

Genericity in multivariate cryptography

Simon Abelard^{1,3}, Pierre Pébère², and Mohab Safey El Din³

¹ LRE, EPITA, 14 rue Voltaire, Le Kremlin-Bicêtre, 94270, France

² COSIC, KU Leuven

³ Sorbonne Université, LIP6, CNRS

Abstract. The results in this paper establish the genericity of some properties of the ideals and varieties generated by UOV public keys, in particular the equidimensionality of the UOV varieties and the radicality of public key ideals. These genericity results justify the various regularity assumptions that are made on polynomial systems of equations arising in the cryptanalysis of UOV and its variants. We also provide examples in the recent literature showing how genericity questions arise in cryptanalysis and why genericity should be taken into consideration when designing cryptographic schemes. Lastly, we perform a retrospective study of various cryptographic schemes through the viewangle of genericity. We identify several cases in which non-genericity led to the cryptanalysis of the scheme, but also provide a counter-example of a scheme whose non-genericity does not seem easy to exploit.

1 Introduction

With the advent of post-quantum cryptography, algebraic geometry has taken an increasingly important part in the design and analysis of cryptographic schemes. One reason is the need for new mathematical problems that would remain hard even for quantum computers, one of them being the resolution of systems of quadratic equations – the groundstone of *multivariate cryptography*. Techniques and results from algebraic geometry are also increasingly popular to attack cryptographic schemes beyond the multivariate setting. One can thus mention algebraic attacks against code-based cryptography, isogeny-based cryptography and lattice-based cryptography, that form such an extensive literature that we only provide one reference per family [1,60,27] for the sake of brevity. In this paper, we discuss genericity, another well-known concept in the field of algebraic geometry, and show how and why it should be part of the cryptographic toolbox.

In multivariate cryptography, public keys are families of equations and can therefore be seen as algebraic varieties. For security reasons, it is crucial that such varieties are indistinguishable from randomly-generated varieties. Through the lens of genericity, we address this point by showing that certain properties of UOV systems are indeed generic in the sense of the Zariski topology.

In cryptanalysis, the so-called algebraic attacks ultimately rely on the resolution of systems of polynomial equations. Estimating the complexity of solving such systems is generally not a simple task and many of the tools used by the

community actually rely on genericity assumptions. Some of these assumptions are required to ensure that the attack can be performed: for instance, some solving techniques like the geometric resolution algorithm [37] require the input system to satisfy some technical properties and some attacks rely on mathematical objects that can only be defined under some assumptions. A recent example can be found in [51,50], where the cryptanalytic use of tangent spaces requires the UOV variety to be equidimensional and the corresponding ideal to be radical.

Of equal importance is the case where genericity is required to ensure that its complexity is accurately estimated. A first example is that the sequence of polynomials in a UOV public key must be a regular sequence, otherwise the complexity analysis of the direct forgery attack against UOV fails. More involved assumptions must be made for more sophisticated attacks, for instance the semi-regularity of the sequences of polynomials arising in the Intersection attack [6], the absence of false positives in the Kipnis-Shamir attack [42], the precise Hilbert series obtained in the different modelings of the MinRank problem [6,8,33], etc.

The tools introduced in this paper intend to partially solve the issue of relying on heuristics that can be hard to verify experimentally, by proving that these regularity properties hold for UOV keys belonging to non-empty Zariski open subsets of quadratic polynomial sequences. Genericity, however, can be seen as an asymptotic statement: a generic property will hold with overwhelming probability when n (the number of variables) or q (the size of the base field) are large enough. In cryptography, the parameters are fixed so we have performed experiments with small parameters, and have noted that our generic properties still hold most of the time. For more details, we refer the reader to Section 6.

1.1 Related work

Regularity assumptions in cryptographic design. Assessing the complexity of classical algorithms for solving polynomial systems is both a difficult and essential task in cryptography, as it dictates the choice of practical parameters (i.e. number of equations and variables). In order to use existing complexity results, the community often assumes that polynomial systems obtained from multivariate keys are regular as in [16], which also motivates experimental work supporting such assumption [29]. The security analysis and parameter choices of the UOV NIST submission [11] rely on both the fact that UOV systems form regular sequences and on Fröberg’s conjecture, but such assumptions can also be found outside of the realm of multivariate cryptography, see for instance the work of Diem [24] on XL, motivated by algebraic attacks against ECDLP.

These regularity assumptions still remain essential to the complexity analyses of more recent attacks, as illustrated by the wedge attack of Ran [53, Conjecture 1], by the Extended MinRank attack of Furue and Ikematsu [33, Section 4.3] and by the Jacobian framework of [59, Hyp 12, Heuristic 20].

Heuristics in cryptanalysis. While regularity is required for assessing their cost, more subtle assumptions can be required to ensure the validity of some attacks. In this paper, we mostly deal with assumptions related to singular points and

tangent spaces. Such assumptions are at the heart of both new attacks [59,51,50] and less recent ones [42].

Genericity and the security of cryptographic schemes. In [36], Gaggero and Gorla define and study Zariski-open sets of polynomial systems of a given degree over finite fields which verify regularity properties in some degrees, a weaker property than semi-regularity which enables the authors to provide upper bounds for the degree of regularity. However, in the literature on UOV, the stronger notion of semi-regularity is used in order to obtain tighter bounds. Proving the non-emptiness of the Zariski-open set of semi-regular UOV sequences would solve the Fröberg conjecture [32,48] for the corresponding parameter regimes.

When designing multivariate schemes, it is essential to consider how easily their public keys could be distinguished from randomly-generated systems. In UOV, one can wonder to what extent the existence of the oil space makes public keys stand out. While this question does not seem to appear in the cryptographic community, it has been addressed by the work of Debarre and Manivel [22] who –among other things– answered the following question: how unusual is it for m quadratic forms to vanish on a common o -dimensional linear space?

Another important question for security is the possible existence of weak keys, i.e. a subset of multivariate keys resulting in polynomial systems that would happen to be much easier to solve. Such keys must be dealt with by either detecting them and re-running the key generation process, or by ensuring that they only occur with a tiny probability. When this is not done, this can lead to attacks such as the one of Beullens against SNOVA [9]. Our genericity-based framework also captures these phenomena as the weak keys identified by Beullens all live in Zariski-closed sets. This, in particular, shows that genericity does not always suffice to ensure security: those weak keys are non-generic but they still occur with a non-negligible probability.

1.2 Main results

In Theorems 1 and 2, we respectively show that the set of UOV keys whose Jacobian matrix has full rank outside of the oil space is open for the Zariski topology and that it is not empty, thus showing that this property is Zariski generic. Note that these results were already proven over finite fields of sufficiently large characteristic in [51]. In this paper, we used a different approach to make the proofs simpler and valid regardless of the size of the field. This is particularly relevant in multivariate cryptography where relatively small fields are used (e.g. $\mathbb{F}_{16}$).

Building upon this, we show in Theorem 3 that the equations defining a generic UOV key form a radical ideal and generate an equidimensional variety. We show in Corollary 1 that this implies that the corresponding public keys form regular sequences.

Theorem 4 computes the dimension of a determinantal ideal associated to generic UOV keys. As already mentioned, the consequences of these theorems are double: they support complexity estimates and prove that common heuristics used in cryptanalysis hold generically (see in particular [53,59,51,50,33,11,12,42]).

The fact that our theorems apply to such a large part of the literature supports our opinion that genericity can be a powerful tool for cryptologists.

1.3 Organization of the paper

In Section 2.3, we define a notion of genericity over the set of UOV keys based on the Zariski topology. We begin the study of regularity assumptions on UOV polynomial systems of equations with a study of the points that induce a rank defect in the Jacobian matrices of UOV systems, in Section 3.

This enables us to prove in Section 4 the genericity of properties that are almost always required in the analysis of UOV systems, namely that the polynomial sequence $p_1, \dots, p_m$ defined by a UOV public key generates a radical ideal and an equidimensional variety. In Section 5, we study the determinantal ideals of the UOV Jacobian matrices in more detail, showing that the rank defect of the Jacobian matrix of a UOV key at any singular point is generically 1. This property allows us to prove many heuristics essential to both MinRank attacks and tangent space approaches.

Section 6 provides experimental results showing that our generic properties are indeed satisfied with high probability, even over small fields. In Section 7, we show the relevance of genericity in cryptography, highlighting how the results from the previous sections can remove heuristics required by well-known attacks against multivariate schemes. We also identify several attacks that could have been anticipated by studying the genericity of keys, but we also produce a false-positive case in which non-genericity does not seem to weaken the scheme.

2 Ideal, varieties and genericity

2.1 Ideals and varieties

We recall some elementary notions related to polynomial systems and their solutions. For more details on this topic, we refer the reader to [21].

Let $\mathbb{K}$ be a field, and let $p_1, \dots, p_m$ be polynomials in $\mathbb{K}[X_1, \dots, X_n]$. The *ideal* of $\mathbb{K}[X_1, \dots, X_n]$ generated by $p_1, \dots, p_m$ is the set

$$\langle p_1, \dots, p_m \rangle := \left\{ \sum_{1 \leq i \leq m} a_i p_i, \quad a_i \in \mathbb{K}[X_1, \dots, X_n] \right\}.$$

The *radical* of an ideal $\mathcal{I}$ is the ideal

$$\sqrt{\mathcal{I}} := \{f \in \mathbb{K}[X_1, \dots, X_n] \mid \exists k \in \mathbb{N}, f^k \in \mathcal{I}\}.$$

An ideal $\mathcal{I}$ is *radical* if $\mathcal{I} = \sqrt{\mathcal{I}}$. A sequence of polynomials $(p_1, \dots, p_m)$ is a *regular sequence* if for $2 \leq i \leq m$, p_i does not divide 0 in $\mathbb{K}[X_1, \dots, X_n]/\langle p_1, \dots, p_{i-1} \rangle$.

Let $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. A point $\mathbf{x} \in \overline{\mathbb{K}}^n$ is a solution of $p_1 = \dots = p_m = 0$ if and only if it cancels all polynomials in $\langle p_1, \dots, p_m \rangle$. Thus, the set of

solutions of a polynomial system is defined with respect to the ideal generated by the polynomials, and called an algebraic set or algebraic variety. The *algebraic variety* defined by an ideal $\mathcal{I}$ is denoted by $V(\mathcal{I}) := \{\mathbf{x} \in \overline{\mathbb{K}}^n, \forall f \in \mathcal{I}, f(\mathbf{x}) = 0\}$. Conversely, the set of ideals that vanish on a given set of points V is denoted by $I(V)$. By Hilbert's Nullstellensatz (see [65, Volume 2, p. 164]), it holds that $I(V(\mathcal{I})) = \sqrt{\mathcal{I}}$. The *dimension* of a variety $V(\mathcal{I})$ is the Krull dimension of the quotient ring $\mathbb{K}[X_1, \dots, X_n]/\mathcal{I}$. Recall that all algebraic varieties admit a minimal decomposition into irreducible varieties which are called irreducible components. A variety is *equidimensional* if all its irreducible components have the same dimension. A variety V is a *complete intersection* if $I(V)$ is generated by $\text{codim} V = n - \dim V$ elements.

The degree of an equidimensional variety V of dimension d is the maximum number of points of the intersection of V with d hyperplanes, provided that this intersection is finite. The degree of an algebraic variety of dimension d is the sum of the degrees of its irreducible components of dimension d . The strong degree of an algebraic variety is the sum of the degrees of its irreducible components.

2.2 Zariski topology

Our goal in this paper is to adapt the classical notion of *genericity* in algebraic geometry based on the Zariski topology to the set of UOV keys. The closed sets of the Zariski topology over some affine space $\overline{\mathbb{K}}^n$ (where $\overline{\mathbb{K}}$ is an algebraically closed field) are algebraic varieties, and a property depending on some parameters chosen in $\mathbb{K}^n$ is said to be *Zariski generic* if it holds on a non-empty Zariski open set of $\overline{\mathbb{K}}^n$.

We start by recalling some basic facts from e.g. [21, Chapter 4]. Let $\mathcal{I}, \mathcal{J}$ be two radical ideals.

- The empty set is the variety defined by the ideal $\langle 1 \rangle$.
- The full space $\overline{\mathbb{K}}^n$ is the variety defined by the ideal $\langle 0 \rangle$.
- The intersection of a collection of varieties is a variety:

$$V(\mathcal{I}) \cap V(\mathcal{J}) = V(\mathcal{I} + \mathcal{J}).$$

- The (finite) union of varieties is a variety:

$$V(\mathcal{I}) \cup V(\mathcal{J}) = V(\mathcal{I} \cap \mathcal{J}).$$

Therefore one can define a topology on $\overline{\mathbb{K}}^n$, where the closed sets are algebraic varieties. It is known as the *Zariski topology*. As in the usual topology, a Zariski open set is the complement of a Zariski closed set.

We often apply this topology to sequences of polynomials with prescribed degrees by considering their coefficients as indeterminates. We say that a property holds for a *generic sequence of polynomials of prescribed degree at most d* if that property holds for all polynomial sequences in a non-empty Zariski open subset of the vector space of all polynomial sequences of degree at most d .

