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

Pierre Pébereau

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

Pierre Pébereau

Sorbonne Université, LIP6, CNRS
Thales SIX
pierre.pebereau@lip6.fr

Abstract. In this note, we show that some of the parameters of the Quotient-Ring transform proposed for VOX are vulnerable. More precisely, they were chosen to defeat an attack in the field extension $\mathbb{F}_{q^l}$ obtained by quotienting $\mathbb{F}_q[X]$ by an irreducible polynomial of degree l. We observe that we may use a smaller extension $\mathbb{F}_{q^{l'}}$ for any $l'|l$, in which case the attacks apply again. We also introduce a simple algebraic attack without the use of the MinRank problem to attack the scheme. These attacks concern a subset of the parameter sets proposed for VOX: I, Ic, III, IIIa, V, Vb. 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, our attack requires $0.3s, 1.35s, 0.56s$ for parameter sets I,III,V for VOX [1], and $56.7s, 6.11s$ for parameter sets IIIa, Vb [2].

Notations

Let $q = p^e$ for p prime and let $\mathbb{F}_q$ denote the finite field of characteristic p with q elements. Vectors are assumed to be column vectors and are denoted by bold letters: $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{o}, \ldots$. Matrices are denoted by capital letters, and transposition is written A^T. Given a field $\mathbb{F}$ and an integer n, we denote $\mathbb{F}[x_1, \ldots, x_n]$ or $\mathbb{F}[\boldsymbol{x}]$ the polynomial ring of $\mathbb{F}$ in n indeterminates. The restriction of a function f to a set E is denoted $f_{|E}$.

Unbalanced oil and vinegar

A UOV key pair for parameters (n, m, q) is composed of a secret key $(A, \mathcal{F})$ and a public key $\mathcal{P}$, with:

- $A \in GL_n(\mathbb{F}_q)$
- $\mathcal{F} = (F_1, \ldots, F_m)$ a quadratic map with $F_i(\boldsymbol{e}_j) = 0$ for all i and for $j \leq m$
- $\mathcal{P} = \mathcal{F} \circ A$ a quadratic map

If we represent the quadratic maps with matrices, we have:

$$\forall 1 \leq i \leq m, F_i = \begin{pmatrix} 0 & F_i^{(1)} \\ F_i^{(2)} & F_i^{(3)} \end{pmatrix}$$

This formulation was introduced by Patarin in [3] and the original motivation was that the system $\mathcal{F}(\boldsymbol{x}) = \boldsymbol{t}$ is linear in $x_1, \ldots, x_m$. These variables are distinguished from the rest of variables and are named "oil variables". The remaining ones are "vinegar variables". The knowledge of A allows the signer to efficiently solve $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}$ using this property. The set of accepted signatures for a message $\boldsymbol{t} \in \mathbb{F}_q^m$, noted $\mathbb{V}(\boldsymbol{t}) = \{\boldsymbol{x} \in \mathbb{F}_q^n, \mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}\}$, is an algebraic variety of dimension $n - m$ generically.

1 VOX

VOX is a signature scheme submitted to the NIST alternative signature round [1]. It relies on the same core principles as UOV, but adds "noise" to the public key to hide the structure of the UOV trapdoor. VOX also relies on additional structure, the QR-transform [4], which is akin to the construction of structured lattices. We view VOX as "QR-UOV$^{\hat{+}}$".

1.1 UOV$^{\hat{+}}$

We start by defining UOV$^{\hat{+}}$. A UOV$^{\hat{+}}$ key pair for parameters (o, v, t, q) is composed of a secret key $(S, A, \mathcal{F})$ and a public key $\mathcal{P}$, with:

- $A \in GL_{o+v}(\mathbb{F}_q)$
- $S = \begin{pmatrix} I_t & S' \\ 0 & I_{o-t} \end{pmatrix}, \quad S' \in \mathbb{F}_q^{(o-t)\times t}, S \in GL_o(\mathbb{F}_q)$
- $\mathcal{F} = (F_1, \ldots, F_o)$ a quadratic map with $F_i(\boldsymbol{e}_j) = 0$ for $i > t$ and $j \leq o$.
- $\mathcal{P} = S^{-1} \circ \mathcal{F} \circ A$ a quadratic map

We will write $n = o+v$ and let $\hat{\mathcal{F}} = (F_{t+1}, \ldots, F_o)$ be the "VOX oil polynomials".

