A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV

Hiroki Furue[1], Yasuhiko Ikematsu [2], Yutaro Kiyomura[3], Tsuyoshi Takagi[1]

1. The University of Tokyo, Japan
2. Kyushu University, Japan
3. NTT Social Informatics Laboratories, Japan

ASIACRYPT 2021

Our Contributions

- Multivariate public key cryptosystems are candidates of post quantum cryptosystems.
- **UOV**: one of multivariate signature schemes
- We proposed a new variant of UOV:
  Quotient Ring UOV (QR-UOV).
  - It utilizes matrices corresponding to elements of a quotient ring.
  - Compared with Rainbow (a variant of UOV), QR-UOV reduces the public key size 50～70 %.

Outline

- Multivariate Public Key Cryptosystems
- UOV Signature Scheme
- Quotient Ring UOV (QR-UOV)
- Conclusion

Post-Quantum Cryptography

We need cryptosystems secure against quantum computer attacks.

- Multivariate polynomial cryptography
- Lattice-based cryptography
- Code-based cryptography
- Hash-based cryptography
- Isogeny-based cryptography

MQ Problem

Multivariate quadratic polynomial problem

$MQ(q, n, m)$

- $\mathbb{F}_q$: the finite field with q elements
- n : the number of variables
- m : the number of equations

Given $\mathcal{F} = (f_1, \ldots, f_m)$: a quadratic system in n variables $\mathbf{x} = (x_1, \ldots, x_n)$ over $\mathbb{F}_q$

Find a solution in $\mathbb{F}_q^n$ to $\mathcal{F}(\mathbf{x}) = \mathbf{0} \in \mathbb{F}_q^m$

$$f_k = \sum_{i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} \beta_i^{(k)} x_i + \gamma^{(k)} \quad \left(\alpha_{ij}^{(k)}, \beta_i^{(k)}, \gamma^{(k)} \in \mathbb{F}_q\right)$$

Outline

- Multivariate Public Key Cryptosystems
- UOV Signature Scheme
- Quotient Ring UOV (QR-UOV)
- Conclusion

Unbalanced Oil and Vinegar

[Kipnis et al., EUROCRYPT 1999]

- One of multivariate signature schemes
- UOV has essentially not been broken for over 20 years.
- Rainbow (a variant of UOV) is one of the third-round finalists of the NIST PQC project.

Advantage

- Small signature
- Short execution time

Disadvantage

- Large public key

Unbalanced Oil and Vinegar

Key Generation

① $\mathcal{F} = (f_1, \ldots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m \ (n > m)$

[invertible quadratic map]

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

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

③ $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$

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

Unbalanced Oil and Vinegar

Message	$\boldsymbol{m} \in \mathbb{F}_q^m$
Signature	$\boldsymbol{s} = \mathcal{S}^{-1} \circ \mathcal{F}^{-1}(\boldsymbol{m})$
Verification	$\boldsymbol{m} \stackrel{?}{=} \mathcal{P}(\boldsymbol{s})$

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

① Fix variables $x_1, \ldots, x_v$ 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 Solving a linear polynomial in $x_{v+1}, \ldots, x_n$
(m equations, m variables)

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

Example

- $q = 3, n = 4, m = 2, v = 2$

$$\begin{cases} f_1(\boldsymbol{x}) = x_1^2 + 2x_1x_2 + 2x_1x_4 + x_2^2 + 2x_2x_4 \\ f_2(\boldsymbol{x}) = x_1x_2 + x_1x_4 + x_2x_3 + 2x_2x_4 \end{cases}$$

Solve $\mathcal{F}(\boldsymbol{x}) = (0,1)$

Fix $(x_1, x_2) = (0,2) \Rightarrow$ $\begin{cases} x_4 + 1 = 0 \\ 2x_3 + x_4 = 1 \end{cases}$