2.3 Generic UOV maps

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be its algebraic closure. The goal of this section is to define a notion of genericity for UOV keys. To this end, we first define UOV keys and *generic private UOV keys*, i.e. UOV keys whose coordinates are undetermined. Such keys can be seen as m -uples of homogeneous quadratic polynomials whose coefficients lie in $\mathbb{K}[\mathbf{a}, \mathbf{b}]$, where $\mathbf{a} = (\mathbf{a}_{i,j}^{(k)})_{i,j,k}$ and $\mathbf{b} = (\mathbf{b}_{i,j}^{(k)})_{i,j,k}$ respectively corresponds to the coefficients of the oil and vinegar terms of f_k . In this setup, a property of UOV keys is generic if it holds when a system of polynomial equations in the variables $\mathbf{a}$ and $\mathbf{b}$ is *not* satisfied.

Definition 1 (Algebraic description of UOV [42]). A UOV key pair for parameters (n, m, o) over the field $\mathbb{K}$ is composed of a secret key $(A, \mathcal{F})$ and a public key $\mathcal{P}$, where:

- $A \in GL_n(\mathbb{K})$, which defines an invertible linear map from $\mathbb{K}^n$ to $\mathbb{K}^n$.
- $\mathcal{F}$ is a quadratic map defined by coefficients $(f_{i,j})_{\substack{o < i \leq n \\ 1 \leq j \leq n}} \in \mathbb{K}^{n-o \times n}$:

$$\begin{aligned} \mathcal{F} : \overline{\mathbb{K}}^n &\rightarrow \overline{\mathbb{K}}^m \\ \mathbf{x} &\mapsto \mathcal{F}(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_m(\mathbf{x})) \end{aligned}$$

where, for all $1 \leq k \leq m$,

$$f_k(\mathbf{x}) = \sum_{o < i \leq n} \sum_{1 \leq j \leq n} f_{i,j}^{(k)} x_i x_j.$$

- $\mathcal{P} = \mathcal{F} \circ A$.

When $\mathbb{K}$ is the field $\mathbb{F}_q$ (where q is the power of a prime), we also say that such a UOV key pair is for (n, m, o, q) .

Note that in the original definition of UOV [42], it holds that $o = m$. However, there are variants of UOV where $o \neq m$. We are also interested in the geometric characterization, which is due to Kipnis and Shamir [43].

Definition 2 (Geometric UOV trapdoor [43]). A UOV public key for parameters (n, m, o) over the field $\mathbb{K}$ is a quadratic map $\mathcal{P} : \overline{\mathbb{K}}^n \rightarrow \overline{\mathbb{K}}^m$ defined by $(p_1, \dots, p_m) \subset \mathbb{K}[X_1, \dots, X_n]$ such that there exists a linear subspace $\mathcal{O}$ of dimension o such that $\mathcal{P}(\mathcal{O}) = \{0\}$. In other words,

$$\mathcal{O} \subset V(\langle p_1, \dots, p_m \rangle). \quad (1)$$

Denote by $\mathbb{K}[X_1, \dots, X_n]_2$ the set of homogeneous quadratic polynomials over a field $\mathbb{K}$ of dimension $N = \binom{n+1}{2}$. Hence, the coefficients of those quadratic maps $\mathcal{P}$ defining UOV public keys lie in $\overline{\mathbb{K}}^{mN}$ (we usually take them in $\mathbb{K}^{mN}$).

Definition 3. Let (n, m, o) be positive integers, with $n \geq 2o$ and let $\mathbb{K}$ be a field. The set of UOV public keys for parameters (n, m, o) is denoted by $\mathcal{K}_{n,m,o,\mathbb{K}}$.

When $\mathbb{K}$ is the field $\mathbb{F}_q$ (with q being a power of p), this is denoted by $\mathcal{K}_{n,m,o,q}$. We have $\mathcal{K}_{n,m,o,\mathbb{K}} \subset (\overline{\mathbb{K}}[X_1, \dots, X_n]_2)^m$ which is a finite dimensional vector space. Therefore, we can define a topology over $\mathcal{K}_{n,m,o,\mathbb{K}}$ which is induced by the Zariski topology over $(\overline{\mathbb{K}}[X_1, \dots, X_n]_2)^m$.

Although it is tempting to use only the geometric characterization for conciseness, using the algebraic point of view greatly simplifies our proofs. Thus, we now define the generic UOV secret key for parameters (n, m, o) . By Definition 1, there is a bijection between a UOV public key and the corresponding UOV secret key. Hence, we can prove genericity results on the set of UOV secret keys, which yield genericity results on the set of UOV public keys.

Definition 4 ([51, Definition 3.2]). *Let (n, m, o) be positive integers, $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. Let $O = [1, \dots, o]$, $V = [o + 1, \dots, n]$ the indices of oil (resp. vinegar) variables in the UOV secret key. Define*

$$d = m \left(o(n - o) + \frac{(n - o)(n - o + 1)}{2} \right).$$

The generic UOV secret map for parameters (n, m, o) over a field $\mathbb{K}$ is the polynomial map

$$\begin{aligned} \Phi : \overline{\mathbb{K}}^n \times \overline{\mathbb{K}}^d &\rightarrow \overline{\mathbb{K}}^m \\ \mathbf{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta}) &\mapsto (\Phi^{(1)}(\mathbf{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta})), \dots, \Phi^{(m)}(\mathbf{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta}))) \end{aligned}$$

where for $1 \leq k \leq m$,

$$\Phi^{(k)}(\mathbf{x}, (\boldsymbol{\alpha}, \boldsymbol{\beta})) = \underbrace{\sum_{i \in O, j \in V} \alpha_{i,j}^{(k)} x_i x_j}_{\text{Oil terms}} + \underbrace{\sum_{i \in V, j \in V} \beta_{i,j}^{(k)} x_i x_j}_{\text{Vinegar terms}}. \quad (2)$$

A UOV secret map over $\mathbb{K}$ is obtained by evaluating Φ on $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{K}^d$:

$$\Phi_\theta : \mathbf{x} \mapsto \Phi(\mathbf{x}, \theta).$$

Further, we endow the coordinates of $\overline{\mathbb{K}}^d$ with the variables $\mathbf{a}_{i,j}^{(k)}$ with $i \in O, j \in V, 1 \leq k \leq m$ and $\mathbf{b}_{i,j}^{(k)}$ for $i \in V, j \in V$ and $1 \leq k \leq m$. Such sequences of variables are denoted by $\mathbf{a}$ and $\mathbf{b}$ in the sequel.

3 Generic smoothness

The goal of this section is to construct a Zariski open set of the set of UOV keys where the Jacobian matrix of the public key is full rank outside of the secret subspace $\mathcal{O}$. As a consequence, we are able to show that any such UOV key generates a radical ideal and an equidimensional variety, allowing us to use simpler definitions for the tangent spaces at UOV varieties.

Note that UOV keys are by design homogeneous, thus the point $(0, \dots, 0) \in \mathbb{K}^n$ is both a point of the affine variety and a point at which the Jacobian matrix has rank 0. Affine varieties are not appropriate for the study of homogeneous ideals so we consider the projective variety, which excludes the zero point.

In [51], a non-empty Zariski open set is obtained in large enough prime fields by applying an algebraic version of Thom's weak transversality theorem (see [56, Appendix B]). In this paper, we improve this construction and prove the same statement *for any finite field* by first constructing a Zariski open set in Theorem 1 below, and then delegating the work of proving its non-emptiness in any finite field to Theorem 2.

As above, we let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$.

Given a sequence of polynomials, say $\mathbf{f} = (f_1, \dots, f_p)$ in $\mathbb{K}[Y_1, \dots, Y_N]$, we denote by $\text{Jac}(\mathbf{f})$ the Jacobian matrix:

$$\begin{bmatrix} \frac{\partial f_1}{\partial Y_1} & \dots & \frac{\partial f_1}{\partial Y_N} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial Y_1} & \dots & \frac{\partial f_p}{\partial Y_N} \end{bmatrix}.$$

Given $\mathbf{y}$ in $\mathbb{L}^n$ where $\mathbb{L} \supset \mathbb{K}$ is a field, we denote by $\text{Jac}_{\mathbf{y}}(\mathbf{f})$ the evaluation of $\text{Jac}(\mathbf{f})$ at $\mathbf{y}$. Finally, given a subsequence $\mathbf{Y} = (Y_{i_1}, \dots, Y_{i_\ell})$ of the sequence of variables $(Y_1, \dots, Y_N)$, we denote by $\text{Jac}(\mathbf{f}, \mathbf{Y})$ the submatrix of the Jacobian matrix $\text{Jac}(\mathbf{f})$ obtained by keeping only the columns corresponding to the partial derivatives with respect to Y_i for $i \in \{i_1, \dots, i_\ell\}$.

We rely on classical notions at the interplay of transversality theory and algebraic geometry, which we briefly recall hereafter. More details can be found in [56, Appendix B]. Let $V \subset \overline{\mathbb{K}}^n$ be an equidimensional algebraic variety of co-dimension c , $\mathbf{f}$ be a system of generators of the ideal associated to V and $\varphi : x \in V \rightarrow (\varphi_1(x), \dots, \varphi_m(x)) \in \overline{\mathbb{K}}^m$ be a polynomial map. We say that a point $x \in V$ is non-singular if and only if $\text{rank}(\text{Jac}_x(\mathcal{P})) = \text{codim}(V)$. If this does not hold, we say that x is a singular point of V . We say that $\mathbf{0} \in \overline{\mathbb{K}}^m$ is a *regular* value of φ if the Jacobian matrix associated to $\mathbf{f}, \varphi_1, \dots, \varphi_m$ has full rank at any point of $x \in V$ such that $\varphi(x) = \mathbf{0}$. This definition extends to any Zariski open subset U of V : we say that $\mathbf{0}$ is a regular value for such a restriction, if at any point of U , the aforementioned Jacobian matrix is full rank.

Finally, we say that a point x in V is a critical point of the polynomial map φ if $\text{Jac}_x(\mathbf{f})$ has rank c and $\text{Jac}_x(\mathbf{f}, \varphi_1, \dots, \varphi_m)$ has rank less than $c + m$. The image of such a critical point by φ is a critical value of φ .

Theorem 1. *Consider UOV parameters (n, m, o) over a field $\mathbb{K}$ with $n \geq m$ and $n > o$. There exists a Zariski open set $\mathcal{U}_{n,m,o,\mathbb{K}} \subset \mathcal{K}_{n,m,o,\mathbb{K}}$ such that for all $\theta = (\alpha, \beta) \in \mathcal{U}_{n,m,o,\mathbb{K}}$, it holds that $\mathbf{0}$ is a regular value of Φ_θ on $\overline{\mathbb{K}}^n \setminus (\overline{\mathbb{K}}^o \times \{0\}^{n-o})$.*

Moreover, the complementary of $\mathcal{U}_{n,m,o,\mathbb{K}}$ is contained in a Zariski closed subset of strong degree bounded by $(2m)^{n-m}3^m$.

In other words, let $\mathcal{P} \in \mathcal{U}_{n,m,o,\mathbb{K}}$ be a UOV public key defining a variety V , with secret subspace $\mathcal{O}$. Then for all $\mathbf{x} \in V \setminus \mathcal{O}$, the Jacobian matrix $\text{Jac}_{\mathbf{x}}(\mathcal{P})$

has full rank m . Further, when $\mathbb{K}$ is the field $\mathbb{F}_q$ (with q some power of a prime), $\mathcal{U}_{n,m,o,\mathbb{K}}$ is denoted by $\mathcal{U}_{n,m,o,q}$.

Proof. The beginning of our proof comes from [51, Theorem 3.2], with minor differences in notations but working over an algebraically closed field, which is crucial to apply some results from commutative algebra and algebraic geometry. Let $\mathcal{O} = \overline{\mathbb{K}}^o \times \{0\}^{n-o}$ (hence, it is defined by $x_{o+1} = \dots = x_n = 0$) and let $\mathcal{S} = \overline{\mathbb{K}}^n \setminus \mathcal{O}$. First, notice that $\mathcal{O} = \overline{\mathbb{K}}^o \times \{0\}^{n-o}$ is a proper Zariski closed subset (provided that $n > o$), therefore $\mathcal{S} = \overline{\mathbb{K}}^n \setminus \mathcal{O}$ is a Zariski open set.

Consider the polynomial Φ defined in Definition 4. We prove further that the $m \times (n+d)$ Jacobian matrix $\text{Jac}(\Phi)$ of Φ has full rank at any point of $\mathcal{S} \times \overline{\mathbb{K}}^d$. To do so, we prove that it contains a full rank sub-matrix of size m (as $n \geq m$). To ease the description of this submatrix, we partition the set of indeterminates into four blocks.

Let $\mathbf{X}_O = (X_1, \dots, X_o)$, $\mathbf{X}_V = (X_{o+1}, \dots, X_n)$. For all $1 \leq k \leq m$, let $\mathbf{a}^{(k)} = (\mathbf{a}_{1,o+1}^{(k)}, \dots, \mathbf{a}_{o,n}^{(k)})$ and $\mathbf{b}^{(k)} = (\mathbf{b}_{o+1,o+1}^{(k)}, \dots, \mathbf{b}_{n,n}^{(k)})$ be new indeterminates. We detail the Jacobian matrix based on the definition of Φ in Equation (2). Let $1 \leq k \leq m$.

