Rectangular Attack on VOX

Gilles Macario-Rat*, Jacques Patarin, Benoît Cogliati, Jean-Charles Faugère
Pierre-Alain Fouque, Louis Goubin, Robin Larrieu and Brice Minaud

VOX Team, gilles.macariorat@orange.com, jacques.patarin@thalesgroup.com,
benoit.cogliati@thalesgroup.com, jcf@cryptonext-security.com,
Pierre-Alain.Fouque@univ-rennes.fr, Louis.Goubin@uvsq.fr,
robin.larrieu@cryptonext-security.com , brice.minaud@gmail.com

Abstract. VOX [PCF$^+$23] has been submitted to the NIST Round 1 Additional Signature of the Post-Quantum Signature Competition in June 2023. VOX is a strengthened variant of UOV which uses the Quotient-Ring (QR) setting to reduce the public-key size. At the end of August 2023, Furue and Ikamatsu posted on the NIST mailing-list a post, indicating that the parameters of VOX can be attacked efficiently using the rectangular attack in the QR setting.

In this note, we explain the attack in the specific case of VOX, we detail the complexity, and show that as Furue and Ikematsu indicated, the attack can be completely avoided by adding one more constraint on the parameter selection. Finally, we show that this constraint does not increase the sizes of the public keys or signature.

Keywords: Multivariate Cryptography, UOV, VOX, QR, Rectangular Attack

1 The Rectangular MinRank Attack on VOX

This attack has been discovered by Ward Beullens on the UOV scheme [Beu21], and has been recently generalized to the Quotient Ring (QR) setting by Furue and Ikematsu at IWSEC 2023 in [FI23]. The QR setting consists in reducing the public key by replacing $c \times c$ coefficients in $\mathbb{F}_q$ of the public-key matrix by one coefficient in $\mathbb{F}_{q^c}$ as in [FIKT21]. This allows to reduce by a factor c the matrices and the public key. The attack applies to VOX, which uses the QR-setting, but not to FOX, which does not use that setting.

1.1 Notation

Let o and v denote the number of Oil and Vinegar variables, and let $n = o + v$. All these quantities have a common divisor c, and we write $O = o/c$, $V = v/c$, $N = n/c$. We denote by t the number of totally random secret polynomials in N variables over $\mathbb{F}_{q^c}$. Let $\{e_i, i = 1, \dots, N\}$ be a canonical vector base of $\mathbb{F}_{q^c}^N$.

1.2 Description of the attack

The original attack exploits the fact that a specific (rectangular) matrix built up by composing the polar forms of the public polynomials by a random vector may have a low rank if the vector happens to belong to the secret Oil space. Therefore, solving a MinRank problem enables to find the secret Oil space. Using the notations of [Beu21],

[*] Corresponding Author

the rectangular matrix can be expressed as the representation of the linear mapping L_x defined by:

$$L_x(y) = \big(\Delta\mathbf{Pub}(x,y)\big)$$

where $\Delta\mathbf{Pub}(x,y) = \mathbf{Pub}(x+y) - \mathbf{Pub}(x) - \mathbf{Pub}(y)$ is the polar form of the public key. Indeed, for a random vector x, the expected rank of the rectangular matrix is $\min(o, N)$. For a vector x in the secret oil space, this rank is bounded by $\min(o, N, V+t)$. In the case $o > N$, the MinRank attack is applicable whenever $t < O$. Indeed, in that parameter regime, $\min(o, N, V+t) = V+t < N = \min(o, N)$, so the behavior of the rank differs between the two cases.

1.3 Complexity of the attack

The underlying MinRank problem: Let $x = \sum_{i=1}^{N} x_i e_i$ be an unknown vector. So $L_x = \sum_{i=1}^{N} x_i L_{e_i}$ has rank at most $V+t$ when x is in the secret oil space, and has a greater rank with overwhelming probability otherwise. Since the secret oil space has dimension O, with high probability, there is still a solution to the MinRank problem for x such that $O-1$ of its coordinates are set to 0. So we have to solve $\text{Rank}(\sum_{i=1}^{k} x_i L_{e_i}) \leq r$ where we note $r = V+t$ and $k = V+1$. Furthermore, we can consider the MinRank problem with $N \times o$ or $o \times N$ matrices, whichever choice leads to a better efficiency for the attack. It appears that for the set of VOX parameters, the second choice is better. We use the Support Minors Modeling to solve the MinRank problem [BBC+20]. For a better efficiency, we can also choose to select only m columns from the MinRank problem, with $r+1 \leq m \leq N$. Using the notation of [Beu21] section 7, let $n_x = k$ be the number of x_i variables, and $n_y = \binom{m}{r}$ the number of Minors variables. The MinRank problem can be expressed as a bilinear system of equations in two groups of n_x and n_y variables. This problem is solved by the XL algorithm on the first group of variables, that is we look for the minimum degree b, such that multiplying all the equations by all the monomials of the first group of variables, of degree $b-1$, then the resulting system has more free equations than the resulting number of monomials, which therefore have bi-degree $(b, 1)$. And then replacing all monomial by new variables (linearization), a solution can be found by the block-Wiedemann algorithm, since all equations are sparse and contains the same number of terms, given by $w = n_x(r+1)$. The number of monomials of bi-degree $(b,1)$ in (n_x, n_y) variables is $M(b) = \binom{n_x+b-1}{b} n_y$. From [Beu21] Section 2, the number of free equations can be expressed as $R(k, o, m, r, b) = \sum_{i=1}^{b} (-1)^{i+1} \binom{m}{i+r} \binom{o+i-1}{i} \binom{k+b-i-1}{b-i}$, whenever this quantity does not exceed the number of monomials $M(b)-1$, and is $M(b)-1$ otherwise. Finally, the complexity of the attack is $3M(b_{min})^2 w$, expressed in field multiplications, where b_{min} is the minimum value of b satisfying $R(k, o, m, r, b) \geq M(b)-1$. We use the following formula $\mu = 2\log_2^2 q^c + \log_2 q^c$ to estimate the cost of a field multiplication. We give the results in table 1.

