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 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 two new algebraic attacks against UOV-based schemes. We show that they 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. This allows us to highlight some heuristics implicitly relied on by the Kipnis-Shamir attack.
We give new attacks for UOV† and VOX targeting singular points of the public key equations. Our attacks lower the security of the schemes, both asymptotically and in number of gates, showing in particular that the parameters sets proposed for these schemes do not meet the NIST security requirements. More precisely, we show that the security of UOV† was overestimated by factors $2^{22}, 2^{36}, 2^{59}$ for security levels I, III, V respectively.
We conclude the attack on VOX by showing that an attacker can perform a full key recovery from one vector obtained in the previous attacks.

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 [10] was a finalist in the third round. The cryptanalysis of Rainbow [4] 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 [3], PROV [6], QR-UOV [17], SNOVA [25], T-UOV [9], (plain) UOV [5] and VOX [7].

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 a 897 bytes public key.

Contribution

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 generically empty (we use here the notion of genericity induced by Zariski topology). These singular points may be targeted by algebraic key recovery attacks. We propose two algebraic modelisations, each leading to an attack. 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 implicitly 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. Moreover, the Kipnis-Shamir attack relies on the existence of rational singular points to succeed, 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 [7] is a scheme based on $\mathrm{UOV}^{\hat{+}}$ 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 $\mathrm{UOV}^{\hat{+}}$, 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. The security model for UOV^{+} 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, and we obtain cheaper attack costs than the estimates found in [12] and [7]. More precisely, for the VOX parameters from [7], we gain factors $2^{19}, 2^{26}, 2^{57}$ for security levels I,III,V respectively, bringing the security below the NIST target of $2^{143}, 2^{207}, 2^{272}$ gates. Asymptotically, we gain a factor q^t for key recovery attacks against these schemes, where q is the size of the field considered in VOX and t is a parameter of the scheme.

We provide a method recovering the full VOX private key from a single oil vector, generalizing a result of [23], by utilizing a MinRank instance solved enumeratively. This allows an attacker to obtain a full key recovery attack from

the previously mentioned singular point computation, but also to mount a new key recovery attack.

Finally, we provide experimental results and 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 existence 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 the 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.

Theorem 1 *Choose $p_1, \ldots, p_m$ uniformly at random among the quadratic forms generating a radical ideal $I = \langle p_1, \ldots, p_m \rangle$ such that $\mathbb{V}(I)$ contains an $o-$dimensional linear subspace $\mathcal{O}$. Let $d = 2o + m - n - 1$. If $d \geq 0$, then the singular locus of $\mathbb{V}(I)$ is non-empty and its intersection with $\mathcal{O}$ has dimension d.*

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

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

Theorem 2 *Let $\mathcal{P}$ be a $UOV^{\hat{+}}$ public key chosen uniformly at random for parameters (q, n, o, t) with $n > o$. Then the $UOV^{\hat{+}}$ variety $\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}_q}^n, \mathcal{P}(\boldsymbol{x}) = \mathbf{0}\}$ has a positive dimensional singular locus. More precisely, let $r \leq o - t$, $d' = 2o + r - n - 1$, $d = d' - t$:*

i. If $d' \geq 0$, the variety defined by r equations of the underlying UOV key has a singular locus of dimension d'.
ii. If $d \geq 0$, the variety defined by r equations of the $UOV^{\hat{+}}$ public key has a singular locus of dimension d.

From one vector computed in the previous attack, we show how to complete a key recovery by adapting a result of [23] to the case of $\text{UOV}^{\hat{+}}$.

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, and let $\boldsymbol{x} \in \mathcal{O}$. Then there exists an algorithm taking as input $\boldsymbol{x}$ and $\mathcal{P}$ and outputting a basis of $\mathcal{O}$, requiring at most $O\left(q^t(n-o)^\omega\right)$ arithmetic operations in $\mathbb{F}_q$.*

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. 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 $(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$.

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,
- $\mathcal{F} = (F_1, \ldots, F_m)$ a quadratic map with $F_i(\boldsymbol{e}_j) = 0$ for $1 \leq i, j \leq m$
- $\mathcal{P} = \mathcal{F} \circ A = (P_1, \ldots, P_m)$ a quadratic map.

In practice, we consider homogeneous quadratic maps: there are no constant and linear terms. If we represent the quadratic maps with matrices, we have for all $1 \leq i \leq m$:

$$F_i = \begin{pmatrix} 0 & F_i^{(1)} \\ F_i^{(2)} & F_i^{(3)} \end{pmatrix} \tag{1}$$

$$P_i = A^T F_i A \tag{2}$$

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

$$\mathcal{F}(\boldsymbol{x}) = \boldsymbol{t} \iff \begin{cases} \boldsymbol{x}^T F_1 \boldsymbol{x} = t_1 \\ \vdots \\ \boldsymbol{x}^T F_m \boldsymbol{x} = t_m \end{cases} \tag{3}$$

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 [2] is the necessity to have a geometric perspective on the equations defining the scheme. More precisely, we 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 homogeneous quadratic form over a vector space $\mathbb{F}_q^n$. In fields of odd characteristic, a homogeneous quadratic form f is characterized by its *polar form* $f^* := (\boldsymbol{x}, \boldsymbol{y}) \mapsto f(\boldsymbol{x}+\boldsymbol{y}) - f(\boldsymbol{x}) - f(\boldsymbol{y})$ which is a symmetric bilinear form. As such, it admits a unique symmetric matrix representation in $\mathbb{F}_q^{n \times n}$. We identify both f and f^* to this matrix.

