The Extended Wedge Attack

John Baena[1], Javier Verbel[2], Luis Villota[1]

[1] Universidad Nacional de Colombia sede Medellín, Medellín, Colombia
{jbbaena,ldvillotav}@unal.edu.co
[2] Technology Innovation Institute, Abu Dhabi, UAE
{javier.verbel}@tii.ae

Abstract. The wedge attack of Ran (EUROCRYPT 2026) recovers the secret oil space of a UOV public key over fields of characteristic two by exploiting the fact that the polar forms of the public map are alternating. It has since been generalized in several directions, each carrying its own algebraic tools, e.g., Jin et al. (PKC 2026). Working directly with the polynomials of an oil and vinegar map, we give a simpler description of the attack, based on a dual decomposition of oil-vinegar polynomials, and we recover the original wedge attack and its odd-characteristic analogue as special cases. This framework leads to a generalization, which we call the *extended wedge attack*. We identify two explicit conditions on the parameters that guarantee that the attack terminates with the recovery of the secret space. We also prove that the matrix of the extended wedge attack is permutation equivalent to the truncated Macaulay matrix in the attack by Furue-Ikematsu (CRYPTO 2026).

1 Introduction

Multivariate cryptography remains one of the most active areas in the search for post-quantum digital signature schemes. Among the many proposals that have appeared over the last three decades, the Unbalanced Oil and Vinegar (UOV) scheme [11] is one of the longest-standing. It has resisted cryptanalysis since its introduction and has served as the basis for several submissions to NIST's additional call for post-quantum signatures, including the UOV specification itself [4] and related constructions such as MAYO [3], QR-UOV [8], and SNOVA [13].

Most practical UOV-based schemes are defined over fields of characteristic 2, largely for efficiency reasons, and this choice introduces additional algebraic structure. Ran [12] observed that the polar forms associated with the public key map are then alternating, so they lie in the exterior algebra $\bigwedge^2 \mathbb{F}_q^n$, where $\mathbb{F}_q$ is a finite field of size $q = p^e$ with prime characteristic p. Exploiting the relationship between these polar forms and the Plücker embedding, his wedge attack recovers the oil space and lowers the claimed security of several UOV parameter sets.

The wedge attack was soon generalized in two directions: Jin et al. [10] reformulated it in terms of reduced symmetric algebras, and an updated version of Ran's work extends it to odd characteristic. Each generalization comes in its own algebraic language, which raises the question we address here: is there a common foundation in which both arise as instances of a single construction?

We give an affirmative answer, and it requires no exterior algebra. Working directly with the polynomial structure of an oil-and-vinegar map, we show that every polynomial in the public key admits a decomposition determined by the linear forms defining the oil space, and that recovering the oil space reduces to solving a linear system read off from that decomposition. The two existing formulations appear as the cases $p = 2$ and $p > 2$ of this single construction, which in turn leads to a generalization of the attack that we call the *extended wedge attack*.

1.1 Previous works

The wedge attack was introduced by Ran [12] for UOV-like signature schemes over fields of characteristic $p = 2$. It exploits the fact that in characteristic two the polar form of a homogeneous quadratic polynomial is alternating, and hence lies in the exterior power $\wedge^2\mathbb{F}_q^n$. Expressing these polar forms in terms of the dual of the secret oil space, Ran derives linear conditions on its Plücker coordinates and reduces the recovery of the oil space to finding a kernel vector of a large sparse linear map, whose analysis is based on a semi-regularity heuristic over $\mathbb{F}_{2^e}$. The attack lowers the security estimates of several UOV and MAYO parameter sets.

A generalization of the wedge attack was given by Jin et al. [10], who proposed an XL-like attack over the p-reduced symmetric algebra. In even characteristic, this algebra reduces to the exterior algebra used in the wedge attack. For odd characteristic p, it generalizes the construction by using a commutative product and imposing a maximum degree p on each variable. This preserves the isomorphism with the corresponding quotient polynomial ring modulo the ideal generated by the p-th powers of the variables.

In an updated version of [12], Ran also considered an extension of the attack to odd characteristic. In this setting, the polar forms are symmetric rather than alternating, and the Plücker embedding is used to formulate the corresponding subspace-recovery problem. This gives a version of the attack that applies over fields of odd characteristic and does not depend on a particular choice of the underlying prime.

More recently, Furue and Ikematsu [7] proposed another XL-like attack over p^ℓ-truncated polynomial rings

$$\mathbb{F}_{p^e}[x_1, \ldots, x_n] / \left\langle x_1^{p^\ell}, \ldots, x_n^{p^\ell} \right\rangle.$$

This attack generalizes the XL-like attack over p-reduced symmetric algebra by Jin et al. The authors also described how to apply their technique to improve the so-called intersection attack against the UOV family of signature schemes. Their complexity estimate rests on a semi-regularity conjecture, whose validity they assess experimentally. They observe that the predicted ranks are accurate in most cases but deviate for certain parameters, a discrepancy they attribute to the specific structure of UOV maps and leave as an open problem.

1.2 Contributions

We revisit the wedge attack from a purely polynomial perspective. This leads to a simpler description of the attack, a natural extension of the original construction, and a clearer understanding of the parameter regimes in which its behavior can be predicted. Our main results are summarized below.

A polynomial description of the wedge attacks. We show that the wedge attack can be developed entirely within the polynomial setting, without explicitly relying on exterior or reduced symmetric algebras. Our starting point is Theorem 1, which states that every polynomial in an OV map $\mathcal{P} \in \mathsf{OV}(p^e, n, o, m)$ belongs to an ideal $\langle \ell_1 \ldots, \ell_{n-o} \rangle$, where the ℓ_i's are homogeneous linear forms that define the oil space associated with $\mathcal{P}$. This yields a homogeneous linear system with a solution given by the coefficients of the polynomial $\ell_1^{p-1}\ell_2^{p-1}\cdots\ell_v^{p-1}$. We show that when $p = 2$, this is exactly the linear system in Ran's wedge attack [12], while for $p > 2$ we obtain the linear system of Jin et al. [10] at degree $o(p-1)$.

The Extended Wedge Attack. The polynomial framework also suggests a natural extension. Instead of working only with the first Frobenius level, we consider powers p^r with $r \geq 1$. The resulting algorithm, which we call the *extended wedge attack*, contains the existing attacks as the case $r = 1$. Choosing $r > 1$ expands the parameter regimes where the attack applies. For example, the extended wedge attack applies to all proposed parameters for MAYO, while Ran's attack only covers MAYO_2. We compare this approach with the attacks of Ran [12] and Jin et al. [10], and derive its complexity in Section 5.

Complexity analysis of the extended wedge attack. We provide a detailed complexity analysis of the extended wedge attack. First, we prove that the matrix $\mathcal{W}$ describing the linear system solved during the attack is permutation-equivalent to the degree-$o(p^r-1)$ truncated Macaulay matrix of the input map $\mathcal{P}$; we denote this truncated matrix by $\text{Mac}_{o(p^r-1)}(\mathcal{P})$. We then investigate when $\mathcal{W}$ can be expected to have a one-dimensional right kernel. We identify one heuristic assumption and two parameter constraints under which this holds: (1) $\mathsf{ker}(\text{Mac}_{o(p^r-1)}(\mathcal{P}_{rnd}))$ has trivial right kernel for a random homogeneous quadratic map $\mathcal{P}_{rnd}$ over $\mathbb{F}_q$ with the same numbers of variables and equations as $\mathcal{P}$, (2) $n - o < \min\{2m, m\frac{o-1}{2}\}$ Eqs. (17) and (18), which rules out the known cases in which $\mathsf{dim}(\mathsf{ker}(\mathcal{W}))$ is more than one; and (3) the condition $o < n - o$ to make OV maps indistinguishable from random homogeneous quadratic maps. Under these conditions, we derive explicit formulas for the cost of the extended wedge attack. The condition $o < n - o$ was not taking into account by Furue-Ikematsu [7], and its violation explains the deviations from semi-regularity shown by the experiments in §4.4 of that paper.

Experimental validation. We experimentally validated the correctness of the extended wedge attack for many small examples using a proof-of-concept implementation of the attack in Magma. For one of them we show how the whole

attack is carried out step by step; see Section 4.5. We evaluate the accuracy of our prediction of the dimension of $\ker(\mathcal{W})$ over 228 parameter sets covering the finite fields $\mathbb{F}_{2^4}$, $\mathbb{F}_{3^2}$, $\mathbb{F}_{3^4}$, and $\mathbb{F}_5$, $2 \le o \le 8$, and extension exponents $r \in \{1, 2, 3\}$, see Section 6. The prediction is correct in 225 cases. Every parameter set satisfying both Eq. (17) and Eq. (18) is correctly predicted, while each of the three failures violates one of these conditions.

Relation to the truncated-ring framework. We make the connection with [7] precise. In Theorem 2 we prove that the Macaulay matrix arising in their p^ℓ-truncated formulation and the matrix $\mathcal{W}$ of the extended wedge attack are equivalent, so that the two approaches produce the same linear algebra. This fact places the two lines of work on a common footing and allows results proved in either framework to be transferred to the other.

A bonus track. Finally, as a contribution of independent interest, we prove that the linear forms $\ell_1, \ldots, \ell_{n-o}$ defining the oil space $\mathcal{O}$, together with the field equations $x_1^q - x_1, \ldots, x_n^q - x_n$, form a Gröbner basis of the vanishing ideal $I(\mathcal{O})$. We believe this result may be useful in other investigations of OV-based constructions.

1.3 Organization of the paper

Section 2 fixes notation and recalls the background material we need: oil and vinegar maps, some signature schemes built from them, and the original wedge attack of Ran [12]. Section 3 develops the polynomial description of the wedge attacks: we introduce the dual decomposition of oil-vinegar polynomials, show how it leads to oil-space recovery, and check that the framework specializes to the original wedge attack when $p = 2$ and to the attack of Jin et al. [10] when $p > 2$. Section 4 introduces the extended wedge attack proper: the construction of the linear system, the recovery of the secret space from a kernel vector, the parameter regimes in which the attack is expected to work, and a toy example worked out in full. Section 5 derives the complexity of the attack, and Section 6 reports our experiments on the accuracy of the resulting kernel-dimension prediction. Section 7 then compares our approach with the truncated-ring framework of Furue and Ikematsu [7]. Two appendices close the paper: Section A proves that the linear forms associated with the secret space of an oil and vinegar map, together with the field equations, form a Gröbner basis of the vanishing ideal of that space, and Section B recalls the intersection attack on OV maps.

2 Preliminaries

2.1 Notation

Throughout this paper we use the following notation. We use $\mathbb{F}_q$ to denote a finite field of size $q = p^e$, where p is its characteristic. We denote by

$$R = \mathbb{F}_q[x_1, \ldots, x_n]$$

the polynomial ring, with a fixed monomial ordering $\prec$, in the variables $x_1, \ldots, x_n$ and coefficients in $\mathbb{F}_q$. For each integer r satisfying $1 \leq r \leq e$, we define the quotient ring

$$R^{(p^r)} := R/\langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle.$$

The *polar form* of a homogeneous quadratic polynomial $p \in R$ is the bilinear map $p'(\mathbf{x}, \mathbf{y}) = p(\mathbf{x}+\mathbf{y}) - p(\mathbf{x}) - p(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Similarly, the *polar form* of a map $\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, where each p_i is a homogeneous quadratic polynomial in R, is the bilinear map $\mathcal{P}'(\mathbf{x}, \mathbf{y}) = \mathcal{P}(\mathbf{x}+\mathbf{y}) - \mathcal{P}(\mathbf{x}) - \mathcal{P}(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$.

For a nonempty $A \subseteq \mathbb{F}_q^n$, we write

$$I(A) := \{f(\mathbf{x}) \in R : f(\mathbf{x}) = 0 \ \forall \mathbf{x} \in A\}.$$

We write $\binom{[n]}{k}$ to denote the set of subsets of $[n] := \{1, \ldots, n\}$ of size k, i.e.,

$$\binom{[n]}{k} := \{J \subset \{1, \ldots, n\} : |J| = k\}.$$

For $\mathbf{M} \in \mathbb{F}_q^{m \times n}$, where $m < n$, we denote by $\det(\mathbf{M}_J)$ the maximal minor of $\mathbf{M}$ obtained by selecting the columns indexed by $J \in \binom{[n]}{m}$. The orthogonal complement of a vector space $\mathcal{O}$ is denoted by $\mathcal{O}^\perp$.

2.2 Oil and Vinegar Maps

Oil–Vinegar (OV) maps provide the algebraic foundation of several multivariate signature schemes. Their defining feature is the existence of a hidden subspace on which a collection of quadratic polynomials simultaneously vanishes [2]. This hidden structure enables efficient computations while serving as the secret information underlying the corresponding cryptographic constructions.

Let $n, o, m \in \mathbb{N}$, we define the set of OV maps, denoted by $\mathsf{OV}(q, n, o, m)$, as the set of all sequences of homogeneous quadratic polynomials $\mathcal{P} = (p_1, \ldots, p_m)$ for which there exists an o-dimensional vector space $\mathcal{O} \subseteq \mathbb{F}_q^n$, called the oil space of $\mathcal{P}$, such that $p_i(\mathbf{x}) = 0$ for every $\mathbf{x} \in \mathcal{O}$ and every $1 \leq i \leq m$.

2.3 Signature Schemes Based on OV Maps

The Unbalanced Oil and Vinegar (UOV) signature scheme [4] is one of the best-known cryptographic constructions based on OV maps. In UOV, the private key is an m-dimensional vector space $\mathcal{O} \subset \mathbb{F}_q^n$. The public key consists of a sequence of homogeneous quadratic polynomials

$$\mathcal{P} = (p_1, \ldots, p_m)$$

forming an $\mathsf{OV}(q, n, m, m)$ sequence with oil space $\mathcal{O}$. A signature of a message msg is a pair $(\mathbf{x}, \mathsf{salt}) \in \mathbb{F}_q^n \times \{0,1\}^{|\mathsf{salt}|}$ such that $\mathcal{P}(\mathbf{x}) = \mathsf{Hash}(\mathsf{msg} \| \mathsf{salt})$, where $\mathsf{Hash} : \{0,1\}^* \to \mathbb{F}_q^m$ is a cryptographic hash function. The security of the scheme

relies on the indistinguishability of OV maps from random quadratic polynomials [4].

