A Cryptanalysis of NOVA Signature Scheme

Dongyu Wu[1]

Beijing Institute of Mathematical Sciences and Applications, Beijing, China
wudongyu@bimsa.cn

Abstract. NOVA signature scheme is a UOV-type signature scheme over a non-commutative coefficient ring with a novel structural map. In this article we show that a randomly generated central map for the scheme is very likely insecure and may suffer from a forgery attack in polynomial time.

Keywords: post-quantum cryptography · multivariate public key cryptography · unbalanced oil and vinegar · NOVA

Introduction

NOVA signature scheme [WTKC22] is a signature scheme based on UOV [KPG99]. The innovation of NOVA is to establish the scheme over a non-commutative coefficient ring, which enables one to compress the overall number of formal variables. As a consequence, NOVA has a much smaller public key compared to other multivariate cryptosystem, such as Rainbow [DS05] and QR-UOV [FIKT21]. Creative as the idea seems, due to the non-commutative structure, the central map has to be constructed with multiple masks to avoid possible leaks of information of the secret key as well as possible signature forgery. We will show the mask of NOVA is not sufficient under most circumstances by constructing a polynomial algorithm to forge a signature for an arbitrary document.

1 Preliminaries

1.1 Unbalanced Oil and Vinegar signature scheme (UOV)

Let v, o be two positive integers, and set $m = o, n = v + o$. For a vector of variables $x = (x_1, ..., x_n)$, call $x_1, ..., x_v$ vinegar variables and $x_{v+1}, .., x_n$ oil variables. A (v, o, q)-UOV signature scheme consists of the following:

1. **Secret key (Central map)**: a quadratic map

$$\mathcal{F} = (f_1, ..., f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m,$$

where each $f_k(x)$ is defined as

$$f_k(x) = \sum_{1 \le i \le n, 1 \le j \le v} a_{ij}^{(k)} x_i x_j, \quad a_{ij} \in \mathbb{F}_q,$$

together with a randomly chosen invertible linear transformation $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$.

2. **Public key**: the composition $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$.

3. **Signature**: a signature for $t \in \mathbb{F}_q^m$ is a vector $u \in \mathbb{F}_q^n$ such that $\mathcal{P}(u) = t$.

4. **Verification**: given a signature u and a document t, accept the signature only if $\mathcal{P}(u) = t$.

The signing procedure for UOV is straightforward. One firstly randomly fixes $x_1, ..., x_v$ and solve for the linear system $f_k(x) = t_k,\ 1 \leq k \leq m$. The linear system will have a solution with an overwhelming probability. Once such a solution x is found, the signature is formulated as $u = \mathcal{S}^{-1}(x)$.

1.2 UOV trapdoor function

To extract the algebraic structure, the UOV scheme could be described or generalized in a more abstract way by using polarization as described in [Beu21]. For a multivariate quadratic polynomial $p(x)$, the polar form p' of p is a bi-multivariate function defined as:

$$p'(x, y) = p(x + y) - p(x) - p(y) + p(0).$$

Similarly, for a multivariate quadratic map $\mathcal{P}$ the polar form $\mathcal{P}'$ is defined component-wise. One can check directly by definition that $\mathcal{P}$ is a symmetric bilinear map.

Now we are ready to define the notion of trapdoor function. The UOV trapdoor function is a multivariate quadratic map

$$\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

which secretly vanishes on an m-dimensional space N. Given a trapdoor function, we could associate to it a UOV scheme with public key being the function and secret key being the secret null space. To sign t, randomly fix a vector v and solve the following linear system

$$\mathcal{P}(o + v) = \mathcal{P}(o) + \mathcal{P}(v) + \mathcal{P}'(o, v) = t$$

for $o \in N$. The system is linear based on the fact that $\mathcal{P}(o) = 0$ and $\mathcal{P}'(o, v)$ is bilinear.

2 Description of NOVA scheme

We will work over the ring $\mathcal{R} = M_{l\times l}(\mathbb{F}_q)$.

