IACR Communications in Cryptology
ISSN 3006-5496, Vol. 3, No. 2, 18 pages.

https://doi.org/10.62056/avur-zn4

Check for updates

Subfield attack: leveraging composite-degree extensions in the Quotient Ring transform

Pierre Pébereau

KU Leuven, COSIC, Leuven, Belgium

Abstract. The VOX signature scheme is a multivariate signature scheme which was submitted to the Round 1 Additional Digital Signature Schemes NIST process. VOX relies on the Hat Plus perturbation and the Quotient-Ring transform. We formalize a dimension criterion enabling the direct attack to be used as a key recovery attack against UOV schemes. This enables a practical cryptanalysis of the Round 1 VOX parameters. Next, we show that some of the alternative parameters proposed for VOX after attacks on the Round 1 submission are still vulnerable. More precisely, these parameters were chosen to defeat an attack of Furue and Ikematsu in the field $\mathbb{F}F_{q^\ell}$ interpreted as an extension of degree ℓ of $\mathbb{F}_q$. We observe that one may use a smaller extension $\mathbb{F}_{q^{\ell'}}$ for any $\ell'|\ell$, in which case the attacks apply again. These attacks are relevant for a subset of the parameter sets proposed for VOX: I, Ic, III, IIIa, V, Vb. In particular, we apply the subfield framework to our previous dimension criterion for the direct attack. We estimate the cost of our attack on these parameter sets and find costs of at most 2^{67} gates, and significantly lower in most cases. In practice on a commercial laptop, our attack requires $0.3s$, $1.35s$, $0.56s$ for parameter sets I, III, V for VOX, and $56.7s$, $6.11s$ for the alternative parameter sets IIIa, Vb. Our analysis also improves the cryptanalysis of some alternative parameters proposed by Guo and Ding, and of the "Minus" variant of VOX.

Keywords: Multivariate cryptography · Algebraic cryptanalysis · Subfield attack

Introduction

In 2022, the American National Institute of Standards and Technology (NIST) selected three post-quantum signature algorithms for standardization. In order to diversify the security assumptions and the performance trade offs of post-quantum standards, NIST has decided to standardize additional signature schemes in a new process. In fact, the size of both public keys and signatures in the initial standards are at least an order of magnitude larger than in ECDSA, which raises issues in many protocols. In some applications, such as spatial or submarine communications, bandwidth may be limited, which also requires compact signatures. Thus, performance is an important criterion in this new NIST process.

Multivariate signature schemes base their security on the hardness of solving systems of multivariate polynomial equations over finite fields. The Unbalanced Oil and Vinegar signature scheme (UOV) [KPG99] is a multivariate signature scheme which is in the spotlight of this additional NIST competition due to its short signatures and stable cryptanalysis for the past 25 years. Seven UOV variants were evaluated during the first round of the additional post-quantum competition, including in particular UOV [BCD+23], QR-UOV [FIKT21] and VOX [CFF+23b]. Four moved on to the second round: UOV, QR-UOV, MAYO [BCC+25], and SNOVA [WCD+25]. The main drawback of UOV is the large public key size (at least 43kB compressed at level 1).

E-mail: pierre.pebereau@esat.kuleuven.be (Pierre Pébereau)

This work is licensed under a "CC BY 4.0" license.
Received: 2026-04-07 Accepted: 2026-06-30

The three UOV variants that progressed to Round 2 tackle this issue by adding structure to reduce public key size. In both QR-UOV and SNOVA, a small field/big field construction enables the compression of the public keys involved in the schemes. In both cases, this construction exposes these schemes to key recovery attacks in a relatively large finite field, which are typically easier algebraic attacks compared to small field instances, as they feature less variables while keeping the same number of polynomial equations. On the other hand, the increase in field size only has a logarithmic impact on the complexity of arithmetic operations.

VOX applies the QR transform to the UOV$\hat{+}$ signature scheme [FMPP22]. The $\hat{+}$ ("Hat Plus") perturbation replaces some secret key polynomials with random quadratic polynomials in order to increase the difficulty of key recovery attacks, at the cost of slowing down the signing algorithm. This enables the scheme to feature less vinegar variables compared with a standard UOV public key, and combined with the QR transform to further reduce public key size, the Round 1 submission achieved a compact construction. This performance, along with the fact that the Hat Plus perturbation was relatively new, motivated a detailed analysis of the security of VOX, both through the lense of the QR transform and through the study of the Hat Plus perturbation.

In this work, which was carried out as VOX was still considered by NIST as a Round 1 candidate, we propose a geometric approach to the cryptanalysis of signature schemes based on the QR transform, with a specific focus on VOX, and leverage the existence of subfields to circumvent countermeasures introduced in VOX to defend against big field attacks.

Context and related work

The Quotient Ring transform for UOV was introduced in [FIKT21] following the cryptanalysis of Block-Anti-Circulant UOV [SP20, FKI+20]. In [FIKT21, Section 5], it is highlighted that the transformation exposes the scheme to attacks in $\mathbb{F}_{q^\ell}$. This "big field" analysis was not detailed in the first specification of VOX [CFF+23b, Section 7.4].

The initial VOX parameters submitted to NIST Round 1 [CFF+23b] suffered a MinRank attack [FI23b], which had an estimated complexity of $2^{39}, 2^{42}, 2^{41}$ gates for parameter sets I, III, V. For a VOX public key for parameters (n, m, o, ℓ, q, t), the attack fails if $o \leq t$. Following this observation, alternative parameters were proposed for VOX in [MRPC+23], enforcing this inequality. These alternative parameters were attacked using another MinRank attack in [GD24, GJP+24], with complexities estimated below 2^{58} for all parameters, and experiments performing the key recovery attack in less than a second in almost all cases.

Our work was carried out independently of [GD24], and a preliminary version was available on the IACR ePrint archive in February 2024, a few days after the first version of [GD24]. We propose an alternative practical cryptanalysis of VOX which is geometric in nature, without relying on the MinRank problem, and highlight a weakness introduced by the QR transform in subfields of $\mathbb{F}_{q^\ell}$ which (when applicable) defeats the countermeasures to the previously mentioned attacks. In particular, we are able to attack not only the VOX parameters proposed in [CFF+23b, MRPC+23], but also alternative parameters proposed in [GD24, GJP+24].

Regarding the security of the scheme UOV$\hat{+}$ without the addition of the QR transform, [Péb25] proposed a generalization of the Kipnis-Shamir attack [KPG99] interpreted as a singular point attack (see also [Luy23]), which improved the cryptanalysis of UOV$\hat{+}$ without leveraging the QR structure.

In [Var25], the VOX-minus variant of VOX is introduced, with the goal to further decrease the public key size by decoupling the number of equations in the base field from the dimension of the oil space.

Main results

The contributions of this paper are twofold.

