On the Security of Round 2 SNOVA

Lih-Chung Wang[1], Chun-Yen Chou[1], Jintai Ding[2], Yen-Liang Kuan[1], Jan Adriaan Leegwater[3], Ming-Siou Li[4], Bo-Shu Tseng[4], Po-En Tseng[*1], and Chia-Chun Wang[4]

[1]Department of Applied Mathematics, National Dong Hwa University, Taiwan
[2]Xi'an Jiaotong-Liverpool University, Suzhou, China
[3]Vacuas, Leiden, The Netherlands
[4]SNPQ, Kaohsiung, Taiwan

Abstract. SNOVA is a second-round candidate in the NIST ongoing project for additional signature schemes. During Round 1 evaluation, there were several discussions regarding the security of SNOVA. Among these discussions, Beullens pointed out that SNOVA public map could be expressed using the language of the whipping technique, which he leveraged to develop a forgery attack. In this paper, we analyze and discuss the whipping structure derived from SNOVA. Additionally, in response to the rank drop issue raised by Beullens, we made modifications in our Round 2 submission. Furthermore, our experiments show that the rank-dropping behavior of the whipping structure derived from Round 2 SNOVA is no different from that of a random whipping structure. As a result, Round 2 SNOVA is fully resistant to the forgery attacks with MinRank.

1 Introduction

With the advance and development of quantum computers, modern public-key cryptography is facing challenges. In response to this challenge, the U.S. National Institute for Standards and Technology (NIST) has organized a series of cryptographic competitions, including the selection and standardization of post-quantum cryptographic systems [7]. Recently, the post-quantum cryptography standards: FIPS-203, FIPS-204, and FIPS-205 have been published. In addition to these, NIST has also conducted an additional selection process for digital signatures [8].

After nearly a year and a half of analysis, NIST announced that fourteen candidates would advance to Round 2 of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography (PQC) Standardization Process. As

[*]Corresponding author: Po-En Tseng, Email: briantseng0320@gmail.com

a multivariate digital signature scheme, SNOVA [10] features relatively small public key and signature sizes and high efficiency, making it one of the Round 2 candidates.

During the analysis phase of Round 1, several discussions about SNOVA emerged [1, 3, 5, 6]. The most critical among them was a paper by Beullens [1], in which he demonstrated that SNOVA and MAYO share a similar whipping structure and developed an attack based on this observation. In response, the SNOVA team explored possible adjustment directions in [12], demonstrating that slight modifications could directly resist Beullens' attack. Following this, we conducted a more comprehensive analysis and investigation in our Round 2 adjustment.

Through our analysis, we found that his attack relied on the low-rank issue in SNOVA public map, making the Round 1 version of SNOVA susceptible to forgery attacks. However, the effectiveness of his attack is determined by the amount of rank drop in the public map. This renders his attack inefficient against the Round 2 version of SNOVA [11].

Contribution. In this paper, we analyze recent attacks on SNOVA. We detail our study of the MinRank distribution in Round 2 SNOVA. We provide the experimental evidence that the whipping structure derived from Round 2 SNOVA is indistinguishable from a fully random whipping structure. We show that the attacks of Beullens [1] and Cabarcas *et al.* [2] are no longer effective. On the other hand, we have completed an initial implementation of SNOVA with odd prime q. Using the parameter set $(24, 5, 11, 4)$ as an example, we present the corresponding performance data.

2 SNOVA

2.1 Notation

Let o and v denote the number of Oil and Vinegar variables. Let $n = o + v$ and $m = o$ denote the number of variables and the number of equations in the SNOVA public map. Let $\mathbb{F}_q$ be a finite field of order q. SNOVA public map is a multivariate quadratic map over $l \times l$ matrix ring $\mathcal{R} = \mathrm{Mat}_{l\times l}(\mathbb{F}_q)$ and a symmetric matrix S with irreducible characteristic polynomial. Let $[\mathbf{P}_1], \ldots, [\mathbf{P}_m] \in \mathcal{R}^{n\times n} \cong \mathbb{F}_q^{ln\times ln}$ be the matrices generated by the public key of SNOVA. For an $l \times l$ matrix A, we adapt the notation in Beullens attack [1], and a positive integer n, $\mathbf{A}^{\otimes n}$ denotes the block diagonal matrix with n copies of A on the block diagonal.

2.2 SNOVA public map

The public map of a (v, o, q, l) SNOVA scheme is defined as the following:

The subring $\mathbb{F}_q[S]$. Let S be an $l \times l$ symmetric matrix with its characteristic polynomial irreducible over $\mathbb{F}_q$. The subring $\mathbb{F}_q[S]$ of $\mathcal{R}$ is defined to be

$$\mathbb{F}_q[S] = \{a_0 + a_1 S + \cdots + a_{l-1} S^{l-1} : a_0, a_1, \cdots, a_{l-1} \in \mathbb{F}_q\}.$$

Public map. Given matrices $[\mathbf{P}_1], \ldots, [\mathbf{P}_m]$, the public map of SNOVA is $\widetilde{P} = (\widetilde{P}_1, \ldots, \widetilde{P}_m) : \mathcal{R}^n \to \mathcal{R}^m$, for $i \in \{1, \ldots, m\}$,

$$\begin{aligned} \widetilde{P}_i(\mathbf{U}) &:= \sum_{\alpha=0}^{l^2+l-1} \sum_{j=1}^{n} \sum_{k=1}^{n} A_{i,\alpha} \cdot U_j^t (Q_{i,\alpha,1} P_{i',jk} Q_{i,\alpha,2}) U_k \cdot B_{i,\alpha} \\ &= \sum_{\alpha=0}^{l^2+l-1} A_{i,\alpha} \cdot \mathbf{U}^t \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot [\mathbf{P}_{i'}] \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} \cdot B_{i,\alpha}, \end{aligned} \tag{2.1}$$

where $i' = (i + \alpha) \mod m$ and $P_{i',jk}$ is the (j,k)-th entry of matrix $[\mathbf{P}_{i'}]$. Here, $\mathbf{U} = (U_1, \ldots, U_n)^t$ is regarded as a $ln \times l$ matrix over $\mathbb{F}_q$, $Q_{i,\alpha,1}, Q_{i,\alpha,2} \in \mathbb{F}_q[S]$ and $A_{i,\alpha}, B_{i,\alpha} \in \mathcal{R}$. Note that $\widetilde{P}_i(\mathbf{U})$ consists of l^2 homogeneous quadratic polynomials of the entries of $\mathbf{U}$, involving a total of $l^2 n$ variables. More details can be found in SNOVA NIST Round 2 specification [11].

