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 quadratic signature schemes submitted to the additional NIST call for signature schemes. Singular points do not exist for generic quadratic systems, which enables us to introduce a new algebraic attack against UOV-based schemes. We show that this attack can be seen as an algebraic variant of the Kipnis-Shamir attack, which can be obtained in our framework as an enumerative approach of solving a bihomogeneous modeling of the computation of singular points.
We give a new attack for UOV$\hat{+}$ and VOX targeting singular points of the underlying UOV key. Our attacks lower 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 [18] to counter the Kipnis-Shamir attack [19] on Oil and Vinegar [22]. Since then, the scheme has suffered no major attack and has been used as a basis for many multivariate signature schemes.

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 [11] 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 [7], QR-UOV [17], SNOVA [26], TUOV [10], (plain) UOV [6] and VOX [8].

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, which 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, where Falcon uses an 897 bytes public key.

Contributions In this paper, we first study the singular locus of the UOV variety, in particular its intersection with the secret subspace $\mathcal{O}$ and the expected dimension of this intersection. The existence of a large singular locus is a very peculiar property for a polynomial system, as it is empty for random quadratic systems. These singular points may be targeted by algebraic key recovery attacks. We study two algebraic modelisations, each leading to an attack, and focus on the bihomogeneous approach from a complexity point of view. We also highlight the connection between these attacks and the Kipnis-Shamir attack described in [18], providing an algebraic alternative to this attack. 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 $\mathbb{F}_q$-rational singular points and an estimation of their number enables one to carry out the Kipnis-Shamir attack, whereas our attacks do not fail when there exists no rational singular point.

As a second contribution, we apply this work to VOX, a UOV variant. VOX [8] is a scheme based on UOV$\hat{+}$ and utilizing the Quotient Ring (QR) transform [17]. It has been submitted to the NIST call for additional signatures. We study the vulnerability of this scheme to our attacks by considering UOV$\hat{+}$, which is equivalent to dismissing the additional structure provided by the QR-transform.

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 [23], by computing a grevlex Gröbner basis for an overdetermined polynomial system.

This allows an attacker to mount a new key recovery attack inspired by the Kipnis-Shamir attack. We obtain cheaper attack costs than the estimates found in [13] and [8]. More precisely, for the VOX parameters from [8], we gain factors $2^2, 2^{18}, 2^{37}$ for security levels I,III,V respectively, bringing the security below the NIST target of $2^{143}, 2^{207}, 2^{272}$ gates. Asymptotically, the exponential factor in our attack is q^{n-2o+t} instead of $q^{n-2o+2t}$ for the Kipnis-Shamir attack.

The security model for UOV$\hat{+}$ key recovery attacks previously estimated that such attacks can only be applied after inverting the $\hat{+}$ transform. Our work proves that this is not the case.

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 [18] 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 isotropic subspace. This observation is due to Luyten [20] 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 [17]. 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 [16], Furue and Ikematsu attacked the parameters of the QR transform used in VOX. This attack did not target 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 quadratic forms, and recall some properties of these objects. 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 [23] 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.

Main results The main result of this paper is the computation of the dimension of the intersection of the singular locus of the UOV variety with the secret subspace $\mathcal{O}$.

Theorem 1 *Let $p_1, \ldots, p_m$ be quadratic forms generating 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 $n > m$.*

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.

This enables us to obtain new algebraic attacks against the UOV scheme.

We obtain a similar result for the UOV$\hat{+}$ variety, which leads to a key recovery attack against UOV$\hat{+}$ that improves the previously known upper bounds for the security of the scheme.

Theorem 2 *Let $\mathcal{P} = (p_1, \ldots, p_o)$ be a UOV$\hat{+}$ public key with t random equations defined over $\mathbb{F}_q[x_1, \ldots, x_n]$, with $n > o$. 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.

This dimension computation enables us to give complexity bounds for the cost of computing one vector in the secret subspace $\mathcal{O}$. We show how to check if a given vector is indeed in $\mathcal{O}$ in polynomial time, and complete a key recovery from one vector in the case of UOV$\hat{+}$ by adapting a result of [23], leading to the following theorem:

Theorem 3 *Let $\mathcal{P}$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t),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 at most $O\left(\binom{n-2o+2t-3}{4}^2 \binom{n-2o+2t+1}{2}\right)$ arithmetic operations in $\mathbb{F}_q$.