2.1 The space $\mathbb{F}_q[S]$

The coefficient ring of NOVA is defined to be a space generated by a randomly chosen symmetric matrix $S \in \mathcal{R}$, or more specifically, the ring $\mathbb{F}_q[S]$. Note that by Cayley-Hamilton theorem, the dimension of the ring is l with an overwhelming probability.

In the following sections we define step-by-step the (v, o, l, q)-NOVA scheme.

2.2 Central map

The central map of NOVA is defined to be

$$F = (F_1, ..., F_o) : \mathcal{R}^n \to \mathcal{R}^m,$$

where

$$F_i = \sum_{\alpha=1}^{l^2} \sum_{1\leq j\leq n, 1\leq k\leq v} A_{\alpha 1} X_j^T (Q_{\alpha 1} F_{i,jk} Q_{\alpha 1}^{-1} - Q_{\alpha 2} F_{i,jk} Q_{\alpha 2}^{-1}) X_k A_{\alpha 2}.$$

In above, $F_{i,jk}, A_{\alpha i} \in_R \mathcal{R}$ and $Q_{\alpha i} \in \mathbb{F}_q[S]$.

2.3 Public key

The public key is defined to be

$$(P_{i,jk} = \tilde{F}_{i,jk} + \epsilon_{i,jk}, A_{\alpha i}, Q_{\alpha i}).$$

In above $\epsilon_{i,jk}$ is randomly chosen over $\mathbb{F}_q[S]$ and $\tilde{F} = F \circ T$, where $T : \mathcal{R}^n \to \mathcal{R}^n$ is an invertible linear map of the form

$$T = \begin{bmatrix} I & T^{12} \\ O & I \end{bmatrix}.$$

Note that the pertubation ϵ does not change the result map by commutativity.

2.4 Signature and verification

In order to sign m, compute $Hash(m) = (y_1, ..., y_o)$. Use UOV-type scheme routine to solve $F(x) = y$ for $x \in \mathcal{R}^n$. Sign with $u = T^{-1}(x)$. The verifier checks if $P(u) = Hash(m)$.

3 The attack

In this section we specifically deal with $q = 16$ and $l = 2, 3, 4$ cases, but it should be noted that similar analyses apply for all finite fields of characteristic 2 and all l, and up to some modifications also for other finite fields to some extent.

3.1 Non-trivial solutions to $\mathcal{P}(x) = 0$

We will first discuss the case $l = 2$ to illustrate the process.

Proposition 3.1. Let $S = \begin{bmatrix} A & B \\ B & C \end{bmatrix} \in M_{2\times 2}(\mathbb{F}_{16})$, and assume

$$\mathbb{F}_{16} \cong \mathbb{F}_2[a]/(a^4 + a + 1).$$

Then

1. If $A \neq C, B = 0$, then for

$$X = \begin{bmatrix} 0 & 0 \\ x_1 & x_2 \end{bmatrix}, Y = \begin{bmatrix} 0 & 0 \\ y_1 & y_2 \end{bmatrix}, \quad \forall x_1, x_2, y_1, y_2 \in \mathbb{F}_{16},$$

   and

$$X' = \begin{bmatrix} x_1' & x_2' \\ 0 & 0 \end{bmatrix}, Y' = \begin{bmatrix} y_1' & y_2' \\ 0 & 0 \end{bmatrix}, \quad \forall x_1', x_2', y_1', y_2' \in \mathbb{F}_{16},$$

   we have

$$X^T(Q_1 P Q_1^{-1} - Q_2 P Q_2^{-1})Y = 0,$$
$$(X')^T(Q_1 P Q_1^{-1} - Q_2 P Q_2^{-1})Y' = 0,$$

   for any $P \in M_{2\times 2}(\mathbb{F}_{16}), Q_1, Q_2 \in \mathbb{F}_{16}[S]$.

