

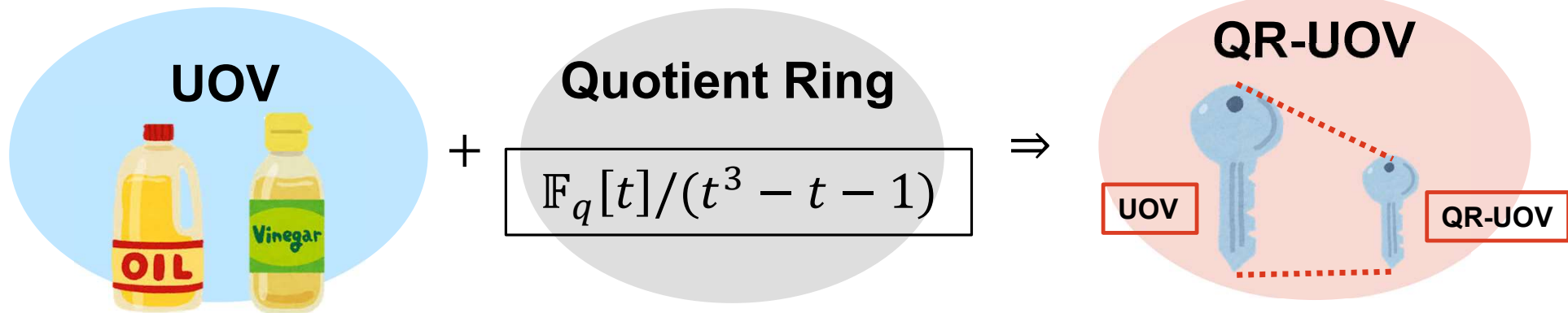
QR-UOV

Hiroki Furue, Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi,
Haruhisa Kosuge, Kimihiro Yamakoshi, Rika Akiyama,
Satoshi Nakamura, Shingo Orihara, Koha Kinjo

Sixth PQC Standardization Conference

September 24, 2025

QR-UOV: Secure Scheme with Small Public Key



- **Conservative Security:** following UOV except for QR structure
- **Small Public Key:** half the public-key size from UOV retaining its advantages



small signatures, fast verification

UOV

\mathbb{F}_q : the finite field with q elements

n : the number of variables

m : the number of equations

$$(n > m)$$

x_1, \dots, x_v : **vinegar** variables

x_{v+1}, \dots, x_n : **oil** variables

$$(v = n - m)$$

① $\mathcal{F} = (f_1, \dots, f_m): \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ [invertible quadratic map]

$$f_k = \sum_{i=1}^n \sum_{j=1}^v \alpha_{ij}^{(k)} x_i x_j$$

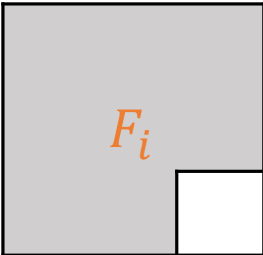
② $\mathcal{S}: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ [linear map]

③ $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$ [quadratic map]

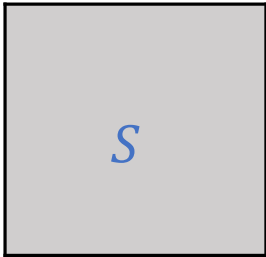
Public key : \mathcal{P} , Private key : $(\mathcal{F}, \mathcal{S})$

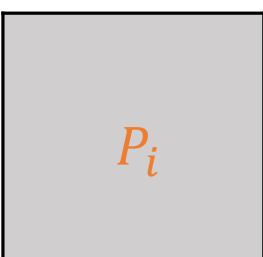
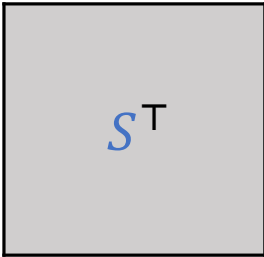
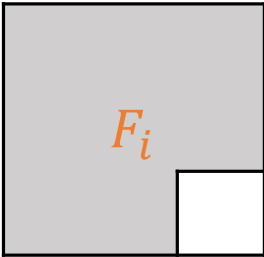
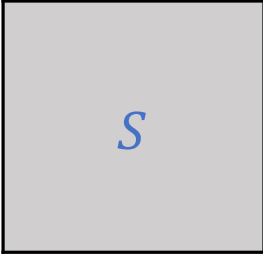
UOV

• $(p_1, \dots, p_m) = (f_1, \dots, f_m) \circ \mathcal{S}$

$f_i(x) = (x_1 \cdots x_n)$

 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

 $m \times m \hat{=}$

$\mathcal{S}(x) =$

 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$p_i(x) = (x_1 \cdots x_n)$

 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x_1 \cdots x_n)$



 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

QR-UOV

QR-UOV: Concept

We reduce the public key size from the original UOV by embedding the structure of **quotient ring** $\mathbb{F}_q[t]/(f)$ into the public key matrices.

