Reformulating the SNOVA Signature Scheme

Jintai Ding[1], Hao Guo[2], Yen-Liang Kuan[3], Jan Adriaan Leegwater[4], Peigen Li[5⋆], Po-En Tseng[3,6⋆⋆], and Lih-Chung Wang[3,6]

[1] Xian Jiaotong-Liverpool University
jintai.ding@gmail.com
[2] Tsinghua University
guoh22@mails.tsinghua.edu.cn
[3] National Dong Hwa University, Taiwan
ylkuan@gms.ndhu.edu.tw, briantseng0320@gmail.com, lcwang@gms.ndhu.edu.tw
[4] Vacuas, Leiden, The Netherlands
info@vacuas.nl
[5] Beijing Institute of Mathematical Sciences and Applications, China
lpg22@bimsa.cn
[6] Hon Hai Research Institute

Abstract. In this note, we review the formulation of SNOVA in three different languages: the ring-equation form, the whipping form, and the tensor form. Based on this, we propose a reformulation of SNOVA and discuss the security analysis of the resulting reformulated scheme. As a conclusion, we find that this new framework allows for greater flexibility in parameter selection and enables us to obtain parameter sets that remain competitive. In particular, as shown in the appendix, parameter sets over odd characteristic $\mathbb{F}_q$ lead to smaller key sizes and may offer improved resistance against certain attacks. This makes parameter sets over odd characteristic $\mathbb{F}_q$ especially interesting from a practical perspective. We propose a number of parameter sets that have certificate sizes below one kilobyte.

1 Introduction

The quantum computers poses a fundamental threat to many of the public-key cryptosystems currently securing digital communications. This has motivated the development of post-quantum cryptography (PQC), which aims to design public key cryptosystems whose security holds even against quantum adversaries. To guide global evaluation and deployment on PQC, the U.S. National Institute of Standards and Technology (NIST) launched an international standardization

⋆ corresponding author
⋆⋆ corresponding author

process, which has accelerated both theoretical analysis and practical optimization of candidate schemes. The effort has led to the selection of initial standards and the "onramp" competition for additional digital signatures. Against this backdrop, multivariate public-key cryptography stands out for its efficiency and compact signature sizes. Therefore, understanding the structural properties and security of multivariate schemes remains an important research direction.

In 2025, the NIST ongoing "onramp" process for additional digital signatures entered the second round. The round 2 multivariate candidates include: UOV, [4], QR-UOV [11], MAYO [3], and SNOVA [25]. SNOVA [25] is a UOV-variant signature scheme [4] defined over noncommutative rings. The UOV scheme suffers from a well-known drawback: its public keys are large, typically ranging from 40 KB to 60 KB when targeting NIST security level I. In contrast, SNOVA achieves a dramatic reduction in public key size, down to roughly 1 KB, while preserving strong performance characteristics and aligning with the compactness of current NIST-selected signature standards.

In the analysis process so far, numerous studies [17,15,2,19,23,24,6,21,12] focused on analyzing the security of SNOVA [25,26]. Subsequently, the wedge attack proposed by Lars Ran [20] offered the cryptographic community a new perspective on the security of the UOV family, inspiring researchers to revisit the UOV variants and leading to additional analysis on SNOVA [22,5]. On the other hand, in [18], the authors presented a tensor-based framework that provides a unified approach for understanding the core structures of all multivariate candidates in the current Round 2 process. We believe that these cryptanalytic studies are positive development on SNOVA. They show that the core design of SNOVA is being thoroughly examined.

This note focuses on three aspect:

- We summarize the three existing approaches for describing the SNOVA scheme: the ring-equation form, the whipping form, and the tensor form and explain the equivalence and connections of these three formulations.
- We present a reformulation of SNOVA and analyze the security of the resulting scheme. Note that, the formulation introduced in Section 4.1 can be viewed as a special case of a generalization of TSUOV with $l = 1$ in the Appendix A of [18]. The reformulated scheme combines the core of SNOVA with the respective advantages of existing members of the UOV family. At the same time, one can observe that the reformulated scheme can also be described within the original ring-equation framework. Our study indicates that this new framework provides greater flexibility in parameter selection and enables the construction of parameter sets that remain competitive.
- In the Appendix A, parameter sets over odd characteristic $\mathbb{F}_q$ lead to smaller key sizes and may offer improved resistance against certain attacks. This observation makes parameter choices over odd characteristic $\mathbb{F}_q$ especially ap-

pealing from a practical standpoint. Thus, we consider the security analysis over odd characteristic $\mathbb{F}_q$ to be an important direction for future research.

2 Preliminaries

2.1 Notation

- v, o, q, l denote the parameters defining SNOVA scheme and $n = v + o$.
- $[c]$ denotes the set $\{1, \ldots, c\}$.
- $\mathbb{F}_q$ denotes a finite field with q elements.
- $\mathbb{F}_q^c$ denotes the space of c-dimensional column vectors over $\mathbb{F}_q$.
- $\mathbb{F}_q^{r\times c}$ denotes the set of matrices of size $r \times c$ with entries in $\mathbb{F}_q$.
- $\mathcal{R} = \mathbb{F}_q^{l\times l}$ denotes the set of $l \times l$ matrices over $\mathbb{F}_q$.
- $S \in \mathcal{R}$ is symmetric matrix with an irreducible characteristic polynomial.
- $\mathbb{F}_q[S]$ denotes the set $\{a_0S^0 + a_1S + \cdots + a_{l-1}S^{l-1} : a_0, \ldots, a_{l-1} \in \mathbb{F}_q\}$.
- $\otimes$ denotes the Kronecker tensor product.
- $\tau : \mathbb{F}_{q^l} \to \mathbb{F}_{q^l}$ denotes the Frobenius map defined by $z \mapsto z^q$.
- $\mathbf{Q}^{\otimes n}$ denotes the block-diagonal matrix with n copies of Q along the diagonal.

2.2 Kronecker product

Definition 1. *If A is an $m \times n$ matrix and B is a $p \times q$ matrix, then the Kronecker product $A \otimes B$ is the $pm \times qn$ block matrix:*

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

From fundamental matrix textbooks such as [14], one can find proofs for the following proposition and lemmas.

Proposition 1. *Let A, B, C, D be given matrices, we have*

1. *The Kronecker product is a special case of the tensor product, so it is bilinear and associative:*

$$\begin{aligned} A \otimes (B + C) &= A \otimes B + A \otimes C, \\ (B + C) \otimes A &= B \otimes A + C \otimes A, \\ (kA) \otimes B &= A \otimes (kB) = k(A \otimes B), \\ (A \otimes B) \otimes C &= A \otimes (B \otimes C), \\ A \otimes 0 &= 0 \otimes A = 0, \end{aligned}$$

   where 0 *is a zero matrix, and* k *is a scalar.*
2. $(A \otimes B)^\top = A^\top \otimes B^\top$*;*
3. *If* C *and* D *are matrices of such size that one can form the matrix products* AC *and* BD*, then* $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$*.*

Lemma 1. *Consider for instance the equation* $AXB = C$*, where* A, X, B *and* C *are given matrices, we have*

$$(B^\top \otimes A) \cdot vec(X) = vec(C), \tag{2.1}$$

where $vec(X)$ *denotes the vectorization of the matrix* X*, i.e., the column vector obtained by stacking the columns of* X *on top of one another.*

3 Description of SNOVA

SNOVA, proposed by Wang *et al.* in [26,25], utilizes a noncommutative ring structure to achieve a significant reduction in public key size. Among the UOV families, SNOVA attains the most compact public key. In this section, we review the description of SNOVA scheme via three different language: ring equations, tensor and whipping structure.

3.1 SNOVA with ring equation

We first review the SNOVA scheme within the framework of ring equations. As described in [25], the authors first extend the UOV scheme to the matrix ring using ring equations, and then incorporate a "scrambling" operation, implemented via ABQ matrices within the matrix ring, to construct the SNOVA scheme. The public map of a SNOVA(v, o, q, l) scheme is defined as follows:

Public map. Let $\mathbf{P}_1, \ldots, \mathbf{P}_o \in \mathbb{F}_q^{ln \times ln}$ be the SNOVA public key. The public map of SNOVA is $\mathcal{P}^* = (\mathcal{P}_1^*, \ldots, \mathcal{P}_o^*) : \mathcal{R}^n \to \mathcal{R}^o$. For $i \in \{1, \ldots, o\}$, each

$\mathcal{P}_i^* : \mathcal{R}^n \to \mathcal{R}$ is defined by

$$\begin{aligned} &\mathcal{P}_i^*(\mathbf{U}) \\ &:= \sum_{\alpha=0}^{l^2+l-1} \sum_{j=1}^{n} \sum_{k=1}^{n} A_{i,\alpha} \cdot U_j^\top \cdot (Q_{i,\alpha,1} P_{i',jk} Q_{i,\alpha,2}) \cdot U_k \cdot B_{i,\alpha} \\ &= \sum_{\alpha=0}^{l^2+l-1} A_{i,\alpha} \cdot \mathbf{U}^\top \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot \mathbf{P}_{i'} \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} \cdot B_{i,\alpha}, \end{aligned} \tag{3.1}$$

where $i' = i + \alpha \pmod{o}$ and $P_{i',jk} \in \mathcal{R}$ is the (j,k)-th entry of $\mathbf{P}_{i'}$. Here, $\mathbf{U}$ is a matrix of variables of size $ln \times l$, and the matrices $Q_{i,\alpha,1}, Q_{i,\alpha,2} \in \mathbb{F}_q[S]$ and $A_{i,\alpha}, B_{i,\alpha} \in \mathcal{R}$. For more details, we refer to the NIST Round 2 specification of SNOVA [25].

Private key. The private key is given by an invertible matrix $\mathbf{T} \in (\mathbb{F}_q[S])^{n \times n}$ and matrices $\mathbf{F}_1, \ldots, \mathbf{F}_o \in \mathbb{F}_q^{ln \times ln}$ such that $\mathbf{P}_i = \mathbf{T}^\top \mathbf{F}_i \mathbf{T}$, for each $i \in \{1, \ldots, o\}$, and each $\mathbf{F}_i$ is of the form

$$\begin{bmatrix} F_i^{11} & F_i^{12} \\ F_i^{21} & 0 \end{bmatrix} \tag{3.2}$$

where $F_i^{11} \in \mathbb{F}_q^{lv \times lv}, F_i^{12} \in \mathbb{F}_q^{lv \times lo}$ and $F_i^{21} \in \mathbb{F}_q^{lo \times lv}$.

3.2 Description via whipping structure

In [2], Beullens observed that the SNOVA scheme can be represented using the whipping structure, and based on this insight, developed a forgery attack targeting the Round 1 public map. Subsequently, the whipping-form representation of the Round 2 SNOVA public map is detailed in [24].

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

$$\mathcal{B}_{i,a,b}(\mathbf{u}, \mathbf{v}) := B_i^{(a,b)}(\mathbf{u}, \mathbf{v}), \tag{3.3}$$

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

$$B_i^{(a,b)} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q, \; B_i^{(a,b)}(\mathbf{u}, \mathbf{v}) := \mathbf{u}^\top \cdot \mathbf{P}_{i,a,b} \cdot \mathbf{v} \tag{3.4}$$

where $\mathbf{P}_{i,a,b} = (\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n}$.