First, we formalize a dimension criterion enabling the direct attack to be used as a key recovery attack against UOV schemes. When this criterion is satisfied, a grevlex Gröbner basis computation will yield linear polynomials characterizing a subspace of $\mathcal{O}$, thus running a change-of-order algorithm (such as [FGLM93]) is not necessary. This criterion is always satisfied in the big field instances of QR-UOV schemes [FIKT21], and in the case of MAYO [Beu21, BCC+25]. Since VOX is a QR-UOV variant, the direct attack can be used to perform a key recovery attack against VOX, as discussed in Section 1.2. Through a comparison between the system of polynomial equations that appears in the direct attack in the big field and a similar semi-regular sequence, we propose a heuristic complexity analysis of this key recovery attack on VOX. This analysis shows the vulnerability of the initial VOX parameters [CFF+23b], without introducing a MinRank formulation of the problem. Following NIST methodology, we estimate that our attack requires $2^{38.1}, 2^{41.2}, 2^{43.7}$ gates for VOX [CFF+23b] parameter sets I, III, V respectively. In practice, our attack requires $0.03s, 0.11s, 0.32s$ for parameter sets I, III, V. This is essentially a reformulation of the security analysis of the QR-UOV scheme [FIKT21]. We observe that our attack against VOX is defeated by enforcing $o \leq t$, which is a countermeasure used by the VOX team to defeat the attack of [FI23b].

Second, we observe that the security of QR-UOV sub-instances in $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$ is a necessary, but not sufficient condition to ensure the security of a QR-UOV scheme. Indeed, an attacker may target the secret key in a subfield $\mathbb{F}_{q^{\ell'}}$ for any ℓ' dividing ℓ. The initial analysis corresponds to the special cases $\ell' = 1$ and $\ell' = \ell$. Denote by $\ell_1, \dots, \ell_r$ the proper factors of ℓ. Thus, the security of the QR-UOV variant instantiated over $\mathbb{F}_{q^\ell}$ necessarily relies on the security of the QR sub-instances over $\mathbb{F}_q, \mathbb{F}_{q^{\ell_1}}, \dots, \mathbb{F}_{q^{\ell_r}}, \mathbb{F}_{q^\ell}$. For VOX, this observation is crucial to analyze the scheme, as the subfield instances may not satisfy $\ell' o \leq t$. We can perform a direct attack on the UOV$\hat{+}$ instance induced over any subfield $\mathbb{F}_{q^{\ell'}}$ such that $\ell' | \ell$ and $\ell' o > t$. We note in Remark 4 that the number of variables is proportional to $\frac{\ell}{\ell'}$, therefore it is more advantageous to choose a larger field in the attack. The subfield attack applies to a subset of the parameters proposed in [CFF+23b, MRPC+23]. Our attack applies to the parameter sets Ic, IIIa, Vb of [MRPC+23], which feature a non-prime extension degree. Following NIST methodology, we estimate the complexity of the subfield direct attack at $2^{67.4}, 2^{59.7}, 2^{51.1}$ gates for parameter sets Ic, IIIa, Vb respectively. Our attack also reduces the security of some alternative VOX parameters proposed in [GD24] and of the initial VOX minus parameters proposed in [Var25].

In practice, the systems are cheaper to solve than predicted. Polynomial systems are generated using SageMath, and we rely on the msolve library for polynomial system solving, which implements the F4 algorithm. An instance of VOX parameter set Ic is solved in 400h CPU-hours using an Intel Xeon CPU E7-4820 running at 2.00GHz. The other two parameter sets are attacked on a commercial laptop using an Intel i7-1165G7 CPU running at 2.80GHz. An instance of IIIa is solved in 83.4 seconds, and of Vb in 12.4 seconds.

Organization of the paper

In Section 1, we recall some background on ideals and varieties, as well as the definitions of UOV, QR-UOV, UOV$\hat{+}$ and VOX. In Section 2, we show that the direct attack against a UOV scheme can be used as a key recovery attack when the public key has a large number of polynomials compared to the dimension of the secret subspace and the dimension of the ambient space. In Section 3, we show that QR-UOV schemes, including VOX, are exposed to subfield attacks. In the case of VOX, this observation enables the previous key recovery attack in subfield instances of the VOX key recovery problem.

1 Preliminaries

In this section, we begin by recalling some properties of ideals and varieties relevant to algebraic attacks. Next, we introduce the signature schemes which are studied in the remainder of the paper. In each case, we propose a succinct description and recall the main framework of the security analysis. For a more complete security analysis of these schemes, we refer the reader to the corresponding NIST submission document.

Notations

For q a power of a prime, the finite field with q elements is noted $\mathbb{F}_q$. Vectors are denoted by bold letters $\boldsymbol{x}, \boldsymbol{t}$, ..., matrices are denoted by capital letters $A, S, ...$, and indeterminates are denoted by $X_1, \ldots, X_n$.

1.1 Ideals and varieties

We recall some notions related to polynomial systems and their solutions. For more details on this topic, we refer the reader to [CLO15].

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

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

A sequence of polynomials $(p_1, \ldots, p_m)$ is a *regular sequence* if for $2 \leq i \leq m$, p_i does not divide 0 in $\mathbb{K}[X_1, \ldots, X_n]/\langle p_1, \ldots, p_{i-1} \rangle$. As a consequence, the Hilbert Series of $\mathcal{R} := \mathbb{K}[X_1, \ldots, X_n]/\langle p_1, \ldots, p_m \rangle$, which is the power series $H(t) = \sum_{d \in \mathbb{N}} \dim_{\mathbb{K}}(\mathcal{R}_d) t^d$ admits a simple closed form:

$$H(t) = \frac{(1-t^2)^m}{(1-t)^n}.$$

As a consequence, the behavior of Gröbner basis algorithms (see [Laz83, Fau99, CKPS00, Fau02]) is very predictable when the input is a regular sequence. A point $\boldsymbol{x} \in \overline{\mathbb{K}}^n$ is a solution of $p_1 = \cdots = p_m = 0$ if and only if it cancels all polynomials in $\langle p_1, \ldots, p_m \rangle$. Thus, the set of solutions of a polynomial system is defined with respect to the ideal generated by the polynomials, and called an algebraic set or algebraic variety. The *algebraic variety* defined by an ideal $\mathcal{I}$ is denoted by $V(\mathcal{I}) := \{\boldsymbol{x} \in \overline{\mathbb{K}}^n, \quad \forall f \in \mathcal{I}, f(\boldsymbol{x}) = 0\}$. The *dimension* of a variety $V(\mathcal{I})$ is the Krull dimension of the quotient ring $\mathbb{K}[X_1, \ldots, X_n]/\mathcal{I}$. Geometrically, it is equal to the number of hyperplanes in general position that one can intersect with the variety before it is reduced to a finite set of points (in an algebraic closure). In particular, the dimension of a linear subspace included in an algebraic variety is a lower bound on the dimension of said variety [CLO15, Chapter 9, Section 4, Proposition 1]. Recall that all algebraic varieties admit a minimal decomposition into irreducible varieties which are called irreducible components [CLO15, Chapter 4, Section 6, Theorem 2].

1.2 UOV

Description

We begin by recalling the definition of UOV [Pat97, KPG99]. The UOV trapdoor is a quadratic map that is linear in a subset of variables, enabling it to be inverted by fixing the quadratic variables to random values during the signing process.