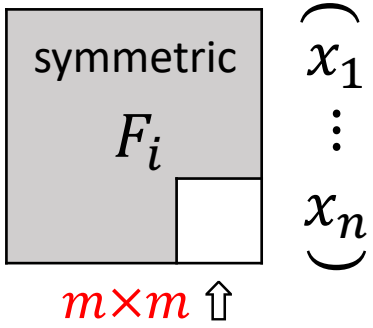
Random values

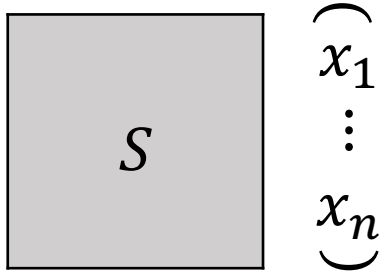
$$(x_3, x_4) = (1,2)$$

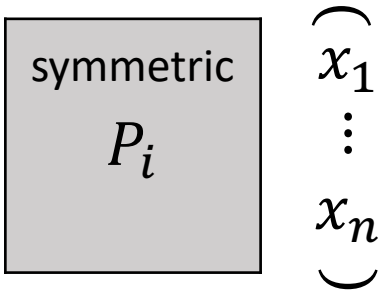
$$\Rightarrow \mathcal{F}(0,2,1,2) = (0,1)$$

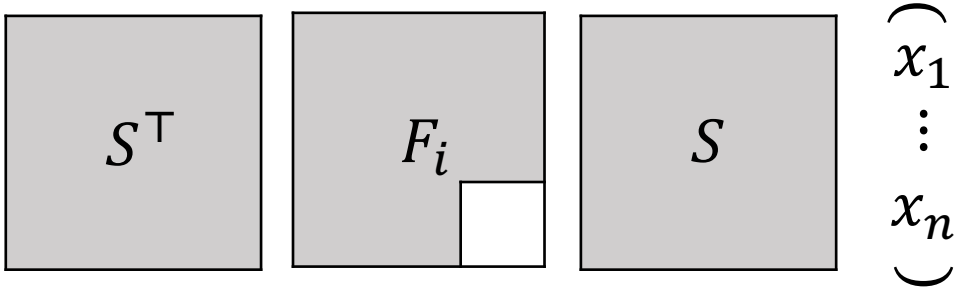
Representation Matrices

$\mathcal{F} = (f_1, \ldots, f_m), \quad \mathcal{P} = (p_1, \ldots, p_m)$

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

$\mathcal{S}(x) =$ 

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

$= (x_1 \cdots x_n)$ 

Outline

- Multivariate Public Key Cryptosystems
- UOV Signature Scheme
- Quotient Ring UOV (QR-UOV)
- Conclusion

Matrices of Quotient Ring

[Def] Polynomial Matrix Φ_g^f

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

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

$$\left(1, x, \ldots, x^{\ell-1}\right)\Phi_g^f = \left(g, xg, \ldots, x^{\ell-1}g\right)$$

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

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

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

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

Matrices of Quotient Ring

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

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

Secret key $S, F_i (i = 1, \ldots, m)$: block Φ_g^f matrix

$\Rightarrow$ Public key $P_i = S^\top F_i S \ (i = 1, \ldots, m)$: block Φ_g^f matrix?

$S^\top$ is not always block Φ_g^f

Matrices of Quotient Ring

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

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

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

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

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

$\boldsymbol{P_i}$ **: block** $\boldsymbol{W\Phi_g^f}$ **matrices**

Matrices of Quotient Ring

Proposition

- $f = x^{\ell} - ax^{i} - 1 \left(a \in \mathbb{F}_q, 1 \le i \le \ell - 1\right)$
- $W = \begin{pmatrix} J_i & 0_{i\times(\ell-i)} \\ 0_{(\ell-i)\times i} & J_{\ell-i} \end{pmatrix}$ ※ $J_{\ell} := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$

$\Rightarrow W\Phi_g^f$: symmetric

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

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

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

Block-Anti-Circulant UOV

[Szepieniec and Preneel, SAC 2019]

$$A_f := \{\Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} | g \in \mathbb{F}_q[x]/(f)\}$$

$A_{x^\ell-1}$: circulant matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix}$$

Block-Anti-Circulant UOV (BAC-UOV)

- By applying (anti) circulant matrix to the public and secret keys, it reduces the public key size.
- The attack utilizing the property of the circulant matrices was proposed. [Furue et al., PQCrypto2020]

