# Attacking UOV-based Signatures with Schur–Macaulay Matrices

Simon-Philipp Merz[1], Lars Ran[2]

[1] ETH Zurich, Switzerland
[2] Radboud University Nijmegen, Netherlands

**Abstract.** Unbalanced Oil and Vinegar (UOV) and its variants are among the candidates in the NIST call for additional post-quantum signatures. Their security rests on the hardness of recovering a hidden subspace on which a public system of quadratic forms vanishes. In characteristic 2 the polar forms of such a system are alternating, which a recent attack exploits by working in the exterior algebra rather than the polynomial ring. Unlike its polynomial-ring counterparts, it either applies at a threshold fixed by the parameters or not at all, and for most proposed parameter sets it does not.

We remove this threshold and improve complexity in two independent ways. First, over the integers the square of an alternating polar form is $\omega \wedge \omega = 2\,\omega^{(2)}$, so in characteristic 2 it vanishes only because the factor 2 does. Dividing that factor out before reducing leaves the divided square $\omega^{(2)}$, which still vanishes on the oil space but is in general not a consequence of the original equations. Iterating gives a whole tower $\omega^{(2^j)}$ of new equations. Second, the symmetric powers $\mathrm{Sym}^d \mathbb{F}_q^n$ and the exterior powers $\bigwedge^a \mathbb{F}_q^n$ are the two extreme shapes of the Schur modules $L_\lambda \mathbb{F}_q^n$. We introduce an extension of Macaulay matrices to an arbitrary shape $\lambda$ which we call Schur–Macaulay matrices. For both constructions we conjecture a Hilbert series and verify it experimentally. We also extend the approach to odd characteristic.

The attack then applies to every Round-2 parameter set of UOV, MAYO, SNOVA, and QR-UOV but one. Four of the alternate Round-2 parameter sets of MAYO fall below their claimed security level while being out of reach of all previous attacks. After disclosing preliminary results to the MAYO team, a parameter set designated for Round-3 was discarded and parameters increased. For SNOVA, the divided powers remove the spurious kernel elements that obstructed the exterior algebra attack, and seven of the eleven Round-2 parameter sets fall below their claimed security level, and the complexity estimates drop further compared to previous attacks.

## 1 Introduction

Multivariate cryptography is among the oldest approaches to post-quantum signatures. The most prominent family of multivariate signatures descends from Unbalanced Oil and Vinegar (UOV) [20], which is at the basis of half of the

Round-3 candidates in NIST's ongoing standardisation process, i.e. UOV itself [7], MAYO [6], QR-UOV [17] and SNOVA [26]. All of these schemes rest on the same problem. A public homogeneous quadratic map $\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is chosen which vanishes on a secret subspace $O \subset \mathbb{F}_q^n$ of dimension $o$. The message is hashed, together with a salt, to a target $\mathbf{t} \in \mathbb{F}_q^m$, and the signature is a vector $\mathbf{s} \in \mathbb{F}_q^n$ with $\mathcal{P}(\mathbf{s}) = \mathbf{t}$. Knowledge of the oil space provides the trapdoor. No $p_i$ contains a quadratic term purely in the $o$ coordinates along $O$, so fixing the remaining $v = n - o$ coordinates turns $\mathcal{P}$ into a linear system, which a signer who knows $O$ solves by linear algebra.

The classical attacks all linearise in the polynomial ring using XL [11]. A direct attack ignores the hidden structure and solves $\mathcal{P}(\mathbf{s}) = \mathbf{t}$ with Gröbner-basis methods. The Kipnis–Shamir attack [21] recovers $O$ as a common invariant subspace of the public forms, broke the original balanced scheme (with $o = v$), and as its cost grows with the imbalance, only the unbalanced case $v > o$ has been considered since. The reconciliation attack [13] looks for one or more oil vectors, which already suffice to recover the whole space [1, 23]. Finally, Beullens' intersection attack [4] improves on this when the parameters are close to balanced.

In characteristic 2 the polar form of a quadratic form is alternating, and Ran [24] used this to change the space in which the problem is linearised. Rather than solving for a basis of $O$ one solves for the single element $\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_v \in \bigwedge^v O^\perp \subset \bigwedge^v \mathbb{F}_q^n$, which depends on $O$ and not on any chosen basis of $O$ or $O^\perp$. The condition that the public forms vanish on $O$ becomes linear in its coordinates, so key recovery turns into a sparse linear algebra problem. In [19], this approach was generalized to arbitrary characteristic by considering reduced symmetric algebras instead of the exterior algebra. Furue and Ikematsu [16] subsequently obtained the same matrices without passing through the exterior or reduced symmetric algebras, by descending the ordinary Macaulay matrix to the truncated ring $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$, and extended the construction to $p^\ell$-truncations. Within this truncated-ring framework, they succeeded in combining the truncated rings with the intersection attack, yielding improved complexities over the wedge attack.

This line of attack has a limitation that was not present for attacks in polynomial rings. The $\bigwedge^a O$ vanishes for $a > o$, so the attack either succeeds at degree $o$ — or, after projecting to a smaller oil space, at some $o' \leq o$ — or it does not apply at all.

By passing to Plücker coordinates and finding *linear* relations therein, Ran's attack [24] takes advantage of the full oil space. The Plücker coordinates made their appearance earlier in cryptanalysis in the Support-Minors model [2] where the system is *bilinear*. The reason for their effectiveness is that the Plücker coordinates encode the subspace, eliminating the redundancy of the GL-action on the parametrized basis. Plücker coordinates are not algebraically independent, they satisfy the quadratic Plücker relations, which cut out the Grassmannian. These relations have also been considered in cryptanalysis, in [3] for the Support-Minors model, and in [24, Section 7] for the exterior algebra attack in odd char-

acteristic. In neither case did they improve on the state-of-the-art complexities. The symmetric powers, exterior powers, and the degree-$d$ part of the homogeneous coordinate ring of the Grassmannian are all examples of Schur modules. We extend this line of attacks by generalizing Macaulay matrices to arbitrary Schur modules which yields a Macaulay-matrix approach specialized to isotropic subspaces.

**Contributions.** We remove the obstruction common to the wedge attack and the truncated-ring attack and further improve this line of attack in two independent directions.

*Divided powers.* Computed over the integers, the square of an alternating polar form is $\omega \wedge \omega = 2\,\omega^{(2)}$, so in characteristic 2 it vanishes only because the factor 2 does. Dividing that factor out before reducing leaves the divided square $\omega^{(2)}$, which still vanishes on the oil space but is generally not a consequence of the original equations, and iterating gives a whole tower $\omega^{(2^j)}$ of new relations that help in a key recovery attack.

*Schur modules.* The symmetric power $\mathrm{Sym}^d \mathbb{F}^n$ and the exterior power $\bigwedge^a \mathbb{F}^n$ are the two extremes of the family of Schur modules $L_\lambda \mathbb{F}^n$ [27]. In characteristic 0 these are precisely the irreducible polynomial representations of $\mathrm{GL}_n$ [15], so they are the minimal $\mathrm{GL}_n$-equivariant spaces in which the problem can be linearised. We introduce Macaulay matrices on an arbitrary $L_\lambda \mathbb{F}_q^n$, hereafter named Schur–Macaulay matrices, so that the classical attack and the exterior algebra attack become special cases of the same attack. The shape $\lambda$ then becomes a parameter of the attack in the same sense as the operating degree $d$ in XL or the projected dimension $o'$ in the wedge attack. The relations defining the quotient $L_\lambda \mathbb{F}_q^n$ of $\bigwedge^{\lambda_1} \mathbb{F}_q^n \otimes \cdots \otimes \bigwedge^{\lambda_k} \mathbb{F}_q^n$ can be defined as multi-homogeneous maps between multi-graded algebras. These maps do not come from multiplications by algebra elements as in XL or the wedge attacks, so the resulting Schur–Macaulay matrices carry non-commutative operator columns alongside the usual ones. We analyse how these maps behave with respect to the multiplication maps and conjecture the Hilbert series predicting the rank of these matrices. The shape determines whether the system saturates, the size of the solution space, and the cost of the attack.

Together, the two extensions make the attack applicable to every parameter set we considered. For MAYO and SNOVA they lower the expected security for several Round-2 parameters below the required security level. Four of MAYO's alternate parameter sets, spread among all the security levels, now fall below their claimed security. For a further sixteen sets the attack applies for the first time, though above the security level, and where the original attack already applied the divided powers lower $o'$ and with it sometimes the cost. After we disclosed preliminary results to the MAYO team, a parameter set designated for Round-3, which our attack would have broken by more than 20 bits, was discarded and the parameters were raised accordingly.

Adjoining the divided squares also removes elements from the solution space, which for $v \geq 2m$ prevented the wedge attack from applying to SNOVA at all. This lets us give complexities for the SNOVA Round-2 parameter sets in Tab. 2.

*Code.* The sage implementation of the experiments, complexity estimators, and toy examples can be found in the repository below

https://github.com/LarsMath/Schur--Macaulay-attack

Concurrently with and independently of this work, Ikematsu and Furue [18] extended Ran's attack in a different direction and applied it to SNOVA. Their truncated ring is the exterior algebra, and the element they target is the same, but where they analyse the structure of the enlarged solution space under a conjecture, we remove the obstruction outright. The two approaches turn out to be effective in different regimes and we compare them in Remark 3.8.

**Outline.** Sect. 2 introduces some notation, and recalls necessary background on UOV and the exterior algebra attack. Sect. 3 introduces divided powers and the resulting extension of the attack within a single exterior power. Sect. 4 develops the case of two exterior powers, where the transfer maps first appear, and Sect. 5 generalises this methodology to arbitrary Schur modules. Sect. 6 gives the cost analysis and the resulting estimates for MAYO [6], SNOVA [26], and QR-UOV [17].

## 2 Preliminaries

In this section, we introduce some notation and recall basic preliminaries regarding UOV and recent attacks on it. Further mathematical concepts that have previously not been used in UOV cryptanalysis will be introduced in later sections as needed.

**Notation.** We will denote vectors by boldface letters like $\mathbf{x}, \mathbf{t}, \mathbf{o}$ and the zero vector by $\mathbf{0}$. Given a ring $\mathcal{R}$ and an element $x \in \mathcal{R}$, we denote by $m_x : \mathcal{R} \to \mathcal{R}$ the multiplication map of $x$. For a power series $f = \sum_{i \geq 0} f_i \, t^i$ with integer coefficients we write $f[t^i] = f_i$ and $[f]_+$ for the power series with coefficients

$$[f]_+[t^i] = \begin{cases} f_i & \text{if } f_{i'} > 0 \text{ for all } 0 \leq i' \leq i, \\ 0 & \text{otherwise.} \end{cases}$$

This is the truncation of $f$ before its first non-positive coefficient.

### 2.1 Symmetric and exterior powers

Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis of $\mathbb{F}_q^n$. The *exterior power* $\bigwedge^d \mathbb{F}_q^n$ has as basis the products $\mathbf{e}_S = \mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_d}$ over $d$-subsets $S = \{i_1 < \cdots < i_d\}$. Thus $\dim \bigwedge^d \mathbb{F}_q^n = \binom{n}{d}$, and it vanishes for $d > n$. The exterior powers sum to the algebra $\bigwedge \mathbb{F}_q^n = \bigoplus_{0 \leq i \leq n} \bigwedge^i \mathbb{F}_q^n$ generated by $\bigwedge^1 \mathbb{F}_q^n$, where the product is determined by $\mathbf{x} \wedge \mathbf{y} = -\mathbf{y} \wedge \mathbf{x}$ and $\mathbf{x} \wedge \mathbf{x} = 0$. In characteristic 2 the sign disappears and $\bigwedge \mathbb{F}_q^n$ is commutative. For an arbitrary element $\mathcal{X} \in \bigwedge^d \mathbb{F}_q^n$ and

subset $S \subset [n]$ we will denote by $\mathcal{X}_S$ the coefficient of $\mathbf{e}_S$ in $\mathcal{X}$ in the standard basis if $|S| = d$ and 0 otherwise.

The *symmetric power* $\operatorname{Sym}^d \mathbb{F}_q^n$ has as basis the monomials of degree $d$ in $\mathbf{e}_{i_1} \cdot \cdots \cdot \mathbf{e}_{i_d}$ with $i_1 \leq \cdots \leq i_d$. Thus $\operatorname{Sym}^d \mathbb{F}_q^n \cong \mathbb{F}[x_1, \ldots, x_n]_d$ via $\mathbf{e}_i \mapsto x_i$ and $\dim \operatorname{Sym}^d \mathbb{F}_q^n = \binom{n+d-1}{d}$.

The dimension sequences for $\bigwedge^k \mathbb{F}_q^n$ and $\operatorname{Sym}^k \mathbb{F}_q^n$ have generating functions $(1+t)^n$ and $(1-t)^{-n}$ respectively.

### 2.2 Sparse linear algebra

Given a square matrix $A \in \mathbb{F}^{N \times N}$ over a finite field $\mathbb{F}$ that has a right kernel of dimension one, we will be interested in finding this unique right kernel element. We will base our complexity estimations on Wiedemann's algorithm [28] and its block variant [10] for black box matrix kernel finding which is a randomized algorithm.

To run the algorithm, we need to apply $A$ to a vector $3N$ times in total. First, $2N$ times to find a minimal polynomial and then another $N$ times to find the kernel element. If $A$ has $\rho \cdot N$ non-zero entries, then we can apply $A$ in a black-box manner using $\rho \cdot N$ field multiplications. Assuming the RAM model and ignoring address-generation costs, this time complexity in field operations is given by[3]

$$3 \cdot \rho \cdot N^2.$$

*Remark 2.1.* The RAM model is an idealized model for computing time complexities of algorithms. Recently, this assumption was challenged for Wiedemann-XL in [12] and the authors derive more precise estimates. For comparison with the specifications of the various involved schemes, we will stick to the RAM model and report the peak-memory usage for completeness.

### 2.3 Unbalanced Oil and Vinegar (UOV)

The security of UOV-based signature schemes rests on the difficulty of recovering a hidden subspace on which a public system of quadratic equations vanishes.

**Definition 2.2.** *Let $v, o, m$ be positive integers and set $n = v + o$. Given a homogeneous quadratic map $\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ vanishing on a subspace $O \subset \mathbb{F}_q^n$ of dimension $o$, the* $(v, o, m)$-UOV problem *asks to find $O$.*

The subspace $O$ is called the *oil space*. Originally the scheme used "balanced" parameters $v = o$, but after an attack by Kipnis and Shamir [21] only the unbalanced case $v > o$ is considered.

[3] In recent work [9], the authors show that the constant factor is rather close to 2 but we will stick with 3 for comparative reasons.