Variant	Security level	q	o/c	v/c	c	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	

Fig. 1: VOX parameters sets submitted to NIST [1] and alternative parameters [2].

1.2 QR-UOV and security assumptions

In [4], the authors introduce a way to reduce key sizes for UOV by representing a UOV public key using structured matrices. Essentially, the scheme may be considered as a "block matrix" variant of UOV, where the matrices in the key pair are block matrices with elements belonging to a matrix ring $\mathbb{F}_q^{l\times l}$. To achieve a gain in performance, we consider the quotient ring $\mathcal{R} = \mathbb{F}_q[x]/(f)$, where $deg(f) = l$, and embed it in $\mathbb{F}_q^{l\times l}$ using an injective ring homomorphism. We will call the integer l the "QR parameter". Not every choice of f will lead to a secure scheme, as observed by the authors of QR-UOV (a subset of the authors had previously attacked a similar construction called BAC-UOV, see [5] and [6]). In short, f must be irreducible to ensure the security of the schemes, and in this case notice that $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^l}$.

The security assumptions highlighted by the authors of [4] are the following: An instance of QR-UOV for parameters (q, v, m, l) is secure only if two (generalized) UOV instances are secure:

1. UOV$(q^l, \frac{v}{l}, \frac{m}{l}, m)$, a UOV$(q^l, \frac{v}{l}, \frac{m}{l})$ instance with m equations instead of $\frac{m}{l}$
2. UOV(q, v, m), a plain UOV instance.

1.3 Analysis of QR-UOV$^{\hat{+}}$

The same reduction applies to VOX when interpreted as QR-UOV$^{\hat{+}}$. In [1], the parameter l is noted c. We keep the original notation l in the following. An instance of QR-UOV$^{\hat{+}}$ for parameters (q, v, o, l, t) is secure only if two (generalized) UOV$^{\hat{+}}$ instances are secure:

1. UOV$^{\hat{+}}(q^l, \frac{v}{l}, \frac{o}{l}, o, t)$, a UOV$^{\hat{+}}(q^l, \frac{v}{l}, \frac{o}{l}, t)$ instance with o equations.
2. UOV$^{\hat{+}}(q, v, o, t)$, a plain UOV$^{\hat{+}}$ instance.

Let $N = \frac{v+o}{l}$, $O = \frac{o}{l}$, $V = \frac{v}{l}$. Let $(P_1, \ldots, P_o)$ be a UOV$^{\hat{+}}(q^l, V, O, o, t)$ instance. Let $I = \langle p_1(\boldsymbol{x}), \ldots, p_o(\boldsymbol{x})\rangle$ the ideal generated by the corresponding system of equations. Let $(\hat{P}_{t+1}, \ldots, \hat{P}_o)$ be the underlying UOV(q^l, V, O, o) instance.
Define the underlying UOV variety:

$$\mathbb{V}(\hat{I}) = \{\boldsymbol{x} \in (\mathbb{F}_{q^l})^N, \boldsymbol{x}^T\hat{P}_{t+1}\boldsymbol{x} = \ldots = \boldsymbol{x}^T\hat{P}_o\boldsymbol{x} = 0\}$$

This variety may be defined by an overdetermined system of quadratic equations, but it is never empty as $\mathcal{O} \subseteq \mathbb{V}(\hat{I})$. When $o > N$, this inclusion is generically an equality. Define the UOV$^{\hat{+}}$ variety:

$$\mathbb{V}(I) = \{\boldsymbol{x} \in (\mathbb{F}_{q^l})^N, \boldsymbol{x}^T P_1\boldsymbol{x} = \ldots = \boldsymbol{x}^T P_o\boldsymbol{x} = 0\}$$

Notice that this variety is the intersection of $\mathbb{V}(\hat{I})$ with t generic quadratic hypersurfaces defined by $p_1(\boldsymbol{x}) = 0, \ldots, p_t(\boldsymbol{x}) = 0$. Therefore, if $\dim \mathbb{V}(\hat{I}) = d$, then we expect, if $d - t \geq 0$, that $\dim \mathbb{V}(I) = d - t$. If this quantity is negative, then $\mathbb{V}(I)$ is empty.