The MAYO signature scheme [3] revisits the UOV construction from a different perspective. Instead of choosing the oil-space dimension to be comparable to the number of public polynomials, MAYO uses a smaller oil space and compensates for this by "whipping" the underlying OV map into a larger quadratic map. More precisely, let $\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be the public OV map, with oil space $\mathcal{O} \subseteq \mathbb{F}_q^n$ of dimension $o < m$. Given a parameter k and a collection of public matrices $\mathbf{E}_{ij} \in \mathbb{F}_q^{m \times m}$, the corresponding whipped map $\mathcal{P}^* : \mathbb{F}_q^{n \times k} \longrightarrow \mathbb{F}_q^m$ is defined as

$$\mathcal{P}^*(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \sum_{i=1}^{k} \mathbf{E}_{ii} \mathcal{P}(\mathbf{x}_i) + \sum_{1 \le i < j \le k} \mathbf{E}_{ij} \mathcal{P}'(\mathbf{x}_i, \mathbf{x}_j).$$

The matrices $\mathbf{E}_{ij}$ are fixed public matrices, chosen so that any non-trivial linear combination of them has full rank. Since $\mathcal{P}$ vanishes on $\mathcal{O}$, both $\mathcal{P}(\mathbf{o})$ and $\mathcal{P}'(\mathbf{o}, \mathbf{o}')$ vanish for all $\mathbf{o}, \mathbf{o}' \in \mathcal{O}$. Consequently, $\mathcal{P}^*$ vanishes on $\mathcal{O}^k = \{(\mathbf{o}_1, \ldots, \mathbf{o}_k) \in \mathbb{F}_q^{kn} : \mathbf{o}_i \in \mathcal{O} \text{ for all } i\}$, which has dimension ko.

To sign a message msg, the signer first computes $\mathbf{y} = \mathsf{Hash}(\mathsf{msg} \| \mathsf{salt}) \in \mathbb{F}_q^m$. Then, the signer chooses $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_k)$ at random and searches for $\mathbf{o} = (\mathbf{o}_1, \ldots, \mathbf{o}_k) \in \mathcal{O}^k$ such that $\mathcal{P}^*(\mathbf{v} + \mathbf{o}) = \mathbf{y}$. Since $\mathcal{P}^*$ vanishes on $\mathcal{O}^k$ and its polar form is bilinear, the resulting equation is linear in the ko unknown oil variables. The signer therefore solves a system of m linear equations in ko variables and outputs $\mathbf{x} = \mathbf{v} + \mathbf{o}$, together with the salt, as the signature.

2.4 The Original Wedge Attack

In [12], Ran proposes a new attack on the UOV scheme focused on fields of characteristic 2. The novelty of this attack consists in rewriting the polar form of the public key polynomials $p_1, \ldots, p_m$ using the exterior product.

In the following definition we index the coordinates of a vector in $\mathbb{F}_q^{\binom{n}{k}}$ by sets $J \in \binom{[n]}{k}$.

Definition 1 (Wedge product). *Given $k \le n$ and $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{F}_q^n$, the wedge product $\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_k$ is defined as the $\binom{n}{k}$-length vector over $\mathbb{F}_q$, whose J-th entry, for $J \in \binom{[n]}{k}$, is $\det(\mathbf{V}_J)$, where $\mathbf{V} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_k \end{bmatrix}^\top \in \mathbb{F}_q^{k \times n}$ and $\mathbf{V}_J$ denotes the column submatrix of $\mathbf{V}$ formed by the columns with indexes in J.*

Definition 2. *Let $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{F}_q^n$ be the canonical vectors. We denote by $\bigwedge^k \mathbb{F}_q^n$ the $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{\binom{n}{k}}$ spanned by elements of the form*

$$\mathbf{e}_J := \mathbf{e}_{j_1} \wedge \cdots \wedge \mathbf{e}_{j_k},$$

where $J = \{j_1, \ldots, j_k\} \in \binom{[n]}{k}$.

By the definition above, given $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{F}_q^n$, we have that $\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_k \bigwedge^k \mathbb{F}_q^n$ and

$$\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_k = \sum_{J \in \binom{[n]}{k}} \det(\mathbf{V}_J)\, \mathbf{e}_J. \tag{1}$$

Remark 1. Any alternating matrix $\mathbf{A} = [a_{i,j}] \in \mathbb{F}_q^{n \times n}$ can be uniquely represented by the element $\sum_{i<j} a_{i,j}(\mathbf{e}_i \wedge \mathbf{e}_j) \in \bigwedge^2 \mathbb{F}_q^n$. We indicate this representation by writing

$$\mathbf{A} = \sum_{i<j} a_{i,j}(\mathbf{e}_i \wedge \mathbf{e}_j).$$

Proposition 1 (Lemma 2 in [12]). *Let $\mathbf{Q} \in \mathbb{F}_q^{n \times n}$ be an alternating matrix such that $\mathbf{o}_1^\top \mathbf{Q}\, \mathbf{o}_2 = 0$ for all $\mathbf{o}_1, \mathbf{o}_2$ in a subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension o, and let $\mathbf{v}_1, \ldots, \mathbf{v}_{n-o}$ be a basis for $\mathcal{O}^\perp$. Then there exist $\mathbf{x}_i \in \mathbb{F}_q^n$ such that*

$$\mathbf{Q} = \sum_{i=1}^{n-o} \mathbf{v}_i \wedge \mathbf{x}_i.$$

Let $(p_1, \ldots, p_m)$ be an $\mathsf{OV}(q, n, o, m)$ sequence with associated secret space $\mathcal{O}$. For fields $\mathbb{F}_q$ of characteristic 2, the matrix $\mathbf{Q}_k$ representing the polar form of p_k is alternating. Furthermore, by Proposition 1, we have

$$\mathbf{Q}_k = \sum_{i=1}^{n-o} \mathbf{v}_i \wedge \mathbf{x}_{i,k},$$

where $\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-o}\}$ is a basis of $\mathcal{O}^\perp$, since by definition the wedge product of linearly dependent vectors is the zero vector, we have that

$$(\mathbf{v}_1, \wedge \cdots \wedge \mathbf{v}_{n-o}) \wedge \mathbf{Q}_k = \mathbf{0} \in \bigwedge^{n-o+2} \mathbb{F}_q^n, \quad \forall k = 1, \ldots, m. \tag{2}$$

Let $\mathbf{Q}_k = [b_{i,j}^{(k)}] \in \mathbb{F}_q^{n \times n}$. By Remark 1, we can write

$$\mathbf{Q}_k = \sum_{I \in \binom{[n]}{2}} b_I^{(k)} \mathbf{e}_I,$$

where for $I = \{i, j\}$ we set $b_I^{(k)} = b_{i,j}^{(k)}$, $\mathbf{e}_I = \mathbf{e}_i \wedge \mathbf{e}_j$. By (1) we have

$$\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_{n-o} = \sum_{J \in \binom{[n]}{n-o}} \det(\mathbf{V}_J)\, \mathbf{e}_J.$$

Therefore

$$(\mathbf{v}_1, \wedge \cdots \wedge \mathbf{v}_{n-o}) \wedge \mathbf{Q}_k = \left(\sum_{I \in \binom{[n]}{2}} b_I^{(k)} \mathbf{e}_I \right) \cdot \left(\sum_{J \in \binom{[n]}{n-o}} \det(\mathbf{V}_J)\, \mathbf{e}_J \right)$$
$$= \sum_{K \in \binom{[n]}{n-o+2}} \left(\sum_{I \subset K,\ |I|=2} \det(\mathbf{V}_{K \setminus I}) \cdot b_I^{(k)} \right) \mathbf{e}_K,$$

and by (2), for each $K \in \binom{[n]}{n-o+2}$ and $k \in [m]$, we have

$$\sum_{I \subset K,\ |I|=2} \det(\mathbf{V}_{K \setminus I}) \cdot b_I^{(k)} = 0. \tag{3}$$

Eq. (3) gives a linear equation in the unknown values $\det(\mathbf{V}_J)$ (where $J \in \binom{[n]}{n-o}$), with coefficients given by the entries of $\mathbf{Q}_k$. Consequently, we can derive a linear system with $m\binom{n}{n-o+2}$ equations and $\binom{n}{n-o}$ variables for which $\det(\mathbf{V}_J)$ with $J \in \binom{[n]}{n-o}$ yields a solution. In [12], Ran describes sufficient conditions for the above linear system to have a one-dimensional solution space, and shows how to recover the secret space $\mathcal{O}$ from a solution under such conditions.

2.5 Generalization of Jin et al.

Jin et al. proposed an XL algorithm over the p-reduced symmetric algebra, which generalize the wedge attack for any finite field [10].

Let p be the characteristic of the field $\mathbb{F}_q$, the p-reduced symmetric algebra is defined as

$$\overline{\mathrm{Sym}(\mathbb{F}_q^n)} := \bigoplus_{k=0}^{\infty} (\mathbb{F}_q^n)^{\otimes k} \Big/ \left\langle \mathbf{x}^{\otimes p},\ \mathbf{x} \otimes \mathbf{y} - \mathbf{y} \otimes \mathbf{x} \;\middle|\; \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n \right\rangle,$$

where $\otimes$ and $\oplus$ denote the tensor product and direct sum, respectively, while $(\mathbb{F}_q^n)^{\otimes k} = \mathbb{F}_q^n \otimes \cdots \otimes \mathbb{F}_q^n$ (k times) and $(\mathbb{F}_q^n)^{\otimes 0} = \mathbb{F}_q$. The multiplication in $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}$ is commutative and is denoted by $\odot$.

For $d \in \mathbb{Z}_{\geq 0}$, the d-homogeneous component of $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}$ denoted by $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}_d$, is the $\mathbb{F}_q$-vector space spanned by the set

$$\{\mathbf{e}_1^{\odot \alpha_1} \odot \mathbf{e}_2^{\odot \alpha_2} \odot \cdots \odot \mathbf{e}_n^{\odot \alpha_n} \mid \alpha_1 + \cdots + \alpha_n = d \text{ and } 0 \leq \alpha_i < p\},$$

where $\mathbf{e}_i^{\odot \alpha_i} = \mathbf{e}_i \odot \cdots \odot \mathbf{e}_i (\alpha_i \text{ times})$.

Lemma 1. *The sets $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}$ and $\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^p, \ldots, x_n^p \rangle$ are isomorphic as $\mathbb{F}_q$-algebras.*

Proof. Fix a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of $\mathbb{F}_q^n$. Consider the isomorphism $\phi : \overline{\mathrm{Sym}(\mathbb{F}_q^n)} \to \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^p, \ldots, x_n^p \rangle$ induced by mapping $\mathbf{e}_i \mapsto x_i$ for $i = 1, \ldots, n$. □

In the XL algorithm, the polynomials in a public OV map $(p_1(\mathbf{x}), \ldots, p_m(\mathbf{x}))$ are seen as 2-forms using ϕ^{-1}. Given the homogeneous quadratic form $p_k(\mathbf{x}) = \sum_{i \leq j} a_{i,j}^{(k)} x_i x_j$, this is rewritten as the 2-form $\sum_{i \leq j} a_{i,j}^{(k)} \mathbf{e}_i \odot \mathbf{e}_j$. The rows of the Macaulay matrix $\mathbf{M}_D$ are given by D-forms

$$\left\{ \boldsymbol{\alpha}_j \odot p_i \ : \ \boldsymbol{\alpha}_j \text{ is a basis element of } \overline{\mathrm{Sym}(\mathbb{F}_q^n)}_{D-2},\ i \in \{1, \ldots, m\} \right\},$$

and the columns are indexed by a basis of $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}_D$.

The authors show that $\mathbf{M}_D$, for $2 \leq D \leq o(p-1)$, is the matrix that represents the linear map

$$\begin{aligned} \mathcal{M}_D \colon \overline{\mathrm{Sym}(\mathbb{F}_q^n)}_{n(p-1)-D} &\longrightarrow \left(\overline{\mathrm{Sym}(\mathbb{F}_q^n)}_{n(p-1)-(D-2)} \right)^m \\ \mu &\longmapsto (\mu \odot p_1, \ldots, \mu \odot p_m). \end{aligned} \tag{4}$$

Additionally, they show that some elements in the kernel of the map $\mathcal{M}_D$ carry information about the oil space associated to the OV map $(p_1(\mathbf{x}), \ldots, p_m(\mathbf{x}))$. In particular, for $D = o(p-1)$, the authors claim that the vinegar element $\mathcal{V} = \mathbf{v}_1^{p-1} \odot \cdots \odot \mathbf{v}_v^{p-1}$ lies in the kernel of $\mathcal{M}_D$.

3 Polynomial description of the Wedge attacks

Here we present a description of the edge attack and its generalization using only the algebraic properties of the polynomial ring R.

3.1 Dual Decomposition of Oil-Vinegar Polynomials

All over this section $\mathcal{O} \subset \mathbb{F}_q^n$ is an o-dimensional vector space given by

$$\mathcal{O} = \mathsf{ColumnSpace}\left(\begin{bmatrix} \mathbf{O} \\ \mathbf{I}_o \end{bmatrix} \right),$$

where $\mathbf{I}_d$ denotes the identity matrix of size d, $\mathbf{O} \in \mathbb{F}_q^{v \times o}$ is a matrix, and $v = n - o$.

The following theorem shows that any homogeneous quadratic polynomial in

$$I(\mathcal{O}) = \{ f(\mathbf{x}) \in R : f(\mathbf{o}) = 0 \ \forall \mathbf{o} \in \mathcal{O} \}$$

lies in the ideal generated by the homogeneous linear polynomials $\ell_1(\mathbf{x}), \ldots, \ell_v(\mathbf{x})$ that are determined by $\mathcal{O}$.