The oil space serves as a trapdoor to invert $\mathcal{P}$. Because each $p_i$ vanishes on $O$, the polynomials contain no quadratic terms consisting solely of oil variables. Consequently, if one fixes the vinegar variables to random values $\mathbf{x} \in \mathbb{F}_q^v$, the resulting map $\mathcal{P}'(\mathbf{x}, \cdot)$, for the polar forms $\mathcal{P}'$, is a linear system in terms of the oil variables. Thus, anyone who knows $O$ can easily find preimages of $\mathcal{P}$ by solving a linear system. These preimages can then be used as a signature for the salted hash in $\mathbb{F}_q^m$ of any message.

Recovering $O$ reduces to finding a single vector in the oil space [1, 23]. Since finding a single oil vector suffices for key recovery, we may look for a subspace of $O$ instead. For $o' \leq o$ let $H = \langle \mathbf{e}_1, \ldots, \mathbf{e}_{v+o'} \rangle_{\mathbb{F}_q}$. Then $O' = O \cap H$ has dimension $o'$ with high probability, and the restrictions of $p_1, \ldots, p_m$ to $H$ form a $(v, o', m)$-UOV instance with oil space $O'$. Throughout the paper we run our attacks on this instance and choose $o'$ to minimise the cost. The attacks only see the polar forms, and $m$ random alternating forms vanish on $q^{o'v - m\binom{o'}{2}}$ subspaces of dimension $o'$ in expectation. Hence $O'$ is the unique solution only if $m(o'-1) > 2v$ and we restrict to such $o'$.

### 2.4 Variants of UOV

UOV uses $m = o$, but this is not necessarily the case for its variants. MAYO [5, 6] uses $o < m$, and both QR-UOV [17] and SNOVA [26] are defined over an extension field which gives a UOV instance over $\mathbb{F}_{q^\ell}$ with $m = \ell o$ for QR-UOV and $m = o$, $v \geq 2m$ for SNOVA. Key recovery for all of them is an instance of Def. 2.2, over $\mathbb{F}_{q^\ell}$ where applicable, with varying ratios between $m$, $v$ and $o$.

### 2.5 Intersection attack

In [4], Beullens introduced the intersection attack on UOV. This gives a randomized way to transform a $(v, o, m)$-UOV instance into a $(2v-o, 2o-v, 3m-2)$-UOV instance.

The idea is as follows, let $\beta_1, \ldots, \beta_m$ be the polar forms of $p_1, \ldots, p_m$. Let $\beta, \beta'$ be any pair of linearly independent invertible[4] polar forms in $\langle \beta_1, \ldots, \beta_m \rangle_{\mathbb{F}_q}$. Without loss of generality take $\beta = \beta_1$ and $\beta' = \beta_2$. Then for an oil vector $\mathbf{o} \in O$ we obtain that $\beta_i \mathbf{o} \in O^\perp$ hence $\beta_i O \subset O^\perp$. Let $V = \beta_1 O \cap \beta_2 O$, then $\dim V \geq 2o - v$ and $\beta_i^{-1} V \subset O$ for $i = 1, 2$. Therefore, $V$ is an oil space for the quadratic maps

$$p_j \circ \beta_1^{-1}, \quad p_j \circ \beta_2^{-1}, \quad p_j \circ (\beta_1^{-1} + \beta_2^{-1}) \qquad \text{for all } 1 \leq j \leq m$$

Since these maps exhibit 2 linear dependencies, this gives us $3m - 2$ maps.

Note that these transformed systems are not generic. For relevant parameters, the UOV instances obtained in this way are a proper subset of all $(2v - o, 2o - v, 3m - 2)$-UOV instances by dimension count. In other words, in algebraic attacks, these systems might behave differently from random UOV systems. However, to the best of our knowledge, no difference in behaviour has been reported in the literature.

[4] In characteristic 2 we need $n$ to be even.

### 2.6 The exterior algebra attack

In [24] an attack against UOV in characteristic 2 was proposed leveraging the fact that the polar forms of quadratic forms are alternating in that case. The main structure of the polar forms $\omega_1, \ldots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ is that they can be written as

$$\omega_j = \sum_{i=1}^{v} \mathbf{v}_i \wedge \mathbf{x}_{ij}$$

for $\langle \mathbf{v}_1, \ldots, \mathbf{v}_v \rangle = O^\perp$ and $\mathbf{x}_{ij} \in \mathbb{F}_q^n$. Using this, one can parametrize $\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v$ as a linear element $\mathcal{X} \in \bigwedge^v \mathbb{F}_q^n$ and obtain $m\binom{n}{v+2}$ linear equations $\mathcal{X} \wedge \omega_j = \mathbf{0}$ by observing $\omega_j \wedge \mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v = \mathbf{0}$.

In [24] it was shown that the resulting Macaulay matrix is the same Macaulay matrix that one would get for the system $\{p_1, \ldots, p_m\}$ as elements of

$$\mathbb{F}[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle.$$

Later, in [16], this identification was taken further and the authors showed how to obtain this matrix without passing through the exterior algebra. They show that the standard $\mathbb{F}[x_1, \ldots, x_n]$ Macaulay matrix for UOV systems must descend to an $\mathbb{F}[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle$ Macaulay matrix using the vanishing on the subspace. Using this, one can define the more general truncated polynomial rings $\mathbb{F}[x_1, \ldots, x_n]/\langle x_1^{2^\ell}, \ldots, x_n^{2^\ell} \rangle$ to relax the solving conditions. Furthermore, by taking this polynomial point of view, one can also apply this reduction to the system occurring in the intersection attack.

In this paper we take a hybrid between these points of view, as in [16] we will work in the dual of the original attack, but we consider the algebra $\bigwedge \mathbb{F}_q^n$ instead of the isomorphic $\mathbb{F}[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle$. In other words, the element $[O] = \mathbf{o}_1 \wedge \cdots \wedge \mathbf{o}_o$ will lie in the cokernel of the map

$$\begin{aligned} \mathcal{M} : \left( \bigwedge^{o-2} \mathbb{F}_q^n \right)^m &\to \bigwedge^o \mathbb{F}_q^n \\ (\mathcal{X}_1, \ldots, \mathcal{X}_m) &\mapsto \sum_{i=1}^{m} \mathcal{X}_i \wedge \omega_i. \end{aligned}$$

## 3 Extending the exterior algebra attack

The behaviour of UOV systems in characteristic 2 was already observed to be surprising in [16, 24]. In this section we exploit the even characteristic further. The failure of the exterior square to detect the vanishing of the square of alternating polar forms, $\omega \wedge \omega$, allows us to extract relations of degree $2^i$ for $i > 1$ which are not consequences of the original equations, and which may therefore be added to the system.

These equations have three effects. First, they lower the minimal $o'$ for which the attack applies for some parameter sets in the literature. Second, they remove

the spurious kernel elements that obstruct the attack on the SNOVA maps in [24]. Third, they simplify the analysis of the attack extensions considered later in the paper.

### 3.1 Additional equations

Let $\omega \in \bigwedge^2 \mathbb{F}_q^n$ be an alternating polar form associated to one of the public quadratics defining a UOV instance and let $\mathbf{v}_1, \ldots, \mathbf{v}_v$ be a basis for the vinegar space $O^\perp$. By [24, Lem. 2], we know that

$$\omega = \sum_i \mathbf{v}_i \wedge \mathbf{x}_i$$

for some $\mathbf{x}_i \in \mathbb{F}_q^n$.

One of the syzygies appearing among these polar forms is the square $\omega \wedge \omega = \mathbf{0}$. Computed over $\mathbb{Z}$, we can write the square as

$$\omega \wedge \omega = \left(\sum_i \mathbf{v}_i \wedge \mathbf{x}_i\right) \wedge \left(\sum_i \mathbf{v}_i \wedge \mathbf{x}_i\right) = 2\sum_{i<j} \mathbf{v}_i \wedge \mathbf{x}_i \wedge \mathbf{v}_j \wedge \mathbf{x}_j,$$

with the terms with $i = j$ vanishing because $\mathbf{v}_i$ repeats, and each unordered pair occurring twice with the same sign since $\mathbf{v}_i \wedge \mathbf{x}_i$ has even degree. In characteristic 2 the left-hand side therefore vanishes for the sole reason that the factor 2 does. Yet, dividing out before reducing modulo 2 leaves the *divided square*

$$\omega^{(2)} \coloneqq \sum_{i<j} \mathbf{v}_i \wedge \mathbf{x}_i \wedge \mathbf{v}_j \wedge \mathbf{x}_j,$$

which is in general non-zero.

This element cannot in general be written as $\alpha \wedge \omega$ with $\alpha \in \bigwedge^2 \mathbb{F}_q^n$, i.e. it does not lie in the ideal generated by $\omega$. However, we have

$$\omega^{(2)} \wedge \mathcal{V} = \left(\sum_{i<j} \mathbf{v}_i \wedge \mathbf{x}_i \wedge \mathbf{v}_j \wedge \mathbf{x}_j\right) \wedge \mathcal{V} = \mathbf{0}$$

and thus $\omega^{(2)}$ lies in the ideal generated by the vinegar space giving us a genuinely new relation on $\mathcal{V}$. To understand equations such as this one better, we introduce divided powers.

**Divided powers** We begin with the definition we are going to use in the following and show that it is well-defined. Recall that for a subset $S = \{s_1 < \cdots < s_k\} \subseteq \{1, \ldots, n\}$ we write $\mathbf{e}_S = \mathbf{e}_{s_1} \wedge \cdots \wedge \mathbf{e}_{s_k}$ and that for $\mathbb{F}_q$ of characteristic 2, we have $\mathbf{e}_S \wedge \mathbf{e}_T = \mathbf{e}_{S \cup T}$ whenever $S$ and $T$ are disjoint, and $\mathbf{e}_S \wedge \mathbf{e}_T = 0$ otherwise.

**Definition 3.1.** *Let $q$ be even, $d \in \mathbb{N}$, and let $\alpha \in \bigwedge^{2d} \mathbb{F}_q^n$, written in the standard basis as*

$$\alpha = \sum_{|S|=2d} c_S \, \mathbf{e}_S, \qquad c_S \in \mathbb{F}_q,$$

*the sum running over the $2d$-element subsets $S \subseteq \{1, \dots, n\}$. For $i \geq 1$ we call*

$$\alpha^{(i)} = \sum_{\substack{\{S_1,\dots,S_i\} \\ \text{pairwise disjoint}}} c_{S_1} \cdots c_{S_i} \, \mathbf{e}_{S_1 \cup \cdots \cup S_i} \in \bigwedge^{2di} \mathbb{F}_q^n,$$

*the sum running over the unordered families of $i$ pairwise disjoint $2d$-element subsets of $\{1, \dots, n\}$, the $i$-th* divided power *of $\alpha$, and set $\alpha^{(0)} = 1$.*

**Lemma 3.2.** *The divided powers of Def. 3.1 do not depend on the choice of basis. Moreover, for $\alpha, \beta \in \bigwedge^{2d} \mathbb{F}_q^n$, we have*

$$\alpha^{(1)} = \alpha, \qquad \alpha^{(i)} \wedge \alpha^{(j)} = \binom{i+j}{i} \alpha^{(i+j)}, \qquad (\alpha + \beta)^{(r)} = \sum_{i+j=r} \alpha^{(i)} \wedge \beta^{(j)}.$$

*Proof.* Each coefficient of the element $\alpha^{(i)}_{\mathcal{B}}$ that Def. 3.1 produces from a basis $\mathcal{B}$ is an integer polynomial in the $c_S$, so for any two bases it suffices to check the assertion $\alpha^{(i)}_{\mathcal{B}} = \alpha^{(i)}_{\mathcal{B}'}$ over $\mathbb{Q}$. Expanding $\alpha^{\wedge i}$ there removes every term whose $i$ index sets are not pairwise disjoint and makes the $i!$ orderings of a disjoint family contribute equally, with factors of even degree and hence commuting. Thus we have $\alpha^{(i)}_{\mathcal{B}} = \frac{1}{i!}\alpha^{\wedge i}$ over $\mathbb{Q}$, which is independent of the basis.

The first identity is immediate. For the second, a product occurring in $\alpha^{(i)} \wedge \alpha^{(j)}$ vanishes unless the two families are jointly pairwise disjoint, in which case it equals $\mathbf{e}_{S_1 \cup \cdots \cup T_j}$ with coefficient $c_{S_1} \cdots c_{T_j}$. Each family of $i+j$ pairwise disjoint subsets thus arises $\binom{i+j}{i}$ times. For the third, $\alpha + \beta$ has coefficients $c_S + d_S$, and expanding $\prod_{k \leq r} (c_{S_k} + d_{S_k})$ and collecting the terms with exactly $i$ factors from $\alpha$ gives $\sum_{i+j=r} \alpha^{(i)} \wedge \beta^{(j)}$.

*Remark 3.3.* Def. 3.1 is restricted to even degree because in odd degree the construction is vacuous. Over $\mathbb{Q}$ the terms of $\alpha^{\wedge 2}$ indexed by $(S, T)$ and $(T, S)$ are negatives of one another, so $\alpha^{\wedge 2} = 0$ identically and $\frac{1}{i!}\alpha^{\wedge i} = 0$ for $i \geq 2$. In even degree these terms are instead equal, so $\alpha^{\wedge 2} = 2\,\alpha^{(2)}$ vanishes in characteristic 2 and the divided square survives.

**Lemma 3.4.** *Let $\alpha \in \bigwedge^{2d} \mathbb{F}_q^n$. Then $\{\alpha^{(2^j)}\}_{j \geq 0}$ generates the same subalgebra as $\{\alpha^{(i)}\}_{i \geq 1}$, and each of these generators squares to zero.*

*Proof.* Let $i = \sum_j \epsilon_j 2^j$ be a binary decomposition. By Kummer's theorem $\binom{a+b}{a}$ is odd whenever $a$ and $b$ have disjoint binary support, whereas $\binom{2^{j+1}}{2^j}$ is even. Iterating the second identity of Lem. 3.2 therefore gives

$$\alpha^{(i)} = \bigwedge_{\epsilon_j = 1} \alpha^{(2^j)}, \qquad \alpha^{(2^j)} \wedge \alpha^{(2^j)} = 0.$$

**Lemma 3.5.** *Let $\omega$ be a UOV polar form, i.e. an alternating form vanishing on the oil space $O$, and let $\mathbf{v}_1, \ldots, \mathbf{v}_v$ be a basis of $O^\perp$ in $\mathbb{F}_q^n$. Then for every $r > 0$ there exist $\gamma_i \in \bigwedge^{2r-1} \mathbb{F}_q^n$ such that*

$$\omega^{(r)} = \sum_{i=1}^{v} \mathbf{v}_i \wedge \gamma_i,$$

*and $\omega^{(r)} = 0$ for $r > v$.*

*Proof.* Since $\omega$ vanishes on $O$, its $\bigwedge^2 O$-component vanishes, so $\omega = \sum_{i=1}^{v} \mathbf{v}_i \wedge \mathbf{x}_i$ for suitable $\mathbf{x}_i \in \mathbb{F}_q^n$. Write $a_i = \mathbf{v}_i \wedge \mathbf{x}_i$, so that $\omega = \sum_{i=1}^{v} a_i$. Each $a_i$ satisfies $a_i^{(j)} = 0$ for $j \geq 2$, every 2-element subset in the support of $a_i = \mathbf{v}_i \wedge \mathbf{x}_i$ contains the index of $\mathbf{v}_i$, so no two of them are disjoint. Iterating the third identity of Lem. 3.2 therefore leaves only the multi-indices with entries in $\{0, 1\}$, giving

$$\omega^{(r)} \;=\; \sum_{|S|=r} \bigwedge_{i \in S} a_i.$$

Every summand contains $\mathbf{v}_i$ for each $i \in S$. Collecting the summands under one such factor gives the claim, and the sum is empty for $r > v$.