The interesting case is when $o > N$ and $O - t > 0$. Then $\mathbb{V}(I)$ is not empty and $\mathbb{V}(I) \subset \mathcal{O}$. If I is radical, this implies in particular that the linear equations defining $\mathcal{O}$ belong to I. Therefore, they must belong to a Gröbner basis of the ideal for a graded monomial ordering. We summarize this in Proposition 1.

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

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

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

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

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

$$\langle LT_{\leq}(g_1), \ldots, LT_{\leq}(g_t) \rangle = \langle LT_{\leq}(I) \rangle$$

This implies that a Gröbner basis of I must contain polynomials whose leading terms are of minimal degree, in our case 1. The collection of linear equations included in a Gröbner basis must have rank at least $n - o$, otherwise we could find a linear equation in I linearily independant from the ones in the basis. We add that in the reduced Gröbner basis for $\leq$, there are only independant linear equations. □

The ideal generated by a general collection of polynomials is radical as a consequence of the theorem of Bertini. Since UOV polynomials are certainly not generic, it is not obvious that the ideal generated by a UOV public key is radical. Experimentally, we observe that the systems we obtain define radical ideals, hence we use the previous result.

Using Proposition 1, we mount a key recovery attack on the scheme by computing a grevlex Gröbner basis of the ideal generated by the system $\mathcal{P}(\boldsymbol{x}) = 0$.

$$\boldsymbol{x} =\in \mathbb{F}_q^N \text{ such that } \begin{cases} P_1(\boldsymbol{x}) = 0 \\ \vdots \\ P_o(\boldsymbol{x}) = 0 \end{cases} \tag{1}$$

Assuming semi-regularity, the degree of regularity d_{reg} is found as the first non-positive coefficient in the Hilbert Series:

$$H_{\mathcal{R}/I}(t) = \frac{(1-t^2)^o}{(1-t)^N}$$

Therefore, if $O - t > 0$ and $N < o$, using dense linear algebra with a matrix multiplication cost identified as $O(n^\omega)$ arithmetic operations, we upper bound the number of arithmetic operations required by our attack by

$$O\left(\binom{N + d_{reg}}{d_{reg}}^\omega\right) \tag{2}$$

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

Once a Gröbner basis has been computed, we retrieve the linear terms, and dismiss the remaining higher degree polynomials. This directly applies to the initial VOX parameter sets, and exploits the same fault as the rectangular MinRank attack of Furue and Ikematsu [7], namely $O > t$.

We describe in the next section a trick to attack a subset of the new parameters proposed for VOX in [2] when l is a composite number. We expect the Rectangular MinRank attack of Furue and Ikematsu [7] to also apply in this case.

Factoring the QR parameter The previous paragraph showed that manipulating the equations of the QR-UOV$^{\hat{+}}$ instance may be more tricky due to the fact that we keep the same number of vinegar equations but have a smaller subspace $\mathcal{O}$ when working in the extension $\mathbb{F}_{q^l}$. Therefore, if l is large, then $\frac{o}{l} < t$ and there is no intersection between $\mathcal{O}$ and the (generic) vinegar variety, which means that we are unable to attack the UOV$^{\hat{+}}$ instance (q^l, V, O, t, m) without inverting S. This happens for the VOX parameters proposed in [2] precisely because the inequality $O > t$ enabled the rectangular MinRank attack on the scheme, therefore the opposite was enforced to defeat it.