Theorem 1. *Let $\mathcal{O}$ be the column space of the matrix of the form $\begin{bmatrix} \mathbf{O}^\top & \mathbf{I}_o \end{bmatrix}^\top$ with $\mathbf{O} \in \mathbb{F}_q^{v \times o}$. Then, for every homogeneous quadratic polynomial $p \in I(\mathcal{O})$ there exist homogeneous linear forms $g_1, \ldots, g_v \in R$ such that*

$$p(\mathbf{x}) = g_1(\mathbf{x})\ell_1(\mathbf{x}) + \cdots + g_v(\mathbf{x})\ell_v(\mathbf{x}), \tag{5}$$

where, for each $i = 1, \ldots, v$, $\ell_i(\mathbf{x}) = \langle \mathbf{x}, \mathbf{v}_i \rangle \in \mathbb{F}_q[\mathbf{x}]$, and $\mathbf{v}_1, \ldots, \mathbf{v}_v \in \mathbb{F}_q^n$ are the columns of $\mathbf{V} = \begin{bmatrix} \mathbf{I}_v & -\mathbf{O} \end{bmatrix}^\top$.

Proof. Clearly, the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_v \in \mathcal{O}^\perp$ and we have that $\langle \ell_1, \ldots, \ell_v \rangle \subseteq I(\mathcal{O})$. Set $\mathbf{x} = (x_1, \ldots, x_n)$ and let $p \in I(\mathcal{O})$ be a homogeneous quadratic polynomial. By the division algorithm between p and $(\ell_1, \ldots, \ell_v)$, there exist a remainder $r \in \mathbb{F}_q[x_1, \ldots, x_n]$ and some quotients $g_1, \ldots, g_v \in \mathbb{F}_q[x_1, \ldots, x_n]$ such that $p(\mathbf{x}) = g_1(\mathbf{x}) \cdot \ell_1(\mathbf{x}) + \cdots + g_v(\mathbf{x}) \cdot \ell_v(\mathbf{x}) + r(\mathbf{x})$, with either $r = 0$ or r is an $\mathbb{F}_q$-linear combination of monomials none of which is divisible by any leading term $\mathrm{LT}(\ell_i) = x_i$ $(1 \leq i \leq v)$. Notice

$$r(\mathbf{x}) = p(\mathbf{x}) - [g_1(\mathbf{x}) \cdot \ell_1(\mathbf{x}) + \cdots + g_v(\mathbf{x}) \cdot \ell_v(\mathbf{x})].$$

Two features of the division algorithm will be used. First, since p and $\ell_1, \ldots, \ell_v$ are homogeneous of degrees 2 and 1 respectively, every intermediate dividend h is homogeneous of degree 2, and every term added to a quotient g_i is of the form $\mathrm{LT}(h)/x_i$; such a term has degree exactly $\deg \mathrm{LT}(h) - 1 = 1$. Hence each g_i is a homogeneous linear form. Second, a monomial divisible by none of the variables $x_1, \ldots, x_v$ is a monomial in the variables $x_{v+1}, \ldots, x_n$ alone. Therefore

$$r \in \mathbb{F}_q[x_{v+1}, \ldots, x_n], \quad \text{with } r = 0 \text{ or } \ r \text{ is homogeneous of degree 2.}$$

Since $r(\mathbf{x}) = p(\mathbf{x}) - [g_1(\mathbf{x}) \cdot \ell_1(\mathbf{x}) + \cdots + g_v(\mathbf{x}) \cdot \ell_v(\mathbf{x})]$, we get that r vanishes on every point of $\mathcal{O}$. By the description of $\mathcal{O}$, the map

$$\mathbf{t} \mapsto \begin{bmatrix} \mathbf{Ot} \\ \mathbf{t} \end{bmatrix}$$

is a bijection $\mathbb{F}_q^o \to \mathcal{O}$ whose composition with the projection onto the last o coordinates $(x_{v+1}, \ldots, x_n)$ is the identity map on $\mathbb{F}_q^o$. As r involves only the variables $x_{v+1}, \ldots, x_n$, we have that $r(\mathbf{o}) = 0$ for all $\mathbf{o} \in \mathcal{O}$ is equivalent to

$$r(\mathbf{t}) = 0 \qquad \text{for all } \mathbf{t} \in \mathbb{F}_q^o.$$

Renaming the variables $y_j := x_{v+j}$, we have $r \in \mathbb{F}_q[y_1, \ldots, y_o]$ with $r = 0$ or r is homogeneous of degree 2, and $r(\mathbf{y}) = 0$ for all $\mathbf{y} \in \mathbb{F}_q^o$. Write

$$r(\mathbf{y}) = \sum_{1 \leq j \leq k \leq o} c_{jk}\, y_j y_k, \qquad c_{jk} \in \mathbb{F}_q.$$

Evaluating at $\mathbf{y} = \mathbf{e}_j$ gives $c_{jj} = 0$ for every j; evaluating then at $\mathbf{y} = \mathbf{e}_j + \mathbf{e}_k$ with $j < k$ gives $c_{jj} + c_{kk} + c_{jk} = c_{jk} = 0$. Therefore r is the zero polynomial and

$$p(\mathbf{x}) = g_1(\mathbf{x}) \cdot \ell_1(\mathbf{x}) + \cdots + g_v(\mathbf{x}) \cdot \ell_v(\mathbf{x}),$$

where the g_i's are homogeneous linear forms. □

Remark 2. Theorem 1 generalizes Lemma 2 in [12], i.e., Lemma 2 is obtained from Theorem 1 in the particular case of $q = 2^e$ for some positive interger e.

Indeed, let $\mathcal{O}$ be as in Theorem 1. Let $\mathcal{P}$ be an OV sequence of polynomials vanishing in $\mathcal{O}$. Given $p \in \mathcal{P}$, let $\mathbf{Q} \in \mathbb{F}_q^{n\times n}$ be the symmetry matrix represeting its polar form. Hence, it holds

$$p'(\mathbf{a},\mathbf{b}) = \mathbf{a}^\top \mathbf{Q}\mathbf{b} = p(\mathbf{a}+\mathbf{b}) - p(\mathbf{a}) - p(\mathbf{b}) \quad \forall\ \mathbf{a},\mathbf{b} \in \mathbb{F}_q^n.$$

In the case of even characteristic, i.e., $q = 2^e$, Theorem 1 implies

$$\begin{aligned}
\mathbf{a}^\top \mathbf{Q}\mathbf{b} &= p'(\mathbf{a},\mathbf{b}) \\
&= \sum_{i=1}^{v} \Big(g_i(\mathbf{a}+\mathbf{b}) \cdot \ell_i(\mathbf{a}+\mathbf{b}) \Big) - \sum_{i=1}^{v} g_i(\mathbf{a})\ell_i(\mathbf{a}) - \sum_{i=1}^{v} g_i(\mathbf{b})\ell_i(\mathbf{b}), \\
&= \sum_{i=1}^{v} \Big(g_i(\mathbf{a})\ell_i(\mathbf{b}) + g_i(\mathbf{b})\ell_i(\mathbf{a}) \Big) \\
&= \mathbf{a}^\top \left(\sum_{i=1}^{v} \mathbf{w}_i \mathbf{v}_i^\top + \mathbf{v}_i \mathbf{w}_i^\top \right) \mathbf{b},
\end{aligned}$$

where $g_i(\mathbf{x}) = \langle \mathbf{w}_i, \mathbf{x}\rangle = \mathbf{x}^\top \mathbf{w}_i = \mathbf{w}_i^\top \mathbf{x}$ and $\ell_i(\mathbf{x}) = \langle \mathbf{v}_i, \mathbf{x}\rangle = \mathbf{v}_i^\top \mathbf{x} = \mathbf{x}^\top \mathbf{v}_i$. By symmetry, we obtain $\mathbf{Q} = \sum_{i=1}^{v} \mathbf{w}_i \wedge \mathbf{v}_i$ with $\mathbf{w}_i \wedge \mathbf{v}_i = \mathbf{w}_i \mathbf{v}_i^\top + \mathbf{v}_i \mathbf{w}_i^\top$.

Remark 3. As a result of independent interest, we can show that the linear polynomials $\ell_1, \ldots, \ell_v$ together with the field equations $x_1^q - x_1, \ldots, x_n^q - x_n$ form a Gröbner basis of the ideal $I(\mathcal{O})$; see Proposition 5 in Section A.

3.2 From Dual Decomposition to Oil-Space Recovery

This section shows that the coefficients of the ℓ_i polynomials, i.e., the entries of the matrix $\mathbf{V}$ (given in Theorem 1) yield a solution of a linear system derived from a given Oil-Vinegar map.

To simplify the description, we introduce the following notation. We set $\mathcal{X}_p$ to denote the ideal generated by monomials of the form x_i^p, that is,

$$\mathcal{X}_p := \langle x_1^p, \ldots, x_n^p \rangle, \tag{6}$$

and we let $\mathcal{M}_n(d; p^r)$ denote the set of tuples of nonnegative integers smaller than p^r whose entries sum up to d, i.e.,

$$\mathcal{M}_n(d; f) := \{ \boldsymbol{\alpha} \in \mathbb{Z}_{\geq 0}^n : |\boldsymbol{\alpha}| = d,\ \alpha_i < f \}. \tag{7}$$

Let $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$ be an OV-map with secret space $\mathcal{O} \subset \mathbb{F}_q^n$. Since each p_k is a quadratic homogeneous polynomials in $I(\mathcal{O})$, then, by Theorem 1, it holds

$$\left(\prod_{i=1}^{v} \left((\ell_i(\mathbf{x}) \right)^{p-1} \right) \cdot p_k(\mathbf{x}) \mod \mathcal{X}_p = 0 \quad \forall k = 1, \ldots, m, \tag{8}$$

where the $\ell_i(\mathbf{x}) = x_i - o_{i,1}x_{v+1} - \cdots - o_{i,o}x_n$ are as in Theorem 1. For a fixed k, each coefficient in the lefthand side of (8) can be expressed as a polynomial $f(o_{1,1}, \ldots, o_{o,v})$ of degree at most $v(p-1)$ in the ov unknown values $o_{i,j}$. Hence (8) yields a multivariate system of polynomials in ov variables.

The above multivariate system is solved by direct linearization. More precisely, each monomial appearing in the system, including the constant monomial 1, is treated as an independent variable. In this way, the original multivariate system is transformed into a homogeneous linear system. When the solution space of this linear system is one-dimensional, its solutions correspond precisely to the coefficients of the polynomials ℓ_i, that is, the entries of the matrix $\mathbf{V}$. In Section 4.3, we show how to extract the secret space $\mathcal{O}$ from this unique solution.

In what follows, we first describe the main characteristics of the resulting linear system. Then, in Sections 3.3 and 3.4, we show that this system coincides with the original wedge attack system when $p = 2$ and with the generalized version introduced in [10] when $p > 2$.

To simplify the exposition, we divide the analysis into two separate cases: $p = 2$ and $p > 2$.

Case $p = 2$. Set $L(\mathbf{x}) = \prod_{i=1}^{v} \ell_i(\mathbf{x}) \mod \mathcal{X}_2$ and consider all its unknowns coefficients as variables. In particular, we can write

$$L(\mathbf{x}) = \sum_{\boldsymbol{\alpha} \in \mathcal{M}_n(v;2)} a_{\boldsymbol{\alpha}} \cdot \mathbf{x}^{\boldsymbol{\alpha}},$$

where $\mathbf{x}^{\boldsymbol{\alpha}} := \prod_{\alpha_i \in \boldsymbol{\alpha}} x^{\alpha_i}$ and the $a_{\boldsymbol{\alpha}} \in \mathbb{F}_q$ are unknown. By (8), for each $1 \leq k \leq m$, each coefficient in

$$L(\mathbf{x}) \cdot p_k(\mathbf{x}) \mod \mathcal{X}_2$$

yields a homogeneous linear equation in the set of unknowns $\{a_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{M}_n(v;2)\}$. In total, we have $m \cdot \binom{n}{v+2}$ linear equations in $\binom{n}{v}$ unknowns (the number of coefficients $a_{\boldsymbol{\alpha}}$), where each equation contains at most $\binom{v+2}{2}$ nonzero coefficients. In Section 3.3, we show that these equations are the same equations obtained in the original wedge attack [12].

Case $p > 2$. In general, we set $L(\mathbf{x}) = \prod_{i=1}^{v} \ell_i^{p-1}(\mathbf{x}) \mod \mathcal{X}_p$ and consider all its unknowns coefficients as variables. In particular, we can write

$$L(\mathbf{x}) = \sum_{\boldsymbol{\alpha} \in \mathcal{M}_n(v(p-1);p)} a_{\boldsymbol{\alpha}} \cdot \mathbf{x}^{\boldsymbol{\alpha}},$$

where each $a_{\boldsymbol{\alpha}} \in \mathbb{F}_q$ is unknown and $\mathcal{M}_n(v(p-1);p)$ is defined in (7). By (8), for each $1 \leq k \leq m$, each coefficient $b_{\boldsymbol{\beta}}$ of $L(\mathbf{x}) \cdot p_k(\mathbf{x}) \mod \mathcal{X}_p$, which is written as

$$L(\mathbf{x}) \cdot p_k(\mathbf{x}) \mod \mathcal{X}_p := \sum_{\boldsymbol{\beta} \in \mathcal{M}_n(v(p-1)+2;p)} b_{\boldsymbol{\beta}} \cdot \mathbf{x}^{\boldsymbol{\beta}},$$

yields a homogeneous linear equation in the set of unknowns

$$A := \{a_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{M}_n(v(p-1);p)\}.$$

We set $H_n(d;f) := |\mathcal{M}_n(d,f)|$. By inclusion–exclusion,

$$H_n(d;f) \;=\; \sum_{j\geq 0}(-1)^j \binom{n}{j}\binom{d-j\cdot f+n-1}{n-1}. \tag{9}$$

In total, we have $m\cdot H_n(v(p-1)+2;p)$ linear equations (m times the number of coefficients $b_{\boldsymbol{\beta}}$) and $H_n(v(p-1);p)$ unknowns (the number of coefficients $a_{\boldsymbol{\alpha}}$). The number of potentially nonzero coefficients appearing in the equation coming from a monomial $\mathbf{x}^{\boldsymbol{\beta}}$ with $\boldsymbol{\beta} \in \mathcal{M}_n(v(p-1),p)$ is the number of quadratic monomials in R that divide $\mathbf{x}^{\boldsymbol{\beta}}$. This number is smaller than $\binom{n+1}{2}$, which is the total number of quadratic monomials in n variables. In Section 3.4 we show that these equations are the same equations obtained in the generalized wedge attack by Jin et al. [10].