For $\omega \in \bigwedge^2 \mathbb{F}_q^n$ the generator $\omega^{(2^j)}$ has degree $2^{j+1}$, and by Lem. 3.5 it vanishes as soon as $2^j > v$. Writing $2^J \leq v < 2^{J+1}$ and assuming that the squarefree monomials in $\omega^{(2^0)}, \ldots, \omega^{(2^J)}$ remain linearly independent, the subalgebra they generate has Hilbert series

$$\prod_{j=0}^{J} (1 + t^{2^{j+1}}) = \frac{1 - t^{2^{J+2}}}{1 - t^2},$$

which agrees with $(1 - t^2)^{-1}$ in all degrees up to $2v$.

Conjecturing that the $m$ towers corresponding to the $m$ alternating forms behave independently, we arrive at the following.

*Conjecture 3.6.* Let $\omega_1, \ldots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ be the polar forms of a generic UOV public key with parameters $(n, o, m)$, and let

$$I \;=\; \left(\, \omega_i^{(2^j)} \;:\; 1 \leq i \leq m,\; j \geq 0 \,\right) \;\subseteq\; \bigwedge \mathbb{F}_q^n$$

be the ideal generated by their divided-power towers. Then $\bigwedge \mathbb{F}_q^n / I$ has Hilbert series

$$\left[(1 + t)^n (1 - t^2)^m\right]_+.$$

### 3.2 Experiments

We computed $\dim(\bigwedge \mathbb{F}_q^n / I)_a$ for random alternating systems with the full divided-power tower adjoined. Each entry is the smallest dimension observed over repeated runs with independently sampled systems, and is retained once an independent run reproduces it. Tab. 1 records the parameters covered. The series

of Conj. 3.6 matches *all* of the 1173 instances, across 111 distinct shapes $(n, a)$ with $n$ up to 19, wedge degrees up to 18, and up to 171 forms, including several instances where the wedge attack would not have saturated.

| $a$ | # instances | $n$ | $m$ | series prediction correct |
|---|---|---|---|---|
| 2 | 833 | 3–19 | 3–171 | 833/833 |
| 3 | 192 | 4–19 | 2–51 | 192/192 |
| 4 | 77 | 5–19 | 1–25 | 77/77 |
| 5 | 20 | 6–17 | 1–9 | 20/20 |
| $\geq 6$ | 51 | 7–19 | 1–4 | 51/51 |
| total | 1173 | 3–19 | 1–171 | 1173/1173 |

**Table 1.** Exterior-power experiments over $\mathbb{F}_{256}$, spanning 111 distinct shapes $(n, a)$ and ambient spaces of dimension up to 6188. In every instance the measured dimension agrees with $[(1+t)^n(1-t^2)^m]_+$ of Conj. 3.6.

*Remark 3.7.* Interestingly, adjoining the towers even produces the correct Hilbert series prediction for $o > v$. Even though this is not relevant for cryptography, it does show the generality of the prediction.

### 3.3 Consequences

The divided powers add rows to the Macaulay matrix and make it more dense. A row coming from $\omega_i^{(2^j)}$ has $\binom{v+2^{j+1}}{2^{j+1}}$ non-zero entries, compared to the $\binom{v+2}{2}$ for the original equations. In return they may lower the smallest $o'$ for which the attack applies.

Furthermore, they change the structure of the solution space. For $v \geq 2m$ the element $P = \omega_1 \wedge \cdots \wedge \omega_m$ satisfies $P \wedge \omega_i = 0$, so the multiples of $P$ lie in the solution space by [24]. And since that space is usually not one-dimensional this obstructs the attack. However, as established in this section, the identity $\omega_i \wedge \omega_i = 0$ is the vanishing of a factor 2 rather than a relation, and $P \wedge \omega_i^{(2^j)}$ does not vanish in characteristic 2 in general. Therefore, adjoining the divided squares removes these additional kernel elements, and the attack applies at parameters where plain wedge multiplication did not saturate before.

To compute the resulting complexities of lifted SNOVA [22] we consider the Hilbert series in [25] with the projection strategy from [8]. We adapt the Hilbert series to incorporate the adjoined towers:

$$\mathcal{H}(\mathbf{t}) = \prod_{i=1}^{l}(1+t_i)^{v+o'_i} \cdot \prod_{i=1}^{l}(1-t_i^2)^m \cdot \prod_{1\leq i<j\leq l}(1-t_it_j)^{2m}.$$

Then, the nullity of the matrix for projection $\mathbf{o}' = (o'_1, \ldots, o'_l)$ is given by $\mathcal{H}[\mathbf{t}^{\mathbf{o}'}]$. The formula for the cost analysis is described in Sect. 6.1. The resulting complexities for the Round 2 parameters of SNOVA [26] can be found in Tab. 2.

| | | | | | [8] | | Divided powers | | |
|---|---|---|---|---|---|---|---|---|---|
| $v$ | $o$ | $m$ | $\ell$ | $q$ | bits | $\mathbf{o}'$ | bits | $\log_2 N$ | $\mathbf{o}'$ |
| 37 | 17 | 17 | 2 | $16^2$ | 109 | $(14, 1)$ | 99 | 38 | $(13, 0)$ |
| 25 | 8 | 8 | 3 | $16^3$ | 109 | $(8, 7, 0)$ | 110 | 43 | $(8, 6, 0)$ |
| 24 | 5 | 5 | 4 | $16^4$ | 157 | $(5, 5, 5, 5)$ | 151 | 64 | $(5, 5, 5, 4)$ |
| 56 | 25 | 25 | 2 | $16^2$ | 147 | $(19, 1)$ | 139 | 56 | $(18, 0)$ |
| 49 | 11 | 11 | 3 | $16^3$ | 246 | $(11, 11, 10)$ | 245 | 107 | $(11, 10, 9)$ |
| 37 | 8 | 8 | 4 | $16^4$ | 213 | $(8, 8, 8, 3)$ | 204 | 88 | $(8, 8, 8, 1)$ |
| 24 | 5 | 5 | 5 | $16^5$ | 155 | $(5, 5, 5, 5, 0)$ | 152 | 64 | $(5, 5, 5, 4, 0)$ |
| 75 | 33 | 33 | 2 | $16^2$ | 188 | $(25, 1)$ | 173 | 71 | $(22, 0)$ |
| 66 | 15 | 15 | 3 | $16^3$ | 312 | $(15, 15, 10)$ | 305 | 132 | $(15, 15, 6)$ |
| 60 | 10 | 10 | 4 | $16^4$ | — | — | — | — | — |
| 29 | 6 | 6 | 5 | $16^5$ | 180 | $(6, 6, 6, 5, 0)$ | 178 | 77 | $(6, 6, 6, 4, 0)$ |

**Table 2.** Bit complexity and projection $\mathbf{o}'$ for the Round 2 SNOVA parameter sets [26] compared to [8].

*Remark 3.8.* Concurrently with and independently of our work, Ikematsu and Furue [18] extend Ran's wedge-product attack [24] in a different direction, and apply it to SNOVA. The setting partially coincides with ours as their truncated ring $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$ is isomorphic to $\bigwedge \mathbb{F}_q^n$, and the kernel element they pursue is $\mathbf{o}_1 \wedge \cdots \wedge \mathbf{o}_o$. The original wedge attack needs the degree-$o$ solution space to be one-dimensional, which fails as soon as $v \geq 2m$, since $P = \omega_1 \wedge \cdots \wedge \omega_m$ is then a second kernel element. Ikematsu and Furue determine the structure of $\langle P, [O] \rangle$ under a conjecture that they support experimentally. This allows them to recover $O$ from an arbitrary kernel element by a linear argument, and derive an explicit complexity. Our route is to remove the obstruction. In characteristic 2 the identity $\omega_i \wedge \omega_i = 0$ on which $P$ rests is not a relation but the vanishing of the factor 2 in $\omega_i \wedge \omega_i = 2\omega_i^{(2)}$ by Remark 3.3. Adjoining the divided squares stops $P$ from lying in the kernel. At their experimental parameters $(q, v, o, m) = (16, 8, 7, 3)$ we measure a degree-$o$ solution space of dimension 103 across five independent instances, confirming their prediction $\dim\langle P, [O] \rangle = H_2 + 1 = 103$, writing $H_d$ in their notation for the degree-$d$ coefficient of $\left[(1+t)^n(1+t^2)^{-m}\right]_+$. Adjoining the divided squares reduces the dimension to 1, and the kernel element is $[O]$. The two approaches are effective in different parameter regimes.

## 4 Bigraded exterior algebras

The main limitation of the original exterior algebra attack is that it either applies or it does not. Whereas XL against the MQ problem can scale the degree indefinitely for example, in the exterior algebra attack we can only scale it up to $o$. In [24] it was remarked that including the Plücker relations might get around this but the analysis was left open. Increasing the degree in this way and including these relations correspond exactly to Schur modules associated with rectangular partitions. Here we take it a step further and extend the attack to arbitrary Schur modules.

To ease exposition, we will explain this structure using the bigraded exterior algebra on $\mathbb{F}_q^n$. These correspond exactly to Schur modules with two columns. In Sect. 5 we will extend this to arbitrary partitions. We will mainly follow the exposition and conventions of [27].

### 4.1 Parametrizing the oil space twice

We can mimic the increase in degree in XL by parametrizing the oil space multiple times and imposing relations among these copies. To do this we define the algebra we are working in.

**Definition 4.1.** *We call* $\bigwedge^{\bullet,\bullet} \mathbb{F}_q^n := \bigwedge(\mathbb{F}_q^n \oplus \mathbb{F}_q^n) \cong \bigwedge \mathbb{F}_q^n \otimes \bigwedge \mathbb{F}_q^n$ *the* bigraded exterior algebra on $\mathbb{F}_q^n$. *The bigrading is given as*

$$\bigwedge^{a,b} \mathbb{F}_q^n := \bigwedge^{a} \mathbb{F}_q^n \otimes \bigwedge^{b} \mathbb{F}_q^n.$$

Note that in this algebra multiplication is inherited from $\bigwedge(\mathbb{F}_q^n \oplus \mathbb{F}_q^n)$ and hence given by

$$\begin{aligned} \wedge : \bigwedge^{a,b} \mathbb{F}_q^n \otimes \bigwedge^{a',b'} \mathbb{F}_q^n &\to \bigwedge^{a+a',b+b'} \mathbb{F}_q^n \\ (\alpha \otimes \beta) \wedge (\alpha' \otimes \beta') &= (-1)^{ba'} (\alpha \wedge \alpha') \otimes (\beta \wedge \beta'). \end{aligned}$$

We work in characteristic 2 and ignore these signs from here on. Since $\bigwedge(\mathbb{F}_q^n \oplus \mathbb{F}_q^n) = \bigwedge \mathbb{F}_q^{2n}$, Def. 3.1 applies to every $\alpha \in \bigwedge^{a,b} \mathbb{F}_q^n$ of even total degree $a+b$ and yields divided powers $\alpha^{(i)} \in \bigwedge^{ia,\, ib} \mathbb{F}_q^n$, with the identities of Lem. 3.2; in particular $\alpha \wedge \alpha = 2\,\alpha^{(2)} = 0$.

Now just as in the exterior algebra attack we have that $\bigwedge^{a,b} O \subset \bigwedge^{a,b} \mathbb{F}_q^n$ and we will put relations on the bigraded exterior algebra on $\mathbb{F}_q^n$ to carve out this piece. Note that $\dim \bigwedge^{a,b} \mathbb{F}_q^n = \binom{n}{a}\binom{n}{b}$ and hence $\dim \bigwedge^{o,o} O = 1$.

**Relating the two parametrized oil spaces** Right now, doubling the oil space appears to double the search space and double the work. Luckily, we can still relate the two coordinates. Without loss of generality, we will assume $a \geq b$ from here on. To build these relations, we will use that we can lower the degree of an element without changing its spanning set. This is known in many forms, we prove the version we need.

**Lemma 4.2.** *Let $W \subset \mathbb{F}_q^n$ be a $k$-dimensional subspace and let $\mathcal{X} \in \bigwedge^a W \subset \bigwedge^a \mathbb{F}_q^n$. For a set $I \subset [n]$ denote the space $\mathcal{H}_I = \langle \mathbf{e}_i : i \notin I \rangle_{\mathbb{F}_q}$. Then for any $I \subset [n]$ with $|I| = i \leq a$ we have*

$$\sum_{\substack{K \subset [n] \setminus I \\ |K| = a-i}} \mathcal{X}_{K \cup I} \cdot \mathbf{e}_K \in \bigwedge^{a-i} (W \cap \mathcal{H}_I) \subset \bigwedge^{a-i} \mathbb{F}_q^n.$$

*Proof.* First note that if $k < a$ then $\mathcal{X} = \mathbf{0}$ and hence the result holds. Write $I = \{i_1 < \cdots < i_i\}$ and pick a basis $\mathbf{w}_1, \ldots, \mathbf{w}_k \in W$ such that

$$(\mathbf{w}_\ell)_{i_j} = \begin{cases} 1 & \text{if } \ell = j \\ 0 & \text{otherwise} \end{cases} \qquad \text{for all } 1 \leq j \leq i, 1 \leq \ell \leq k.$$

If this is not possible, then that must mean that $\mathcal{X}_{K \cup I} = 0$ for all $K \subset [n], |K| = a - i$ and hence the result follows. So let us assume we have such a basis and write

$$\mathcal{X} = \sum_{\substack{J \subseteq [k] \\ |J| = a}} \alpha_J \mathbf{w}_{j_1} \wedge \cdots \wedge \mathbf{w}_{j_a}.$$

Now let us denote

$$\mathcal{Y} = \sum_{\substack{L \subseteq [k] \setminus I \\ |L| = a-i}} \alpha_{I \cup L} \, \mathbf{w}_{l_1} \wedge \cdots \wedge \mathbf{w}_{l_{a-i}}.$$

From the specifically chosen basis it follows that $\mathcal{Y}_K = \mathcal{X}_{K \cup I}$. Thus $\mathcal{Y}$ is exactly the given element and is indeed an element of $\bigwedge^{a-i} (W \cap \mathcal{H}_I)$.

