A Practical MinRank Attack on VOX

Hao Guo[1,2] and Jintai Ding[1,2]

[1] Beijing Institute of Mathematical Sciences and Applications, Beijing, China
[2] Yau Mathematical Sciences Center, Tsinghua University, Beijing, China
guoh22@mails.tsinghua.edu.cn
jintai.ding@gmail.com

Abstract. VOX is a UOV-like signature scheme submitted to Round 1 additional signatures of NIST PQC standardization process. In 2023 Furue and Ikematsu proposed a rectangular MinRank attack on VOX, resulting in the submitters changing their parameters to counter this attack. In this paper we propose a new type of MinRank attack called padded MinRank attack. We show that the attack is highly efficient in its running time, taking less than one minute to break eight of nine parameters and about eight hours for the remaining one. Therefore the parameters of VOX should be reexamined to ensure its safety.

1 Introduction

The Unbalanced Oil and Vinegar (UOV) signature scheme has been introduced for more than 20 years, and remains competitive in its short signature and fast verification. However UOV and its variants share the disadvantage of long public key length. Therefore the successors put a lot of effort into compressing the public key size. Recently NIST announced an additional round for post-quantum signatures and received about 50 submissions. Among the submissions seven of them are UOV-like schemes: MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV and VOX.

The VOX scheme [PFF+23] is proposed by Patarin et al., and it combines the idea of QR-UOV[FIKT21] and plus modification [FMPP22]. After the publication of VOX, Furue and Ikematsu [FI23] proposed a equivalent key recovery attack using rectangular MinRank attack. Rectangular MinRank attack was proposed by Beullens in [Beu21a], and the idea has also been found in [TPD21]. In [FI23] the authors show that MAYO and QR-UOV remains safe under the attack. However VOX is shown to be vulnerable under this attack. In [MPC+23] the authors adjusted the parameters to counter this attack, claiming that those new parameters are safe.

In this paper, we developed a new kind of MinRank attack called padded rectangular MinRank attack. The name “padded” comes from the construction of our MinRank instance, where zero matrices are padded to the side of matrices occured in rectangular MinRank attack. Using this attack, we extracted two vectors in oil space from VOX public key using less than one minute for eight of

λ	q	O	V	c	t	Running time (second)	Total Memory Usage (MB)
128	251	4	5	13	6	0.170	32.09
		5	6	11	6	0.510	32.09
		6	7	9	6	27357.799	6147.06
192	1021	5	6	15	7	0.440	32.09
		6	7	13	7	0.790	32.09
		7	8	11	7	26.170	157.69
256	4093	6	7	17	8	1.240	64.12
		7	8	14	8	1.870	64.12
		8	9	13	8	51.530	256.00

Table 1. Experiment result of our MinRank attack.

nine parameters proposed, and the remaining parameter costs only eight hours. Therefore the parameters should be reexamined to meet the complexity need.

Our paper is organized as follows. After introducing the VOX scheme and rectangular MinRank attack, we proposed our padded rectangular MinRank attack. After analyzing the properties of this new MinRank instance, we show how this attack can be applied to VOX and list our experiment result with the Magma [BCP97] computer algebra system. We also look into this phenomenon and proposed our hypothesis of why this attack works. The Magma code for our generation of VOX instance and MinRank attack is contained in appendix for completeness.

2 Previous Rectangular MinRank Attack on VOX

2.1 About the VOX scheme

VOX scheme was first proposed by Patarin et al. in [PFF+23]. As a multivariate public key cryptosystem, it still follows the bipolar construction [DPS20]: The public key is a multivariate quadratic map $\mathcal{P}\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$, which can be decomposed as $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$, where $\mathcal{F}\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ is the central quadratic map which is easy to be inverted, and $\mathcal{S}\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T}\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ are two linear invertible maps. $\mathcal{F}, \mathcal{S}, \mathcal{T}$ form the private key. As a UOV-like scheme, the number of oil variables o in VOX is equal to that of m, and the number of vinegar variables is $v = n - o$.