- a) For $\ell \in O$, $\frac{\partial \Phi^{(k)}}{\partial X_\ell} =: L_k^{(1)}(\mathbf{X}_V, \mathbf{a})$ does not depend on $\mathbf{X}_O$.
- b) For $\ell \in V$, $\frac{\partial \Phi^{(k)}}{\partial X_\ell} = \sum_{i \in O} \mathbf{a}_{i,\ell}^{(k)} X_i + \sum_{i \in V, i \neq \ell} \mathbf{b}_{i,\ell}^{(k)} X_i + 2\mathbf{b}_{\ell,\ell}^{(k)} X_\ell =: L_k^{(2)}(\mathbf{X}, \mathbf{a}, \mathbf{b})$.
- c) For $i, j \in O \times V$, we have $\frac{\partial \Phi^{(k)}}{\partial \mathbf{a}_{i,j}^{(k)}} = X_i X_j$.
- d) Similarly, for $i, j \in V \times V$, we have $\frac{\partial \Phi^{(k)}}{\partial \mathbf{b}_{i,j}^{(k)}} = X_i X_j$.
- e) For $1 \leq \ell \neq k \leq n$ and $i, j \in O \times V$, we have $\frac{\partial \Phi^{(\ell)}}{\partial \mathbf{a}_{i,j}^{(k)}} = 0$.
- f) For $1 \leq \ell \neq k \leq n$ and $i, j \in V \times V$, we have $\frac{\partial \Phi^{(\ell)}}{\partial \mathbf{b}_{i,j}^{(k)}} = 0$.

All in all, $\text{Jac}(\Phi)$ has the following shape:

$$\text{Jac}(\Phi) = \begin{bmatrix} \mathbf{X}_O & \mathbf{X}_V & \mathbf{a}^{(1)} & \mathbf{b}^{(1)} & \dots & \mathbf{a}^{(m)} & \mathbf{b}^{(m)} \\ L_1^{(1)}(\mathbf{X}_V, \mathbf{a}) & L_1^{(2)}(\mathbf{X}, \mathbf{a}, \mathbf{b}) & X_i X_j & X_i X_j & \dots & 0 & 0 \\ \vdots & & & & & & \vdots \\ L_m^{(1)}(\mathbf{X}_V, \mathbf{a}) & L_m^{(2)}(\mathbf{X}, \mathbf{a}, \mathbf{b}) & 0 & 0 & \dots & X_i X_j & X_i X_j \end{bmatrix} \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \quad (3)$$

Let $\mathbf{x} \in \mathcal{S} = \overline{\mathbb{K}}^n \setminus \mathcal{O}$. As $\mathbf{x} \notin \mathcal{O}$, there exists $i \in V$ such that $x_i \neq 0$. Therefore, for all $1 \leq k \leq m$, we have:

$$\frac{\partial \Phi^{(k)}}{\partial \mathbf{b}_{i,i}^{(k)}}(\mathbf{x}) = x_i^2 \text{ and for all } \ell \neq k, \quad \frac{\partial \Phi^{(\ell)}}{\partial \mathbf{b}_{i,i}^{(k)}}(\mathbf{x}) = \frac{\partial \Phi^{(k)}}{\partial \mathbf{b}_{i,i}^{(\ell)}}(\mathbf{x}) = 0.$$

In other words, the sub-matrix $\text{Jac}(\Phi, [\mathbf{b}_{i,i}^{(1)}, \dots, \mathbf{b}_{i,i}^{(m)}])$ of $\text{Jac}(\Phi)$ is x_i^2 times the identity matrix. Since $x_i \neq 0$, then $x_i^2 \cdot I_m$ is invertible, therefore $\text{Jac}(\Phi)$ is full rank, and therefore $\mathbf{0} \in \overline{\mathbb{K}}^m$ is a regular value of Φ on $\mathcal{S} \times \overline{\mathbb{K}}^d$ as claimed.

From here on, our proof differs significantly from [51, Theorem 3.2], as we no more rely on transversality results which do require large enough base field to prove the existence of the Zariski open subset $\mathcal{U}_{n,m,o,\mathbb{K}}$ through algebraic elimination arguments.

Take $A' = \Phi^{-1}(\mathbf{0}) \cap (\mathcal{S} \times \overline{\mathbb{K}}^d)$ and let A denote the Zariski closure of A' . We first prove that if A' is non-empty, then A is equidimensional of codimension m .

Let B be an irreducible component of A . Since A is the Zariski closure of A' which is assumed to be non-empty, B contains a point $\mathbf{p} = (x, \vartheta) \in A'$. Note that, by construction, the Jacobian matrix of Φ at $\mathbf{p}$ is full rank. Hence, in the ring $\mathbb{K}[\mathbf{X}, \mathbf{a}, \mathbf{b}]_{\mathbf{p}}$ of polynomials localized by $\mathbf{p}$, the height of the ideal generated by the m polynomials $\Phi^{(1)}(\mathbf{X}, \mathbf{a}, \mathbf{b}), \dots, \Phi^{(m)}(\mathbf{X}, \mathbf{a}, \mathbf{b})$ defining $\Phi^{-1}(\mathbf{0})$ is m (thanks to the rank property of the Jacobian implies that they are locally independent). We deduce that this localized ideal (which is prime and contained in $\mathbf{p}$) has codimension m and then B has codimension m too [2, Prop. 4.8(ii)]. Therefore, all irreducible components of A have codimension m and then A is equidimensional of codimension m if A' is not empty.

Note also that at every point of A' the Jacobian matrix associated to Φ is full rank. Then, we can deduce that its right kernel (at these points) is the tangent space to A . In other words, A' is contained in the regular locus of A .

Let π be the projection $\overline{\mathbb{K}}^n \times \overline{\mathbb{K}}^d \rightarrow \overline{\mathbb{K}}^d$. Following *mutatis mutandis* the proof of [56, Prop. B.3], the fact that the tangent space to A is the right kernel of $\text{Jac}(\Phi)$ at any point of A' , implies (through basic linear algebra) that, if (α, β) is such that $\mathbf{0}$ is not a regular value of $\Phi_{(\alpha, \beta)}$ then (α, β) is a critical value of the restriction of π to A .

We now consider the ideal J generated by all maximal minors of $\text{Jac}(\Phi, \mathbf{X})$ and the equations defining $\Phi^{-1}(\mathbf{0})$. Note that, by definition, this ideal contains the critical points of the restriction of π to A .

Let $\mathcal{Z}$ be the Zariski closed subset associated to $J \cap \mathbb{K}[\mathbf{a}, \mathbf{b}]$. Note that, by definition, the set $\mathcal{Z}$ contains the critical values of the restriction of π to A and for all $\vartheta = (\alpha, \beta) \notin \mathcal{Z}$, $\mathbf{0}$ is a regular value of Φ_{ϑ} . Thus, we can define the Zariski-open set $\mathcal{U}_{n,m,o,\mathbb{K}}$ as the complementary of $\mathcal{Z}$ and all that remains to prove is a bound on the degree of $\mathcal{Z}$.

Finally, note that J is generated by m polynomial equations of total degree 3 (the ones defining $\Phi^{-1}(\mathbf{0})$ and $\binom{n}{m}$ of total degree $2m$ (the maximal minors of $\text{Jac}(\Phi, \mathbf{X})$). Applying Heintz-Bézout theorem [39, Sec. 2], we deduce that the sum of the degrees of the equidimensional components of $V(J)$ is bounded above by $(2m)^{n-m}3^m$. Hence, the sum of the degrees of Zariski closures of their projection by π is also bounded above by $(2m)^{n-m}3^m$ [40, Lemma 2]. $\square$

Remark 1. Note that $\mathcal{Z}$ (the complementary of $\mathcal{U}_{n,m,o,\mathbb{K}}$) is defined by polynomials in $\mathbb{K}[\mathbf{a}, \mathbf{b}]$ since it is defined as the vanishing set of $J \cap \mathbb{K}[\mathbf{a}, \mathbf{b}]$ and J is generated by polynomials with coefficients in $\mathbb{K}$.

In [51, Theorem 3.2], the construction of $\mathcal{U}_{n,m,o,\mathbb{K}}$ is done with the algebraic version of Thom's weak transversality theorem [56, Prop. B.3], which defines the Zariski-open set and proves that it is non-empty. However, since this latter

result relies on an algebraic version of Sard's theorem (see e.g. [56, prop. B.2]) which requires the base field to have characteristic 0, the tools used to reduce the construction modulo a prime p imply that the final result requires a large enough finite field, and the size requirement was not derived explicitly in the paper. This also explains why [51] used the notation $\mathcal{U}_{n,m,o,q}$, highlighting the dependency in q . Instead, our Theorem 1 holds over any field $\mathbb{K}$ (finite or not) and establishes the existence of a Zariski-open set $\mathcal{U}_{n,m,o,\mathbb{K}}$. We then propose an alternative approach to prove the non-emptiness of $\mathcal{U}_{n,m,o,\mathbb{K}}$ in any field under reasonable constraints on n, m, o .

Theorem 2. *Let (n, m, o) be UOV parameters such that $m \leq o$ and $m \leq n$ and let $\mathbb{K}$ be a field. Then $\mathcal{U}_{n,m,o,\mathbb{K}}$ is a non-empty Zariski-open set.*

Proof. Our goal is to construct a sequence of polynomials which belongs to $\mathcal{U}_{n,m,o,\mathbb{K}}$ (regardless the choice of the field $\mathbb{K}$). In other words, this sequence should be a sequence of secret UOV polynomials whose Jacobian matrix has full rank outside of $\mathcal{O}$, where $\mathcal{O}$ is the linear subspace defined by

$$\mathcal{O} := \text{span}(e_1, \dots, e_o) = \{\mathbf{x} \in \mathbb{K}, \quad x_{o+1} = \dots = x_n = 0\}.$$

We define the map $\mathbf{x} \mapsto \mathcal{F}(\mathbf{x}) := (f_1(\mathbf{x}), \dots, f_m(\mathbf{x}))$ for $1 \leq k \leq m$ with two cases depending on the parity of $n - o + k$:

- When $k = n - o + 1 \pmod{2}$,

$$f_k = \sum_{i=1}^{\lceil \frac{n-o+k}{2} \rceil} X_{o-(k-1)+i} X_{n-(i-1)}, \quad (4)$$

- When $k = n - o \pmod{2}$,

$$f_k = \sum_{i=1}^{\frac{n-o+k}{2}-1} X_{o-(k-1)+i} X_{n-(i-1)} + X_1 X_{o-(k-1)+\frac{n-o+k}{2}}. \quad (5)$$

By assumption, $o \geq m$ therefore the index $o - (k - 1) + i$ is strictly greater than 1 for $k = m$ and $i = 1$ and thus for any $k \neq m$ and any index i in the above sums.

We show that the Jacobian has full rank outside of $\mathcal{O}$. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{K}^n \setminus \mathcal{O}$ be a vector that does not belong to $\mathcal{O}$. By definition, the variables used in the secret key satisfy

$$\mathbf{x} \in \mathcal{O} \iff x_{o+1} = \dots = x_n = 0.$$

Thus, $\mathbf{x} \notin \mathcal{O}$ implies that there exists an index $o+1 \leq i \leq n$ such that $x_i \neq 0$. Let j be the largest such index. As $n \geq m$, a maximal minor of the Jacobian matrix of $\mathcal{F}$ contains all rows and m columns. We assume without loss of generality that $n - o + m = 0 \pmod{2}$, thus f_m is defined by Equation (5). There are two cases:

- Assume $j < o - (m - 1) + \frac{n-o+m}{2}$ or $j > o + \frac{n-o+m}{2}$: this excludes indices of indeterminates multiplied to X_1 in Equation (5). By our remark above, the indices of the m columns of $\text{Jac}_{\mathbf{x}}(\mathcal{F})$ containing entries equal to X_j are $o - (k - 1) + (n - j + 1)$ for $1 \leq k \leq m$. The maximal submatrix corresponding to these columns is the following lower triangular matrix

$$J = \begin{bmatrix} \partial X_{o+(n-j+1)} & \cdots & \partial X_{o-m+1+(n-j+1)} \\ x_j & & \\ & \ddots & \\ * & & x_j \end{bmatrix},$$

which has full rank since $x_j \neq 0$.

- If the above does not hold, then $o - (m - 1) + \frac{n-o+m}{2} \leq j \leq o + \frac{n-o+m}{2}$. In this case, the indices of the m columns of $\text{Jac}_{\mathbf{x}}(\mathcal{F})$ containing entries equal to X_j are 1 and $o - (k - 1) + (n - j + 1)$ for $1 \leq k \neq n - 2j + o - 2 \leq m$. Thus, the maximal submatrix corresponding to these columns is

$$J = \begin{bmatrix} \partial X_{o+(n-j+1)} & \cdots & \partial X_{o-m+1+(n-j+1)} & \partial X_1 \\ x_j & & & \\ & x_j & & \\ & & \ddots & \\ & & & x_j \\ * & & & x_j \end{bmatrix},$$

whose columns can be permuted to obtain a lower triangular matrix, and again has full rank since $x_j \neq 0$.