What this lemma implies is that for any element $\mathcal{Y} \in \bigwedge^b O$ and any $I \subset [n]$ with $|I| = b - 1$ we obtain an oil vector

$$\mathbf{y}_I = (\mathcal{Y}_{I \cup \{1\}}, \ldots, \mathcal{Y}_{I \cup \{n\}}) \in \bigwedge^1 O = O.$$

But that also means that for an element $\mathcal{X} \otimes \mathcal{Y} \in \bigwedge^{o,b} O$ we obtain $\binom{n}{b-1}$ equations $\mathbf{y}_I \wedge \mathcal{X} = \mathbf{0} \in \bigwedge^{o+1} O$. This might look like a lot of bookkeeping but luckily we can bundle these relations as follows.

$$\begin{aligned} \theta_1 : \bigwedge^{a+1,b-1} \mathbb{F}_q^n &\to \bigwedge^{a,b} \mathbb{F}_q^n \\ \mathbf{e}_I \otimes \mathbf{e}_J &\mapsto \sum_{i \in I} \mathbf{e}_{I \setminus \{i\}} \otimes \mathbf{e}_{J \cup \{i\}} \end{aligned}$$

We can extend this reasoning to $I$ of any size to obtain $\binom{n}{b-i}$ equations $\mathbf{y}_I \wedge \mathcal{X} = \mathbf{0} \in \bigwedge^{o+i} O$. Similarly we obtain

$$\theta_\ell : \bigwedge^{a+\ell,b-\ell} \mathbb{F}_q^n \to \bigwedge^{a,b} \mathbb{F}_q^n$$

$$\mathbf{e}_I \otimes \mathbf{e}_J \mapsto \sum_{\substack{K \subset I \\ |K|=\ell}} \mathbf{e}_{I \setminus K} \otimes \mathbf{e}_{J \cup K}.$$

For convenience, we denote $\theta_0 \coloneqq \mathrm{id}$.

Note that the $\theta_i$ maps are completely independent of the UOV instance. And indeed, the quotient of $\bigwedge^{a,b} \mathbb{F}_q^n$ by these relations is the Schur module corresponding to $(a, b)$. Denote

$$\Theta^{a,b} = \sum_{i \geq 1} \mathrm{im}(\bigwedge^{a+i,b-i} \mathbb{F}_q^n \xrightarrow{\theta_i} \bigwedge^{a,b} \mathbb{F}_q^n),$$

then the Schur module is given by

$$L_{(a,b)}\mathbb{F}_q^n = \bigwedge^{a,b} \mathbb{F}_q^n \Big/ \Theta^{a,b}.$$

**Properties of the $\theta_i$.** The $\theta_i$ are themselves far from independent. Splitting off $i$ factors and then $j$ further ones produces each splitting into $i + j$ factors exactly $\binom{i+j}{i}$ times, so that

$$\theta_i \circ \theta_j = \binom{i+j}{i} \theta_{i+j}. \tag{1}$$

In characteristic 0 this collapses the whole family, $\sum_i \mathrm{im}\, \theta_i = \mathrm{im}\, \theta_1$. In characteristic $p$ it does not, since $\theta_i \circ \theta_{p-i} = \binom{p}{i}\theta_p = 0$, so that $\theta_p$ can contribute new elements. Yet by Lucas' theorem the family reduces to the powers of $p$,

$$\Theta^{a,b} = \sum_{1 \leq i \leq b} \mathrm{im}\, \theta_i = \sum_{0 \leq j \leq \log_p b} \mathrm{im}\, \theta_{p^j}. \tag{2}$$

*Remark 4.3.* As the same arithmetic applies, the identity Eq. (1) is the second identity of Lem. 3.2 for divided powers, and Eq. (2) reduces the family to $\{\theta_{2^j}\}$ in characteristic 2 for exactly the same reason as for divided powers in Lem. 3.4.

We record one further property, a *Leibniz rule* which we will later use repeatedly

$$\theta_i(\alpha \cdot \beta) = \sum_{0 \leq j \leq i} \theta_j(\alpha) \cdot \theta_{i-j}(\beta).$$

Finally, we record how the $\theta_i$ act on divided powers. Over a ring in which 2 is invertible the following is then a direct consequence of the Leibniz rule and the following lemma shows that the identity persists in characteristic 2.

**Lemma 4.4.** *Let $\alpha \in \bigwedge^{(a,b)} \mathbb{F}_q^n$ with $a + b \equiv 0 \bmod 2$. Then for every $k \geq 1$*

$$\theta_k\big(\alpha^{(2)}\big) = \sum_{0 \leq l < k/2} \theta_l(\alpha) \cdot \theta_{k-l}(\alpha) \; + \begin{cases} \big(\theta_{k/2}(\alpha)\big)^{(2)} & k \text{ even}, \\ 0 & k \text{ odd}. \end{cases}$$

*Proof.* Both sides of the identity are integer polynomial expressions in the coordinates of $\alpha$. As in the proof of Lem. 3.2 it therefore suffices to verify them over $\mathbb{Q}$. Over $\mathbb{Q}$ the second identity of Lem. 3.2 gives $\alpha \cdot \alpha = 2\,\alpha^{(2)}$, so $\alpha^{(2)} = \frac{1}{2}\,\alpha \cdot \alpha$, and the Leibniz rule yields

$$\theta_k\big(\alpha^{(2)}\big) = \tfrac{1}{2} \sum_{l=0}^{k} \theta_l(\alpha) \cdot \theta_{k-l}(\alpha).$$

Each $\theta_l$ preserves the total degree $a+b$, which is even, so the elements $\theta_l(\alpha)$ commute and the terms indexed by $l$ and by $k-l$ coincide.

If $k$ is odd, we have $(k+1)/2$ equal pairs and $\theta_k(\alpha^{(2)}) = \sum_{0 \le l < k/2} \theta_l(\alpha) \cdot \theta_{k-l}(\alpha)$. If $k$ is even, the term $l = k/2$ occurs once and the remaining ones pair, so

$$\theta_k\big(\alpha^{(2)}\big) = \tfrac{1}{2}\,\theta_{k/2}(\alpha) \cdot \theta_{k/2}(\alpha) + \sum_{0 \le l < k/2} \theta_l(\alpha) \cdot \theta_{k-l}(\alpha),$$

and using $\frac{1}{2}\,\beta \cdot \beta = \beta^{(2)}$ for $\beta = \theta_{k/2}(\alpha)$, again of even total degree, finishes the proof.

### 4.2 Relations on the bigraded exterior algebra

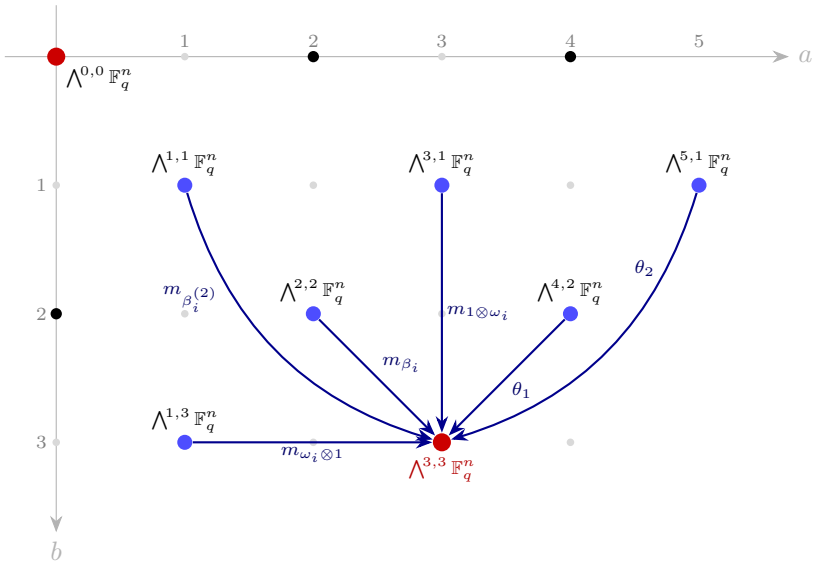
Just as in the exterior algebra attack, the 2-forms $\omega_1, \ldots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ imply relations on $\bigwedge^{a,b} \mathbb{F}_q^n$. However, this time, there are two slots to apply them. We can treat them as elements of $\bigwedge^{2,0} \mathbb{F}_q^n$ or as elements of $\bigwedge^{0,2} \mathbb{F}_q^n$ and hence each $\omega_i \in \bigwedge^2 \mathbb{F}_q^n$ implies maps

$$m_{\omega_i \otimes 1} : \bigwedge^{a-2,b} \mathbb{F}_q^n \to \bigwedge^{a,b} \mathbb{F}_q^n \quad \text{and} \quad m_{1 \otimes \omega_i} : \bigwedge^{a,b-2} \mathbb{F}_q^n \to \bigwedge^{a,b} \mathbb{F}_q^n.$$

Furthermore, recall that the polar forms are bilinear maps $\beta_i : \mathbb{F}_q^n \otimes \mathbb{F}_q^n \to \mathbb{F}_q$. These forms vanish on the oil space and hence we also obtain relations

$$m_{\beta_i} : \bigwedge^{a-1,b-1} \mathbb{F}_q^n \to \bigwedge^{a,b} \mathbb{F}_q^n.$$

Moreover, these elements are all even-graded, so we can include multiplying by their divided squares. It will be useful to see these maps pictorially.




**Interaction between the relations.** Now that we have these relations $\theta_i$ and multiplying with $\omega_i \otimes 1$, $\beta_i$, and $1 \otimes \omega_i$, let us see how they interact.

At first, we might hope that all these maps are independent, but this is too much to ask for. For instance in the multiplication maps we have the trivial syzygies

$$m_x \circ m_y = m_y \circ m_x$$

and hence $\operatorname{im} m_x \cap \operatorname{im} m_y \neq 0$. However, due to the Leibniz rule, and the fact that $\theta_1(\omega_i \otimes 1) = \beta_i$ and $\theta_2(\omega_i \otimes 1) = 1 \otimes \omega_i$, we can say even more

$$\begin{aligned}\theta_1 \circ m_{\omega\otimes 1}(\alpha) &= \theta_1((\omega \otimes 1) \wedge \alpha) \\ &= \beta \wedge \alpha + (\omega \otimes 1) \wedge \theta_1(\alpha) \\ &= (m_\beta + m_{\omega\otimes 1} \circ \theta_1)(\alpha).\end{aligned}$$

In other words $\operatorname{im} m_\beta \subset \operatorname{im} \theta_1 + \operatorname{im} m_{\omega\otimes 1}$. Likewise

$$\begin{aligned}\theta_2 \circ m_{\omega\otimes 1}(\alpha) &= \theta_2((\omega \otimes 1) \wedge \alpha) \\ &= (1 \otimes \omega) \wedge \alpha + \beta \wedge \theta_1(\alpha) + (\omega \otimes 1) \wedge \theta_2(\alpha) \\ &= (m_{1\otimes\omega} + m_\beta \circ \theta_1 + m_{\omega\otimes 1} \circ \theta_2)(\alpha).\end{aligned}$$

and hence $\operatorname{im} m_{1\otimes\omega} \subset \operatorname{im} \theta_2 + \operatorname{im} m_{\omega\otimes 1} + \operatorname{im} m_\beta$. In fact, in Lem. 4.5 we will see that for general $\alpha \in \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n$ we have $\langle \theta_i(\alpha) : i \geq 0 \rangle \subset \langle \alpha \rangle + \Theta$.

However, for UOV, we would also like to include all the divided powers of $(\omega_i \otimes 1)$, $\beta_i$, and $(1 \otimes \omega_i)$ as they are all valid equations. More precisely, we want to study the ideal

$$J = \langle \theta_k(\omega_i \otimes 1)^{(j)} : 0 \leq k \leq 2, 1 \leq j \leq n, 1 \leq i \leq m \rangle$$

and the graded vector space $J + \Theta$.

**Lemma 4.5.** *Let $x \in \bigwedge^{s,t} \mathbb{F}_q^n$ with $s + t \equiv 0 \bmod 2$. Then, the ideals*

$$I \coloneqq \langle x^{(j)} : 1 \le j \le n \rangle$$
$$J \coloneqq \langle \theta_i(x)^{(j)} : 0 \le i \le s, 1 \le j \le n \rangle$$

*are equivalent modulo $\Theta$, i.e. $I + \Theta = J + \Theta$.*

*Proof.* As $\theta_0 = \mathrm{id}$, we have $I \subseteq J$, so we only need to show $J \subseteq I + \Theta$. Consider the largest ideal contained in $I + \Theta$, i.e. $S \coloneqq \{ \gamma \in \bigwedge^{(\bullet,\bullet)} \mathbb{F}_q^n \ : \ \langle \gamma \rangle \subseteq I + \Theta \}$. It suffices to place every generator $\theta_i(x)^{(j)}$ of $J$ in $S$. Note that $S$ is indeed an ideal and that $x^{(j)} \in S$ for every $j$.

We can show that $S$ is closed under every $\theta_k$ by induction. The case $k = 0$ being $\theta_0 = \mathrm{id}$. For $\gamma \in S$ and any $\alpha$ the Leibniz rule gives

$$\theta_k(\gamma) \wedge \alpha = \theta_k(\gamma \wedge \alpha) + \sum_{0 \le l < k} \theta_l(\gamma) \wedge \theta_{k-l}(\alpha),$$

whose first term lies in $\operatorname{im} \theta_k \subseteq \Theta$ and whose remaining terms lie in $I + \Theta$ because $\theta_l(\gamma) \in S$ for $l < k$. In particular every $\theta_i(x^{(j)})$ lies in $S$, and so does the ideal $\mathcal{T}$ they generate.