The central map consists of two parts: the first t quadratic polynomials are randomly chosen quadratic polynomials with no linear and constant terms, while the last $m - t$ quadratic polynomials are (v, o)-OV polynomials, which has the form of

$$f_i(x_1, \ldots, x_v; x_{v+1}, \ldots, x_{v+o}) = \sum_{j=1}^{v} \sum_{k=i}^{v+o} a_{i,j,k} x_j x_k \tag{1}$$

To sign a given message m or its hash $\mathbf{y} = H(m) \in \mathbb{F}_q^m$, i.e. finding a solution of the equation $\mathcal{P}(\mathbf{x}) = \mathbf{y}$, the signer uses the private key and calculate $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$, and tries to solve $\mathcal{F}(\mathbf{w}) = \mathbf{z}$, from which a signature $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{w})$

is generated. To solve $\mathcal{F}(\mathbf{w}) = \mathbf{z}$, the signer randomly fixes the vinegar varibles, uses OV-polynomials to eliminate $m - t$ variables, and solves the remaining quadratic system with t equations and t variables using Gröbner basis based techniques. Therefore the value of t should not be too large.

In [PFF+23] the authors also introduced the QR-variant of VOX. The aim is to decrease the public key and secret key size. Here we adopt the explanation of [FIKT21]. The method is to construct a embedding ϕ from $\mathbb{F}_{q^c}$ to $M_c(\mathbb{F}_q)$ via $(1, g, \dots, g^{c-1})\phi(\overline{a}) = (\overline{a}, \overline{a}g, \dots, \overline{a}g^{c-1})$ for $\overline{a} \in \mathbb{F}_{q^c}$. Then by Theorem 1 of [FIKT21], there exists an invertible symmetric matrix $W \in M_c(\mathbb{F}_q)$ such that $W\phi(\overline{a})$ is symmetric for any $\overline{a} \in \mathbb{F}_{g^c}$. We extend the definition of ϕ to $M_N(\mathbb{F}_{q^c})$ entrywisely.

For constructing the private key, $\mathcal{T}\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ is still chosen as a invertible linear map of the form

$$\begin{bmatrix} \mathbf{I}_t & \mathbf{0}_{t\times(m-t)} \\ *_{(m-t)\times t} & \mathbf{I}_{m-t} \end{bmatrix} \in M_m(\mathbb{F}_q)$$

while $\mathcal{S} = \phi(\overline{\mathbf{S}})\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ is constucted from a matrix $\overline{\mathbf{S}} \in M_N(\mathbb{F}_{q^c})$ where

$$\overline{\mathbf{S}} = \begin{bmatrix} \mathbf{I}_V & *_{V\times O} \\ \mathbf{0}_{O\times V} & \mathbf{I}_O \end{bmatrix}$$

Suppose $\overline{\mathbf{F}}_1, \dots, \overline{\mathbf{F}}_m \in M_N(\mathbb{F}_{q^c})$ are given such that $\overline{\mathbf{F}}_1, \dots, \overline{\mathbf{F}}_t$ are random symmetric matrix, $\overline{\mathbf{F}}_{t+1}, \dots, \overline{\mathbf{F}}_m$ are symmetric and have the OV-form of

$$\begin{bmatrix} *_V & *_{V\times O} \\ *_{O\times V} & \mathbf{0}_O \end{bmatrix}$$

then the central map will be

$$f_i(\mathbf{x}) = \mathbf{x}(\mathbf{I}_N \otimes W)\phi(\overline{\mathbf{F}}_i)\mathbf{x}^t$$

for $\mathbf{x} = (x_1, \dots, x_n)$, $i = 1, \dots, m$, and the public key is given by

$$p_i(\mathbf{x}) = \mathbf{x}\phi(\overline{\mathbf{S}})^t(\mathbf{I}_N \otimes W)\left(\sum_{j=1}^m t_{i,j}\phi(\overline{\mathbf{F}}_j)\right)\phi(\overline{\mathbf{S}})\mathbf{x}^t$$

Notice that $\phi(\overline{\mathbf{S}})^t(\mathbf{I}_N \otimes W) = (\mathbf{I}_N \otimes W)\phi(({}^t\overline{\mathbf{S}}))$, we can obtain $\sum_{j=1}^m t_{i,j}\overline{\mathbf{S}}^t\overline{\mathbf{F}}_i\overline{\mathbf{S}}$ from public key, therefore we can define

$$\overline{p}_i(\mathbf{y}) = \mathbf{y}\overline{\mathbf{S}}^t\left(\sum_{j=1}^m t_{i,j}\overline{\mathbf{F}}_j\right)\overline{\mathbf{S}}\mathbf{y}^t$$

Then the public key and central map can be viewed as a UOV map with $V = v/c$ new vinegar variables, $O = o/c$ new oil variables and m equations over the extension field $\mathbb{F}_{q^c}$. In fact, the attack by Furue and Ikematsu in [FI23] is conducted on this extension field.