Thus, the Jacobian matrix $\text{Jac}_{\mathbf{x}}(\mathcal{F})$ always contains an $m \times m$ full rank submatrix, therefore the Jacobian matrix has full rank on $\mathbb{K}^n \setminus \mathcal{O}$. Therefore, we have constructed an element of $\mathcal{U}_{n,m,o,\mathbb{K}}$ for any field, under the constraint that $m \leq o$ and $m \leq n$. $\square$

Example 1. We give an example of the previous construction for $n = 10$, $m = o = 4$ and any field.

$$\begin{aligned} f_1 &= X_7 X_8 + X_6 X_9 + X_5 X_{10} \\ f_2 &= X_1 X_7 + X_6 X_8 + X_5 X_9 + X_4 X_{10} \\ f_3 &= X_6 X_7 + X_5 X_8 + X_4 X_9 + X_3 X_{10} \\ f_4 &= X_1 X_6 + X_5 X_7 + X_4 X_8 + X_3 X_9 + X_2 X_{10}. \end{aligned}$$

$$\text{Jac}(\mathcal{F}) = \begin{bmatrix} \partial X_{10} & \partial X_9 & \partial X_8 & \partial X_7 & \partial X_6 & \partial X_5 & \partial X_4 & \partial X_3 & \partial X_2 & \partial X_1 \\ X_5 & X_6 & X_7 & X_8 & X_9 & X_{10} & 0 & 0 & 0 & 0 \\ X_4 & X_5 & X_6 & X_1 & X_8 & X_9 & X_{10} & 0 & 0 & X_7 \\ X_3 & X_4 & X_5 & X_6 & X_7 & X_8 & X_9 & X_{10} & 0 & 0 \\ X_2 & X_1 & X_4 & X_5 & X_1 & X_7 & X_8 & X_9 & X_{10} & X_6 \end{bmatrix} \begin{bmatrix} \partial f_1 \\ \partial f_2 \\ \partial f_3 \\ \partial f_4 \end{bmatrix}$$

One can check that the minors we extract in the proof are the correct ones.

- In the first case, if $x_{10} \neq 0$: 10 is greater than $o - (m-1) + \frac{n-o+m}{2} = 1+5 = 6$. The indices of the 4 columns of $\text{Jac}(\mathcal{F})$ containing entries equal to X_{10} are $4 - (k-1) + (10-10+1)$ for $1 \leq k \leq m$, which indeed specializes to 5, 4, 3, 2.
- In the second case, if $x_6 \neq 0$. The indices of the 4 columns of $\text{Jac}(\mathcal{F})$ containing entries equal to X_6 are 1 and $4 - (k-1) + (10-6+1)$ for $1 \leq k \neq 4 \leq m$, which indeed specializes to 9, 8, 7.

A curious reader will find in Appendix A the details of how this family of examples was constructed.

Remark 2. The previous theorems yield a purely algebraic characterization of UOV keys lying outside of $\mathcal{U}_{n,m,o,\mathbb{K}}$, bounding the degree of its complementary $\mathcal{Z}$. One could then hope to bound the probability that a randomly generated key belongs to $\mathcal{Z}$, ideally below $2^{-\lambda}$ where λ is the desired security level. We expect that doing so requires bounding both the strong degree and dimension of $\mathcal{Z}$. While we managed to bound the strong degree of $\mathcal{Z}$, bounding its dimension seems more complicated and is left for future work. We provide in Appendix B a preliminary result as a stepping stone for tighter probability bounds.

With Theorems 1 and 2, we prove that the UOV map has full rank outside of $\mathcal{O}$ for a generic choice of $(\alpha, \beta) \in \mathbb{K}^d$. In the next section, we use this result to show that all elements of $\mathcal{U}_{n,m,o,\mathbb{K}}$ generate radical ideals which in turn define equidimensional varieties under the only additional assumption that $n - m \geq o$. This allows us not only to study singular points of V but to establish some regularity results that are ubiquitous in the cryptanalysis of multivariate schemes.

4 Genericity of regularity assumptions

In this section, we aim to prove that the main regularity assumptions required in most algebraic attacks against UOV, are Zariski generic [6, 8, 33]. Namely, the fact that $p_1, \dots, p_m$ is a regular sequence generating a radical ideal and that $V(\mathcal{I})$ is an equidimensional complete intersection.

Lemma 1 ([58, Corollary 1.14]). *Let $\mathbb{K}$ be a field and let $(p_1, \dots, p_m)$ be a collection of non-constant polynomials in $\mathbb{K}[\mathbf{X}]$. Denote by $\mathcal{I}$ the ideal $\langle p_1, \dots, p_m \rangle$ and assume that $V(\mathcal{I}) \neq \emptyset$. Then all irreducible components of $V(\mathcal{I})$ have codimension at most m .*

Lemma 2. *Let $p_1, \dots, p_m$ be a UOV public key for parameters (n, m, o, q) with $n - m > o$. Denote by $\mathcal{I}$ the ideal $\langle p_1, \dots, p_m \rangle$ and $V = V(\mathcal{I})$. Let $\mathcal{O} \subset V$ be an o -dimensional linear subspace. Then $V \setminus \mathcal{O}$ is Zariski dense in V .*

Proof. The ideal $\mathcal{I}$ is generated by m elements. By Lemma 1, it holds that $\dim V \geq n - m$ and that all irreducible components of V have dimension at least $n - m$. Denote by $(W_i)_{1 \leq i \leq \ell}$ the irreducible components of V . For all $1 \leq i \leq \ell$, W_i has codimension at most m . Since $\mathcal{O} \subset V$, it holds that

$$\mathcal{O} = V \cap \mathcal{O} = \bigcup_{1 \leq i \leq \ell} (W_i \cap \mathcal{O}).$$

For $1 \leq i \leq \ell$, denote by $E_i = (W_i \cap \mathcal{O})$. It holds that $\dim E_i < \dim W_i$ since $\dim \mathcal{O} = o < \dim W_i$. Therefore by [21, Chapter 4, Section 5, Proposition 13], $W_i \setminus E_i$ is Zariski dense in W_i . It holds that

$$V \setminus \mathcal{O} = \bigcup_{1 \leq i \leq \ell} W_i \setminus E_i.$$

Thus,

$$\overline{V \setminus \mathcal{O}} = \bigcup_{1 \leq i \leq \ell} \overline{W_i \setminus E_i} = \bigcup_{1 \leq i \leq \ell} W_i = V.$$

Therefore, $V \setminus \mathcal{O}$ is Zariski dense in V . $\square$

Lemma 3 ([55, Lemma 15]). *Let $(g_1, \dots, g_n) \subset \mathbb{F}[X_1, \dots, X_n]$, let I be the ideal $\langle g_1, \dots, g_n \rangle \subset \mathbb{F}[X_1, \dots, X_n]$, let Z be its zero-set, and let X be the constructible set*

$$X = \{x \in Z \mid \text{rank}(\text{Jac}(g, [X_1, \dots, X_n])) = p\}.$$

Suppose that Z is not empty and that X is Zariski-dense in Z . Then, I is an equidimensional radical ideal of dimension $n - p$.

Theorem 3. *Let (n, m, o, q) be UOV parameters with $n > 2o$ and $n - m > o$. For all UOV public keys $\mathcal{P} \in \mathcal{U}_{n,m,o,q}$, $\mathcal{I} = \langle p_1, \dots, p_m \rangle$ is radical, and $V(\mathcal{I})$ is equidimensional of dimension $n - m$.*

Proof. By Theorem 1, for all $\mathcal{P} \in \mathcal{U}_{n,m,o,q}$, it holds that for all $\mathbf{x} \in V(\mathcal{I}) \setminus \mathcal{O}$, $\text{Jac}_{\mathbf{x}}(\mathcal{P})$ has rank m . By Lemma 2, $V(\mathcal{I}) \setminus \mathcal{O}$ is Zariski dense in $V(\mathcal{I})$. Therefore, by Lemma 3, for all $\mathcal{P} \in \mathcal{U}_{n,m,o,q}$, $\mathcal{P}$ generates a radical ideal and $V(\mathcal{I})$ is equidimensional of dimension $n - m$. $\square$

Corollary 1. *Let (n, m, o, q) be UOV parameters with $n > 2o$ and $n - m > o$. All elements of $\mathcal{U}_{n,m,o,q}$ form regular sequences.*

Proof. Let $\mathcal{P} \in \mathcal{U}_{n,m,o,q}$ be a UOV key. By Theorem 3, $\dim V(\langle p_1, \dots, p_m \rangle) = n - m$. Since $\mathbb{F}_q[X_1, \dots, X_n]$ is Cohen-Macaulay, this implies that $p_1, \dots, p_m$ forms a regular sequence. $\square$

We have shown that any UOV key in $\mathcal{U}_{n,m,o,q}$ forms a regular sequence, but we point out that the converse is not true. To illustrate this, notice that the sequence $(X_1^2, \dots, X_m^2) \in \mathbb{F}_q[X_1, \dots, X_n]_2^m$ is a UOV (n, m, o, q) sequence if $m < n - o$ since it is linear in $X_{n-o}, \dots, X_n$, and it is also clearly a regular sequence. However, it does not generate a radical ideal, and the map $\mathbf{x} \mapsto (x_1^2, \dots, x_m^2)$ is not regular in 0: any point with $x_i = 0$ for $1 \leq i \leq m$ is singular and outside of $\mathcal{O} = \{0\}^{n-o} \times \mathbb{F}_q^o$.

Corollary 2. *Let (n, m, o, q) be UOV parameters with $n > 2o$ and $n - m > o$. Let $\mathcal{P}$ be a UOV public key lying in the Zariski open set $\mathcal{U}_{n,m,o,q}$ defined in Theorem 1. Denote by V the variety defined by $\mathcal{P}$. The singularities of V , if any, belong to the corresponding oil space $\mathcal{O}$.*

Proof. Let $\mathbf{x} \in V \setminus \mathcal{O}$. By Theorem 3, V is an equidimensional variety of codimension m . Thus, at any singular point of V , $\text{Jac}_{\mathbf{x}}(\mathcal{P})$ must have rank $< m$. By Theorem 1, for any $\mathcal{P}$ lying in $\mathcal{U}_{n,m,o,q}$ and any $\mathbf{x} \notin \mathcal{O}$, $\text{Jac}_{\mathbf{x}}(\mathcal{P})$ has rank m . The variety generated by any such $\mathcal{P}$ is therefore regular outside of $\mathcal{O}$. $\square$

5 Generic determinantal varieties of UOV

It is straightforward to lower-bound the dimension of a non-empty determinantal variety using e.g. [15, Theorem 2.1]. This bound is tight and achieved for generic polynomial matrices, see [30]. Our goal is to also obtain dimension results in the context of MinRank attacks against UOV and its variants, however the polynomial matrices involved in this setting are Jacobian matrices whose entries are not independent from one another, so that we cannot simply apply results from [30]. In this section, we avoid that issue by explicitly constructing the Zariski-closed sets of keys which have unusually high-dimensional determinantal ideals using the same tools as in Theorem 1. Such ideals arise naturally as tangent spaces to UOV varieties, which is why computing their dimension is instrumental in estimating the complexity of some key recovery attacks, such as [59, 50].

In particular, in [59] the authors observed that higher rank defects may occur in Jacobian matrices of keys of UOV variants such as MAYO and QR-UOV, where the ratio between n and m is closer to one. This enables the authors to improve existing Rectangular MinRank attacks.