Attack on BAC-UOV

(Anti-)Circulant Matrix ⇒

The sum of the elements of every row (column) has the same value.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Circulant Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{array}{|c|c|} \hline * & 0 \\ \hline 0 & * \\ \hline \end{array}$$

Transformation on Φ_g^f

Theorem

f : **Irreducible** polynomial

W : An invertible matrix that makes $W\Phi_g^f$ symmetric

$\Rightarrow$ For $\{W\Phi_g^f \mid g \in \mathbb{F}_q[x]/(f)\}$,

there is **no** $L \in \mathbb{F}_q^{\ell\times\ell}$ and $i, j \in \{1, \dots, \ell\}$ such that

$$\forall g \in \mathbb{F}_q[x]/(f), \quad \left(L^{\mathsf{T}}\left(W\Phi_g^f\right)L\right)_{ij} = 0.$$

※ If f is reducible, $W\Phi_g^f$ can be transformed.

[BAC-UOV] $(x^\ell - 1 = (x-1)(x^{\ell-1} + \cdots + 1))$

Quotient Ring UOV (QR-UOV)

Key Generation

① Irreducible polynomial: $f = x^{\ell} - ax^{i} - 1$

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

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

S : block Φ_g^f matrix

③ The representation matrices P_i $(i = 1, \ldots, m)$ for the public key is obtained by $P_i = S^{\top} F_i S$.

$\Rightarrow P_i$: Block $W\Phi_g^f$ Matrix

Quotient Ring UOV (QR-UOV)

$\Rightarrow P_i$: Block $W\Phi_g^f$ Matrix

$$\left(\begin{array}{ccc|ccc} 0 & 5 & 1 & 3 & 0 & 1 \\ 5 & 1 & 1 & 0 & 1 & 3 \\ 1 & 1 & 1 & 1 & 3 & 3 \\ \hline 6 & 5 & 6 & 0 & 5 & 4 \\ 5 & 6 & 3 & 5 & 4 & 1 \\ 6 & 3 & 2 & 4 & 1 & 3 \end{array}\right)$$

$(q = 7, f = x^3 - 3x - 1)$

This $n \times n$ matrix can be represented by n^2/ℓ elements.

(block size: $\ell \times \ell$)

Reduce the public key size

(We proposed parameters considering some transformations over $\mathbb{F}_q^\ell$)

Our Results

Security level	scheme	parameters	public key size (KB)	signature size (B)
I	Compressed Rainbow	$(q, v, o_1, o_2) = (16,36,32,32)$	57.4	66.0
	QR-UOV	$(q, v, m, \ell) = (7,189,72,3)$	**23.8**	**113.9**
III	Compressed Rainbow	$(q, v, o_1, o_2) = (256,68,32,48)$	252.3	164.0
	QR-UOV	$(q, v, m, \ell) = (7,291,111,3)$	**85.8**	**166.8**
V	Compressed Rainbow	$(q, v, o_1, o_2) = (256,96,36,64)$	511.2	212.0
	QR-UOV	$(q, v, m, \ell) = (7,411,162,3)$	**264.3**	**230.9**

Security of QR-UOV

The complexity ($\log_2(\#\text{gates})$) of the plain, pull-back, and lifting attacks on the proposed parameters of QR-UOV.

lv	model	plain				pull-back			lifting			
		dir	uov	rec	int	uov	rec	int	dir	uov	rec	int
I	cla	152	355	373	679	346	**149**	242	210	346	**149**	242
	quo	**91**	192	252	411	186	148	175	182	186	148	175
III	cla	224	534	555	1022	525	**214**	351	311	525	**214**	351
	quo	**140**	283	371	616	277	213	250	267	277	213	250
V	cla	317	730	768	1394	721	**279**	446	440	721	**279**	446
	quo	**205**	382	511	844	376	275	316	376	376	275	316

See Table 4 in the proceeding.

Outline

- Multivariate Public Key Cryptosystems
- UOV Signature Scheme
- Quotient Ring UOV (QR-UOV)
- Conclusion

Conclusion

Our contributions

- We proposed a new variant of UOV (QR-UOV) using polynomial matrix.
- QR-UOV reduces the public key size 50～70 % compared with Rainbow.

Future works

- Extend QR-UOV to a multilayer version of the “QR-Rainbow”
- Optimized implementations