Then, the author of [2] showed that the public map of SNOVA can be represented in a whipping structure form (3.5): For $j, k \in \{0, \ldots, l-1\}$, there exist matrices $\mathbf{E}_{j,k} \in \mathbb{F}_q^{l^2 o \times l^2 o}$ such that the SNOVA public map $\mathcal{P}^* : \mathcal{R}^n \to \mathcal{R}^o$ can be expressed as

$$\mathcal{P}^*(\mathbf{U}) = \sum_{j=0}^{l-1} \sum_{k=0}^{l-1} \mathbf{E}_{j,k} \cdot \mathcal{B}(\mathbf{u}_j, \mathbf{u}_k). \tag{3.5}$$

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

As explained by Beullens [2], for the Round 1 SNOVA public map, the matrix $\mathbf{E}_{j,k}$ is a block-diagonal matrix with identical diagonal blocks, i.e., $\mathbf{E}_{j,k} = \tilde{\mathbf{E}}_{j,k}^{\otimes o}$ for some $l^2 \times l^2$ matrix $\tilde{\mathbf{E}}_{j,k}$. This structure enables the forgery attack demonstrated in [2]. In response, the SNOVA team made minor adjustments to the public map $\mathcal{P}(\mathbf{U})$ for the Round 2 submission to NIST [25]. Under the whipping structure, the only difference between Round 1 and Round 2 map is that the block-diagonal matrix with identical diagonal blocks structure is removed.

3.3 SNOVA with tensor language

In [18], the authors observed that the tensor language provides a unified framework for describing the Round 2 NIST PQC multivariate candidates: QR-UOV [11], MAYO [3] and SNOVA [25]. By employing the language of tensors, they introduce a clear and systematic approach to represent multivariate schemes. In the following, we review the description of SNOVA using the Kronecker product, as presented in [18].

We begin with the observation in [18]. Since $\mathbf{Q}_{i,\alpha,1}^{\otimes n}, \mathbf{Q}_{i,\alpha,2}^{\otimes n} \in \mathbb{F}_q[S]$, then, for $i \in \{1, \ldots, o\}$ and $\alpha \in \{0, \ldots, l^2 + l - 1\}$, by collecting the coefficients, one can have

$$\mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot \mathbf{P}_{i'} \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} = \sum_{0 \le a,b \le l-1} c_{i,\alpha}^{a,b} \cdot (\mathbf{S}^a)^{\otimes n} \mathbf{P}_{i'} (\mathbf{S}^b)^{\otimes n} \tag{3.6}$$

for some $c_{i,\alpha}^{a,b} \in \mathbb{F}_q$. Therefore, the core part of SNOVA public map can be written as

$$\mathbf{U}^\top \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot \mathbf{P}_{i'} \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} = \sum_{0 \le a,b \le l-1} c_{i,\alpha}^{a,b} \cdot \mathbf{U}^\top \cdot (\mathbf{S}^a)^{\otimes n} \mathbf{P}_{i'} (\mathbf{S}^b)^{\otimes n} \cdot \mathbf{U} \tag{3.7}$$

From this, one can observe that the true defining components of the SNOVA scheme are the matrices $\mathbf{P}_{i,a,b} := (\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n}$. Then, by Lemma 1, we then have

$$\begin{aligned}
&\mathrm{vec}(\mathcal{P}_i^*(\mathbf{U})) \\
&= \sum_{\alpha=0}^{l^2+l-1} B_{i,\alpha}^\top \otimes A_{i,\alpha} \cdot \mathrm{vec}(\mathbf{U}^\top \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot \mathbf{P}_{i'} \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U}) \\
&= \sum_{\alpha=0}^{l^2+l-1} \sum_{0 \le a,b \le l-1} c_{i,\alpha}^{a,b} \cdot (B_{i,\alpha}^\top \otimes A_{i,\alpha}) \cdot \mathrm{vec}(\mathbf{U}^\top \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U}) \\
&= \sum_{\alpha=0}^{l^2+l-1} \sum_{0 \le a,b \le l-1} D_{i,\alpha}^{a,b} \cdot \mathrm{vec}(\mathbf{U}^\top \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U}),
\end{aligned} \tag{3.8}$$

where $D_{i,\alpha}^{a,b} := c_{i,\alpha}^{a,b} \cdot (B_{i,\alpha}^{\top} \otimes A_{i,\alpha}) \in \mathbb{F}_q^{l^2 \times l^2}$. Thus, for the r-th entry of $\mathrm{vec}(\mathcal{P}_i^*(\mathbf{U}))$ we then will have

$$\mathrm{vec}(\mathcal{P}_i^*(\mathbf{U}))_r = \sum_{\alpha=0}^{l^2+l-1} \sum_{0 \le a,b \le l-1} \sum_{s=1}^{l^2} D_{i,\alpha}^{a,b}(r,s) \cdot \mathrm{vec}(\mathbf{U}^{\top} \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U})_s, \tag{3.9}$$

where $D_{i,\alpha}^{a,b}(r,s)$ the (r,s)-entry of $D_{i,\alpha}^{a,b}$. Note that the (e,f)-th entry of $\mathbf{U}^{\top} \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U}$ is the $e + (f-1)l$-th component of $\mathrm{vec}(\mathbf{U}^{\top} \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U})$, which can also be expressed as

$$(\mathbf{U}^{\top} \cdot \mathbf{P}_{i',a,b} \cdot \mathbf{U})(e,f) = \mathrm{vec}(\mathbf{U})^{\top} \cdot (I_{e,f} \otimes \mathbf{P}_{i',a,b}) \cdot \mathrm{vec}(\mathbf{U}), \tag{3.10}$$

where $I_{e,f}$ is the matrix with 1 in the (e,f)-th position and zeros elsewhere. Let $\mathcal{P}_{i,c,d}^*(\mathbf{U})$ be the (c,d)-th entry of $\mathcal{P}_i^*(\mathbf{U})$ and by writing it into quadratic form, one can have

$$\mathcal{P}_{i,c,d}^*(\mathbf{U}) = \mathrm{vec}(\mathbf{U})^{\top} \cdot \mathbf{P}_{i,c,d}^* \cdot \mathrm{vec}(\mathbf{U}), \quad \mathbf{P}_{i,c,d}^* \in \mathbb{F}_q^{l^2 n \times l^2 n} \tag{3.11}$$

where $c,d \in \{1,\ldots,l\}$. Where, $\mathbf{P}_{i,c,d}^*$ is the matrix corresponding to the multivariate quadratic polynomial in the (c,d)-th entry of $\mathcal{P}_i^*(\mathbf{U})$. Then we have

$$\mathbf{P}_{i,c,d}^* = \sum_{\alpha=0}^{l^2+l-1} \sum_{0 \le a,b \le l-1} \sum_{1 \le e,f \le l} D_{i,\alpha}^{a,b}(c+(d-1)l, e+(f-1)l) \cdot I_{e,f} \otimes \mathbf{P}_{i',a,b}. \tag{3.12}$$

Define

$$E_{i,\alpha}^{a,b,c,d} := \sum_{1 \le e,f \le l} D_{i,\alpha}^{a,b}(c+(d-1)l, e+(f-1)l) \cdot I_{e,f} \in \mathbb{F}_q^{l \times l}. \tag{3.13}$$

We have

$$\mathbf{P}_{i,c,d}^* \tag{3.14}$$

$$= \sum_{\alpha=0}^{l^2+l-1} \sum_{0 \le a,b \le l-1} E_{i,\alpha}^{a,b,c,d} \otimes \mathbf{P}_{i',a,b} \tag{3.15}$$

$$= \sum_{j=1}^{o} \sum_{0 \le a,b \le l-1} \Big(\sum_{\alpha \equiv j-i \mod o} E_{i,\alpha}^{a,b,c,d} \Big) \otimes \mathbf{P}_{j,a,b}, \tag{3.16}$$

where $i' = i + \alpha \pmod{o}$, $i \in \{1,\ldots,o\}$ and $c,d \in \{1,\ldots,l\}$.

Therefore, by relabeling the index, we can write the equation (3.14) into

$$\mathbf{P}_s^* = \sum_{j=1}^{o} \sum_{a,b} E^{s,j,a,b} \otimes \mathbf{P}_{j,a,b} \tag{3.17}$$

where $s \in \{1,\ldots,l^2 o\}$ and $E^{s,j,a,b} \in \mathbb{F}_q^{l \times l}$.

More precisely, we have

$$E_{i,\alpha}^{a,b,c,d} = c_{i,\alpha}^{a,b} \cdot B_{i,\alpha}(\cdot, d) \cdot A_{i,\alpha}(c, \cdot) \tag{3.18}$$

where $B_{i,\alpha}(\cdot, d)$ is the d-th coloum of $B_{i,\alpha}$ and $A_{i,\alpha}(c, \cdot)$ is the c-th row of $A_{i,\alpha}$. By equation (3.18), each $E_{i,\alpha}^{a,b,c,d}$ has rank lower than 1. Thus if the number of the term in the summation

$$\sum_{\alpha \equiv j-i \mod o} E_{i,\alpha}^{a,b,c,d} \tag{3.19}$$

is lower than l^2 when α run through the set $\{0, \cdots, l^2 + l - 1\}$, we have

$$\operatorname{rank}\Big(\sum_{\alpha \equiv j-i \mod o} E_{i,\alpha}^{a,b,c,d} \Big) < l^2. \tag{3.20}$$

Thus the new formulation equation (3.17) will give more equations when $E^{s,j,a,b}$ run through in $\mathbb{F}_q^{l \times l}$ than the original SNOVA. For fixed i, α, by considering the map $\Phi : \mathbb{F}_q^{l^6} \to \mathbb{F}_q^{l^6}$: defined by

$$\{A_{i,\alpha}, B_{i,\alpha}, Q_{i,\alpha 1}, Q_{i,\alpha 2}\} \mapsto \{E_{i,\alpha}^{a,b,c,d} : \ a, b \in \{0, \ldots, l-1\}, c, d \in \{1, \ldots, l\}\}. \tag{3.21}$$

In general, if Φ is bijective then the two descriptions are equivalent. Indeed, when any $A_{i,\alpha}$, $B_{i,\alpha}$, $Q_{i,\alpha 1}$ or $Q_{i,\alpha 2}$ is zero, Φ yields zero. Thus, Φ will never be surjective.

Relation between three descriptions. In the case of Round 2 SNOVA, the SNOVA team fixed the seed used to generate the ABQ matrices and, in [24], provided the explicit expressions for $\mathbf{E}_{j,k}$ induced by $\{A_{i,\alpha}, B_{i,\alpha}, Q_{i,\alpha 1}, Q_{i,\alpha 2}\}$. as pointed out in the [18], the tensor structure is essentially a reordering and recombination of coefficients from the whipping structure. Since the seed for generating the ABQ matrices is fixed, the three expression: ring-equation (3.1), whipping form (3.5), tensor form (3.17) are equivalent.

4 Reformulation of SNOVA

In this section, we aim to leverage the strengths of both the TSUOV framework [18] and the core structure of SNOVA [25], i.e., the matrices $\mathbf{P}_{i,a,b}$ to explore the potential of the SNOVA scheme. We believe that the following reformulated scheme provides greater flexibility on parameter selection, facilitates a deeper understanding of the core structure of SNOVA.