Compress the public key size

$$\mathbb{F}_7^{6 \times 6} \ni \left(\begin{array}{ccc|ccc} 0 & 5 & 1 & 3 & 0 & 1 \\ 5 & 1 & 1 & 0 & 1 & 3 \\ 1 & 1 & 1 & 1 & 3 & 3 \\ \hline 6 & 5 & 6 & 0 & 5 & 4 \\ 5 & 6 & 3 & 5 & 4 & 1 \\ 6 & 3 & 2 & 4 & 1 & 3 \end{array} \right) \longleftrightarrow \left(\begin{array}{c|c} 5t^2 + t & t + 3 \\ \hline 5t^2 + 6t + 6 & 5t^2 + 4t \end{array} \right) \in (\mathbb{F}_7[t]/(t^3 - 3t - 1))^{2 \times 2}$$

following the direction from LWE to the Module LWE

QR-UOV

[Definition]

$\ell \in \mathbb{N}$, $f \in \mathbb{F}_q[t]$ ($\deg f = \ell$)

$\forall g \in \mathbb{F}_q[t]/(f)$, $\Phi_g^f \in \mathbb{F}_q^{\ell \times \ell}$: $(1, t, \dots, t^{\ell-1}) \Phi_g^f = (g, tg, \dots, t^{\ell-1}g)$

ex) $q = 2$, $f = t^3 + t + 1$, $g = at^2 + bt + c$ ($a, b, c \in \mathbb{F}_2$)

$$\Rightarrow \Phi_g^f = \begin{pmatrix} c & a & b \\ b & a+c & a+b \\ a & b & a+c \end{pmatrix}$$

We can represent this 3-by-3 matrix by only 3 elements.



By applying the structure of Φ_g^f to P_i , we can reduce the public key size.

QR-UOV

$W \in \mathbb{F}_q^{\ell \times \ell}$ s.t. $\forall g \in \mathbb{F}_q[t]/(f), W\Phi_g^f$: **symmetric**

- F_i : block $W\Phi_g^f$ matrices ($i = 1, \dots, m$)
- S : block Φ_g^f matrix

$$\begin{array}{c} P_i \\ \left(\begin{array}{c|c} W\Phi_*^f & W\Phi_*^f \\ \hline W\Phi_*^f & W\Phi_*^f \end{array} \right) \\ \end{array} = \begin{array}{c} S^\top \\ \left(\begin{array}{c|c} (\Phi_*^f)^\top & (\Phi_*^f)^\top \\ \hline (\Phi_*^f)^\top & (\Phi_*^f)^\top \end{array} \right) \\ \end{array} \cdot \begin{array}{c} F_i \\ \left(\begin{array}{c|c} W\Phi_*^f & W\Phi_*^f \\ \hline W\Phi_*^f & W\Phi_*^f \end{array} \right) \\ \end{array} \cdot \begin{array}{c} S \\ \left(\begin{array}{c|c} \Phi_*^f & \Phi_*^f \\ \hline \Phi_*^f & \Phi_*^f \end{array} \right) \\ \end{array}$$

P_i : block $W\Phi_g^f$ matrices



represented by only n^2/ℓ elements

Round 2 Updates

Comprehensive specification

- We revised and detailed the specification.
- We refined the security proof.