Definition 1 (Algebraic description of UOV [KPG99])**.** A UOV key pair for parameters (n, m, o, q) is composed of a secret key $(A, \mathcal{F})$ and a public key $\mathcal{P}$, where:

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

$$\begin{array}{rccl} \mathcal{F}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^m \\ & \boldsymbol{x} & \mapsto & \mathcal{F}(\boldsymbol{x}) = (f_1(\boldsymbol{x}), \dots, f_m(\boldsymbol{x})) \end{array}$$

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

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

- $\mathcal{P} = \mathcal{F} \circ A$ is a quadratic map.

$$\begin{array}{rccl} \mathcal{P}: & \mathbb{F}_q^n & \to & \mathbb{F}_q^m \\ & \boldsymbol{x} & \mapsto & \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \dots, p_m(\boldsymbol{x})) \end{array}$$

Note that in the original definition of UOV [KPG99], it holds that $o = m$. It is imposed in UOV that $n > 2o$, due to the Kipnis-Shamir attack on OV [KS98]. We mainly rely on the geometric characterization of UOV, which is due to Kipnis and Shamir [KS98].

Definition 2 (Geometric UOV trapdoor [KS98])**.** A UOV public key for parameters (n, m, o, q) is a quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined by $(p_1, \dots, p_m)$ such that there exists a (secret) linear subspace $\mathcal{O}$ of dimension o such that $\mathcal{P}(\mathcal{O}) = \{0\}$. In other words,

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

Direct attack on UOV

Let $\mathcal{P} = (p_1, \dots, p_m)$ be a UOV public key for parameters (n, m, o, q). Let $\boldsymbol{t} \in \mathbb{F}_q^m$ be a target vector. Recall that $\boldsymbol{x} \in \mathbb{F}_q^n$ is a signature of $\boldsymbol{t}$ for $\mathcal{P}$ if and only if

$$\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}. \tag{2}$$

Denote by $\mathcal{I}_{\boldsymbol{t}}$ the ideal $\langle p_1 - t_1, \dots, p_m - t_m \rangle$. The *UOV forgery problem* is the task of finding an $\mathbb{F}_q$-rational point in the variety $V(\mathcal{I}_{\boldsymbol{t}})$. In UOV, since $m = o$, it holds that $n > 2m$. Thus, the systems of equations defined by UOV public keys have less equations than variables, and therefore the variety they define is positive dimensional. Such systems are called *underdetermined*. If $(p_1 - t_1, \dots, p_m - t_m)$ forms a regular sequence, this variety has dimension $n - m$. The direct attack against UOV consists in finding points in $V(\mathcal{I}_{\boldsymbol{t}})$ by adding $n - m$ random linear polynomials to the system of Equation (2) to reach dimension zero, and then using a Gröbner basis algorithm to find solutions of the resulting zero-dimensional system. After eliminating $n - m$ variables with the linear polynomials, we obtain an equivalent zero-dimensional system of polynomial equations of degree two:

$$\mathcal{E}: \begin{cases} \tilde{p}_1(X_1, \dots, X_m) - t_1 = 0 \\ \quad \vdots \\ \tilde{p}_m(X_1, \dots, X_m) - t_m = 0 \end{cases}. \tag{3}$$

Denote by $\mathcal{I}$ the ideal generated by $\mathcal{E}$ and by $\mathcal{R} = \mathbb{F}_q[X_1, \dots, X_m]$.

The complexity of this attack is estimated using [BFS15, Proposition 1]. The degree of regularity of a balanced regular quadratic polynomial system is obtained from the following Hilbert series:

$$\mathsf{HS}_{\mathcal{R}/\mathcal{I}}(z) = \frac{(1-z^2)^m}{(1-z)^n} = (1+z)^m.$$

Thus, the degree of regularity d_{reg} is $m+1$. This attack can be improved with the hybrid method [BFP09] and with precomputations [TW12, Has23], but this will not be relevant in this paper.

1.3 QR-UOV

Description

Quotient ring UOV (QR-UOV, [FIKT21], [FIH+23]) is a signature scheme designed to offer smaller public keys than UOV. Let ℓ be a positive integer, which we refer to as the *QR parameter*. Let $S \in \mathbb{F}_q^{\ell\times\ell}$ be a matrix whose characteristic polynomial is irreducible. Each element of $\mathbb{F}_{q^\ell}$ can be represented as a linear combination of the matrices $I_\ell, S^1, S^2, \ldots, S^{\ell-1}$ in $\mathbb{F}_q^{\ell\times\ell}$ by the isomorphism:

$$\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[S] = \left\{ \sum_{0\le i<\ell} a_i S^i, (a_i)_i \in \mathbb{F}_q^\ell \right\}.$$

Consider a UOV public key for parameters $(n, \ell m, m, q^\ell)$. Let $(P_1, \ldots, P_{\ell m}) \in \mathbb{F}_{q^\ell}^{(n\times n)\ell m}$ be the square matrices representing this public key. For all $1 \le i \le \ell m$, we define the matrix $\mathsf{QR}_\ell(P_i)$ which is an $\ell n \times \ell n$ block matrix over $\mathbb{F}_q$, where each block represents the corresponding element of $\mathbb{F}_{q^\ell}$ in $\mathbb{F}_q[S]$. Thus, the matrices $\mathsf{QR}_\ell(P_i)$ are described by $\ell\binom{n}{2}$ elements in $\mathbb{F}_q$, instead of $\ell^2\binom{n}{2}$ for a generic quadratic form of similar dimensions. Therefore, a factor ℓ compression is achieved, compared to a usual UOV $(\ell n, \ell m, \ell m, q)$ instance.

A QR-UOV public key for parameters (n, m, ℓ, q) is the quadratic map induced over $\mathbb{F}_q$ by the transformation QR_ℓ applied to a UOV $(n, \ell m, m, q^\ell)$ public key. The corresponding trapdoor is the corresponding secret subspace over $\mathbb{F}_q$, of dimension ℓm.

Security analysis

For QR-UOV to be secure, it is necessary that the following schemes are secure:

- UOV for parameters $(\ell n, \ell m, \ell m, q)$.
- UOV for parameters $(n, \ell m, m, q^\ell)$.

Remark 1. Algebraic attacks are typically more efficient on the big field scheme defined in $\mathbb{F}_{q^\ell}$, as the modelings have less variables, and the cost of arithmetic is only logarithmically impacted by the growth of the field size. On the other hand, combinatorial attacks usually have no advantage in the small field, as the size of the field is compensated by the factor ℓ in the parameters. As an example, consider the number of guessing steps in the Kipnis-Shamir attack in both settings, which is the exponential factor in the complexity:

$$\mathsf{KS}(\ell n, \ell m, \ell m, q) = q^{\ell n - 2\ell m} = (q^\ell)^{n-2m}. \tag{4}$$

$$\mathsf{KS}(n, \ell m, m, q^\ell) = (q^\ell)^{n-2m} = \mathsf{KS}(\ell n, \ell m, \ell m, q). \tag{5}$$

1.4 UOV Hat Plus

Description

UOV$\hat{+}$ ("hat plus" [FMPP22], [CFF+23b]) is a signature scheme designed to increase the difficulty of key recovery attacks compared to UOV with similar parameters, at the cost of increasing signing time. As the hardness of key recovery attacks increases, public key size can be reduced. The high level idea is to add a small number of random quadratic polynomials to a UOV public key, which means that the signer must solve a small polynomial system to sign a message instead of a linear system as in UOV. In turn, an attacker cannot apply standard UOV key recovery attacks to the public key, as the random polynomials do not verify the trapdoor structure. This construction is the *hat plus perturbation*.