Round 1 SNOVA and Round 2 adjustment. In the first round of SNOVA submitted to NIST, $A_{i,\alpha}, B_{i,\alpha}, Q_{i,\alpha 1}, Q_{i,\alpha 2}$ depend only on α and $\mathbf{P}_{i'} = \mathbf{P}_i$ for

all i', the public map is defined as

$$\mathcal{P}_i^*(\mathbf{U}) = \sum_{\alpha=1}^{l^2} \sum_{j,k} A_\alpha \cdot U_j^\top \cdot (Q_{\alpha 1} P_{i,jk} Q_{\alpha 2}) \cdot U_k \cdot B_\alpha. \tag{4.1}$$

In such case,

$$\mathbf{P}_{i,c,d}^* = \sum_{a,b} E^{a,b,c,d} \otimes \mathbf{P}_{i,a,b}. \tag{4.2}$$

The adjustments introduced by the SNOVA team in Round 2 were primarily designed to counter the forgery attack proposed by Beullens [2]. Within the original ring-equation framework, the SNOVA team implemented minor modifications that disrupt the block-diagonal structure with identical diagonal blocks present in the Round 1 map, as described in [2]. Since the success of the attacks in [2,6] depends heavily on this rank structure, the Round 2 modifications render these attacks ineffective.

In the following, we employ both the tensor and whipping descriptions to present the most general formulation. This general description proves to be highly flexible and offers a better foundation for selecting well-balanced parameters.

4.1 General form

In the following, we use the whipping language to describe the general form of the SNOVA scheme. Let v, o denote the number of vinegar and oil variables, respectively. Let l denotes the size of matrix S. Let $n = v + o$.

Public key. Let m_1 denote the number of matrices in the public key, i.e., the public key is consisting of $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1} \in \mathbb{F}_q^{ln \times ln}$. Let $\mathbf{P}_{i,a,b} := (\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n}$ for $i \in \{1, \ldots, m_1\}$.

When $\mathbb{F}_q$ is of characteristic 2, the matrices $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1}$ are constructed in the same manner as in SNOVA [25]. In the odd characteristic case, for UOV variants, it is natural to consider symmetric $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1}$. The only difference is that, when generating the matrices $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1}$ from the private key, symmetric matrices $\mathbf{F}_1, \ldots, \mathbf{F}_{m_1}$ are used in the process.

Bilinear map. Let $\mathcal{B} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q^{l^2 m_1}$ be the bilinear map defined by

$$\mathcal{B}_{i,a,b}(\mathbf{u}, \mathbf{v}) := B_i^{(a,b)}(\mathbf{u}, \mathbf{v}), \tag{4.3}$$

where, for $i \in \{1, \ldots, m_1\}$ and $(a, b) \in \{0, \ldots, l-1\}^2$,

$$B_i^{(a,b)} : \mathbb{F}_q^{ln} \times \mathbb{F}_q^{ln} \to \mathbb{F}_q, \ B_i^{(a,b)}(\mathbf{u}, \mathbf{v}) := \mathbf{u}^\top \cdot \mathbf{P}_{i,a,b} \cdot \mathbf{v}. \tag{4.4}$$

Public map. Let r, m_2 be two positive integers. The public map of the general form is defined by

$$\mathcal{P}^*(\mathbf{U}) = \sum_{j=0}^{r-1}\sum_{k=0}^{r-1} \mathbf{E}_{j,k} \cdot \mathcal{B}(\mathbf{u}_j, \mathbf{u}_k). \tag{4.5}$$

where $\mathbf{u}_j$ is the $(j+1)$-th column of $\mathbf{U}$ for $j \in \{0, \ldots, r-1\}$ and for all $j, k \in \{0, \ldots, l-1\}$, the matrices $\mathbf{E}_{j,k} \in \mathbb{F}_q^{m_2 \times l^2 m_1}$ are the matrices we used to scramble the entries of the bilinear map $\mathcal{B}$. When m_2 is chosen to be different from $l^2 m_1$, the matrices $\mathbf{E}_{j,k}$ become rectangular[7]. As the result, the number of equations in the public map can be independent with the parameters l and m_1. Note that r, m_2 are the number of columns of $\mathbf{U}$[8] and the number of equations in $\mathcal{P}^*(\mathbf{U})$, respectively. It would be required that $rlo \geq m_2$ to ensure that $\mathcal{P}^*(\mathbf{U})$ can efficiently find a preimage by exploiting the Oil-Vinegar structure.

Since the whipping form and tensor are equivalent, one can also write the form (4.5) into the tensor form. Note that $\mathcal{P}^*(\mathbf{U})$ can be regarded as a quadratic map of m_2 equations in rln variables. By relabeling the index, for $s \in \{1, \ldots, m_2\}$, the matrix corresponding to the s-th entry of $\mathcal{P}^*(\mathbf{U})$ is

$$\mathbf{P}_s^* = \sum_{j=1}^{m_1}\sum_{a,b} E^{s,j,a,b} \otimes \mathbf{P}_{j,a,b}, \tag{4.6}$$

where $s \in \{1, \ldots, m_2\}$, $E^{s,j,a,b} \in \mathbb{F}_q^{r \times r}$ and $rlo \geq m_2$. Note that the matrices $\mathbf{E}_{j,k}$ or $E^{s,j,a,b}$ can be generated from a seed. Note that $\mathbf{E}_{j,k}$ and $E^{s,j,a,b}$ are just the rearrangement of each other. Therefore, the above extension will not affect the public key size. (4.5)

Description via the ring equations. On the other hand, in some way[9], we can still use ring equations to describe the general mapping. In general, if we assume that $A_{i,\alpha} \in \mathbb{F}_q^{r_1 \times r}$ and $B_{i,\alpha} \in \mathbb{F}_q^{r \times r_2}$ for some integers r_1 and r_2, we have

$$\mathcal{P}_i^*(\mathbf{U}) = \sum_{\alpha=0}^{l^2+l-1} A_{i,\alpha} \cdot \mathbf{U}^\top \cdot \mathbf{Q}_{i,\alpha,1}^{\otimes n} \cdot \mathbf{P}_{i'} \cdot \mathbf{Q}_{i,\alpha,2}^{\otimes n} \cdot \mathbf{U} \cdot B_{i,\alpha} \in \mathbb{F}_q^{r_1 \times r_2} \tag{4.7}$$

and $\mathcal{P}^* = (\mathcal{P}_1^*, \cdots, \mathcal{P}_{m_1}^*) : \mathbb{F}_q^{rln} \to \mathbb{F}_q^{m_1 r_1 r_2}$. In this case, we require $rlo \geq m_1 r_1 r_2 = m_2$ to ensure that $\mathcal{P}^*$ can efficiently find a preimage by exploiting the Oil-Vinegar structure. It is worth noting that describing the scheme using ring equations can lead to a more efficient implementation.

[7] A similar idea can be found in the Appendix of [25] and [18].

[8] This aligns with Beullens observation in [2] that the whipping dimension r need not be chosen equal to l.

[9] Although the representations are equivalent, for an arbitrary $\mathbf{E}_{j,k}$ or $E^{s,j,a,b}$, it may not be possible to recover the specific $A_{i,\alpha}, B_{i,\alpha}, Q_{i,\alpha,1}, Q_{i,\alpha,2}$ in equation (4.7).

5 Security analysis

In this section, we analyze the security of the reformulated scheme against known attacks and present the corresponding complexity estimates. Since the design and its security properties exhibit subtle differences between the odd- and even-characteristic settings, we provide the analysis of all known attacks of the even characteristic case in this section. In Appendix A we propose parameter sets for odd q. A full analysis of these parameter sets with odd characteristic is left for future work.

5.1 Complexity estimation

We give a brief overview of the tools used to estimate the complexity of solving an MQ problem.

MQ solver and hybrid approach. The complexity of solving M homogeneous quadratic equations in N variables can be estimated by

$$3 \cdot \binom{N-1+d_{reg}}{d_{reg}}^2 \cdot \binom{N+1}{2} \tag{5.1}$$

field multiplications. The term d_{reg} is determined by the smallest positive integer d such that the coefficient of t^d term in the series generated by

$$\frac{(1-t^2)^M}{(1-t)^N} \tag{5.2}$$

is non-positive.

In the literature, several algebraic algorithms, such as F_4 [8], F_5 [9] and XL [7] have been proposed for solving MQ systems. The hybrid approach [1] randomly guesses k variables before solving the MQ system and the corresponding complexity is

$$\mathsf{MQ}(N, M, q) = \min_k q^k \cdot 3 \cdot \binom{N-k+d_{reg,k}}{d_{reg,k}}^2 \cdot \binom{N-k+2}{2} \tag{5.3}$$

field multiplications where $d_{reg,k}$ is the smallest positive integer d such that the coefficient of t^d term in the series generated by

$$\frac{(1-t^2)^M}{(1-t)^{N-k+1}} \tag{5.4}$$

is non-positive.

The number of gates required for an attack against a digital signature scheme can be computed by

$$\sharp\text{gates} = \sharp\text{field multiplication} \cdot (2 \cdot (\log_2 q)^2 + \log_2 q)$$

with the assumption that one field multiplication in the field $\mathbb{F}_q$ needs about $(\log_2 q)^2$ bit multiplications and same for bit additions, and for each field multiplication in the computation, it will need an addition of field elements, each takes $\log_2 q$ bit additions. For the sake of the convience on the notation, we define $g(x) = (2 \cdot (\log_2 x)^2 + \log_2 x)$.

Methods for solving underdetermined MQ. For the underdetermined case, i.e., $N > M$, several methods have been proposed to solve underdetermined MQ systems more efficiently. Among these, the method of [13] is generally the most effective. Accordingly, for attacks that involve underdetermined MQ systems, we adopt Hashimoto's algorithm in our complexity estimates. The complexity estimation formula of Hashimoto's algorithm [13] is

$$\min_{k,\alpha}(M - \alpha - k + 1)\mathsf{MQ}(\alpha, \alpha, q) \tag{5.5}$$

$$+q^k \left(\mathsf{MQ}(\alpha - 1, \alpha - 1, q) + \mathsf{MQ}(M - \alpha - k, M - \alpha, q)\right) \tag{5.6}$$

provided that $N \geq \max\{(\alpha+1)(M-k-\alpha+1, \alpha(M-k) - (\alpha-1)^2 + k\}$ holds.

5.2 Lifting techniques

We first review the technique of lifting the SNOVA scheme to the extension field $\mathbb{F}_{q^l}$ introduced in [6,12].

Let $\tau : \mathbb{F}_{q^l} \to \mathbb{F}_{q^l}$ denote the Frobenius map defined by $z \mapsto z^q$. By abuse of notation, we also use τ to represent its entry-wise extension to vectors and matrices. Let $\lambda \in \mathbb{F}_{q^l}$ be an eigenvalue of S and $\xi \in \mathbb{F}_{q^l}^l$ be the eigenvector of S corresponding to eigenvalue λ. It can be checked that $\tau^i(\xi)$ is the eigenvector corresponding to $\tau^i(\lambda)$ and L is invertible due to the fact that the characteristic polynomial of S is irreducible. Let $L = [\xi \ \tau(\xi) \ \cdots \ \tau^{l-1}(\xi)] \in \mathbb{F}_{q^l}^{l \times l}$, then

$$L^{-1} \cdot S \cdot L = \begin{bmatrix} \lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{l-1}} \end{bmatrix} = \begin{bmatrix} \lambda & & & \\ & \tau(\lambda) & & \\ & & \ddots & \\ & & & \tau^{l-1}(\lambda) \end{bmatrix}. \tag{5.7}$$

Let $\mathbf{U}$ be the commutation matrix corresponding to index (n, l), i.e.,

$$\mathbf{U} = \begin{bmatrix} E_{11} & E_{21} & \cdots & E_{l1} \\ E_{12} & E_{22} & \cdots & E_{l2} \\ \vdots & \vdots & \ddots & \vdots \\ E_{1l} & E_{2l} & \cdots & E_{nl} \end{bmatrix} \tag{5.8}$$

where E_{ij} is the matrix of size $l \times n$ whose (i,j)-entry is one and other entries are zero. Given the public key $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1} \in \mathbb{F}_q^{ln \times ln}$, the Theorem 1 below demonstrates how to lift the scheme to the extension field $\mathbb{F}_q^l$.

