Notes on Beullens attack on SNOVA

Jan Adriaan Leegwater[*]

December 13, 2025

1 Introduction

SNOVA [3] is one of the candidates in the NIST competition [1] for additional digital signatures. It has been selected as a Round 2 candidate in NIST's ongoing "onramp" process for additional digital signatures. During Round 1, Beullens analyzed the security of SNOVA [2] and found an attack that basically broke SNOVA Round 1. In response, the SNOVA team introduced refined adjustments [3, 4] to its parameter choices and public map in response to these attacks.

In this note we detail the analysis that has led to the results presented in [4]. We will not repeat a detailed description of SNOVA and refer to [3] instead.

2 The E matrix

The SNOVA Round 2 public map is

$$P_i(\vec{\mathbf{U}}) = \sum_{\alpha=1}^{N_\alpha} \sum_{j=1}^{n} \sum_{k=1}^{n} A_{i,\alpha} \cdot U_j^t (Q_{i,\alpha 1} P_{i',jk} Q_{i,\alpha 2}) U_k \cdot B_{i,\alpha}$$

where $i'i' = (i + \alpha) \bmod o$.

In this note we consider a minor extension of SNOVA with rectangular signatures of size $nl \times r$, so $\mathbf{U} \in \mathbb{F}_q^{nl \times r}$. Moreover, we stretch the public map as in the appendix of the NIST Round 2 submission [3] such that $i' \in \{1, ..., m_1\}$. The number of equation in the public map is $m_2 = o \cdot l \cdot r$. This requires that the A and B matrices have dimensions of $r \times r$ and $r \times l$ respectively. The extended SNOVA has two more parameters, r and m_1. As shown below, it is advised to use $m_1 \geq \lceil o \cdot r/l \rceil$ with $m_1 = \lceil o \cdot r/l \rceil$ usually being a good choice.

[*] Email: info@vacuas.nl

Denote the components of the $nl \times r$ matrix $\vec{\mathbf{U}}$ as $U_{k,j}$. Adding explicit matrix indices, P can be written as

$$P_{i,i_1,j_1}(\vec{\mathbf{U}}) = \sum_{\substack{\alpha,i_2,j_2,k_1\\k_2,k_3,k_4}} A_{i,\alpha,i_1,i_2} U_{k_1,i_2} Q^{\otimes n}_{1(i,\alpha,k_1,k_2)} P_{i',k_2,k_3} Q^{\otimes n}_{2(i,\alpha,k_3,k_4)} U_{k_4,j_2} B_{i,\alpha,j_2,j_1}$$

As the Q matrices are in $\mathbb{F}_q[S]$, the $Q^{\otimes n}$ matrices can be expressed in terms of its coefficients $q_{1(i,\alpha,a)}$ as

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

and similarly $Q^{\otimes n}_{2i,\alpha}$ and $q_{2(i,\alpha,b)}$. In terms of these coefficients, P can be expressed as

$$P_{i,i_1,j_1}(\mathbf{U}) = \sum_{(i_2,a),(j_2,b)} E_{(i,i_1,j_1),(i'',i_2,a,j_2,b)} D_{(i'',i_2,a,j_2,b)}(\mathbf{U})$$

where

$$D_{(i'',i_2,a,j_2,b)}(\mathbf{U}) = \sum_{k_1,k_2,k_3,k_4} U_{k_1,i_2} \left(S^a\right)^{\otimes n}_{k_1,k_2} P_{i'',k_2,k_3} \left(S^b\right)^{\otimes n}_{k_3,k_4} U_{k_4,j_2} \tag{2.1}$$

and

$$E_{(i,i_1,j_1),(i'',i_2,a,j_2,b)} = \sum_{\alpha} q_{1(i,\alpha,a)} q_{2(i,\alpha,b)} A_{i,\alpha,i_1,i_2} B_{i,\alpha,j_2,j_1} \delta_{i'(i,\alpha),i''}$$

where the Kronecker $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ if $x \neq y$.

In an abstract tensor-like notation we can write this as

$$E = \sum_{\alpha} A^t_{\alpha} \otimes q_{\alpha,1} \otimes q_{\alpha,2} \otimes B_{\alpha},$$

but this can be imprecise as the index to which the tensor (Kronecker) product $\otimes$ applies is not made explicit.