In fields of even characteristic, there is no longer an equivalence with symmetric bilinear forms. Instead, we can represent quadratic forms uniquely using triangular matrices. Dense square matrices are valid representations, but there are many dense matrices representing the same quadratic form. Changes of variables are not as straightforward with triangular representations, as the set of triangular matrices is not stable by congruence: if F is upper triangular, and $A \in GL_n(\mathbb{F}_q)$, $A^T F A$ is not necessarily upper triangular. Notice in particular that the triangular representation of $A^T F A$ does not necessarily have the same rank as F. In characteristic two, using triangular representation, we may therefore not refer to the "rank of the quadratic form" as it is not uniquely defined. It

is uniquely defined in dense or symmetric representation by property of matrix multiplication.

Therefore, when referring to the rank, we will assume that the matrices representing the quadratic forms are either dense in characteristic two or symmetric in odd characteristic. This way, we may define the rank of a quadratic form: we say that f has *rank* r if the matrix associated to f has rank r. The rank is preserved by linear changes of variables.

Finally, we recall the definition of *isotropic subspaces* which is the core of the study of the UOV key pair. A subspace $V \subset \mathbb{F}^n$ is *isotropic* for f if there exists $\boldsymbol{x} \in V$ such that $f(\boldsymbol{x}) = 0$, *totally isotropic* if for all $\boldsymbol{x} \in V, f(\boldsymbol{x}) = 0$, and *anisotropic* if for all $\boldsymbol{x} \in V \setminus \{0\}, f(\boldsymbol{x}) \neq 0$.

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 B, a basis of $\mathbb{F}_q^n$. Then a matrix 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".

Observe that the dimension of a totally isotropic subspace of a quadratic form of a certain rank is bounded:

Lemma 2. *Let f be a quadratic form of rank n defined over a field $\mathbb{K}$. Let $\mathcal{O}$ be a totally isotropic subspace of f. Then $\mathcal{O}$ has dimension no greater than $\lfloor \frac{n}{2} \rfloor$.*

Proof. By contradiction, assume that f has rank n and $\dim(\mathcal{O}) = r > \lfloor \frac{n}{2} \rfloor$. Let B be a basis of $\mathcal{O}$, let $\hat{B}$ be a completion of B into a basis of $\mathbb{K}^n$. Then the matrix representing f^* in basis $\hat{B}$ has a block of zeros of size $r \times r$ in the top left corner. Therefore its rank is less than n, which is a contradiction. □

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 [23] Lemma 1 shows that once one or more vectors of the secret key have been obtained, one obtains linear equations characterizing the remaining vectors. This formulation 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 less variables. If $n-m < 2m$, by 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 generic 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. 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:

Definition 1. *Let $(p_1,\dots,p_m)$ be a collection of homogeneous polynomials over $\mathbb{K}[\boldsymbol{x}]$. Let $I = \langle p_1,\dots,p_m\rangle$ be a radical ideal. 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 $\mathsf{Sing}(\mathbb{V}(I))$.*

For generic polynomial systems, there are no singular points. Note that the determinantal ideal generated by the maximal minors of $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})$ has dimension

$m-1$ when $\mathcal{P}$ is generic: there exist points that drop the rank of the Jacobian, but they do not belong to the variety defined by the system generically.

In odd characteristic, we represent the UOV public key using symmetric matrices $P_1, \ldots, P_m$. Notice that

$$\frac{1}{2}\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \begin{pmatrix} \boldsymbol{x}^T P_1 \\ \vdots \\ \boldsymbol{x}^T P_m \end{pmatrix} \tag{4}$$

In even characteristic, using triangular matrices, we observe a similar property by dismissing the diagonal terms. This is always possible as these entries correspond to squares of variables x_j^2 which are linear due to the Frobenius endomorphism $x \mapsto x^p$.

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

A constant factor does not affect the ideals that we consider, therefore we will also denote this matrix $\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})$ in odd characteristic.

Theorem 1 (Homogeneous singularities). *Choose $p_1, \ldots, p_m$ uniformly at random among the quadratic forms generating a radical ideal $I = \langle p_1, \ldots, p_m \rangle$ such that $\mathbb{V}(I)$ contains an $o-$dimensional linear subspace $\mathcal{O}$. Let $d = 2o + m - n - 1$. If $d \geq 0$, then the singular locus of $\mathbb{V}(I)$ is non-empty and its intersection with $\mathcal{O}$ has dimension 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:

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

where $J'(\boldsymbol{x})$ is a matrix of $(\mathbb{F}_q[x_1, \ldots, x_o])^{m \times (n-o)}$ with entries that are generic 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 terminology of [14], $\mathsf{Jac}_{\mathcal{F}}(\boldsymbol{x})$ 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 [14, Theorem 10] , this ideal has dimension $d = o-(n-o-(m-1))(m-(m-1))$ if $d \geq 0$, or more succintly:

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

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

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 in this theorem, we make a distinction between the values m and o, even though they are equal for UOV. There are two reasons for this:

- There are schemes, such as MAYO and PrUOV, 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.

