), https://www.sagemath.org, dOI 10.5281/zenodo.6259615
33. Van der Waerden, B.L.: On hilbert's function, series of composition of ideals and a generalization of the theorem of bezout. In: Proc. roy. acad. amsterdam. vol. 31, pp. 749–770 (1929)
34. Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: SNOVA (2023), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SNOVA-spec-web.pdf, consulted 02/01/2024
35. Zariski, O., Samuel, P.: Commutative Algebra. Springer Berlin, Heidelberg, 1 edn. (1960)