Theorem 4. *Let (n, m, o, q) be UOV parameters with $n > 2o$ and $n - m > o$. Let $1 \leq r \leq m$ and $\delta = o - r(n - o - m + r)$. There exists a Zariski open set $\mathcal{M}_{r,n,m,o,q} \subset \mathcal{K}_{n,m,o,q}$ such that for all UOV public keys $\mathcal{P}$ in $\mathcal{M}_{r,n,m,o,q}$, the variety $\mathcal{O} \cap V(\langle \text{Minors}_{m-r+1}(\text{Jac}(\mathcal{P})) \rangle)$ has dimension δ if $\delta \geq 0$ and is empty otherwise. Furthermore, the ideal $I(\mathcal{O}) + \langle \text{Minors}_{m-r+1}(\text{Jac}_{\mathbf{X},\alpha,\beta}(\mathcal{P})) \rangle$ is radical.*

Proof. Let Φ be an indeterminate UOV secret key, and recall that

$$\text{Jac}_{\mathbf{X},\alpha,\beta}(\Phi) = \begin{bmatrix} \mathbf{X}_O & \mathbf{X}_V \\ L_1^{(1)}(\mathbf{X}_V, \alpha) & L_1^{(2)}(\mathbf{X}, \alpha, \beta) \\ \vdots & \vdots \\ L_m^{(1)}(\mathbf{X}_V, \alpha) & L_m^{(2)}(\mathbf{X}, \alpha, \beta) \end{bmatrix} \begin{matrix} 1 \\ \vdots \\ m \end{matrix}. \quad (6)$$

We consider an indeterminate oil vector $\mathbf{X}_O = (X_1, \dots, X_o, 0, \dots, 0)$. Thus,

$$\text{Jac}_{\mathbf{X}_O,\alpha,\beta}(\Phi) = \begin{pmatrix} \mathbf{X}_O & \mathbf{X}_V \\ 0 & L_1^{(2)}(\mathbf{X}_O, \alpha, \beta) \\ \vdots & \vdots \\ 0 & L_m^{(2)}(\mathbf{X}_O, \alpha, \beta) \end{pmatrix} \begin{matrix} 1 \\ \vdots \\ m \end{matrix}.$$

We omit the superscript $^{(2)}$ in the rest of the proof. More precisely, for all $1 \leq i \leq m$ and for all $o+1 \leq j \leq n$, it holds that

$$L_i(\mathbf{X}_O, \alpha, \beta)_j = \sum_{1 \leq k \neq j \leq o} \alpha_{jk}^{(i)} X_k + \sum_{o+1 \leq k \leq n} \beta_{jk}^{(i)} \cdot 0.$$

Thus the Jacobian matrix evaluated at a formal oil vector does not depend on the vinegar coefficients. We write

$$L_i(\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha})_j = \sum_{1 \leq k \leq o} \alpha_{jk}^{(i)} X_k.$$

Given θ such that $\mathcal{P} = \Phi_\theta$, by definition of the rank of a matrix since $n - o \geq m$, it holds that $\mathbf{x} \in \mathcal{O}$ and $\mathbf{x} \in V(\langle \text{Minors}_{m-r+1}(\text{Jac}(\mathcal{P})) \rangle)$ if and only if there exists a matrix $Y \in \mathbb{F}_q^{r \times m}$ of full rank such that

$$\mathbf{x} \in \mathcal{O} \text{ and } Y \cdot \text{Jac}_{\mathbf{x}, \theta}(\Phi) = [0] \in \mathbb{F}_q^{r \times n}. \quad (7)$$

We assume without loss of generality that Y is in echelon form:

$$Y = \begin{bmatrix} & Y^{(1)} \\ I_r & \vdots \\ & Y^{(r)} \end{bmatrix}.$$

Thus, $V(\langle \text{Minors}_{m-r+1}(\text{Jac}(\mathcal{P}, \mathbf{X})) \rangle)$ is the projection on $\mathbb{F}_q^n$ (by eliminating the $\mathbf{Y}$ variables) of the variety defined by the matrix system

$$S = \begin{bmatrix} & Y^{(1)} \\ I_r & \vdots \\ & Y^{(r)} \end{bmatrix} \cdot \begin{bmatrix} 0 & L_1(\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha}) \\ \vdots & \vdots \\ 0 & L_m(\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha}) \end{bmatrix} = [0] \in \mathbb{F}_q[\mathbf{X}, \mathbf{Y}, \boldsymbol{\alpha}]^{r \times n}. \quad (8)$$

The system is composed of the entries of S , therefore it is a system of $r \times (n - o)$ equations in $r(m - r) + o$ variables (and the parameters $\boldsymbol{\alpha}$).

We exhibit an identity sub-matrix in the Jacobian of the quadratic map induced by the entries of S to prove that 0 is a regular value for the map $(\mathbf{x}, \mathbf{y}) \mapsto S(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha})$. The Jacobian of the entries of S is a matrix of $r \times (n - o)$ rows and $o + r(m - r) + mo(n - o)$ columns. We denote by $S_{i,j}$ the entry i, j of the matrix $S = Y \cdot \text{Jac}_{\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha}}(\Phi)$.

$$S_{i,j} = \begin{bmatrix} i & r+1 & m \\ 0 \cdots 1 \cdots 0 & Y_1^{(i)} & \cdots Y_{n-r}^{(i)} \end{bmatrix} \cdot \begin{bmatrix} L_1(\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha})_j \\ \vdots \\ L_m(\mathbf{X}_{\mathcal{O}}, \boldsymbol{\alpha})_j \end{bmatrix}. \quad (9)$$

Thus,

$$S_{i,j} = 1 \cdot \left(\sum_{1 \leq k \leq o} \alpha_{jk}^{(i)} X_k \right) + \sum_{r+1 \leq \ell \leq m} \left(\sum_{1 \leq k \leq o} \alpha_{jk}^{(\ell)} X_k Y_\ell \right). \quad (10)$$

Consequently, it holds that for all $1 \leq i \leq r$, $1 \leq k \leq o$, $o \leq j \leq n$,

$$\frac{\partial S_{i,j}}{\partial \alpha_{j,k}^{(i)}} = X_k. \quad (11)$$

The partial derivatives with respect to $\alpha^{(i)}$ that do not appear in a polynomial $S_{\ell,j}$ for $\ell \neq i$ are zero:

$$\frac{\partial S_{\ell,j}}{\partial \alpha_{j,k}^{(i)}} = 0. \quad (12)$$

Therefore, for all $1 \leq k \leq o$, we construct a submatrix of $\text{Jac}(S)$ of the form:

$$J_k = \begin{matrix} & \alpha_{o,k}^{(1)} & \alpha_{o,k}^{(2)} & \cdots & \alpha_{o,k}^{(r)} & \cdots & \alpha_{n,k}^{(r)} \\ \begin{matrix} S_{o,1} \\ S_{o,2} \\ \vdots \\ S_{o,r} \\ \vdots \\ S_{n-o,r} \end{matrix} & \begin{pmatrix} X_k & 0 & \cdots & 0 & \cdots & 0 \\ 0 & X_k & & & & \\ & & \ddots & & & \\ \vdots & & & X_k & & 0 \\ & & & & \ddots & \vdots \\ 0 & & \cdots & & & X_k \end{pmatrix} \end{matrix} \in \mathbb{F}_p[\mathbf{X}, \mathbf{Y}, \boldsymbol{\alpha}]^{r(n-o) \times r(n-o)}$$

We dehomogenize by choosing a hyperplane at infinity, say $H_\infty = V(\langle X_1 \rangle)$. Recall that $\mathcal{O} = V(\langle X_{o+1}, \dots, X_n \rangle)$, which yields $\mathcal{O} \not\subset H_\infty$. In this affine chart, J_1 is an identity matrix times a non-zero scalar, thus, for all $(\mathbf{x}, \mathbf{y}) \in (\mathcal{O} \setminus H_\infty) \times \mathbb{F}_p^{(n-r) \times r}$, $\text{Jac}_{\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}}(S)$ has full rank $(n-o)r$. In other words, 0 is a regular value of the map $(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}) \mapsto S(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha})$ on $\mathcal{S} = (\mathcal{O} \setminus V(X_1)) \times \mathbb{F}_p^{(n-r) \times r}$.

Following the proof of Theorem 1, we build a Zariski open set $\mathcal{M}_{r,n,m,o,q} \subset \mathcal{K}_{n,m,o,q}$ such that for all $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathcal{M}_{r,n,m,o,q}$, 0 is a regular value of the map $(\mathbf{x}, \mathbf{y}) \mapsto S(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}, \boldsymbol{\beta})$. Since we have seen that $\boldsymbol{\beta}$ is never involved in the computations, it can take any value so we remove it from the proof for brevity.

Let us define $A' = S^{-1}(0) \cap \mathcal{S}$ and A its Zariski closure. Likewise, any point $(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha})$ in A' belongs to an irreducible component B of A whose codimension is $(n-o)r$. As in the proof of Theorem 1, this holds because the $(n-o)r$ polynomials defining $S^{-1}(0)$ are independent due to the rank property of $\text{Jac}_{\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha}}(S)$. Hence, we deduce once again that A is equidimensional of codimension $(n-o)r$.

Still following the proof, we define a projection π whose critical values contain all the choices of $\boldsymbol{\alpha}$ such that 0 is a critical point of $S(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha})$. Defining J the ideal generated by the maximal minors of $\text{Jac}_{\mathbf{x}, \mathbf{y}, \mathbf{a}}(S)$, we define $\mathcal{Z} = J \cap \mathbb{F}_q[\mathbf{a}]$. As in the proof of Theorem 1, $\mathcal{Z}$ has been constructed to contain all the critical points of π . We can thus define $\mathcal{M}_{r,n,m,o,q}$ as the set of the $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta})$ such that $\boldsymbol{\alpha} \notin \mathcal{Z}$ as, for any $\boldsymbol{\alpha}$ outside of $\mathcal{Z}$, 0 is a regular value of $S(\mathbf{x}, \mathbf{y}, \boldsymbol{\alpha})$.

The set $\mathcal{O} \setminus V(\langle X_1 \rangle)$ is dense in $\mathcal{O}$ since $\mathcal{O}$ is irreducible and $\mathcal{O} \not\subset V(\langle X_1 \rangle)$ by Definition 4, as $\mathcal{O} = V(\langle \mathbf{X}_V \rangle)$. Therefore by Lemma 3, for all $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathcal{M}_{r,n,m,o,q}$, the sequence

$$1 \leq i \leq r, o \leq j \leq n-o, \quad S_{i,j}(\mathbf{X}, \mathbf{Y}, \boldsymbol{\alpha}) \quad (13)$$

generates a radical ideal $\mathcal{L}$ of $\mathbb{F}_q[\mathbf{X}, \mathbf{Y}]$ and an equidimensional variety W of dimension $\delta = r(m-r) + o - r(n-o)$.

Let $\theta \in \mathcal{M}_{r,n,m,o,q}$ and denote by $\mathcal{P}$ the quadratic map Φ_θ . We eliminate the $\mathbf{Y}$ variables to compute the dimension of

$$\mathcal{O} \cap V(\langle \text{Minors}_{m-r+1}(\text{Jac}(\mathcal{P}, \mathbf{X})) \rangle).$$

Denote by $(h_1, \dots, h_{n-o}) \in \mathbb{F}_q[\mathbf{X}]_1^{n-o}$ a collection of linear polynomials such that

$$\mathcal{O} = V(\langle h_1, \dots, h_{n-o} \rangle).$$

Let us define $\mathcal{I}_{\mathcal{O}} = \langle h_1, \dots, h_{n-o} \rangle$, and $\mathcal{J}_{m-r+1} = \langle \text{Minors}_{m-r+1}(\text{Jac}(\mathcal{P}, \mathbf{X})) \rangle$. Recall that $\mathcal{O} \cap V(\mathcal{J}_{m-r+1}) = V(\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1})$ by the Algebra-Geometry dictionary (see [21, Chapter 4, Section 9]). Consider the projection π defined by

$$\begin{aligned} \pi : W &\mapsto \pi(W) \\ (\mathbf{x}, \mathbf{y}) &\mapsto (\mathbf{x}) \end{aligned}.$$

Recall the equivalence between $\mathbf{x} \in V(\mathcal{J}_{m-r})$ and the existence of a matrix $Y \in \mathbb{K}^{r \times m}$ of full rank such that $Y \cdot \text{Jac}_{\mathbf{x}, \theta}(\Phi) = [0] \in \mathbb{F}_q^{r \times n}$. This shows that $\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1} = \mathcal{L} \cap \mathbb{F}_q[\mathbf{X}]$. By the Closure Theorem [21, Chapter 3, Section 2, Theorem 3], this yields $\pi(W) = V(\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1})$. By the Fiber Dimension Theorem [25, Corollary 10.10], for all $\mathbf{x} \in \pi(W)$,

$$\dim(\pi^{-1}(\mathbf{x})) \geq \dim(W) - \dim(V(\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1})).$$

For $\mathbf{x} \in \pi(W) \setminus \{0\}$, $\pi^{-1}(\mathbf{x})$ is the following set:

$$\pi^{-1}(\mathbf{x}) = \{(\mathbf{x}, \mathbf{y}) \mid 1 \leq i \leq r, o \leq j \leq n-o, \quad S_{i,j}(\mathbf{x}, \mathbf{y}) = 0\}.$$

The system of equations $1 \leq i \leq r, o \leq j \leq n, \quad S_{i,j}(\mathbf{x}, \mathbf{Y}) = 0$ is linear in $r(n-o)$ variables. Since $\theta \in \mathcal{M}_{r,n,m,o,q}$, all the linear polynomials must be independent (otherwise the variety $V(\mathcal{L})$ is not equidimensional of dimension δ), thus the system has dimension 0. Therefore, $\pi^{-1}(\mathbf{x})$ is a singleton. A singleton has dimension 0, hence $\dim(\pi^{-1}(\mathbf{x})) = 0$. On the other hand, since π is a projection, $\dim(W) \geq \dim(V(\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1}))$. Thus, $\dim(W) = \dim(V(\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1})) = \delta$.