2.3 SNOVA with whipping structure

Define the bilinear map $\mathcal{B} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q^{l^2 m}$ by

$$\mathcal{B}_{i,a,b}(\mathbf{u}, \mathbf{v}) := B_i^{(a,b)}(\mathbf{u}, \mathbf{v}), \tag{2.2}$$

where, for $i \in \{1, \ldots, m\}$ and $(a, b) \in \{0, \ldots, l-1\}^2$,

$$B_i^{(a,b)} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q, \ B_i^{(a,b)}(\mathbf{u}, \mathbf{v}) := \mathbf{u}^t \left(\mathbf{S}^a\right)^{\otimes n} [\mathbf{P}_i] \left(\mathbf{S}^b\right)^{\otimes n} \mathbf{v}.$$

As shown in Beullens paper [1], the public map of SNOVA can be represented in a whipping structure form (2.3):

Lemma 1 (Corollary 1 in [1])**.** *Let $\mathcal{B} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q^{l^2 m}$ be the bilinear map defined by the equation (2.2). Then, for all $j, k \in \{0, \ldots, l-1\}$, there exist matrices $\mathbf{E}_{j,k} \in \mathbb{F}_q^{l^2 m \times l^2 m}$ such that the SNOVA public map $\widetilde{P} : \mathcal{R}^n \to \mathcal{R}^m$ can be expressed as*

$$\widetilde{P}(\mathbf{U}) = \sum_{j=0}^{l-1} \sum_{k=0}^{l-1} \mathbf{E}_{j,k} \cdot \mathcal{B}(\mathbf{u}_j, \mathbf{u}_k). \tag{2.3}$$

where $\mathbf{u}_j$ is the $(j+1)$-th column of $\mathbf{U}$ for $j \in \{0, \ldots, l-1\}$.

Furthermore, as noted by Beullens [1], for all $j, k \in \{0, \ldots, l-1\}$, the matrix $\mathbf{E}_{j,k}$ corresponding to the Round 1 SNOVA public map is a block-diagonal matrix with identical diagonal blocks, i.e., $\mathbf{E}_{j,k} = \tilde{\mathbf{E}}_{j,k}^{\otimes m}$ for some $l^2 \times l^2$ matrix $\tilde{\mathbf{E}}_{j,k}$. The most immediate impact is that even a slight rank drop in the linear combinations of $\tilde{\mathbf{E}}_{j,k}$ can lead to a substantial overall rank drop in the corresponding linear combinations of $\mathbf{E}_{j,k}$.

However, this is not the case for Round 2 SNOVA. Through the modifications introduced in Round 2, each equation no longer shares a common set of ABQ matrices (i.e. the matrices $A_{i,\alpha}$, $Q_{i,\alpha,1}$, $Q_{i,\alpha,2}$, $B_{i,\alpha}$), and for every fixed i, more entries of $[\mathbf{P}_1], \ldots, [\mathbf{P}_m]$ are involved in a single equation $\widetilde{P}_i$. As a result, the block-diagonal structure is broken. In the following theorem, we describe the explicitly construction and the structure of $\mathbf{E}_{j,k}$ in the Round 2 case. Appendix A has an explicit expression for $\mathbf{E}_{j,k}$ in terms of the coefficients of ABQ matrices in SNOVA public map and a toy example to demonstrate the computation details of Theorem 2.

Theorem 2. *For fixed $j, k \in \{0, \ldots, l-1\}$, consider $\mathbf{E}_{j,k} \in \mathbb{F}_q^{l^2 m \times l^2 m}$ as an $m \times m$ block matrix, where each block is of size $l^2 \times l^2$. Fix $i, i' \in \{1, \ldots, m\}$. The (i, i')-th block entry of $\mathbf{E}_{j,k}$ is determined by the set*

$$\left\{ A_{i,\alpha},\ Q_{i,\alpha,1},\ Q_{i,\alpha,2},\ B_{i,\alpha} \;\middle|\; \alpha \in \{0, \ldots, l^2 + l - 1\} \text{ and } i + \alpha \equiv i' \pmod{m} \right\}.$$

More precisely, for each α such that $i + \alpha \equiv i' \pmod{m}$, the term

$$A_{i,\alpha} \cdot \mathbf{U}^t \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot [\mathbf{P}_{i'}] \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} \cdot B_{i,\alpha}$$

in $\widetilde{P}_i(\mathbf{U})$ yields an $l^2 \times l^2$ matrix contributing to bilinear form $B_{i'}^{(a,b)}(\mathbf{u}_j, \mathbf{u}_k)$ for each quadruple $(j, k, a, b) \in \{0, \ldots, l-1\}^4$, determined by the matrices $A_{i,\alpha}, Q_{i,\alpha,1}, Q_{i,\alpha,2}, B_{i,\alpha}$. The (i, i')-th block of $\mathbf{E}_{j,k}$ is then the sum of all such $l^2 \times l^2$ matrices over the indices α satisfying $i + \alpha \equiv i' \pmod{m}$.

Proof. Since $Q_{i,\alpha,1}$ and $Q_{i,\alpha,2}$ are elements of $\mathbb{F}_q[S]$, they can be expressed as linear combinations of $I, S, \ldots, S^{l-1}$. Therefore, for fixed $i, i' \in \{1, \ldots, m\}$ and fixed α satisfying $i + \alpha \equiv i' \pmod{m}$, each entry of the matrix

$$A_{i,\alpha} \cdot \mathbf{U}^t \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot [\mathbf{P}_{i'}] \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} \cdot B_{i,\alpha}$$

is a linear combination of the bilinear forms $B_{i'}^{(a,b)}(\mathbf{u}_j, \mathbf{u}_k)$ for $0 \leq j, k \leq l-1$, which contributes a summand of the (i, i')-th block of $\mathbf{E}_{j,k}$. Note that, for fixed i, i', each such term contains l^2 entries and depends only on the single public key $[\mathbf{P}_{i'}]$. By collecting the coefficients in these linear combinations, we obtain an $l^2 \times l^2$ matrix representing a specific linear combination of the bilinear forms $B_{i'}^{(a,b)}(\mathbf{u}_j, \mathbf{u}_k)$, determined by the entries of $A_{i,\alpha}$, $Q_{i,\alpha,1}$, $Q_{i,\alpha,2}$, and $B_{i,\alpha}$.

By running over α, we obtain a total of $l^2 + l$ such $l^2 \times l^2$ matrices. Each $l^2 \times l^2$ matrices corresponding to indices α that satisfy the same congruence condition $i + \alpha \equiv i' \pmod{m}$ is a summand of the (i, i')-th block of $\mathbf{E}_{j,k}$. Hence, the (i, i')-th block of $\mathbf{E}_{j,k}$ is the sum of all such $l^2 \times l^2$ matrices indexed by α with $i + \alpha \equiv i' \pmod{m}$. □

Theorem 2 provides a method to construct each (i, i')-th block of $\mathbf{E}_{j,k}$ for all $i, i' \in \{1, \ldots, m\}$, enabling us to analyze the overall structure of the whipping matrices $\mathbf{E}_{j,k}$.