Here we list the current parameters given in [MPC+23] in Table 2

λ	q	$O = m/c$	$V = v/c$	c	t
128	251	4	5	13	6
		5	6	11	6
		6	7	9	6
192	1021	5	6	15	7
		6	7	13	7
		7	8	11	7
256	4093	6	7	17	8
		7	8	14	8
		8	9	13	8

Table 2. Current parameters of VOX.

2.2 The MinRank problem

Put it simply, the MinRank problem asks for a linear (or affine) combination of given matrices that has a small rank. This problem is first abstracted by Courtois [Cou01], where he generalized the problem of Syndrome Decoding from coding theory. The problem we are interested is the search version of the MinRank problem:

Definition 1 (Homogeneous MinRank problem). *Let* $\mathbf{M}_1, \ldots, \mathbf{M}_K$ *be some* m*-by-*n *matrices over a* finite *field* $\mathbb{F}_q$*, and let* $r < \min(m, n)$*. The problem asks for* $x_1, \ldots, x_K \in \mathbb{F}_q$ *which are not all zero, such that*

$$\mathbf{M} := \sum_{k=1}^{K} x_k \mathbf{M}_k$$

has rank no more than r*.*

We denote the set of problems with parameter (m, n, K, r, q) as $\mathrm{MR}(m, n, K, r, q)$. When the field is clear from context we also omit q. There is also the inhomogeneous version:

Definition 2 (Inhomogeneous MinRank problem). *Let* $\mathbf{M}_0$*;* $\mathbf{M}_1, \ldots, \mathbf{M}_K$ *be some* m*-by-*n *matrices over a* finite *field* $\mathbb{F}_q$*, and let* $r < \min(m, n)$*. The problem asks for* $x_1, \ldots, x_K \in \mathbb{F}_q$*, such that*

$$\mathbf{M} := \mathbf{M}_0 + \sum_{k=1}^{K} x_k \mathbf{M}_k$$

has rank no more than r*.*

We denote the set of problems with parameter (m, n, K, r, q) as $\overline{\mathrm{MR}}(m, n, K, r, q)$. When the field is clear from context we also omit q.

In homogeneous case, we require that all the $\mathbf{M}_k$'s are of rank at least $r + 1$; In inhomogeneous case, we require that $\mathbf{M}_0$ is of rank at least $r + 1$. This is to avoid trivial solutions.

2.3 Combinatoric and algebraic methods for solving the MinRank problem

Courtois mentioned in [Cou01] that the MinRank problem is NP-hard via reduction from syndrome decoding problem of a linear error correcting code which is NP-complete. Faugère [FLP08] on another hand gives a reduction from rank decoding problem, also showing its hardness. Nonetheless, there have been many methods to solve the MinRank problem. These methods fall into two categorys: combinatoric method, and algebraic method.

Kernel attack [GC00] is the first method proposed to solve the MinRank problem. It is proposed by Goubin and Courtois. The idea is to choose vectors $\mathbf{y}_k \in \mathbb{F}_q^n$ randomly, hoping they could fall into the kernel of $\mathbf{M}$, the linear (affine) combination of given matrices, then solve for the coefficient x_k's using the linear equations $\mathbf{M}\mathbf{y}_k = \mathbf{0}$. This is a combinatoric method, and the complexity of kernel attack is $O(q^{\lceil K/m \rceil r} K^3)$.

Minors attack [FDS10] is the simple algebraic method, which takes out all $(r+1)$-minors of $\mathbf{M}$, and solving the system equations where all these minors are equal to zero. While it only involves the x_k variables, the degree of each equation is $r+1$. This causes complexity of the method to rely heavily on the general method of solving system of multivariate equations using Gröbner basis, which has complexity $O(\binom{K+d}{d}^{\omega})$ where d is the degree of regularity for the determinant ideal, and ω is the constant for matrix multiplication.

Kipnis–Shamir attack [KS99] tries to solve for the right kernel of $\mathbf{M}$. Since $\mathbf{M}$ is of size m-by-n and has rank at most r, its right kernel has at least $n-r$ dimensions, which means $n-r$ linear independent vectors $\mathbf{y}_k$ can be chosen such that $\mathbf{M}\mathbf{y}_k = \mathbf{0}$. Different with kernel attack, Kipnis–Shamir attack sets new variables as coordinates of $\mathbf{y}_k$'s, and gets bilinear quadratic equations. Kipnis–Shamir attack is analyzed [FLP08] to contain equations in Minors attack. Recent complexity analysis of Kipnis–Shamir method includes [VBC$^+$19] and [NWI23].