2. If $A \neq C, B \neq 0$ and $(AC + B^2) \cdot (A + C)^{-2}$ does not contain a term in a^3, then define the map

$$\varphi : \mathbb{F}_2 + \mathbb{F}_2 a + \mathbb{F}_2 a^2 \to \mathbb{F}_{16}$$

   as

x	$\varphi(x)$
0	0
1	a^2+a
a	a^3+a
$a+1$	a^3+a^2
a^2	a^3
a^2+1	a^3+a^2+a
a^2+a+1	a^2
a^2+a	a

and let $\omega = (A+C)\varphi((AC+B^2)\cdot(A+C)^{-2})$. Then we have

$$X = \begin{bmatrix} (\omega+C)x_1 & (\omega+C)x_2 \\ Bx_1 & Bx_2 \end{bmatrix}, Y' = \begin{bmatrix} (\omega+C)y_1 & (\omega+C)y_2 \\ By_1 & By_2 \end{bmatrix}$$

and

$$X = \begin{bmatrix} (\omega+A)x'_1 & (\omega+A)x'_2 \\ Bx'_1 & Bx'_2 \end{bmatrix}, Y' = \begin{bmatrix} (\omega+A)y'_1 & (\omega+A)y'_2 \\ By'_1 & By'_2 \end{bmatrix},$$

$\forall x_1, x_2, y_1, y_2, x'_1, x'_2, y'_1, y'_2 \in \mathbb{F}_{16}$, we have

$$X^T(Q_1PQ_1^{-1} - Q_2PQ_2^{-1})Y = 0,$$

$$(X')^T(Q_1PQ_1^{-1} - Q_2PQ_2^{-1})Y' = 0,$$

for any $P \in M_{2\times 2}(\mathbb{F}_{16}), Q_1, Q_2 \in \mathbb{F}_{16}[S]$.

3. If $A = C$, then for

$$X = \begin{bmatrix} x_1 & x_2 \\ x_1 & x_2 \end{bmatrix}, Y = \begin{bmatrix} y_1 & y_2 \\ y_1 & y_2 \end{bmatrix}, \quad \forall x_1, x_2, y_1, y_2 \in \mathbb{F}_{16},$$

we have

$$X^T(Q_1PQ_1^{-1} - Q_2PQ_2^{-1})Y = 0,$$

for any $P \in M_{2\times 2}(\mathbb{F}_{16}), Q_1, Q_2 \in \mathbb{F}_{16}[S]$.

Proof. We will mainly prove the statement for case 2. One can directly verify for each case that by definition ω solves the following quadratic equation:

$$\omega^2 + (A+C)\omega + (AC+B^2) = 0.$$

Define the matrix

$$O = \begin{bmatrix} \omega+A & \omega+C \\ B & B \end{bmatrix}.$$

One can again directly verify the following properties for O:

1. $$O^TO = \begin{bmatrix} \omega^2+A^2+B^2 & 0 \\ 0 & \omega^2+C^2+B^2 \end{bmatrix} =: D_O$$

2. $$O^TSO = \begin{bmatrix} A\omega^2+A^3+B^2C & 0 \\ 0 & A\omega^2+AC^2+B^2C \end{bmatrix} =: D_S$$

Note that the two properties above imply

$$O^T(sI+tS)O = sD_O + tD_S$$

which means that any matrix in $\mathbb{F}_q[S]$ is diagonalized by a congruence by O.

Thus, for any P and $Q \in \mathbb{F}_q[S]$, we have

$$\begin{aligned}
&X^T O^T QPQ^{-1}OY \\
=&X^T O^T QO(O^{-1}PO)O^{-1}Q^{-1}O^{-T}O^T OY \\
=&X^T(O^TQO)(O^{-1}PO)(O^TQO)^{-1}D_OY \\
=&X^T(DP'D^{-1})D_OY,
\end{aligned}$$

where $P' = O^{-1}PO$ and D is some diagonal matrix.