Combined with the dimension computation of Theorem 2, this gives a key recovery attack against VOX with an improved exponential coefficient:

Theorem 4 *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:

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

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

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

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

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

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

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 [22] and the motivation was that the secret system $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{t}$ is linear in $x_1, \ldots, x_m$:

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

These variables are distinguished from the rest of variables and are named "oil variables". The remaining ones 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 $I = \langle p_1, \ldots, p_m \rangle$. The set of accepted signatures for a message $\boldsymbol{t} \in \mathbb{F}_q^m$ is an algebraic variety of dimension $n - m$ generically. We distinguish the case $\boldsymbol{t} = (0, \ldots, 0)$ and define the *UOV variety*

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

2.3 Quadratic forms

One of the key insights from the cryptanalysis of Oil and Vinegar [19] and Rainbow [3] is the necessity to have 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.

We use the formalism of quadratic forms with the following definitions. Let f be a quadratic form on a vector space $\mathbb{F}_q^n$. The *polar form* associated to f is $f^* : (\boldsymbol{x}, \boldsymbol{y}) \mapsto f(\boldsymbol{x}+\boldsymbol{y}) - f(\boldsymbol{x}) - f(\boldsymbol{y})$. A subspace $V \subset \mathbb{F}^n$ is *isotropic* for f if there exists $\boldsymbol{x} \in V$ such that $f(\boldsymbol{x}) = 0$, and *totally isotropic* 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 1. *The linear subspace $\mathcal{O}$ is a totally isotropic subspace of a quadratic form f if and only if for all $(\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2$, $f^*(\boldsymbol{x}, \boldsymbol{y}) = f^*(\boldsymbol{y}, \boldsymbol{x}) = 0$.*

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 of dimension m shared by each of the public key quadratic forms. This observation was made as early as the Kipnis-Shamir attack against OV in 1998 [19], with the name "oil space".

2.4 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 [18], [19] The Kipnis-Shamir attack on Oil and Vinegar [19, Theorem 7] is a polynomial time algorithm retrieving a basis of $\mathcal{O}$ when $n = 2m$. It motivated the "unbalanced" property of UOV introduced in [18]. The attack has been generalized to UOV by [18, 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 $p = \frac{q^{3m-n}-1}{q^m-1}$. We compute eigenvectors using the characteristic polynomial, which 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 [12] [3], [1], [23] 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 ([12], [3]), 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:

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

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 [23, 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 $\mathcal{O}$.

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

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 exist 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 $P_1, \ldots, P_m$, the Jacobian of the system $\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x})$ 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 1. *Let $(p_1, \ldots, p_m)$ be a collection of homogeneous polynomials over $\mathbb{K}[\boldsymbol{x}]$. Let $I = \langle p_1, \ldots, p_m \rangle$. We say that $\boldsymbol{x} \in \mathbb{V}(I) \setminus \{0\}$ is a* singular point *of $\mathbb{V}(I)$ if the Jacobian matrix $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}]^{m\times n}$ has rank less than $\mathsf{codim}(I)$. The set of singular points of $\mathbb{V}(I)$ is noted $\mathsf{Sing}(\mathbb{V}(I))$.*

In the rest of the paper, we assume that $n > m$ and that the system $(p_1, \ldots, p_m)$ forms a regular sequence, therefore $\mathsf{codim}(I) = m$. 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 [7], based on the same core ideas as UOV but which distinguish these two values.
- This allows us to obtain different modelisations to compute singular points leveraging the positive dimension of the singular locus.

Theorem 1 (Homogeneous singularities). *Let $p_1, \ldots, p_m$ be quadratic forms generating 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 $n > m$.*

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. This proof uses the shape of a UOV key.