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.

We highlight the following hypothesis, that has been used implicitly by the Kipnis-Shamir attack and that is supported by experiments on small instances. We reuse the notations introduced above.

Hypothesis 1 *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 generic collection of quadrics with a common totally isotropic subspace* $\mathcal{O}$*. Assume* $\dim(\mathcal{O}) = o$*. If* $2o + m - n - 1 > 0$*, then* $\mathsf{Sing}(\mathbb{V}) \subset \mathcal{O}$*.*

Here, genericity means that we choose the quadrics uniformly at random among those that vanish on $\mathcal{O}$. From a practical perspective, this is the key generation process in UOV: we choose all coefficients of $\mathcal{F}$ at random, except for the blocks of zeros that we impose.

This hypothesis is implicitly used in [18, Lemma 3] as the invariant subspace H computed by the attack is one-dimensional. We detail the relationship between these invariant subspaces and singular points in Section 3.5.

This hypothesis has a very interesting consequence that we can leverage in attacks against UOV. If it holds, then the singular locus is entirely included in $\mathcal{O}$, a linear subspace.

In particular, assuming the ideal is radical, there must be $n-m$ linear forms in a reduced Gröbner basis with respect to a graded ordering for the previous ideal. Their kernels define $n-m$ distinct hyperplanes, the intersection of which is exactly $\mathcal{O}$. The main consequence is that we do not need rational singular points to obtain a key recovery attack against the scheme using an algebraic approach. We detail this in the next result.

Proposition 1. *Let $\mathcal{O}$ be a linear subspace of $\mathbb{F}_q^n$ of dimension o. Let $I = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of $\mathbb{F}_q[\boldsymbol{x}]$ such that $\mathbb{V}(I) \neq \emptyset$ and $\mathbb{V}(I) \subset \mathcal{O}$. Then, a Gröbner basis of I for any graded monomial ordering contains linear equations $H_1(\boldsymbol{x}), \ldots, H_{n-o}(\boldsymbol{x})$ such that*

$$\mathcal{O} = \cap_{i=1}^{n-o} H_i$$

Proof. By assumption, $\mathbb{V}(I) \subset \mathcal{O}$. Therefore, if H is a linear form such that $\mathcal{O} \subset \ker(H)$, then $H(\boldsymbol{x}) \in I(\mathbb{V}(I))$. By the Nullstellensatz (see [8, Theorem 6]), this implies that $H(\boldsymbol{x}) \in \sqrt{I}$. Since I is radical by assumption, then $\sqrt{I} = I$ and $H(\boldsymbol{x}) \in I$.

Next, let $\prec$ be a graded monomial ordering. On the first hand, a graded monomial ordering is a monomial ordering which first compares the total degree before breaking ties. Therefore, if p is a polynomial in $\mathbb{F}_q[\boldsymbol{x}]$, then the leading term of p with respect to $\prec$ has degree equal to the total degree of p.

On the other hand, a Gröbner basis of I for $\prec$ is a set $G = \{g_1, \ldots, g_t\} \subset I$ such that

$$\langle LT_\prec(g_1), \ldots, LT_\prec(g_t) \rangle = \langle LT_\prec(I) \rangle$$

This implies that a Gröbner basis of I must contain polynomials whose leading terms are of minimal degree, in our case 1. The collection of linear equations included in a Gröbner basis must have rank at least $n-o$, otherwise we could find a linear equation in I linearily independent from the ones in the basis. We add that in the reduced Gröbner basis for $\prec$, there are only independent linear equations, otherwise the basis would not be reduced. □

3.2 Modeling singularities

Under Hypothesis 1, we use Theorem 1 to obtain key recovery attacks against UOV by computing singular points of the variety defined by subsets of equations of the UOV public key. Intuition suggests that including all the 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 [2]).

We propose two attacks based on two different modelings, one based on minors of the Jacobian, 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 spans a determinantal ideal and the latter is bihomogeneous of bidegree (2,1)) and are suited for Gröbner basis approaches.

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:*

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

2. *Bihomogeneous modeling:*

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

If they exist, solutions $\boldsymbol{x}$ of either of these systems 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. 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.

We analyze the complexity results associated to each 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 minors modeling

Determinantal ideals are not semi-regular, and therefore the degree of regularity of these ideals is obtained through a different Hilbert series than the usual semi-regular case. The problem of computing critical points is well-studied and is closely related to the problem of singular points. We use results from [1] to obtain the Hilbert series of the ideal we consider.