Therefore for a difference of two such expressions we have

$$\begin{aligned}
&X^T O^T(Q_1PQ_1^{-1} - Q_2PQ_2^{-1})OY \\
=&X^T(D_1P'D_1^{-1} - D_2P'D_2^{-1})D_OY \\
=&X^T \begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix} Y.
\end{aligned}$$

It is easy to observe by setting X, Y to be of type $\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}$ or $\begin{bmatrix} 0 & 0 \\ * & * \end{bmatrix}$ respectively we obtain solutions in the null space, and also note that a left multiplication by D_O does not change either of the two types. At last, in order to get the result we expect, simply note that

$$O\begin{bmatrix} x_1 & x_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} (\omega+A)x_1 & (\omega+A)x_2 \\ Bx_1 & Bx_2 \end{bmatrix}$$

and

$$O\begin{bmatrix} 0 & 0 \\ x_1 & x_2 \end{bmatrix} = \begin{bmatrix} (\omega+C)x_1 & (\omega+C)x_2 \\ Bx_1 & Bx_2 \end{bmatrix}.$$

As for case 1 and 3, one can use the same method to obtain the proof. □

Example 3.2. As a petite instance, consider

$$S = \begin{bmatrix} 0 & a^3+a^2 \\ a^3+a^2 & a^2+1 \end{bmatrix}$$

Then $\omega = a^3+a^2+a$. By choosing randomly $x_1 = a^2, x_2 = a^3+1, x_1' = a^3+a+1, x_2' = a^2+a+1$, we define

$$X_1 = \begin{bmatrix} (\omega+C)x_1 & (\omega+C)x_2 \\ Bx_1 & Bx_2 \end{bmatrix} = \begin{bmatrix} a^3+a & a^3+a^2 \\ a^3+a^2+a & a^2+1 \end{bmatrix},$$

and

$$X_2 = \begin{bmatrix} (\omega+C)x_1' & (\omega+C)x_2' \\ Bx_1' & Bx_2' \end{bmatrix} = \begin{bmatrix} a^3+1 & a^2 \\ a & a+1 \end{bmatrix}.$$

Then one could verify

$$X_i^T(Q_1PQ_1^{-1} - Q_2PQ_2^{-1})X_j = 0,$$

for any $P \in M_{2\times 2}(\mathbb{F}_{16})$, $Q_k \in \mathbb{F}_{16}[S]$. Hence one would get

$$\sum_{\alpha=1}^{4} \sum_{i,j\in\Omega} A_{\alpha 1}X_i^T(Q_{\alpha 1}P_{ij}Q_{\alpha 1}^{-1} - Q_{\alpha 2}P_{ij}Q_{\alpha 2}^{-1})X_jA_{\alpha 2} = 0,$$

for any $A_{\alpha k}, P_{ij} \in M_{2\times 2}(\mathbb{F}_{16})$, $Q_{\alpha k} \in \mathbb{F}_{16}[S]$ and any subset $\Omega \subset \{0,1\}^2$.

In general, we have the following statement.

Proposition 3.3. Let $S \in M_{l\times l}(\mathbb{F}_{16})$ be symmetric. Assume that $v \in \mathbb{F}_{16}^l$ is an eigenvector of S of eigenvalue λ, and let $v^\perp$ be the orthogonal complement of v. Then the arrangement

$$X_i = \begin{bmatrix} v & r_{i,1} & ... & r_{i,l-1} \end{bmatrix} \begin{bmatrix} * \\ 0_{(l-1)\times l} \end{bmatrix},$$

where $r_{i,1}, ..., r_{i,l-1} \in v^\perp$ linearly independent, solves

$$X_i^T (Q_1 P Q_1^{-1} - Q_2 P Q_2^{-1}) X_j = 0,$$

for all i, j and all $P \in M_{l\times l}(\mathbb{F}_{16}), Q_1, Q_2 \in \mathbb{F}_{16}[S]$.