Support-Minors attack is the state-of-the-art method of solving homogeneous MinRank problems. It decomposes the matrix $\mathbf{M}$ as product of two rank r matrices $\mathbf{M} = \mathbf{SC}$ where $\mathbf{C}$ is a r-by-n matrix, and sets the maximal minors of $\mathbf{C}$ as new variables. Equations are obtained by augmenting $\mathbf{C}$ with each row of $\mathbf{M}$, and letting the new maximal minors (the size increased by one) be zero. This new attack has been analyzed [BB22,GD22] to contain the equations in Kipnis–Shamir attack.

2.4 Previous MinRank Attacks on UOV-like schemes

Among UOV-like schemes, MinRank attack was first applied to Rainbow [DS05], where a linear combination of public key matrices has exceptionally small rank. In this attack the matrices are chosen as the public key itself. In [Beu21a] the author introduced a new type of MinRank attack on Rainbow, called *rectangular* MinRank attack. The idea can be abstracted using Ikematsu's matrix deformation [INT23]: Let $(\mathbf{Q}_1, \ldots, \mathbf{Q}_m)$ be a set of n-by-n matrices over $\mathbb{F}_q$, and let $\mathbf{q}_k^{(j)}$

denote the j-th column vector of $\mathbf{Q}_k$. Then we define the new set $(\tilde{\mathbf{Q}}_1, \ldots, \tilde{\mathbf{Q}}_n)$ of n-by-m matrices as

$$\begin{aligned}
\tilde{\mathbf{Q}}_1 &= \left[\mathbf{q}_1^{(1)}\ \mathbf{q}_2^{(1)}\ \cdots\ \mathbf{q}_m^{(1)}\right] \\
\tilde{\mathbf{Q}}_2 &= \left[\mathbf{q}_1^{(2)}\ \mathbf{q}_2^{(2)}\ \cdots\ \mathbf{q}_m^{(2)}\right] \\
&\ \vdots \\
\tilde{\mathbf{Q}}_n &= \left[\mathbf{q}_1^{(n)}\ \mathbf{q}_2^{(n)}\ \cdots\ \mathbf{q}_m^{(n)}\right]
\end{aligned} \tag{2}$$

It is stated in [INT23] that if $\mathbf{S}$ is a n-by-n matrix and $\mathbf{T}$ is a m-by-m matrix, and $(\mathbf{F}_1, \ldots, \mathbf{F}_m)$ is a set of n-by-n matrices, then the matrix deformation of $(\mathbf{P}_1, \ldots, \mathbf{P}_m) = (\mathbf{S}\mathbf{F}_1\mathbf{S}^t, \ldots, \mathbf{S}\mathbf{F}_m\mathbf{S}^t)\mathbf{T}$ is

$$(\tilde{\mathbf{P}}_1, \ldots, \tilde{\mathbf{P}}_n) = (\mathbf{S}\tilde{\mathbf{F}}_1\mathbf{T}, \ldots, \mathbf{S}\tilde{\mathbf{F}}_n\mathbf{T})\mathbf{S}^t \tag{3}$$

Therefore if some of the $\tilde{\mathbf{F}}_i$'s have some low rank property, then a linear combination of $\tilde{\mathbf{P}}_i$ should also be low rank.

[FI23] also applied rectangular MinRank attack on MAYO [Beu21b] and QR-UOV [FIKT21], and confirmed that MAYO and QR-UOV are secure under rectangular MinRank attack. VOX, however, is shown to be weak under this attack. In [MPC+23], the authors summarized the attack given by [FI23]. The idea is to notice that if we view the UOV map as on extension field $\mathbb{F}_{q^c}$ and generate the $\mathbf{F}_i$'s and $\mathbf{P}_i$'s correspondingly, the matrix deformation $\tilde{\mathbf{F}}_N$ have rank at most $V + t$, due to its special shape: the last $m - t$ columns of $\tilde{\mathbf{F}}_N$ have the last O rows as zero rows, so the rank they can contribute is at most V; the first t columns of $\tilde{\mathbf{F}}_N$ are random, however since $O > t$, the rank they can contribute additionally is at most t.

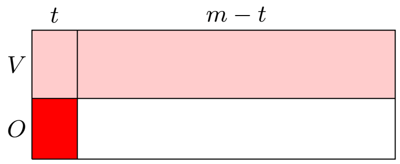

Fig. 1. Shape of $\tilde{\mathbf{F}}_N$. The rank does not exceed $V + t$.

Since $\mathbf{S}\tilde{\mathbf{F}}_N\mathbf{T}$ is a linear combination of $\tilde{\mathbf{P}}_1, \ldots, \tilde{\mathbf{P}}_N$, this creates a MinRank instance. The authors used the support minors method to estimate the complexity of the attack, and the results are listed in Table 3.

