

Exploiting SNOVA's Structure in the Wedge Product Attack

Hung Le^{1,2} Maxime Bros³ Jacob Lichtinger³ Brice Minaud²
Ray Perlner³ Daniel Smith-Tone^{3,4} Cristian Valenzuela⁴

¹LTCI, Telecom Paris, IP Paris, France

²École normale supérieure, PSL, CNRS, Inria, France

³NIST, Maryland, USA

⁴University of Louisville, KY, USA

Outline

- 1 Motivation & Context
- 2 Background: UOV and SNOVA
- 3 Wedge-Product Attack [Ran25]
- 4 Application to SNOVA
- 5 Conclusion

Motivation & Context

- Post-quantum signatures: aim for short signatures and practical speed.
- **UOV** (since 1999): robust, fast, but **large public keys**.
- Structured variants (MAYO, QR-UOV, **SNOVA**) reduce key sizes via algebraic structure.
- A wedge-based attack on UOV-like schemes has been proposed recently [[Ran25](#)].
- Question: *Does SNOVA's structure enable stronger wedge-based key-recovery attacks?*

Contributions

SL	(v, o, q, ℓ)	Our attack	Best attack
I	(37, 17, 16, 2)	141	153
	(25, 8, 16, 3)	144	166
	(24, 5, 16, 4)	177	180
III	(56, 25, 16, 2)	179	221
	(49, 11, 16, 3)	257	220
	(24, 5, 16, 5)	177	257
IV	(75, 33, 16, 2)	233	288
	(66, 15, 16, 3)	310	293
	(60, 10, 16, 4)	314	343
	(29, 6, 16, 5)	189	310

Background: UOV (Unbalanced Oil & Vinegar)

- **Public key:** m quadratic maps \mathcal{P} in $n = v + o$ variables over \mathbb{F}_q .
- **Signature:** a preimage $x \in \mathbb{F}_q^n$ of $\text{hash}(\text{message}) \in \mathbb{F}_q^m$ under the public key maps.
- **Secret key:** a trapdoor that enables efficient solving of the corresponding MQ system: a subspace \mathcal{O} of dimension o such $\mathcal{P}(\mathcal{O}) = 0$.
- Without the trapdoor, solving the MQ system is conjecturally hard.

- UOV-like scheme with two layers of structure:
 - *Whipping* layer (MAYO-like).
 - *Block-ring* layer over $\mathbb{F}_q[\mathbf{S}]$ with \mathbf{S} symmetric and $\chi_{\mathbf{S}}$ irreducible (so $\mathbb{F}_q[\mathbf{S}]$ is a field); n blocks of size $\ell \Rightarrow n\ell$ variables.
- **Public key:** m bilinear forms $\{\mathbf{P}_i\}_{i=1}^m$ in $n\ell$ variables that vanish on the oil subspace $\mathcal{O} \subseteq \mathbb{F}_q^{n\ell}$ with $\dim \mathcal{O} = ol$.
- **Observations:**
 - [LD24; Cab+25] An attacker can derive an $m\ell^2$ -dimensional family of bilinear forms that also vanish on \mathcal{O} :
$$(\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n} \quad (a, b \in \{0, \dots, \ell - 1\})$$
 - Both the vinegar and the oil subspace carry the block-ring structure.

Definition

Let $p = (p_1, \dots, p_m)$ be quadratic maps on \mathbb{F}_q^n (so p_i homogeneous of degree 2). For each i , the *polar form* Q_i is

$$Q_i(\mathbf{x}, \mathbf{y}) = p_i(\mathbf{x} + \mathbf{y}) - p_i(\mathbf{x}) - p_i(\mathbf{y}),$$

which is bilinear, and is alternating in characteristic 2.

- We identify Q_i with a bilinear 2-form $\widehat{Q}_i \in \bigwedge^2(\mathbb{F}_q^n)^*$.
- In our setting, the published bilinear forms are exactly these polars, so we set $\mathbf{P}_i := \widehat{Q}_i$.
- Matrix view: pick a basis, then $Q_i(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top M_i \mathbf{y}$ with $M_i^\top = -M_i$ (alternating in char 2).

Lars Ran' wedge attack [Ran25]

- A v -vector $\hat{\mathcal{A}} = \mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_v \in \bigwedge^v \mathbb{F}_q^n$ encodes a v -dimensional subspace $\mathcal{V} = \{\mathbf{a}_1, \dots, \mathbf{a}_v\}$ via its coordinates.