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 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 $J'(\boldsymbol{x})$ is a matrix of $(\mathbb{F}_q[x_1, \ldots, x_o])^{m \times (n-o)}$ 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, following the notations of [15], $\mathsf{Jac}_{\mathcal{F}}(\boldsymbol{x})$ 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'. By [15, Theorem 10], this ideal generically has dimension $d = o - (n - o - (m - 1))(m - (m - 1))$ if $d \geq 0$, namely:

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

Non-genericity may only increase this dimension. 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 $\dim \mathsf{Sing}(\mathbb{V}(I)) \geq d$. □

This property distinguishes the UOV system of equations from random systems of equations since random systems of homogeneous quadratic equations do not admit non-zero singular points.

Notice that by setting $m = o$ and $n = \alpha m$, Theorem 1 shows that the UOV variety has a non-empty singular locus, which has an intersection of dimension $(3 - \alpha)m - 1$ with $\mathcal{O}$ for the practical parameter range $2 < \alpha \leq 3$.

We consider a zero-dimensional system by restricting to a subset of r equations from the key.

$$2o + r - n - 1 \geq 0 \iff r \geq n - 2o + 1 = (\alpha - 2)o + 1$$

In particular, for $r_0 = \lceil (\alpha - 2)o + 1 \rceil$, the singular locus is 0 dimensional. This could motivate one to compute solutions, which, if they exist, would with high probability belong to $\mathcal{O}$.

The Kipnis-Shamir attack implicitly relies on two ingredients: the fact that all singular points are elements of $\mathcal{O}$, and the existence of $\mathbb{F}_q$-rational singular

points. We study the consequences of the first hypothesis in the rest of this section, and show that it 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 [18, "How to find O?"] as the invariant subspace H computed by the attack is one-dimensional, and one cannot use [18, Lemma 3] to distinguish lines in the variety from lines in $\mathcal{O}$. To apply this lemma, one requires a two-dimensional subspace at least. Note however that if the hypothesis does not hold, the attack is not prevented, but it may return false positives. The relationship between these invariant subspaces and singular points is clarified in Section 3.4.

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. We do so using the next result and a slightly stronger reformulation of Hypothesis 1.

Proposition 1. *Let* I *be an ideal. Assume there exist 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 $l_1 \ldots, l_d$ *are the linear polynomials contained in a Gröbner basis with respect to* $\prec$*, then* $\bigcap_{1 \leq i \leq d} \ker(l_i) = \bigcap_{f \in I, \deg(f)=1} \ker(f)$*.*

Proof. a) Let $G = (g_1, \ldots, g_t)$ be a Gröbner basis of I with respect to $\prec$. 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 $i \in [1, d]$ 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 $g_1, \ldots, g_d$ 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 $(1, \ldots, d)$). 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 $f = \sum_{i=1}^{d} a_i g_i$ of the degree 1 elements of the Gröbner basis. Therefore,

$$\bigcap_{1 \leq i \leq d} \ker(g_i) \subset \bigcap_{f \in I, \deg(f)=1} \ker(f)$$

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

We add that if the Gröbner basis is reduced, the same argument shows that the linear equations in the Gröbner basis must define distinct hyperplanes.

In the UOV case, if $\mathcal{O}$ is the smallest subspace containing $\mathsf{Sing}(\mathbb{V}(I))$, one hopes to find exactly $n-o$ linear equations in a reduced grevlex Gröbner basis for the ideal $\langle p_1, \ldots, p_m \rangle + \langle \mathsf{Minors}_m(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \rangle + \langle x_0 - 1 \rangle$. This behavior is observed in practice in Section 5.

But this cannot be obtained from Hypothesis 1 and Proposition 1 alone: in short, a geometric property on $\mathbb{V}(J)$ yields an algebraic property on $\sqrt{J}$. Let $J = \langle p_1, \ldots, p_m \rangle + \langle \mathsf{Minors}_m(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \rangle + \langle x_0 - 1 \rangle$. Notice that $\mathsf{Sing}(\mathbb{V}(I)) = \mathbb{V}(J)$ and if $\mathbb{V}(J) \subset \mathcal{O}$, there exists a linear polynomial $\ell \in I(\mathbb{V}(J)) = \sqrt{J}$ by the Nullstellensatz [27, Theorem 14, p. 164].