Theorem 3. *Consider $\mathbf{E}_{j,k} \in \mathbb{F}_q^{l^2m \times l^2m}$ as an $m \times m$ block matrix, where each block is of size $l^2 \times l^2$. Then, the $\mathbf{E}_{j,k}$ matrices corresponding to Round 2 SNOVA public map $\widetilde{P}$ is no longer block diagonal with identical blocks. Equivalently, with Round 2 SNOVA public map, $\mathbf{E}_{j,k} \neq \tilde{\mathbf{E}}_{j,k}^{\otimes m}$ for any $\tilde{\mathbf{E}}_{j,k}$, in general.*

Proof. By running through i' from 1 to m, Theorem 2 yields a collection of $l^2 \times l^2$ matrices corresponding to $\widetilde{P}_i(\mathbf{U})$. These matrices form the block entries in the i-th row of the matrices $\mathbf{E}_{j,k}$, for all $j, k \in \{0, \ldots, l-1\}$. Thus, for each fixed i, we obtain the full i-th row of $\mathbf{E}_{j,k}$. Finally, by assembling these rows over all i, we reconstruct the entire matrices $\mathbf{E}_{j,k}$. Since $m = o > 1$, in general, the effect of varying i' in $\widetilde{P}_i$ generally breaks the block-diagonal structure. □

Remark 4. In Round 1 case, for every $i \in \{1, \ldots, m\}$, we have $i' = i$ for all $\alpha \in \{0, \ldots, l^2 + l - 1\}$. Therefore, the only non-zero block entries in $\mathbf{E}_{j,k}$ are the diagonal blocks. Furthermore, since for every $i \in \{1, \ldots, m\}$, $\widetilde{P}_i(\mathbf{U})$ share a common set of ABQ matrices. Therefore, in this case, $\mathbf{E}_{j,k}$ is a block diagonal matrices with identical diagonal blocks. As shown in Beullens paper [1], this issue accounts for the higher likelihood of weak keys in the Round 1 design [10].

3 Forgery attack proposed by Beullens

$\mathbf{E}_\alpha$ attack. This attack attempts to forge a signature by solving for $\mathbf{U}$ such that the columns $\mathbf{u}_j = a_j\mathbf{u}_0 + \mathbf{v}_j$ where $\mathbf{v}_j \in \mathbb{F}_q^{ln}$ is randomly chosen for all $j \in \{1, \ldots, l-1\}$, for some $a_1, \ldots, a_{l-1} \in \mathbb{F}_q$. Under the representation (2.3), the quadratic part of public map $\widetilde{P}(\mathbf{U})$ is $\mathbf{E}_\alpha \cdot \mathcal{B}(\mathbf{u}_0, \mathbf{u}_0)$ where

$$\mathbf{E}_\alpha = \sum_{j=0}^{l-1}\sum_{k=0}^{l-1} a_j a_k \mathbf{E}_{j,k}. \tag{3.1}$$

The attack is divided into two steps:

- Find a linear combination of matrices $\mathbf{E}_{j,k}$ has rank drop. This yields a generalized MinRank problem.
- Following the first step, an attacker aiming to forge a signature only needs to solve a smaller MQ system, rather than tackling the full signature forgery problem directly.

$\mathbf{E}_\mathbf{R}$ attack. Leveraging the algebraic structure of $\mathbb{F}_q[S]$, the generalized MinRank problem can be further extended. Instead of using scalar coefficients a_j, one considers

$$\mathbf{u}_j = \mathbf{R}_j^{\otimes n}\mathbf{u}_0 + \mathbf{v}_j,$$

for $j \in \{1, \ldots, l-1\}$, where each $\mathbf{R}_j \in \mathbb{F}_q[S]$. This leads to a more general MinRank problem with $l(l-1)$ variables and yields a new matrix $\mathbf{E}_\mathbf{R}$, representing the quadratic part of $\widetilde{P}(\mathbf{U})$. This extended setting allows the attacker to search over a richer space of linear combinations, increasing the chance of finding a matrix with lower rank, thus making the attack more effective. The overall idea is to find some set of $\mathbf{R}_1, \ldots, \mathbf{R}_{l-1}$ matrices so that the MQ problem for $\mathbf{u}_0$ has fewer variables than $\mathbf{E}_\alpha$ attack.

In the following, we provide an explicit expression of $\mathbf{E}_{\mathbf{R}}$.

Lemma 5. *Let $\mathcal{B} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q^{l^2 m}$ be the bilinear map defined by the equation (2.2). For $i \in \{1, \ldots, m\}$ and fixed $a, b, a', b' \in \{0, \ldots, l-1\}$, the bilinear form $B_i^{(a,b)}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right)$ is a linear combination of*

$$\{B_i^{(0,0)}(\mathbf{u},\mathbf{v}), B_i^{(0,1)}(\mathbf{u},\mathbf{v}), \ldots, B_i^{(l-1,l-2)}(\mathbf{u},\mathbf{v}), B_i^{(l-1,l-1)}(\mathbf{u},\mathbf{v})\}.$$

Therefore, for $a', b' \in \{0, \ldots, l-1\}$, there exists a matrix $\tilde{\mathbf{E}}'_{a'b'} \in \mathbb{F}_q^{l^2 \times l^2}$ such that

$$\begin{bmatrix} B_i^{(0+a',0+b')}(\mathbf{u},\mathbf{v}) \\ B_i^{(0+a',1+b')}(\mathbf{u},\mathbf{v}) \\ \vdots \\ B_i^{(l-1+a',l-2+b')}(\mathbf{u},\mathbf{v}) \\ B_i^{(l-1+a',l-1+b')}(\mathbf{u},\mathbf{v}) \end{bmatrix} = \tilde{\mathbf{E}}'_{a'b'} \cdot \begin{bmatrix} B_i^{(0,0)}(\mathbf{u},\mathbf{v}) \\ B_i^{(0,1)}(\mathbf{u},\mathbf{v}) \\ \vdots \\ B_i^{(l-1,l-2)}(\mathbf{u},\mathbf{v}) \\ B_i^{(l-1,l-1)}(\mathbf{u},\mathbf{v}) \end{bmatrix}.$$

Proof. Since $B_i^{(a,b)}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right) = B_i^{(a+a',b+b')}(\mathbf{u},\mathbf{v})$, by using the Cayley-Hamilton theorem on $S^{a+a'}$ and $S^{b+b'}$, we can write $S^{a+a'}$ and $S^{b+b'}$ as linear combinations of $\{I, \ldots, S^{l-1}\}$.

By re-collecting the terms, this shows that $B_i^{(a+a',b+b')}(\mathbf{u},\mathbf{v})$ can be expressed as a linear combination of $\{B_i^{(0,0)}(\mathbf{u},\mathbf{v}), B_i^{(0,1)}(\mathbf{u},\mathbf{v}), \ldots, B_i^{(l-1,l-1)}(\mathbf{u},\mathbf{v})\}$. Note that the coefficients of linear combinations form the (a,b)-th row of $\tilde{\mathbf{E}}'_{a'b'}$. Therefore, by collecting the coefficients of linear combinations with respect to the index (a,b) where $a, b \in \{0, \ldots, l-1\}$, we can obtain the matrix $\tilde{\mathbf{E}}'_{a'b'}$ for fixed $a', b' \in \{0, \ldots, l-1\}$. □

Corollary 6. *Let $\mathcal{B} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q^{l^2 m}$ be the bilinear map defined by the equation (2.2). Then, there exists a matrix $\mathbf{E}'_{a',b'} \in \mathbb{F}_q^{l^2 m \times l^2 m}$ such that*

$$\mathcal{B}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right) = \mathbf{E}'_{a',b'} \cdot \mathcal{B}(\mathbf{u},\mathbf{v})$$

where $a', b' \in \{0, \ldots, l-1\}$. Moreover, $\mathbf{E}'_{a',b'} = \left(\tilde{\mathbf{E}}'_{a',b'}\right)^{\otimes m}$ where $\tilde{\mathbf{E}}'_{a',b'}$ are the matrices constructed by Lemma 5.