We use the following trick to bypass this obstacle in some instances of VOX: if l' divides l, then $\mathbb{F}_{q^l}$ is a field extension of degree $\frac{l}{l'}$ of $\mathbb{F}_{q^{l'}}$.

Remark 1. If l' divides l, we may interpret a QR-UOV$^{\hat{+}}$ instance for parameters (q, v, m, l) as a QR-UOV$^{\hat{+}}$ instance for parameters (q, v, m, l'). This holds also for QR-UOV.

For VOX, it enables the simple attack described in Equation (1) on intermediate fields for QR-UOV$^{\hat{+}}$, while the attack would fail in the field q^l because of the dimension considerations. In Figure 1, the attack applies to the parameter sets with c in bold. The best complexity will be obtained by minimizing the number of variables, therefore we choose the largest divisor l' of l such that $\frac{o}{l'} > t$. Notice that this attack will only be able to target the parameters Ic, IIIa, Vb, since for all other parameter sets, l is prime. For parameter sets I,III,V, the attack applies in the large field $\mathbb{F}_{q^l}$ without using an intermediate field.

Performing the attack We evaluate the attack for the largest admissible factor of l. Figure 2 gives the estimation for the VOX parameters submitted to

NIST, and for the parameters proposed in [2]. We generate random instances of the corresponding $\text{UOV}^{\hat{+}}(q^{l'}, \frac{v}{l'}, \frac{o}{l'}, o, t)$ scheme, and solve them using msolve [8] on a laptop with an i7-1165G7 CPU running at 2.80GHz with 8 cores and 8 GB of RAM. Parameter sets that are omitted are not concerned by the attack. Notice that the variety $\mathbb{V}(I)$ is zero-dimensional in case $t = O$. In this case, we believe that the attack does not applies in the large field $\mathbb{F}_{q^l}$, because the only solution of the homogeneous system is $(0, \ldots, 0)$.

Parameter set	l	l'	$\log_2$ gates	msolve time (s)
I	6	6	41.5	0.29
Ic	9	3	67.4	
III	7	7	37.5	1.35
IIIa	15	5	59.7	56.7
V	8	8	39.6	0.56
Vb	14	7	51.1	6.11

Fig. 2: Gates counts for the intermediate field attack on QR-$\text{UOV}^{\hat{+}}$ and practical results.

MinRank attack on VOX

In [9], Guo and Ding introduce a MinRank attack that also targets the new parameters proposed for VOX. The attack is practical and breaks all of the new 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 1.3. In particular, they target all parameter sets, while our attack only targets the parameter sets with composite c. Guo and Ding propose alternative parameters for VOX to improve the security of the scheme against the MinRank attack. We recall these possible parameters and their expected security in Figure 3.

q,t	Parameter set	o/c, v/c, c	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

Fig. 3: Possible VOX parameters proposed in [9].

To illustrate the difference in our approach, notice that our attack applies to the subset of these new parameters where c is composite. We detail the cost in arithmetic operations to match the estimates in [9].

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

Fig. 4: Binary operation counts for the intermediate field attack on some VOX parameters proposed in [9].

This shows that while our attack is not as general as the attack of Guo and Ding, it is significantly more efficient when it applies.

2 Patching the scheme

We identify the following countermeasure to our attack: use a QR parameter l that is prime.

References

1. 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.
2. 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`.
3. Jacques Patarin. The oil and vinegar signature scheme. In *Dagstuhl Workshop on Cryptography September, 1997*, 1997.
4. 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.
5. 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.
6. 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.
7. Hiroki Furue and Yasuhiko Ikematsu. A new security analysis against mayo and qr-uov using rectangular minrank attack. In *Advances in Information and Computer Security: 18th International Workshop on Security, IWSEC 2023, Yokohama,*

Japan, August 29–31, 2023, Proceedings, page 101–116, Berlin, Heidelberg, 2023. Springer-Verlag.

8. 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.
9. Hao Guo and Jintai Ding. A practical minrank attack against vox. Cryptology ePrint Archive, Paper 2024/166, 2024. `https://eprint.iacr.org/2024/166`.