This ideal $\mathcal{T}$ is closed under divided squares. Elements of even total degree commute, so for $\mu, \nu$ of even total degree Lem. 3.2 gives the integral identities

$$(\mu \wedge \nu)^{(2)} = \tfrac{1}{2}(\mu \wedge \mu) \wedge (\nu \wedge \nu) = 2\, \mu^{(2)} \wedge \nu^{(2)}, \quad \left(x^{(j)}\right)^{(2)} = \tfrac{1}{2}\binom{2j}{j} x^{(2j)} = \binom{2j-1}{j-1} x^{(2j)},$$

of which the first vanishes in characteristic 2. Applying Lem. 4.4 to $x^{(j)}$ with $k = 2i$ and substituting the second yields, for every $i \ge 1$, the case $i = 0$ being the second identity itself,

$$\left(\theta_i(x^{(j)})\right)^{(2)} = \binom{2j-1}{j-1} \theta_{2i}\left(x^{(2j)}\right) + \sum_{0 \le l < i} \theta_l(x^{(j)}) \wedge \theta_{2i-l}(x^{(j)}) \ \in \ \mathcal{T},$$

a generator plus products of generators. Any bihomogeneous element in $\mathcal{T}$ of even total degree is a sum $\sum_r g_r \wedge \alpha_r$ of generators times bihomogeneous factors, all of even total degree as $s + t$ is even. Expanding its square using the additive identity of Lem. 3.2 leaves the pairwise products, which lie in $\mathcal{T}$, together with the $(g_r \wedge \alpha_r)^{(2)}$, which vanish by the first identity unless $\alpha_r$ is a scalar $c$, in which case they equal $c^2 g_r^{(2)} \in \mathcal{T}$.

Since $\theta_i(x) = \theta_i(x^{(1)})$ is a generator, iterating divided squares gives $\theta_i(x)^{(2^r)} \in \mathcal{T}$ by Lem. 3.4, and writing $j = \sum_r 2^{j_r}$ gives $\theta_i(x)^{(j)} = \bigwedge_r \theta_i(x)^{(2^{j_r})} \in \mathcal{T} \subseteq S$ by Lem. 3.2 and Kummer's theorem. Hence $J \subseteq I + \Theta$.

### 4.3 Rank analysis

The prior section told us that the equations on $\bigwedge^{\bullet,\bullet} \mathbb{F}_q^n$ from a UOV system are spanned by $I + \Theta$, where

$$I = \langle (\omega_i \otimes 1)^{(2^j)} : 1 \le i \le m, 0 \le j \le \log_2 n \rangle.$$

From these equations we can build a matrix which we call a Schur–Macaulay matrix

$$M_{a,b} : \bigoplus_{\substack{1\le i\le m\\ 1\le j\le \log_2 n}} \bigwedge^{a-2^j,\, b} \mathbb{F}_q^n \;\oplus\; \bigoplus_{0\le j\le \log_2 b} \bigwedge^{a+2^j,\, b-2^j} \mathbb{F}_q^n \longrightarrow \bigwedge^{a,b} \mathbb{F}_q^n$$

As always with Macaulay matrices, we are interested in the right nullity. This can be exactly computed from the bivariate Hilbert series of the bigraded vector space $\bigwedge^{\bullet,\bullet} \mathbb{F}_q^n/(I+\Theta) = L_{(\bullet,\bullet)}\mathbb{F}_q^n/I$. Before we conjecture a Hilbert series, we need to understand how to apply truncation.

**Lemma 4.6.** *If $(I+\Theta)_{a,b} = \bigwedge^{a,b} \mathbb{F}_q^n$, then $(I+\Theta)_{a,b+1} = \bigwedge^{a,b+1} \mathbb{F}_q^n$. Additionally, if $b = 0$ then $(I+\Theta)_{a+1,0} = \bigwedge^{a+1,0} \mathbb{F}_q^n$.*

*Proof.* For $b = 0$ we have $(I+\Theta)_{a,0} = I_a = \bigwedge^a \mathbb{F}_q^n$. Since $I$ is an ideal, $I_{a+1} = \bigwedge^{a+1} \mathbb{F}_q^n$. Now let $b \ge 0$ and let $\alpha \in (I+\Theta)_{a,b}$ with $\alpha = y + \sum \theta_i(z_i)$ with $y \in I_{a,b}$. In that case, let $x \in \bigwedge^{0,1} \mathbb{F}_q^n$, so that $\theta_i(x) = 0$ for $i \ge 1$, we obtain

$$\begin{aligned} x \cdot \alpha &= xy + \sum_i x \cdot \theta_i(z_i) \\ &= xy + \sum_i \theta_i(xz_i) - \sum_{j<i} \theta_{i-j}(x)\theta_j(z_i) \\ &= xy + \sum_i \theta_i(xz_i) \\ &\cong 0 \qquad \mod I + \Theta. \end{aligned}$$

In other words, $x \cdot \alpha \in I + \Theta$ and thus

$$\bigwedge^{a,b+1} \mathbb{F}_q^n = \bigwedge^{0,1} \mathbb{F}_q^n \cdot \bigwedge^{a,b} \mathbb{F}_q^n = \bigwedge^{0,1} \mathbb{F}_q^n \cdot (I+\Theta)_{a,b} \subset (I+\Theta)_{a,b+1}.$$

This gives us the following truncation operator on Laurent series

**Definition 4.7.** *For a formal Laurent series $f = \sum_{(a,b)\in\mathbb{Z}^2} f_{a,b}\, t^a s^b$ in $t, s$ with integer coefficients we write $[f]_+$ for the series supported on $\mathbb{N}^k$ with coefficients*

$$[f]_+[t^a s^b] = \begin{cases} f_{a,b} & \text{if } f_{a',0} > 0 \text{ for all } 0 \le a' \le a \text{ and } f_{a,b'} > 0 \text{ for all } 0 \le b' \le b, \\ 0 & \text{otherwise,} \end{cases}$$

We conjecture the following Hilbert series.

*Conjecture 4.8.* Let $\omega_1, \dots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ be random alternating 2-forms and denote

$$I = \langle (\omega_i \otimes 1)^{(2^j)} : 1 \le i \le m, 0 \le j \le \log_2 n \rangle \subset \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n.$$

With high probability the Hilbert series of $L_{(\bullet,\bullet)}\mathbb{F}_q^n/I$ is given by

$$\mathcal{H}_{L_{(\bullet,\bullet)}\mathbb{F}_q^n/I}(t,s) = [(1+t)^n(1+s)^n(1-t^2)^m(1-ts)^m(1-s^2)^m(1-t^{-1}s)]_+.$$

*Remark 4.9.* This Hilbert series might look surprising, we have just demonstrated that $(\omega_i \otimes 1)^{(2^j)}$ generate all equations and yet $\beta_i^{(2^j)}$ and $(1 \otimes \omega_i)^{(2^j)}$ seem to contribute factors to the Hilbert series. By Lem. 4.5 this is no contradiction, as modulo $\Theta$ the towers of $\beta_i$ and $1 \otimes \omega_i$ lie in the ideal generated by those of $\omega_i \otimes 1$, and the series counts all three. Each divided power tower contributes a factor $(1-u^d)$, as a single generator of degree $d$ in a semi-regular sequence would. However, as the $\theta_i$ are not multiplication maps, we were not able to make this precise, and the usual semi-regularity arguments do not apply. Sect. A explains which factors of the series are exact and where the argument breaks down.

Since we were not able to reduce the Hilbert series conjecture to more elementary assumptions, we tested the Hilbert series extensively. Tab. 3 shows all of our 820 tested parameters. In these tests we excluded the parameters for which the expected number of oil spaces of dimension $a$ is at least 1. Out of all tests, there is one instance that fails consistently, $n = 5, m = 8, a = 2, b = 1$, which predicts 0 and is experimentally 1.

| $(a, b)$ | $(2,1)$ | $(2,2)$ | $(3,1)$ | $(3,2)$ | $(3,3)$ | $(4,1)$ |
|---|---|---|---|---|---|---|
| $n$ | $\leq 19$ | $\leq 15$ | $\leq 18$ | $\leq 11$ | $\leq 9$ | $\leq 14$ |

**Table 3.** An overview of all 820 tested parameters over $\mathbb{F}_{256}$ of the Hilbert series given in Conj. 4.8. An entry $\leq 19$ means that all relevant values of $m$ and $n \leq 19$ were tested for that specific $(a, b)$. Only one parameter set, $n = 5, m = 8, a = 2, b = 1$, failed the prediction.

### 4.4 The UOV system

For UOV, we know that the forms $\omega_1, \ldots, \omega_m$ must admit a solution and therefore we expect the following rank of $M$ to be given by

$$\dim \ker M_{a,b}^T = \max(\mathcal{H}[t^a s^b], \dim \bigwedge^{a,b} O).$$

This means that unless $a, b \geq \dim O$, we will have multiple kernel vectors. As we saw in Lem. 4.2 this does not pose a problem and finding any such kernel element will lead us to recover at least one oil vector. Thus, to make sure we find a unique kernel element, we can remove $\dim \bigwedge^{a,b} O - 1$ random columns and still succeed.

However, given this redundancy, we might be able to do better. Recall that in most UOV attacks we project the $(v, o, m)$-UOV problem to a $(v, o', m)$-UOV problem with $o' \leq o$ as low as possible so that the attack still succeeds. We can do the same here to make sure that $a = \dim O$, but we can even take it a step further.

Let $H_i = \langle \mathbf{e}_1, \ldots, \mathbf{e}_i \rangle_{\mathbb{F}_q}$ be the subspace with support on the first $i$ coordinates. Then $\dim(H_i \cap O) \geq i+o-n$ which reaches equality with high probability. This means that we can instead search for the subspace

$$\bigwedge^a (H_{n-o+a} \cap O) \otimes \bigwedge^b (H_{n-o+b} \cap O) \subset \bigwedge^{a,b} O$$

which now has dimension $\geq 1$ with equality with high probability again. Effectively, this means that we can reduce the column support of our Macaulay matrices to

$$\bigwedge^a \mathbb{F}_q^{n-o+a} \otimes \bigwedge^b \mathbb{F}_q^{n-o+b}.$$

We conjecture that this influences the Hilbert series accordingly.

*Conjecture 4.10.* Let $\omega_1, \ldots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ be random alternating 2-forms and denote $I$ as before. Let $n \geq n_1 \geq n_2$ and denote $H = \langle \mathbf{e}_{n_1+1} \otimes 1, \ldots, \mathbf{e}_n \otimes 1, 1 \otimes \mathbf{e}_{n_2+1}, \ldots, 1 \otimes \mathbf{e}_n \rangle$. With high probability the Hilbert series of $A = \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n / (\Theta + I + H)$ is given by

$$\mathcal{H}_A(t,s) = [(1+t)^{n_1}(1+s)^{n_2}(1-t^2)^m(1-ts)^m(1-s^2)^m(1-t^{-1}s)]_+.$$

The two-column shapes of Tab. 6, 57 parameter sets with $n_1 = n$ and $n_2 = n - a + b$, all agree with this conjecture.

## 5 Schur module attack

The attacks of the previous sections take place inside the single exterior power $\bigwedge^a \mathbb{F}_q^n$ or double exterior power $\bigwedge^{a,b} \mathbb{F}_q^n$. This already extended the applicability of the attack. Using several exterior powers at once gives us even more room, but at the price of a much larger ambient space. The Schur modules which we introduce in the coming subsection make this worthwhile. They are quotients of the tensor product and passing to the quotient amounts to adjoining their defining relations as columns to the Macaulay matrix. The motivation is that imposing the UOV restrictions on such a quotient leaves a smaller space to annihilate than the full tensor product, so that we may hope for smaller degrees and above all, for an attack where none applied before.

### 5.1 Schur modules

We begin by introducing Schur modules following the conventions of [27]. Following this we will extend the attack using partitions of two columns to give a Hilbert series for partitions of arbitrary size.

A *partition* is a non-increasing sequence $\lambda = (\lambda_1 \geq \cdots \geq \lambda_k)$ of positive integers, drawn as a diagram with $\lambda_j$ boxes in its $j$-th column. To every partition $\lambda$ and positive integer $n$ we attach a vector space $L_\lambda \mathbb{F}_q^n$, the *Schur module*

*of shape* $\lambda$, obtained from the tensor product $\bigwedge^{\lambda_1}\mathbb{F}_q^n \otimes \cdots \otimes \bigwedge^{\lambda_k}\mathbb{F}_q^n$ of the exterior powers of its columns by imposing certain relations. We will extend our superscript notation to multigraded exterior algebras so that

$$\bigwedge^{\lambda}\mathbb{F}_q^n = \bigwedge^{\lambda_1,\ldots,\lambda_k}\mathbb{F}_q^n := \bigwedge^{\lambda_1}\mathbb{F}_q^n \otimes \cdots \otimes \bigwedge^{\lambda_k}\mathbb{F}_q^n.$$

For a single column there are no relations to impose, and

$$L_{(a)}\mathbb{F}_q^n = \bigwedge^{a}\mathbb{F}_q^n.$$

This is exactly the space in which the exterior algebra attack operates.

The relations are built from the multiplication and comultiplication map. The latter is defined as the exterior power of the diagonal $\mathbb{F}_q^n \to \mathbb{F}_q^n \oplus \mathbb{F}_q^n$,

$$\Delta : \bigwedge \mathbb{F}_q^n \to \bigwedge(\mathbb{F}_q^n \oplus \mathbb{F}_q^n) \cong \bigwedge \mathbb{F}_q^n \otimes \bigwedge \mathbb{F}_q^n,$$

whose component $\bigwedge^{a+b}\mathbb{F}_q^n \to \bigwedge^{a,b}\mathbb{F}_q^n$ is given on basis vectors by

$$\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_{a+b} \mapsto \sum_{\substack{|I|=a,\ |J|=b \\ I \sqcup J = [a+b]}} \pm\, \mathbf{x}_{i_1} \wedge \cdots \wedge \mathbf{x}_{i_a} \otimes \mathbf{x}_{j_1} \wedge \cdots \wedge \mathbf{x}_{j_b},$$

extended linearly, where the sign is irrelevant in characteristic 2 but otherwise given by the permutation that shuffles $(1,\ldots,a+b)$ to $(i_1,\ldots,i_a,j_1,\ldots,j_b)$.

**Two columns.** Let $\lambda = (a,b)$ with $a \geq b$. Combining comultiplication with the multiplication of the exterior algebra gives us the relation maps.

$$\vartheta_i : \bigwedge^{a+i,b-i}\mathbb{F}_q^n \xrightarrow{\Delta\otimes 1} \bigwedge^{a,i,b-i}\mathbb{F}_q^n \xrightarrow{\mathrm{id}\otimes m} \bigwedge^{a,b}\mathbb{F}_q^n. \tag{3}$$

These are exactly the $\theta_i$ maps that we saw in Sect. 4. So our earlier definition of $L_{(a,b)}$ agrees with this more general definition.