Proof. Let

$$O = \begin{bmatrix} v & r_{i,1} & ... & r_{i,l-1} \end{bmatrix}.$$

Then from the assumption we have the following two properties for O:

1. $$O^T O = \begin{bmatrix} vv^T & 0 \\ 0 & *_{(l-1)\times(l-1)} \end{bmatrix} =: D_O$$

2. $$O^T S O = \begin{bmatrix} \lambda vv^T & 0 \\ 0 & *_{(l-1)\times(l-1)} \end{bmatrix} =: D_S$$

Then for any S^k,

$$\begin{aligned} & O^T S^k O \\ =& (O^T S O) O^{-1} O^{-T} (O^T S O) ... O^{-1} O^{-T} (O^T S O) \\ =& D_S D_O^{-1} D_S ... D_O^{-1} D_S. \end{aligned}$$

Therefore, for any matrix Q in $\mathbb{F}_q[S]$, we have

$$O^T Q O = \begin{bmatrix} *_{1\times 1} & 0 \\ 0 & *_{(l-1)\times(l-1)} \end{bmatrix}.$$

Thus, under the congruence by O, the upper left entry of the inner matrix of the public key is automatically zero, i.e.

$$(O^T (Q_1 P Q_1^{-1} - Q_2 P Q_2^{-1}) O)_{11} = 0.$$

This means $X_i = \begin{bmatrix} * \\ 0_{(l-1)\times l} \end{bmatrix}$ is a solution in the null space up to a linear transformation by O. □

Example 3.4. We randomly pick

$$S = \begin{bmatrix} a & 1 & a^3+1 & 0 \\ 1 & a^3+a^2+a+1 & a^3+a^2+a & a^3+a^2 \\ a^3+1 & a^3+a^2+a & 1 & a^3+a^2+a+1 \\ 0 & a^3+a^2 & a^3+a^2+a+1 & a^3+a^2 \end{bmatrix}$$

Then the characteristic polynomial of S is

$$\begin{aligned} c_S(x) &= x^4 + (a^3+a^2+1)x^2 + (a^2+1)x + a^3+a^2+a+1 \\ &= (x+a^2+1)(x^3+(a^2+1)x^2+(a^3+a^2+a+1)x+a+1). \end{aligned}$$

For the eigenvalue a^2+1, one of the corresponding eigenvectors is

$$v=(1,a^3+a^2+a,1,a^2+1)^T.$$

Now we may take any three linearly independent vectors which are orthogonal to the eigenvector. In this example, we pick

$$u_1=(1,0,1,0)^T,\ u_2=(a^2,1,0,a)^T,\ u_3=(0,0,a^2+1,1)^T.$$

Therefore, following the proposition above O is formulated as

$$O=(v,u_1,u_2,u_3)=\begin{bmatrix} 1 & 1 & a^2 & 0\\ a^3+a^2+a & 0 & 1 & 0\\ 1 & 1 & 0 & a^2+1\\ a^2+1 & 0 & a & 1 \end{bmatrix}$$

One could verify under this setting we have

$$O^TSO=\begin{bmatrix} a^3+a+1 & 0 & 0 & 0\\ 0 & a+1 & a^3 & 1\\ 0 & a^3 & a^3+a^2 & a\\ 0 & 1 & a & a^3+a^2+a \end{bmatrix},$$

$$O^TO=\begin{bmatrix} a^3+1 & 0 & 0 & 0\\ 0 & 0 & a^2 & a^2+1\\ 0 & a^2 & a^2+a & a\\ 0 & a^2+1 & a & a+1 \end{bmatrix}$$