3.3 Obtaining the original Wedge attack for p=2

Here we show that for $p = 2$, the linear system described in Section 3.2 is the same obtained by Ran in [12]. Indeed, each $\ell_i(\mathbf{x})$ in Theorem 1 is a homogeneous linear polynomial that can be written as

$$\ell_i(\mathbf{x}) = \sum_{j=1}^{n} v_{i,j}x_j \quad \forall i = 1,\ldots,v,$$

where $\mathbf{v}_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,n})$ is the i-th column of the matrix $\mathbf{V}$. Hence,

$$\begin{aligned} L(\mathbf{x}) &= \ell_1(\mathbf{x})\cdot\ell_2(\mathbf{x})\cdot\cdots\cdot\ell_v(\mathbf{x}) \mod \mathcal{X}_2 \\ &= \sum_{I\in\binom{[n]}{v}} \left(\sum_{\sigma\in S_I}\prod_{i=1}^{v} v_{i,\sigma(i)}\right)\mathbf{x}_I, \end{aligned}$$

where S_I is the symmetric group in the set I and $\mathbf{x}_I := \prod_{i\in I} x_i$. By the Leibniz's formula for determinants, we have

$$L(\mathbf{x}) = \sum_{I\in\binom{[n]}{v}} \det(\mathbf{V}_I)\,\mathbf{x}_I, \tag{10}$$

where $\det(\mathbf{V}_I)$ denotes the maximal minor of the matrix $\mathbf{V}$ (given in Theorem 1) obtained by selecting the columns indexed by I. Therefore, for any quadratic polynomial $p(\mathbf{x}) = \sum_{1\leq i\leq j\leq n} b_{\{i,j\}}\cdot x_i x_j$, it holds

$$\begin{aligned} L(\mathbf{x})\cdot p(\mathbf{x}) \mod \mathcal{X}_2 &= \left(\sum_{I\in\binom{[n]}{v}} \det(\mathbf{V}_I)\cdot\mathbf{x}_I\right)\cdot\left(\sum_{I'\in\binom{[n]}{2}} b_{I'}\cdot\mathbf{x}_{I'}\right) \mod \mathcal{X}_2 \\ &= \sum_{J\in\binom{[n]}{v+2}} \left(\sum_{I\subset K,\,|I|=2} \det(\mathbf{V}_{K\setminus I})\cdot b_I\right)\mathbf{x}_J. \end{aligned}$$

The coefficients of $\mathbf{x}_J$ are the same equations as in Eq. (3). Therefore, for $p = 2$, the linear system derived by Eq. (8) is the same as in the original wedge attack [12, Section 3.2].

3.4 Obtaining Jin et al.'s attack for $p > 2$

Let ϕ be the isomorphism defined in Lemma 1. Applying its inverse to the polynomials in Eq. (8), we obtain

$$\begin{aligned}\phi^{-1}\left(\left(\prod_{i=1}^{v}(\ell_i(\mathbf{x}))^{p-1}\right)\cdot p_k(\mathbf{x})\right) &= \phi^{-1}\left(\prod_{i=1}^{v}\ell_i(\mathbf{x})^{p-1}\right)\odot\phi^{-1}\left(p_k(\mathbf{x})\right),\\ &= \left(\bigodot_{i=1}^{v}\phi^{-1}\left(\ell_i(\mathbf{x})\right)^{p-1}\right)\odot p_k,\\ &= \left(\bigodot_{i=1}^{v}\mathbf{v}_i^{p-1}\right)\odot p_k, \quad \forall k=1,\ldots,m.\end{aligned}$$

Consequently, for $p > 2$, the equations obtained for Eq. (8) are the same as the linear equations given by the kernel of the linear map $\mathcal{M}_{o(p-1)}$ defined in Eq. (4).

4 Extended Wedge Attack

In Section 3.2 we used Theorem 1 and the ideal $\mathcal{X}_p$ to derive a homogeneous linear system whose solution encodes the secret space $\mathcal{O}$. This section generalizes that idea by using p^r instead of p for some $1 \leq r \leq \log_p(q) = e$. To this end, we work with the ideal

$$\mathcal{X}_{p^r} := \langle x_1^{p^r}, \ldots, x_n^{p^r}\rangle, \tag{11}$$

and use the generalized relation

$$\left(\prod_{i=1}^{v}\left(\ell_i(\mathbf{x})\right)^{p^r-1}\right)\cdot p(\mathbf{x}) \mod \mathcal{X}_{p^r} = 0$$

which follows (by Theorem 1) for any homogeneous quadratic polynomial p in $I(\mathcal{O})$.

4.1 Construction of the Linear System

Throughout this subsection we fix an integer $1 \leq r \leq \log_p(q) = e$.

By Theorem 1, for each homogeneous quadratic polynomial $p \in I(\mathcal{O})$ we have

$$L(\mathbf{x})\cdot p(\mathbf{x}) \mod \mathcal{X}_{p^r} = 0, \tag{12}$$

where

$$L(\mathbf{x}) = \prod_{i=1}^{v} \left(\ell_i(\mathbf{x})\right)^{p^r-1} \mod \mathcal{X}_{p^r}, \tag{13}$$

the $\ell_i(\mathbf{x})$ are as in Theorem 1, and $\mathcal{X}_{p^r}$ is as in (11).

Since $L(\mathbf{x})$ is homogeneous of degree $v(p^r-1)$ and every exponent occurring in it is smaller than p^r, we can write

$$L(\mathbf{x}) = \sum_{\boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1);p^r)} a_{\boldsymbol{\alpha}} \cdot \mathbf{x}^{\boldsymbol{\alpha}},$$

where $\mathcal{M}_n(d;f)$ is defined in (7) and each $a_{\boldsymbol{\alpha}} \in \mathbb{F}_q$ is unknown. Similarly, for a homogeneous quadratic polynomial $p(\mathbf{x}) = \sum_{\boldsymbol{\gamma} \in \mathcal{M}_n(2,p^r)} b_{\boldsymbol{\gamma}} \mathbf{x}^{\boldsymbol{\gamma}}$, we have

$$L(\mathbf{x}) \cdot p(\mathbf{x}) \mod \mathcal{X}_{p^r} := \sum_{\boldsymbol{\beta} \in \mathcal{M}_n(v(p^r-1)+2;p^r)} c_{\boldsymbol{\beta}} \cdot \mathbf{x}^{\boldsymbol{\beta}},$$

where, restricted to $\boldsymbol{\gamma} \in \mathcal{M}_n(2,p^r)$ and $\boldsymbol{\alpha} \in \mathcal{M}_n(vp^r-1);p^r)$,

$$c_{\boldsymbol{\beta}} = \sum_{\boldsymbol{\gamma}+\boldsymbol{\alpha}=\boldsymbol{\beta}} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\gamma}}.$$

Hence each $c_{\boldsymbol{\beta}}$ is a homogeneous linear polynomial in the unknown $a_{\boldsymbol{\alpha}}$'s.

Let $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$ be an OV-map with secret space $\mathcal{O} \subset \mathbb{F}_q^n$ determined as in Theorem 1, i.e., $\mathcal{O}$ is the column space of the matrix $\begin{bmatrix}\mathbf{O}^\top & \mathbf{I}_o\end{bmatrix}^\top$ with $\mathbf{O} \in \mathbb{F}_q^{v \times o}$. By (12), each coefficient $c_{\boldsymbol{\beta}}^{(k)}$ in $L(\mathbf{x}) \cdot p_k(\mathbf{x}) \mod \mathcal{X}_{p^r}$ is a homogeneous linear equation in the set of unknowns

$$A := \{a_{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1);p^r)\}.$$

Here we consider the homogeneous linear system, in the unknowns $a_{\boldsymbol{\alpha}}$, given by all the equations of the form $c_{\boldsymbol{\beta}}^{(k)} = 0$. By (12), the unknown coefficients of the linear polynomial $\ell_i(\mathbf{x})$, i.e., the entries of the matrix $\mathbf{V}$ (as in Theorem 1), yield a solution of the linear system given by all the $c_{\boldsymbol{\beta}}^{(k)}$. In Section 4.3 we show how the secret space $\mathcal{O}$ is extracted from the knowledge of the set A when the linear system has a one-dimensional solution space.

4.2 The Matrix $\mathcal{W}$ Representing the Linear System

Here we describe the matrix $\mathcal{W}$ that represents the homogeneous linear system explained above. We index its rows by pairs $(k, \boldsymbol{\beta})$ where $1 \le k \le m$, and $\boldsymbol{\beta} \in \mathcal{M}_n(v(p^r-1)+2;p^r)$, while its columns are indexed by $\boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1);p^r)$. The columns of $\mathcal{W}$ are sorted using the following ordering in $\mathcal{M}_n(v(p^r-1);p^r)$:

$$\boldsymbol{\alpha}_1 \le \boldsymbol{\alpha}_2 \;\Leftrightarrow\; \mathbf{x}^{\alpha_1} \preceq \mathbf{x}^{\alpha_2}, \tag{14}$$

where $\prec$ is the monomial ordering in the underlying polynomial ring. The set $\mathcal{M}_n(v(p^r-1)+2;p^r)$ is ordered analogously. The rows of $\mathcal{W}$ are ordered using a lexicographic ordering[3] in $[k] \times \mathcal{M}_n(v(p^r-1)+2;p^r)$. The $((k,\boldsymbol{\beta}),\boldsymbol{\alpha})$ entry of

[3] Lexicographic order in $[k] \times \mathcal{M}_n(v(p^r-1)+2;p^r)$ means that in the second component $\mathcal{M}_n(v(p^r-1)+2;p^r)$ the order is the one given in (14).

$\mathcal{W}$ is given by

$$\mathcal{W}_{(k,\boldsymbol{\beta}),\boldsymbol{\alpha}} = \begin{cases} b^{(k)}_{\boldsymbol{\beta}-\boldsymbol{\alpha}} & \text{if } \alpha_i \le \beta_i \ \forall i \in [n] \\ 0 & \text{otherwise} \end{cases}, \tag{15}$$

where $p_k(\mathbf{x}) = \sum_{\boldsymbol{\gamma}\in\mathcal{M}_n(2,p^r)} b^{(k)}_{\boldsymbol{\gamma}}\mathbf{x}^{\boldsymbol{\gamma}}$.

With this definition of $\mathcal{W}$, in Section 4.3 we show how to recover the secret space $\mathcal{O}$ from a solution $\mathbf{a}$ of the linear system $\mathcal{W}\cdot\mathbf{a} = \mathbf{0}$, given that the dimension of the right kernel of $\mathcal{W}$ is one. In Section 5.1, we show that $\mathcal{W}$ is permutation equivalent to the p^r-truncated Macaulay matrix of $\mathcal{P}$.

4.3 Recovering the Secret Space Elements in the Kernel of $\mathcal{W}$

If $\mathsf{dim}(\mathsf{ker}(\mathcal{W})) = 1$ we can extract the secret space using an approach similar to the one given in [7, Section 4.1]. Recall that a vector $\mathbf{a} \in \mathsf{ker}(\mathcal{W})$ carrying the elements of the solution set A is, by construction, the coordinate vector of the polynomial $L(\mathbf{x}) = \prod_{i=1}^{v} \ell_i^{p^r-1}$ in the basis $\{\mathbf{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1); p^r)\}$; that is, the entry of $\mathbf{a}$ in the column indexed by $\boldsymbol{\alpha}$ is the coefficient $a_{\boldsymbol{\alpha}}$ of $\mathbf{x}^{\boldsymbol{\alpha}}$ in L. The secret space is $\mathcal{O} = \mathsf{ColumnSpace}\big([\,\mathbf{O}^\top\ \mathbf{I}_o\,]^\top\big)$, so it is determined by the matrix $\mathbf{O} = [o_{i,j}] \in \mathbb{F}_q^{v\times o}$, and by construction the linear forms are $\ell_i(\mathbf{x}) = x_i - \sum_{j=1}^{o} o_{i,j}\, x_{v+j}$. The idea of the recovery is that the entries $o_{i,j}$ can be read off directly from some of the coordinates $a_{\boldsymbol{\alpha}}$, without any further linear algebra: we simply have to identify which monomial of L carries $o_{i,j}$ as its coefficient.

Writing $\ell_i(\mathbf{x}) = x_i - \sum_{j=1}^{o} o_{i,j}\, x_{v+j}$ and expanding the product $L(\mathbf{x}) = \prod_{i=1}^{v} \ell_i^{p^r-1}$, we can extract $o_{i,j}$ directly if we read off the coefficient of the monomial

$$x_{v+j}\cdot x_i^{p^r-2}\cdot \prod_{\substack{k=1\\k\neq i}}^{v} x_k^{p^r-1},$$

which corresponds to the n-tuple

$$\boldsymbol{\alpha}_{i,j} = \underbrace{(p^r-1,\ldots,\underbrace{p^r-2}_{i\text{ -position}},\ldots,p^r-1}_{v\text{ entries}},0,\ldots,\underbrace{1}_{v+j\text{ position}},\ldots,0).$$

Thus, given $\mathbf{u} \in \mathsf{ker}(\mathcal{W})$, we only need to read the entries $o_{i,j}$ directly in the appropriate positions of $\mathbf{u}$. These positions correspond to the locations of the indices $\boldsymbol{\alpha}_{i,j}$ in the columns of $\mathcal{W}$, according to the order chosen for $\mathcal{M}_n(v(p^r-1); p^r)$.

