2nd Oxford Post-Quantum Cryptography Summit 2023

QR-UOV

(Quotient Ring Unbalanced Oil and Vinegar)

Hiroki Furue

The University of Tokyo, Japan

Yasuhiko Ikematsu, Fumitaka Hoshino, Tsuyoshi Takagi,
Kan Yasuda, Toshiyuki Miyazawa, Tsunekazu Saito, Akira Nagai

Outline

- **UOV**
- QR-UOV: Construction
- QR-UOV: Security
- QR-UOV: Parameter
- Conclusion

UOV

$n, m \in \mathbb{N} \quad (n > m)$
n : the number of variables
m: the number of equations

$x_1, \ldots, x_v$: **vinegar** variables
$x_{v+1}, \ldots, x_n$: **oil** variables
※ $n - v = m$

① **Central map**

$$\mathcal{F} = (f_1, \ldots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m$$ **[invertible quadratic map]**

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

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

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

Public Key: $\mathcal{P}$, **Secret Key:** $(\mathcal{F}, \mathcal{S})$

UOV

Computing $\mathcal{F}^{-1}$

① Fix variables $x_1, \dots, x_v$ (vinegar variables) randomly.

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

② Solve a linear polynomial in $x_{v+1}, \dots, x_n$ (oil variables).

(m equations, m variables)

※ If there does not exist a solution, return to ①.

Signer ($\mathcal{F}, \mathcal{S}$)

Message： $\boldsymbol{m} \in \mathbb{F}_q^m$

SigGen $\boldsymbol{s} = \underbrace{\mathcal{S}^{-1} \circ \mathcal{F}^{-1}}_{\mathcal{P}^{-1}}(\boldsymbol{m})$

$\boldsymbol{m}, \boldsymbol{s}$ →

Verifier ($\mathcal{P}$)

Verify $\boldsymbol{m} \stackrel{?}{=} \underbrace{\mathcal{P}(\boldsymbol{s})}_{\mathcal{P} \circ \mathcal{P}^{-1}(\boldsymbol{m})}$

Representation Matrices

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

$$f_i(x) = (x_1 \cdots x_n) \; MF_i \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \mathcal{S}(x) = MS \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$m \times m$ ⇧

$$p_i(x) = (x_1 \cdots x_n) \; MP_i \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$= (x_1 \cdots x_n) \; MS^{\top} \; MF_i \; MS \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Outline

- UOV
- **QR-UOV: Construction**
- QR-UOV: Security
- QR-UOV: Parameter
- Conclusion

Matrices of Quotient Ring

[Def] Polynomial Matrix Φ_g^f

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

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

$$(1, t, \ldots, t^{\ell-1})\Phi_g^f = (g, tg, \ldots, t^{\ell-1}g)$$

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

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

This 3×3 matrix can be represented by only 3 elements.

If we can apply this Φ_g^f to the public key MP_i, then we can reduce the public key size.

Matrices of Quotient Ring

$$\{\Phi_g^f \mid g \in \mathbb{F}_q[t]/(f)\} \cong \mathbb{F}_q[t]/(f)$$

- $\Phi_{g_1}^f + \Phi_{g_2}^f = \Phi_{g_1+g_2}^f$
- $\Phi_{g_1}^f \cdot \Phi_{g_2}^f = \Phi_{g_1 \cdot g_2}^f$

$MS, MF_i (i = 1, \dots, m)$: block Φ_g^f matrices $\left(\begin{array}{c|c|c} \Phi_{g_{11}}^f & \Phi_{g_{12}}^f & \Phi_{g_{13}}^f \\ \hline \Phi_{g_{21}}^f & \Phi_{g_{22}}^f & \Phi_{g_{23}}^f \\ \hline \Phi_{g_{31}}^f & \Phi_{g_{32}}^f & \Phi_{g_{33}}^f \end{array}\right)$

$\Rightarrow MP_i = MS^\top \cdot MF_i \cdot MS \ (i = 1, \dots, m)$: block Φ_g^f matrices?

$MS^\top$ is not always block Φ_g^f

Matrices of Quotient Ring

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

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

$$\left(\Phi_{g_2}^f\right)^\top \left(W\Phi_{g_1}^f\right)\Phi_{g_2}^f = \left(\Phi_{g_2}^f\right)^\top W^\top \Phi_{g_1}^f \Phi_{g_2}^f \quad [W \text{ is symmetric since } \Phi_1^f = I_\ell.]$$

$$= \left(W\Phi_{g_2}^f\right)^\top \Phi_{g_1}^f \Phi_{g_2}^f$$

$$= \left(W\Phi_{g_2}^f\right)\Phi_{g_1}^f \Phi_{g_2}^f = W\Phi_{g_2 g_1 g_2}^f$$

MP_i : block $W\Phi_g^f$ matrices

Matrices of Quotient Ring

Lemma

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

there exist an invertibel $\ell \times \ell$ matrix W such that

$W\Phi_g^f$ is **symmetric** for any $g \in \mathbb{F}_q[t]/(f)$.