In order to verify the claim, we will also pick randomly a matrix

$$P=\begin{bmatrix} a & a^2+1 & a^3 & 1\\ a^3+a+1 & a^2 & a^3+a^2+1 & 1\\ a+1 & a^3+a^2+a & a^3 & a^2+1\\ a^3+a^2+a+1 & a^3+1 & a+1 & a^3+a \end{bmatrix},$$

and also two random matrices in the space $\mathbb{F}_{16}[S]$:

$$Q_1=\begin{bmatrix} a+1 & a^3+a^2 & a^3+a^2+a & a^3+a\\ a^3+a^2 & a^3+a^2+a+1 & a^3+a & a^3+a^2\\ a^3+a^2+a & a^3+a & a^2+1 & 0\\ a^3+a & a^3+a^2 & 0 & a^2+1 \end{bmatrix},$$

$$Q_2=\begin{bmatrix} a^3+1 & a & a^3+a^2+a & 0\\ a & a^3+a+1 & 0 & a^3+a^2+a\\ a^3+a^2+a & 0 & a^2+a & 0\\ 0 & a^3+a^2+a & 0 & 1 \end{bmatrix}$$

Then one can directly verify

$$O^T(Q_1PQ_1^{-1}-Q_2PQ_2^{-1})O=\begin{bmatrix} 0 & a^3+1 & a & a\\ a+1 & a^2+a+1 & a^3+a+1 & a^3+a^2\\ a^3+a & a^2+1 & a^3+a+1 & a^3+a^2+1\\ a^3+a^2+1 & a & a+1 & a^3+a^2+1 \end{bmatrix}$$

Note that the $(1,1)$ entry is 0 as expected.

Thus, in a generic $(v, o, 16, 4)$-NOVA scheme, there exists a $4n$-dimensional null space consisting explicitly of elements expressed below:

$$X_i = \begin{bmatrix} x_{i,1} & \dots & x_{i,4} \\ 0_{l-1} & \dots & 0_{l-1} \end{bmatrix} O$$
$$= \begin{bmatrix} x_{i,1} & x_{i,2} & x_{i,3} & x_{i,4} \\ (a^3+a^2+a)x_{i,1} & (a^3+a^2+a)x_{i,2} & (a^3+a^2+a)x_{i,3} & (a^3+a^2+a)x_{i,4} \\ x_{i,1} & x_{i,2} & x_{i,3} & x_{i,4} \\ (a^2+1)x_{i,1} & (a^2+1)x_{i,2} & (a^2+1)x_{i,3} & (a^2+1)x_{i,4} \end{bmatrix}$$

where $x_{i,j} \in \mathbb{F}_{16}$ is arbitrary. As an instance, consider a claimed level-5-secure NOVA scheme with the parameter set $v = 28, o = 8$. The null space described above has dimension 144, while the total number of oil variables in this setting is 128, which is smaller.

In conclusion, we have

Corollary 3.5. There is a polynomial algorithm against NOVA scheme that generates an nl dimensional oil space whenever the matrix S has an eigenvalue in $\mathbb{F}_{16}$, or equivalently, the characteristic polynomial of S has a root in $\mathbb{F}_{16}$.

Proof. If an eigenvector is found for S, we may apply the proposition above and directly write out the solution space. □

3.2 Signature forgery attack

From the corollary in the previous section we know for a vulnerable S we could have an nl dimensional oil space. Below shows the proposed parameter setting for the NOVA signature scheme. Note that for all of the parameter sets we have $nl > l^2m$.

(v, o, q, l)	Claimed Security
$(23, 15, 16, 2)$	150
$(17, 7, 16, 3)$	149
$(14, 4, 16, 4)$	152
$(38, 23, 16, 2)$	219
$(26, 10, 16, 3)$	213
$(21, 6, 16, 4)$	213
$(54, 32, 16, 2)$	295
$(35, 14, 16, 3)$	288
$(28, 8, 16, 4)$	285