Theorem 1 ([12, Theorem 1]). *Let* $\bar{\mathbf{T}} = \mathbf{U}^\top \cdot (\mathbf{L}^{\otimes n})^{-1} \cdot \mathbf{T} \cdot \mathbf{L}^{\otimes n} \cdot \mathbf{U}$. *For* $k \in \{1, \ldots, m\}$, *let* $\bar{\mathbf{F}}_k = \mathbf{U}^\top \cdot (\mathbf{L}^{\otimes n})^\top \cdot \mathbf{F}_k \cdot \mathbf{L}^{\otimes n} \cdot \mathbf{U}$ *and* $\bar{\mathbf{P}}_k = \mathbf{U}^\top \cdot (\mathbf{L}^{\otimes n})^\top \cdot \mathbf{P}_k \cdot \mathbf{L}^{\otimes n} \cdot \mathbf{U}$. *For each* $i, j \in \{1, \ldots, l\}$, *we define* $\bar{F}_{k,(i,j)} \in \mathbb{F}_{q^l}^{n \times n}$ *and* $\bar{P}_{k,(i,j)} \in \mathbb{F}_{q^l}^{n \times n}$ *by the* (i,j)*-th submatrices of* $\bar{\mathbf{F}}_k$ *and* $\bar{\mathbf{P}}_k$, *respectively. Then, we have*

(i) For all k, i, j, *the lower right o-by-o submatrix of* $\bar{F}_{k,(i,j)}$ *is the zero matrix, i.e.,* $\bar{F}_{k,(i,j)}$ *is a UOV-type matrix, and we have*

$$\tau(\bar{F}_{k,(i,j)}) = \bar{F}_{k,((i+1) \bmod l,\,(j+1) \bmod l)}. \tag{5.9}$$

More precisely, we have

$$\bar{\mathbf{F}}_k = \begin{bmatrix} \bar{F}_{k,(1,1)} & \bar{F}_{k,(1,2)} & \cdots & \bar{F}_{k,(1,l)} \\ \tau(\bar{F}_{k,(1,l)}) & \tau(\bar{F}_{k,(1,1)}) & \cdots & \tau(\bar{F}_{k,(1,l-1)}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau^{l-1}(\bar{F}_{k,(1,2)}) & \tau^{l-1}(\bar{F}_{k,(1,3)}) & \cdots & \tau^{l-1}(\bar{F}_{k,(1,1)}) \end{bmatrix}, \tag{5.10}$$

(ii) For the matrix $\bar{\mathbf{T}} = \mathbf{U}^\top \cdot (\mathbf{L}^{\otimes n})^{-1} \cdot \mathbf{T} \cdot \mathbf{L}^{\otimes n} \cdot \mathbf{U}$, *we have*

$$\bar{\mathbf{T}} = \begin{bmatrix} \bar{T}_1 & & & \\ & \tau(\bar{T}_1) & & \\ & & \ddots & \\ & & & \tau^{l-1}(\bar{T}_1) \end{bmatrix}, \tag{5.11}$$

where $\bar{T}_1 \in \mathbb{F}_{q^l}^{n \times n}$ *is of the form*

$$\begin{bmatrix} I_{v \times v} & *_{v \times o} \\ 0 & I_{o \times o} \end{bmatrix}. \tag{5.12}$$

(iii) For all k, i, j, *we have*

$$\tau(\bar{P}_{k,(i,j)}) = \bar{P}_{k,((i+1) \bmod l,\,(j+1) \bmod l)}, \tag{5.13}$$

$$\bar{P}_{k,(i,j)} = (\tau^{i-1}(\bar{T}_1))^\top \cdot \bar{F}_{k,(i,j)} \cdot \tau^{j-1}(\bar{T}_1). \tag{5.14}$$

5.3 Direct attack

In the plain direct attack, the attacker attempts to forge a signature by solving the system

$$\mathcal{P}^*(\mathbf{U}) = \mathsf{Hash}(\mathsf{msg} \| \mathsf{salt}) = \mathbf{z} \in \mathbb{F}_q^{m_2}. \tag{5.15}$$

This yields a set of m_2 multivariate quadratic equations in rln variables. Since the system is underdetermined, our complexity estimate is based on the algorithm proposed by Hashimoto [13]. The complexity of the plain direct attack is given by

$$\mathrm{Comp}_{\mathsf{Dir}} = \mathsf{MQ}(rln, m_2, q) \cdot g(q) \tag{5.16}$$

gates which holds for both even and odd characteristic cases.

5.4 Forgery attacks

Forgery attack with MinRank. In [2], the author proposed a rank attack to find a fake signature. In the tensor language, take random $\mathbf{y} \in \mathbb{F}_q^{rln}$ and suppose $\mathbf{x}$ has the form $\mathbf{a} \otimes \mathbf{u}_0 + \mathbf{y}$ where $\mathbf{u}_0$ is the first column of matrix $\mathbf{U}$ and $\mathbf{a} \in \mathbb{F}_q^r$. Then

$$\begin{aligned} &\mathbf{x}^\top \cdot \mathbf{P}^*_{i,c,d} \cdot \mathbf{x} \\ =&\sum_{a,b} (\mathbf{a}^\top \otimes \mathbf{u}_0 + \mathbf{y})^\top \cdot E^{a,b,c,d} \otimes \mathbf{P}_{i,a,b} \cdot (\mathbf{a}^\top \otimes \mathbf{u}_0 + \mathbf{y}) \\ =&\sum_{a,b} (\mathbf{a}^\top \cdot E^{a,b,c,d} \cdot \mathbf{a}) \cdot \mathbf{u}_0^\top \cdot \mathbf{P}_{i,a,b} \cdot \mathbf{u}_0 + \text{linear part of } \mathbf{u}_0. \end{aligned} \tag{5.17}$$

The method of [2] is to find an $\mathbf{a} \in \mathbb{F}_q^r$ such that the matrix $(\mathbf{a}^\top \cdot E^{a,b,c,d} \cdot \mathbf{a})_{a,b,c,d} \in \mathbb{F}_q^{m_2 \times l^2 m_1}$ has lower rank, then the system $\mathbf{x}^\top \cdot \mathbf{P}^*_{i,c,d} \cdot \mathbf{x}$ will increase many linear equations. Furthermore, to find a lower-rank matrix, the author in [2] used $\mathbf{U} = (\mathbf{R}_0^{\otimes n}\mathbf{u}_0, \cdots, \mathbf{R}_{r-1}^{\otimes n}\mathbf{u}_0)$. This formulation assumes that the vector $\mathbf{x}$ has the form

$$\mathbf{x} = \mathbf{y} + \mathbf{a}_0 \otimes \mathbf{u}_0 + \cdots + \mathbf{a}_{l-1} \otimes (\mathbf{S}^{l-1})^{\otimes n}\mathbf{u}_0, \tag{5.18}$$

where $\mathbf{a}_0, \ldots, \mathbf{a}_{l-1} \in \mathbb{F}_q^r$. This involves a generalized MinRank problem with $l(r-1)$ variables. Under this formulation of $\mathbf{x}$, the quadratic part of the public map $\mathcal{P}^*(\mathbf{U})$ is

$$\mathbf{E}_{\mathbf{R}} \cdot \mathcal{B}(\mathbf{u}_0, \mathbf{u}_0), \tag{5.19}$$

where $\mathbf{E}_{\mathbf{R}} \in \mathbb{F}_q^{m_2 \times l^2 m_1}$. If the rank of $\mathbf{E}_{\mathbf{R}}$ is $R := \mathrm{rank}(\mathbf{E}_{\mathbf{R}})$, then for an attacker who wants to forge a fake signature, the remaining is to solving an MQ system of R equations in $ln - (m_2 - R)$ variables. Therefore, the complexity of solving this MQ is estimated by

$$\mathsf{MQ}(ln - (m_2 - R), R, q). \tag{5.20}$$

We approximate the distribution of $\mathrm{rank}(\mathbf{E}_{\mathbf{R}})$ by that of a uniformly random matrix in $\mathbb{F}_q^{m_2 \times l^2 m_1}$. Under this approximation, the probability that such a matrix has rank exactly R is roughly

$$q^{-(l^2 m_1 - R)(m_2 - R)}. \tag{5.21}$$

Thus, the expected number of $\mathbf{a}_0, \ldots, \mathbf{a}_{l-1}$ such that $\mathrm{rank}(\mathbf{E_R}) = R$ is approximately

$$q^{l(r-1)} \cdot q^{-(l^2m_1-R)(m_2-R)} = q^{l(r-1)-(l^2m_1-R)(m_2-R)}. \tag{5.22}$$

Therefore, we estimate the complexity by

$$\begin{aligned} &\mathrm{Comp}_{\mathsf{For}} \\ &= \min_R \max\{q^{(l^2m_1-R)(m_2-R)-l(r-1)}, \mathsf{MQ}(ln - m_2 + R, R, q)\} \cdot g(q) \end{aligned} \tag{5.23}$$

gates for both even and odd characteristic cases.

In practical implementations, one could fix a set of the matrices $\mathbf{E}_{jk}$ so as to guarantee the absence of weak public keys. In [24], the authors showed that, in the case of Round 2 SNOVA, even when the matrices $\mathbf{E}_{jk}$ are generated using ABQ matrices, from the perspective of rank drops they still follow the above distribution. Using the explicit expressions of Appendix C.4, we have found that this probability describes the numerical data well when the matrices $\mathbf{E}_{jk}$ are chosen appropriately. When a set of $\mathbf{E}_{jk}$ is fixed, one can attempt to determine the true MinRank of $\mathbf{E_R}$ (when $l = 2, 3$) by performing an exhaustive search on the MinRank of the matrix $\mathbf{E_R}$. However, when $l = 4$, an exhaustive search cannot cover all possible $\mathbf{E_R}$. In this case, the true MinRank cannot be determined. Therefore, to be conservative, our complexity estimation incorporates equation (5.22) in order to ensure the security.

Forgery attack with stable ideal. In [6], the authors proposed a forgery attack against Round 1 SNOVA that combining the block diagonal structure in the MinRank step discovered by Beullens in [2] and the technique of the stable ideal. In their forgery attack strategy, they construct a system of equations and aim to solve it using their multi-homogeneous XL-like algorithm in order to produce forgeries. However, this multi-homogeneous XL-like algorithm cannot be directly applied to solve the constructed system, since the system itself may not be multi-homogeneous.

To overcome this problem, their overall strategy is to first exploit the multi-homogeneous structure to perform the XL and to define a degree D_{md} via a generating function $H'(t_1, \ldots, t_l)$. More precisely, the authors define $D_{md} := \sum_{i=1}^{l} d_i$ where $d_1, \ldots, d_l$ are the degree such that $H'(t_1, \ldots, t_l)[\mathbf{t}^{(d_1,\ldots,d_l)}] < 0$. In the most cases of the experiment, they observe that the solving degree is less or equal than D_{md}. Therefore, the author conclude that the rows and columns of the largest matrix in the Gröbner basis computation are bounded by

$$\binom{l^2o - k + p + D_{md}}{D_{md}} \tag{5.24}$$

where k and p which are the parameters in their algorithm. Based on these experimental results, they therefore use D_{md} to estimate the complexity and

obtain the following complexity estimate

$$\binom{l^2o - k + p + D_{md}}{D_{md}}^{\omega} \tag{5.25}$$

where ω is the linear algebra constant.