We have seen that $\mathcal{L}$ is radical. Assume by contradiction that $\mathcal{L} \cap \mathbb{F}_q[\mathbf{X}]$ is not radical. Thus, there exists $f^\ell \in \mathcal{L} \cap \mathbb{F}_q[\mathbf{X}] \subset \mathcal{L}$ such that f is not in $\mathcal{L} \cap \mathbb{F}_q[\mathbf{X}]$. Since $f^\ell \in \mathcal{L}$ and $f \notin \mathcal{L}$, this implies that $\mathcal{L}$ is not radical, which is a contradiction. Therefore, it holds that $\mathcal{I}_{\mathcal{O}} + \mathcal{J}_{m-r+1}$ is radical. $\square$

Remark 3. Note that contrarily to Theorem 2, we do not exhibit elements of $\mathcal{M}_{r,n,m,o,q}$ in small fields. Note that one can use Thom's weak transversality Theorem [56, Prop. B.3] to prove that it is non-empty in large enough fields, as in [51] for Theorem 1. Instead, we provide an experimental study of $\mathcal{M}_{r,n,m,o,q}$ in the next section. We leave to future work the task of explicitly constructing a family of elements of $\mathcal{M}_{r,n,m,o,q}$ similarly to Theorem 2.

6 Experiments on UOV keys over small fields

In this section, we detail the experiments concerning Theorem 4 in small characteristic. We experimentally verify the non-emptiness of the Zariski open set $\mathcal{M}_{r,n,m,o,q}$ defined in Theorem 4, for various values of n, m, o , and q ranging from 16 to 4093, which reflects field sizes used in UOV-based submissions to the

NIST process [11,10,35,63]. One can tweak the experiments of this section to obtain statistics regarding the corresponding Zariski open-sets $\mathcal{U}_{n,m,o,q}$ defined in Theorem 1 when $r = 1$. A more detailed experimental study of the singular loci of UOV varieties in small characteristic was already proposed in [51].

We detail our approach. We select UOV parameters $(n_i, m_i, o_i)_{1 \leq i \leq k}$ satisfying $n_i - m_i \geq o_i$, along with a selection of primes $p_1, \dots, p_\ell$. For each parameter set and each prime, 1000 UOV public keys are drawn uniformly at random for parameters (n_i, m_i, o_i, p_k) . For each parameter set, we predict the dimension of the determinantal variety corresponding to a rank defect of $1 \leq r \leq m_i$ using Theorem 4. We then experimentally compute the dimension of this determinantal variety for each public key, and compare the experimental result with the prediction. The dimension is computed by computing a Gröbner basis of the ideal $\mathcal{L}$, defined in the proof of Theorem 4, with the msolve polynomial system solver [4] in prime fields and with M4gb [47] in $\mathbb{F}_{16}$. We provide SAGEMATH code for this experiment under MIT licence at

<https://github.com/pi-r2/Genericity>

We count, for each prime and each parameter set, the proportion $\mathcal{D}_p$ (in percent) of public keys for which the dimension prediction matched the estimate. The results are summarized in Figure 1.

n, m, o	r	δ	$\mathcal{D}_{16}$	$\mathcal{D}_{31}$	$\mathcal{D}_{251}$	$\mathcal{D}_{1021}$	$\mathcal{D}_{4093}$
10, 4, 4	1	1	93.3%	96.5%	99.8%	100%	99.9%
10, 5, 5	1	4	99.9%	99.9%	100%	100%	100%
	2	1	93.1%	97.6%	99.4%	99.7%	100%
12, 5, 5	1	2	99.5%	100%	100%	100%	100%
12, 7, 5	1	4	100%	99.9%	100%	100%	100%
	2	1	94.4%	97.6%	99.6%	99.8%	100%
12, 6, 6	1	5	100%	100%	100%	100%	100%
	2	2	99.4%	100%	100%	100%	100%
14, 6, 6	1	3	100%	100%	100%	100%	100%
14, 8, 6	1	5	100%	99.6%	100%	100%	100%

Fig. 1. Proportion of UOV keys in the Zariski open sets of Theorem 4, for various parameters and prime fields of sizes 16, 31, 251, 1021, 4093.

We observe that a high proportion of UOV polynomial systems belong to the Zariski open sets $\mathcal{M}_{r,n,m,o,q}$. For the various parameter sets tested, it is shown that the Zariski open sets defined in Theorem 4 are non-empty. Although running the same experiments on cryptographic parameters is not feasible (as the experiment is in fact a key recovery attack against UOV), we expect the proportion of generic keys to tend to 1 when n, m, o are increased. A goal for future work is to provide probability bounds similar to Corollary 3 for every Zariski-open set defined in this paper.

Note that we also ran experiments to verify the widely accepted fact that randomly sampled UOV public keys form regular sequences. Unsurprisingly, this holds for 100% of our samples (same setup as in Figure 1, 1000 keys drawn uniformly at random for various parameter sets). Also note that being a regular sequence is a weaker property than belonging to $\mathcal{U}_{n,m,o,q}$ or $\mathcal{M}_{r,n,m,o,q}$.

7 Applications to the analysis of UOV and its variants

The goal of this section is to discuss various regularity assumptions that are used in the study of the correctness and complexity of attacks against UOV and its variants. More precisely, we show that a large number of assumptions made in the field of multivariate cryptanalysis can be proven generic under the framework introduced above, in the sense that any UOV key lying in one of the Zariski-open sets defined in the previous sections also satisfy these assumptions. We believe that this strongly supports the relevance of our genericity-based approach.

We also provide examples of cryptographic schemes whose keys are non-generic. In many cases, the schemes or some subset of weak keys could be successfully broken, some of the attacks precisely leveraging non-generic properties that we identify retrospectively. We also describe one case where experiments suggests that using non-generic behavior to build a distinguisher could remain as hard as directly attacking the scheme. This shows that genericity is a nice property to have but it is not a necessary and sufficient condition for security. We therefore believe that genericity should come as a good practice in multivariate cryptography: while it may sometimes not be necessary and provides no absolute guarantee, it can definitely thwart some elementary attacks, and often comes at a limited cost in the size of parameters.

7.1 Direct attack against UOV

We begin with the most fundamental attack against UOV, which is the direct attack, i.e. attempting to obtain forgeries for arbitrary messages by solving a quadratic polynomial system of equations. A strong motivation to study the behavior of this attack is that it is the dimensioning attack against most UOV parameters (i.e. the fastest attack at the time of writing). Let us consider a UOV (n, m, o, q) instance, denoted by $\mathcal{P} = (p_1, \dots, p_m)$ and with $\mathcal{I} = \langle p_1, \dots, p_m \rangle$.

Given $\mathbf{t} \in \mathbb{F}_q^m$ a target drawn uniformly at random, the task of an (EUF-CMA) attacker is to find at least one element $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathcal{P}(\mathbf{x}) = \mathbf{t}$. The direct attack is a method to approach this task which consists in reducing this polynomial system of m equations in n variables to a zero-dimensional quadratic polynomial system of equations. This can be done in two manners:

- *Method 1*: adding $r = \max(n - m, o)$ random linear polynomials $h_1, \dots, h_r$ to the system, which corresponds to intersecting the variety $V = V(\langle p_1 - t_1, \dots, p_m - t_m \rangle)$ with $\dim V$ hyperplanes in general position.

- *Method 2*: running a precomputation (e.g. [61,18,38]) to reduce this task to solving a polynomial system of strictly smaller codimension, which has a similar geometric interpretation but where the hyperplanes are not chosen uniformly at random.

This has two motivations: first, when the codimension is fixed, the cost of finding a solution to a polynomial systems of equations decreases when the number of variables decreases. Second, it is in general much harder to compute Gröbner bases of positive-dimension ideals –especially compared to the tools available in dimension zero, for instance the FGLM algorithm [28] whose complexity is well understood when the ideal is in shape position. After applying either of these methods, a solution of the zero-dimensional system is obtained using either a Gröbner basis algorithm [45,31,19,26], or by combining such an algorithm with partial enumeration in a hybrid method [5].

The complexity analysis of the direct attack against UOV is made through the assumption that the sequence $p_1, \dots, p_m$ is a regular sequence [11], which we have proven to be a generic property of UOV keys in Corollary 1 for all elements of $\mathcal{U}_{n,m,o,q}$ when $m \leq o$, which encapsulates all UOV parameters submitted to NIST. Then, under Fröberg’s conjecture [32], the overdetermined polynomial systems to be solved in a hybrid approach are semi-regular, since $p_1, \dots, p_m$ forms a regular sequence. Note that, although Fröberg’s conjecture is stated over the field of complex numbers, it is expected to hold regardless of the field (as stated in [32]) and it would be a significant achievement to find a finite field over which it fails. Also note that when the system is slightly overdetermined, i.e. has one or two more equations than variables, Fröberg’s conjecture has been established [62] (under further assumptions for the case of two more equations).

Regularity is a desirable property for a multivariate signature scheme, and it was verified for the main multivariate competitors of the UOV variants, namely HFE [49] and its successors (see [17]): the HFE public key system was not a regular sequence, and could be distinguished from a regular sequence at a relatively low degree (see e.g. [52]).

There exists parameters of UOV, typically when $n - m < o$, such that the public key does not form a regular sequence either. This was the case in the first versions of MAYO [7], but was changed in the second version of the NIST submission [10]. This specific dimension issue was highlighted in the changelog of the second version of the NIST submission [10] as the reason for this change, although the submitters were not aware of attacks leveraging this non-genericity. In addition, we point out that both QR-UOV [35,34] and SNOVA [64] can be mapped to UOV instances where $n - m < o$ (the *big field* instances), which prevents our genericity results from being applied to the big field direct attack against these schemes. A significant difference between these schemes and HFE however, is that experimental data (see e.g. [34, Table 9]) suggests that the degree of regularity required to attack big field instances matches the expected degree of regularity of a semi-regular sequence [3] with the same number of quadratic polynomials and variables. This is an example where non-genericity does not seem to lead to an attack. A more pragmatic approach can be taken: trying

to achieve genericity by default and, when deemed necessary, identifying and justifying any non-generic behavior in terms of expected gain (i.e. improvement of performance) and security (i.e. justifying why non-genericity does not lead to improved attacks).

7.2 Direct attack against MAYO

Recall that a $\text{MAYO}(n, m, o, q, k)$ public key is a $\text{UOV}(n, m, o, q)$ map $\mathcal{P}$, where the parameters satisfy $ko \geq m$. The direct attack against MAYO depends on the whipped map $\mathcal{P}^*$ defined by

$$\mathcal{P}^*(\mathbf{x}_1, \dots, \mathbf{x}_k) = \sum_{1 \leq i < j \leq k} E_{i,j} \mathcal{P}'(\mathbf{x}_i, \mathbf{x}_j) + \sum_{1 \leq i \leq k} E_{i,i} \mathcal{P}(\mathbf{x}_i),$$

where the matrices $E_{i,j} \in \mathbb{F}_q^{m \times m}$ are multiplication matrices in $\mathbb{F}_q^m$. Given $\mathbf{t} \in \mathbb{F}_q^m$ a target drawn uniformly at random, the task of an (EUF-CMA) attacker is to find at least one element $(\mathbf{x}_1, \dots, \mathbf{x}_k) \in \mathbb{F}_q^{kn}$ such that:

$$\mathcal{P}^*(\mathbf{x}_1, \dots, \mathbf{x}_k) = \mathbf{t}.$$

This is an instance of the $\text{UOV}(kn, m, ko, q)$ forgery problem, where by design $m \leq ko < kn$, a regime in which Theorem 2 applies. However, whipped MAYO maps are (clearly) not generic among $\text{UOV}(kn, m, ko, q)$ maps, thus a dedicated analysis is required to prove the regularity of the sequence $\mathcal{P}^*$. It is sufficient to show that the collection of quadratic polynomials of $\mathcal{P}$ has codimension m , which is possible with Theorem 3 when $n - m > o$. The currently proposed parameters of Mayo [10] feature $n - m = o$, therefore a direct application of the Theorem fails. The only failure point is Lemma 3, and one can fix it by constructing a smaller set of singular points of the variety: indeed, the use of Lemma 3 in Theorem 3 relies on the assumption that singular points may only lie in $\mathcal{O}$; in practice, one expects that singular points lie in a strict subvariety of $\mathcal{O}$, which can be shown for generic keys via Theorem 4. Thus we expect that the result can be extended to the case $n - m = o$, but no further since if $n - m < o$ the dimension of the variety already disqualifies $\mathcal{P}$ as a regular sequence.

For such generic Mayo keys, it holds that $\mathcal{P}$ forms a regular sequence. Then it must be the case that $\mathcal{P}^*$ also forms a regular sequence, since it is obtained by an invertible linear combination of polynomials $(\mathcal{P}'(X_i, X_j))_{1 \leq i < j \leq k}$. Indeed, otherwise one could construct a non-trivial syzygy of $\mathcal{P} \in \mathbb{F}_q[X_1, \dots, X_n]^m$ by specialising $\mathcal{P}^*$ to $\mathcal{P}^*((X_1, \dots, X_n), 0, \dots, 0)$.

7.3 Wedge attack

Recently, progress in the cryptanalysis of UOV and its variants has been achieved by the Wedge Attack of [53] which improves the cryptanalysis over field extensions of small characteristic. The main heuristic on which this attack relies is [53, Conjecture 1], which requires that for parameters $(n, m, o, q = 2^\ell)$, if

$\min(\frac{o-1}{2}, 2) \cdot m > n - o > o$, then the public key polynomials $p_1, \dots, p_m$ form a semi-regular sequence over $\mathbb{F}_q/\langle x_1^2, \dots, x_n^2 \rangle$. Corollary 1 shows the regularity of the sequence over $\mathbb{F}_q$, which is a first step towards the full statement of Ran.