3 The Padded rectangular MinRank Attack

Our idea comes from the disadvantage that rectangular MinRank attack cannot be applied to VOX now, due to the fact that $\tilde{\mathbf{F}}_i$'s are all full row rank now.

λ	q	O	V	c	t	$\log_2 C$
128	251	8	9	6	6	50.8
192	1021	10	11	7	7	54.8
256	4093	12	13	8	8	55.3

Table 3. Complexity of the Rectangular MinRank attack on VOX parameters

However, if we concatenate $\tilde{\mathbf{F}}_{N-1}$ and $\tilde{\mathbf{F}}_N$ vertically, the concatenated matrix will have rank at most $2V + t$, due to the fact that $2O > t$ and $m - t > 2V$ for the modified parameters.

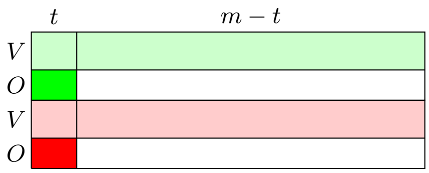

Fig. 2. The shape of $\begin{bmatrix}\tilde{\mathbf{F}}_{N-1}\\ \tilde{\mathbf{F}}_N\end{bmatrix}$. The rank does not exceed $2V + t$.

Generally, for $l \leq O$, if $m - t > lV$ and $lO > t$, then the following matrix

$$\mathbf{M}'_{\mathbf{s}} = \begin{bmatrix}\mathbf{S}\tilde{\mathbf{F}}_{N-l+1}\mathbf{T}\\ \vdots\\ \mathbf{S}\tilde{\mathbf{F}}_N\mathbf{T}\end{bmatrix} = \begin{bmatrix}\mathbf{S}\tilde{\mathbf{F}}_{N-l+1}\\ \vdots\\ \mathbf{S}\tilde{\mathbf{F}}_N\end{bmatrix}\mathbf{T} = (\mathbf{I}_l \otimes \mathbf{S})\begin{bmatrix}\tilde{\mathbf{F}}_{N-l+1}\\ \vdots\\ \tilde{\mathbf{F}}_N\end{bmatrix}\mathbf{T}$$

has rank at most $lV + t$. Using the formula (3), since $\mathbf{S}\tilde{\mathbf{F}}_{N-l+1}\mathbf{T}, \ldots, \mathbf{S}\tilde{\mathbf{F}}_N\mathbf{T}$ are all linear combinations of $\tilde{\mathbf{P}}_1, \ldots, \tilde{\mathbf{P}}_N$, it seems that we need to find choices of $x_{1,i}, \ldots, x_{l,i}$ such that

$$\mathbf{M}'_{\mathbf{s}} = \begin{bmatrix}\sum_{i=1}^{N} x_{1,i}\tilde{\mathbf{P}}_i\\ \vdots\\ \sum_{i=1}^{N} x_{l,i}\tilde{\mathbf{P}}_i\end{bmatrix}$$

has rank at most $lV + t$. However, if we naively solve this, we will get many spurious solutions which we do not really want. For example, if we choose $x_{1,i} = \cdots = x_{l,i}$ for all i, then $\mathbf{M}'_{\mathbf{s}}$ will have rank at most N, which is not what we want. However, from (3) notice that $\mathbf{x}_j = (x_{j,1}, \ldots, x_{j,N})$ should be the $N - l + j$ column of $(\mathbf{S}^t)^{-1}$, which is a block upper triangular matrix, therefore we have $x_{j,i} = \delta_{i,N-l+j}$ for $i > V$. As such we have

$$\mathbf{M}_{\mathbf{s}} = \begin{bmatrix}\sum_{i=1}^{V} x_{1,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_{N-l+1}\\ \vdots\\ \sum_{i=1}^{V} x_{l,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_N\end{bmatrix} \tag{4}$$

which is an inhomogeneous MinRank instance. If we write out each component of linear combination, we notice that each component has the form of

$$\tilde{\mathbf{F}}_i^{(j,l)} = \begin{bmatrix} \mathbf{0} \\ \vdots \\ \tilde{\mathbf{F}}_i \\ \vdots \\ \mathbf{0} \end{bmatrix} \tag{5}$$

where l is the number of matrices concatenated, hence the name "padded" rectangular MinRank.