Note that, the strategy in [6] is based on the diagonal block structure in the MinRank step of Round 1 SNOVA and the observation that the solving degree is less or equal than D_{md}. However, the block diagonal structure no longer exists in the case Round 2 SNOVA. Moreover, the modifications introduced in Round 2 SNOVA cause the rank found in the MinRank step to be significantly higher than the rank that could previously be obtained. As also noted in their paper, we believe that these changes make their attack strategy unlikely to succeed against Round 2 SNOVA. For the same reason, we also expect that their attack would not be effective against the reformulated scheme presented in this note.

5.5 Collision attack

To forge a fake signature, an attacker can also try to check M intended signatures $\mathbf{U}_1, \ldots, \mathbf{U}_M$ and N hash values $\mathsf{Hash}(\mathsf{msg}||\mathsf{salt}_1), \ldots, \mathsf{Hash}(\mathsf{msg}||\mathsf{salt}_N)$, whether there exists a collision $\mathcal{P}^*(\mathbf{U}_j) = \mathsf{Hash}(\mathsf{msg}||\mathsf{salt}_k)$. And if it does, then the attacker has a valid fake signature. Thus, M signature computations and N hash value computations are involved. In our estimation, we include the computational cost of calculating the public map which is $m_1 \cdot n^2 \cdot l^3 \cdot r$. Thus, we estimate the costs required for this attack by

$$\mathrm{Comp}_{\mathsf{Col}} = 2 \cdot \left(q^{m_2} \cdot m_1 \cdot n^2 \cdot l^3 \cdot r \cdot g(q) \cdot 2^{17}\right)^{\frac{1}{2}} \tag{5.26}$$

gates.

5.6 KS attack

Plain KS attack. For both even and odd characteristic cases, the oil space corresponding to the public keys $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1} \in \mathbb{F}_q^{ln \times ln}$ is of dimension lo. Therefore, a lower bound to the complexity can be estimated as

$$\mathrm{Comp}_{\mathsf{PlainKS}} = q^{lv - lo} \cdot g(q) \tag{5.27}$$

gates for both even and odd characteristic cases.

Lifting KS attack. Note that the public key after lifting, $\bar{\mathbf{P}}_1, \ldots, \bar{\mathbf{P}}_{m_1}$, has a oil space of dimension lo. Thus, a lower bound to the complexity can be estimated as

$$\mathrm{Comp}_{\mathsf{LiftingKS}} = q^{lv - lo} \cdot g(q^l) \tag{5.28}$$

gates for both even and odd characteristic cases.

By comparing the equation (5.27) and the equation (5.28), we use the minimal value to estimate the complexity of KS attack. i,e,

$$\mathrm{Comp}_{\mathsf{KS}} = \min(\mathrm{Comp}_{\mathsf{PlainKS}}, \mathrm{Comp}_{\mathsf{LiftingKS}}) = \mathrm{Comp}_{\mathsf{PlainKS}} \tag{5.29}$$

gates for both even and odd characteristic cases.

5.7 Reconciliation attack

Plain reconciliation attack. A reconciliation attack on SNOVA over the ground field $\mathbb{F}_q$ is carried out by considering the system

$$\mathbf{x}^\top \cdot \mathbf{P}_{i,a,b} \cdot \mathbf{x} = \mathbf{x}^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^b \cdot \mathbf{x} = 0. \tag{5.30}$$

Even characteristic. Since $\mathbf{P}_i$ is not symmetric, the system (5.30) yields a MQ system consisting of $l^2 m_1$ equations in $ln - (lo - 1) = lv + 1$ variables. Hence the complexity of reconciliation attack is estimated by

$$\mathrm{Comp}_{\mathsf{PlainRec}} = \min_k q^k \cdot \mathsf{MQ}(lv + 1 - k, l^2 m_1, q) \cdot g(q) \tag{5.31}$$

gates where $\max\{0, lv + 1 - l^2 \cdot m_1\} \leq k \leq lv$.

Lifting reconciliation attack. Following the strategy in [12], the lifting reconciliation attack is trying to solve the following system

$$\mathbf{x}_i{}^\top \cdot \bar{P}_{k,(i,j)} \cdot \mathbf{x}_j = 0, \quad k \in [m_1],\ i, j \in [l] \tag{5.32}$$

where $\mathbf{x}_i \in \tau^{i-1}(\bar{T_1}^{-1}\bar{\mathcal{O}})$ and $\mathbf{x}_j \in \tau^{j-1}(\bar{T_1}^{-1}\bar{\mathcal{O}})$.

Even characteristic. The system (5.32) has $N = lv$ variables in total. For each $i = j \in [l]$, there are m_1 independent homogeneous quadratic equations. For each $1 \leq i < j \leq l$, there are $2m_1$ homogeneous bilinear equations (or equivalently, for each $1 \leq i, j \leq l, i \neq j$, there are m_1 homogeneous bilinear equations). Hence, $M = l(m_1) + \binom{l}{2} 2m_1 = l^2 m_1$ equations in total.

When $lv \geq l^2 m_1$, one can first assign $N - M = lv - l^2 m_1$ random values in the base field $\mathbb{F}_q$ (as mentioned in [6]) and then try to solve the system over the extension field $\mathbb{F}_{q^l}$ and seek for a solution that corresponds to a solution in the based field $\mathbb{F}_q$. After randomly assigning variables, the resulting system has $l^2 m_1$ variables and $l^2 m_1$ equations in total.

It is worth noting that, since we are attempting to solve these $\mathbf{x}_i \in \tau^{i-1}(\bar{T_1}^{-1}\bar{\mathcal{O}})$, when we attempt to solve the multi-homogeneous subsystem over the extension

field $\mathbb{F}_{q^l}$ and randomly assign an additional entry of $\mathbf{x}_1$ over $\mathbb{F}_{q^l}$ to facilitate the solving process, the Frobenius structure then directly determines the corresponding entries of $\mathbf{x}_2, \ldots, \mathbf{x}_l$.

Consequently, the attack can be summarized in the following steps:

- Consider the system (5.32) constructed by lifting reconciliation attack.
- Randomly assign $N - M = lv - l^2 m_1$ values in the based field $\mathbb{F}_q$ to the system (5.32). Then, this results in a system of $l^2 m_1$ variables and equations in total. The resulting system has l sets of variables and each set has lm_1 variables.
- Randomly guess $0 \leq k \leq lm_1$ entries in the extension field $\mathbb{F}_{q^l}$. This will contribute a factor $(q^l)^k$ in the complexity estimation.
- Solve the system over extension field and try to find a solution lies in the based field. If this succeeds, the procedure terminates. Otherwise, the attacker returns to the first step. This will contribute a factor $q^{N-M} = q^{lv-l^2m_1}$ in the complexity estimation.

Therefore, the complexity is given as

$$\begin{aligned} &\mathrm{Comp}_{\mathsf{LiftingRec}} \\ &= \min_{k \in [lm_1]} q^{lv-l^2m_1} \cdot (q^l)^k \cdot 3 \cdot (lm_1 - k)^2 \cdot \prod_{i=1}^{l} \binom{lm_1 - k + d_i}{d_i}^2 \cdot g(q^l) \end{aligned} \tag{5.33}$$

gates.

The solving degree $\mathbf{d}$ is the multi-degree so that the coefficient of $\prod_{i=1}^{l} t_i^{d_i}$ in the following series

$$\frac{\prod\limits_{1 \leq i < j \leq l} (1 - t_i t_j)^{2m_1} \cdot \prod\limits_{i \in [l]} (1 - t_i^2)^{m_1}}{\prod\limits_{i \in [l]} (1 - t_i)^{lm_1 - k + 1}}. \tag{5.34}$$

is non-positive.

We can only consider multi-degree $\mathbf{d}$ with $d_1 \geq d_2 \geq \cdots \geq d_l$ due to the symmetry in the generating function. Thus, we use the minimal value to estimate the complexity of reconciliation attack. i,e,

$$\mathrm{Comp}_{\mathsf{Rec}} = \min(\mathrm{Comp}_{\mathsf{PlainRec}}, \mathrm{Comp}_{\mathsf{LiftingRec}}) \tag{5.35}$$

gates.

Remark 1. In [6], the Cabarcas *et al.* proposed a variant of reconciliation attack utilizing multi-homogeneous structure. The attack presented in this subsection

equivalent to the reconciliation attack in [6]. On the other hand, note that the reconciliation attack proposed by Nakamura *et al.* [19] is corresponding to the case of $l' = 1$. In general, the lifting attacks proposed by Nakamura *et al.* [19] is not expected to be more effective than the lifting attacks proposed by Furue *et al.* [12], since it does not exploit the multi-homogeneous structure.

5.8 Intersection attack

Plain intersection attack. The intersection attack aims to find a vector

$$\mathbf{y} \in \mathbf{L}_1\big(\mathbf{T}^{-1}\mathcal{O}\big) \cap \mathbf{L}_2\big(\mathbf{T}^{-1}\mathcal{O}\big), \tag{5.36}$$

where $\mathbf{L}_1, \mathbf{L}_2 \in \mathbb{F}_q^{ln \times ln}$ are two invertible linear combinations of the matrices $\mathbf{P}_1, \ldots, \mathbf{P}_{m_1}$ and $\mathcal{O}$ denotes the oil space of the underlying UOV scheme. On the other hand, besides treating $\mathbf{L}_1$ and $\mathbf{L}_2$ as linear combinations of the matrices $\mathbf{P}_i$, we can further regard them as linear combinations of the matrices $\mathbf{P}_{i,a,b}$. This affects the system of equations relevant to the intersection attack and results in a different number of equations. In our security analysis of the intersection attack, we take both cases into account.

Even characteristic. In this case, the attack is trying to solve the following system

$$\begin{cases} \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_2^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_2^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) = 0 \end{cases} \tag{5.37}$$

If $\mathbf{L}_1$ and $\mathbf{L}_2$ are taken as linear combinations of the matrices $\mathbf{P}_i$, then the system of equations (5.37) contains $2l$ redundant equations. Consequently, this results in a system with $4l^2m_1 - 2l$ equations in ln variables.

On the other hand, if $\mathbf{L}_1$ and $\mathbf{L}_2$ are regarded as linear combinations of the matrices $\mathbf{P}_{i,a,b}$, then the system (5.37) contains only 2 redundant equations. A detailed explanation is provided in Appendix B. In our complexity estimation, we consider both scenarios. Note that throughout our analysis we assume $v \geq 2o$. Let

$$\mathrm{Comp}_{\mathsf{PlainInta}} = \min_{k_1} q^{lv-2lo+1} \cdot q^{k_1} \cdot \mathsf{MQ}(ln - k_1 + 1, 4l^2m_1 - 2l, q) \tag{5.38}$$

$$\mathrm{Comp}_{\mathsf{PlainIntb}} = \min_{k_2} q^{lv-2lo+1} \cdot q^{k_2} \cdot \mathsf{MQ}(ln - k_2 + 1, 4l^2m_1 - 2, q) \tag{5.39}$$

where

$$\max\{0, ln - (4l^2m_1 - 2l)\} \leq k_1 \leq ln - 1 \tag{5.40}$$

$$\max\{0, ln - (4l^2m_1 - 2)\} \leq k_2 \leq ln - 1. \tag{5.41}$$

Then, we estimate the complexity of intersection attack as

$$\mathrm{Comp}_{\mathsf{PlainInt}} = \min(\mathrm{Comp}_{\mathsf{PlainInta}}, \mathrm{Comp}_{\mathsf{PlainIntb}}) \cdot g(q) \tag{5.42}$$

gates.