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

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

$$W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Quotient Ring UOV (QR-UOV)

Key Generation

① **Irreducible** polynomial: $f \in \mathbb{F}_q[t]$ $(\deg f = \ell)$

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

② MF_i: block $W\Phi_g^f$ matrices $(i = 1, \dots, m)$

MS : block Φ_g^f matrix

③ $MP_i = MS^\top \cdot MF_i \cdot MS$ $(i = 1, \dots, m)$

$\Rightarrow MP_i$: block $W\Phi_g^f$ matrices

➡ **Reduce the public key size**

Outline

- UOV
- QR-UOV: Construction
- **QR-UOV: Security**
- QR-UOV: Parameter
- Conclusion

Security Proof

From the result of Kosuge and Xagawa [Kosuge, Xagawa, ePrint 2022], the EUF-CMA security of our QR-UOV is reduced to the difficulty of

- **UOV problem**

  distinguish a randomized quadratic map and
  a public key map of the plain UOV

- **QR-MQ problem**

  solve the MQ problem constructed from block $W\Phi_g^f$ matrices

in the quantum random oracle model (QROM).

QR-MQ Problem (Direct attacks)

- We have no theoretical security proof for the difficulty of the QR-MQ problem.
- We experimentally confirmed that the solving degree of the public key system is the same as that of the random system.

- Wiedemann XL [Yang et al., FSE 2007]
- polynomial XL [Furue, Kudo, ePrint 2021]
- Thomae-Wolf method [Thomae, Wolf, PKC 2012]
- Hashimoto's method [Hashimoto, ePrint 2021]

UOV Problem (Key Recovery Attacks)

$N = n/\ell$

$MP_k = \sum_{i=0}^{\ell-1} \bar{P}_k^{(i)} \otimes W \Phi_{t^i}^{f} \ \left(\bar{P}_k^{(i)} \in \mathbb{F}_q^{N\times N}\right)$, $\overline{MP_k} = \sum_{i=0}^{\ell-1} t^i \bar{P}_k^{(i)} \in \mathbb{F}_{q^\ell}^{N\times N}$

$MF_k = \sum_{i=0}^{\ell-1} \bar{F}_k^{(i)} \otimes W \Phi_{t^i}^{f} \ \left(\bar{F}_k^{(i)} \in \mathbb{F}_q^{N\times N}\right)$, $\overline{MF_k} = \sum_{i=0}^{\ell-1} t^i \bar{F}_k^{(i)} \in \mathbb{F}_{q^\ell}^{N\times N}$

$MS = \sum_{i=0}^{\ell-1} \bar{S}^{(i)} \otimes \Phi_{t^i}^{f} \ \left(\bar{S}^{(i)} \in \mathbb{F}_q^{N\times N}\right)$, $\overline{MS} = \sum_{i=0}^{\ell-1} t^i \bar{S}^{(i)} \in \mathbb{F}_{q^\ell}^{N\times N}$

$\Rightarrow \ \overline{MP_k} = \overline{MS}^\top \cdot \overline{MF_k} \cdot \overline{MS}$

We can apply key recovery attacks on **UOV**$(q^\ell, v/\ell, m/\ell, m)$.

- Kipnis-Shamir attack [Kipnis, Shamir, CRYPTO 1998]
- reconciliation attack [Ding et al., ACNS 2008]
- intersection attack [Beullens, EUROCRYPT 2021]
- rectangular MinRank attack [Beullens, EUROCRYPT 2021]

Outline

- UOV
- QR-UOV: Construction
- QR-UOV: Security
- **QR-UOV: Parameter**
- Conclusion

Public Key and Signature Size

Security Level 1

※ We applied some techniques which reduce the public key size.

[Czypek et al., CHES 2012], [Petzoldt, PQCrypto 2020]

parameter	public key (B)	signature (B)
$(q, v, m, \ell) = (7,740,100,10)$	20,657	331
$(q, v, m, \ell) = (31,165,60,3)$	23,657	157
$(q, v, m, \ell) = (31,600,70,10)$	12,282	435
$(q, v, m, \ell) = (127,156,54,3)$	24,271	200

- The size of the secret key is 256 bits.

Performance

64-bit environments (in C)

Processor: AMD EPYC 7763.
Clock Speed: Boost Clock : Up to 3.5GHz, Base Clock: 2.45GHz.
Memory: 128GB (32GB RDIMM, 3200MT/s, Dual Rank, 8Gb base x4)
Operating System: Linux 5.19.0-41-generic, gcc version 11.3.0.
Measurement Software: supercop-20221122.

parameter	keygen (Mcycles)	sign (Mcycles)	verify (Mcycles)
$(q, v, m, \ell) = (7{,}740{,}100{,}10)$	177.911	167.711	99.755
$(q, v, m, \ell) = (31{,}165{,}60{,}3)$	20.223	15.813	11.614
$(q, v, m, \ell) = (31{,}600{,}70{,}10)$	93.984	92.480	73.814
$(q, v, m, \ell) = (127{,}156{,}54{,}3)$	16.700	13.419	10.575

Outline

- UOV
- QR-UOV: Construction
- QR-UOV: Security
- QR-UOV: Parameter
- **Conclusion**

Conclusion

- We proposed a new variant of UOV (QR-UOV) using quotient ring to reduce the public key size.
- **Public key size:** Our proposed parameters reduce the public key size by approximately 50% compared with the plain UOV without significantly increasing the signature size.
- **Simplicity:** Our QR-UOV is a natural extension of UOV utilizing the quotient rings structure, like an extension from LWE to MLWE.