- A bilinear form $\mathbf{P}_i \in \bigwedge^2 (\mathbb{F}_q^n)^*$ acts as a 2-form. The wedge

$\hat{\mathcal{A}} \wedge \mathbf{P}_i \in \bigwedge^{v+2} \mathbb{F}_q^n$ tests isotropy:

$$\hat{\mathcal{A}} \wedge \mathbf{P}_i = 0 \iff \mathbf{P}_i(x) = 0 \text{ for all } x \in \mathcal{V}^\perp.$$

- Note: the conditions $\hat{\mathcal{A}} \wedge \mathbf{P}_i = 0$ are **linear** in the coordinates of $\hat{\mathcal{A}}$.

- **Goal:** recover the hidden split by finding a v -dimensional subspace \mathcal{V} (“vinegar” / oil-annihilator) such that the public 2-forms vanish on it.
- **Unknown:** a v -vector $\hat{A} \in \bigwedge^v \mathbb{F}_q^n$ representing \mathcal{V} .
- **Constraints** (linear in coordinates of \hat{A}):

$$\hat{A} \wedge \mathbf{P}_i = 0 \quad \text{for all } i = 1, \dots, m.$$

- Solve the resulting homogeneous linear system; decode \hat{A} (Plücker relations) to obtain \mathcal{V} .

Application to SNOVA

- From SNOVA, we have m public bilinear forms $\{\mathbf{P}_i\}$ on $n\ell$ variables that vanish on the oil subspace \mathcal{O} of $\dim ol$.
- Block-ring structure yields an $m\ell^2$ -family

$$\mathbf{P}_{i,a,b} = (\mathbf{S}^a)^{\otimes n} \mathbf{P}_i (\mathbf{S}^b)^{\otimes n}, \quad a, b \in \{0, \dots, \ell - 1\},$$

which also vanish on \mathcal{O} .

- We can use all $\mathbf{P}_{i,a,b}$ in the wedge constraints $\hat{\mathcal{A}} \wedge \mathbf{P}_{i,a,b} = 0$ to amplify rank and stabilize recovery of \mathcal{V} ; or we can use just m public bilinear forms $\hat{\mathcal{A}} \wedge \mathbf{P}_{i,0,0} = 0$.
- Block-ring structure also reduces the number of variables in the linear system.

Wedge map

$$\Phi : \bigwedge^v \mathbb{F}_q^n \longrightarrow \left(\bigwedge^{v+2} \mathbb{F}_q^n \right)^m, \quad \hat{\mathcal{A}} \mapsto (\hat{\mathcal{A}} \wedge \hat{Q}_1, \dots, \hat{\mathcal{A}} \wedge \hat{Q}_m).$$

- If $\ker \Phi$ is 1-D, its (projective) vector is $\hat{\mathcal{A}}$.
- Then recover the oil/vinegar decomposition via Gaussian elimination.
- Coordinates of $\hat{\mathcal{A}}$ correspond to **maximal minors** of an annihilator basis matrix \mathbf{A} .

$$\Phi_{\text{SNOVA}} : \bigwedge^{lv} \mathbb{F}_q^{\ell n} \rightarrow \left(\bigwedge^{\ell v+2} \mathbb{F}_q^{\ell n} \right)^{m\ell^2}, \quad \hat{\mathcal{A}} \mapsto (\hat{\mathcal{A}} \wedge \hat{Q}_1, \dots, \hat{\mathcal{A}} \wedge \hat{Q}_{m\ell^2}).$$

- Goal: exploit SNOVA's block-ring structure to reduce **dimension** (the number of variables) + keep the **rank** (the number of equations) sufficient to solve the system.

Dimension of Φ_{SNOVA} : Number of Independent Maximal Minors

- $\mathbb{F}_q[\mathbf{S}] \cong \mathbb{F}_q^\ell$ has only ℓ degrees of freedom; \mathbf{S} is diagonalizable over \mathbb{F}_q .
- Experimentally, the number of variables is $\binom{n}{v}^\ell$ not $\binom{\ell n}{\ell v}$

Proposition

Let $\mathbf{A} \in \mathbb{F}_q[\mathbf{S}]^{n \times v}$, with \mathbf{S} as in SNOVA. The number of linearly independent maximal minors of the embedded matrix $\iota(\mathbf{A}) \in \mathbb{F}_q^{n\ell \times v\ell}$ is

$$\binom{n}{v}^\ell$$

Rank of Φ_{SNOVA} : Equation Count (Heuristics)

- Attacker can generate an ml^2 -family of bilinear forms with same oil space.
- Many linear dependencies: forms $\mathbf{P}_{i,a,b}$ reduce to those with $\mathbf{P}_{i,a-b,0} \implies ml^2 \mapsto ml$ forms.
- We consider two equation-count heuristics:
 - 1 **Conservative:** use only the base m 2-forms.
 - 2 **Less conservative:** scale $m \mapsto ml$.