We now regard a (v, o, q, l)-NOVA scheme as a (l^2v, l^2o, q)-UOV scheme. Hence we have l^2m quadratic equations as public key, namely

$$\mathcal{P} = (P_{i,j})_{1 \le i \le m, 1 \le j \le l^2}.$$

- **Step 1**: In order to perform the forgery attack, we first collect all $Q_{\alpha k}$. If there exists a matrix whose minimal polynomial is of degree l, then we may well choose S to be that matrix as they will generate the same space. If none of the matrices satisfy such a condition, which is almost never the case unless S is really badly chosen, then take any matrix with minimal polynomial of the highest degree. In either case, the space $\mathbb{F}_q[S]$ can be recovered by an observation of all $Q_{\alpha k}$.
- **Step 2**: Once a generator of the space $\mathbb{F}_q[S]$ is found. We try using the Berlekamp's algorithm or the Cantor–Zassenhaus algorithm to find a root of the characteristic

polynomial of S. Once we find such a root, i.e. an eigenvalue, we could solve for the corresponding eigenvector. We may then apply the polynomial algorithm in the previous section to find out an nl dimensional null space N.

- **Step 3**: Now by polarization, we may write

  $$\mathcal{P}(n+v) = \mathcal{P}(n) + \mathcal{P}(v) + \mathcal{P}'(n,v).$$

  In order to sign $t \in \mathbb{F}_{16}^{l^2m}$, one could fix a random v, and then solve for $n \in N$ in the system

  $$\mathcal{P}(n) + \mathcal{P}(v) + \mathcal{P}'(n,v) = t.$$

  Note that n is chosen to be a vector in the null space we found which has dimension nl. Therefore $\mathcal{P}(n) = 0$ and the system is simply a linear system with l^2m equations. Since $nl > l^2m$, the system is underdetermined and will have a solution with an overwhelming probability.

- **Step 4**: Once a solution is found for the linear system, say n_0, sign the document with $v + n_0$. From the argument above we know it is a valid signature. We emphasize this algorithm can deal with a generic MQ-system with this certain structural map. It is not required the system is UOV-type.

The procedure above shows that

Corollary 3.6. There is a polynomial algorithm against NOVA scheme that generates a signature for an arbitrary vector $t \in \mathbb{F}_{16}^m$ whenever the matrix S has an eigenvalue in $\mathbb{F}_{16}$, or equivalently, the characteristic polynomial of S has a root in $\mathbb{F}_{16}$.

3.3 Security analysis

By a direct counting we get the proportion of the number of vulnerable S in 2 × 2 and 3 × 3 cases as follows. As for 4 × 4 case, the attack is only applicable if the characteristic polynomial has a factor of degree 1, and we did not find a good way to count the number of such matrices in the ambient space. Note that one may not apply Gauss' theorem on the number of irreducible polynomials in this case as similar matrices can share identical characteristic polynomials. However, we instead performed an experiment on 50000 random symmetric 4 × 4 matrices and the result shows around 65% of them are vulnerable.

l	# vulnerable S	Ratio
2	2176	53%
3	701776	67%
4	-	$\sim$ 65%

It can then be concluded that a randomly chosen S is prone to be vulnerable. Therefore, to guarantee that the attack does not hold, it is suggested one uses reject sampling to generate S if not fixes S.

References

[Beu21] W. Beullens, *Improved cryptanalysis of uov and rainbow*, Advances in cryptology – eurocrypt 2021, 2021, pp. 348–373.

[DS05] J. Ding and D. Schmidt, *Rainbow, a new multivariable polynomial signature scheme*, Applied cryptography and network security, 2005, pp. 164–175.

[FIKT21] H. Furue, Y. Ikematsu, Y. Kiyomura, and T. Takagi, *A new variant of unbalanced oil and vinegar using quotient ring: Qr-uov*, Advances in cryptology – asiacrypt 2021, 2021, pp. 187–217.

[KPG99] A. Kipnis, J. Patarin, and L. Goubin, *Unbalanced oil and vinegar signature schemes*, Advances in cryptology — eurocrypt '99, 1999, pp. 206–222.

[WTKC22] L.-C. Wang, P.-E. Tseng, Y.-L. Kuan, and C.-Y. Chou, *Nova, a noncommutative-ring based unbalanced oil and vinegar signature scheme with key-randomness alignment*, 2022. https://eprint.iacr.org/2022/665.