One point deserves attention. A basis vector $\mathbf{u}$ of $\mathsf{ker}(\mathcal{W})$ is only determined up to a nonzero scalar $\lambda \in \mathbb{F}_q^*$; a solver returns $\mathbf{u} = \lambda\,\mathbf{a}$ rather than $\mathbf{a}$ itself, so the entry at position $\boldsymbol{\alpha}_{i,j}$ is $\lambda\, a_{\boldsymbol{\alpha}_{i,j}} = \lambda\, o_{i,j}$, which recovers $\mathbf{O}$ only up to the

common factor λ. We remove this ambiguity by normalizing against a coordinate whose value we know. The monomial $\mathbf{x}^{\boldsymbol{\alpha}_{\text{ref}}} = x_1^{p^r-1} \cdots x_v^{p^r-1}$, corresponding to

$$\boldsymbol{\alpha}_{\text{ref}} = (\underbrace{p^r-1, \ldots, p^r-1}_{v}, \underbrace{0, \ldots, 0}_{o}),$$

is the product of the leading terms $\text{LT}(\ell_k) = x_k$ and hence has coefficient 1 in L; thus $u_{\boldsymbol{\alpha}_{\text{ref}}} = \lambda$. Dividing $\mathbf{u}$ by $u_{\boldsymbol{\alpha}_{\text{ref}}}$ rescales it to $\mathbf{a}$ exactly, after which $a_{\boldsymbol{\alpha}_{i,j}} = o_{i,j}$ for every i, j.

Once the entries $o_{i,j}$ are known we recover $\mathbf{O} = [o_{i,j}] \in \mathbb{F}_q^{v \times o}$ and hence the secret space as

$$\mathcal{O} = \mathsf{ColumnSpace}\left(\begin{bmatrix}\mathbf{O} \\ \mathbf{I}_o\end{bmatrix}\right),$$

which completes the attack.

4.4 Parameter Regimes for the Attack to Work

This section shows that whenever $v > 2m$ or $v > \frac{o-1}{2}m$, the polynomial $L(\mathbf{x})$ given in (13) is not expected to be the only polynomial of degree $v(p^r-1)$ satisfying equation (12) for each $p_k(\mathbf{x})$ in an OV map. In this case, we expect that at least two polynomials of degree $v(p^r-1)$ fulfill the aforementioned equation, so that the dimension of the kernel of $\mathcal{W}$ would not be greater than 1. Thus, our attack is only expected to work provided that

$$v < \min\left\{\frac{o-1}{2}, 2\right\} \cdot m. \tag{16}$$

We now explain the rationale behind the expression (16). The polynomial $P(\mathbf{x}) = \prod_{k=1}^{m} \left(p_k(\mathbf{x})\right)^{p^r-1}$ has degree $2m(p^r-1)$ for any homogeneous quadratic polynomials $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x}) \in R$. Additionally, for each $k \in [m]$,

$$P(\mathbf{x}) \cdot p_k(\mathbf{x}) \bmod \mathcal{X}_{p^r} = 0.$$

In the case $v \geq 2m$, for any polynomial $h(\mathbf{x})$ of degree $(v-2m)(p^r-1)$, the product $h(\mathbf{x}) \cdot P(\mathbf{x})$ is a polynomial of degree $v(p^r-1)$ different from $L(\mathbf{x})$ that satisfies equation (12) for each $p_k(\mathbf{x})$. Consequently, for our attack to work, we impose the condition

$$v < 2m. \tag{17}$$

Let $(p_1, \ldots, p_k)$ be an $\mathsf{OV}(q, n, o, m)$ sequence with oil space $\mathcal{O}$. Suppose that there exists another o-dimensional vector space $\mathcal{O}' \neq \mathcal{O}$ such that $p_k(\mathbf{o}') = 0$ for each $k \in [m]$ and $\mathbf{o}' \in \mathcal{O}'$. As for $\mathcal{O}$, there is a degree $v(p^r-1)$ polynomial $L'(\mathbf{x})$ (given by the product of the (p^r-1)-th power of the linear polynomials $\ell'_1(\mathbf{x}), \ldots, \ell'_{n-o}(\mathbf{x})$ defining $\mathcal{O}'$) such that $L'(\mathbf{x}) \cdot p_k(\mathbf{x}) \bmod \mathcal{X}_{p^r} = 0$, for each $k \in [m]$. Consequently, our attack is not expected to work when this additional oil space $\mathcal{O}'$ exits.

Now we evaluate the parameter conditions to be fulfilled so that the additional vector space $\mathcal{O}'$ does not exist. In particular, if $\mathcal{O}'$ exits, then

$$p'_k(\mathbf{o}'_i, \mathbf{o}'_j) = 0, \quad \forall 1 \leq i < j \leq o,$$

where $\mathbf{o}'_1, \ldots, \mathbf{o}'_o$ form a basis of $\mathcal{O}'$. That is, any basis of $\mathcal{O}'$ yields a solution of a quadratic system with $m \cdot \binom{o}{2}$ equations and vo variables (an echelonized basis of $\mathcal{O}'$ has vo unknown values). Therefore, we do not expect an additional oil space $\mathcal{O}'$ to exist as long as the aforementioned system is overdetermined, that is, when

$$v < m\frac{o-1}{2}. \tag{18}$$

4.5 Toy Example

We now illustrate every step of the extended wedge attack on a UOV instance with parameters

$$m = 4, \quad v = 3, \quad o = 2, \quad p = 2, \quad e = 2,$$

so that $n = 5$ and $q = p^e = 4$. For this case, the value of r that works is $r = 2$, giving $p^r = 4$, and obtaining a matrix $\mathcal{W}$ with $\mathsf{dim}(\mathsf{ker}(\mathcal{W})) = 1$. We write $\mathbb{F}_4 = \mathbb{F}_2(\theta)$ with $\theta^2 = \theta + 1$, and use the power representation of the nonzero elements, $1 = \theta^0,\ \theta,\ \theta^2$ (recall $\theta^3 = 1$). All computations take place in $R^{(p^r)} = R^{(4)} = \mathbb{F}_4[x_1, \ldots, x_5]/\langle x_1^4, \ldots, x_5^4 \rangle$.

Secret key. Let

$$\mathbf{O} = \begin{pmatrix} \theta & \theta^2 \\ 1 & \theta \\ \theta^2 & 1 \end{pmatrix} \in \mathbb{F}_4^{v \times o}, \qquad \mathbf{V} = \begin{bmatrix} \mathbf{I}_v & -\mathbf{O} \end{bmatrix}^\top = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \theta & 1 & \theta^2 \\ \theta^2 & \theta & 1 \end{pmatrix}.$$

The columns $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ of $\mathbf{V}$ form a basis of $\mathcal{O}^\perp$, and the corresponding linear forms $\ell_i(\mathbf{x}) = \langle \mathbf{x}, \mathbf{v}_i \rangle = x_i - \sum_{j=1}^{o} o_{i,j}\, x_{v+j}$ are

$$\begin{aligned} \ell_1 &= \langle \mathbf{x}, \mathbf{v}_1 \rangle = x_1 + \theta\, x_4 + \theta^2 x_5, \\ \ell_2 &= \langle \mathbf{x}, \mathbf{v}_2 \rangle = x_2 + x_4 + \theta\, x_5, \\ \ell_3 &= \langle \mathbf{x}, \mathbf{v}_3 \rangle = x_3 + \theta^2 x_4 + x_5. \end{aligned}$$

None of this is known to the attacker.

Public key. The attacker is given the public key polynomials $\mathcal{P} = (p_1, p_2, p_3, p_4)$, where each $p_k \in \langle \ell_1, \ell_2, \ell_3 \rangle$ is homogeneous of degree 2:

$$\begin{aligned}
p_1 &= \theta^2 x_1^2 + \theta\, x_1x_2 + x_1x_4 + x_1x_5 + \theta^2 x_2x_3 + x_2x_4 + x_2x_5 + \theta\, x_3^2 \\
&\quad + \theta^2 x_4^2 + \theta\, x_4x_5 + x_5^2, \\
p_2 &= \theta\, x_1^2 + \theta^2 x_1x_2 + x_1x_3 + \theta\, x_1x_4 + \theta^2 x_1x_5 + \theta^2 x_2^2 + x_2x_4 + \theta^2 x_2x_5 \\
&\quad + \theta\, x_3x_4 + x_4^2 + \theta^2 x_4x_5 + \theta\, x_5^2, \\
p_3 &= \theta^2 x_1^2 + \theta\, x_1x_2 + x_1x_3 + \theta^2 x_1x_4 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 \\
&\quad + \theta\, x_3x_5 + x_4x_5 + \theta\, x_5^2, \\
p_4 &= \theta\, x_1^2 + x_1x_2 + x_1x_3 + \theta^2 x_1x_4 + x_1x_5 + x_2^2 + \theta\, x_2x_4 + x_2x_5 \\
&\quad + \theta\, x_3^2 + \theta^2 x_3x_5 + \theta^2 x_4^2 + \theta\, x_5^2.
\end{aligned}$$

Step 1: set up the system. The attacker forms the degree-$v(p^r-1) = 9$ polynomial

$$L(\mathbf{x}) \;=\; \ell_1^3(\mathbf{x})\,\ell_2^3(\mathbf{x})\,\ell_3^3(\mathbf{x}) \;=\; \sum_{\boldsymbol{\alpha} \in \mathcal{M}_5(9;4)} a_{\boldsymbol{\alpha}}\, \mathbf{x}^{\boldsymbol{\alpha}},$$

with unknown coefficients $a_{\boldsymbol{\alpha}} \in \mathbb{F}_4$ and indexed by the bounded exponent set

$$\mathcal{M}_n(v(p^r-1); p^r) = \mathcal{M}_5(9;4) = \Big\{(\alpha_1, \ldots, \alpha_5) : 0 \le \alpha_i < 4,\ \textstyle\sum_i \alpha_i = 9\Big\},$$

which has $|\mathcal{M}_5(9;4)| = H_5(9;4) = 135$ monomials. Next, the attacker imposes

$$L \cdot p_k \;\equiv\; 0 \quad \text{in } R^{(4)}, \qquad k = 1, \ldots, 4. \tag{19}$$

Collecting the coefficient of every degree-11 monomial in each product yields a homogeneous linear system in the 135 unknowns $a_{\boldsymbol{\alpha}}$, whose matrix is $\mathcal{W}$ of size 260×135 (that is, $m\, H_5(4;4) = 4 \cdot 65 = 260$ rows and $H_5(6;4) = 135$ columns).

A couple of the equations. Each equation of the system is indexed by a pair $(k, \boldsymbol{\beta})$ with $1 \le k \le 4$ and $\boldsymbol{\beta} \in \mathcal{M}_5(11;4)$, i.e. a degree-11 exponent tuple with all entries at most 3. The equation is the vanishing of the coefficient of the monomial $\mathbf{x}^{\boldsymbol{\beta}}$ in $L \cdot p_k = \sum_{\boldsymbol{\alpha} \in \mathcal{M}_5(9;4)} a_{\boldsymbol{\alpha}}\, (\mathbf{x}^{\boldsymbol{\alpha}}\, p_k)$, taken modulo $\langle x_1^4, \ldots, x_5^4 \rangle$. Concretely, an unknown $a_{\boldsymbol{\alpha}}$ occurs in the equation $(k, \boldsymbol{\beta})$ precisely when $\mathbf{x}^{\boldsymbol{\beta}}/\mathbf{x}^{\boldsymbol{\alpha}} = \mathbf{x}^{\boldsymbol{\beta}-\boldsymbol{\alpha}}$ is a degree-2 monomial of p_k (and $\boldsymbol{\beta} - \boldsymbol{\alpha}$ has all entries in $\{0, \ldots, 3\}$), in which case its coefficient is the coefficient of $\mathbf{x}^{\boldsymbol{\beta}-\boldsymbol{\alpha}}$ in p_k. Thus building the row $(k, \boldsymbol{\beta})$ never requires forming any product: one simply scans the quadratic monomials $\mathbf{x}^{\boldsymbol{\gamma}}$ of p_k and, for each, places the entry in column $\boldsymbol{\alpha} = \boldsymbol{\beta} - \boldsymbol{\gamma}$.

For instance, take $k = 2$ and $\boldsymbol{\beta} = (3,3,3,0,2)$, that is $\mathbf{x}^{\boldsymbol{\beta}} = x_1^3 x_2^3 x_3^3 x_5^2$. Scanning the quadratic terms $\mathbf{x}^{\boldsymbol{\gamma}}$ of p_2 and keeping those for which $\boldsymbol{\alpha} = \boldsymbol{\beta} - \boldsymbol{\gamma}$ lies in $\mathcal{M}_5(9;4)$ yields the equation

$$\begin{aligned}
&\theta\, a_{(3,3,3,0,0)} + \theta^2 a_{(3,2,3,0,1)} + \theta^2 a_{(3,1,3,0,2)} + \theta^2 a_{(2,3,3,0,1)} \\
&\qquad + a_{(2,3,2,0,2)} + \theta^2 a_{(2,2,3,0,2)} + \theta\, a_{(1,3,3,0,2)} = 0,
\end{aligned}$$

where, for example, the term $\theta^2 a_{(3,2,3,0,1)}$ arises because $\boldsymbol{\beta} - (3,2,3,0,1) = (0,1,0,0,1)$ corresponds to the monomial x_2x_5, whose coefficient in p_2 is θ^2. Similarly, $k = 4$ and $\boldsymbol{\beta} = (0,3,3,3,2)$, that is $\mathbf{x}^{\boldsymbol{\beta}} = x_2^3x_3^3x_4^3x_5^2$, produces

$$\begin{aligned}\theta\, a_{(0,3,3,3,0)} + \theta^2 a_{(0,3,3,1,2)} + \theta^2 a_{(0,3,2,3,1)} + \theta\, a_{(0,3,1,3,2)} \\ + a_{(0,2,3,3,1)} + \theta\, a_{(0,2,3,2,2)} + a_{(0,1,3,3,2)} = 0.\end{aligned}$$

The full system consists of $m \cdot |\mathcal{M}_5(11;4)| = 4 \cdot 65 = 260$ such equations in the $|\mathcal{M}_5(9;4)| = 135$ unknowns $a_{\boldsymbol{\alpha}}$, i.e. the matrix $\mathcal{W}$ is 260×135.