Proposition 2. *[1, Proposition 5 and paragraph 3.4] Let $\mathcal{P}(\boldsymbol{x})$ be a system of r equations in n variables. The system $\mathcal{M}(\mathcal{P}, r)$ is a system of $r + \binom{n}{r}$ equations, of which r are of degree 2 and $\binom{n}{r}$ are of degree r. Let $\mathcal{I}_{\mathcal{M}}$ be the ideal generated by the system $\mathcal{M}(\mathcal{P}, r)$. The Hilbert series of $\mathbb{F}_q[\boldsymbol{x}]/\mathcal{I}_{\mathcal{M}}$ is*

$$H(t) = \left(\sum_{k=0}^{r-1} \binom{n-r-1+k}{k} t^k \right) (1+t)^r$$

Notice that if $\boldsymbol{x} \in \mathcal{O}$, then it satisfies the remaining equations of the public key: $p_{r+1}(\boldsymbol{x}) = \ldots = p_m(\boldsymbol{x}) = 0$. Assuming they are not zero-divisors

in $\mathbb{K}[\boldsymbol{x}]/\mathcal{I}_{\mathcal{M}}$, the Hilbert series (in this case a polynomial) of the ideal $I = \mathcal{I}_{\mathcal{M}} + \langle p_{r+1}, \ldots, p_m \rangle$ is:

$$H_I(t) = H(t) \cdot (1-t^2)^{m-r} = (\sum_{k=0}^{r-1} \binom{n-r-1+k}{k} t^k)(1+t)^m (1-t)^{m-r}$$

The degree of regularity of the system is the first non-positive coefficient in this polynomial [11]. Given the degree of regularity d_{reg}, the number of arithmetic operations is upper-bounded by:

$$C(n, d_{reg}) = O\left(\binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$$

Figure 1 lists the number of field operations required for the minor modeling systems with $r = \frac{m}{2}+1$ on modern UOV parameters. We also list the corresponding degrees of regularity.

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	382	266	426	564
d_{reg}	38	27	42	55

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

We note that these costs are over twice the security levels expected of each parameter set. The utility of this modeling and the one detailed in Section 3.4 is that increasing the size of the field does not affect the number of field operations: therefore the increase in the number of binary operations in a larger field is polylogarithmic. This makes these algebraic approaches suitable for large fields, such as those that appear in the security assumptions behind QR-UOV [17].

3.4 Computing singular points using the bihomogeneous modeling

From a complexity perspective, we can obtain better bounds by considering the bihomogeneous system described in Equation (7). From a practical perspective, the improvement is significant. The results we rely on are described in detail in [24, Chapter 6] and [13].

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[1] 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 dehomogeneize 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 ideal. 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 [13, 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:

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

Remark 1. This formula is valid in the zero-dimensional case: using it to evaluate the cost of a hybrid approach is pessimistic.

We give in Figure 2 the estimated number of arithmetic operations required to solve the bihomogeneous system 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	370	256	419	558
d_{reg}	33	23	37	49

Fig. 2: Cost of the singular point attack via bihomogeneous modeling for UOV

3.5 Revisiting the Kipnis-Shamir attack [19]

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

[1] This kernel must but of dimension at least one by definition of a singular point, and of dimension no greater than one as the dimension of the determinatal ideal $\mathcal{J}_{m-2}$ of the $m - 1$ minors of the Jacobian from Theorem 1 is negative: $d = m - (n - (n - m - (m - 2)))(m - (m - 2)) = -4$ for $n = \frac{5}{2}m$.

rewriting the modeling:

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

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 $\sum_{i=1}^{m} y_i P_i$ 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 $M(\boldsymbol{y}) = \sum_{i=1}^{m} y_i P_i$.

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. For each singular point $\boldsymbol{x}$, there exists $q-1$ vectors $\boldsymbol{y} \in \ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$ as the rank defect of the Jacobian is only 1. Let $S = |\mathsf{Sing}(\mathbb{V}(I))|$ be the number of rational singular points of the UOV variety. This yields $(q-1)S$ valid choices of $\boldsymbol{y}$ out of q^m possibilities. We delay the estimation of S, and 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 canceled. 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_r 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 $\mathbb{F}_q[y]_{\leq 1}$ $O(mn^2)$
- Compute $\det(M(y))$, a determinant in $\mathbb{F}_q[y]$ $\tilde{O}(n^\omega)$
- 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 vanishes the quadratic system $O(\ell n^2)$

Denote ℓ the expected number of rational roots of a univariate polynomial Q of degree n in $\mathbb{F}_q$. By [15], if Q is square-free, we have:

$$\ell = \sum_{i=0}^{n-2} \left(-\frac{1}{q}\right)^i \leq 1$$

[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.

which tends to $\frac{q}{q+1}$ when n tends to infinity. We are interested in the roots of $\det(M(y))$, therefore if it is not square-free, we consider without loss of generality its square-free part, which has degree less than n. In this case, we still upper bound the expected number of rational roots ℓ by 1. This gives the following complexity for each guess:

$$O(mn^2)$$

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

$$C(q,n,m) = O(\frac{q^{m-1}}{S}mn^2) \tag{9}$$

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 combinations of public key matrices $M = \sum_{i=1}^{m-1} y_i P_i$.

Lemma 3. *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 $\chi_{P_m^{-1}M}$ be the characteristic polynomial of $P_m^{-1}M$.

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

Therefore:

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

In the previous section, we solved $\det(M-\lambda P_m)(y) = 0$ to compute y_r. 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 hypothesis is used in [18, Note above Theorem 4.2].