**More columns.** For a partition with $k$ columns one proceeds in the same way. We quotient $\bigwedge^{\lambda_1,\ldots,\lambda_k}\mathbb{F}_q^n$ by the images of the transfer maps applied to each pair of adjacent columns. In other words, let

$$\Theta_i^{\lambda} = \bigwedge^{\lambda_1,\ldots,\lambda_{i-1}}\mathbb{F}_q^n \otimes \Theta^{\lambda_i,\lambda_{i+1}} \otimes \bigwedge^{\lambda_{i+2},\ldots,\lambda_k}\mathbb{F}_q^n$$

and define

$$\Theta^{\lambda} = \sum_{i=1}^{k-1}\Theta_i^{\lambda}.$$

Then we define the Schur functor

$$L_{\lambda}\mathbb{F}_q^n = \bigwedge^{\lambda_1,\ldots,\lambda_k}\mathbb{F}_q^n / \Theta^{\lambda}.$$

Restricting to adjacent columns loses nothing. For $p < q$ and $\ell \geq 0$ write

$$\theta_\ell^{pq} : \bigwedge^{\lambda_1, \ldots, \lambda_p+\ell, \ldots, \lambda_q-\ell, \ldots, \lambda_k} \mathbb{F}_q^n \longrightarrow \bigwedge^{\lambda_1, \ldots, \lambda_k} \mathbb{F}_q^n$$

for the map that applies $\theta_\ell$ of Sect. 4 to the $p$-th and $q$-th tensor factors and the identity to all others, so that $\Theta_i^\lambda = \sum_{\ell \geq 1} \operatorname{im} \theta_\ell^{i,i+1}$.

**Lemma 5.1.** *For all $p < q$ and $\ell \geq 1$ we have $\operatorname{im} \theta_\ell^{pq} \subseteq \Theta^\lambda$.*

*Proof.* By induction on $q-p$ it suffices to treat three columns. Just as in Def. 4.1 we regard $\bigwedge^{\bullet,\bullet,\bullet} \mathbb{F}_q^n = \bigwedge(\mathbb{F}_q^n \oplus \mathbb{F}_q^n \oplus \mathbb{F}_q^n)$ as an algebra and write $\mathbf{e}_I \otimes \mathbf{e}_J \otimes \mathbf{e}_L = \alpha\beta\gamma$ with $\alpha = \mathbf{e}_I \otimes 1 \otimes 1$, $\beta = 1 \otimes \mathbf{e}_J \otimes 1$ and $\gamma = 1 \otimes 1 \otimes \mathbf{e}_L$. Each $\theta_k^{pq}$ satisfies the Leibniz rule of Sect. 4, and for $k \geq 1$ it vanishes on factors that do not involve the $p$-th slot, since there is nothing to move. Two applications of the Leibniz rule therefore give

$$\theta_k^{23}\theta_k^{12}(\alpha\beta\gamma) = \theta_k^{23}\big(\theta_k^{12}(\alpha)\,\beta\,\gamma\big) = \sum_{r=0}^{k} \theta_r^{23}\theta_k^{12}(\alpha) \cdot \theta_{k-r}^{23}(\beta) \cdot \gamma.$$

By definition $\theta_k^{12}(\alpha) = \sum_{K \subseteq I,\, |K|=k} \mathbf{e}_{I\setminus K} \otimes \mathbf{e}_K \otimes 1$, and $\theta_r^{23}$ then moves an $r$-subset $K_1$ of $K$ onto the third slot. Hence $\theta_r^{23}\theta_k^{12}(\alpha)$ is the sum of $\mathbf{e}_{I\setminus K} \otimes \mathbf{e}_{K\setminus K_1} \otimes \mathbf{e}_{K_1}$ over all pairs $K_1 \subseteq K \subseteq I$ with $|K_1| = r$ and $|K| = k$, which is also what one obtains by first moving the $(k-r)$-subset $K \setminus K_1$ to the second slot and then $K_1$ to the third, i.e. $\theta_r^{23}\theta_k^{12}(\alpha) = \theta_r^{13}\theta_{k-r}^{12}(\alpha)$. Applying the Leibniz rule to the right-hand side in the same way, we obtain on all of $\bigwedge^{\bullet,\bullet,\bullet} \mathbb{F}_q^n$

$$\theta_k^{23}\,\theta_k^{12} = \sum_{r=0}^{k} \theta_r^{13}\,\theta_{k-r}^{12}\,\theta_{k-r}^{23}. \tag{4}$$

The term $r = k$ is $\theta_k^{13}$. The left-hand side has image in $\operatorname{im}\theta_k^{23}$, the term $r = 0$ has image in $\operatorname{im}\theta_k^{12}$, and for $0 < r < k$ the terms have image in $\operatorname{im}\theta_r^{13} \subseteq \Theta^\lambda$ by induction on $k$. Hence $\operatorname{im}\theta_k^{13} \subseteq \Theta^\lambda$.

*Example 5.2.* At the opposite extreme from a single column stands a single row, $\lambda = (1, \ldots, 1)$ with $a$ parts, where the construction returns

$$L_{(1^a)}\mathbb{F}_q^n = \operatorname{Sym}^a \mathbb{F}_q^n,$$

the space of degree-$a$ forms in which an ordinary Macaulay matrix operates.

*Remark 5.3.* This example emphasizes the reason to study Schur modules as ambient space for Macaulay matrix computations. Both the symmetric and the exterior algebra have been used in cryptanalysis but both have their advantages and disadvantages. A general $L_\lambda$ interpolates between the two.

**Dimensions.** The quotient $L_\lambda \mathbb{F}_q^n$ is substantially smaller than the tensor product it comes from. It has a basis indexed by semistandard Young tableaux of shape $\lambda$ with entries in $[n]$ as shown in [27, Section 2.1]. Its dimension is then given by the hook content formula for counting semistandard Young tableaux [14, Section 4.3][5]

$$\dim L_\lambda \mathbb{F}_q^n = \prod_{(i,j)\in\lambda} \frac{n+i-j}{h_{ij}},$$

where $h_{ij}$ denotes the hook length of the box $(i,j)$, i.e. the number of boxes to the right and below. Alternatively, fix $k \geq 1$ we can use the following Laurent series [14] for determining the dimension

$$\mathcal{S}(\mathbf{t}) = \prod_{i=1}^{k} (1+t_i)^n \cdot \prod_{1\leq i<j\leq k} \left(1 - t_i^{-1} t_j\right).$$

Now, the dimension is given by

$$\dim L_\lambda \mathbb{F}_q^n = \mathcal{S}[\mathbf{t}^\lambda]$$

the coefficient of $t_1^{\lambda_1} \cdots t_k^{\lambda_k}$.

### 5.2 UOV relations

As one might expect, we obtain similar lemmas and results as before, now with transfer maps between any two of the $k$ columns; by Lem. 5.1 the adjacent ones already generate all of them.

We extend the definition of truncation recursively.

**Definition 5.4.** *For a formal Laurent series $f = \sum_{\mathbf{a}\in\mathbb{Z}^k} f_{\mathbf{a}}\, \mathbf{t}^{\mathbf{a}}$ in $t_1, \ldots, t_k$ with integer coefficients we write $[f]_+$ for the series supported on $\mathbb{N}^k$ with coefficients*

$$[f]_+[\mathbf{t}^{\mathbf{a}}] = \begin{cases} f_{\mathbf{a}} & \text{if } f_{\bar{\mathbf{a}},a'_k} > 0 \text{ for all } 0 \leq a'_k \leq a_k \text{ and } [\bar{f}]_+[\bar{\mathbf{t}}^{\bar{\mathbf{a}}}] > 0, \\ 0 & \text{otherwise.} \end{cases}$$

*Here $\bar{\mathbf{t}} = (t_1, \ldots, t_{k-1})$, $\bar{\mathbf{a}} = (a_1, \ldots, a_{k-1})$, $\bar{f}(\bar{\mathbf{t}}) = f(\bar{\mathbf{t}}, 0)$, and truncation on a univariate power series is the usual one.*

This now agrees with our definition of $[\cdot]_+$ for both the univariate and bivariate power series. This yields the following conjecture on the multivariate Hilbert series

$$\mathcal{H}_{L_\lambda/I}(\mathbf{t}) = \prod_{i\leq j}(1-t_it_j)^m \cdot \prod_i (1+t_i)^n \cdot \prod_{i<j}(1-t_i^{-1}t_j) \tag{5}$$

We tested this series again for multiple different parameter sets. Out of these 94 had a partition of length at least 3. We show these new tests in Tab. 4 and all mispredictions in Tab. 5.

| $\lambda$ | $(2,1,1)$ | $(2,2,1)$ | $(2,2,2)$ | $(3,1,1)$ | $(2,1,1,1)$ |
|---|---|---|---|---|---|
| $n$ | $\leq 12$ | $\leq 8$ | $\leq 7$ | $\leq 9$ | $\leq 7$ |

**Table 4.** An overview of all 94 tested parameters over $\mathbb{F}_{256}$ of the Hilbert series given in Eq. (5). An entry $\leq 12$ means that all relevant values of $m$ and $n \leq 12$ were tested for that specific $\lambda$. The anomalies are shown in Tab. 5.

| $n$ | $m$ | $a$ | experimental | prediction |
|---|---|---|---|---|
| 5 | 8 | $(2,1)$ | 1 | 0 |
| 5 | 7 | $(2,1,1)$ | 1 | 0 |
| 6 | 10 | $(2,1,1)$ | 1 | 0 |
| 6 | 9 | $(2,2,1,1)$ | 1 | 0 |
| 7 | 12 | $(2,2,1)$ | 1 | 0 |

**Table 5.** Mispredictions of Eq. (5).

Likewise, for the projected variant we obtain

$$\mathcal{H}_{L_\lambda/I}(\mathbf{t}) = \prod_{i\leq j}(1-t_it_j)^m \cdot \prod_i (1+t_i)^{n_i} \cdot \prod_{i<j}(1-t_i^{-1}t_j)$$

We tested this Hilbert series for the projection used in the attack, $n_i = n - \lambda_1 + \lambda_i$, on all shapes with $\lambda_1 \geq 2$ and $n \leq 9$ whose matrices fit into our server's memory, 121 parameter sets in total. Tab. 6 lists the shapes with at least two columns. The prediction is correct in all but one cases, which is the same edge-case in which the exceptions of Tab. 5 occur.

| columns | shapes $\lambda$ | # instances | $n$ | $m$ | correct |
|---|---|---|---|---|---|
| 2 | $(2,1),(2,2),(3,1),(3,2)$ | 57 | 3–9 | 3–26 | 57/57 |
| 3 | $(2,1,1),(2,2,1),(2,2,2),(3,1,1)$ | 33 | 5–9 | 7–21 | 32/33 |
| 4 | $(2,1,1,1)$ | 6 | 6–8 | 9–15 | 6/6 |
| total | | 121 | 3–9 | 1–26 | 120/121 |

**Table 6.** Experiments over $\mathbb{F}_{256}$ for the projected Hilbert series of Eq. (5) with $n_i = n - \lambda_1 + \lambda_i$. The only misprediction is $n = 6$, $m = 9$, $\lambda = (2,2,1)$, where the measured dimension is 1 and the series predicts 0.

### 5.3 Odd characteristic

The construction of Schur modules does not depend on the characteristic, so the attack applies in odd characteristic $p$ as well, with the following changes.

[5] Note that there are some conflicting conventions in partition orientation.

First, the polar forms are no longer alternating. Instead of $\omega_i \in \bigwedge^2 \mathbb{F}_q^n$ we have symmetric bilinear forms $\beta_i \in \bigwedge^{1,1} \mathbb{F}_q^n$, so at least two columns are needed. These $\beta_i$ play the role of the $\beta_i$ of Sect. 4, and as there $\theta_j \beta_i = 0$ for all $i$ and all $j \geq 1$, since $\theta_j$ moves the two factors of $\beta_i$ into one slot, where they cancel by symmetry.

Second, in characteristic $p$ we have vanishing of $\beta^p = \beta \wedge \cdots \wedge \beta = \mathbf{0}$ for any $\beta \in \bigwedge^{\bullet,\ldots,\bullet} \mathbb{F}_q^n$. Therefore, we need to also consider the divided powers $\beta_i^{(p^j)}$. Furthermore, in this case, we obtain

$$\Theta^{a,b} = \sum_{j \geq 0} \operatorname{im} \theta_{p^j}.$$

Taking all of these together, we conjecture the following series for the Schur–Macaulay matrix on $\beta_1, \ldots, \beta_m$ of shape $\lambda$.

*Conjecture 5.5.* Let $I \subset \bigwedge^{\lambda_1,\ldots,\lambda_k} \mathbb{F}_q^n$ be the ideal generated by the divided powers $\beta_i^{(p^j)}$, $1 \leq i \leq m$, $j \geq 0$, of the $\beta_i$ placed in the first two columns. With high probability we have

$$\mathcal{H}_{L_\lambda/I}(\mathbf{t}) = \prod_{i<j} (1 - t_i t_j)^m \cdot \prod_i (1 + t_i)^n \cdot \prod_{i<j} (1 - t_i^{-1} t_j). \tag{6}$$

We tested this series experimentally for 215 parameter sets with $q = 31$ of which 176 were correctly predicted. The tested parameter ranges are summarized in Tab. 7 All 39 mispredictions satisfy $m < v$, where $v = n - \lambda_1$. These can be explained, just as in the wedge attack, by the elements

$$\alpha\beta_1 \cdots \beta_m \in \bigwedge^v \mathbb{F}_q^{v+\lambda_1} \otimes \cdots \otimes \bigwedge^v \mathbb{F}_q^{v+\lambda_k} \cong \bigwedge^{\lambda_1} \mathbb{F}_q^n \otimes \cdots \otimes \bigwedge^{\lambda_k} \mathbb{F}_q^{n-\lambda_1+\lambda_k}.$$

| $\lambda$ | $(2,1)$ | $(2,2)$ | $(3,1)$ | $(4,1)$ | $(5,1)$ |
|---|---|---|---|---|---|
| $n$ | $\leq 9$ | $\leq 8$ | $\leq 9$ | $\leq 8$ | $\leq 9$ |

| $\lambda$ | $(2,1,1)$ | $(3,1,1)$ | $(2,1,1,1)$ | $(3,1,1,1)$ |
|---|---|---|---|---|
| $n$ | $\leq 7$ | $\leq 6$ | $\leq 5$ | $\leq 5$ |

**Table 7.** An overview of all 215 tested parameters over $\mathbb{F}_{31}$ of the Hilbert series given in Eq. (6). An entry $\leq 9$ means that all relevant values of $m$ and $n \leq 9$ were tested for that specific $\lambda$. All mispredictions satisfy $m \leq v$.