To address the potential cases where J is not radical, we rely on a stronger hypothesis compared with Hypothesis 1, but the hypotheses are equivalent if J is indeed radical:

Hypothesis 2 *Let $p_1(\boldsymbol{x}), ..., p_m(\boldsymbol{x})$ be the equations defining a UOV public key for parameters (q, n, m). Let $l_1, ..., l_{n-o}$ be linear forms defining distinct hyperplanes such that $\mathcal{O} = \cap_{i=1}^{n-o} \ker(l_i)$ and $2o + m - n - 1 \geq 0$. Then*

$$\forall 1 \leq i \leq n - o,\ l_i \in \langle p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}) \rangle + \langle \mathsf{Minors}_m(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \rangle + \langle x_0 - 1 \rangle$$

This hypothesis is motivated by the proof of Theorem 1: it assumes that restricting to the case $\boldsymbol{x} \in \mathcal{O}$ does not add any information, and geometrically, it implies that $\mathsf{Sing}(\mathbb{V}(I)) \subset \mathcal{O}$. We add the equation $x_0 - 1$ to dehomogenize the ideal: without this, the linear forms defining $\mathcal{O}$ will only divide elements of the grevlex Gröbner basis (and the lowest degree in the basis will be two). The choice of x_0 is arbitrary.

We note that in our experiments, J was always found to be radical, and therefore in practice Hypothesis 1 would have been sufficient.

3.2 Modeling singularities

We use Theorem 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. If Hypothesis 2 holds, then such a Gröbner basis contains linear equations that characterize $\mathcal{O}$. In particular, one does not require the singular points to be $\mathbb{F}_q$-rational to complete the attack. If the hypothesis does not hold, then one concludes the computation using FGLM to obtain a lex Gröbner basis and the set of $\mathbb{F}_q$-rational solutions.

Including all the public key equations may be too costly: a naive minors modeling would yield equations of degree m, far above the degree of regularity of any competitive attack on UOV (see for instance [3]).

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 polynomial 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.

Definition 2. *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:*

$$\mathcal{M}(\mathcal{P}, r) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{x} \neq \boldsymbol{0} \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathsf{Minors}_r(\mathsf{Jac}_{\mathcal{P},r}(\boldsymbol{x})) = 0 \end{cases} \tag{6}$$

2. *Bihomogeneous modeling:*

$$\mathcal{B}(\mathcal{P}, r) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^r, \boldsymbol{x} \neq \boldsymbol{0}, \boldsymbol{y} \neq \boldsymbol{0} \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P},r}(\boldsymbol{x}) = 0 \end{cases} \tag{7}$$

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 [20] 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 (6) and (7) 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 1. By intersecting it with an arbitrary hyperplane to dehomogenize (for instance the one defined by $x_0 - 1$), we obtain a zero-dimensional variety.

Notice that a priori, Theorem 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 (6) and (7), the quadratic equations include all m public key equations. This is because Theorem 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. Because of this overdetermination, one expects that there are no "parasitic" solutions (and therefore that Hypothesis 2 holds).

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.

3.3 Computing singular points using the bihomogeneous modeling

The results we rely on are described in detail in [24, Chapter 6] and [14].

Definition 3. *Let $\boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_m)$ two sets of variables. Let p 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*

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

We can slightly improve the formulation of Equation 7: $\boldsymbol{y}$ is any element of the one-dimensional[2] left kernel of the Jacobian evaluated on a singular point. Thus, for each $\boldsymbol{x} \in \mathsf{Sing}(\mathbb{V}(I))$, there exist q choices of $\boldsymbol{y}$ in $(\mathbb{F}_q)^r$. We may normalize either to $y_1 = 1$ or $y_1 = 0$ and for some $i \neq 1$, $y_i = 1$ to obtain a unique solution. In doing so, we dehomogenize the system, allowing us to consider an affine bihomogeneous system.