Let (n, m, o, q) be UOV parameters, let $t \in \mathbb{N}$ be an integer. A UOV$\hat{+}$ key pair for parameters (n, m, o, q, t) is defined by:

- A secret key $\mathcal{F} = (f_{t+1}, \dots, f_m), S \in GL_m(\mathbb{F}_q), A \in GL_n(\mathbb{F}_q)$ where $(\mathcal{F}, A)$ is a UOV secret key for parameters $(n, m-t, o, q)$.
- A public key $\mathcal{P} = S \circ \hat{\mathcal{F}} \circ A$ where $\hat{\mathcal{F}} = (r_1, \dots, r_t, f_{t+1}, \dots, f_m)$ and $r_1, \dots, r_t$ are quadratic polynomials drawn uniformly at random in $\mathbb{F}_q[X_1, \dots, X_n]_2$.

In [FMPP22, CFF+23b], all parameters have t upper bounded by 10, as the signer is unable to sign efficiently if t is large.

As in UOV, the scheme is instantiated with $m = o$, but it can be defined in more generality as above. The map $\hat{\mathcal{P}} = \hat{\mathcal{F}} \circ A = (\hat{p}_1, \dots, \hat{p}_m)$ is referred to as the underlying UOV map: its first t components are quadratic polynomials sampled uniformly at random over $\mathbb{F}_q$, while the remaining $m - t$ are UOV polynomials. Notice that composing with S performs linear combinations of components of $\hat{\mathcal{P}}$, which prevents an attacker from isolating the underlying UOV map in a UOV$\hat{+}$ public key. In UOV, such an operation does not add to the security of the scheme, as linear combinations of UOV polynomials for a given secret key are still UOV polynomials for the same secret key.

Finally, note that the matrices S and A are chosen with some additional structure in [CFF+23b]. For S, it consists in imposing that $p_1, \dots, p_t = \hat{p}_1, \dots, \hat{p}_t$ (which corresponds to a $t \times t$ identity block), which means that the random polynomials are not secret. For A, as in UOV, it imposes that the "vinegar" part of the transformation is the identity. This makes no difference in currently known attacks.

Security analysis

Let us detail a public UOV$\hat{+}$ polynomial. Let $\mathcal{P} = S \circ \hat{\mathcal{P}}$ be a UOV$\hat{+}$ public key for parameters (n, m, o, q, t). Let $1 \leq i \leq m$.

$$p_i = \sum_{1 \leq j \leq m} s_{i,j} \hat{p}_j = \underbrace{\sum_{1 \leq j \leq t} s_{i,j} \hat{p}_j}_{\text{Random polynomials}} + \underbrace{\sum_{t+1 \leq j \leq m} s_{i,j} \hat{p}_j}_{\text{UOV Polynomials}}.$$

The polynomials $\hat{p}_i, 1 \leq i \leq t$ form an at most t dimensional linear subspace of the vector space $\mathsf{span}(p_1, \dots, p_m) \subset K[\boldsymbol{X}]$, therefore there exist linear combinations of $t+1$ polynomials among $p_1, \dots, p_m$ canceling the contribution of $\hat{p}_1, \dots, \hat{p}_m$. Algebraically, there exist scalars $(c_i)_{1 \leq i \leq t} \in \mathbb{F}_q^t$ and $(C_j)_{t+1 \leq j \leq m}$ such that

$$g_{\boldsymbol{c}} = \sum_{1 \leq i \leq t} c_i p_i + 1 \cdot p_{m+1} = 0 + \sum_{t+1 \leq j \leq m} C_j \hat{p}_j,$$

where we have assumed without loss of generality that $c_{t+1} \neq 0$. Thus, $g_{\boldsymbol{c}}$ is a UOV polynomial for the underlying UOV secret key of the UOV$\hat{+}$ public key.

Therefore, an attack against UOV$\hat{+}$ can be obtained by guessing the values of c_i which yield a UOV polynomial. There is (at least) one correct guess out of q^t values. The authors of UOV$\hat{+}$ have observed that UOV attacks require at least two polynomials from the UOV public key, therefore an attacker should obtain at least two linearly independent UOV polynomials before being able to apply an attack. Therefore, the attacker must correctly guess $2t$ scalars in $\mathbb{F}_q$ before applying a UOV attack. In the security analysis of UOV$\hat{+}$ [FMPP22], [CFF+23b], an attack against the scheme has an expected cost decomposed as follows:

$$q^{2t} \times C_{UOV}(n, 2, o, q),$$

where $C_{UOV}(n, 2, o, q)$ denotes the expected cost of attacking a UOV$(n, 2, o, q)$ instance.

1.5 VOX

Description

VOX [CFF+23b] is the scheme obtained by applying the QR transform to UOV$\hat{+}$, which enables the scheme to benefit from smaller public keys by applying both transformations. In [CFF+23b], the parameter ℓ is noted c. We follow the notation of [FIKT21] in this paper for coherence.

A VOX public key for parameters (n, m, o, ℓ, q, t) is the quadratic map induced by applying the QR_ℓ transform to a UOV$\hat{+}$ public key for parameters $(n, \ell m, o, q^\ell, t)$. The corresponding secret key is the underlying UOV secret subspace in $\mathbb{F}_q^{\ell n}$.

Security analysis

The same observations that applied to QR-UOV in Section 1.3 apply to VOX. Namely, for a VOX instance to be secure, it is necessary that the following associated UOV$\hat{+}$ instances are secure:

- The $(n, \ell m, o, q^\ell, t)$ UOV$\hat{+}$ instance must be secure.
- The $(\ell n, \ell m, \ell o, q, t)$ UOV$\hat{+}$ instance must be secure.

In [CFF+23b], the large field analysis is neglected (the first bullet point). The initial VOX parameters [CFF+23b] (see Figure 1) suffered a MinRank attack [FI23b], which had an estimated complexity of $2^{39}, 2^{42}, 2^{41}$ gates for parameter sets I, III, V. For a VOX public key for parameters (n, m, o, ℓ, q, t), the attack is defeated by enforcing $o \leq t$. Following this observation, alternative parameters were proposed for VOX in [MRPC+23]. These alternative parameters were attacked using a MinRank attack in [GD24, GJP+24], with complexities estimated below 2^{58} for all parameters, and experiments performing the key recovery attack in less than a second in almost all cases.

2 Direct attack as a key recovery attack

We consider the direct attack of Section 1.2, and focus on the case where $n - m < o$. This is the setting in which the UOV subinstances lie when using the QR transform [FIKT21].