*Remark 5.6.* Note that a specific subclass of these Schur–Macaulay matrices appeared in [24]. There, the author looked at a system of degree 2 in the Plücker

coordinates and included the Plücker relations. Since the Plücker relations are exactly given by

$$\theta_i : \bigwedge^{o'+i,o'-i} \mathbb{F}_q^n \to \bigwedge^{o',o'} \mathbb{F}_q^n,$$

this corresponds exactly to the Schur attack with $\lambda = (o', o')$.

*Remark 5.7.* Note that this is a different generalization than the attack proposed in [19]. A dimension analysis of the matrices in both attacks shows us that the attacks cannot be equivalent. Still, it would be interesting to see what the relation between those attacks is.

## 6 Results

Now that we have a Hilbert series for determining the nullity of these new Schur–Macaulay matrices we can incorporate them in an attack.

**Definition 6.1.** *Let $\omega_1, \ldots, \omega_m \in \bigwedge^2 \mathbb{F}_q^n$ (resp. $\beta_1, \ldots, \beta_m \in \bigwedge^{1,1} \mathbb{F}_q^n$). We call a partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ with $k \geq 1$ (resp. $k \geq 2$) and $n \geq \lambda_1 \geq \cdots \geq \lambda_k \geq 1$* admissible *if*

$$\dim \operatorname{coker} M_\lambda \leq 1$$

*where $M_\lambda$ is the Schur–Macaulay matrix on $\omega_1, \ldots, \omega_m$ (resp. $\beta_1, \ldots, \beta_m$).*

With this definition, each admissible $\lambda$ gives us an attack against UOV in even (resp. odd) characteristic. It remains to compute the complexity for each $\lambda$ and determine the cheapest admissible $\lambda$.

### 6.1 Cost analysis

The most expensive step in the attack is the sparse linear algebra step. To compute the oil space, we need to find the unique cokernel element of the maps $m_{\omega_i^{(2^j)}} \otimes \mathrm{id}$ and $\mathrm{id} \otimes \theta_{2^j}^{i,i+1} \otimes \mathrm{id}$. To compute this, we write $M_\lambda$ as the Macaulay matrix of these maps with

$$\left( m \cdot \prod_{i'=2}^{k} \binom{v+\lambda_{i'}}{\lambda_{i'}} \cdot \sum_{j=1}^{\log_2 n} \binom{v+\lambda_1}{\lambda_1 - 2^j} \right) + \sum_{i=1}^{k-1} \sum_{j=0}^{\log_2 n} \binom{v+\lambda_i}{\lambda_i+2^j} \binom{v+\lambda_{i+1}}{\lambda_{i+1}-2^j} \cdot \prod_{\substack{i'=1 \\ i' \neq i, i+1}}^{k} \binom{v+\lambda_{i'}}{\lambda_{i'}}$$

rows and

$$\prod_i \binom{v+\lambda_i}{\lambda_i}$$

columns.

To do sparse linear algebra we will reduce $M_\lambda$ to a square matrix by removing random rows. Since the densities of the different types of rows differ we need to compute the average density of the matrix. We assume that the randomly reduced matrix has the same average density with high probability. To compute

| Type | Bounds | Number of rows | Density |
|---|---|---|---|
| $m_{\omega_i^{(2^{j-1})}} \otimes \mathrm{id}$ | $1 \leq j \leq \log_2 \lambda_1$ | $m\binom{v+\lambda_1}{\lambda_1-2^j}\prod_{i'>1}\binom{v+\lambda_{i'}}{\lambda_{i'}}$ | $\binom{v+2^j}{2^j}$ |
| $m_{\beta_i^{(p^j)}} \otimes \mathrm{id}$ | $0 \leq j \leq \log_p \lambda_2$ | $m\binom{v+\lambda_1}{\lambda_1-p^j}\binom{v+\lambda_2}{\lambda_2-p^j}\prod_{i'>2}\binom{v+\lambda_{i'}}{\lambda_{i'}}$ | $\binom{v+p^j}{p^j}^2$ |
| $\mathrm{id} \otimes \theta_{p^j}^{i,i+1} \otimes \mathrm{id}$ | $1 \leq i \leq k-1$<br>$0 \leq j \leq \log_p \lambda_{i+1}$ | $\binom{v+\lambda_i}{\lambda_i+p^j}\binom{v+\lambda_{i+1}}{\lambda_{i+1}-p^j}\prod_{i'\neq i,i+1}\binom{v+\lambda_{i'}}{\lambda_{i'}}$ | $\leq \binom{\lambda_i+p^j}{p^j}$ |

**Table 8.** Row distribution of $M_\lambda$. Note that the maps $m_\omega$ are only included in characteristic 2 and $m_\beta$ maps are only included in odd characteristic $p$. The density for $\theta$ does not include a correction for terms that vanish due to projection.

the average row density $\rho$ we compute the weighted average of densities provided in Tab. 8.

Finally, we can compute the oil space in time

$$3 \cdot \rho \cdot \prod_i \binom{v+\lambda_i}{\lambda_i}^2$$

field operations and

$$\mathcal{O}\left(\prod_i \binom{v+\lambda_i}{\lambda_i}\right)$$

peak memory. In line with [6, 7, 17, 26] we count one multiplication in $\mathbb{F}_q$ as $2(\log_2 q)^2 + \log_2 q$ bit operations, where $q$ is the size of the field over which the instance is defined. For the final cost of the attack, we minimize over admissible partitions $\lambda$.

*Remark 6.2.* As discussed in Remark 2.1, we do not analyse the cost of memory access and only report peak memory in field elements. We note, however, that the block-like structure of $m_\omega \otimes \mathrm{id}$ and $\mathrm{id} \otimes \theta \otimes \mathrm{id}$ might lead to more "local" operations than regular WXL.

*Remark 6.3.* Ideally, we would like to solve a system over $L_\lambda$ instead of $\bigwedge^\lambda \mathbb{F}_q^n$. This would significantly decrease the number of columns. Unfortunately, we did not find a way to achieve this without destroying sparsity. We leave it as an open problem to find a way to apply sparse linear algebra directly in $L_\lambda$. There is one class of exceptions, where we can already look at smaller matrices. If $\lambda_1 = \ldots = \lambda_k$, then $\mathrm{Sym}^k\left(\bigwedge^{\lambda_i} \mathbb{F}_q^n\right)$ is a quotient sitting between $\bigwedge^\lambda \mathbb{F}_q^n$ and $L_\lambda \mathbb{F}_q^n$ which is easy to construct due to symmetry. In the case that $\lambda_1 = \ldots = \lambda_k = 1$ this makes the column space equal to $\mathrm{Sym}^k \mathbb{F}_q^n \cong \mathbb{F}_q[x_1, \ldots, x_n]_k$ which make Schur–Macaulay matrices a strict generalization of Macaulay matrices. This can save a factor of up to $(k!)^2$ in time complexity which we leave for future research.

### 6.2 Schur attack

Finally, we are able to compute the cost of this attack against cryptographic schemes. It turns out that the true power of this attack is extending applicability

of the exterior algebra attack. This is most clear in Tab. 9 which shows the alternative parameter sets in the MAYO Round-2 specifications [6][6]. The table shows that time and memory grow quickly with the number of Schur components. Accordingly, the cheapest admissible $\lambda$ always had the fewest components, and every row of Tab. 9 with more than one component was out of reach of the wedge attack before.

For UOV, all parameter sets, including those induced by the intersection attack, are already affected by the exterior algebra attack. Therefore, there is no gain in increasing the number of Schur components for these parameter sets.

For SNOVA, we could consider a multi-homogeneous Schur attack. However, note that, in SNOVA vectors of two different oil space components are related through $2m$ bilinear equations while vectors in the same oil component are only related through $m$ polar forms. For this reason, we do not expect that multi-homogeneous Schur modules will improve the complexities in Tab. 2 and we chose not to pursue this further.

Finally, Tab. 10 gives the results for QR-UOV. Interestingly, we see that the Schur attack not only extends applicability but that unbalanced partitions improve complexity.

## 7 Conclusion and future work

Our results show that Schur–Macaulay matrices exploit the existence of a totally isotropic subspace beyond what the wedge attack does. It would be interesting to see how this framework applies to other problems where a hidden subspace is sought, such as MinRank or subcode equivalence. Furthermore, current algorithms for solving underdetermined MQ, such as Hashimoto's algorithm, rely on finding totally isotropic subspaces of subsets of the polynomial systems. Schur–Macaulay matrices might tip the trade-off in these algorithms as well.

That said, the XL literature is vast and there are likely more techniques that can be ported to Schur–Macaulay matrices. To do this, the gap between the Macaulay and Schur–Macaulay matrices as described by Remark 6.3 could be explored further. This might show what an FXL variant for Schur–Macaulay matrices looks like and yield better time–memory trade-offs, which would in turn make the cost of the attack far less sensitive to small changes of the parameters.

**Acknowledgements.** This research was partially supported by the Dutch government through the NWO grant OCNW.M.21.193 (ALPaQCa) and by the DFG (German Research Foundation) under the Walter Benjamin Programme.

**AI disclosure.** In preparing this paper, we used Claude Opus 5 to edit the text for flow, consistency, and typographical errors throughout and to compile the tables of experimental results from our databases. Our initial guess for the Hilbert

[6] We communicated these results to the MAYO team, leading them to raise parameters for one of their Round-3 parameter sets.

series failed for several choices of parameters. While discussing these counterexamples, Claude identified syzygies arising from divided powers and suggested a preliminary version of the Hilbert series in Conj. 4.8. In this discussion, we realized that we can include divided powers directly as relations in the wedge attack which led to the actual conjectured Hilbert series. The idea to consider Schur–Macaulay matrices is our own. The authors verified all results in the paper and take full responsibility for them.

## References


1. Thomas Aulbach, Fabio Campos, Juliane Krämer, Simona Samardjiska, and Marc Stöttinger. Separating oil and vinegar with a single trace: side-channel assisted kipnis-shamir attack on uov. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(3):221–245, 2023.
2. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 507–536, Cham, 2020. Springer International Publishing.
3. Magali Bardet and Alban Gilard. Computation of the Hilbert Series for the Support-Minors Modeling of the MinRank Problem, July 2025. arXiv:2502.12721.
4. Ward Beullens. Improved cryptanalysis of uov and rainbow. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 348–373. Springer, 2021.
5. Ward Beullens. Mayo: practical post-quantum signatures from oil-and-vinegar maps. In *International Conference on Selected Areas in Cryptography*, pages 355–376. Springer, 2021.
6. Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. MAYO specification document – round 2. Submission to the NIST call for additional post-quantum digital signature schemes, round 2, 2025.
7. 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 specification document – round 2. Submission to the NIST call for additional post-quantum digital signature schemes, round 2, 2025.
8. Maxime Bros, Thai Hung Le, Jacob Lichtinger, Brice Minaud, Ray Perlner, Daniel Smith-Tone, and Cristian Valenzuela. Exploiting SNOVA's Structure in the Wedge Product Attack, 2026. Publication info: A minor revision of an IACR publication in ASIACRYPT 2026.
9. Tung Chou and Ruben Niederhagen. A Practical Optimization for Wiedemann XL, 2026. Publication info: Preprint.
10. Don Coppersmith. Solving Homogeneous Linear Equations Over GF(2) via Block Wiedemann Algorithm. *Mathematics of Computation*, 62(205):333–350, 1994.
11. Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, pages 392–407, Berlin, Heidelberg, 2000. Springer.
12. Jintai Ding, Hao Guo, and Bo-Yin Yang. On Memory Effects in PWXL variants, 2026. Publication info: Preprint.

13. Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng. New Differential-Algebraic Attacks and Reparametrization of Rainbow. In Steven M. Bellovin, Rosario Gennaro, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security*, pages 242–257, Berlin, Heidelberg, 2008. Springer.
14. William Fulton. *Young Tableaux: With Applications to Representation Theory and Geometry*. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1996.
15. William Fulton and Joe Harris. *Representation Theory*, volume 129 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2004.
16. Hiroki Furue and Yasuhiko Ikematsu. Key Recovery Attacks on UOV Using $p^\ell$-truncated Polynomial Rings, 2026. Publication info: Published by the IACR in CRYPTO 2026.
17. Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi, Haruhisa Kosuge, Kimihiro Yamakoshi, Rika Akiyama, Shuhei Nakamura, Shingo Orihara, and Koha Kinjo. QR-UOV specification document – round 2. Submission to the NIST call for additional post-quantum digital signature schemes, round 2, 2025.
18. Yasuhiko Ikematsu and Hiroki Furue. Extending the applicability of algebraic key recovery attacks on the uov signature scheme. *Cryptology ePrint Archive*, 2026.
19. 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, *Public-Key Cryptography – PKC 2026*, pages 428–454, Cham, 2026. Springer Nature Switzerland.
20. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.
21. Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil and vinegar signature scheme. In *Annual international cryptology conference*, pages 257–266. Springer, 1998.
22. Shuhei Nakamura, Yusuke Tani, and Hiroki Furue. Lifting approach against the SNOVA scheme, 2024. Publication info: Preprint.
23. Pierre Pébereau. One vector to rule them all: Key recovery from one vector in uov schemes. In *International Conference on Post-Quantum Cryptography*, pages 92–108. Springer, 2024.
24. Lars Ran. Wedges, Oil, and Vinegar. In Joan Daemen and Emmanuel Thomé, editors, *Advances in Cryptology – EUROCRYPT 2026*, pages 363–388, Cham, 2026. Springer Nature Switzerland.
25. Po-En Tseng, Lih-Chung Wang, Peigen Li, and Yen-Liang Kuan. Investigating the Wedge Map on SNOVA, 2026. Publication info: Preprint.
26. Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Jan Adriaan Leegwater, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang. SNOVA specification document – round 2. Submission to the NIST call for additional post-quantum digital signature schemes, round 2, 2025.
27. Jerzy Weyman. *Cohomology of Vector Bundles and Syzygies*. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 2003.
28. D. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Transactions on Information Theory*, 32(1):54–62, January 1986.

## A Heuristics behind the Hilbert series

We do not have a proof of Conj. 4.8, nor a semi-regularity assumption which would imply it. In this appendix we explain which parts of the series are exact and why the natural attempt at a proof fails.