Hypothesis 2 *Among a collection of q^{n-2m} distinct linear maps of the form $P_j^{-1}M$, the 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 hypothesis allows for an estimate of S, such that Equation (9) matches the complexity of the Kipnis-Shamir attack:

$$C(q,n,m) = O(q^{n-2m}mn^2) \tag{10}$$

Note that in the litterature this cost is identified as $O(q^{n-2m}n^\omega)$ by neglicting the cost of summing m $n \times n$ square matrices, but this is a negligible difference for current UOV parameters.

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 two hypotheses used in the original Kipnis-Shamir attack of [18], and reproduce the experiments of [18] in low dimension in a new algebraic framework. This also shows that the Kipnis-Shamir attack fails when $n \geq 3m$ by Theorem 1.

We point out that the algebraic approach has an advantage over the Kipnis-Shamir attack: under Hypothesis 1, 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

VOX [7] 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 [12]. 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.

4.1 Definition of UOV$^{\hat{+}}$

We dismiss this additional structure for now, 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:

- $A \in GL_{o+v}(\mathbb{F}_q)$
- $\mathcal{S} = \begin{pmatrix} I_t & S' \\ 0 & I_{o-t} \end{pmatrix}, \quad S' \in \mathbb{F}_q^{(o-t)\times t}, S \in GL_o(\mathbb{F}_q)$
- $\mathcal{F} = (F_1, \ldots, F_o)$ a quadratic map with $F_i(\boldsymbol{e}_j) = 0$ for $i > t$ and $j \leq o$.
- $\mathcal{P} = S \circ \mathcal{F} \circ A$ 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 $(\hat{\mathcal{F}}, A), \hat{\mathcal{P}} = \hat{\mathcal{F}} \circ A$. These polynomials are called "oil polynomials" in analogy with "oil variables".

The "vinegar polynomials" are $p_1, \ldots, p_t$ and they define the vinegar variety $\mathbb{V}_t = \{\boldsymbol{x} \in \overline{\mathbb{F}_q}^n, p_1(\boldsymbol{x}) = \ldots = p_t(\boldsymbol{x}) = 0\}$.

Figure 3 includes the parameter sets submitted at NIST for VOX in [7], 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. 3: VOX parameters in [7] 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 vinegar 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. The choice of nearly-balanced parameters $o \approx v$ implies that singular point computations are significantly more efficient than in the case of UOV.

Theorem 2. *Let $\mathcal{P}$ be a UOV$^{\hat{+}}$ public key chosen uniformly at random for parameters (q, n, o, t) with $n > o$. Then the UOV$^{\hat{+}}$ variety $\mathbb{V}(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}_q}^n, \mathcal{P}(\boldsymbol{x}) = \mathbf{0}\}$ has a positive dimensional singular locus. More precisely, let $r \leq o - t$, $d' = 2o + r - n - 1$, $d = d' - t$:*

i. If $d' \geq 0$, the variety defined by r equations of the underlying UOV key has a singular locus of dimension d'.

ii. If $d \geq 0$, the variety defined by r equations of the UOV$^{\hat{+}}$ public key has a singular locus of dimension d.

Proof. We construct the Jacobian matrices of all intermediate keys to highlight the way the singular points of the secret key are mapped throughout the process. Let $\mathcal{F}' = (P_1 \circ A^{-1}, \ldots, P_t \circ A^{-1}, F_{t+1}, \ldots, F_o)$. Let $\boldsymbol{x} \in \mathcal{O}$ be a singular point of $\hat{\mathcal{F}}$, the underlying UOV secret key.
We obtain, as in Theorem 1, the shape of the secret UOV$^{\hat{+}}$ Jacobian:

$$\mathsf{Jac}_{\mathcal{F}'}(\boldsymbol{x}) = \begin{array}{c} \begin{matrix} 1 \ldots o & o+1 \ldots n \end{matrix} \\ \left[\begin{array}{cc} J_1(\boldsymbol{x}) & \\ 0 \ldots 0 & J_2(\boldsymbol{x}) \\ \vdots \quad \vdots & \\ 0 \ldots 0 & \end{array}\right] \end{array} \begin{matrix} 1 \\ \vdots \\ t \\ t+1 \\ \vdots \\ o \end{matrix}$$

Since $\boldsymbol{x}$ is a singular point of $\hat{\mathcal{F}}$, $J_2(\boldsymbol{x})$ has rank at most $o - t - 1$. Therefore, $\mathsf{Jac}_{\mathcal{F}'}(\boldsymbol{x})$ has rank at most $o - 1$. We move on to the next intermediate key, and deduce the Jacobian from the chain rule:

$$\mathcal{P}' = \mathcal{F}' \circ A$$

$$\mathsf{Jac}_{\mathcal{P}'}(\boldsymbol{y}) = \mathsf{Jac}_{\mathcal{F}'}(A\boldsymbol{y}) \cdot A \tag{11}$$

Notice that these operations cannot increase the rank of the Jacobian matrix, and that the right product with A acts on the columns of the Jacobian.