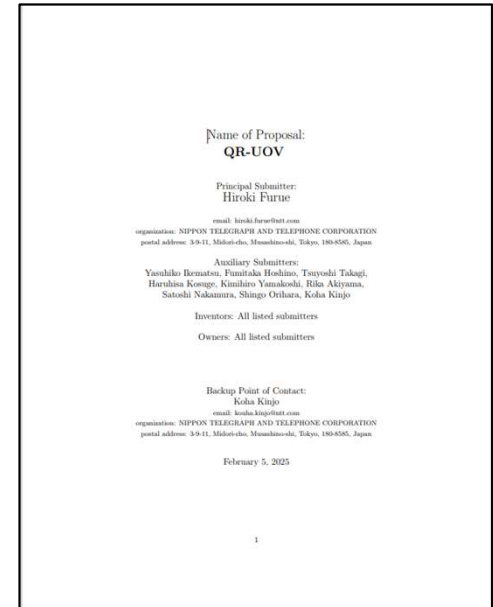
Parameters

- We selected one main parameter for each security level.

Level I

$$(q, v, m, \ell) = (127, 156, 54, 3) \Rightarrow \text{fast performance}$$
$$(q, v, m, \ell) = (7, 740, 100, 10)$$
$$(q, v, m, \ell) = (31, 165, 60, 3)$$
$$(q, v, m, \ell) = (31, 600, 70, 10)$$

(All parameters remain secure since the Round 1 specification.)



Security

Security

The EUF-CMA security of QR-UOV is reduced to the hardness of

- **UOV problem** (distinguishing MQ and UOV maps)
 - common assumption in UOV-based schemes
- **QR-MQ problem** (MQ problem with QR structure)
 - original, with no known structural attacks

Response to NIST's comment

The attack on VOX does not affect the security of QR-UOV.

[Guo and Ding, PQCrypto'24]

(We have already considered the rectangular MinRank attack.)

Recent Attacks

[L. Ran. ePrint 2025/1143]

- A new key recovery attack on UOV variants over fields of characteristic 2
- QR-UOV uses **odd characteristic** fields and thus is **not affected**.

[Y. Jin et al. ePrint 2025/1137]

- A variant of the attack in **odd characteristic** has also been proposed.
- It does **not outperform** the existing reconciliation attack.

➔ All proposed parameters of QR-UOV remain secure.



Size and Performance

Key and Signature Size

level	(q, v, m, ℓ)	public key (bytes)	private key (bytes)	signature (bytes)
I	(127,156,54,3)	24,255	32	200
III	(127,228,78,3)	71,891	48	292
V	(127,306,105,3)	173,676	64	392

reduce the public key size from UOV

$\left\{ \begin{array}{l} 44\text{KB} \rightarrow 24\text{KB} \\ 189\text{KB} \rightarrow 72\text{KB} \\ 447\text{KB} \rightarrow 174\text{KB} \end{array} \right.$

AVX2 Implementation



The AVX2 implementation of QR-UOV was improved [AUH25].

Architecture: Skylake

EC2 instance type: c5n.metal

CPU base frequency: 3.0GHz

80% reduction

level	KeyGen (Mcycles)		Sign (Mcycles)		Verify (Mcycles)	
	[AUH25]	Round2	[AUH25]	Round2	[AUH25]	Round2
I	3.27	16.74	0.87	3.16	0.46	2.61
III	11.59	62.45	2.48	9.59	1.38	7.77
V	33.34	211.02	6.24	23.86	3.64	18.42

[AUH25] H. Amagasa, R. Ueno, N. Homma: AVX2 Implementation of QR-UOV for Modern x86 Processors. ePrint (2025)

Cortex-m4 Implementation



We developed the implementation on ARM Cortex-M4 chips.

(using crypt library from pqm4 project [KKP24])

<https://github.com/mupq/pqm4?tab=readme-ov-file>

speed (Mcycles), STM32L4R5ZIT6

level	Keygen	Sign	Verify
I	157.1	52.1	43.8
III	675.5	196.5	173.9
V	2020.5	468.9	414.3

Advantages and Applications

Advantages of QR-UOV

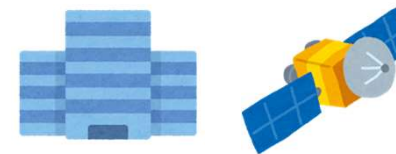
- Conservative security
- Small signatures (< 512 bytes)
- Fast verification
- Reducing the public key size from UOV



Suitable Applications

- The public key is preinstalled.
 - ✂ It is necessary to store multiple public keys.
- We have to verify many signatures.

ex) root certificate, satellite communication





Thank you for your attention!



- UOV

<https://info.isl.ntt.co.jp/crypt/qruov/index.html>