3.1 Nontrivial rank fall of $\mathbf{M_s}$

In this subsection we show that, due to the symmetry property of public key and central map, the rows of $\mathbf{M_s}$ have a structured linear combination which amounts to zero. Recall that if the central map $\mathbf{F}_i$'s are symmetric, so are the public keys $\mathbf{P}_i$. Now notice that

$$\sum_{i=1}^{V} x_{1,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_{N-l+1} = \begin{bmatrix}\mathbf{P}_1\mathbf{x}_1{}^t \; \mathbf{P}_2\mathbf{x}_1{}^t \cdots \; \mathbf{P}_o\mathbf{x}_1{}^t\end{bmatrix}$$

Similarly we have

$$\sum_{i=1}^{V} x_{2,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_{N-l+2} = \begin{bmatrix}\mathbf{P}_1\mathbf{x}_2{}^t \; \mathbf{P}_2\mathbf{x}_2{}^t \cdots \; \mathbf{P}_o\mathbf{x}_2{}^t\end{bmatrix}$$

Therefore

$$\begin{aligned}\mathbf{x}_2\left(\sum_{i=1}^{V} x_{1,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_{N-l+1}\right) &= \begin{bmatrix}\mathbf{x}_2\mathbf{P}_1\mathbf{x}_1{}^t \; \mathbf{x}_2\mathbf{P}_2\mathbf{x}_1{}^t \cdots \; \mathbf{x}_2\mathbf{P}_o\mathbf{x}_1{}^t\end{bmatrix} \\ &= \begin{bmatrix}\mathbf{x}_1\mathbf{P}_1\mathbf{x}_2{}^t \; \mathbf{x}_1\mathbf{P}_2\mathbf{x}_2{}^t \cdots \; \mathbf{x}_1\mathbf{P}_o\mathbf{x}_2{}^t\end{bmatrix} \\ &= \mathbf{x}_1\left(\sum_{i=1}^{V} x_{2,i}\tilde{\mathbf{P}}_i + \tilde{\mathbf{P}}_{N-l+2}\right)\end{aligned}$$

which shows that a nonzero linear combination of the first $2N$ rows is zero. For every pair of blocks such syzygy such syzygy exists, so we expect $\mathbf{M_s}$ to have rank at most $lN - \binom{l}{2}$. To make the MinRank attack works, the parameters should satisfy $lV + t < lN - \binom{l}{2}$, or equivalently $t < lO - \binom{l}{2}$. Since l can be $1, 2, \ldots, O$, we expect that such attack works when $t < O(O+1)/2$.

3.2 Experimental Results

Since we are dealing with an inhomogeneous MinRank instance, we adapt the Kipnis–Shamir attack and solve for the left kernel of $\mathbf{M_s}$. The equations come from the following matrix equation:

$$\left[\mathbf{K}\ \mathbf{I}_{N-r}\right]\mathbf{M_s} = \mathbf{0} \tag{6}$$

where $\mathbf{K}$ is a $(N-r)$-by-N matrix whose entries form the kernel variables.

To solve for the Gröbner basis of the ideal generated by the Kipnis–Shamir attack, we used the Gröbner basis algorithm F4 with respect to the graded revese lexicographic monomial order in Magma V2.28-2 [BCP97] on CPU a 2.40GHz Intel Xeon Silver 4214R CPU. The detailed running time of the Gröbner basis solving is listed in Table 4.

λ	q	O	V	c	t	Running time (second)	Total Memory Usage (MB)
128	251	4	5	13	6	0.170	32.09
		5	6	11	6	0.510	32.09
		6	7	9	6	27357.799	6147.06
192	1021	5	6	15	7	0.440	32.09
		6	7	13	7	0.790	32.09
		7	8	11	7	26.170	157.69
256	4093	6	7	17	8	1.240	64.12
		7	8	14	8	1.870	64.12
		8	9	13	8	51.530	256.00

Table 4. Experiment result of our MinRank attack.

In the experiment, we saw that all the nine systems have first degree fall at degree 3, which matches the analysis above.

3.3 Our hypothetical analysis for the result

To give a theoretical upper bound for the complexity of our attack, here we adopt the analysis of [NWI23], and introduce the monomial graded degree D_{mgd} which is the smallest total degree of monomials in

$$\frac{\prod_{i=1}^{d}(1-t_0t_i)^m}{(1-t_0)^{lV}(1-t_1)^r\dots(1-t_d)^r}$$

whose coefficient is negative. The monomial D_{mgd} is believed to bound from above the solving degree, hence it gives an upper bound for the complexity estimation. d is the number of kernel vectors we choose, and should range between 1 and $lN-r$. Using the formula $\binom{lV+dr+D_{mgd}}{D_{mgd}}^{\omega}$ to estimate the complexity C, we list the complexity estimation in Table 5.