Lifting Intersection attack. Following the strategy in [12], the lifting intersection attack is trying to solve the following system

$$\begin{cases} \left(W_1^{(q^{i-1})^{-1}} \cdot \mathbf{x}_i\right)^\top \cdot \bar{P}_{k,(i,j)} \cdot \left(W_1^{(q^{j-1})^{-1}} \cdot \mathbf{x}_j\right) = 0, \\ \left(W_1^{(q^{i-1})^{-1}} \cdot \mathbf{x}_i\right)^\top \cdot \bar{P}_{k,(i,j)} \cdot \left(W_2^{(q^{j-1})^{-1}} \cdot \mathbf{x}_j\right) = 0, \\ \left(W_2^{(q^{i-1})^{-1}} \cdot \mathbf{x}_i\right)^\top \cdot \bar{P}_{k,(i,j)} \cdot \left(W_1^{(q^{j-1})^{-1}} \cdot \mathbf{x}_j\right) = 0, \\ \left(W_2^{(q^{i-1})^{-1}} \cdot \mathbf{x}_i\right)^\top \cdot \bar{P}_{k,(i,j)} \cdot \left(W_2^{(q^{j-1})^{-1}} \cdot \mathbf{x}_j\right) = 0, \end{cases} , k \in [m_1],\ i,j \in [l']. \tag{5.43}$$

where $1 \leq l' \leq l$.

Even characteristic. For each $i = j \in [l']$, there are $4m_1 - 2$ independent homogeneous quadratic equations. For each $1 \leq i < j \leq l'$, there are $4 \cdot 2m_1 = 8m_1$ homogeneous bilinear equations (or equivalently, for each $1 \leq i, j \leq l', i \neq j$, there are $4 \cdot m_1$ homogeneous bilinear equations). Hence, $l'(4m_1 - 2) + \binom{l'}{2} 8m_1 = 4m_1 l'^2 - 2l'$ equations in total. The complexity is given as

$$\mathrm{Comp}_{\mathsf{LiftingInt}} = \min_{1 \leq l' \leq l} (q^l)^{v-2o+1} \cdot 3 \cdot \binom{n+1}{2} \cdot \prod_{i=1}^{l'} \binom{n+d_i-1}{d_i}^2 \cdot g(q^l) \tag{5.44}$$

where $d_1, \ldots, d_{l'}$ denote the solving degree for the l' sets of variables $\mathbf{x}_1, \ldots, \mathbf{x}_{l'}$. The solving degree is chosen such that the coefficient of $\prod_{i=1}^{l'} t_i^{d_i}$ in the following series

$$\frac{\prod\limits_{1 \leq i < j \leq l'} (1 - t_i t_j)^{8m_1} \cdot \prod\limits_{i \in [l']} (1 - t_i^2)^{4m_1 - 2}}{\prod\limits_{i \in [l']} (1 - t_i)^n}. \tag{5.45}$$

We can only consider multi-degree $\mathbf{d}$ with $d_1 \geq d_2 \geq \cdots \geq d_{l'}$ due to the symmetry in the generating function and l' so that $nl' \leq 4m_1 l'^2 - 2l'$.

Thus, we use the minimal value to estimate the complexity of intersection attack. i.e.,

$$\mathrm{Comp}_{\mathsf{Int}} = \min(\mathrm{Comp}_{\mathsf{PlainInt}}, \mathrm{Comp}_{\mathsf{LiftingInt}}) \tag{5.46}$$

gates.

5.9 Rectangular MinRank attack

In [12], Furue *et al.* proposed a rectangular MinRank attack against SNOVA. If $v < 2m_1 l'$, for some $l' \in [l]$, then an attacker can perform the rectangular

MinRank attack on SNOVA over the extension field by solving the following problems for variables $\mathbf{x}_1, \ldots, \mathbf{x}_{l'} \in \mathbb{F}_{q^\ell}^n$:

$$\text{(i)} \quad \operatorname{rank}\left(L_{l'}(\mathbf{x}_1, \ldots, \mathbf{x}_{l'})\right) \leq v, \tag{5.47}$$

$$\text{(ii)} \quad \mathbf{x}_i^\top \cdot \bar{P}_{k,(i,j)} \cdot \mathbf{x}_j = 0, \quad (k \in [m_1],\, i, j \in [l']), \tag{5.48}$$

where $L_{l'}(\mathbf{x}_1, \ldots, \mathbf{x}_{l'}) \in \mathbb{F}_{q^l}^{n \times 2l' m_1}$ is a matrix constructed by $\bar{P}_1, \cdots, \bar{P}_{m_1}$ via matrix deformation technique, for more details, we refer to [12].

The complexity of the attack is given by

$$\text{Comp}_{\mathsf{RecMinRank}} = \min_{\substack{1 \leq l' \leq l \\ v < n' \leq n}} 3 \cdot (v+1)^2 \cdot \binom{n'}{v}^2 \cdot \prod_{i=1}^{l'} \binom{v + d_i}{d_i}^2 \cdot g(q^l) \tag{5.49}$$

gates where $\mathbf{d} = (d_1, \ldots, d_{l'})$ denote the solving degree for the l' set of variables $\mathbf{x}_1, \ldots, \mathbf{x}_{l'}$ and $v < n' \leq n$. The multi-degree $\mathbf{d} = (d_1, \ldots, d_{l'})$ is chosen by the condition that the coefficient of $\prod_{i=1}^{l'} t_i^{d_i}$ in $G(\mathbf{t})$ is non-positive. Where,

$$G(\mathbf{t}) = G'(\mathbf{t}) \cdot \prod_{1 \leq i < j \leq l'} (1 - t_i t_j)^{2m_1} \cdot \prod_{i \in [l']} (1 - t_i^2)^{m_1} \tag{5.50}$$

and the each coefficient of $\prod_{i=1}^{l'} t_i^{d_i}$ in $G'(t)$ is given as

$$\binom{n'}{v} \cdot \prod_{i \in [\ell']} \binom{v + d_i}{d_i} \tag{5.51}$$

$$- \sum_{\mathbf{b} \in A_{\mathbf{d}}} \left((-1)^{|\mathbf{b}|+1} \cdot \prod_{i \in [\ell']} \binom{2m_1 + b_i - 1}{b_i} \cdot \binom{n'}{v + |\mathbf{b}|} \cdot \prod_{i \in [\ell']} \binom{v + d_i - b_i}{d_i - b_i} \right), \tag{5.52}$$

and the set $A_{\mathbf{d}}$ is defined by

$$A_{\mathbf{d}} = \left\{ \mathbf{b} = (b_1, \ldots, b_{l'}) \in \mathbb{Z}_{\geq 0}^{l'} \;\middle|\; 0 \leq b_i \leq d_i \;\; (i \in [l']),\;\; |\mathbf{b}| \geq 1 \right\}, \tag{5.53}$$

under the condition of $0 \leq |\mathbf{d}| \leq v + 1$.

Note that, in [12], the authors state that the complexity estimated by the above can be regarded as the lower bound for the correct complexity. Therefore, from the scheme designing perspective, the complexity in this subsection are conservative, the actual complexity of the attack is expected to be higher.

5.10 Wedge attack

The wedge attack proposed by Lars Ran [20] offered the cryptographic community a new perspective on the security of the UOV family, inspiring researchers to revisit the UOV variants and leading to additional analysis on SNOVA [22,5]

Recently, similar results were independently obtained by Bros *et al* [5] and Tseng *et al.* [22]. in their recent works. These two works indicate how to correctly understand the behavior of the wedge map in the wedge attack on SNOVA, in particular how to properly estimate the dimension of its kernel or its rank. Utilizing the framework of [22], the dimension of the kernel of the wedge map can be estimated by the generating function:

$$H_{m_1,n'}(\mathbf{t}) = \frac{\prod_{i=1}^{l}(1+t_i)^{n'}}{\prod_{i=1}^{l}(1+t_i^2)^{m_1}\prod_{1\le i<j\le l}(1+t_it_j)^{2m_1}}. \tag{5.54}$$

where $n' = v + o'$ and $1 < o' \le o$. Then, the complexity[10] of the wedge attack is given by

$$\mathrm{Comp}_{\mathsf{Wedge}} = 3\cdot(v+1)^2\cdot\prod_{i=1}^{l}\binom{v+o'}{o'}\cdot g(q^l) \tag{5.55}$$

where $o' = \min\left\{\, o' \middle| 1 < o' \le o,\ H_{m_1,n'}[\mathbf{t}^{\mathbf{o}'}] \le 1 \,\right\}$.

On the other hand, in [5], the authors proposed the unbalanced project-down technique. However, at this stage, it remains unclear to us how to correctly construct the corresponding wedge map with the framework of unbalanced project down. Therefore, we only include the analysis based on balanced project down. It is worth noting that, even with the unbalanced project down technique, the wedge attack is still not applicable to the parameter sets listed in Table 1.

5.11 Key recovery attack using p^l-truncated polynomial rings

In [10], Furue *et al.*, introduce a new framework for analyzing key recovery attacks on the UOV over finite fields $\mathbb{F}_{p^e}$. The authors show that the XL algorithm can recover the secret subspace by exploiting the structure of a p^l-truncated polynomial ring. This formulation simplifies previous symmetric-algebra-based descriptions by Jin *et al.* [16] and generalizes them to p^l-truncated polynomial rings, which can relax constraints on the solving degree by increasing l. The framework also enables the analysis of reconciliation and intersection attacks, including an intersection attack not previously considered in this context. Their complexity estimates show that the reconciliation attack matches the complexity of the symmetric-algebra attack by Jin *et al.*, while the intersection attack performs better and reduces the security of several UOV parameter sets.

[10] The wedge attack can be considered either over the base field or over an extension field. The complexity of these two versions of the attack differs by only a few bits. We believe the difference between them is very minor.

This new framework appears to provide a further avenue for analyzing the security of the UOV variants. We leave the question of how this framework can be applied to SNOVA as a direction for future research.

6 Parameters

In this section, we propose the parameter sets of the scheme. We can observe that the reformulated scheme provides greater flexibility in parameter selection. Even in the case where $r = l$ and $m_1 = o$, we can still resist existing attacks by increasing the size of the vinegar variables. The most immediate benefit of the framework proposed in this paper is that, when facing attacks, it allows us to better adapt and defend against them. At the same time, such flexibility enables a more thorough exploration of a wider range of parameters sets.

In [24,25], the authors announced a parameter set having a very small public key size, using an odd prime for the field order. Table 1 shows that there are more SNOVA parameter sets at SL I that have certificate sizes below 1 KB, not just parameter sets using an odd prime q. We also present a parameter set at SL III having a certificate size below 2 KB. There are multiple options to obtain SNOVA signatures that have sizes that are comparable to those of RSA 4096. We would like to emphasize that all proposed parameter sets are secure against all known attacks. The lowest complexity among all known attacks is marked in bold font.

Table 1. Demonstrative parameter sets. The sizes are reported in bytes.

