

## Round 2 SNOVA Update

Lih-Chung Wang, Chun-Yen Chou, Jintai Ding,  
Yen-Liang Kuan, Jan Adriaan Leegwater, Ming-Siou Li,  
Bo-Shu Tseng, **Po-En Tseng**, Chia-Chun Wang

6th NIST PQC Standardization Conference

# Outline

SNOVA

Wedge Attack

SNOVA with Odd Prime  $q$

Now and Next

## SNOVA Rationale

SNOVA generalizes UOV to the matrix ring with added structure

- coefficients of public key  $[\mathbf{P}_1], \dots, [\mathbf{P}_m]$  belong to  $\text{Mat}_{l \times l}(\mathbb{F}_q)$
- oil space  $\mathcal{O} \subset (\mathbb{F}_q[S])^n$  where

$$\mathbb{F}_q[S] = \{a_0 + a_1S + \dots + a_{l-1}S^{l-1} \mid a_0, \dots, a_{l-1} \in \mathbb{F}_q\}$$

- scramble the public matrices using fixed  $ABQ$  matrices

$\implies$  compact key and signature + relatively fast performance

## Round 2 Tweaks

- Round 1 public map

$$P_i(\mathbf{U}) = \sum_{\alpha=0}^{l^2-1} \sum_{j=1}^n \sum_{k=1}^n A_{\alpha} \cdot U_j^t(Q_{\alpha 1} P_{i,jk} Q_{\alpha 2}) U_k \cdot B_{\alpha}$$

- Round 2 public map

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

where  $i' = i + \alpha \pmod{m}$

## Round 2 Tweaks

We made 3 tweaks in Round 2:

- Varying  $ABQ$  matrices:

$$A_\alpha, Q_{\alpha,1}, Q_{\alpha,2}, B_\alpha \longrightarrow A_{i,\alpha}, Q_{i,\alpha,1}, Q_{i,\alpha,2}, B_{i,\alpha}$$

- Increasing the no. of terms in the summation over  $\alpha$ :

$$l^2 \longrightarrow l^2 + l$$

- Mixing  $[P_i]$  in the public map:

$$P_{i,jk} \longrightarrow P_{i',jk}$$

## Parameters

Security Level	Round 1 $(v, o, q, l)$	Round 2 $(v, o, q, l)$
I	$(28, 17, 16, 2)$	$(37, 17, 16, 2)$
	$(25, 8, 16, 3)$	$(25, 8, 16, 3)$
	$(24, 5, 16, 4)$	$(24, 5, 16, 4)$
III	$(43, 25, 16, 2)$	$(56, 25, 16, 2)$
	$(49, 11, 16, 3)$	$(49, 11, 16, 3)$
	$(37, 8, 16, 4)$	$(37, 8, 16, 4)$
		$(24, 5, 16, 5)$
V	$(61, 33, 16, 2)$	$(75, 33, 16, 2)$
	$(66, 15, 16, 3)$	$(66, 15, 16, 3)$
	$(60, 10, 16, 4)$	$(60, 10, 16, 4)$
		$(29, 6, 16, 5)$

## Other Changes

- We add the option to use SHAKE for public key expansion
- Implement AVX2 Version of SNOVA
  - We have  $20 - 30\times$  speedup in Round 2 compared to Round 1
- Our optimization is still ongoing
  - Compared to the beginning of Round 2, we now have a faster  $l = 4$  implementation (constant time).
- Round 2 tweaks enhance the “whipping structure”
  - This mitigates forgery attacks with MinRank [Beu25]

## Other Changes

Security Level	Round 2 $(v, o, q, l)$	seed for generating $ABQ$
I	(37, 17, 16, 2)	fixed
	(25, 8, 16, 3)	fixed
	(24, 5, 16, 4)	random
III	(56, 25, 16, 2)	fixed
	(49, 11, 16, 3)	fixed
	(37, 8, 16, 4)	random
	(24, 5, 16, 5)	random
V	(75, 33, 16, 2)	fixed
	(66, 15, 16, 3)	fixed
	(60, 10, 16, 4)	random
	(29, 6, 16, 5)	random

# Performance

Benchmarks on a desktop (Arrow Lake), Intel(R) Core(TM) Ultra 7 265K, compiler: gcc 14.2.0