The goals of this section are two-fold. First, we derive a criterion enabling the direct attack against the UOV public key to be used as a key recovery attack, and generalize it to UOV hat plus. Next, we leverage the structure introduced by the Quotient Ring transform from $\mathbb{F}_q$ to $\mathbb{F}_{q^\ell}$ to apply this attack in $\mathbb{F}_{q^\ell}$, in the framework of [FIKT21].

In the case of QR-UOV, these tasks are straightforward. However, in VOX, the random quadratic polynomials have an impact on our approach which requires some care.

2.1 Irregular UOV systems yield a direct key recovery attack

In the next lemma, we show that overdetermined UOV instances, such as those involved in the big field instance of QR-UOV and VOX, are easier to distinguish from generic polynomial sequences of degree two than their underdetermined counterparts. In this section and in the remainder of the paper, *generic* should be interpreted in the sense of Zariski topology, and more precisely in the sense of [DM98, Théorème 2.1]: the dimension of the largest linear subspace which vanishes a *generic* collection of m quadratic polynomials in n variables is bounded by an integer, which is strictly smaller than o in all UOV, QR-UOV and VOX parameters submitted to NIST.

Lemma 1. *Let $\mathcal{P} = (p_1, \dots, p_m)$ be a UOV public key for parameters (n, m, o, q) such that $n - m < o$. Denote by $\mathcal{I}$ the ideal $\langle p_1, \dots, p_m \rangle$. Let $\mathcal{R} = (r_1, \dots, r_m)$ be a generic collection of quadratic polynomials in n variables. Denote by $\mathcal{J}$ the ideal $\langle r_1, \dots, r_m \rangle$. Then it holds that $\dim V(\mathcal{I}) > \dim V(\mathcal{J})$.*

Proof. By Definition 2, the variety $V(\mathcal{I})$ contains the secret subspace $\mathcal{O}$ of dimension o. Thus, $\dim V(\mathcal{I}) \geq o$. However, if $n - m \geq 0$, then $V(\mathcal{J})$ has dimension $n - m$, which is less than o by assumption. If $n - m < 0$, $V(\mathcal{J})$ is empty. In any case,

$$\dim V(\mathcal{I}) > \dim V(\mathcal{J}).$$

In other words, the dimension of $V(\mathcal{I})$ distinguishes a UOV instance with $n - m < o$ from a collection of generic polynomials in $\mathbb{F}_q[X_1, \dots, X_n]_2$. □

From the previous lemma, we obtain a distinguisher between a UOV variety with $n - m < o$ and a semi-regular sequence based on the dimension of the variety. To obtain a key recovery attack, we compute points in $\mathcal{O}$ by intersecting $V(\mathcal{I})$ with random hyperplanes. Under the following hypothesis, all solutions of such a system of polynomial equations are in $\mathcal{O}$, thus Lemma 1 implies that the direct attack against $\mathcal{P}$ targeting the vector $(0, \dots, 0) \in \mathbb{F}_q^m$ is a key recovery attack.

Hypothesis 1. *Let $\mathcal{P} = (p_1, \dots, p_m)$ be a UOV public key for parameters (n, m, o, q) such that $n - m < o$. Denote by $\mathcal{I}$ the ideal $\langle p_1, \dots, p_m \rangle$ and by $\mathcal{O}$ the secret subspace $\mathcal{O} \subset V(\mathcal{I})$. Then $\mathcal{O}$ is the component of highest dimension of $V(\mathcal{I})$.*

In practice, this hypothesis is verified: we observe the absence of parasitic solutions (components of $V(\mathcal{I})$ of maximal dimension which do not belong to $\mathcal{O}$). We conjecture that this is a generic property of the systems we consider, and leave to further work the proof of this fact in the framework of Zariski topology.

2.2 Direct attack as a key recovery attack against VOX

In this section, we adapt Lemma 1 to the case of VOX, where random polynomials of degree two are involved, and study the hardness of performing this attack. This has two consequences: first, we enable an alternative geometric cryptanalysis of the initial VOX parameters. Second, we obtain a criterion which will allow us to identify subfields in which the VOX subinstances are exposed to a direct key recovery attack.

Lemma 2. *Let $\mathcal{P}$ be a UOV$\hat{+}$ public key for parameters (n, m, o, q, t) and write $\mathcal{P} = (p_1, \dots, p_m)$. Let $\mathcal{I} = \langle p_1, \dots, p_m \rangle$. If $o - t > 0$ and $n - m < o - t$, under Hypothesis 1, then the secret key of $\mathcal{P}$ can be computed by finding a point in the component of highest dimension of $V(\mathcal{I})$. This can be achieved by solving a polynomial system of m quadratic equations in $n - o + t$ variables.*

Proof. Let $\hat{\mathcal{P}} = (\hat{p}_{t+1}, \ldots, \hat{p}_m)$ be the underlying UOV instance, for parameters $(n, m-t, o, q)$. Define the underlying UOV variety:

$$V(\hat{\mathcal{I}}) = \{\boldsymbol{x} \in (\mathbb{F}_q)^n, \hat{p}_{t+1}(\boldsymbol{x}) = \cdots = \hat{p}_m(\boldsymbol{x}) = 0\}.$$

This variety is not empty, as there exists by Definition 2 a linear subspace $\mathcal{O}$ of $\mathbb{F}_q^n$ of dimension o such that $\mathcal{O} \subseteq V(\hat{\mathcal{I}})$. Define the UOV$\hat{+}$ variety:

$$V(\mathcal{I}) = \{\boldsymbol{x} \in (\mathbb{F}_q)^n, p_1(\boldsymbol{x}) = \cdots = p_m(\boldsymbol{x}) = 0\}.$$

Let $\hat{\mathcal{F}} = (\hat{f}_{t+1}, \ldots, \hat{f}_m) = \mathcal{P} \circ A^{-1}$ be the underlying algebraic UOV secret key. Denote by $\mathcal{F} = \boldsymbol{x} \mapsto (p_1(\boldsymbol{x}), \ldots, p_t(\boldsymbol{x}), \hat{f}_{t+1}(\boldsymbol{x}), \ldots, \hat{f}_m(\boldsymbol{x}))$ the quadratic map obtained by concatenating $\hat{\mathcal{F}}$ with the random polynomials $p_1, \ldots, p_t$. Algebraically, we have

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

The geometry remains simple. Indeed, $V(\mathcal{I})$ is the intersection of $V(\hat{\mathcal{I}})$ with t quadric hypersurfaces defined by $p_1 = \cdots = p_t = 0$. Therefore, if $\dim V(\hat{\mathcal{I}}) = d$ and if $d - t \geq 0$, by genericity of $p_1, \ldots, p_t$,

$$\dim V(\mathcal{I}) = d - t. \tag{6}$$

Note that, in general, $d = \max(n - m + t, o)$. If $d - t$ is negative or equal to zero, then $V(\mathcal{I})$ is empty in projective space (since the systems are homogeneous, 0 is always a solution, but not a useful one in cryptanalysis).