SL	$(v, o, q, l, r, m_1, m_2)$	**|pk|**	**|sig|**	**|pk| + |sig|**
I	$(43, 6, 16, 2, 6, 16, 72)$	1168	310	1478
	$(44, 5, 16, 2, 8, 16, 80)$	816	408	1224
	$(36, 5, 16, 3, 5, 9, 75)$	1029	324	1353
	$(24, 3, 16, 4, 7, 6, 84)$	448	394	842
	$(28, 4, 16, 4, 5, 5, 80)$	656	336	992
III	$(52, 8, 16, 2, 7, 24, 112)$	3088	436	3524
	$(48, 8, 16, 3, 4, 11, 96)$	3184	352	3536
	$(38, 5, 16, 4, 5, 7, 100)$	1416	446	1862
	$(44, 6, 16, 4, 5, 8, 120)$	2320	516	2836
V	$(86, 11, 16, 2, 6, 32, 132)$	8002	598	8600
	$(64, 9, 16, 3, 5, 15, 135)$	5484	564	6048
	$(52, 6, 16, 4, 6, 9, 144)$	2608	712	3320
	$(52, 7, 16, 4, 5, 9, 140)$	3544	606	4150
	$(56, 8, 16, 4, 5, 10, 160)$	5136	656	5792

Table 2. Security estimates of the proposed parameter sets.

SL	$(v, o, q, l, r, m_1, m_2)$	Dir	For	Col
I	$(43, 6, 16, 2, 6, 16, 72)$	**156**	158	166
	$(44, 5, 16, 2, 8, 16, 80)$	166	**162**	182
	$(36, 5, 16, 3, 5, 9, 75)$	**163**	180	172
	$(24, 3, 16, 4, 7, 6, 84)$	**180**	201	190
	$(28, 4, 16, 4, 5, 5, 80)$	**175**	186	182
III	$(52, 8, 16, 2, 7, 24, 112)$	246	**230**	247
	$(48, 8, 16, 3, 4, 11, 96)$	**214**	223	**214**
	$(38, 5, 16, 4, 5, 7, 100)$	**218**	236	223
	$(44, 6, 16, 4, 5, 8, 120)$	**262**	274	263
V	$(86, 11, 16, 2, 6, 32, 132)$	**286**	289	287
	$(64, 9, 16, 3, 5, 15, 135)$	**293**	299	**293**
	$(52, 6, 16, 4, 6, 9, 144)$	**309**	318	311
	$(52, 7, 16, 4, 5, 9, 140)$	304	314	**303**
	$(56, 8, 16, 4, 5, 10, 160)$	348	350	**343**

Table 3. Security estimates of the proposed parameter sets.

SL	$(v, o, q, l, r, m_1, m_2)$	KS	Rec	Int
I	$(43, 6, 16, 2, 6, 16, 72)$	301	250	360
	$(44, 5, 16, 2, 8, 16, 80)$	317	258	384
	$(36, 5, 16, 3, 5, 9, 75)$	377	301	443
	$(24, 3, 16, 4, 7, 6, 84)$	341	221	391
	$(28, 4, 16, 4, 5, 5, 80)$	389	316	459
III	$(52, 8, 16, 2, 7, 24, 112)$	357	263	402
	$(48, 8, 16, 3, 4, 11, 96)$	485	412	560
	$(38, 5, 16, 4, 5, 7, 100)$	533	414	615
	$(44, 6, 16, 4, 5, 8, 120)$	613	479	702
V	$(86, 11, 16, 2, 6, 32, 132)$	605	474	697
	$(64, 9, 16, 3, 5, 15, 135)$	665	536	763
	$(52, 6, 16, 4, 6, 9, 144)$	741	578	858
	$(52, 7, 16, 4, 5, 9, 140)$	725	578	832
	$(56, 8, 16, 4, 5, 10, 160)$	773	611	875

Table 4. Security estimates of the proposed parameter sets.

SL	$(v, o, q, l, r, m_1, m_2)$	RecMinRank	Wedge
I	$(43, 6, 16, 2, 6, 16, 72)$	263	N/A
	$(44, 5, 16, 2, 8, 16, 80)$	285	N/A
	$(36, 5, 16, 3, 5, 9, 75)$	N/A	N/A
	$(24, 3, 16, 4, 7, 6, 84)$	202	N/A
	$(28, 4, 16, 4, 5, 5, 80)$	N/A	N/A
III	$(52, 8, 16, 2, 7, 24, 112)$	238	N/A
	$(48, 8, 16, 3, 4, 11, 96)$	N/A	N/A
	$(38, 5, 16, 4, 5, 7, 100)$	N/A	N/A
	$(44, 6, 16, 4, 5, 8, 120)$	N/A	N/A
V	$(86, 11, 16, 2, 6, 32, 132)$	486	N/A
	$(64, 9, 16, 3, 5, 15, 135)$	N/A	N/A
	$(52, 6, 16, 4, 6, 9, 144)$	N/A	N/A
	$(52, 7, 16, 4, 5, 9, 140)$	N/A	N/A
	$(56, 8, 16, 4, 5, 10, 160)$	N/A	N/A

Acknowledgment

The third author is partially supported by NSTC 114-2115-M-259-002-MY2. The sixth and seventh authors are partially supported by the Hon Hai Research Institute. The seventh author is partially supported by NSTC 114-2115-M-259-003-MY2

References

1. Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009.
2. Ward Beullens. Improved cryptanalysis of SNOVA. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 277–293. Springer, 2025.
3. Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. Mayo. *NIST Computer Security Resource Center (CSRC)*, 2025.
4. Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang. Uov: Unbalanced oil and vinegar. *NIST Computer Security Resource Center (CSRC)*, 2025.
5. Maxime Bros, Thai Hung Le, Jacob Lichtinger, Brice Minaud, Ray Perlner, Daniel Smith-Tone, and Cristian Valenzuela. Exploiting SNOVAs structure in the wedge product attack. *Cryptology ePrint Archive, Paper 2026/237*, 2026.

6. Daniel Cabarcas, Peigen Li, Javier Verbel, and Ricardo Villanueva-Polanco. Improved attacks for snova by exploiting stability under a group action. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 358–389, Cham, 2025. Springer Nature Switzerland.
7. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.
8. Jean-Charles Faugere. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.
9. Jean-Charles Faugere. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.
10. Hiroki Furue and Yasuhiko Ikematsu. Key recovery attacks on UOV using p^l-truncated polynomial rings. Cryptology ePrint Archive, Paper 2026/298, 2026.
11. Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi, Haruhisa Kosuge, Kimihiro Yamakoshi, Rika Akiyama, Satoshi Nakamura, Shingo Orihara, and Koha Kinjo. Qr-uov. *NIST Computer Security Resource Center (CSRC)*, 2025.
12. Hiroki Furue, Yasuhiko Ikematsu, Shuhei Nakamura, and Rika Akiyama. Improved cryptanalysis of snova by solving multi-homogeneous systems via matrix transformations. In Goichiro Hanaoka and Bo-Yin Yang, editors, *Advances in Cryptology – ASIACRYPT 2025*, pages 405–435, Singapore, 2026. Springer Nature Singapore.
13. Yasufumi Hashimoto. Minor improvements of algorithm to solve under-defined systems of multivariate quadratic equations. *IACR Cryptol. ePrint Arch.*, 2021:1045, 2021.
14. Roger A Horn and Charles R Johnson. *Topics in matrix analysis*. Cambridge university press, 1994.
15. Yasuhiko Ikematsu and Rika Akiyama. Revisiting the security analysis of SNOVA. In *Proceedings of the 11th ACM Asia Public-Key Cryptography Workshop*, pages 54–61, 2024.
16. Yi Jin, Yuansheng Pan, Xiaoou He, Boru Gong, and Jintai Ding. Security analysis on UOV families with odd characteristics: Using symmetric algebra. Cryptology ePrint Archive, Paper 2025/1137, 2025.
17. Peigen Li and Jintai Ding. Cryptanalysis of the SNOVA signature scheme. In *International Conference on Post-Quantum Cryptography*, pages 79–91. Springer, 2024.
18. Peigen Li, Hao Guo, and Jintai Ding. Unified approach to UOV-like multivariate signature schemes. Cryptology ePrint Archive, Paper 2025/1778, 2025.
19. Shuhei Nakamura, Yusuke Tani, and Hiroki Furue. Lifting approach against the snova scheme. In *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2025, Volume E108.A, Issue 10*, pages 1373–1381, 2025.
20. Lars Ran. Wedges, oil, and vinegar – an analysis of UOV in characteristic 2. Cryptology ePrint Archive, Paper 2025/1143, 2025.
21. Toshihiro Suzuki, Hiroki Furue, Takuma Ito, Shuhei Nakamura, and Shigenori Uchiyama. An extended rectangular minrank attack against UOV and its variants. *Cryptology ePrint Archive*, 2025.
22. Po-En Tseng, Lih-Chung Wang, Peigen Li, and Yen-Liang Kuan. Investigating the wedge map on SNOVA. *Cryptology ePrint Archive, Paper 2026/260*, 2026.

23. Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Jan Adriaan Leegwater, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang. A note on the snova security. *NIST Computer Security Resource Center (CSRC)*, 2025.
24. Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Jan Adriaan Leegwater, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang. On the security of round 2 snova. *NIST Computer Security Resource Center (CSRC)*, 2025.
25. Lih-Chung Wang, Chun-Yen Chou, Jintai Ding, Yen-Liang Kuan, Jan Adriaan Leegwater, Ming-Siou Li, Bo-Shu Tseng, Po-En Tseng, and Chia-Chun Wang. Snova. *NIST Computer Security Resource Center (CSRC)*, 2025.
26. Lih-Chung Wang, Po-En Tseng, Yen-Liang Kuan, and Chun-Yen Chou. A Simple Noncommutative UOV Scheme. *Taiwanese Journal of Mathematics*, pages 1–35, 2026.

A Reformulated scheme in odd characteristic

We provide several parameter sets to demonstrate the advantages and significant potential of this variant. The parameters in the Table 5 are obtained simply by changing q from 16 to 19 for some of the parameter sets in Table 1. When $\mathbb{F}_q$ has odd characteristic, we can choose the public key $\mathbf{P}_i$ to be symmetric. This further reduces the size of the public key. This is advantageous and likely to be well received in practice. Compared with the reported sizes in Table 1, we observe that schemes over odd characteristic finite fields also exhibit strong potential.

Table 5. Demonstrative parameter sets. The sizes are reported in bytes.

SL	$(v, o, q, l, r, m_1, m_2)$	**|pk|**	**|sig|**	**|pk| + |sig|**
I	$(43, 6, 19, 2, 6, 16, 72)$	486	426	912
	$(28, 4, 19, 4, 5, 5, 80)$	379	358	737
III	$(38, 5, 19, 4, 5, 7, 100)$	800	475	1275
	$(44, 6, 19, 4, 5, 8, 120)$	1296	550	1846
V	$(52, 6, 19, 4, 6, 9, 144)$	1456	759	2215
	$(52, 7, 19, 4, 5, 9, 140)$	1965	646	2611
	$(56, 8, 19, 4, 5, 10, 160)$	2832	699	3531

While increasing q will in general increase the security, it is possible that the combination of SNOVA structure and symmetric public matrix leads to new, specific attacks. Because of this possibility we used $q = 16$ only in the main text. A complete security analysis for $\mathbb{F}_q$ of odd characteristic is left for future work.