**The factors of the series.** The first two and the last factor of Conj. 4.8 are exact. Indeed, for $a \geq b$ the coefficient of $t^a s^b$ in $(1+t)^n(1+s)^n(1-t^{-1}s)$ equals

$$\binom{n}{a}\binom{n}{b} - \binom{n}{a+1}\binom{n}{b-1} = \dim \bigwedge^{a,b} \mathbb{F}_q^n - \dim \bigwedge^{a+1,b-1} \mathbb{F}_q^n = \dim L_{(a,b)}\mathbb{F}_q^n,$$

the last equality because $\Theta^{a,b}$ has the dimension of $\bigwedge^{a+1,b-1} \mathbb{F}_q^n$. Hence $(1+t)^n(1+s)^n(1-t^{-1}s)$, restricted to exponents with $a \geq b$, is the Hilbert series of $L_{(\bullet,\bullet)}\mathbb{F}_q^n = \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n/\Theta$, and the conjecture concerns only the effect of the UOV equations on this quotient.

Recall that the ideal $I$ of Conj. 4.8 is generated by the divided-power towers $(\omega_i \otimes 1)^{(2^j)}$ only, whereas the series has a factor for each of $\omega_i \otimes 1$, $\beta_i = \theta_1(\omega_i \otimes 1)$ and $1 \otimes \omega_i = \theta_2(\omega_i \otimes 1)$. This is explained by Lem. 4.5. Namely, modulo $\Theta$ the ideal $I$ coincides with the ideal $J$ generated by all three towers, i.e.

$$L_{(\bullet,\bullet)}\mathbb{F}_q^n/I = \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n/(J+\Theta),$$

and the middle factors count the $3m$ towers of $J$.

To see why a tower contributes a factor $(1-u^d)$, let $x$ have even total degree $d$. By Lem. 3.4 the subalgebra generated by $x, x^{(2)}, x^{(4)}, \ldots$ is spanned by the squarefree monomials in the $x^{(2^j)}$, which square to zero and have degrees $d, 2d, 4d, \ldots$. If these monomials are linearly independent its Hilbert series agrees in all degrees $\leq n$ with

$$\prod_{j\geq 0}(1+u^{d2^j}) = \frac{1}{1-u^d},$$

which is also the Hilbert series of a polynomial ring in one variable of degree $d$. Conj. 3.6 thus states that the $m$ towers behave like $m$ quadrics in a semi-regular sequence, and Conj. 4.8 states the same for the $3m$ towers of $J$ in degrees $t^2$, $ts$ and $s^2$, together with the transfer relations. Without divided powers $\omega_i$ is a single square-zero element with Hilbert series $1+u^2$, and $m$ of them give the factor $(1+t^2)^{-m}$ found in [18].

**Relations on $L_{(a,b)}$** Intuitively, we would like to prove this by working on the space $L_{(a,b)}\mathbb{F}_q^n$ and showing that the multiplication maps have full rank. However, our multiplication maps do not nicely descend to it. For example, let $x \in \bigwedge^{s,t} \mathbb{F}_q^n$, then the map

$$m_x : \bigwedge^{a-s,b-t} \mathbb{F}_q^n \to L_{(a,b)}\mathbb{F}_q^n$$

does not have $\Theta^{a-s,b-t}$ in its kernel. Hence we do not get a map

$$L_{(a-s,b-t)}\mathbb{F}_q^n \xrightarrow{?} L_{(a,b)}\mathbb{F}_q^n.$$

The obstruction to $\Theta$ lying in the kernel is that

$$x \wedge \theta_i(\alpha) = \theta_i(x \wedge \alpha) + \sum_{j<i} \theta_{i-j}(x) \wedge \theta_j(\alpha) \equiv \sum_{j<i} \theta_{i-j}(x) \wedge \theta_j(\alpha) \mod \Theta.$$

Therefore, we can define a multiplication map for $x$ if we quotient out all $\theta_i(x)$. Let $I \subset \bigwedge^{\bullet,\bullet} \mathbb{F}_q^n$ be an ideal so that $\theta_i(x) \in I$ for all $i > 0$. Then, we get a well-defined map

$$m_x : (L_{(a-s,b-t)}\mathbb{F}_q^n)/I \to (L_{(a,b)}\mathbb{F}_q^n)/I.$$

This leads us to the following definition.

**Definition A.1.** *Let $I$ be an ideal in $\bigwedge^{\bullet,\bullet} \mathbb{F}_q^n$, then $I$ is $\Theta$-stable if $\theta_i(I) \subset I$ for all $i \geq 0$. Likewise let $X = (x_1, \ldots, x_k)$ be a sequence of elements in $\bigwedge^{\bullet,\bullet} \mathbb{F}_q^n$, then $X$ is $\Theta$-stable if $I_r = \langle x_1, \ldots x_r \rangle$ is $\Theta$-stable for all $r$.*

By the Leibniz rule, an ideal is $\Theta$-stable if the $\theta_k$ of its generators lie in it. This gives us the following.

**Lemma A.2.** *Let $x \in \bigwedge^{s,t} \mathbb{F}_q^n$ with $s + t \equiv 0 \bmod 2$ and denote $\ell = \lfloor \log_2 n \rfloor$. Then*

$$(\theta_s(x), \ldots, x,\ \theta_s(x)^{(2)}, \ldots, x^{(2)},\ \ldots,\ \theta_s(x)^{(2^\ell)}, \ldots, x^{(2^\ell)})$$

*is $\Theta$-stable.*

*Proof.* By Eq. (1) we have $\theta_k(\theta_i(x)) = \binom{i+k}{k}\theta_{i+k}(x)$, which is zero or occurs earlier in the sequence. By Lem. 4.4, $\theta_k(\theta_i(x)^{(2)})$ is a sum of products of elements of the first block plus, for even $k$, a multiple of $\theta_{i+k/2}(x)^{(2)}$, which again occurs earlier. The higher divided powers are treated in the same way, using that the ideal generated by the earlier blocks is closed under divided squares, as in the proof of Lem. 4.5.

Thus, by constructing our ideal generator by generator with

$$\mathcal{F} = \left((1 \otimes \omega_1), \ldots, (1 \otimes \omega_m)^{(2^{\log_2 b})}, \beta_1, \ldots, \beta_m^{(2^{\log_2 b})}, (\omega_1 \otimes 1), \ldots, (\omega_m \otimes 1)^{(2^{\log_2 a})}\right)$$

and $I_r = \langle \mathcal{F}_1, \ldots, \mathcal{F}_r \rangle$ we can safely define multiplication maps

$$m_{\mathcal{F}_{r+1}} : (L_{a-s_{r+1},b-t_{r+1}}\mathbb{F}_q^n)/I_r \to (L_{a,b}\mathbb{F}_q^n)/I_r.$$

**Semi-regularity.** Now that we have multiplication maps we might hope that we can define semi-regular $\Theta$-stable sequences. But unfortunately, the incremental nature of semi-regularity causes problems. Recall that a sequence $f_1, \ldots, f_n$ is semi-regular if

$$R/\langle f_1, \ldots, f_{i-1}\rangle \xrightarrow{m_{f_i}} R/\langle f_1, \ldots, f_{i-1}\rangle$$

is full rank for each $i$. Slightly more relevant for us is boolean semi-regularity which requires

$$R/\langle f_1, \ldots, f_i\rangle \xrightarrow{m_{f_i}} R/\langle f_1, \ldots, f_{i-1}\rangle$$

to be full rank instead.

If we try to mimic this we unfortunately run into problems. For example, consider the map

$$L_{(s,t)}\mathbb{F}_q^n/\langle \theta_s(x), \ldots, \theta_1(x)\rangle \xrightarrow{m_{\theta_1(x)}} L_{(2s-1,2t+1)}\mathbb{F}_q^n/\langle \theta_s(x), \ldots, \theta_2(x)\rangle.$$

We compute

$$m_{\theta_1(x)}(x) = \theta_1(x) \wedge x = \frac{1}{2}\theta_1(x \wedge x) = \theta_1(x^{(2)}) \in \Theta.$$

Note that $x$ cannot lie in $\langle \theta_s(x), \ldots, \theta_1(x)\rangle + \Theta$ for degree reasons, thus the multiplication maps cannot be full rank.

For the UOV system this happens with $x = \omega_i \otimes 1$, where $\theta_1(x) = \beta_i$ and $x^{(2)} = (\omega_i \otimes 1)^{(2)}$, and the computation above reads

$$\beta_i \wedge (\omega_i \otimes 1) = \theta_1\big((\omega_i \otimes 1)^{(2)}\big) \in \Theta.$$

So the product of two generators of $J$ vanishes in $L_{(\bullet,\bullet)}\mathbb{F}_q^n$, which never happens for a regular sequence, and any count that treats $\beta_i$ and $\omega_i \otimes 1$ as independent equations overcounts by this syzygy. On the other hand, the element it originates from, $(\omega_i \otimes 1)^{(2)}$, is itself a generator of $J$, and it is plausible that the two effects cancel: the tower of $\omega_i \otimes 1$ is counted once by the factor $(1 - t^2)$, which already accounts for $(\omega_i \otimes 1)^{(2)}$ and hence for the relation above. We do not know how to turn this into a definition of semi-regularity for a sequence of operators, and so we cannot derive the series from such an assumption. We therefore state it as a conjecture and test it experimentally in Tabs. 3 and 4.

| Parameters | | | | Old [24] | | New (this paper) | | |
|---|---|---|---|---|---|---|---|---|
| Level | $v$ | $o$ | $m$ | bit | $o'$ | bit | $\log_2 N$ | $\lambda$ |
| | 78 | 8 | 78 | — | — | 231 | 106 | $(8, 8, 8)$ |
| | 76 | 9 | 76 | — | — | 205 | 93 | $(9, 9, 3)$ |
| | 74 | 10 | 74 | — | — | 178 | 79 | $(10, 9)$ |
| | 70 | 11 | 70 | — | — | 155 | 67 | $(11, 5)$ |
| I | **68** | **12** | **68** | — | — | **125** | **51** | $(\mathbf{12}, \mathbf{1})$ |
| | 66 | 14 | 66 | 113 | 13 | 112 | 45 | $(12)$ |
| | 64 | 17 | 64 | 112 | 13 | 111 | 44 | $(12)$ |
| | 64 | 22 | 64 | 112 | 13 | 111 | 44 | $(12)$ |
| | 67 | 33 | 64 | 114 | 13 | 118 | 48 | $(13)$ |
| | 114 | 9 | 114 | — | — | 351 | 166 | $(9, 9, 9, 7)$ |
| | 108 | 10 | 108 | — | — | 291 | 135 | $(10, 10, 9)$ |
| | 106 | 11 | 106 | — | — | 273 | 126 | $(11, 11, 5)$ |
| | 104 | 12 | 104 | — | — | 232 | 105 | $(12, 12)$ |
| | 102 | 13 | 102 | — | — | 225 | 101 | $(13, 10)$ |
| III | **100** | **15** | **100** | — | — | **191** | **83** | $(\mathbf{15}, \mathbf{4})$ |
| | **98** | **17** | **98** | — | — | **152** | **63** | $(\mathbf{16})$ |
| | 98 | 20 | 98 | 151 | 17 | 152 | 63 | $(16)$ |
| | 96 | 25 | 96 | 150 | 17 | 151 | 63 | $(16)$ |
| | 96 | 33 | 96 | 150 | 17 | 151 | 63 | $(16)$ |
| | 101 | 49 | 96 | 158 | 18 | 160 | 66 | $(17)$ |
| | 146 | 10 | 146 | — | — | 451 | 215 | $(10, 10, 10, 10, 2)$ |
| | 144 | 11 | 144 | — | — | 413 | 196 | $(11, 11, 11, 6)$ |
| | 142 | 12 | 142 | — | — | 368 | 173 | $(12, 12, 12)$ |
| | 140 | 13 | 140 | — | — | 351 | 164 | $(13, 13, 8)$ |
| | 138 | 14 | 138 | — | — | 318 | 147 | $(14, 14, 3)$ |
| | 136 | 16 | 136 | — | — | 287 | 131 | $(15, 14)$ |
| V | 134 | 17 | 134 | — | — | 272 | 122 | $(17, 10)$ |
| | **132** | **20** | **132** | — | — | **193** | **81** | $(\mathbf{20})$ |
| | 132 | 23 | 132 | 189 | 21 | 193 | 81 | $(20)$ |
| | 130 | 27 | 130 | 188 | 21 | 192 | 81 | $(20)$ |
| | 128 | 33 | 128 | 187 | 21 | 191 | 81 | $(20)$ |
| | 128 | 44 | 128 | 187 | 21 | 191 | 81 | $(20)$ |
| | 137 | 65 | 128 | 203 | 23 | 208 | 88 | $(22)$ |

**Table 9.** Estimates for attack cost in $\log_2$ on various MAYO Round-2 parameter sets [6] using Schur modules of shape $\lambda$. Compared against the wedge attack [24]. For all parameters $q = 16$. Rows in bold are parameter sets that fall below their claimed security level and were out of reach of previous attacks.

| | Parameters | | | | [24]† | | This work | | |
|---|---|---|---|---|---|---|---|---|---|
| SL | $v$ | $o$ | $m$ | $q$ | bits | $o'$ | bits | $\log_2 N$ | $\lambda$ |
| I | 52 | 18 | 54 | $127^3$ | 198 | 13 | 191 | 84 | $(16, 9)$ |
| | 74 | 10 | 100 | $7^{10}$ | — | — | 229 | 102 | $(8, 7, 5, 2)$ |
| | 55 | 20 | 60 | $31^3$ | 201 | 13 | 195 | 86 | $(15, 10)$ |
| | 60 | 7 | 70 | $31^{10}$ | — | — | 211 | 93 | $(7, 7, 5, 2)$ |
| III | 76 | 26 | 78 | $127^3$ | 266 | 17 | 264 | 120 | $(20, 14)$ |
| | 110 | 14 | 140 | $7^{10}$ | — | — | 340 | 156 | $(11, 7, 7, 7)$ |
| | 82 | 29 | 87 | $31^3$ | 282 | 18 | 276 | 126 | $(19, 16)$ |
| | 89 | 10 | 100 | $31^{10}$ | — | — | 301 | 137 | $(10, 10, 10, 1)$ |
| V | 102 | 35 | 105 | $127^3$ | 345 | 22 | 342 | 159 | $(27, 17)$ |
| | 149 | 19 | 190 | $7^{10}$ | — | — | 455 | 209 | $(16, 9, 9, 8)$ |
| | 108 | 38 | 114 | $31^3$ | 361 | 23 | 355 | 165 | $(26, 19)$ |
| | 112 | 12 | 120 | $31^{10}$ | — | — | 381 | 177 | $(12, 12, 10, 4)$ |

**Table 10.** Comparison of bit complexities of the exterior algebra attack and Schur attack against QR-UOV. †: The bit complexities of [24] are remodeled using a matrix of size $\dim \bigwedge^{o',o'} \mathbb{F}_q^n$ instead of $\dim L_{(o',o')}\mathbb{F}_q^n$ for comparative reasons, also field operation cost is included.