We may choose r such that the system $\mathcal{B}(\mathcal{P}, r)$ is a bihomogeneous system of $n + m$ equations in $n + r - 1$ variables defining a zero-dimensional variety. It is bihomogeneous of bidegree (2,1) in the variables $(x_1, \ldots, x_n), (y_2, \ldots, y_r)$. More precisely, 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). Using [14, Theorem 6.1], this zero-dimensional affine bilinear system has degree of regularity $\min(n + 1, r) = r$. This value matches the experiments performed on small instances of UOV. Therefore, the number of arithmetic operations required to obtain a Gröbner basis is dominated by:

$$O\left(\binom{n + 2r - 1}{r}^{\omega}\right)$$

We give in Figure 1 the estimated number of arithmetic operations required to solve the bihomogeneous system (7) using a generic Gröbner basis algorithm.

[2] 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 [15, Theorem 10] is negative.

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	370	272	452	592
d_{reg}	33	25	41	53

Fig. 1: Cost of the singular point attack via bihomogeneous modeling for UOV

3.4 Revisiting the Kipnis-Shamir attack [19], [18]

The goal of this section is to use the work of [18] to deduce the number of $\mathbb{F}_q$-rational singular points of the UOV variety. Computing the cardinality of a variety, let alone the number of rational elements, is a hard task in general.

Bihomogeneous modeling - $\boldsymbol{y}-$Enumeration. Consider a hybrid approach to the bihomogeneous system defined in Equation (7), where we enumerate over all possible values of $\boldsymbol{y}$. In this case, we will 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:

$$\exists \boldsymbol{x}, \boldsymbol{y}, \quad \begin{cases} \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \\ \mathcal{P}(\boldsymbol{x}) = 0 \end{cases} \iff \exists \boldsymbol{x}, \boldsymbol{y}, \quad \begin{cases} (\sum_{i=1}^{m} y_i (P_i + P_i^T))\boldsymbol{x} = 0 \\ \mathcal{P}(\boldsymbol{x}) = 0 \end{cases} \tag{8}$$

Instead of using a Gröbner basis algorithm, observe that the linear equations entirely determine $\boldsymbol{x}$, and there are no $\boldsymbol{x}$ solutions unless the linear combination $\sum_{i=1}^{m} y_i (P_i + P_i^T)$ is singular. If $\boldsymbol{x}$ is a solution to the linear system, we check whether it is a solution to the quadratic system simply by evaluating $\mathcal{P}(\boldsymbol{x})$. Such a point will be singular for the system $\{p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x})\}$ by (8).

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 (8) 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.

Before estimating S, we focus on the cost of finding a valid value of $\boldsymbol{y}$.

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 $m-1$ variables, then we can consider the determinant as a univariate polynomial in the remaining variable. We may solve this univariate equation with a fast finite field algorithm 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]. To summarize, for each guess of the $m-1$ variables, we proceed as follows:

- Compute $M(y)$ a sum of m $n \times n$ matrices in $\mathbb{F}_q[y]_{\leq 1}$ (amortized[3]) $O(n^2)$
- 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[4]) $O(\ell n^2)$

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:

$$C(q, n, m) = O(\frac{q^{m-1}}{S} n^\omega) \tag{9}$$

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 [20], 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 [19, 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 (8).

Lemma 2. *For $1 \leq i \leq m$, let $P_i^* = P_i + P_i^T$. Assume P_m^* is invertible.*

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

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

$$\chi_{(P_m^*)^{-1}M}(\lambda) = \det\left((P_m^*)^{-1}M - \lambda I\right)$$

Therefore:

$$\det(P_m^*) \cdot \chi_{(P_m^*)^{-1}M}(\lambda) = \det(M - \lambda P_m^*) \tag{10}$$

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

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

[4] 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

At the start of this section, we solved $\det(M - \lambda P_m^*)(y) = 0$ to compute y_m.

This shows that eigenvectors of $(P_m^*)^{-1}M$ associated to an eigenvalue λ_0 induce a rank defect in $\mathsf{Jac}_{\mathcal{P}}$ by Equation (8), 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 $(P_m^*)^{-1}M$ 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 [18, Note above Theorem 4.2].