Denote by $W = V(\langle p_1, \ldots, p_t \rangle)$. By assumption, it holds that $o - t > 0$ and $n - m + t < o$. Thus, $d = o$ and the underlying UOV key is irregular: it is distinguished from a generic variety defined by m quadratic polynomials by Lemma 1. Under Hypothesis 1, $\mathcal{O} \cap W$ is the component of largest dimension of $V(\mathcal{I})$. By choosing $h_1 = X_1 - 1$ to dehomogenize and $h_2, \ldots, h_{o-t} \in \mathbb{F}_q[X_1, \ldots, X_n]_1$ generic linear polynomials, we have

$$V(\mathcal{I} + \langle h_1, \ldots, h_{o-t} \rangle) \subset \mathcal{O}.$$

Furthermore, by definition of dimension, the affine variety $V(\mathcal{I} + \langle h_1, \ldots, h_{o-t} \rangle)$ has dimension 0. Therefore, we obtain a key recovery attack on the scheme by using any solving algorithm to compute the variety of the ideal $\mathcal{I} + \langle h_1, \ldots, h_{o-t} \rangle$. Using the $o - t$ linear polynomials to eliminate $o - t$ variables, we obtain a polynomial system in m quadratic equations and $n - (o - t)$ variables. □

In the next remark, we compare this polynomial system with a semi-regular sequence with the same number of variables and polynomials.

Remark 2. Consider a semi-regular polynomial system of m equations of degree two in $n - o + t$ variables. The degree of regularity d_{reg} of a semi-regular sequence is found as the first non-positive coefficient in the Hilbert Series:

$$H(z) = \frac{(1 - z^2)^m}{(1 - z)^{n-o+t}}$$

We estimate the cost of computing a grevlex Gröbner basis for such a sequence using [BFS15, Proposition 1].

$$O\left(m \cdot d_{\text{reg}} \binom{n - o + t + d_{\text{reg}} - 1}{d_{\text{reg}}}^{\omega}\right) \tag{7}$$

Following NIST methodology, an arithmetic operation in $\mathbb{F}_q$ is assumed to be equal to $2\log_2(q)^2 + \log_2(q)$ gates.

Remark 3. We have proven that systems that stem from VOX public keys are not regular (as they are not complete intersections due to the existence of $\mathcal{O}$, see Section 1.2). Thus, the polynomial systems we obtain in Lemma 2 may not form semi-regular sequences.

We observe experimentally that the Gröbner basis computations in our setting display no degree fall until the degree d_{reg} computed in Remark 2. At this stage, a degree fall is observed. The subsequent computations, although involving polynomials of degree larger than d_{reg}, have a negligible runtime compared to the prior computations. Therefore, we heuristically use the cost of solving semi-regular polynomial systems from Remark 2 as an indication towards the cost of attacking the VOX subfield instances. Note that this is not a bound on the cost of the Gröbner basis computation, and is only used as an indication of the cost of an attack. We are able to practically solve all the polynomial systems for which we use this indication in Section 3.2, and we observe that it is an overestimation of the cost of our attack.

As we noted that $V(\mathcal{I} + \langle h_1, \dots, h_{o-t} \rangle) \subset \mathcal{O}$, we expect that the grevlex Gröbner bases we compute contain linear polynomials. We obtain a subset of $\mathcal{O}$ by computing the kernel of said linear polynomials.

We apply this attack to the big field instance of QR-UOV$\hat{+}$, which is a UOV$\hat{+}$ instance with parameters $(n, \ell m, m, q^\ell, t)$. The conditions for the success of the attack are found by instantiating Lemma 2 with these parameters:

$$m - t > 0 \text{ and } n - (\ell + 1)m + t < 0. \tag{8}$$

These conditions are satisfied for all the initial VOX parameter sets [CFF+23b]. Notice that the conditions of Equation (8) are also required to perform the rectangular MinRank attack of Furue and Ikematsu [FI23a, FI23b]. One can choose m such that $m \leq t$ and the UOV$\hat{+}$ variety does not intersect $\mathcal{O}$ in $\mathbb{F}_{q^\ell}$, in which case we are unable to attack the UOV$\hat{+}$ instance $(n, \ell m, m, q^\ell, t)$ without inverting S. Thus, the attack presented in this section is defeated by the parameters of VOX proposed in [MRPC+23] to defeat the attack of Furue and Ikematsu [FI23a, FI23b].

3 Subfield attack

In this section, we adapt our attack when ℓ is composite, which applies to a subset of the parameters proposed for VOX in [MRPC+23], where it is imposed that $m \leq t$. We rely on the existence of intermediate subfields of $\mathbb{F}_{q^\ell}$, i.e. different from $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$, in which the hypotheses of Lemma 2 are verified.

3.1 Factoring the QR parameter

We use the following classical result to target subfield instances of the VOX key recovery problem, interpreted as QR-UOV$\hat{+}$. If ℓ' divides ℓ, then $\mathbb{F}_{q^\ell}$ is a field extension of degree $\frac{\ell}{\ell'}$ of $\mathbb{F}_{q^{\ell'}}$ [Lan02, Chapter V, Section 6, Theorem 5.5]. This yields the following observation.

Remark 4. Let (n, m, o, q, t, ℓ) be QR-UOV$\hat{+}$ parameters. If ℓ' divides ℓ, then it holds that a QR-UOV$\hat{+}$ instance for parameters (n, m, o, q, t, ℓ) is also a QR-UOV$\hat{+}$ instance for parameters $(\ell' n, \ell' m, \ell' o, q^{\ell'}, t, \frac{\ell}{\ell'})$.

Denote by $\ell_1, \dots, \ell_r$ the proper factors of ℓ (those different from 1 or ℓ). In other words, a QR-UOV$\hat{+}$ instance is secure only if the following UOV$\hat{+}$ sub-instances are secure:

- UOV$\hat{+}$ for parameters $(\ell n, \ell m, \ell o, q^1, t)$.
- UOV$\hat{+}$ for parameters $(\frac{\ell}{\ell_1} n, \ell m, \frac{\ell}{\ell_1} o, q^{\ell_1}, t)$.

$$\vdots$$

- UOV$\hat{+}$ for parameters $(\frac{\ell}{\ell_r}n, \ell m, \frac{\ell}{\ell_r}o, q^{\ell_r}, t)$.
- UOV$\hat{+}$ for parameters $(n, \ell m, o, q^{\ell}, t)$.

This also holds for QR-UOV.

Notice that the security analysis of QR-UOV [FIKT21] (see Section 1.3) focuses on the special cases $\ell' = 1$ and $\ell' = \ell$, and indeed the subfield instances do not seem to have much interest in the study of QR-UOV itself, as all algebraic attacks that apply in a subfield would also apply in the largest field, and feature more variables than in the largest field. However, for VOX, Remark 4 allows us to apply the attack of Lemma 2 on intermediate fields, while the attack would fail in the largest field $\mathbb{F}_{q^\ell}$.