Proof. Fixed $i \in \{1, \ldots, m\}$. For $a, b \in \{0, \ldots, l-1\}$, we apply Lemma 5 on the entries of $\mathcal{B}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right)$ corresponding to index i, i.e., the entries $B_i^{(a,b)}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right)$. Then, we obtain the matrices $\tilde{\mathbf{E}}'_{a',b'}$. By noticing that the construction of $\tilde{\mathbf{E}}'_{a',b'}$ is independent with the index i, we then have $\mathbf{E}'_{a',b'} = \left(\tilde{\mathbf{E}}'_{a',b'}\right)^{\otimes m}$. Hence, $\mathcal{B}\left((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}, (\mathbf{S}^{b'})^{\otimes n}\mathbf{v}\right) = \mathbf{E}'_{a',b'} \cdot \mathcal{B}(\mathbf{u}, \mathbf{v})$. □

With these in place, we are able to derive the explicit expression for $\mathbf{E}_{\mathbf{R}}$.

Theorem 7. *For SNOVA public map $\widetilde{P}(\mathbf{U})$, if we let $\mathbf{u}_j = \mathbf{R}_j^{\otimes n}\mathbf{u}_0 + \mathbf{v}_j$, where $R_j = \sum_{a'=0}^{l-1} r_{j,a'} S^{a'} \in \mathbb{F}_q[S]$, for $j = 1, \ldots, l-1$. Then, the quadratic part of $\widetilde{P}(\mathbf{U})$ is of the form*

$$\mathbf{E}_{\mathbf{R}}\mathcal{B}(\mathbf{u}_0, \mathbf{u}_0).$$

More precisely,

$$\mathbf{E}_{\mathbf{R}} = \sum_{jk}\sum_{a'b'} r_{j,a'} r_{k,b'} \mathbf{E}_{j,k,a',b'}$$

where $\mathbf{E}_{j,k,a',b'} = \mathbf{E}_{j,k}\mathbf{E}'_{a',b'}$ for those $\mathbf{E}_{j,k}, \mathbf{E}'_{a',b'}$ matrices derived from Lemma 1 and Corollary 6.

Proof. By Lemma 1 and Corollary 6, for $j, k \in \{1, \ldots, l-1\}$, the quadratic part is

$$\begin{aligned} &\sum_{jk} \mathbf{E}_{j,k}\mathcal{B}(\mathbf{R}_j^{\otimes n}\mathbf{u}_0, \mathbf{R}_k^{\otimes n}\mathbf{u}_0) \\ =&\sum_{jk}\sum_{a'b'} r_{j,a'} r_{k,b'} \mathbf{E}_{j,k}\mathcal{B}((\mathbf{S}^{a'})^{\otimes n}\mathbf{u}_0, (\mathbf{S}^{b'})^{\otimes n}\mathbf{u}_0) \\ =&\sum_{jk}\sum_{a'b'} r_{j,a'} r_{k,b'} \mathbf{E}_{j,k}\mathbf{E}'_{a',b'}\mathcal{B}(\mathbf{u}_0, \mathbf{u}_0) \end{aligned} \tag{3.2}$$

Therefore, $\mathbf{E}_{\mathbf{R}} = \sum_{jk}\sum_{a'b'} r_{j,a'} r_{k,b'} \mathbf{E}_{j,k,a',b'}$. □

This gives us a generalized MinRank problem with $l(l-1)$ variables and l^4 matrices. The effectiveness of this attack hinges on the extent to which the rank of $\mathbf{E}_{\mathbf{R}}$ can be reduced. For an attacker, finding a lower-rank $\mathbf{E}_{\mathbf{R}}$ significantly facilitates the attack. In other words, ensuring SNOVA's resistance against such forgery attacks critically depends on the strength of the ABQ matrices that generate $\mathbf{E}_{\mathbf{R}}$. In the design of Round 2 SNOVA [11], each key pair uses a fixed seed to deterministically generate the ABQ matrices. We then perform an exhaustive search on the coefficients $r_{j,a'}$ to verify the minimal rank of the resulting $\mathbf{E}_{\mathbf{R}}$. This ensures that every public key provides the same level of security against this class of forgery attacks, effectively avoiding the issue of weak keys.

In the next section we show that, under the modifications introduced in Round 2 evaluation [11], the distribution of the minimal rank of the $\mathbf{E}_{\mathbf{R}}$ matrices, derived from the ABQ matrices, is statistically indistinguishable from that of a random instance. By eliminating the block-diagonal structure present in the Round 1 design, these modifications significantly strengthen the scheme's resistance to forgery attacks based on the MinRank problem.

4 MinRank problem of $\mathbf{E_R}$ and its structure

We can observe that the severity of the rank drop in $\mathbf{E_R}$ is determined by its structure. Originally, Beullens exploited the block-diagonal structure to carry out his attack. It's worth noting that Lemma 1 shows us there are two different ways to define the SNOVA public map[1]:

- Approach 1: using ring equation (2.1). In this approach, the entries of $\mathbf{E}_{j,k}$ are determined by the entries of the ABQ matrices in $\widetilde{P}(\mathbf{U})$. Therefore, the coefficients of the entries of $\mathbf{E_R}$ come from a combinations of the entries of the ABQ matrices.
- Approach 2: using bilinear form (2.3). In this approach, the $\mathbf{E}_{j,k}$ matrices can either be explicitly determined (such as in MAYO, $\mathbf{E}_{j,k}$ are the matrices corresponding to the field multiplication), or generated randomly without any additional structure. In the former case, where the $\mathbf{E}_{j,k}$ matrices are explicitly chosen, the entries of $\mathbf{E_R}$ are determined by the entries of $\mathbf{E}_{j,k}$. In the latter case, if the $\mathbf{E}_{j,k}$ matrices are generated randomly, then $\mathbf{E_R}$ will also be determined randomly.

We found that the $\mathbf{E_R}$ matrices derived from Approach 1 exhibit the same rank drop distribution as those derived from randomly generated $\mathbf{E}_{j,k}$ matrices in Approach 2. The distributions of the minimal rank of $\mathbf{E_R}$ in two approaches are indistinguishable. In other words, even when SNOVA public map is defined via ring equations (the Approach 1), under the modifications introduced in Round 2, the structure of the resulting $\mathbf{E_R}$ matrices is indistinguishable from that of random matrices in the sense of rank drop. This effectively eliminates the structural weaknesses that previously raised security concerns. In the following section, we present experimental data to support this observation. Note that the similar argument on the distribution of minimal rank of $\mathbf{E_R}$ can be found in Beullens paper [1].

4.1 Full rank possibility

We would first like to investigate the possibility of achieving full-rank $\mathbf{E_R}$. We found that ensuring all $\mathbf{E_R}$ matrices are full rank is significantly more difficult than ensuring all $\mathbf{E}_\alpha$ matrices are of full rank. To ensure that all $\mathbf{E}_\alpha$ are full rank, it suffices to find a set of $\mathbf{E}_{j,k}$ matrices that satisfy the full-rank condition: every non-trivial linear combination of the $\mathbf{E}_{j,k}$ matrices is of full rank.