$$\mathsf{Jac}_{\mathcal{P}'}(\boldsymbol{y}) = \begin{array}{c} \begin{matrix} 1 \ldots o & o+1 \ldots n \end{matrix} \\ \left[\begin{array}{c} J_1(A\boldsymbol{y})A \\ J_2(A\boldsymbol{y})A \end{array}\right] \end{array} \begin{matrix} 1 \\ \vdots \\ t \\ t+1 \\ \vdots \\ o \end{matrix}$$

In particular, we have that $\mathsf{Jac}_{\mathcal{P}'}(A^{-1}\boldsymbol{x})$ has rank at most $o - 1$. Finally, we apply the linear map $\mathcal{S}$ to obtain the full UOV$^{\hat{+}}$ public key, again with the chain rule.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{P}'$$

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{y}) = \mathcal{S} \cdot \mathsf{Jac}_{\mathcal{P}'}(\boldsymbol{y}) \tag{12}$$

Again, this left product cannot increase the rank of the matrix.

$$\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{y}) = \begin{array}{c} \begin{matrix} 1 \dots o & o+1 \dots n \end{matrix} \\ \left[\begin{array}{cc} J_1(A\boldsymbol{y})A & \\ (\mathcal{S}'J_1 + J_2)(A\boldsymbol{y})A & \end{array}\right] \end{array} \begin{matrix} 1 \\ \vdots \\ t \\ t+1 \\ \vdots \\ o \end{matrix}$$

Since the rank may not increase at any step, singular points of the underlying UOV key drop the rank of the UOV$^{\hat{+}}$ public Jacobian.

$$\mathsf{rank}(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x})) \leq \mathsf{rank}(\mathsf{Jac}_{\hat{\mathcal{P}}}(\boldsymbol{x})) + t$$

In particular, if $A^{-1}\boldsymbol{x}$ also vanishes the vinegar polynomials, then $A^{-1}\boldsymbol{x}$ is a singular point of the full UOV$^{\hat{+}}$ public key. We give the dimension estimates below.

i. Let $\mathcal{J}_r$ be the ideal generated by $(\hat{\mathcal{P}}(\boldsymbol{x}), \mathsf{Minors}_r(\mathsf{Jac}_{\hat{\mathcal{P}}}(\boldsymbol{x})))$. By construction, $\hat{\mathcal{P}}$ is a truncated UOV public key with r equations which vanish on the linear subspace $\mathcal{O}$ of dimension o. By Theorem 1, we have:

$$d' = \dim \mathcal{J}_r = 2o + r - n - 1$$

ii. Since $p_1(\boldsymbol{x}), \dots, p_t(\boldsymbol{x})$ are random quadratic equations, we can assume they define generic hypersurfaces, and the ideal $\mathcal{J}_r + \langle p_1(\boldsymbol{x}), \dots, p_t(\boldsymbol{x})\rangle$ has dimension $\dim(\mathcal{J}_r) - t$. Notice that by the previous observations, if $\boldsymbol{x}$ is a singular point of the underlying UOV key, then the Jacobian of the UOV$^{\hat{+}}$ public system is also rank deficient. Therefore, if $\boldsymbol{x}$ is singular for the underlying UOV key and $\boldsymbol{x} \in \mathbb{V}_t$, then $\mathcal{P}(\boldsymbol{x}) = 0$ and therefore $\boldsymbol{x}$ is singular for the UOV$^{\hat{+}}$ public system.

□

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}. This assumption allows VOX and UOV$^{\hat{+}}$ to use UOV parameters that would otherwise be weak to key recovery attacks.

In Theorem 2, we show that this estimate is optimistic: we target the partial UOV key by computing singular points of the UOV$^{\hat{+}}$ key without knowing $\mathcal{S}$, since the singular locus of the partial key generically intersects the vinegar variety if the quantity d' is non-negative. In light of Section 3.5, 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 use Equation (9), which predicts the cost of the Kipnis-Shamir attack interpreted as an enumerative singular point computation, along with Hypothesis 2 to estimate the number of rational singular points. We have $\dim \mathsf{Sing}\mathbb{V}(I) = 3o - n - 1 - t$, therefore we have the following cost for the Kipnis-Shamir attack against $\text{UOV}^{\hat{+}}$:

$$C(q, n, o, t) = O(q^{n-2o+t} o n^2) \tag{13}$$

This cost was previously identified as $O\left(q^{n-2o+2t} n^{\omega}\right)$ in [12], [7], which we improve by a factor q^t.

We give below $\log_2$(field operations) estimates, using $\omega = 2.81$. We add the previous best attacks that target $\text{UOV}^{\hat{+}}$ and the Full VOX key, as described in [12], [7]. Multiplication cost is taken to be $2\log(q)^2 + \log(q)$ gates. In [7], costs were given in number of arithmetic operations, therefore we use the previous cost to convert to gate counts, as per NIST methodology.

Security level	143	207	272
Parameters	I	III	V
$\log_2$ gates	**121**	**167**	**221**
Previous	142	206	280

Fig. 4: Computational cost of our version of the Kipnis-Shamir attack on VOX parameters submitted to NIST [7].