Conservative Modelling

Let o' be the projected oil dimension used in the attack ($1 \leq o' < \min\{m, \frac{o\ell}{2}\}$).

$$U_{\text{SNOVA (exact)}} = \binom{v + o'}{v}^\ell,$$

$$E_{\text{SNOVA (estimated)}} = \sum_{i=1}^{o'} (-1)^{i+1} \binom{m+i-1}{i} \sum_{a_0+\dots+a_{\ell-1}=2i} \prod_{j=0}^{\ell-1} \binom{v+o'}{v+a_j}.$$

Sparse linear algebra cost (field ops in \mathbb{F}_q)

$$\min\left(EU^{\omega-1}, \tau EU\right), \quad \tau = \binom{v+2}{2}^{o'}$$

Estimated Complexities via Conservative Modelling

$(v, o', m = o, \ell)$	Variables and equations		Our attack	Best attack in [Wan+25]
	$\log_2(U_{\text{SNOVA}})$	$\log_2(E_{\text{SNOVA}})$		
(37, 7, 17, 2)	50.38	50.59	141	153
(25, 5, 8, 3)	51.36	51.68	144	166
(24, 5, 5, 4)	67.43	67.90	177	180
(56, 8, 25, 2)	64.09	64.13	179	221
(49, 8, 11, 3)	91.87	92.12	257	220
(24, 4, 5, 5)	71.61	72.08	177	257
(75, 10, 33, 2)	83.02	83.19	233	288
(66, 9, 15, 3)	110.61	110.83	310	293
(60, 7, 10, 4)	118.78	118.82	314	343
(29, 4, 6, 5)	76.60	76.88	189	310

Conclusion

- SNOVA's block-ring structure \implies dependencies among minors / equations \implies reduce the linear system \implies lower security estimates.
- Observed complexities fit between our two heuristics; we report the *conservative* side.
- Result: 5/10 Round-2 SNOVA parameters are below the target SL.
- Ongoing works
 - Build the exact formula for the ranks in both approaches.
 - Investigate the case $v > 2m$.
 - A new modelling to reduce further number of variables.
- We would like to thank Lars Ran and Po-En Tseng (SNOVA team) for their helpful discussions.

Thank you for your attention!

New modelling

- Write the annihilator basis as $A_2 = \text{diag}(B_1, \dots, B_\ell)$ $B_j \in \mathbb{F}^{n \times v}$
- Only global minors that pick *exactly* v rows per block can be nonzero. Keep *block* Plücker variables $p_I^{(j)} = \det((B_j)_{I,*})$, $|I|=v$.
- *Case 1* equations (choose $v+2$ rows in one block) are **linear in a single block**: constants from other blocks factor out and can be divided away.
- Normalize per block with a nonzero pivot minor so each block has $\binom{n}{v} - 1$ free variables.
- Solve blocks first (linear), then form cross-block (*Case 2*) bilinear equations on the **reduced** variable set.

Bibliography

- [Cab+25] Daniel Cabarcas et al. “Improved Attacks for SNOVA by Exploiting Stability under a Group Action”. In: *CRYPTO*. 2025.
- [LD24] Peigen Li and Jintai Ding. “Cryptanalysis of the SNOVA Signature Scheme”. In: *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part II*. Ed. by Markku-Juhani O. Saarinen and Daniel Smith-Tone. Vol. 14772. Lecture Notes in Computer Science. Springer, 2024, pp. 79–91. URL: https://doi.org/10.1007/978-3-031-62746-0%5C_4.
- [Ran25] Lars Ran. *Wedges, oil, and vinegar – An analysis of UOV in characteristic 2*. Cryptology ePrint Archive, Paper 2025/1143. 2025. URL: <https://eprint.iacr.org/2025/1143>.
- [Wan+25] Lih-Chung Wang et al. *SNOVA: Specification Document* –