One of the possible ways is to choose a $l^2m \times l^2m$ matrix E with an irreducible characteristic polynomial. As $\mathbb{F}_q[E]$ is a field, all non-zero elements are invertible. Then, for $j,k \in \{0,\dots l-1\}$, let

$$\mathbf{E}_{j,k} := E^{j\cdot l+k}. \tag{4.1}$$

[1] If the index α is allowed to run up to l^4m the relation can generally be reversed; for any set of $\mathbf{E}_{j,k}$ matrices an equivalent set of ABQ matrices can be found.

This is similar to MAYO case: the matrix E is chosen to be the companion matrix of some irreducible polynomial. However, choosing E as the companion matrix of an irreducible polynomial does not guarantee that all $\mathbf{E_R}$ matrices are of full rank. The experimental results, shown in Table 1, confirm this observation. Consequently, we have not yet found a construction of the $\mathbf{E}_{j,k}$ matrices that ensures all $\mathbf{E_R}$ matrices are of full rank.

Table 1: Distribution of the rank drop $d(\mathbf{E_R})$ for the full rank $\mathbf{E_R}$ attempt in the case of $(37, 17, 16, 2)$. The data is for 1000 randomly chosen permutations of rows and columns. For comparison we added similar data for fully random $\mathbf{E}_{j,k}$ matrices and the Round 2 proposal [11].

the distribution of minimal rank of $\mathbf{E_R}$			
$d(\mathbf{E_R})$	$\mathbf{E}_{j,k}$ by (4.1)	random $\mathbf{E}_{j,k}$	$\mathbf{E}_{j,k}$ by (2.1)
0	0	0	0
1	983	995	990
2	17	5	10

4.2 Experimental results on rank drop

As shown in the previous section, choosing $\mathbf{E}_{j,k}$ as the matrices corresponding to the $\mathrm{GF}(q^{l^2m})$ field multiplications does not make $\mathbf{E_R}$ full rank. In this section, we investigate the benefits of accepting the rank drop and using a set of random $\mathbf{E}_{j,k}$ matrices. This is done from a security perspective. Actually using a fully random set of $\mathbf{E}_{j,k}$ matrices will not result in a practical, efficient scheme.

We define the rank drop

$$d(\mathbf{E_R}) := l^2m - \mathrm{MinRank}(\mathbf{E_R}). \tag{4.2}$$

Extending the argument of Beullens [1], the minimal value of the rank drop d_{min} is expected to be $l - 1$ for the ”fully whipped” version with random $\mathbf{E}_{j,k}$ matrices.

The question can be asked to what extent the Approach 1 (SNOVA defined by 2.1) is comparable to the Approach 2 (the random $\mathbf{E}_{j,k}$ matrix approach). For this, we have collected statistics on the rank drop for $(37, 17, 16, 2)$ in Table 2 and for $(25, 8, 16, 3)$ in Table 3. Here, we discuss the impact of different values of n_α on the rank distribution of $\mathbf{E_R}$, where n_α is defined by the number of terms in the summation over α, i.e., we consider

$$\widetilde{P}_i(\mathbf{U}) := \sum_{\alpha=0}^{n_\alpha} \sum_{j=1}^{n} \sum_{k=1}^{n} A_{i,\alpha} \cdot U_j^t (Q_{i,\alpha,1} P_{i',jk} Q_{i,\alpha,2}) U_k \cdot B_{i,\alpha}.$$

Based on these results, Round 2 SNOVA was decided to use $n_\alpha = l^2 + l$ and to fix the ABQ matrices for the $l = 2, 3$ parameter sets. For $l = 4$, there are $q^{l^2-l} = 2^{48}$ possibility for $\mathbf{E_R}$. Considering all these values is thus infeasible for us. In Table 4, we present results on rank drop for 50 different values of ABQ matrices or $\mathbf{E}_{j,k}$ evaluated for 10^6 random values of $\mathbf{E}_\mathbf{R}$. These results suggest that all values for n_α result in ABQ matrices that are as good as the random $\mathbf{E}_{j,k}$ matrices.

Table 2: Distribution of the rank drop $d(\mathbf{E}_\mathbf{R})$ for $(v, o, q, l) = (37, 17, 16, 2)$ depending on the number of terms n_α in the sum over α. The last column is the result using random $\mathbf{E}_{j,k}$ matrices generated from a XOF. Only for $l = 2$ parameter sets an exhaustive search over all values of $\mathbf{E}_\mathbf{R}$ for a large number of different ABQ matrices sets is feasible.

$d(\mathbf{E}_\mathbf{R})$	$n_\alpha = 4$	$n_\alpha = 5$	$n_\alpha = 6$	$n_\alpha = 8$	random
0	0	0	0	0	0
1	0	79592	99155	99559	99602
2	420	19404	841	441	398
3	8088	967	4		
4	27267	36			
5	33206	1			
6	20791				
7	7803				
8	2039				
9	334				
10	46				
11	5				
12	1				

Table 3: Frequency distribution of the rank drop $d(\mathbf{E}_\mathbf{R})$ for a number of values of n_α compared to that of a random set of $\mathbf{E}_{j,k}$ matrices in the case of $(v, o, q, l) = (25, 8, 16, 3)$. The data is for all values of $\mathbf{E}_\mathbf{R}$ for 25 seeds.

$d(\mathbf{E}_\mathbf{R})$	$n_\alpha = 9$	$n_\alpha = 10$	$n_\alpha = 11$	$n_\alpha = 12$	random
0	391423736	391496371	391512986	391505232	391507712
1	27880527	27842144	27829885	27837675	27835272
2	37208	11252	6896	6860	6783
3	8285				
4	7				
5	4				

Table 4: Frequency distribution of the rank drop $d(\mathbf{E_R})$ for different values of n_α, compared to that of a random set of $\mathbf{E}_{j,k}$ matrices for $(v, o, q, l) = (24, 5, 16, 4)$. The data is based on 10^6 samples of $\mathbf{E_R}$, generated using 150 seeds. In the last column, Q represents the ratio of the number of samples with a rank drop $\geq d$ to the total number of samples for the random matrices. The heuristic of Beullens [1] states that $d(\mathbf{E_R})$ follows a q^{-d^2} distribution. If the heuristic holds, then $\log_2(Q)$ should be approximately $-4d^2$, which aligns well with the data.

$d(\mathbf{E_R})$	$n_\alpha = 16$	$n_\alpha = 17$	$n_\alpha = 18$	$n_\alpha = 20$	random	$\log_2(Q)$
0	140036838	140042410	140041395	140043721	140039787	0
1	9960759	9955084	9956087	9953795	9957839	-3.913
2	2403	2506	2518	2484	2374	-15.947

Table 5: Frequency distribution of the rank drop $d(\mathbf{E_R})$ for Rank 5, the case of $(v, o, q, l) = (24, 5, 16, 5)$. The data is based on 10^6 samples for $\mathbf{E_R}$, generated using 35 seeds. In the last column, Q is the ratio of the numbers of samples with a rank drop $\geq d$ to the total number of samples for the random matrices. The heuristic of Beullens [1] states that $d(\mathbf{E_R})$ follows a q^{-d^2} distribution. If the heuristic works then $\log_2(Q)$ should be $-4d^2$, which fits the data well.