λ	q	$O = m/c$	$V = v/c$	c	t	d	D_{mgd}	$\log_2 C$
128	251	4	5	13	6	1	5	41.28
		5	6	11	6	1	6	49.64
		6	7	9	6	1	7	58.02
192	1021	5	6	15	7	2	4	43.41
		6	7	13	7	1	5	45.92
		7	8	11	7	1	6	54.54
256	4093	6	7	17	8	1	4	45.35
		7	8	14	8	1	5	48.04
		8	9	13	8	2	6	56.83

Table 5. Complexity of our attack.

Using this estimation, we try to fix the parameters for VOX. It is hard to tweak t respect to O, because small t will not exceed $lO - \binom{l}{2}$, while large t will make signature harder due to Gröbner basis calculation. While making c smaller can reduce the equations occured in Kipnis–Shamir method, it will decrease the number of variables when viewed over $\mathbb{F}_q$, resulting in a decrease of security. Therefore we decided to only tweak V. We found that the complexity grows as V increases, and we checked the parameters for $V < 2O$. We found that all of the parameters still fail the estimation, with complexity less than 140 bits.

λ	q	$O = m/c$	$V = v/c$	c	t	d	D_{mgd}	$\log_2 C$
128	251	4	7	13	6	1	8	78.10
		5	9	11	6	1	11	99.80
		6	11	9	6	2	13	133.96
192	1021	5	9	15	7	1	8	84.95
		6	11	13	7	1	10	101.51
		7	13	11	7	1	14	129.55
256	4093	6	11	17	8	1	8	90.60
		7	13	14	8	1	11	113.72
		8	15	13	8	1	13	130.61

Table 6. Estimated complexity of our attack on possible VOX parameters.

4 Conclusion

In this paper, we demostrated a new kind of MinRank attack called padded MinRank attack. We show that under this attack, current parameters provided by the VOX team remains weak, with most attacks succeeding in less than one minute. Therefore, the parameters of VOX still need careful examination and tweak.

Since padded MinRank attack is a new kind of MinRank attack, the analysis of it is not sufficient, and we call for more inspection into this attack and its applicability into other UOV-like schemes.

Acknowledgement We would like to thank Peigen Li from Beijing Institute of Mathematics Sciences and Applications (BIMSA) and Yi Jin from CCBFT for useful discussion. This work is supported by National Key R&D Program of China (No. 2021YFB3100100) and Beijing Natural Science Foundation (No. M22001).

References

BB22. Magali Bardet and Manon Bertin. Improvement of algebraic attacks for solving superdetermined minrank instances. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022, Virtual Event, September 28-30, 2022, Proceedings*, volume 13512 of *Lecture Notes in Computer Science*, pages 107–123. Springer, 2022.

BCP97. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

Beu21a. Ward Beullens. Improved cryptanalysis of UOV and rainbow. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 348–373. Springer, 2021.

Beu21b. 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.

Cou01. Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 402–421. Springer, 2001.

DPS20. Jintai Ding, Albrecht Petzoldt, and Dieter S. Schmidt. *Multivariate Public Key Cryptosystems, Second Edition*, volume 80 of *Advances in Information Security*. Springer, 2020.

DS05. Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos D. Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

FDS10. Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In Wolfram Koepf, editor, *Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings*, pages 257–264. ACM, 2010.

FI23. 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, *Advances in Information and Computer Security - 18th International Workshop on Security, IWSEC 2023, Yokohama, Japan, August 29-31, 2023, Proceedings*, volume 14128 of *Lecture Notes in Computer Science*, pages 101–116. Springer, 2023.

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 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV*, volume 13093 of *Lecture Notes in Computer Science*, pages 187–217. Springer, 2021.

FLP08. Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret. Cryptanalysis of minrank. In David A. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 280–296. Springer, 2008.

FMPP22. Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret. A new perturbation for multivariate public key schemes such as HFE and UOV. *IACR Cryptol. ePrint Arch.*, page 203, 2022.

GC00. Louis Goubin and Nicolas T. Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Springer, 2000.

GD22. Hao Guo and Jintai Ding. Algebraic relation of three minrank algebraic modelings. In Sihem Mesnager and Zhengchun Zhou, editors, *Arithmetic of Finite Fields - 9th International Workshop, WAIFI 2022, Chengdu, China, August 29 - September 2, 2022, Revised Selected Papers*, volume 13638 of *Lecture Notes in Computer Science*, pages 239–249. Springer, 2022.