Note also that the analysis of parasitic solutions to the Wedge Attack in [53, Section 3.4] performs a heuristic count that can be formalized precisely using the Debarre and Manivel bound [22, Théorème 2.1] to obtain a dimension result, and then the count of rational solutions can be derived from the Lang-Weil estimate [44, Lemma 1]. Both methods agree but ours no longer relies on a heuristic.

7.4 Tangent spaces and key recovery from one vector

Consider a UOV (n, m, o, q) instance, denoted by $\mathcal{P} = (p_1, \dots, p_m)$, with $\mathcal{I} = \langle p_1, \dots, p_m \rangle$ and with trapdoor $\mathcal{O} \subset V(\mathcal{I})$. In [50], a polynomial-time algorithm performing key recovery from one element $\mathbf{x} \in \mathcal{O}$ is introduced, relying on regularity assumptions summarized in [50, Theorem 1]. These assumptions are readily verified for regular points but no longer hold for singular points. This could be a problem in practice, as finding points in $\mathcal{O}$ can be done via the Kipnis-Shamir attack [42], which always return singular points of $V(\mathcal{I})$ (see [46, 51]). Similarly, [59] shows that the Rectangular MinRank attacks against UOV and its variants compute singular points, sometimes inducing higher rank defects than 1.

It is therefore relevant to ensure that the algorithm from [50] is also successful when run on singular points, and it had been addressed informally in [50, Remark 3]. In this section, we show that the algorithm from [50] always runs correctly (even on singular points) for generic UOV keys.

Remark 4. When we apply Theorem 4 to the case $r = 2$, the dimension formula specializes to $\delta = 3o + 2m - 2n - 5$. If $\delta < 0$, then singular points of a generic UOV variety only decrease the rank of the Jacobian matrix by 1. In that case, [50, Algorithm (a)] will not fail on singular points of the UOV variety. This is the case for all UOV parameters in the regime $\frac{n}{m} = \frac{5}{2}$, which corresponds to those submitted to the NIST competition.

More generally, the constraint for the algorithm to succeed is that the dimension of the tangent space at the input point is smaller than $2o$.

7.5 Rectangular MinRank attack and Singular point attack

It has been shown in [46, 51] that singular point computations yield key recovery attacks against UOV. For mainstream UOV parameters ($n = \frac{5}{2}m$), we have seen in Remark 4 that the rank defect at a singular point of a generic UOV key is expected to be at most 1. For UOV variants, the rank defect in the Jacobian matrix evaluated at a point of $\mathcal{O}$ can be strictly greater than 1, which enables an attacker to find some singular points by solving a system of equations of lower degrees. The larger the rank defect, the more we can expect to decrease the cost of the resulting attack. This idea was introduced in [59], who linked singular point attacks with the Rectangular MinRank attack [8, 33].

In [59], the success of the attack relies on two assumptions on UOV varieties. The tools introduced in Section 4 enable us to prove that both of these assumptions are Zariski-generic.

Dimension of the UOV variety. To apply the Jacobian criterion [25, Theorem 16.19] to design a MinRank attack, it is necessary to know the dimension of the variety, thus [59, Hypothesis 12] asks that $\dim V(\mathcal{I}) = \max(n - m, o)$. Theorem 3 shows that [59, Hypothesis 12] holds on the Zariski open set $\mathcal{U}_{n,m,o,q}$, which is non-empty when $m \leq o$ and $m \leq n$ by Theorem 2.

No singular points outside of $\mathcal{O}$. To turn such a MinRank into a key recovery attack, one needs to estimate the number, if any, of parasitic solutions (solutions that are not related to the secret key). More precisely, [59, Hypothesis 14] asks that $\text{Sing}V(\mathcal{I}) \subset \mathcal{O}$ and provides experimental results supporting such a claim, following a similar assumption made in [51, Hypothesis 1]. When $m \leq o$ and $m \leq n$, we have shown in Theorem 2 above that this holds generically in **any finite field**. Note that this had already been proven to be Zariski-generic in a large enough prime field in [51]. By working in arbitrary finite fields instead, our results also directly support the analysis of the Kipnis-Shamir attack [42] as pointed out in [51, Hypothesis 1, Hypothesis 2].

Genericity beyond UOV. The same paper introduces an original heuristic [59, Heuristic 20] to study the correctness of their Extended MinRank attack. When $o < n - m$, our Theorem 4 shows that this heuristic is generically satisfied by UOV keys. However, as mentioned earlier, our theorem does not guarantee that this remains the case for the attacks of [59] targeting SNOVA and QR-UOV, as $o > n - m$. Furthermore, for all UOV keys lying in the Zariski-open set defined in Theorem 4, we show that the determinantal ideal defining the singular points is radical, which was also a requirement to obtain linear polynomials in the algebraic attacks of [51, Proposition 1].

Note that we **do not** recommend building non-generic multivariate schemes in the hope of defeating cryptanalytic assumptions. Indeed, the complexity of solving generic systems is much better understood, leading to safer options for the design of cryptographic primitives.

7.6 Forgery attacks and weak SNOVA keys

In [9], a forgery attack is obtained on the SNOVA Round 1 submission to NIST [63] by finding rank defects in some matrices related to the public key. Beulens observes that all keys are vulnerable to such an attack with a low rank defect, however a fraction of all keys is exposed to higher rank defects. Notice that using the tools introduced earlier, for instance Theorem 4, one may be tempted to dismiss these weak keys as non-generic. This would be a misuse of our work: in cryptography, the consensus is that accidental events such as weak keys or decryption failures must only occur with a dramatically small probability, depending on the security level (e.g. 2^{-128} for NIST level I). Showing that a

property is generic, however, is a topological result that does not say anything *a priori* on the probability that such a property holds, unless a deeper analysis is performed, as in Corollary 3.

8 Conclusion

In this paper, we used the classical notion of Zariski genericity with a dual purpose. On the one hand, we show that numerous heuristics made by the community can indeed be shown to be generic in the sense of the Zariski topology, providing solid theoretical grounds to assumptions that have been hanging around for decades. On the other hand, we also suggest that genericity should be used in the design and analysis of multivariate schemes. This novel idea (to the best of our knowledge) significantly extends the applications of results like Theorems 2 and 4 as they could play a role in the design of cryptosystems.

A future line of work is to extend this approach to other families of post-quantum schemes. An example of non-generic behavior is the use of quadratic relations in [20,54,14], leading both to faster distinguishers and attacks. The main difficulty is that such generic properties seem much less natural than the ones introduced here, which are quite common in algebraic geometry.

Finally, an important next step is to derive (upper bounds for) the dimension of the Zariski-closed sets defining $\mathcal{U}_{n,m,o,q}$ and $\mathcal{M}_{r,n,m,o,q}$ in order to obtain upper bounds on the probability to draw non-generic UOV keys uniformly at random for a given parameter set.

References

1. Arora, S., Ge, R.: New algorithms for learning in presence of errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) Automata, Languages and Programming. pp. 403–415. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
2. Atiyah, M.F., MacDonald, I.: Introduction to commutative algebra. CRC press (1969)
3. Bardet, M., Faugère, J.C., Salvy, B.: Asymptotic Behaviour of the Index of Regularity of Semi-Regular Quadratic Polynomial Systems. In: MEGA 2005 - 8th International Symposium on Effective Methods in Algebraic Geometry. pp. 1–17. Porto Conte, Alghero, Sardinia, Italy (May 2005), <https://hal.science/hal-01486845>
4. Berthomieu, J., Eder, C., Safey El Din, M.: 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>
5. Bettale, L., Faugère, J., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. **3**(3), 177–197 (2009). <https://doi.org/10.1515/JMC.2009.009>, <https://doi.org/10.1515/JMC.2009.009>
6. 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
7. 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
 8. 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
 9. Beullens, W.: Improved cryptanalysis of snova. In: Fehr, S., Fouque, P.A. (eds.) Advances in Cryptology – EUROCRYPT 2025. pp. 277–293. Springer Nature Switzerland, Cham (2025)
 10. Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.J.: Mayo, NIST round 2 (2025), <https://pqmayo.org/assets/specs/mayo-round2.pdf>, consulted 06/06/2025
 11. 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
 12. Beullens, W., Chen, M., Hung, S., Kannwischer, M.J., Peng, B., Shih, C., Yang, B.: Oil and vinegar: Modern parameters and implementations. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2023**(3), 321–365 (2023). <https://doi.org/10.46586/tches.v2023.i3.321-365>, <https://doi.org/10.46586/tches.v2023.i3.321-365>
 13. Bourbaki, N.: Commutative Algebra: Chapters 1–7. Elements of Mathematics, Springer, Berlin, Heidelberg, New York (1981), translated from the French
 14. Briaud, P., Lemoine, A., Randriambololona, H., Tillich, J.P.: A heuristic subexponential attack on the McEliece cryptosystem. Cryptology ePrint Archive, Paper 2026/1232 (2026), <https://eprint.iacr.org/2026/1232>
 15. Bruns, W., Vetter, U.: Determinantal Rings. Springer Berlin Heidelberg, Berlin, Heidelberg (1988). <https://doi.org/10.1007/BFb0080379>
 16. Bulygin, S., Petzoldt, A., Buchmann, J.: Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks. Cryptology ePrint Archive, Paper 2010/420 (2010), <https://eprint.iacr.org/2010/420>
 17. Casanova, A., Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: Gemss: A great multivariate short signature (2017), <https://api.semanticscholar.org/CorpusID:8432066>
 18. Cheng, C.M., Hashimoto, Y., Miura, H., Takagi, T.: A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics. In: Mosca, M. (ed.) Post-Quantum Cryptography. pp. 40–58. Springer International Publishing, Cham (2014)
 19. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Preneel, B. (ed.) Advances in Cryptology — EUROCRYPT 2000. pp. 392–407. Springer Berlin Heidelberg, Berlin, Heidelberg (2000)

20. Couvreur, A., Mora, R., Tillich, J.P.: A new approach based on quadratic forms to attack the mceliece cryptosystem. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 3–38. Springer (2023)
21. 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)
22. Debarre, O., Manivel, L.: Sur la variété des espaces linéaires contenus dans une intersection complète. *Math. Annalen* **312** (1998), 549–574 (1998). <https://doi.org/https://doi.org/10.1007/s002080050235>
23. DeMillo, R.A., Lipton, R.J.: A probabilistic remark on algebraic program testing. *Information Processing Letters* **7**(4), 193–195 (1978). [https://doi.org/https://doi.org/10.1016/0020-0190\(78\)90067-4](https://doi.org/https://doi.org/10.1016/0020-0190(78)90067-4), <https://www.sciencedirect.com/science/article/pii/0020019078900674>
24. Diem, C.: The xl-algorithm and a conjecture from commutative algebra. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 323–337. Springer (2004)
25. Eisenbud, D.: Commutative Algebra with a view toward Algebraic Geometry. Springer New York (1995)
26. Faugère, J.C.: A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. p. 75–83. ISSAC ’02, Association for Computing Machinery, New York, NY, USA (2002). <https://doi.org/10.1145/780506.780516>, <https://doi.org/10.1145/780506.780516>
27. Faugère, J.C., Perret, L., De Portzamparc, F.é.: Algebraic attack against variants of mceliece with goppa polynomial of a special form. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 21–41. Springer (2014)
28. Faugère, J., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation* **16**(4), 329–344 (1993). <https://doi.org/https://doi.org/10.1006/jsco.1993.1051>, <https://www.sciencedirect.com/science/article/pii/S0747717183710515>
29. Faugère, J.C., Perret, L.: On the security of UOV. *Cryptology ePrint Archive*, Paper 2009/483 (2009), <https://eprint.iacr.org/2009/483>
30. 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>
31. Faugère, J.C.: A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra* **139**(1), 61–88 (1999). [https://doi.org/https://doi.org/10.1016/S0022-4049\(99\)00005-5](https://doi.org/https://doi.org/10.1016/S0022-4049(99)00005-5), <https://www.sciencedirect.com/science/article/pii/S0022404999000055>
32. Froberg, R.: An inequality for hilbert series of graded algebras. *Mathematica Scandinavica* **56**, 117–144 (1985)
33. 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