$d(\mathbf{E_R})$	$n_\alpha = 25$	$n_\alpha = 26$	$n_\alpha = 27$	$n_\alpha = 30$	random	$\log_2(Q)$
0	32675723	32674550	32675192	32676376	32675030	0
1	2323700	2324898	2324233	2323045	2324414	-3.912
2	577	552	575	579	556	-15.942

For the random set of $\mathbf{E}_{j,k}$ matrices, the frequency distribution of the matrix $\mathbf{E_R}$ has rank $\leq l^2m - d$ with probability of about q^{-d^2}, where $d = d(\mathbf{E_R})$. In Table 2, 3, we present numerical results supporting this frequency distribution. For values of $n_\alpha < l^2+l$, we observed increasing deviations between the experimental results and the heuristic distribution. This suggests that when $n_\alpha < l^2 + l$, the distribution of $\mathbf{E_R}$ generated by ABQ matrices may not be well-approximated to a random matrix. Extending the argument of Beullens [1], we expect the minimal rank of $\mathbf{E_R}$ when considering all values of $R_1, \dots, R_{l-1}$ is $l^2m - l + 1$.

Complexity and weak keys. The cost of this attack is estimated by the complexity of solving an $MQ(ln - l^2m + \mathrm{rank}(\mathbf{E_R}), \mathrm{rank}(\mathbf{E_R}), q)$. If $\mathbf{E_R}$ is a block-diagonal matrix with identical blocks, this would result in an excessively low rank. In Beullens attack [1], such a weak key issue was pointed out. For $l = 2, 3$, we can perform exhaustive search to determine the minimal rank. In SNOVA NIST Round 2 specification [11], for the case of $l = 2, 3$, a fixed seed was chosen to ensure that all public maps have the same strength. According to our analysis, for the cases $l = 4, 5$, the rank degradation behavior of $\mathbf{E_R}$ is statistically indistinguishable from that of a random matrix. As a result, the expected minimal rank is approximately l^2m-l+1. The efficiency of the forgery attacks proposed by Beullens and by Cabarcas *et al.* [1, 2] is closely related to $\mathrm{rank}(\mathbf{E_R})$. Their attacks utilize the structure that the rank of the $\mathbf{E_R}$ tends to drop for the Round 1 case, where $\mathbf{E_R}$ is a block matrix with identical diagonal blocks, so even a slight rank drop in each diagonal block can significantly amplify the overall rank drop of $\mathbf{E_R}$. However, our analysis shows that, in the Round 2 setting, the distribution of rank drops in $\mathbf{E_R}$ is indistinguishable from that of a random instance. This behavior in the public map effectively mitigates their attacks.

Other known attacks. In addition to the forgery attack proposed by Beullens, other methods such as those presented in [3, 5, 6] focus primarily on key recovery attacks. For Round 2 SNOVA, the complexity of these attacks remains well above the NIST security requirements. For more details, we refer to [11].

4.3 Considering fields of odd prime order

Recently, a new key-recovering algorithm for UOV scheme (and UOV variants) in characteristic 2 was proposed by Lars Ran [9]. There are two possible countermeasures: the more straightforward one is to increase the number of vinegar variables. The other is to choose a field $\mathbb{F}_q$ with an odd prime q instead of $\mathbb{F}_{16}$.

Increasing the number of vinegar variables v does not affect the public key size and makes the "project down" step in Ran's attack more difficult. For SNOVA, increasing the number of vinegar variables also can help to prevent wedge-like attacks. We can adjust the number of vinegar variables to ensure the complexity meets the required level. However, increasing the number of vinegar variables may slightly impact performance.

For UOV, choosing an odd prime q as a countermeasure can block Ran's attack since in this case the polar forms of UOV are not alternating. For SNOVA, one can consider the alternating form $q_i(x, y) = x^t([\mathbf{P}_i] - [\mathbf{P}_i]^t)y$ which still satisfies the Lemma 2 and proposition 1 of Ran's paper [9]. Moreover, Peigen Li [4] suggested that the attacker could actually consider the form

$$q_i(x, y) = x^t((S^a)^{\otimes n}[\mathbf{P}_i](S^b)^{\otimes n} - ((S^a)^{\otimes n}[\mathbf{P}_i](S^b)^{\otimes n})^t)y,$$

which serves as a new starting point of a variant of Ran's attack. Therefore, we need further study to eliminate the alternating forms induced by public key completely. Also note that, the kernel prediction in Ran's attack does not apply to SNOVA [9].

Choosing an odd prime q allows SNOVA to use a symmetric public matrix as first suggested by Ikematsu and Akiyama [3]. Note that it is not a good idea to use a symmetric public matrix for q is even. The strategy "symmetric $[\mathbf{P}_i]$ + odd prime q" will reduce the number of the alternating forms roughly a factor of 2. We consider it likely that some form of Ran's wedge attack can be formulated for SNOVA. Based on our study, the strategy of using a symmetric $[\mathbf{P}_i]$ together with an odd prime q offers several advantages: it reduces the public key size by half, and according to our experiments this also improves the efficiency of signature verification.

While using a symmetric public matrix when q is an odd prime may not entirely block the wedge attack, we are proposing to use it as alternative parameter set as it allows for a reduction of the public key size by almost a factor of 2. When working in odd characteristic, symmetrizing $[\mathbf{P}_i]$ may introduce new attacks. We may consider approaches similar to the following to mitigate the risks:

- choose q such that $o \cdot \frac{l(l-1)}{2} \log_2(q) > 128, 192, 256$,
- require that none of the matrices in the signature is symmetric.

We have taken both of these measures. A more detailed security analysis of using an odd prime q and symmetric $[\mathbf{P}_i]$, along with complete parameter sets and performance benchmarks, will be presented in a forthcoming paper. We provide some example parameter sets in the following table:

Table 6: Preliminary key-sizes and lengths of the signature of odd q SNOVA parameter settings (in bytes).

SL	(v, o, q, l)	Public Key Size	Signature Size	Secret Key Size
I	(24, 5, 23, 4)	616	282	48
III	(37, 8, 19, 4)	2269	400	48
V	(60, 10, 23, 4)	4702	656	48

Changing q amounts to introducing a new parameter set and as a consequence, some symmetric matrix S with an irreducible characteristic polynomial must be chosen. We have created a new version of the software that supports odd prime q for $q \in \{7, ..., 31\}$. We have a reference version and a constant-time optimized implementation. If q is an odd prime then a symmetric $[\mathbf{P}_i]$ is used. Performance numbers for the optimized version are presented in Table 7.

Table 7: Benchmark results on a laptop (Intel(R) Core(TM) Ultra 7 155H (Meteor Lake), compiler: gcc 15.1.1) for the optimized constant-time version. The performance is the median number of CPU cycles over 2048 benchmark runs. For comparison, we included the results on the same platform of the AVX2 optimized version as submitted to NIST Round 2 ("R2").