We consider the cost of the attack on the original $\text{UOV}^{\hat{+}}$ parameters. This scheme is not concerned by the rectangular MinRank attack of [16]. As this paper was used as a foundation for VOX, it is not surprising that the cost is almost equal.

Security level (λ)	143 (128)	207 (192)	272 (256)
Parameters (q, o, v, t)	$(2^6, 48, 56, 8)$	$(2^9, 64, 72, 8)$	$(2^{12}, 88, 96, 8)$
$\log_2$ ops	**120**	**171**	**221**

Fig. 5: Computational cost of our version of the Kipnis-Shamir attack on $\text{UOV}^{\hat{+}}$ [12].

New parameters for VOX have been proposed in [21], to protect the QR transform used in the scheme. We give an analysis of our attack against these parameters in Figure 6.

Security level	143			207			272		
Parameters	Ia	Ib	Ic	IIIa	IIIb	IIIc	Va	Vb	Vc
$\log_2$ ops	177	161	**145**	248	228	**208**	329	293	**281**
Previous	145	151	150	209	219	215	287	276	293

Fig. 6: Computational cost of our version of the Kipnis-Shamir attack for VOX parameters proposed in [21].

In the next section, we show how to recover the rest of the secret key using a single secret vector. This will also highlight a method to lower the complexity of attacks against $\hat{\text{UOV}}$ independently of improvements to the Kipnis-Shamir attack against UOV.

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

Once we have obtained a vector in $\mathcal{O}$, we wish to complete a full key recovery attack. A polynomial-time key recovery from one vector against UOV is introduced in [23], by studying the kernel of the Jacobian of the system evaluated on an element of the secret subspace. In [23, Section 4], these tools are applied to VOX, interpreted as $\hat{\text{UOV}}$: 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 $\hat{\text{UOV}}$ without inverting $\mathcal{S}$, and thus show how to perform a key recovery against $\hat{\text{UOV}}$ and VOX using a single oil vector.

Lemma 4. *Let $\mathcal{P} = (P_1, \dots, P_m)$ be a $\hat{\text{UOV}}$ public key for parameters (q, o, v, t), let $\mathcal{O}$ be the associated UOV secret subspace, let $\mathbb{V}_t = \{\boldsymbol{x} \in \mathbb{F}_q, p_1(\boldsymbol{x}) = \ldots = p_t(\boldsymbol{x})\}$ be the vinegar variety of $\mathcal{P}$. 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 $o - t$. 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, and let $\boldsymbol{x} \in \mathcal{O}$. Then there exists an algorithm taking as input $\boldsymbol{x}$ and $\mathcal{P}$ and outputting a basis of $\mathcal{O}$, using at most $O\left(q^t(n-o)^\omega\right)$ 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. We assume that $\boldsymbol{x}$ is singular. Indeed, when $\boldsymbol{x}$ is not singular, the dimension becomes $n - o$ 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.

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

We also define the restriction of the underlying UOV key for clarity:

$$\hat{P}_{i|B} := B^T \cdot \hat{P}_i \cdot B \text{ for } t+1 \leq i \leq o$$

The collection $P_{|B} = (P_{1|B}, \ldots, P_{o|B})$ can be considered as the 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 4. Notice that $\hat{P}_{|B}$, the underlying UOV key, is composed only of singular matrices as $n - o + 1 < 2(o - t)$, using Lemma 2. In particular, as observed in [23], the UOV matrices $\hat{P}_{i|B}$ have rank $r = 2 \cdot (n - 2o + t + 1)$, which is significantly lower than $n - o + 1$ for all proposed parameter sets.

Therefore, once this restriction has been computed, the attacker may determine $(s_{i,j})_j$ for any fixed i by solving a MinRank instance:

$$\mathsf{rank}(P_{i|B} + \sum_{j=1}^{t} s_{i,j} P_{j|B}) \leq 2(n - 2o + t + 1)$$

Denote $M(\boldsymbol{s}) = P_{i|B} + \sum_{j=1}^{t} s_{i,j} P_{j|B}$. This MinRank instance has t variables over a matrix of dimension $n' \times n'$ and a target rank $r = 2 \cdot (n - 2o + t + 1)$.

If we solve this instance by enumerating all values of $(s_{i,j})_{1 \leq j \leq t}$, the cost is $q^t(n - o + 1)^\omega$, which achieves the announced upper bound.

Once we have found one collection $(s_{i,j})_{1 \leq j \leq t}$ for some i, we obtain $\hat{P}_{i|B}$, and the kernel of $\hat{P}_{i|B}$ has dimension $n - o + 1 - 2(n - 2o + t + 1) = 3o - n - 2t$ and

is entirely included in $\mathcal{O}$. This value is greater than t, and therefore this yields a free family of vectors of $\mathcal{O}$ that allows to retrieve $\mathcal{S}$ using the method presented in [23], and therefore yields the remaining vectors required to form a basis of $\mathcal{O}$ in polynomial time.