Table 1: Complexity of the Rectangular MinRank attack on VOX parameters

λ	q	O	V	c	t	m	b	$\log_2 C$
128	251	8	9	6	6	17	3	50.8
192	1021	10	11	7	7	20	3	54.8
256	4093	12	13	8	8	22	4	55.3

2 New parameters for VOX

In the choice of our parameters, we now add the condition $O \leq t$. With this additional constraint, the Rectangular MinRank attack is no longer possible. Indeed, in that parameter regime, $V + t \geq N$, hence $\min(o, N, V + t) = \min(o, N)$: the rank difference exploited by the attack no longer exists.

If we add this constraint in the parameter selection estimation, we can propose many other parameter choices. The security in the last column has been evaluated using the MQEstimator tool [BMSV22], and considering the security for quantum estimation given by NIST[1]: 2^{143} for Level-I, 2^{207} for Level-III, and 2^{274} for Level-V.

Table 2: Impact of the new constraint on VOX parameters

	λ	q	$O = o/c$	$V = v/c$	c	t	$\|Sig\|$	$\|cpk\|$	Sec.
VOX-I	128	251	8	9	6	6	102B	9104B	
VOX-III	192	1021	10	11	7	7	184B	30351B	
VOX-V	256	4093	12	13	8	8	300B	82400B	
	128	251	4	5	13	6	117B	5980B	145
		251	5	6	11	6	121B	8117B	151
		251	6	7	9	6	117B	9104B	150
	192	1021	5	6	15	7	207B	19157B	209
		1021	6	7	13	7	212B	24261B	219
		1021	7	8	11	7	207B	26982B	215
	256	4093	6	7	17	8	332B	50337B	287
		4093	7	8	14	8	315B	52920B	276
		4093	8	9	13	8	332B	67392B	293

3 Conclusion

In this note, we explain how the rectangular attack can be adapted to VOX and why by adding an extra constraint, this attack completely disappears. Moreover, we also show that this constraint has practically no impact on the public-key and signature sizes.

References

[BBC+20] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *ASIACRYPT*, volume 12491 of *LNCS*, pages 507–536. Springer, 2020.

[Beu21] Ward Beullens. Improved cryptanalysis of UOV and rainbow. In *EUROCRYPT*, volume 12696 of *LNCS*, pages 348–373. Springer, 2021.

[BMSV22] Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. In *AFRICACRYPT*, LNCS, pages 323–347. Springer, 2022.

[FI23] Hiroki Furue and Yasuhiko Ikematsu. A new security analysis against MAYO and QR-UOV using rectangular minrank attack. In *IWSEC*, volume 14128 of *LNCS*, 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 *ASIACRYPT*, volume 13093 of *LNCS*, pages 187–217. Springer, 2021.

[1] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

[PCF$^+$23] J. Patarin, B. Cogliati, J.-C. Faugère, P.-A. Fouque, L. Goubin, R. Larrieu, G. Macario-Rat, and B. Minaud. Vox scheme. https://vox-sign.com/, 06 2023.

A Security Analysis

Table 3: Security Analysis of the new constraint on VOX parameters

Security Level	Parameters set (n,m,c,t,q)	Hybrid F5			Hybrid XLWiedemann			Kipnis Shamir		Intersection Attack		
		T	M	k	T	M	k	T	M	T	M	k
128 (143)	(110,50,10,6,251)	139.6	116.9	2	145.7	69.2	2	93.2	20.3	62.5	52.9	5
	(121,52,13,6,251)	145.1	122.4	6	151.3	72.0	2	149.3	20.7	89.7	80.5	4
	(121,55,11,6,251)	151.9	121.2	3	158.2	71.5	3	101.5	20.7	64.0	54.2	5
	(117,54,9,6,251)	150.6	127.8	2	156.9	74.9	2	85.4	20.6	62.5	52.7	5
192 (207)	(165,75,15,7,1021)	209.8	172.6	3	216.5	98.1	3	164.6	22.0	78.2	68.0	5
	(169,78,13,7,1021)	219.8	182.5	3	226.6	103.2	3	144.7	22.2	69.9	59.2	6
	(165,77,11,7,1021)	215.3	178	3	222.1	101	3	124.6	22	67.1	56.8	5
256 (274)	(201,98,14,8,4093)	276.6	244.9	2	283.8	135.2	2	183.4	23.1	73.9	62.4	7
	(221,102,17,8,4093)	287.6	255.9	2	294.9	140.8	2	219.5	23.3	84.4	73.2	6
	(221,104,13,8,4093)	293.2	261.3	2	300.4	143.6	2	171.5	23.3	72.5	61.4	6