- SL I, SNOVA(24, 5, 16, 4)
  - public key: 1016 / signature: 248 / secret key: 48 (bytes)
  - sign (ssk): 666,219 / verify: 164,064 (cycles)
- SL III, SNOVA(37, 8, 16, 4)
  - public key: 4112 / signature: 376 / secret key: 48 (bytes)
  - sign (ssk): 2,322,163 / verify: 454,935 (cycles)
- SL V, SNOVA(60, 10, 16, 4)
  - public key: 8016 / signature: 576 / secret key: 48 (bytes)
  - sign (ss): 6,528,442 / verify: 1,167,715 (cycles)

⇒ an attractive candidate for continued study

## Wedge Attack

Recently, Lars Ran [Ran25] proposed an attack on UOV-like schemes in characteristic 2. The attack can be summarized in:

1. Construct alternating forms  $q_1, \dots, q_m$  vanishing on  $\mathcal{O}$
2. Construct the linear map

$$\mathcal{M} : \bigwedge^v \mathbb{F}_q^n \longrightarrow \left( \bigwedge^{v+2} \mathbb{F}_q^n \right)^m, \alpha \mapsto (\alpha \wedge q_1, \dots, \alpha \wedge q_m).$$

Then, the  $v$ -form  $\mathcal{V} \in \ker(\mathcal{M})$ .

3. Recover the oil space  $\mathcal{O}$  from the  $v$ -form  $\mathcal{V}$

## Ran's Wedge Attack on UOV

Note that the attack relies on:

- polar forms of UOV in char 2 are symmetric and alternating
  - Range of  $v, o$  of UOV variant in char 2 need further study
  - UOV variants over odd prime  $q$  is unaffected.
- random UOV instances
  - To obtain an accurate prediction of  $\dim(\ker \mathcal{M})$
- $v < \min(\frac{o-1}{2}, 2) \cdot m$ 
  - To ensure there's no undesirable kernel element
- the projecting down technique  $o \rightarrow o'$ 
  - To minimize the size of  $\mathcal{M}$

## Wedge Attack on SNOVA

Peigen Li suggests that the attacker can consider

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

However,

- the underlying  $(lv, lo, q, l^2o)$ -UOV is structured  
→ How to accurately predict  $\dim(\ker \mathcal{M})$  ?
- one can consider the lifted variant,  $(v, o, q^l)$ -UOV  
→ In this case  $v > 2m$ , we observe that  $\dim(\ker \mathcal{M})$  increases
- How to eliminate the undesirable kernel element in  $\ker \mathcal{M}$  ?

⇒ Lars withdrew his complexity claim on SNOVA

## Countermeasures

There are two possible countermeasures:

- increase the no. of vinegar variables
  - makes the “project down” step more difficult, in general
  - the complexity will increase significantly, in general
  - this can easily resist wedge attacks
- choose a field  $\mathbb{F}_q$  with an odd prime  $q$ 
  - we could choose  $[\mathbf{P}_i]$  of SNOVA as symmetric matrices

## SNOVA with Odd Prime $q$

When  $[\mathbf{P}_i]$  is symmetric, we will have:

- + reduce the public key size by about 40%
  - + mitigate key-recovery attacks [IA24]
  - + reduce the no. of alternating forms
  - + no significant impact on performance
  - further cryptanalysis is needed
- ⇒ A detailed security analysis will be presented in a later paper.

Preliminary proposed parameter set SNOVA(24,5,23,4):

- public key: 616 / signature: 282 / secret key: 48 (bytes)
- sign(ssk): 614,670 / verify: 130,466 (cycles)

## Where Do We Stand Now and Our Next Step

- Current state of cryptanalysis:
  - Some variant of the wedge attack might work for SNOVA.  
May reduce security below SL for some parameters
  - $l = 4$  parameter sets currently seems secure.
- Reconsidering the SNOVA parameter sets in the wake of the wedge attack.
  - For example, we are considering preliminary changes like  $(37, 17, 16, 2) \rightarrow (43, 17, 16, 2)$ .
- SNOVA with an odd prime  $q$  is very promising as a general purpose scheme

We will share full analysis and updates after further study.

Thank you!

## Reference

- [Beu25] Ward Beullens. Improved cryptanalysis of SNOVA. In Advances in Cryptology - EUROCRYPT 2025.
- [IA24] Yasuhiko Ikematsu and Rika Akiyama. Revisiting the security analysis of SNOVA. Proceedings of the 11th ACM Asia Public-Key Cryptography Workshop, 2024.
- [Ran25] Lars Ran. Wedges, oil, and vinegar – An analysis of UOV in characteristic 2. Cryptology ePrint Archive, 2025.