Step 2: solve for L. One finds $\operatorname{rank}\mathcal{W} = 134$, hence $\mathsf{dimker}(\mathcal{W}) = 1$. The unique solution (up to an $\mathbb{F}_4$-scalar) is the coefficient vector of

$$L = \ell_1^3\,\ell_2^3\,\ell_3^3 \;\in R^{(4)},$$

a polynomial with 59 monomials; the attacker now knows L explicitly, though not yet its factorization.

Step 3: recover $\mathcal{O}$ directly from the kernel vector. Following Section 4.3, we do not need any further linear algebra: the entries $o_{i,j}$ of $\mathbf{O}$ can be read off directly from the kernel vector. Write $\ell_i = x_i - \sum_{j=1}^{o} o_{i,j}\, x_{v+j}$, so that $\mathbf{O} = [o_{i,j}] \in \mathbb{F}_4^{v\times o}$. Since $L = \prod_{i=1}^{v} \ell_i^{p^r-1}$ and $\mathrm{LT}(\ell_i) = x_i$, the coefficient $a_{\boldsymbol{\alpha}_{i,j}}$ of the monomial

$$x_{v+j}\; x_i^{p^r-2} \prod_{\substack{k=1\\k\neq i}}^{v} x_k^{p^r-1} \qquad \Big(\text{index } \boldsymbol{\alpha}_{i,j}\Big)$$

equals $o_{i,j}$. A kernel vector $\mathbf{u} \in \mathsf{ker}(\mathcal{W})$ is determined only up to a scalar; we normalize it by its entry at the reference index $\boldsymbol{\alpha}_{\mathrm{ref}} = (p^r-1,\ldots,p^r-1,0,\ldots,0)$ (here $x_1^3x_2^3x_3^3$), whose coefficient in L is 1. After this normalization, reading $\mathbf{u}$ at the six indices $\boldsymbol{\alpha}_{i,j}$ gives

$$\begin{aligned}
\boldsymbol{\alpha}_{1,1} &= (2,3,3,1,0)\ \big[x_1^2x_2^3x_3^3x_4\big] \Rightarrow O_{1,1} = \theta,\\
\boldsymbol{\alpha}_{1,2} &= (2,3,3,0,1)\ \big[x_1^2x_2^3x_3^3x_5\big] \Rightarrow O_{1,2} = \theta^2,\\
\boldsymbol{\alpha}_{2,1} &= (3,2,3,1,0)\ \big[x_1^3x_2^2x_3^3x_4\big] \Rightarrow O_{2,1} = 1,\\
\boldsymbol{\alpha}_{2,2} &= (3,2,3,0,1)\ \big[x_1^3x_2^2x_3^3x_5\big] \Rightarrow O_{2,2} = \theta,\\
\boldsymbol{\alpha}_{3,1} &= (3,3,2,1,0)\ \big[x_1^3x_2^3x_3^2x_4\big] \Rightarrow O_{3,1} = \theta^2,\\
\boldsymbol{\alpha}_{3,2} &= (3,3,2,0,1)\ \big[x_1^3x_2^3x_3^2x_5\big] \Rightarrow O_{3,2} = 1.
\end{aligned}$$

Hence

$$\mathbf{O} = \begin{pmatrix} \theta & \theta^2 \\ 1 & \theta \\ \theta^2 & 1 \end{pmatrix}, \quad \mathcal{O} = \mathsf{ColumnSpace}\begin{bmatrix}\mathbf{O}\\ \mathbf{I}_o\end{bmatrix} = \mathsf{Span}\big\{(\theta,1,\theta^2,1,0),\ (\theta^2,\theta,1,0,1)\big\}.$$

This $\mathbf{O}$ is exactly the secret matrix fixed at the start of the example, so $\mathcal{O}$ is the secret oil space and the attack succeeds.

Remark 4. The plain ($r = 1$) system is too small here: with $p^r = 2$ the set $\mathcal{M}_5(3;2)$ consists of the squarefree monomials of degree $v = 3$, so $\mathcal{W}$ has $\binom{n}{v} = \binom{5}{3} = 10$ columns and $m\binom{n}{v+2} = 4\binom{5}{5} = 4$ rows, hence corank at least 6. (For $p = 2$, $r = 1$ this system is exactly the one of the original wedge attack.) Passing to $r = 2$ enlarges it to 260×135 and brings the corank down to 1.

5 Complexity Analysis

In this section, we address the cost of the extended wedge attack and compare it to the cost of other known attacks against the UOV and MAYO signature schemes. We start estimating the rank of the matrix $\mathcal{W}$ by deriving a relationship between the extended wedge attack and the truncated XL algorithm [7].

5.1 Estimating the Rank of $\mathcal{W}$

For a sequence of homogeneous quadratic polynomials $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$, we denote by $\mathrm{Mac}_d(\mathcal{P})$ its truncated Macaulay matrix of degree d in the quotient ring $R^{(p^r)}$. More precisely, $\mathrm{Mac}_d(\mathcal{P})$ is the matrix constructed from the set

$$\left\{ \mathrm{m} \cdot p \pmod{\langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle} : \mathrm{m} \in \mathcal{M}(x_1, \ldots, x_n)_{d-2},\ p \in \mathcal{P} \right\},$$

where $\mathcal{M}(x_1, \ldots, x_n)_d$ denotes the set of monomials of degree d in $R^{(p^r)}$ in the variables $x_1, \ldots, x_n$. The columns of $\mathrm{Mac}_d(\mathcal{P})$ are ordered according to the monomial ordering of the underlying polynomial ring R.

Recall that $\mathcal{M}_n(d; f) = \{\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0} : |\boldsymbol{\alpha}| = d,\ \alpha_i < f\}$. The next is a technical lemma that will be used to prove the main theorem of this section.

Lemma 2. *The complement map $\boldsymbol{\alpha} \mapsto \boldsymbol{\alpha}^c := (p^r-1, \ldots, p^r-1) - \boldsymbol{\alpha}$ is a bijection from $\mathcal{M}_n(v(p^r-1); p^r)$ to $\mathcal{M}_n(o(p^r-1); p^r)$ and from $\mathcal{M}_n(v(p^r-1)+2; p^r)$ to $\mathcal{M}_n(o(p^r-1)-2; p^r)$.*

Proof. The map is clearly an involution ($(\boldsymbol{\alpha}^c)^c = \boldsymbol{\alpha}$) and hence a bijection. For $\boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1); p^r)$, we have $\sum_i \alpha_i = v(p^r-1)$, so $\sum_i (p^r - 1 - \alpha_i) = n(p^r-1) - v(p^r-1) = o(p^r-1)$, showing $\boldsymbol{\alpha}^c \in \mathcal{M}_n(o(p^r-1); p^r)$. Likewise for the other two sets. □

The next theorem shows that the truncated Macaulay matrix $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ and the matrix $\mathcal{W}$ of the extended wedge attack are equivalent up to a permutation of rows and columns.

Recall that we index the columns of $\mathcal{W}$ by n-tuples $\boldsymbol{\alpha}$ in the set $\mathcal{M}_n(v(p^r-1); p^r)$, which is sorted using (14). Similarly, we index the rows of $\mathcal{W}$ by pairs $(k, \boldsymbol{\beta})$, where $1 \leq k \leq m$, and $\boldsymbol{\beta} \in \mathcal{M}_n(v(p^r-1)+2; p^r)$. The set $[k] \times \mathcal{M}_n(v(p^r-1)+2; p^r)$ is sorted using lexicographic ordering.

Theorem 2. *Let $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$ be a homogeneous* OV *map. Given a fixed monomial ordering $\prec$ for $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ and $\mathcal{W}$, there exist permutation matrices $\mathbf{S}_1$ and $\mathbf{S}_2$ such that*

$$\mathrm{Mac}_{o(p^r-1)}(\mathcal{P}) = \mathbf{S}_1 \cdot \mathcal{W} \cdot \mathbf{S}_2.$$

Proof. By Lemma 2, the complement map $\boldsymbol{\alpha} \mapsto \boldsymbol{\alpha}^c$ is a bijection pairing $\mathcal{M}_n(v(p^r-1);p^r) \leftrightarrow \mathcal{M}_n(o(p^r-1);p^r)$ and $\mathcal{M}_n(v(p^r-1)+2;p^r) \leftrightarrow \mathcal{M}_n(o(p^r-1)-2;p^r)$.

Let $\boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1);p^r)$ and $\boldsymbol{\beta} \in \mathcal{M}_n(v(p^r-1)+2;p^r)$. The entries of $\mathcal{W}$ are given by

$$(\mathcal{W})_{(k,\boldsymbol{\beta}),\boldsymbol{\alpha}} = \mathrm{coeff}(a_{\boldsymbol{\alpha}}, (k,\boldsymbol{\beta})),$$

where $\mathrm{coeff}(a_{\boldsymbol{\alpha}}, (k,\boldsymbol{\beta}))$ is the coefficient of $a_{\boldsymbol{\alpha}}$ in the linear equation associated with $\mathbf{x}^{\boldsymbol{\alpha}}$, and the monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ is generated by $L(\mathbf{x}) \cdot p_k \mod \langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle$. For the matrix $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$, we index its rows and columns exactly the same way as for $\mathcal{W}$. The entries of $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ are given by

$$(\mathrm{Mac}_{o(p^r-1)}(\mathcal{P}))_{(k,\boldsymbol{\beta}^c),\boldsymbol{\alpha}^c} = \mathrm{coeff}(\mathbf{x}^{\boldsymbol{\alpha}^c}, (k,\boldsymbol{\beta}^c)),$$

where $\mathrm{coeff}(\mathbf{x}^{\boldsymbol{\alpha}^c}, (k,\boldsymbol{\beta}^c))$ is the coefficient of $\mathbf{x}^{\boldsymbol{\alpha}^c}$ in $\mathbf{x}^{\boldsymbol{\beta}^c} \cdot p_k \mod \langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle$. For each $1 \le k \le m$, write $p_k(\mathbf{x}) = \sum_{1 \le i \le j \le n} b_{i,j}^{(k)} x_i x_j$. Therefore, for any $1 \le k \le m$, $\boldsymbol{\alpha} \in \mathcal{M}_n(v(p^r-1);p^r)$, and $\boldsymbol{\beta} \in \mathcal{M}_n(v(p^r-1)+2;p^r)$, we have

$$(\mathcal{W})_{(k,\boldsymbol{\beta}),\boldsymbol{\alpha}} = \mathrm{coeff}(a_{\boldsymbol{\alpha}}, (k,\boldsymbol{\beta})) = \begin{cases} b_{\boldsymbol{\beta}-\boldsymbol{\alpha}}^{(k)} & \text{if } \alpha_i \le \beta_i \ \forall i \in [n], \\ 0 & \text{otherwise,} \end{cases}$$

$$\begin{aligned} (\mathrm{Mac}_{o(p^r-1)}(\mathcal{P}))_{(k,\boldsymbol{\beta}^c),\boldsymbol{\alpha}^c} = \mathrm{coeff}(\mathbf{x}_{\boldsymbol{\alpha}^c}, (k,\boldsymbol{\beta}^c)) &= \begin{cases} b_{\boldsymbol{\alpha}^c-\boldsymbol{\beta}^c}^{(k)} & \text{if } \beta_i^c \le \alpha_i^c \ \forall i \in [n], \\ 0 & \text{otherwise,} \end{cases} \\ &= \begin{cases} b_{\boldsymbol{\beta}-\boldsymbol{\alpha}}^{(k)} & \text{if } \alpha_i \le \beta_i \ \forall i \in [n], \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

So, if we use $\prec$ as the monomial ordering, the matrices $\mathcal{W}$ and $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ are equal up to a permutation of their elements. More precisely, let $\mathbf{D}_N$ be the anti-diagonal matrix of size $N \times N$. It can be shown that, if we premultiply $\mathcal{W}$ by $\mathbf{I}_m \otimes \mathbf{D}_{|\mathcal{M}_n(v(p^r-1)+2;p^r)|}$, the matrix $\mathbf{I}_m \otimes \mathbf{D}_{|\mathcal{M}_n(v(p^r-1)+2;p^r)|}$ permutes the rows of $\mathcal{W}$ so that its rows correspond to the rows of the matrix $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$. Similarly, it can be shown that if we post-multiply $\mathcal{W}$ by the matrix $\mathbf{D}_{|\mathcal{M}_n(v(p^r-1);p^r)|}$, its columns correspond to the columns of $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$. Thus

$$\mathrm{Mac}_{o(p^r-1)}(\mathcal{P}) = \left(\mathbf{I}_m \otimes \mathbf{D}_{|\mathcal{M}_n(v(p^r-1)+2;p^r)|}\right) \cdot \mathcal{W} \cdot \mathbf{D}_{|\mathcal{M}_n(v(p^r-1);p^r)|}.$$

□

Corollary 1. *Let $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$ be a homogeneous* OV *map. Given a fixed monomial ordering $\prec$ for $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ and $\mathcal{W}$, we have that*

$$\dim(\ker(\mathcal{W})) = \dim(\ker(\mathrm{Mac}_{o(p^r-1)}(\mathcal{P}))).$$

Proof. Note that $\mathbf{I}_m \otimes \mathbf{D}_{|\mathcal{M}_n(v(p^r-1)+2;p^r)|}$ and $\mathbf{D}_{|\mathcal{M}_n(v(p^r-1);p^r)|}$ are permutation matrices. □

5.2 Complexity of Extended Wedge

The complexity analysis of our extended wedge attack relies on a natural generalization of the conjecture made for the complexity analysis of the original wedge attack [12].