SL	(v, o, q, l)	XOF	KeyGen SSK	Sign SSK	Verify
I	(24, 5, 23, 4)	AES	305,808	608,058	218,082
	R2(24, 5, 16, 4)	AES	371,054	839,914	317,134
	(24, 5, 23, 4)	SHAKE	455,838	753,462	360,950
	R2(24, 5, 16, 4)	SHAKE	486,749	964,477	430,798
III	(37, 8, 19, 4)	AES	1,501,148	2,402,748	667,888
	R2(37, 8, 16, 4)	AES	1,627,368	2,882,394	1,091,840
	(37, 8, 19, 4)	SHAKE	2,052,261	2,946,949	1,197,672
	R2(37, 8, 16, 4)	SHAKE	2,176,692	3,380,944	1,529,565
V	(60, 10, 23, 4)	AES	5,286,896	6,670,477	2,045,487
	R2(60, 10, 16, 4)	AES	7,136,373	10,135,882	3,249,581
	(60, 10, 23, 4)	SHAKE	6,832,575	8,079,354	3,473,244
	R2(60, 10, 16, 4)	SHAKE	8,517,743	11,923,319	4,579,079

While these results are promising, the analysis of the wedge attack as applied to SNOVA is in full swing. At this moment it is unclear whether the odd prime q combined with a symmetric public matrix actually reduces the impact of the wedge attack. We may still need to increase the number of vinegar variables. This will be elaborated on in future work.

5 Conclusion

In [1], it was shown that the original Round 1 version of SNOVA may contain a small fraction of weak keys vulnerable to forgery attacks. The efficiency of these attacks is closely related to the rank drop of the matrix $\mathbf{E_R}$. To investigate this, we provide an explicit expression for $\mathbf{E_R}$. Based on this expression, our analysis and experiments indicate that the rank drop distribution of $\mathbf{E_R}$ in Round 2 SNOVA is indistinguishable from that of a random matrix. As a result, the rank drop is limited, rendering the attacks ineffective. In addition, we have completed an implementation of SNOVA over fields of odd prime order and provided the corresponding security and performance results. The impact of this parameter change on size and CPU cycles is expected to be minor.

Acknowledgment

The authors would like to thank Prof. Peigen Li for his valuable suggestions and insightful discussions regarding the security of SNOVA. The authors would like to thank Prof. Javier A. Verbel for sharing his code and for the related discussions. The first author is partially supported by 113-2115-M-259-003. The first and eighth authors are partially supported by the Hon Hai Research Institute. The fourth author is partially supported by 113-2115-M-259 -001.

References

[1] Beullens, W.: **Improved Cryptanalysis of SNOVA.** Cryptology ePrint Archive, Report 2024/1297, 2024. https://eprint.iacr.org/2024/1297.pdf.

[2] Cabarcas, D., Li, P., Verbel, J., Villanueva-Polanco, R.: **Improved Attacks for SNOVA by Exploiting Stability under a Group Action**. Cryptology ePrint Archive, Paper 2024/1770, 2024, https://eprint.iacr.org/2024/1770

[3] Ikematsu, Y., Akiyama, R.: **Revisiting the security analysis of SNOVA.** Cryptology ePrint Archive. Available at https://eprint.iacr.org/2024/096.pdf

[4] Li, P.: private comunication.

[5] Li, P., Ding, J.: **Cryptanalysis of the SNOVA signature scheme.** Cryptology ePrint Archive. Available at https://eprint.iacr.org/2024/110.pdf

[6] Nakamura, S., Tani, Y., Furue, H.: **Lifting approach against the SNOVA scheme.** Cryptology ePrint Archive, Paper 2024/1374, 2024. Available at https://eprint.iacr.org/2024/1374.

[7] NIST: **Post-quantum cryptography CSRC.** Available at https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[8] NIST: **Post-Quantum Cryptography: Digital Signature Schemes.** Available at https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals.

[9] Ran, L.: **Wedges, oil, and vinegar – An analysis of UOV in characteristic 2.** Cryptology ePrint Archive, Paper 2025/1143, 2025. Available at https://eprint.iacr.org/2025/1143.

[10] Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: **SNOVA.** Technical report, National Institute of Standards and Technology, 2023. Available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures.

[11] Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Leegwater, J.A., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: **SNOVA.** Technical report, National Institute of Standards and Technology, 2025. Available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf.

[12] Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Leegwater, J.A., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: **A Note on the SNOVA Security**. 2024. Available at https://eprint.iacr.org/2024/1517.

A Relation between the A,B,Q matrices and the E matrices

The public map $\widetilde{P}(\mathbf{U})$ of Round 2 SNOVA is defined by, for $i \in \{1, \dots, m\}$, the i-th entry is

$$\widetilde{P}_i(\mathbf{U}) = \sum_{\alpha=0}^{l^2+l-1} \sum_{j=1}^{n} \sum_{k=1}^{n} A_{i,\alpha} \cdot U_j^t (Q_{i,\alpha,1} P_{i',j,k} Q_{i,\alpha,2}) U_k \cdot B_{i,\alpha}$$

where $i' \coloneqq i'(i,\alpha) = (i+\alpha) \bmod o$. Denote the components of the $nl \times l$ matrix $\mathbf{U} = (U_1, \dots, U_n)^t$ as $u_{k,j}$ where $k \in \{0, \dots, nl-1\}$ and $j \in \{0, \dots, l-1\}$. Adding explicit matrix indices, we can express $\widetilde{P}_{i,i_1,j_1}(\mathbf{U})$ as

$$\sum_{\alpha, i_*, j_*, k_*} A_{i,\alpha,i_1,i_2} u_{i_2,k_1} \mathbf{Q}^{\otimes n}_{i,\alpha,1,k_1,k_2} P_{i',k_2,k_3} \mathbf{Q}^{\otimes n}_{i,\alpha,2,k_3,k_4} u_{k_4,j_2} B_{i,\alpha,j_2,j_1}$$

Here, and in the following, we use $i_1, i_2, j_1, j_2 \in \{0, \dots, l-1\}$ and $k_1, \dots, k_4 \in \{0, \dots, nl-1\}$. As the $Q_{i,\alpha,1}, Q_{i,\alpha,2}$ matrices are in $\mathbb{F}_q[S]$, we can express $Q_{i,\alpha,1}$ as a polynomial

$$Q_{i,\alpha,1} = \sum_{a=0}^{l-1} q_{1,a,(i,\alpha)} \left(S^a\right)$$

and similarly $Q_{i,\alpha,2}$. Then, the $(i_2, a), (j_2, b)$-th entry of $l^2 \times l^2$ matrix in the Theorem 2 corresponding to the term $A_{i,\alpha} \cdot \mathbf{U}^t \cdot \mathbf{Q}^{\otimes n}_{i,\alpha,1} \cdot [\mathbf{P}_{i'}] \cdot \mathbf{Q}^{\otimes n}_{i,\alpha,2} \cdot \mathbf{U} \cdot B_{i,\alpha}$ in $\widetilde{P}_i(\mathbf{U})$ with respect to the bilinear form $B_{i'}^{(a,b)}(\mathbf{u}_j, \mathbf{u}_k)$, for $a, b \in \{0, \dots, l-1\}$, is defined by

$$q_{1,a,(i,\alpha)} q_{2,b,(i,\alpha)} A_{i,\alpha,i_2,i_1} B_{i,\alpha,j_1,j_2}.$$

Toy example. We take a specific case with $q = 5, m = 2, l = 2$ as a toy example. We provide the ABQ matrix for each equation and the corresponding $\mathbf{E}_{00}, \mathbf{E}_{01}, \mathbf{E}_{10}, \mathbf{E}_{11}$ matrices.