The Round 2 E matrix is a $olr \times m_1 l^2$ matrix rather than a matrix of o identical blocks of $l^2 \times l^2$ matrices as it was in Round 1.

3 Beullens attack

The attack of Beullens [2] is looking for a solution of a specific form

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

where $\mathbf{R}_i \in \mathbb{F}_q[S]$. In general, this will not result in an efficient attack but Beullens has shown that the complexity of finding a solution can be reduced if R is well-chosen.

The R matrices can be expressed in terms of its coefficients as

$$R_i^{\otimes n} = \sum_{a_1=0}^{l-1} r_{i,a_1} \left(S^{a_1}\right)^{\otimes n}$$

Explicitly, for the $\mathbf{u}$ part only

$$U_{k_1,i} = \sum_{a_1,k_2} r_{i,a_1} \left(S^{a_1}\right)^{\otimes n}_{k_1,k_2} U_{k_2,0}$$

Using equation (2.1) and the expression for $R_i^{\otimes n}$ we get

$$D_{(i'',i_2,a,j_2,b)}(\mathbf{U}) = \sum U_{k_1,0} r_{i_2,a_1} \left(S^{a+a_1}\right)^{\otimes n}_{k_1,k_2} P_{i'',k_2,k_3} \left(S^{b+b_1}\right)^{\otimes n}_{k_3,k_4} r_{j_2,b_1} U_{k_4,0}$$

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

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

In terms of this C, D can be expressed as

$$\begin{aligned} &D_{(i'',i_2,a,j_2,b)}(\mathbf{U}) \\ &= \sum U_{k_1,0} r_{i_2,a_1} \left(C^{a_1}\right)_{a_2,a} \left(S^{a_2}\right)^{\otimes n}_{k_1,k_2} P_{i'',k_2,k_3} \left(S^{b_2}\right)^{\otimes n}_{k_3,k_4} \left(C^{b_1}\right)_{b_2,b} r_{j_2,b_1} U_{k_4,0} \\ &= \sum r_{i_2,a_1} r_{j_2,b_1} \left(C^{a_1}\right)_{a_2,a} \left(C^{b_1}\right)_{b_2,b} D_{(i'',0,a_2,0,b_2)}(\mathbf{U}_0) \end{aligned}$$

Using this, P_i can be expressed as

$$P_{i,i_1,j_1}(\mathbf{U}_0) = \sum_{(i_2,a),(j_2,b)} E_{(i,i_1,j_1),(i'',i_2,a,j_2,b)} D_{(i'',i_2,a,j_2,b)}(\mathbf{U}_0)$$

which is identical to

$$P_{i,i_1,j_1}(\mathbf{U}_0) = \sum_{i'',a_2,b_2} \tilde{E}_{(i,i_1,j_1),(i'',a_2,b_2)}(\mathbf{r}) D_{(i'',0,a_2,0,b_2)}(\mathbf{U}_0)$$

where

$$\tilde{E}_{(i,i_1,j_1),(i'',a_2,b_2)}(\mathbf{r}) = \sum_{\substack{i_2,j_2\\a,a_1\\b,b_1}} r_{i_2,a_1} \left(C^{a_1}\right)_{a_2,a} r_{j_2,b_1} \left(C^{b_1}\right)_{b_2,b} E_{(i,i_1,j_1),(i'',i_2,a,j_2,b)} \tag{3.1}$$

The matrix $\tilde{E} \in \mathbb{F}_q^{m_2 \times l^2 m_1}$.

For SNOVA to be hard to break, $\tilde{E}$ must be of high rank for all non-trivial values of $\mathbf{a}$. This requires at least that $l^2 m_1 \geq m_2$, setting a constraint on m_1.

Equation (3.1) can be evaluated for any $\mathbf{r}$. It depends on the E matrix (or equivalently, the ABQ matrices) as well as characteristic polynomial of the S matrix of SNOVA. In a way, the E 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`.

References

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

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

[3] 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`.

[4] 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.: **On the security of Round 2 SNOVA**. NIST Sixth Standardization Conference, 2025. Available at `https://csrc.nist.gov/csrc/media/events/2025/sixth-pqc-standardization-conference/on%20the%20security%20of%20round%202%20snova.pdf`.