Conjecture 1. Given a random homogeneous quadratic sequence $(f_1, \ldots, f_m) \in R^{(p^r)}$, with high probability, the Hilbert series of $R^{(p^r)}/\langle f_1, \ldots, f_m \rangle$ is

$$\mathcal{H}^{p,r}_{n,m}(y) = \left[\frac{(1-y^{p^r})^n}{(1-y)^n} \left(\frac{1-y^2}{1-y^{2p^r}} \right)^m \right]_+ .$$

We stress that above conjecture does not claim that random sequences in $S^{(p^r)} := \mathbb{F}_{p^r}[x_1, \ldots, x_n]/\langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle$ are semi-regular. This last claim has been experimentally tested in [1]. However,

Remark 5. The series $\mathcal{H}^{p,r}_{n,m}(y)$ is the Hilbert series of semi-regular sequences in $S^{(p^r)}$ [1, Theorem 3.3]. Since $S^{(p^r)} \subsetneq R^{(p^r)}$ [4], Conjecture 1 does not imply that random homogeneous sequences in $R^{(p^r)}$ are semi-regular.

Let $\mathcal{P} = (p_1, \ldots, p_m) \in R^m$ be a homogeneous OV map with associated o-dimensional secret space $\mathcal{O}$. Under the condition derived in Section 4.4,

$$v < \min \left\{ \frac{o-1}{2}, 2 \right\} \cdot m,$$

we expect the polynomial $L(\mathbf{x})$ defined in (12) to be the only degree $v(p^r-1)$ polynomial satisfying (12), i.e., $K(\mathbf{x}) \cdot p_k \mod \mathcal{X}_{p^r} = 0$ for each $k \in [m]$. By Theorem 2, the matrices $\mathcal{W}$ and $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ are permutation equivalent. Hence, the polynomial $L(\mathbf{x})$ yields one element in the right kernel of the truncated Macaulay matrix at degree $o(p^r-1)$.

Given $o < v$, assuming OV maps and random homogeneous quadratic polynomials are indistinguishable, make the following prediction

$$\dim\left(\ker\left(\mathcal{W}\right)\right) = \max\left\{ \left[y^{o(p^r-1)} \right] \mathcal{H}^{p,r}_{n,m}(y), 1 \right\}, \tag{20}$$

for $1 \leq r \leq \log_p(q) = e$. We experimentally evaluate the accuracy of that prediction and report the results in Section 6.

The number of columns of the matrix $\mathcal{W}$ is given by

$$H_n\left(o(p^r-1); p^r\right), \quad \text{for } 1 \leq r \leq \log_p(q) = e.$$

As in the original wedge attack [12], we use the projection strategy to reduce the size of the oil space and the number of variables by k units. From Section 4.4, we know that one of the conditions is $v < \frac{o-1}{2} \cdot m$. If we reduce the dimension

[4] Remember $R^{(p^r)} = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{p^r}, \ldots, x_n^{p^r} \rangle$ and $p^r \leq p^e = q$.

of the oil space to $o-k$, it must also meet this condition. Thus, we obtain the restriction $v < \frac{o-k-1}{2} \cdot m$, or equivalently

$$0 \leq k < o - \frac{2v}{m} - 1.$$

If we use the Block Wiedemann algorithm to recover a vector in the kernel of $\mathcal{W}$, we can estimate the time complexity of our attack in field operations using the expression

$$\min_k \; 3\mathcal{D} \cdot \left(H_{n-k}\left((o-k)(p^{r'}-1); p^{r'}\right)\right)^2 \; (2\log_2(q)^2 + \log_2(q)),$$

where

$$\mathcal{D} = \begin{cases} \binom{v+2}{2} & \text{If } p = 2, \\ \binom{n-k+1}{2} & \text{Otherwise.} \end{cases}$$

is the maximum number of non-zero coefficients in each row of the matrix $\mathcal{W}$ and $H_{n-k}\left((o-k)(p^{r'}-1); p^{r'}\right)$ is the number of columns of $\mathcal{W}$. Note that for $p = 2$ the above expression reduces to the time complexity estimate for Ran's attack in [12, Section 6.2].

In Table 1 we present the complexity estimates of our attack against some instances of the UOV and MAYO signature schemes. Notice how our extended wedge attack allows us to cover other parameters of MAYO that the original wedge attack did not include, namely, MAYO_x with $x = 1, 3, 5$.

Table 1. Comparison of the complexity (in $\log_2$) for various parameter sets of both MAYO and UOV. The best attack taken from the Round 2 specifications [3,4] and the p^ℓ-truncated attack [7], [10] is the attack by Jin et al., and [12] is the wedge attack.

					complexity				
scheme	v	o	m	q	best attack	[10]	[12]	this work	(r', k, D)
uov-Ip	68	44	44	256	**128**	140	141	141	(1,26,18)
uov-Is	96	64	64	16	**143**	175	176	176	(1,42,22)
uov-III	112	72	72	256	**182**	206	207	207	(1,46,26)
uov-V	148	96	96	256	**223**	257	258	258	(1,64,32)
MAYO_1	78	8	78	16	**156**	-	-	241	(3,2,42)
MAYO_2	64	17	64	16	**112**	**112**	113	113	(1,4,13)
MAYO_3	108	10	108	16	**224**	-	-	323	(3,2,56)
MAYO_5	142	12	142	16	**296**	-	-	410	(3,2,70)

6 Experimental Evaluation

We experimentally evaluated the accuracy of the formula presented in (20) to predict $\mathsf{dim}(\mathsf{ker}(\mathcal{W}))$ across a wide range of parameters. Recall that the extended

wedge attack recovers the secret space $\mathcal{O}$ by computing a vector in $\mathsf{ker}(\mathcal{W})$, and that this recovery is precisely successful when $\mathsf{dim}(\mathsf{ker}(\mathcal{W})) = 1$.

Our experiments address two goals: quantify how often (20) matches the true kernel dimension, and understand the cases for which it does not. Our experiments show that every observed discrepancy is associated with the failure of one of the two conditions identified in Section 4.4; see Eqs. (17) and (18). We only tested instances satisfying the condition $v < o$, since otherwise we cannot use the behavior of random homogeneous quadratic maps to predict the corank of $\mathcal{W}$ as suggested by Conjecture 1. This last assumption was not made by Furue-Ikematsu [7], and we argue that its violation explains the deviations from semi-regularity reported in §4.4 of that work.

For each parameter tuple (p, e, r, o, v, m), we generated a random OV map over $\mathbb{F}_q$, $q = p^e$, built the respective matrix $\mathcal{W}$ as in (15), and computed its kernel dimension $\mathsf{dim}(\mathsf{ker}(\mathcal{W}))_{\text{exp}}$. We write

$$\Delta := \mathsf{dim}(\mathsf{ker}(\mathcal{W}))_{\text{exp}} - \mathsf{dim}(\mathsf{ker}(\mathcal{W}))_{\text{formula}},$$

where $\mathsf{dim}(\mathsf{ker}(\mathcal{W}))_{\text{formula}}$ denotes the predicted dimension using (20), so that $\Delta = 0$ indicates a perfect match. The experiments cover the fields $\mathbb{F}_{2^4}$, $\mathbb{F}_{3^2}$, $\mathbb{F}_{3^4}$, and $\mathbb{F}_5$, with $2 \le o \le 8$, $3 \le v \le 18$, $2 \le m \le 18$, and $r \in \{1, 2, 3\}$, resulting in 228 parameter sets. All computations were carried out in Magma.

We tested the prediction on 228 parameter sets, obtaining a perfect match in 225 of them. The three failures are far from random. Table 2 presents the three parameter sets for which Eq. (20) fails. We can observe that in all cases at least one of the conditions (17) or (18) fails. Therefore, our experiments confirm that if we impose the conditions (17) and (18) on the parameters (p, e, r, o, v, m), Eq. (20) has an accuracy of 100% to predict $\mathsf{dim}(\mathsf{ker}(\mathcal{W}))_{\text{exp}}$.

$\mathbb{F}_q$	r	o	v	m	$v < 2m$	$v < m\frac{o-1}{2}$	formula	experimental	Δ
$\mathbb{F}_{2^4}$	1	6	8	4	$8 < 8$ ✗	$8 < 10$ ✓	1	2	+1
$\mathbb{F}_5$	1	2	3	2	$3 < 4$ ✓	$3 < 1$ ✗	20	21	+1
$\mathbb{F}_{3^2}$	2	2	3	2	$3 < 4$ ✓	$3 < 1$ ✗	1	21	+20

Table 2. The three parameter sets (out of 228) whose kernel dimension is mispredicted by Eq. (20), with conditions Eqs. (17) and (18) evaluated on each. Every failure violates exactly one condition while satisfying the other. In all cases, the true kernel dimension exceeds the predicted one ($\Delta > 0$).

7 Relation with Furue-Ikematsu's Paper

In this section we relate the extended wedge attack to the attack by Furue and Ikematsu in [7]. Both attacks work in the same truncated polynomial ring, and

Theorem 2 shows that our matrix $\mathcal{W}$ and their truncated Macaulay matrix are equivalent descriptions of the same linear map. We also describe how the parameter analysis for the extended wedge attack (Section 4.4) describes parameters regimes where the algorithm is expected to work.

Furue and Ikematsu attack recovers the oil space of an OV-map $\mathcal{P}$ using the XL algorithm over the truncated polynomial ring

$$R^{(p^r)} = \mathbb{F}_{p^e}[x_1, \ldots, x_n] / \left\langle x_1^{p^r}, \ldots, x_n^{p^r} \right\rangle, \qquad 1 \leq r \leq e.$$

The attack works in three steps: we first build the truncated Macaulay matrix $\mathrm{Mac}_d(\mathcal{P})$ for $2 \leq d \leq o(p^r - 1)$. The degree d is chosen large enough so that, for a random homogeneous quadratic $\mathcal{P}_{rnd} \in R^m$, the kernel dimension of $\mathrm{Mac}_d(\mathcal{P}_{rnd})$ is expected to be zero. Then, we compute a vector $\mathbf{a}$ in the kernel of $\mathrm{Mac}_d(\mathcal{P})$, and finally read the oil space off that vector $\mathbf{a}$. This works because for every degree $2 \leq d \leq o(p^r - 1)$, the right kernel of $\mathrm{Mac}_d(\mathcal{P})$ contains several linearly independent vectors such that the oil space $\mathcal{O}$ can be reconstructed from selected entries of any of those kernel vectors.

The matrix $\mathcal{W}$ of the extended wedge attack (Section 4.2) represents polynomial equations in the same truncated ring, but its rows and columns are not produced by the XL expansion. They are fixed by the combinatorial structure of $L(\mathbf{x}) = \prod_{i=1}^{v} (\ell_i(\mathbf{x}))^{p^r - 1}$ and its product by homogeneous quadratic polynomials. The nonzero entries of $\mathcal{W}$ are given by the coefficients of the public polynomials as described in (15). The connection between $\mathcal{W}$ and the truncated Macaulay matrix is given by Theorem 2, the matrices $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ and $\mathcal{W}$ are equal up to a permutation of rows and columns. At this degree, the secret-space information carried by $\mathrm{Mac}_{o(p^r-1)}(\mathcal{P})$ reduces to a single kernel vector which, under the complement bijection of Lemma 2, is the coefficient vector of $L(\mathbf{x})$ — exactly the vector that the extended wedge attack solves for.

The connection also holds below the top degree $d = o(p^r - 1)$, and it comes from the proper subspaces of the oil space $\mathcal{O}$. Given $2 \leq s < o$, every s-dimensional subspace $\mathcal{S} \subseteq \mathcal{O}$ is a vanishing space for $\mathcal{P}$, so Theorem 1 applied to a basis $\mathbf{t}_1, \ldots, \mathbf{t}_{n-s}$ of $\mathcal{S}^\perp$ gives the polynomial

$$L_{\mathcal{S}}(\mathbf{x}) = \prod_{i=1}^{n-s} \langle \mathbf{x}, \mathbf{t}_i \rangle^{p^r - 1},$$

of degree $(n - s)(p^r - 1)$ such that $L_{\mathcal{S}}(\mathbf{x}) \cdot p(\mathbf{x}) \bmod \mathcal{X}_{p^r} = 0$ for every $p \in \mathcal{P}$. Similarly, as for the oil-space $\mathcal{O}$, the last polynomial equation yields a linear system $\mathcal{W}_{\mathcal{S}} \cdot \mathbf{a} = 0$ in the unknown coefficients $\mathbf{a}$ of $L_{\mathcal{S}}(\mathbf{x})$. Analogously to Theorem 2, we can proof $\mathcal{W}_{\mathcal{S}}$ is permutation equivalent to $\mathrm{Mac}_{s(p^r-1)}(\mathcal{P})$. Thus, the secret-space information that Theorem 2 of [7] attaches to $\mathrm{Mac}_{s(p^r-1)}(\mathcal{P})$ at the intermediate degree $s(p^r - 1)$ arises, in our framework, from the proper subspaces of $\mathcal{O}$.

Finally, we highlight that, as for the extended wedge attack, Theorem 1 can also be used to mount the intersection attack described in [7], the polynomial decomposition of the intersection equations is given in Proposition 6 in Appendix B, and the attack follows analogously as the extended wedge attack.