Notice that in the sequence of instances of Remark 4, the number of variables is inversely proportional to the size of the field:

$$\mathbb{F}_q \to \ell n, \quad \mathbb{F}_{q^{\ell_1}} \to \frac{\ell}{\ell_1} n, \quad \ldots, \quad \mathbb{F}_{q^\ell} \to n.$$

On the other hand, the number of polynomials is constant and equal to ℓm. Thus, the larger the field, the more overdetermined the instances. This significantly affects the complexity of Gröbner basis algorithms (see [BFS05, BFP09, BFS15]). Therefore, the preferred subfield for our attack is the largest subfield in which Lemma 2 applies, which corresponds to the largest divisor $\ell' | \ell$ such that $\frac{\ell}{\ell'} o > t$.

Notice that this attack is only able to target the parameters Ic, IIIa, Vb of the NIST submission [MRPC+23], since for all other parameter sets, ℓ is prime. For parameter sets I, III, V, the attack applies in the large field $\mathbb{F}_{q^\ell}$ without using an intermediate field, as noted in the previous section.

3.2 Performing the attack

We recall in Figure 1 the initial VOX parameter sets [CFF+23b] (I, III, V), and the alternative parameter sets proposed in [MRPC+23] (*a, *b, *c). In all cases, $o = m$. The attack applies to the parameter sets with ℓ in bold.

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

Figure 1: VOX parameters sets (I, III, V) submitted to NIST [CFF+23b] and alternative parameters (*a, *b, *c) [MRPC+23].

We evaluate the cost of the attack for the largest suitable factor of ℓ, as noted previously. Figure 2 gives the estimate of the cost of solving a comparable semi-regular system, along with the practical results for VOX systems. We began by generating random instances of the corresponding UOV$\hat{+}$ instances for parameters $(\frac{\ell}{\ell'}n, \ell m, \frac{\ell}{\ell'}m, q^{\ell'}, t)$ in SageMath,

and solved them using msolve [BES21] on a laptop with an Intel i7-1165G7 CPU running at 2.80GHz with 1 thread and 8 GB of RAM. Parameter sets that are omitted are not concerned by the attack.

Parameter set	Security level	ℓ	ℓ'	$\log_2$ gates	CPU time
I	143	6	6	38.1	0.03s
Ic	143	9	3	71.0	400h*
III	192	7	7	41.2	0.11s
IIIa	192	15	5	55.4	83.4s
V	272	8	8	43.7	0.32s
Vb	272	14	7	54.6	12.4s

Figure 2: Gate counts for the intermediate field attack on QR-UOV$\hat{+}$ and practical results on an Intel i7-1165G7 CPU running at 2.80GHz. A * indicates that the experiment was run on an Intel Xeon CPU E7-4820 running at 2.00GHz.

The msolve library was called with the option $-$g 2, which returns a grevlex Gröbner basis, as we require the linear polynomials in the Gröbner basis to perform the key recovery attack. The threading parameter is the default $-$t 1, meaning a single thread is used. From the logs of the solver, one can check that the linear polynomials appear early in the computation, thus one could stop the computation early to marginally improve the practical results (this would save 1 second on the IIIa reported time in Figure 2). This supports the comparison with semi-regular polynomial systems proposed in Remark 2.

Our comparison with semi-regular systems of polynomial equations suggests that the instances corresponding to the parameter set Ic are 2^{16} times harder to solve than those of IIIa. Thus, the experiments for parameter set Ic were performed on a server, with threading enabled via $-$t 24. We point out that this does not divide the wall time by 24, as only the linear algebra steps benefit from extra threads. The CPU used was an Intel Xeon CPU E7-4820 running at 2.00GHz, and the RAM usage peaked at 54.3GB.

We note that while the bit complexity estimates concern semi-regular systems, the linear polynomials in the Gröbner bases appear below the predicted degree of regularity, and before any degree falls. Notice also that the complexity growth is overestimated by Equation (7). For example, between parameter sets I and III, the predicted growth is $\approx 2^3 = 8$, while experimentally (see Figure 2), we obtain only a factor 4 increase. Similar observations can be made for all other parameter sets, and in particular for Ic which should have required $10^{4.8}$ CPU-hours by extrapolating the cost of attacking parameter set IIIa.

3.3 MinRank attack on VOX

In [GD24, GJP+24], a MinRank attack is introduced that also targets the alternative parameters proposed for VOX. The attack is practical and breaks all of the alternative parameters sets proposed for VOX under 2^{58} arithmetic operations.

The attack of Guo and Ding does not exploit the same vulnerability we exploit in Section 2.2. In particular, they target all parameter sets, while our attack only targets the parameter sets with composite ℓ. Guo and Ding also propose alternative parameters for VOX to improve the security of the scheme against their MinRank attack. We recall these possible parameters and their expected security in Figure 3.

q, t	Parameter set	m, $n-m$, ℓ	Security ($\log_2$ ops)
251, 6	GD-Ia	4, 7, 13	78.1
	GD-Ib	5, 9, 11	99.8
	GD-Ic	6, 11, 9	134
1021, 7	GD-IIIa	5, 9, 15	85
	GD-IIIb	6, 11, 13	101.5
	GD-IIIc	7, 13, 11	129.55
4093, 8	GD-Va	6, 11, 17	90.6
	GD-Vb	7, 13, 14	113.7
	GD-Vc	8, 15, 13	130.6

Figure 3: Alternative VOX parameters proposed in [GD24].

To illustrate the difference in our approach, notice that our attack applies to the subset of these new parameters where ℓ is composite. We detail the cost in arithmetic operations to match the estimates in [GD24].

Parameter set	ℓ	ℓ'	$\log_2$ ops	Previous [GD24]
GD-Ic	9	3	**99.7**	134
GD-IIIa	15	5	**62.1**	85
GD-Vb	14	7	**54.3**	113.7

Figure 4: Binary operation counts for the intermediate field attack on some VOX parameters proposed in [GD24].

While our attack lacks the generality of the attack of Guo and Ding, it may outperform it on well-chosen parameter sets.

3.4 VOX Minus

The UOV$\hat{+}$ signature scheme results from the application of a "perturbation" to the UOV scheme. The application of perturbations (transformations applied to a polynomial map) to multivariate cryptosystems is a method that was used to improve the performance or security of the HFE cryptosystem (see for example [Pat96, PCY+15]). Varjabedian [Var25] proposed to apply another perturbation to QR-UOV schemes, and in particular to VOX, the minus perturbation, which consists in removing polynomials from the public key. This is akin to the transformation applied in PrOV (see [CFF+23a]). Our work directly applies to VOX minus, as we distinguish the values of m and o.

In the initial version of VOX Minus [Var25], published on the IACR eprint archive, the security analysis in the field extension $\mathbb{F}_{q^\ell}$ and in subfields was omitted, as in [CFF+23b]. Thus, the parameters proposed in the initial version were insecure, and could be attacked with similar performance as parameter sets I, III, V in Figure 2. This weakness was patched in a revision, based on our comments.

3.5 Countermeasures

The simplest countermeasure to our attack is to use a QR parameter ℓ that is prime. Alternatively, one should take into account subfield attacks in the security analysis of a small field/big field multivariate scheme.

Acknowledgements

This work is supported by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02. The author would like to thank Simon Abelard, Mohab Safey el Din, Alain Couvreur, Daniel Smith-Tone and Ward Beullens for their comments on earlier versions of this paper.