For $i = 1$, let

$$A_{1,0} = \begin{bmatrix} 2 & 4 \\ 2 & 2 \end{bmatrix}, \quad A_{1,1} = \begin{bmatrix} 2 & 4 \\ 3 & 3 \end{bmatrix}, \quad A_{1,2} = \begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix},$$

$$A_{1,3} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad A_{1,4} = \begin{bmatrix} 0 & 2 \\ 3 & 4 \end{bmatrix}, \quad A_{1,5} = \begin{bmatrix} 3 & 0 \\ 4 & 1 \end{bmatrix},$$

$$B_{1,0} = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}, \quad B_{1,1} = \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}, \quad B_{1,2} = \begin{bmatrix} 0 & 3 \\ 4 & 0 \end{bmatrix},$$

$$B_{1,3} = \begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix}, \quad B_{1,4} = \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \quad B_{1,5} = \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix},$$

and let the coefficients of $Q_{1,\alpha,1}, Q_{1,\alpha,2}$ matrices are

$$q_{1,0,(1,0)} = 1,\ q_{1,1,(1,0)} = 0,\ q_{1,0,(1,1)} = 4,\ q_{1,1,(1,1)} = 4,$$

$$q_{1,0,(1,2)} = 2,\ q_{1,1,(1,2)} = 4,\ q_{1,0,(1,3)} = 4,\ q_{1,1,(1,3)} = 2,$$

$$q_{1,0,(1,4)} = 0,\ q_{1,1,(1,4)} = 0,\ q_{1,0,(1,5)} = 3,\ q_{1,1,(1,5)} = 0,$$

$$q_{2,0,(1,0)} = 4,\ q_{2,1,(1,0)} = 4,\ q_{2,0,(1,1)} = 2,\ q_{2,1,(1,1)} = 0,$$

$$q_{2,0,(1,2)} = 1,\ q_{2,1,(1,2)} = 4,\ q_{2,0,(1,3)} = 0,\ q_{2,1,(1,3)} = 1,$$

$$q_{2,0,(1,4)} = 3,\ q_{2,1,(1,4)} = 1,\ q_{2,0,(1,5)} = 1,\ q_{2,1,(1,5)} = 4.$$

For $i = 2$, let

$$A_{2,0} = \begin{bmatrix} 3 & 0 \\ 2 & 3 \end{bmatrix}, \quad A_{2,1} = \begin{bmatrix} 2 & 4 \\ 4 & 1 \end{bmatrix}, \quad A_{2,2} = \begin{bmatrix} 3 & 0 \\ 3 & 2 \end{bmatrix},$$

$$A_{2,3} = \begin{bmatrix} 3 & 2 \\ 3 & 4 \end{bmatrix}, \quad A_{2,4} = \begin{bmatrix} 1 & 3 \\ 0 & 4 \end{bmatrix}, \quad A_{2,5} = \begin{bmatrix} 0 & 4 \\ 2 & 2 \end{bmatrix},$$

$$B_{2,0} = \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}, \quad B_{2,1} = \begin{bmatrix} 1 & 3 \\ 4 & 4 \end{bmatrix}, \quad B_{2,2} = \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix},$$

$$B_{2,3} = \begin{bmatrix} 0 & 3 \\ 3 & 0 \end{bmatrix}, \quad B_{2,4} = \begin{bmatrix} 4 & 3 \\ 4 & 0 \end{bmatrix}, \quad B_{2,5} = \begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix},$$

and let the coefficients of $Q_{2,\alpha,1}, Q_{2,\alpha,2}$ matrices are

$$q_{1,0,(2,0)} = 1,\ q_{1,1,(2,0)} = 4,\ q_{1,0,(2,1)} = 1,\ q_{1,1,(2,1)} = 1,$$

$$q_{1,0,(2,2)} = 2,\ q_{1,1,(2,2)} = 4,\ q_{1,0,(2,3)} = 3,\ q_{1,1,(2,3)} = 0,$$

$$q_{1,0,(2,4)} = 3,\ q_{1,1,(2,4)} = 3,\ q_{1,0,(2,5)} = 1,\ q_{1,1,(2,5)} = 3,$$

$$q_{2,0,(2,0)} = 2,\ q_{2,1,(2,0)} = 1,\ q_{2,0,(2,1)} = 2,\ q_{2,1,(2,1)} = 4,$$

$$q_{2,0,(2,2)} = 4,\ q_{2,1,(2,2)} = 0,\ q_{2,0,(2,3)} = 1,\ q_{2,1,(2,3)} = 1,$$

$$q_{2,0,(2,4)} = 3,\ q_{2,1,(2,4)} = 0,\ q_{2,0,(2,5)} = 4,\ q_{2,1,(2,5)} = 2.$$

Then the $\mathbf{E}_{jk}$ matrices, as illustrated in Theorem 2 are:

$$\mathbf{E}_{0,0} = \begin{bmatrix} 0 & 0 & 0 & 0 & 3 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 4 & 4 & 0 & 0 & 0 & 3 & 1 & 1 \\ 1 & 2 & 4 & 1 & 1 & 3 & 4 & 0 \\ 4 & 3 & 4 & 3 & 3 & 1 & 4 & 4 \\ 1 & 0 & 2 & 3 & 3 & 4 & 2 & 1 \\ 4 & 1 & 2 & 4 & 2 & 1 & 1 & 4 \\ 3 & 1 & 0 & 1 & 1 & 4 & 3 & 1 \end{bmatrix}, \quad \mathbf{E}_{0,1} = \begin{bmatrix} 3 & 3 & 0 & 0 & 0 & 3 & 1 & 1 \\ 4 & 2 & 2 & 3 & 1 & 3 & 4 & 0 \\ 1 & 1 & 0 & 0 & 2 & 4 & 0 & 3 \\ 1 & 1 & 0 & 0 & 1 & 4 & 0 & 0 \\ 3 & 4 & 1 & 2 & 4 & 0 & 2 & 0 \\ 2 & 0 & 1 & 1 & 3 & 0 & 1 & 0 \\ 1 & 2 & 1 & 2 & 1 & 1 & 1 & 4 \\ 0 & 3 & 1 & 1 & 2 & 4 & 0 & 1 \end{bmatrix},$$

$$\mathbf{E}_{1,0} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 4 & 2 & 2 & 3 & 2 & 2 & 2 & 1 \\ 1 & 2 & 4 & 1 & 2 & 1 & 4 & 2 \\ 4 & 4 & 1 & 0 & 3 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 & 1 & 1 & 2 & 4 \\ 1 & 3 & 1 & 4 & 1 & 0 & 1 & 0 \\ 4 & 4 & 2 & 0 & 2 & 1 & 0 & 4 \end{bmatrix}, \quad \mathbf{E}_{1,1} = \begin{bmatrix} 4 & 3 & 1 & 4 & 2 & 2 & 2 & 1 \\ 4 & 2 & 2 & 3 & 2 & 1 & 4 & 2 \\ 2 & 2 & 0 & 0 & 0 & 1 & 0 & 3 \\ 1 & 1 & 0 & 0 & 4 & 3 & 0 & 1 \\ 1 & 0 & 0 & 3 & 3 & 0 & 3 & 0 \\ 2 & 1 & 2 & 3 & 1 & 0 & 3 & 0 \\ 3 & 2 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 3 & 3 & 1 & 0 & 4 \end{bmatrix}.$$