Hypothesis 3 *Let $P_1, \ldots, P_m$ be matrices from a UOV public key for parameters q, n, m. 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, such that Equation (9) matches the complexity of the Kipnis-Shamir attack:

$$C(q, n, m) = O(q^{n-2m} m n^2) \tag{11}$$

In conclusion, an enumerative approach to the computation of singular points provides an algebraic interpretation of the Kipnis-Shamir attack from [18]. Furthermore, we highlight an hypothesis (Hypothesis 1) used in the original Kipnis-Shamir attack of [18], and reproduce the experiments of [18] in low dimension in a new algebraic framework.

We point out that the algebraic approach described in Section 3.3 has an advantage over the Kipnis-Shamir attack: under Hypothesis 2, it does not fail if no rational singular points exist. In the next section, we use the properties of this algebraic formulation to study the security of schemes derived from UOV.

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

In this section, after defining VOX and UOV$\hat{+}$ in Section 4.1, we study the dimension of the singular locus of the VOX variety in 4.2. The rest of the section is dedicated to an attack that improves the cryptanalysis of the scheme. In Section 4.3, we propose a polynomial time key recovery from one vector against VOX, which we turn into a full key recovery attack in Section 4.4.

4.1 Definition of UOV$\hat{+}$

VOX [8] 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 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 [13]. 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 [17], 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 (o, v, t, q) is composed of a secret key $(S, A, \mathcal{F})$ and a public key $\mathcal{P}$, with:

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

Let $n = o + v$ and let $\hat{\mathcal{F}} = (F_{t+1}, \ldots, F_o)$ 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 $p_1, \ldots, p_t$ are uniformly random (they are called "vinegar polynomials" in [8]) 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.

Figure 2 includes the parameter sets submitted at NIST for VOX in [8], and new parameters following an attack on the QR transform (see [16], [21]). The initial VOX parameters were the parameter sets VOX I, III, V. Notice that in every case, the underlying UOV instance is unbalanced by a small term c.

Variant	Security level	q	o/c	v/c	c	t
I	2^{143}	251	8	9	6	6
Ia		251	4	5	13	6
Ib		251	5	6	11	6
Ic		251	6	7	9	6
III	2^{207}	1021	10	11	7	7
IIIa		1021	5	6	15	7
IIIb		1021	6	7	13	7
IIIc		1021	7	8	11	7
V	2^{272}	4093	12	13	8	8
Va		4093	6	7	17	8
Vb		4093	7	8	14	8
Vc		4093	8	9	13	8

Fig. 2: VOX parameters in [8] and [21].

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

We now apply the work of Section 3 to UOV$\hat{+}$. The core idea is to study, as previously 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 2. *Let $\mathcal{P} = (p_1, \ldots, p_o)$ be a UOV$\hat{+}$ public key with t random equations defined over $\mathbb{F}_q[x_1, \ldots, x_n]$, with $n > o$. 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 $\hat{\mathcal{P}} = \hat{\mathcal{F}} \circ A$. By Theorem 1, it defines a variety $V(\hat{I}) = \{\boldsymbol{x} \in \overline{\mathbb{F}_q}^n, \hat{\mathcal{P}}(\boldsymbol{x}) = \mathbf{0}\}$ with a singular locus of dimension at least $d + t$. The UOV$\hat{+}$ variety $\mathbb{V}(I)$ is obtained by intersecting $V(\hat{I})$ 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 $V(\hat{I})$, then $\boldsymbol{x}$ must be singular point of $\mathbb{V}(I)$. This implies that the singular locus of $\mathbb{V}(I)$ contains the intersection of the singular locus of $V(\hat{I})$ with V_t, the variety defined by the random equations.

By [9, 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 2 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 generically intersects the variety V_t if d is non-negative. In light of Section 3.4, 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.

We can use Equation (9), which predicts the cost of the Kipnis-Shamir attack interpreted as an enumerative singular point computation, along with Hypothesis 3 to estimate the number of rational singular points, by assuming that the relationship between the dimension and the number of rational solutions still holds for UOV$\hat{+}$. We have $\dim \mathsf{Sing}\mathbb{V}(I) = 3o - n - 1 - 2t$. This yields the following expectated cost for the Kipnis-Shamir attack against UOV$\hat{+}$:

$$C(q, n, o, t) = O\left(\frac{q^{o-1}}{|\mathsf{Sing}V(I)|} n^\omega\right) = O(q^{n-2o+2t} n^\omega) \tag{12}$$

This cost is identical to the estimations in [13], [8]. Note though that this assumes that the number of rational singular points is only reduced by q^t after cutting the singular locus with t generic quadrics. Therefore, we consider that this complexity underestimates the cost of the direct Kipnis-Shamir attack on VOX.