34. Furue, H., Ikematsu, Y., Hoshino, F., Takagi, T., Yasuda, K., Miyazawa, T., Saito, T., Nagai, A.: QR-UOV specification (2023), <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/gruov-spec-web.pdf>, consulted 08/02/2024
35. 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)
36. Gaggero, G., Gorla, E.: The complexity of solving a system of equations of the same degree (2026), <https://arxiv.org/abs/2309.03855>
37. Giusti, M., Lecerf, G., Salvy, B.: A gröbner free alternative for polynomial system solving. *Journal of Complexity* **17**(1), 154–211 (2001). <https://doi.org/https://doi.org/10.1006/jcom.2000.0571>, <https://www.sciencedirect.com/science/article/pii/S0885064X00905715>
38. Hashimoto, Y.: An improvement of algorithms to solve under-defined systems of multivariate quadratic equations. *JSIAM Letters* **15**, 53–56 (2023). <https://doi.org/10.14495/jsiaml.15.53>
39. Heintz, J., Schnorr, C.P.: Testing polynomials which are easy to compute (extended abstract). In: *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing*. p. 262–272. STOC '80, Association for Computing Machinery, New York, NY, USA (1980). <https://doi.org/10.1145/800141.804674>, <https://doi.org/10.1145/800141.804674>
40. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science* **24**(3), 239–277 (1983). [https://doi.org/https://doi.org/10.1016/0304-3975\(83\)90002-6](https://doi.org/https://doi.org/10.1016/0304-3975(83)90002-6), <https://www.sciencedirect.com/science/article/pii/0304397583900026>
41. Kemper, G.: *A Course in Commutative Algebra*, Graduate Texts in Mathematics, vol. 256. Springer, Berlin, Heidelberg (2011). <https://doi.org/10.1007/978-3-642-03545-4>
42. 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
43. 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>
44. Lang, S., Weil, A.: Number of points of varieties in finite fields. *American Journal of Mathematics* **76**(4), 819–827 (1954), <http://www.jstor.org/stable/2372655>
45. Lazard, D.: Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (ed.) *Computer Algebra*. pp. 146–156. Springer Berlin Heidelberg, Berlin, Heidelberg (1983)
46. Luyten, P.: Understanding Kipnis Shamir with two quadrics (2023), Master thesis, KU Leuven
47. Makarim, R.H., Stevens, M.: M4gb: An efficient gröbner-basis algorithm. In: *Proceedings of the 2017 ACM International Symposium on Symbolic and Alge-*

- braic Computation. p. 293–300. ISSAC '17, Association for Computing Machinery, New York, NY, USA (2017). <https://doi.org/10.1145/3087604.3087638>, <https://doi.org/10.1145/3087604.3087638>
48. Pardue, K.: Generic sequences of polynomials. *Journal of Algebra* **324**(4), 579–590 (2010). <https://doi.org/10.1016/j.jalgebra.2010.04.018>, <https://www.sciencedirect.com/science/article/pii/S0021869310001948>
49. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U. (ed.) *Advances in Cryptology — EUROCRYPT '96*. pp. 33–48. Springer Berlin Heidelberg, Berlin, Heidelberg (1996)
50. Pébereau, P.: One vector to rule them all: Key recovery from one vector in UOV schemes. In: Saarinen, M.O., Smith-Tone, D. (eds.) *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024*, Oxford, UK, June 12–14, 2024, *Proceedings, Part II. Lecture Notes in Computer Science*, vol. 14772, pp. 92–108. Springer (2024). https://doi.org/10.1007/978-3-031-62746-0_5, https://doi.org/10.1007/978-3-031-62746-0_5
51. Pébereau, P.: Singular points of UOV and VOX. In: Fehr, S., Fouque, P. (eds.) *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Madrid, Spain, May 4–8, 2025, *Proceedings, Part VI. Lecture Notes in Computer Science*, vol. 15606, pp. 294–323. Springer (2025). https://doi.org/10.1007/978-3-031-91095-1_11, https://doi.org/10.1007/978-3-031-91095-1_11
52. Petzoldt, A.: On the complexity of the hybrid approach on HFEv-. *Cryptology ePrint Archive*, Paper 2017/1135 (2017), <https://eprint.iacr.org/2017/1135>
53. Ran, L.: Wedges, oil, and vinegar. In: Daemen, J., Thomé, E. (eds.) *Advances in Cryptology – EUROCRYPT 2026*. pp. 363–388. Springer Nature Switzerland, Cham (2026)
54. Randriambololona, H.: The syzygy distinguisher. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. pp. 324–354. Springer (2025)
55. Safey el Din, M., Schost, É.: A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete & Computational Geometry* **45**(1), 181–220 (Jan 2011). <https://doi.org/10.1007/s00454-009-9239-2>, <https://doi.org/10.1007/s00454-009-9239-2>
56. Safey El Din, M., Schost, E.: A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM* **63**(6) (jan 2017). <https://doi.org/10.1145/2996450>, <https://doi.org/10.1145/2996450>
57. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. *J. ACM* **27**(4), 701–717 (Oct 1980). <https://doi.org/10.1145/322217.322225>, <https://doi.org/10.1145/322217.322225>
58. Shafarevich, I.R.: *Basic algebraic geometry*; 3rd ed. Springer, Berlin (2013). <https://doi.org/10.1007/978-3-642-37956-7>, <https://cds.cern.ch/record/1596976>
59. Suzuki, T., Furue, H., Ito, T., Nakamura, S., Uchiyama, S.: An extended rectangular minrank attack against uov and its variants. In: Cid, C., Yanai, N. (eds.) *Advances in Information and Computer Security*. pp. 111–130. Springer Nature Singapore, Singapore (2026)
60. Takahashi, Y., Kudo, M., Fukasaku, R., Ikematsu, Y., Yasuda, M., Yokoyama, K.: Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology* **15**(1), 31–44 (2020)

61. Thomae, E., Wolf, C.: Solving underdetermined systems of multivariate quadratic equations revisited. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7293, pp. 156–171. Springer (2012). https://doi.org/10.1007/978-3-642-30057-8_10, https://doi.org/10.1007/978-3-642-30057-8_10
62. Trung, V.D.: The initial ideal of generic sequences and fr\"berg's conjecture. arXiv preprint arXiv:1803.04997 (2018)
63. 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
64. Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: SNOVA (2025), <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf>, consulted 29/08/2025
65. Zariski, O., Samuel, P.: Commutative Algebra. Springer Berlin, Heidelberg, 1 edn. (1960)
66. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. p. 216–226. EUROSAM '79, Springer-Verlag, Berlin, Heidelberg (1979)

A Construction of the example of Theorem 2

Our construction may seem quite ad hoc at first sight, therefore we explain how it was obtained. In the previous proof, our method was to first construct a polynomial matrix J in $\mathbb{K}[X_1, \dots, X_n]^{m \times n}$ with entries that are linear forms, ensuring that it is a plausible Jacobian matrix of a homogeneous quadratic map. Then, we obtained the map through formal integration as indeed we may read the coefficients of f_k from its partial derivatives:

$$\forall 1 \leq k \leq m, \quad f_k = \sum_{o+1 \leq i \leq j \leq n} f_{i,j}^{(k)} X_i X_j,$$

$$\forall 1 \leq k \leq m, \quad 1 \leq j \leq n, \quad \frac{\partial f_k}{\partial X_j} = 2f_{j,j} X_j + \sum_{i \neq j} f_{i,j}^{(k)} X_i.$$

Notice that the coefficient $f_{i,j}^{(k)}$ appears both in $\frac{\partial f_k}{\partial X_j}$ and in $\frac{\partial f_k}{\partial X_i}$, thus we must respect the following “commutativity rule” in order to define a valid Jacobian:

$$\frac{\partial f}{\partial X_i} = X_j + \dots \iff \frac{\partial f}{\partial X_j} = X_i + \dots \quad (14)$$

In characteristic not 2, any polynomial matrix whose entries are linear forms respecting this rule is a valid Jacobian matrix of a homogeneous quadratic map. In characteristic 2, there is an additional difficulty as there is no primitive to X_j with respect to X_j .

The goal of our construction is to obtain a Jacobian matrix where each vinegar indeterminate appears exactly once per row (ie per polynomial) and in at least m columns, so that we may extract full rank m -minors when at least one is non-zero. This explains the choice of indices: $\frac{\partial f_k}{\partial X_{n-i+1}} = X_{o-(k-1)+i}$. If we index i from 1 to $n - o$, we are counting some monomials twice when

$$o - (k - 1) + i \geq n - i + 1 \iff 2i \geq n - o + k,$$

therefore we stop halfway. When $2i = n - o + k$, we would get a square term $X_{o+i-(k-1)}^2$ which would prevent the construction from succeeding in characteristic two. This happens for half of the values of k , as this behavior requires that $n - o + k$ be even. Thus, we replace this term by $X_1 X_{o+i-(k-1)}$ which is a valid choice only when $m \geq o$.

Finally, as we must define an element of $\mathcal{K}_{n,m,o,q}$, a UOV secret key, we also require that J does not depend on $X_1, \dots, X_o$ in the columns corresponding to $\partial X_1, \dots, \partial X_o$, which ensures that the primitive map is indeed linear in $X_1, \dots, X_o$ and thus a valid UOV secret map. The natural construction in characteristic not 2 is the following Toeplitz matrix, and we simply tweaked the square terms as mentionned previously to obtain a result also in characteristic 2 which is the construction obtained in the proof.

$$J = \begin{bmatrix} \partial X_n & \partial X_{n-1} & \cdots & \partial X_{n-m} & \partial X_{n-m-1} & \cdots & \partial X_{o+1} & \cdots & \partial X_{o+1-m} & \cdots & \partial X_1 \\ X_{o+1} & X_{o+2} & \cdots & X_{o+1+m} & X_{o+2+m} & \cdots & X_n & & & & \\ X_o & X_{o+1} & \ddots & X_{o+m} & X_{o+1+m} & & & \ddots & & & \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & & & & \\ X_{o+1-m} & X_{o+2-m} & \cdots & X_{o+1} & X_{o+2} & \cdots & & & X_n & & \end{bmatrix}.$$

B Preliminary probability result for $\mathcal{U}_{n,m,o,q}$

Corollary 3. *Let $\mathbb{K}$ be a field and $S \subset \mathbb{K}$ be a finite set of cardinality σ . Let (n, m, o) be UOV parameters with $n \geq m$ and $n > 0$ and let $\mathcal{U}_{n,m,o,\mathbb{K}}$ be the Zariski open set defined in Theorem 1.*

Then, $\mathcal{U}_{n,m,o,\mathbb{K}}$ is a non-empty Zariski open set and the probability that a point in S does not lie in $\mathcal{U}_{n,m,o,\mathbb{K}}$ is at most $\frac{(2m)^{n-m} 3^m}{\sigma}$.

Proof. Both, the facts that $\mathcal{U}_{n,m,o,\mathbb{K}}$ is Zariski open and non-empty are restatements of Theorems 1 and 2.

By Theorem 1, the complementary $\mathcal{Z}$ of $\mathcal{U}_{n,m,o,\mathbb{K}}$ has strong degree at most $(2m)^{n-m} 3^m$. In other words, letting $\mathcal{Z}_1, \dots, \mathcal{Z}_\ell$ be the irreducible components of $\mathcal{Z}$ of respective degrees $\delta_1, \dots, \delta_\ell$, it holds that $\delta_1 + \dots + \delta_\ell \leq (2m)^{n-m} 3^m$. Let I_i be the ideal associated to $\mathcal{Z}_i$. Note that I_i is prime (because $\mathcal{Z}_i$ is irreducible) and distinct from $\{0\}$ since $\mathcal{Z}_i \neq \mathbb{K}^d$ by Theorem 2. Assume for the moment that we have proved that each I_i contains a non-zero polynomial g_i of degree no greater than δ_i . Then, the polynomial $g = g_1 \cdots g_\ell$ is non-zero and has degree no greater than $(2m)^{n-m} 3^m$ and lies in the ideal associated to $\mathcal{Z}$.

Our conclusion then follows from a straightforward application of the DeMillo, Lipton, Schwartz, Zippel lemma [23,57,66].

We prove now that for all $i \in \{1 \dots, \ell\}$, I_i contains a non-zero polynomial g_i of degree less than or equal to δ_i . Let $\{i_1, \dots, i_k\}$ be a minimal set (for the partial order induced by inclusion) such that $J_i = I_i \cap \mathbb{K}[\mathbf{c}_{i_1}, \dots, \mathbf{c}_{i_k}] \neq \{0\}$. Such a set exists since $I_i \neq \{0\}$. By [41, Theorem 5.9 and Proposition 5.10] applied to $\frac{\mathbb{K}[\mathbf{c}_{i_1}, \dots, \mathbf{c}_{i_k}]}{J_i}$, the codimension of J_i is 1. By the dimension formula [25, Corollary 13.4], we deduce that the height of J_i is 1 (codimension and height coincide here because $\frac{\mathbb{K}[\mathbf{c}_{i_1}, \dots, \mathbf{c}_{i_k}]}{J_i}$ is an affine domain since J_i is prime). By [13, Chap. 7, Theorem 1, pp. 502], we deduce that J_i is principal. Since $J_i \neq \{0\}$, it is generated by a non-zero polynomial g_i , whose vanishing set is the algebraic variety associated to J_i , hence a hypersurface which we denote by $\mathcal{H}_i$. By the closure theorem [21, Chap. 3, Theorem 3], $\mathcal{H}_i$ the Zariski closure of the projection of $\mathcal{Z}_i$ on the $(\mathbf{c}_{i_1}, \dots, \mathbf{c}_{i_k})$ coordinate subspace. Hence, the hypersurface $\mathcal{H}_i$ has degree bounded by δ_i (which is the degree of $\mathcal{Z}_i$, the algebraic set associated to $\mathcal{I}_i$) [40, Lemma 2]. Since J_i is prime, principal and generated by g_i , it holds that g_i is irreducible. We deduce that g_i has degree bounded by δ_i . $\square$