Let us look at the complexity of this process:

1. Compute B a basis of $\ker(\mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}))$	$O(n^\omega)$
2. Compute $P_{t+1\|B}$	$O(n^\omega)$
3. Find $(s_{t+1,j})_{1\leq j\leq t}$	$O(q^t n'^\omega)$
4. Invert $\mathcal{S}$	$O(n^\omega)$
5. Retrieve $\mathcal{O}$	$O(n^\omega)$

The total cost is dominated by $O\left(q^t(n-o)n'^\omega\right)$. □

Notice that the MinRank instance presented in the proof of Theorem 3 is solved very naively. Let $T(q,n,o,t)$ be the cost of solving this MinRank instance. This work provides the upper bound $T(q,n,o,t) < q^t(n-o+1)^\omega$. Notice that this yields a test "$\boldsymbol{x} \in \mathcal{O}$?" with the same complexity: if there exists $t+1 \leq i \leq o$ such that no family $(s_{i,j})_j$ can be found, then $x \notin \mathcal{O}$, otherwise $\boldsymbol{x} \in \mathcal{O}$.

For larger field sizes, we may improve the complexity by solving this MinRank instance using a Gröbner basis approach.

4.4 Combining singular point computations with "$\boldsymbol{x} \in \mathcal{O}$?"

By combining our study of the singular points from Section 4.2 with the one vector key recovery from Section 4.3, we can obtain a novel attack on UOV$^{\hat{+}}$ and VOX.

The Kipnis-Shamir attack computes vectors that drop the rank of the Jacobian of a UOV public key among eigenvector 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$^{\hat{+}}$, vectors of $\mathcal{O}$ do not vanish the public key equations. Therefore, we may replace this step of the attack by using the key recovery from one vector (Theorem 3) as a test "$\boldsymbol{x} \in \mathcal{O}$?". In this case, we pay a factor $T(q,n,o,t)$ for each point computed: these points are among the points that drop the rank of the public Jacobian by Theorem 2. This yields a more obvious separation between the cost of attacking the $\hat{+}$ transformation versus the security of the underlying UOV key:

$$O\left(q^{n-2o}on^2 \times T(q,n,o,t)\right)$$

The first part of the formula corresponds to the security of UOV against the Kipnis-Shamir attack, while the second part is the cost of solving a MinRank instance that is related to the $\hat{+}$ transform. Compared with the Kipnis-Shamir attack described in Section 4.2, this is only worse by a polynomial factor $(n-o+1)^\omega$ using the algorithm introduced in Section 4.3. Any improvement to the key recovery from one vector would yield improved complexity for this attack.

4.5 Consequences for UOV$^{\hat{+}}$ and VOX

We have shown that the hat plus structure only improves the security of UOV by a factor at most q^t asymptotically against the Kipnis-Shamir attack, as opposed to the factor q^{2t} claimed in [7]. The new VOX parameters introduced in [21] for VOX increase the value c, which is directly equal to $n - 2o$, compared with the previous parameter sets. Therefore, even though this change was made to protect the QR transform, it significantly improves the security of the scheme against our attacks as well.

5 Experimental results

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.

Dimension of the singular locus

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 dehomogeneize 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. This is not entirely equivalent to setting d variables to arbitrary values, as in doing so one assumes that there exists a rational solution with these specific coordinates.

This is essential in our case, as singular points are not always rational, but their existence (in an extension) will always allow to mount an algebraic attack against the scheme. This means that in cases where there are no rational singular points, the Kipnis-Shamir attack will fail, while our attacks will not. We demonstrate this property using the Gröbner bases computed in our experiments.

We can study experimentally the degree and dimension of the 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.

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:

$$\boldsymbol{x} \in \mathbb{F}_q^n, x_1 = 1, \boldsymbol{y} \in \mathbb{F}_q^m, y_1 = 1 \begin{cases} \mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^m \\ \boldsymbol{y}^T \mathsf{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \in \mathbb{F}_q^n \\ f(\boldsymbol{x}) = 0 \in \mathbb{F}_q^d \end{cases} \tag{14}$$

The dimensions obtained experimentally match Theorem 1. In every case, the Gröbner basis contains exactly $n - m$ linear polynomials defining $\mathcal{O}$, which supports Hypothesis 1.

We list in Figure 7 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. 7: Experimental computation of Gröbner bases for bihomogeneous modelisations of the singularities of UOV systems in $\mathbb{F}_{251}$.

Acknowledgements

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

References

1. Berthomieu, J., Bostan, A., Ferguson, A., Safey El Din, M.: Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems. Journal of Algebra **602**, 154–180 (2022). https://doi.org/https://doi.org/10.1016/j.jalgebra.2022.03.002

2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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)
9. 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
10. 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
11. Faugère, J.C., Bardet, M., Salvy, B.: On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations (2004)
12. Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L.: A new perturbation for multivariate public key schemes such as hfe and uov. Cryptology ePrint Archive, Paper 2022/203 (2022), https://eprint.iacr.org/2022/203
13. 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

14. 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
15. Fulman, J.: A generating function approach to counting theorems for square-free polynomials and maximal tori. Annals of Combinatorics **20**(3), 587–599 (Sep 2016). https://doi.org/10.1007/s00026-016-0310-4, https://doi.org/10.1007/s00026-016-0310-4
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 uov schemes. Cryptology ePrint Archive, Paper 2023/1131 (2023), https://eprint.iacr.org/2023/1131
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. 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