Instead, we propose 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.

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 $\mathcal{O}$ vanish the public key polynomials.

A polynomial-time key recovery from one vector against UOV is introduced both in [1] and [23].

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 [23, Section 4], these tools are applied to VOX, interpreted as UOV$\hat{+}$: the underlying UOV public key may be 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 [23, 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 [8], we achieve a complexity polynomial in n and o.

Lemma 3. *Let $\mathcal{P} = (P_1, \ldots, P_m)$ 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

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

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

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

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 [23] is that

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

Therefore in our case

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

This intersection has dimension at least $o - t$, therefore

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

By genericity of $P_1, \ldots, P_t$, we expect this to be an equality in most cases. This concludes the proof. □

We obtain a key recovery from one vector by restricting the VOX public key to this kernel, and by considering the properties of this new UOV$\hat{+}$ instance.

Theorem 3. *Let $\mathcal{P}$ be a UOV$\hat{+}$ public key for parameters (q, o, v, t), 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 at most $O\left(\binom{n-2o+2t-3}{4}^2 \binom{n-2o+2t+1}{2}\right)$ arithmetic operations in $\mathbb{F}_q$.

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

Following the methodology of [23], 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 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 3.

Let $\mathcal{O}' = \mathcal{O} \cap \ker \begin{pmatrix} \boldsymbol{x}^T P_1 \\ \vdots \\ \boldsymbol{x}^T P_t \end{pmatrix}$ be the oil space associated to this key. Define the following ideals: $I = \langle P_{1|B}, \ldots, P_{o|B} \rangle$ and $I_t = \langle P_{1|B}, \ldots, P_{t|B} \rangle$. We have:

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

Note that $\dim(V(I_t) \cap \mathcal{O}') \geq o - t - t$ and therefore $\dim V(I) \geq o - 2t$. On the other hand, the expected dimension of the variety defined by a generic collection of o equations in dimension $n - o + 1$ is $n - 2o + 1 = t + 1$. Therefore, if $n - 2o + 1 < o - 2t$, then the variety $V(I)$ 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 $J = I + < h_1, \ldots, h_{o-2t} >$, where $h_1, \ldots, h_{o-2t}$ are generic linear forms that we add to the system to reach dimension 0. Note that $V(J) \subset \mathcal{O}'$, therefore by Proposition 1, the grevlex Gröbner basis will contain $o - 2t$ (the number of h_i) $+ 2t$ (the number of hyperplanes defining $\mathcal{O}'$) $= o$ linear forms.

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 constant. 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 first non-positive index 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:

[5] Each hyperplane eliminates one variable.

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

We use the complexity estimate for solving a quadratic polynomial system in [8, Section 7.1], yielding the following upper bound on the number of arithmetic operations required for the computation of a grevlex Gröbner basis:

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

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 grevlex Gröbner basis is [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 [23]. The cost of these last steps is at most $O(on^\omega)$, 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, the generalization of the attack computes singular points of the VOX public key when checking $\mathcal{P}(\boldsymbol{x}) = \mathbf{0}$, but this approach suffers from the drop in dimension of the singular locus due to the random polynomials:

We propose to 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 are only interested in the singular locus of the underlying UOV key, which has dimension $d+t$: this is important to prove the complexity result, as Hypothesis 3 gives a precise estimate for the cardinality of the set of rational singular points for the underlying UOV variety, but it does not a priori apply to the VOX variety.

Theorem 4 (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 2, 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 $3o-t-n-1$, the expected number of rational singular points of $\hat{\mathcal{P}}$ is $S = q^{3o-t-n-1}$ by Hypothesis 3. Following the methodology of Section 3.4, we 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 3.4, each trial costs:

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

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 3 and for UOV$\hat{+}$ in Figure 4.