References

[BCC+25] Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. Mayo, NIST round 2, 2025. https://pqmayo.org/assets/specs/mayo-round2.pdf, consulted 06/06/2025.

[BCD+23] 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, 2023. uovsig.org, consulted 05/10/2023.

[BES21] Jérémy Berthomieu, Christian Eder, and Mohab Safey El Din. msolve: A library for solving polynomial systems. In Frédéric Chyzak and George Labahn, editors, *ISSAC '21: International Symposium on Symbolic and Algebraic Computation, Virtual Event, Russia, July 18-23, 2021*, pages 51–58. ACM, 2021. doi:10.1145/3452143.3465545.

[Beu21] Ward Beullens. MAYO: practical post-quantum signatures from oil-and-vinegar maps. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers*, volume 13203 of *Lecture Notes in Computer Science*, pages 355–376. Springer, 2021. doi:10.1007/978-3-030-99277-4_17.

[BFP09] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *J. Math. Cryptol.*, 3(3):177–197, 2009. doi:10.1515/JMC.2009.009.

[BFS05] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. Asymptotic Behaviour of the Index of Regularity of Semi-Regular Quadratic Polynomial Systems. In *MEGA 2005 - 8th International Symposium on Effective Methods in Algebraic Geometry*, pages 1–17, Porto Conte, Alghero, Sardinia, Italy, May 2005. URL: https://hal.science/hal-01486845.

[BFS15] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the f5 gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015. URL: https://www.sciencedirect.com/science/article/pii/S0747717114000935, doi:10.1016/j.jsc.2014.09.025.

[CFF+23a] Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, Brice Minaud, and Jacques Patarin. Provable unbalanced oil and vinegar, 2023. http://prov-sign.github.io, consulted 05/10/2023.

[CFF+23b] Benoît Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, Brice Minaud, and Jacques Patarin. Vox-sign, 2023. http://vox-sign.com/files/vox_nist.pdf, consulted 05/10/2023.

[CKPS00] 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 Berlin Heidelberg. doi:10.1007/3-540-45539-6_27.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Publishing Company, Incorporated, 4th edition, 2015. doi:10.1007/978-3-031-91841-4.

[DM98] Olivier Debarre and Laurent Manivel. Sur la variété des espaces linéaires contenus dans une intersection complète. *Math. Annalen 312 (1998), 549-574*, 1998. doi:10.1007/s002080050235.

[Fau99] Jean-Charles Faugère. A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 139(1):61–88, 1999. URL: https://www.sciencedirect.com/science/article/pii/S0022404999000055, doi:10.1016/S0022-4049(99)00005-5.

[Fau02] Jean Charles Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, page 75–83, New York, NY, USA, 2002. Association for Computing Machinery. doi:10.1145/780506.780516.

[FGLM93] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993. URL: https://www.sciencedirect.com/science/article/pii/S0747717183710515, doi:10.1006/jsco.1993.1051.

[FI23a] Hiroki Furue and Yasuhiko Ikematsu. A new security analysis against MAYO and QR-UOV using rectangular MinRank attack. In Junji Shikata and Hiroki Kuzuno, editors, *IWSEC 23: 18th International Workshop on Security, Advances in Information and Computer Security*, volume 14128 of *Lecture Notes in Computer Science*, pages 101–116, Yokohama, Japan, August 29–31, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-41326-1_6.

[FI23b] Hiroki Furue and Yasuhiko Ikematsu. Vox round 1 - official comment, 2023. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/VOX-round1-dig-sig-official-comment.pdf, consulted 20/08/2025.

[FIH+23] Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi, Kan Yasuda, Toshiyuki Miyazawa, Tsunekazu Saito, and Akira Nagai. QR-UOV specification, 2023. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/qruov-spec-web.pdf, consulted 08/02/2024.

[FIKT21] Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 187–217, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-92068-5_7.

[FKI+20] Hiroki Furue, Koha Kinjo, Yasuhiko Ikematsu, Yacheng Wang, and Tsuyoshi Takagi. A structural attack on block-anti-circulant uov at sac 2019. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 323–339, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-44223-1_18.

[FMPP22] Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. A new perturbation for multivariate public key schemes such as HFE andUOV. Cryptology ePrint Archive, Paper 2022/203, 2022. https://eprint.iacr.org/2022/203.

[GD24] Hao Guo and Jintai Ding. A practical minrank attack against vox. Cryptology ePrint Archive, Paper 2024/166, 2024. https://eprint.iacr.org/2024/166.

[GJP+24] Hao Guo, Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong, and Jintai Ding. Practical and theoretical cryptanalysis of vox. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography*, pages 186–208, Cham, 2024. Springer Nature Switzerland. doi:10.1007/978-3-031-62746-0_9.

[Has23] Yasufumi Hashimoto. An improvement of algorithms to solve under-defined systems of multivariate quadratic equations. *JSIAM Letters*, 15:53–56, 2023. doi:10.14495/jsiaml.15.53.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999. doi:10.1007/3-540-48910-X_15.

[KS98] Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil & vinegar signature scheme. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Springer, 1998. doi:10.1007/BFb0055733.

[Lan02] Serge Lang. *Algebra*. Springer, New York, NY, 2002. doi:10.1007/978-1-4613-0041-0.

[Laz83] D. Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Computer Algebra*, pages 146–156, Berlin, Heidelberg, 1983. Springer Berlin Heidelberg. doi:10.1007/3-540-12868-9_99.

[Luy23] Pieter Luyten. Understanding Kipnis Shamir with two quadrics. Master thesis, KU Leuven, 2023.

[MRPC+23] Gilles Macario-Rat, Jacques Patarin, Benoit Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Gouin, Robin Larrieu, and Brice Minaud. Rectangular attack on VOX. Cryptology ePrint Archive, Paper 2023/1822, 2023. https://eprint.iacr.org/2023/1822.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 33–48, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg. doi:10.1007/3-540-68339-9_4.

[Pat97] Jacques Patarin. The oil and vinegar signature scheme. In *Dagstuhl Workshop on Cryptography September, 1997*, 1997.

[PCY+15] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev- based multivariate signature schemes. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 311–334, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg. doi:10.1007/978-3-662-48797-6_14.

[Péb25] Pierre Pébereau. Singular points of UOV and VOX. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VI*, volume 15606 of *Lecture Notes in Computer Science*, pages 294–323. Springer, 2025. doi:10.1007/978-3-031-91095-1_11.

[SP20] Alan Szepieniec and Bart Preneel. Block-anti-circulant unbalanced oil and vinegar. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography – SAC 2019*, pages 574–588, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-38471-5_23.

[TW12] Enrico Thomae and Christopher Wolf. Solving underdetermined systems of multivariate quadratic equations revisited. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, volume 7293 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2012. doi:10.1007/978-3-642-30057-8_10.

[Var25] Pierre Varjabedian. Improvements on the schemes VOX and QR UOV when minus is a plus. Cryptology ePrint Archive, Paper 2025/842, 2025. URL: https://eprint.iacr.org/2025/842.

[WCD+25] Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang. SNOVA, 2025. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf, consulted 29/08/2025.