References

1. John Baena, Daniel Cabarcas, Sharwan K. Tiwari, Javier Verbel, and Luis Villota. Admissible parameters for the crossbred algorithm and semi-regular sequences over finite fields. *Designs, Codes and Cryptography*, 2025.
2. Ward Beullens. Improved cryptanalysis of UOV and Rainbow. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 348–373. Springer, Cham, October 2021.
3. Ward Beullens. MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography*, pages 355–376, Cham, 2022. Springer International Publishing.
4. Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang. UOV: Unbalanced oil and vinegar algorithm specifications and supporting documentation, 2023. Available online.
5. David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 4th edition, 2015.
6. Carina Curto, Vladimir Itskov, Alan Veliz-Cuba, and Nora Youngs. The neural ring: An algebraic tool for analyzing the intrinsic structure of neural codes. *Bulletin of Mathematical Biology*, 75(9):1571–1611, 2013.
7. Hiroki Furue and Yasuhiko Ikematsu. Key recovery attacks on UOV using p^ℓ-truncated polynomial rings. Cryptology ePrint Archive, Paper 2026/298, 2026.
8. Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 187–217, Cham, 2021. Springer International Publishing.
9. Sudhir R. Ghorpade. A note on Nullstellensatz over finite fields, 2018. arXiv:1806.09489 [math.AC].
10. Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong, and Jintai Ding. Security analysis on UOV families with odd characteristics: Using symmetric algebra. In Shi Bai and Edoardo Persichetti, editors, *PKC 2026, Part I*, volume 16551 of *LNCS*, pages 428–454. Springer, Cham, May 2026.
11. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, pages 206–222, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.
12. Lars Ran. Wedges, oil, and vinegar - an analysis of UOV in the exterior algebra. In Joan Daemen and Emmanuel Thomé, editors, *EUROCRYPT 2026, Part IV*, volume 16545 of *LNCS*, pages 363–388. Springer, Cham, May 2026.
13. Lih-Chung Wang, Po-En Tseng, Yen-Liang Kuan, and Chun-Yen Chou. A simple noncommutative UOV scheme. Cryptology ePrint Archive, Paper 2022/1742, 2022.

A A Gröbner Basis for the Vanishing Ideal of $\mathcal{O}$.

Let $R = \mathbb{F}_q[x_1, \ldots, x_n]$ and choose a monomial ordering $\prec$ on it. We first recall some important concepts about Gröbner bases.

Definition 3 (Gröbner basis). *A finite subset $G = \{g_1, \ldots, g_s\} \subseteq I$ of a nonzero ideal I is a* Gröbner basis *of I (with respect to the ordering $\prec$) if* $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. *A Gröbner basis generates its ideal: $I = \langle g_1, \ldots, g_s \rangle$.*

Definition 4 (S-polynomial). *For nonzero polynomials $f, g \in R$ set $\gamma = \operatorname{lcm}\big(\operatorname{LM}(f), \operatorname{LM}(g)\big)$. The* S-polynomial *of f and g is $S(f,g) = \dfrac{\gamma}{\operatorname{LT}(f)} f - \dfrac{\gamma}{\operatorname{LT}(g)} g$.*

The next two propositions are very useful to determine if a finite set is a Gröbner basis of and ideal; see [5, Ch. 2].

Proposition 2 (Buchberger's criterion). *A finite set $G = \{g_1, \ldots, g_s\}$ generating an ideal I is a Gröbner basis of I if and only if the remainder of the S-polynomial $S(g_i, g_j)$ on division by G is 0 for all $i \neq j$.*

Proposition 3 (Product criterion). *If $\operatorname{LM}(g_i)$ and $\operatorname{LM}(g_j)$ are coprime, i.e., $\operatorname{lcm}(\operatorname{LM}(g_i), \operatorname{LM}(g_j)) = \operatorname{LM}(g_i)\operatorname{LM}(g_j)$, then $S(g_i, g_j)$ reduces to 0 modulo $\{g_i, g_j\}$. Consequently, if the leading monomials of $g_1, \ldots, g_s$ are pairwise coprime, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis of $\langle g_1, \ldots, g_s \rangle$.*

We also use the finite-field form of the strong Nullstellensatz theorem over an arbitrary finite field.

Proposition 4 (Finite-field Nullstellensatz). *For every ideal $J \subseteq R$,*

$$I\big(\mathrm{V}_{\mathbb{F}_q}(J)\big) = J + \big\langle x_1^q - x_1, \ldots, x_n^q - x_n \big\rangle,$$

where $V_{\mathbb{F}_q}(J) := \{\mathbf{a} \in \mathbb{F}_q^n : f(\mathbf{a}) = 0 \text{ for all } f \in J\}$ is the set of $\mathbb{F}_q$-rational zeros of J. Equivalently, $J + \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle$ is a radical ideal equal to the vanishing ideal of its $\mathbb{F}_q$-points [9,6].

The next proposition shows that the linear polynomials $\ell_1, \ldots, \ell_v$ together with the field equations $x_1^q - x_1, \ldots, x_n^q - x_n$ form a Gröbner basis of the ideal $I(\mathcal{O})$.

Proposition 5. *Let the notation be as in Theorem 1, and let*

$$G := \{\ell_1, \ldots, \ell_v, x_1^q - x_1, \ldots, x_n^q - x_n\}.$$

Then

$$I(\mathcal{O}) = \langle \ell_1, \ldots, \ell_v, x_1^q - x_1, \ldots, x_n^q - x_n \rangle,$$

and G is a Gröbner basis of $I(\mathcal{O})$ with respect to every monomial ordering satisfying $x_1 \succ \cdots \succ x_n$.

Proof. Since the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_v$ form a basis of $\mathcal{O}^\perp$, we have that

$$\begin{aligned} V_{\mathbb{F}_q}(\langle \ell_1, \ldots, \ell_v \rangle) &= V_{\mathbb{F}_q}(\ell_1, \ldots, \ell_v) \\ &= \{\mathbf{x} \in \mathbb{F}_q^n : \ell_i(\mathbf{x}) = 0 \text{ for all } i = 1, \ldots, v\} \\ &= \{\mathbf{x} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{v}_i \rangle = 0 \text{ for all } i = 1, \ldots, v\} \\ &= \big(\mathcal{O}^\perp\big)^\perp \\ &= \mathcal{O}. \end{aligned}$$

Notice that the last equality holds because the standard dot product is non-degenerate, so $(W^{\perp})^{\perp} = W$ for every subspace $W \subseteq \mathbb{F}_q^n$. The finite-field Nullstellensatz [9,6] states that for every ideal $J \subseteq R$,

$$I\big(V_{\mathbb{F}_q}(J)\big) = J + \langle x_1^q - x_1, \ldots, x_n^q - x_n \rangle.$$

Applying this result with $J = \langle \ell_1, \ldots, \ell_v \rangle$ gives

$$I(\mathcal{O}) = I\big(V_{\mathbb{F}_q}(J)\big) = \langle \ell_1, \ldots, \ell_v, x_1^q - x_1, \ldots, x_n^q - x_n \rangle\,.$$

It remains to prove that G is a Gröbner basis of $I(\mathcal{O})$. Since $\mathbf{V} = \big[\mathbf{I}_v \; -\mathbf{O}\big]^{\top}$, each polynomial ℓ_i has the form $\ell_i(\mathbf{x}) = x_i - \mathcal{L}_i(\mathbf{x})$, where

$$\mathcal{L}_i(\mathbf{x}) = \sum_{k=1}^{o} o_{i,k} x_{v+k}, \qquad i = 1, \ldots, v.$$

Hence $\mathrm{LM}(\ell_i) = x_i$, and the leading monomials of the ℓ_i's are pairwise distinct.

For $1 \le i \le v$ we claim

$$x_i^q - x_i = \ell_i^q - \ell_i + \sum_{j=1}^{o} o_{ij}\,(x_{v+j}^q - x_{v+j}). \tag{21}$$

Indeed, since q is a power of the characteristic of $\mathbb{F}_q$, the Frobenius identity gives $\ell_i^q = (x_i - \mathcal{L}_i)^q = x_i^q - \mathcal{L}_i^q$, and, using $o_{ij}^q = o_{ij}$ for $o_{ij} \in \mathbb{F}_q$, we obtain

$$\mathcal{L}_i^q = \Big(\sum_j o_{ij} x_{v+j}\Big)^q = \sum_j o_{ij}^q x_{v+j}^q = \sum_j o_{ij} x_{v+j}^q.$$

Thus

$$\begin{aligned}
\ell_i^q - \ell_i + \sum_{j=1}^{o} o_{ij}\,(x_{v+j}^q - x_{v+j}) &= (x_i^q - \mathcal{L}_i^q) - (x_i - \mathcal{L}_i) \\
&\quad + \Big(\sum_j o_{ij} x_{v+j}^q - \sum_j o_{ij} x_{v+j}\Big) \\
&= x_i^q - \mathcal{L}_i^q - x_i + \mathcal{L}_i + \mathcal{L}_i^q - \mathcal{L}_i \\
&= x_i^q - x_i,
\end{aligned}$$

proving (21). Since $\ell_i^q - \ell_i = (\ell_i^{q-1} - 1)\ell_i \in \langle \ell_i \rangle$, equality (21) shows that $x_i^q - x_i \in \langle \ell_i, x_{v+1}^q - x_{v+1}, \ldots, x_n^q - x_n \rangle$ for each $i \le v$. Hence, setting

$$G' := \{\ell_1, \ldots, \ell_v,\; x_{v+1}^q - x_{v+1}, \ldots, x_n^q - x_n\} \subseteq G,$$

we have $\langle G \rangle = \langle G' \rangle$, i.e., the field equations $x_1^q - x_1, \ldots, x_v^q - x_v$ are redundant in $\langle G \rangle$. Addionally, the leading monomials of the elements of G' are

$$x_1, \ldots, x_v, \quad x_{v+1}^q, \ldots, x_n^q,$$

which are pairwise coprime (distinct single variables, or a single variable against a power of a different variable). By the product criterion (Proposition 3), G' is a Gröbner basis of $\langle G' \rangle = \langle G \rangle$. Since $G' \subseteq G \subseteq \langle G \rangle = \langle G' \rangle$,

$$\big\langle \mathrm{LT}(G') \big\rangle \subseteq \big\langle \mathrm{LT}(G) \big\rangle \subseteq \mathrm{LT}\big(\langle G \rangle\big) = \mathrm{LT}\big(\langle G' \rangle\big) = \big\langle \mathrm{LT}(G') \big\rangle,$$

so all inclusions are equalities and $\langle \mathrm{LT}(G) \rangle = \mathrm{LT}(\langle G \rangle)$, i.e., G is also a Gröbner basis of $\langle G \rangle = I(\mathcal{O})$. □

B Intersection Attack on UOV

The intersection attack recovers a vector lying in the intersection of two images of the secret space $\mathcal{O}$ under two linear maps given by linear combinations of the matrices representing the polar quadratic polynomials vanishing in $\mathcal{O}$ [2]. Furue and Ikematsu formulate it over the p^ℓ-truncated ring improving the state-of-the-art attacks against UOV [7].

This appendix places that attack inside the present framework. We rewrite the three blocks of the intersection system in terms of the linear forms supplied by Theorem 1 (Proposition 6) and show that the resulting system reproduces the intersection attack of [7].

Let $(p_1, \ldots, p_m)$ be an OV map with secret space $\mathcal{O}$. Let $\mathbf{P}_k, \mathbf{P}'_k \in \mathbb{F}_q^{n \times n}$ be the matrices representing the polynomials p_k and its polar form p'_k, respectively.

For two invertible matrices $\mathbf{W}_1, \mathbf{W}_2$ chosen from the span of the matrices $\mathbf{P}'_1, \ldots, \mathbf{P}'_m$, the intersection attack finds $\mathbf{x} \in \mathbb{F}_q^n$ that satisfies the $3m$ equations

$$\begin{cases} (\mathbf{W}_1^{-1}\mathbf{x})^\top \mathbf{P}_k (\mathbf{W}_1^{-1}\mathbf{x}) = 0, \\ (\mathbf{W}_1^{-1}\mathbf{x})^\top \mathbf{P}'_k (\mathbf{W}_2^{-1}\mathbf{x}) = 0, \quad (\text{for each } k \in [m]) \\ (\mathbf{W}_2^{-1}\mathbf{x})^\top \mathbf{P}_k (\mathbf{W}_2^{-1}\mathbf{x}) = 0, \end{cases} \tag{22}$$

of which $3m - 2$ are linearly independent [2].

We now rewrite (22) using Theorem 1. Let $\ell_1, \ldots, \ell_v$ be the linear forms cutting out $\mathcal{O}$, and $g_{k,j}$ the linear factor such that

$$p_k(\mathbf{y}) \;=\; \sum_{j=1}^{v} g_{k,j}(\mathbf{y})\, \ell_j(\mathbf{y}), \qquad k \in [m]. \tag{23}$$

In the following proposition, for each $(j, i) \in [v] \times [2]$, we set

$$\ell_j^{(i)}(\mathbf{x}) \;:=\; \ell_j\big(\mathbf{W}_i^{-1}\mathbf{x}\big), \text{ and } g_{k,j}^{(i)}(\mathbf{x}) \;:=\; g_{k,j}\big(\mathbf{W}_i^{-1}\mathbf{x}\big).$$

Proposition 6. *For each $k \in [m]$ the three quadratic forms of* (22) *are given by*

$$
\begin{aligned}
(\mathbf{W}_1^{-1}\mathbf{x})^\top \mathbf{P}_k (\mathbf{W}_1^{-1}\mathbf{x}) &= \sum_{j=1}^{v} g_{k,j}^{(1)}(\mathbf{x})\, \ell_j^{(1)}(\mathbf{x}) \\
(\mathbf{W}_1^{-1}\mathbf{x})^\top \mathbf{P}'_k (\mathbf{W}_2^{-1}\mathbf{x}) &= \sum_{j=1}^{v} \Big[g_{k,j}^{(1)}(\mathbf{x})\, \ell_j^{(2)}(\mathbf{x}) \;+\; g_{k,j}^{(2)}(\mathbf{x})\, \ell_j^{(1)}(\mathbf{x}) \Big], \\
(\mathbf{W}_2^{-1}\mathbf{x})^\top \mathbf{P}_k (\mathbf{W}_2^{-1}\mathbf{x}) &= \sum_{j=1}^{v} g_{k,j}^{(2)}(\mathbf{x})\, \ell_j^{(2)}(\mathbf{x}).
\end{aligned}
$$

Since each $\ell_j^{(i)}$ vanishes in $\mathcal{O}_{int} := \mathbf{W}_1\mathcal{O} \cap \mathbf{W}_2\mathcal{O}$ and $\mathsf{dim}(\mathcal{O}_{int}) \geq 3o - n$, the vector space spanned by the $2v$ polynomials $\ell_j^{(i)}$ is of dimension $n - \mathsf{dim}(\mathcal{O}_{int}) \leq 2v - o$, so there are at least o linear relations among the $\ell_j^{(i)}$'s.