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

Fig. 3: Complexity of the key recovery attack against VOX [8].

q, o, v, t	Bit complexity	Target
$2^6, 48, 56, 8$	153	143
$2^9, 64, 72, 8$	**198**	207
$2^{12}, 88, 96, 8$	**242**	272

Fig. 4: Complexity of the key recovery attack against UOV$\hat{+}$ [13].

5 Experimental results

In this section, we start by presenting an experiment to confirm the dimension computation of Theorem 1, along with the property described in Proposition 1.

Finally, we present an implementation of the attacks of Section 4.3 and Section 4.4.

The degree of regularity and complexity claims of Theorem 3 are verified by the algorithm provided. Based on this, the complexity of the algorithm in Theorem 4 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.

The code for all attacks and experiments can be found at

`https://github.com/pi-r2/SingPoints`

5.1 Dimension of the singular locus of the UOV variety

We verified our results on the singular locus of the UOV variety with various experiments in low dimensions ($m \leq 10$) and for the field $\mathbb{F}_{251}$. The size of the field does not significantly affect Gröbner basis algorithms.

To study the properties of the singular locus, we use the bihomogeneous modeling defined in Equation (7). The minors modeling is highly impractical to manipulate: computing the minors is already a hard task due to their number: $\binom{n}{r}$.

We also point out that the statement of Theorem 1 is homogeneous: to obtain a useful result from a Gröbner basis algorithm, one must dehomogenize the equations (typically done by setting $x_1 = 1$). In doing so, we reduce the dimension of the singular locus by one compared with the homogeneous result, as this is equivalent to intersecting the variety with an arbitrary hyperplane.

Another important remark is that Gröbner basis algorithms are efficient in the zero-dimensional case: therefore, when we expect the variety to have dimension d, we add d random linear forms in the $\boldsymbol{x}$ variables to obtain a zero-dimensional variety.

Let $\mathcal{P}$ be the public key of a UOV instance for parameters n, m, q, let $d = 3m - n - 1$ (as in Theorem 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:

$$\boldsymbol{x} \in \mathbb{F}_q^n, x_1 = 1, \boldsymbol{y} \in \mathbb{F}_q^m, y_1 = 1 \begin{cases} \mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^m \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^n \\ f(\boldsymbol{x}) = 0 \in \mathbb{F}_q^d \end{cases} \tag{13}$$

We list in Figure 5 the results obtained on UOV systems. We provide code to reproduce our experiments.

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

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.

The dimensions obtained experimentally match Theorem 1: if the dimensions had been overestimated, the Gröbner bases would be [1]. In every case, the Gröbner basis contains exactly $n - m$ linear polynomials defining $\mathcal{O}$, which supports Hypothesis 2.

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

We give in Figure 6 the experimental results of the algorithm of Theorem 3 on all security levels for VOX. The experiments were ran on a laptop with 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 [25].

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

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. 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
8. 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
9. 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)
10. 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
11. 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
12. 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
13. 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
14. 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
15. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: On the complexity of the generalized minrank problem. Journal of Symbolic Computation **55**, 30–58 (2013). https://doi.org/https://doi.org/10.1016/j.jsc.2013.03.004
16. 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
17. 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)
18. 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
19. 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
20. Luyten, P.: Understanding Kipnis Shamir with two quadrics (2023), Master thesis, KU Leuven
21. 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
22. Patarin, J.: The oil and vinegar signature scheme. In: Dagstuhl Workshop on Cryptography September, 1997 (1997)
23. Pébereau, P.: One vector to rule them all: Key recovery from one vector in UOVschemes. 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
24. Spaenlehauer, P.J.: Résolution de systèmes multi-homogènes et déterminantiels algorithmes - complexité - applications. Ph.D. thesis (2012), http://www.theses.fr/2012PA066467, thèse de doctorat dirigée par Faugère, Jean-Charles Informatique Paris 6 2012
25. The Sage Developers: SageMath, the Sage Mathematics Software System (2022), https://www.sagemath.org, dOI 10.5281/zenodo.6259615
26. 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
27. Zariski, O., Samuel, P.: Commutative Algebra. Springer Berlin, Heidelberg, 1 edn. (1960)