B Remark on Intersection attack

In case of intersection attack against SNOVA, the possible strategy is attack the (lv, lo, q)-UOV corresponding to SNOVA with matrices

$$\mathbf{P}_{i,a,b} := (\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n} \tag{B.1}$$

for $a, b = 0, \ldots, l-1$ and $i = 1, \ldots, m_1$. If the characteristic is odd, we are in the case that $\mathbf{P}_i$ is symmetric and $a \leq b$.

The attacker is trying to find a vector $\mathbf{y} \in \mathbf{L}_1\big(\mathbf{T}^{-1}\mathcal{O}\big) \cap \mathbf{L}_2\big(\mathbf{T}^{-1}\mathcal{O}\big)$ where $\mathbf{L}_1, \mathbf{L}_2$ are two invertible linear combinations of the matrices $\mathbf{P}_i$ or $\mathbf{P}_i + \mathbf{P}_i^\top$ of size $ln \times ln$ over $\mathbb{F}_q$.

B.1 Even characteristic

Then, in this setting, since $\mathbf{L}_1^{-1}\mathbf{y}$, $\mathbf{L}_2^{-1}\mathbf{y} \in \mathbf{T}^{-1}(\mathcal{O})$, we have

$$\begin{cases} \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_2^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) = 0 \\ \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i^\top (\mathbf{S}^{\otimes n})^b \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) = 0 \end{cases} \tag{B.2}$$

Note that the last equation in equation (B.2) is equivalent with

$$\big(\mathbf{L}_2^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^b \mathbf{P}_i (\mathbf{S}^{\otimes n})^a \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big) = 0 \tag{B.3}$$

If $\mathbf{L}_1, \mathbf{L}_2$ are the linear combination of $\mathbf{P}_i$, suppose that

$$\begin{aligned} \mathbf{L}_1 &= \sum_{i=1}^{m_1} \alpha_i \mathbf{P}_i \\ \mathbf{L}_2 &= \sum_{i=1}^{m_1} \beta_i \mathbf{P}_i \end{aligned} \tag{B.4}$$

We have

$$\begin{aligned} &\sum_{i=1}^{m_1} \beta_i \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) \\ =& \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_2 \cdot \big(\mathbf{L}_2^{-1}\mathbf{y}\big) \\ =& \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_1 \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big) \\ =& \sum_{i=1}^{m_1} \alpha_i \big(\mathbf{L}_1^{-1}\mathbf{y}\big)^\top (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot \big(\mathbf{L}_1^{-1}\mathbf{y}\big). \end{aligned} \tag{B.5}$$

and

$$\begin{aligned}
&\sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_1 \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_2 \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\sum_{i=1}^{m_1} \beta_i \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right).
\end{aligned} \tag{B.6}$$

Hence there are also $2l$ redundant equations in equation (B.2).

If $\mathbf{L}_1, \mathbf{L}_2$ are the linear combination of $\mathbf{P}_i + \mathbf{P}_i^\top$, suppose that

$$\begin{aligned}
\mathbf{L}_1 &= \sum_{i=1}^{m_1} \alpha_i (\mathbf{P}_i + \mathbf{P}_i^\top) \\
\mathbf{L}_2 &= \sum_{i=1}^{m_1} \beta_i (\mathbf{P}_i + \mathbf{P}_i^\top)
\end{aligned} \tag{B.7}$$

Then we have

$$\begin{aligned}
&\sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{P}_i + \mathbf{P}_i^\top)(\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_1 \cdot (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_2 \cdot (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\sum_{i=1}^{m_1} \beta_i \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{P}_i + \mathbf{P}_i^\top)(\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right)
\end{aligned} \tag{B.8}$$

and

$$\begin{aligned}
&\sum_{i=1}^{m_1} \beta_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a (\mathbf{P}_i + \mathbf{P}_i^\top) \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_2 \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
=&\left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_1 \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\
=&\sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top (\mathbf{S}^{\otimes n})^a \cdot (\mathbf{P}_i + \mathbf{P}_i^\top) \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right).
\end{aligned} \tag{B.9}$$

Hence there are $2l$ redundant equations in equation (B.2).

If $\mathbf{L}_1, \mathbf{L}_2$ are the linear combination of $(\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b$ or $(\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b + (\mathbf{S}^{\otimes n})^b \mathbf{P}_i^\top (\mathbf{S}^{\otimes n})^a$, there are only 2 redundant equations in equation (B.2). In-

deed, suppose that

$$\begin{aligned}\mathbf{L}_1 &= \sum_{i,a,b} \alpha_i^{ab} (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \\ \mathbf{L}_2 &= \sum_{i,a,b} \beta_i^{ab} (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b\end{aligned} \tag{B.10}$$

We have

$$\begin{aligned}&\sum_{i,a,b} \beta_i^{ab} \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\ =& \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_2 \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\ =& \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_1 \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\ =& \sum_{i,a,b} \alpha_i^{ab} \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right)\end{aligned} \tag{B.11}$$

and

$$\begin{aligned}&\sum_{i,a,b} \alpha_i^{ab} \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\ =& \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_1 \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\ =& \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_2 \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\ =& \sum_{i,a,b} \beta_i^{ab} \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right)\end{aligned} \tag{B.12}$$

Hence there are only 2 redundant equations. It's same for the linear combinations of $(\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b + (\mathbf{S}^{\otimes n})^b \mathbf{P}_i^\top (\mathbf{S}^{\otimes n})^a$.

B.2 Odd characteristic.

Then, in this setting, since $\mathbf{L}_1^{-1}\mathbf{y}$, $\mathbf{L}_2^{-1}\mathbf{y} \in \mathbf{T}^{-1}(\mathcal{O})$, we have

$$\begin{cases} \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) = 0 \\ \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) = 0 \end{cases} \tag{B.13}$$

where $0 \le a \le b \le l-1$ and

$$\left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) = 0 \tag{B.14}$$

where $0 \le a, b \le l-1$.

If $\mathbf{L}_1, \mathbf{L}_2$ are the linear combination of $\mathbf{P}_i$, suppose that

$$\begin{aligned}\mathbf{L}_1 &= \sum_{i=1}^{m_1} \alpha_i \mathbf{P}_i \\ \mathbf{L}_2 &= \sum_{i=1}^{m_1} \beta \mathbf{P}_i\end{aligned} \tag{B.15}$$

We have

$$\begin{aligned}
&\sum_{i=1}^{m_1} \beta_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \mathbf{P}_i \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
&= \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_2 \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
&= \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot (\mathbf{S}^{\otimes n})^a \cdot \mathbf{L}_1 \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\
&= \sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top (\mathbf{S}^{\otimes n})^a \cdot \mathbf{P}_i \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right) \\
&= \sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^a \cdot \left(\mathbf{L}_1^{-1}\mathbf{y}\right)
\end{aligned} \tag{B.16}$$

and

$$\begin{aligned}
&\sum_{i=1}^{m_1} \alpha_i \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^a \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
&= \left(\mathbf{L}_1^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_1 \cdot (\mathbf{S}^{\otimes n})^a \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
&= \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot \mathbf{L}_2 \cdot (\mathbf{S}^{\otimes n})^a \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right) \\
&= \sum_{i=1}^{m_1} \beta_i \left(\mathbf{L}_2^{-1}\mathbf{y}\right)^\top \cdot \mathbf{P}_i \cdot (\mathbf{S}^{\otimes n})^a \cdot \left(\mathbf{L}_2^{-1}\mathbf{y}\right).
\end{aligned} \tag{B.17}$$

Hence there are also $2l$ redundant equations in equation (B.13) and equation (B.14). For the same reason, if $\mathbf{L}_1, \mathbf{L}_2$ are the linear combination of $(\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b$ or $(\mathbf{S}^{\otimes n})^a \mathbf{P}_i (\mathbf{S}^{\otimes n})^b + (\mathbf{S}^{\otimes n})^b \mathbf{P}_i^\top (\mathbf{S}^{\otimes n})^a$, there are only 2 redundant equations equation (B.13) and equation (B.14).

C Explicit expressions for the MinRank Attack

In [2], Beullens proposed a rank attack to find a forged signature as described in Section 5.4. This attack considers signature of the form

$$\mathbf{x} = \mathbf{y} + \mathbf{a}_0 \otimes \mathbf{u}_0 + \cdots + \mathbf{a}_{l-1} \otimes (\mathbf{S}^{l-1})^{\otimes n} \mathbf{u}_0. \tag{C.1}$$

The attack works by first finding some "good" coefficients $\mathbf{a}_i$, so that a forged $\mathbf{u}_0$ can be found more efficiently, before actually solving for $\mathbf{u}_0$. In this appendix we give explicit an expression that such an optimal $\mathbf{a}_i$ needs to satisfy.

As show in Section 3.3 we can write

$$\mathrm{vec}(\mathcal{P}_i^*(\mathbf{U})) = \sum_{i',a,b} D_{i,i',\alpha}^{a,b} \cdot \mathrm{vec}(\mathbf{U}^t \cdot (\mathbf{S}^a)^{\otimes n} \mathbf{P}_{i'} (\mathbf{S}^b)^{\otimes n} \cdot \mathbf{U}), \tag{C.2}$$

where

$$D_{i,i'}^{a,b} := \sum_{\alpha} c_{i,i',\alpha}^{a,b} \cdot (B_{i,\alpha}^t \otimes A_{i,\alpha}).$$

Inserting (C.1) into (C.2) we will get a equation that quadratic in $\mathbf{u}_0$. Due to the Cayley-Hamilton theorem, S^{a+a_1} is a sum of powers of S with some matrix of coefficients $C_{a_2,a}$ that depend only on a_1 and the characteristic polynomial of S. As $C^{a+1} = C^a \cdot C$, S^{a+a_1} can be expressed in terms of powers of the companion matrix C to the characteristic polynomial of S as

$$S^{a+a_1} = \sum_{a_2=0}^{l-1} \left(C^{a_1}\right)_{a_2,a} S^{a_2}. \tag{C.3}$$

With equation (C.3), we can express $\mathcal{P}_i^*(\mathbf{U})$ as

$$\mathrm{vec}(\mathcal{P}_i^*(\mathbf{U})) = \sum_{i',a_2,b_2} \tilde{\mathbf{E}}_{i,i',a_2,b_2}(\mathbf{a}) \cdot X_{i',a_2,b_2}(\mathbf{u}_0),$$

where

$$X_{i',a_2,b_2}(\mathbf{u}_0) = \mathrm{vec}(\mathbf{u}_0^t \cdot (\mathbf{S}^{a_2})^{\otimes n} \mathbf{P}_i (\mathbf{S}^{b_2})^{\otimes n} \cdot \mathbf{u}_0),$$

and

$$\tilde{\mathbf{E}}_{i,i',a_2,b_2}(\mathbf{a}) = \sum_{\substack{a,b \\ a_1,b_1}} \mathbf{a}_{a_1} \mathbf{a}_{b_1} \left(C^{a_1}\right)_{a_2,a} \left(C^{b_1}\right)_{b_2,b} D_{i,i'}^{a,b}. \tag{C.4}$$

The matrix $\tilde{\mathbf{E}} \in \mathbb{F}_q^{m_2 \times l^2 m_1}$. Equation (C.4) can be evaluated for any $\mathbf{a}$. It depends on the $\mathbf{E}_{jk}$ matrix (or equivalently, the ABQ matrices) as well as characteristic polynomial of the S matrix of SNOVA. In a way, the $\mathbf{E}_{jk}$ matrix must be "compatible" with the S matrix for SNOVA to be safe against the attack of Beullens [2].

We have made our software available at https://github.com/PQCLAB-SNOVA/SNOVA_Analysis.