INT23. Yasuhiko Ikematsu, Shuhei Nakamura, and Tsuyoshi Takagi. Recent progress in the security evaluation of multivariate public-key cryptography. *IET Inf. Secur.*, 17(2):210–226, 2023.

KS99. Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

MPC$^+$23. Gilles Macario-Rat, Jacques Patarin, Benoit Cogliati, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, and Brice Minaud. Rectangular attack on VOX. *IACR Cryptol. ePrint Arch.*, page 1822, 2023.

NWI23. Shuhei Nakamura, Yacheng Wang, and Yasuhiko Ikematsu. A new analysis of the kipnis-shamir method solving the minrank problem. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 106(3):203–211, 2023.

PFF+23. Jacques Patarin, Jean-Charles Faugère, Pierre-Alain Fouque, Louis Goubin, Robin Larrieu, Gilles Macario-Rat, and Brice Minaud. Vox specification v1.0 – 06/01/2023. *Round 1 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes*, 2023.

TPD21. Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Efficient key recovery for all HFE signature variants. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 70–93. Springer, 2021.

VBC+19. Javier A. Verbel, John Baena, Daniel Cabarcas, Ray A. Perlner, and Daniel Smith-Tone. On the complexity of "superdetermined" minrank instances. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 167–186. Springer, 2019.

A Magma code for our attack

Here we list the Magma code we used for the attack.

```
q := 251;
O := 6;
V := 7;
c := 9;
t := 6;
o := O*c;
v := V*c;
N := O+V;
n := N*c;
m := o;
l := 2;
r := l*V+t;
field<z> := GF(q^c);

F0 := [RandomMatrix(field, N, N): i in [1..t]];
F1 := [RandomMatrix(field, V, V): i in [1..m-t]];
F2 := [RandomMatrix(field, V, O): i in [1..m-t]];
F3 := [RandomMatrix(field, O, V): i in [1..m-t]];

FF := F0 cat [VerticalJoin(
    HorizontalJoin(F1[i], F2[i]),
    HorizontalJoin(F3[i], ZeroMatrix(field, O, O))
): i in [1..m-t]];
```

```
S2 := RandomMatrix(field, V, O);
S := VerticalJoin(
    HorizontalJoin(
        ScalarMatrix(V, One(field)), S2
    ),
    HorizontalJoin(
        ZeroMatrix(field, O, V), ScalarMatrix(O, One(field))
    )
);

T2 := RandomMatrix(BaseField(field), t, m-t);
T := VerticalJoin(
    HorizontalJoin(
        ScalarMatrix(t, One(BaseField(field))), T2
    ),
    HorizontalJoin(
        ZeroMatrix(BaseField(field), m-t, t),
        ScalarMatrix(m-t, One(BaseField(field)))
    )
);

P := [Transpose(S)*FF[i]*S: i in [1..m]];
PP := [
    &+[T[i][j]*P[j]: j in [1..m]]
    : i in [1..m]
];

PTP := [(Transpose(PP[i]) + PP[i]): i in [1..m]];

PMD := [(Matrix(
    [PTP[j][i]: j in [1..m]]
)): i in [1..N]];

Z := ZeroMatrix(field, m, N*l);

RM := [
    [InsertBlock(Z, PMD[i], 1, N*j+1): i in [1..N]]: j in [0..l-1]
];

Ans := &+[
    &+[
        -S2[j][O-l+i] * RM[i][j]: j in [1..V]
    ]: i in [1..l]
]
```

```
+
&+[
    RM[i][i+N-l]: i in [1..l]
];

PP<[w]> := PolynomialRing(field, l*V+r*(l*N-r), "glex");

X := [Eltseq(w)[(i-1)*V+1..i*V]: i in [1..l]];
Y := [Eltseq(w)[l*V+(i-1)*r+1..l*V+i*r]: i in [1..l*N-r]];

MatX := &+[
    &+[
        X[i][j] * RMatrixSpace(PP, m, N*l)!RM[i][j]: j in [1..V]
    ]: i in [1..l]
]
+
&+[
    RMatrixSpace(PP, m, N*l)!RM[i][i+N-l]: i in [1..l]
];

MatY := Matrix([
    Y[i][1..r] cat [0: j in [r+1..l*N]]: i in [1..l*N-r]
]);
for i in [1..l*N-r] do
    MatY[i][r+i] := 1;
end for;
MatY := Transpose(MatY);

KS := MatX * MatY;

Poly := &cat[&cat[[KS[i][j]: j in [1..l*N-r]]: i in [1..m]]];

I := ideal<PP | Poly>;
SetVerbose("Groebner", 1);
time Groebner(I);
print("");
I;
```