An elementary construction of QR-UOV

Yasufumi Hashimoto *

Abstract

QR-UOV is a variant of UOV with smaller keys proposed at Asiacrypt 2021. In this paper, we show that QR-UOV can be constructed by a smaller UOV over an extension field.

Keywords. multivariate public-key cryptosystems, UOV, QR-UOV

1 Introduction

The unbalanced oil and vinegar signature scheme, UOV in short [14, 12, 11], is a signature scheme whose public key is a set of multivariate quadratic polynomials over a finite field. It has been considered that the original UOV is secure enough and its signature generation is efficient enough under suitable parameter selections. However, its key size is relatively large and then reducing key sizes of UOV has been an issue in this field. Until now, several variants of UOV with smaller keys have been proposed [16, 4, 17, 15, 1, 19, 18] although some of them have resulted in weakening the security [7, 10, 8, 13, 3, 9, 6]. QR-UOV [5] is also one of variants of UOV with smaller keys, inspired by the BAC-UOV [18, 6]. Its keys of QR-UOV are generated by companion matrices of an irreducible polynomial. This paper shows that the keys of QR-UOV can be constructed by the keys of a smaller UOV over an extension field. This result simplifies (future) discussions on QR-UOV; in fact, it shows that the problem of recovering an equivalent secret key of QR-UOV is equivalent to that of a smaller UOV over an extension field.

The following is the list of notations used in this paper.

Basic notations.

$\mathbf{F}_q$: a finite field of order q.
$\mathbf{F}_q^n$: the set of n-column vectors over $\mathbf{F}_q$.
$\mathbf{F}_q^{n\times m}$: the set of $n \times m$-matrices over $\mathbf{F}_q$.
$(a_{ij})_{1\leq i\leq n,1\leq j\leq m}$: the $n \times m$-matrix whose (i,j)-entry is a_{ij}.
$A^{(q)} := \left(a_{ij}^q\right)_{1\leq i\leq n,1\leq j\leq m}$ for $A = (a_{ij})_{1\leq i\leq n,1\leq j\leq m}$ and an integer q.
$A \otimes B := (a_{ij}B)_{i,j}$ for two matrices $A = (a_{ij})_{i,j}$ and B.
$A_1 \oplus \cdots \oplus A_k := \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{pmatrix}$ for square matrices (or scalars) $A_1, \ldots, A_k$.
$\mathrm{Tr}\alpha := \alpha + \alpha^q + \cdots + \alpha^{q^{l-1}} \in \mathbf{F}_q$ for an element $\alpha \in \mathbf{F}_{q^l}$ of an extension field $\mathbf{F}_{q^l}$ of $\mathbf{F}_q$.

*Department of Mathematical Science, University of the Ryukyus, hashimoto@math.u-ryukyu.ac.jp

2 UOV and QR-UOV

We first describe the original UOV [14, 11] and the original construction of QR-UVO [5].

2.1 UOV

Let $n, m, o, v \geq 1$ be integers with $v > 2o$, $o \geq m$, $n = o + v$. Define the quadratic map $F : \mathbf{F}_q^n \to \mathbf{F}_q^m$, $\mathbf{x} = {}^t(x_1, \ldots, x_n) \mapsto F(\mathbf{x}) = {}^t(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$ by

$$\begin{aligned} f_j(\mathbf{x}) &= \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+1}, \ldots, x_n) + (\text{quadratic form of } x_{o+1}, \ldots, x_n) \\ &= {}^t\mathbf{x} \begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix} \mathbf{x} + (\text{linear form}), \qquad (1 \leq j \leq m) \end{aligned}$$

where the coefficients of the polynomials above are elements of $\mathbf{F}_q$. The unbalanced oil and vinegar signature scheme (UOV) [14, 11] is constructed as follows.

Secret key. An invertible affine map $S : \mathbf{F}_q^n \to \mathbf{F}_q^n$ and the quadratic map F defined above.

Public key. The quadratic map $P := F \circ S : \mathbf{F}_q^n \to \mathbf{F}_q^m$.

Signature generation. For a message $\mathbf{m} = {}^t(m_1, \ldots, m_m) \in \mathbf{F}_q^m$ to be signed, choose $u_1, \ldots, u_v \in \mathbf{F}_q$ randomly, and find $(y_1, \ldots, y_o) \in \mathbf{F}_q^o$ with

$$f_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_1, \quad \ldots, \quad f_m(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_m. \tag{1}$$

Since the equations in (1) are linear, $(y_1, \ldots, y_o)$ is given efficiently. The signature for $\mathbf{m}$ is $\mathbf{z} := S^{-1t}(y_1, \ldots, y_o, u_1, \ldots, u_v)$.

Signature verification. The signature $\mathbf{z}$ is verified if $P(\mathbf{z}) = \mathbf{m}$ holds.

For most UOVs, S is taken to be $S(\mathbf{x}) = \begin{pmatrix} I_o & \\ * & I_v \end{pmatrix} \mathbf{x}$. We call the set of maps (S, F, P) above an $(\mathbf{F}_q; o, v, m)$-UOV map.

2.2 QR-UOV

Let $l, N, O, V, n, m \geq 1$ be integers with $n = lN$, $o = lO$, $v = lV$, $V > 2O$, $o \geq m$ and $g(x) = a_0 + a_1 x + \cdots + a_{l-1}x^{l-1} + x^l$ an irreducible polynomial of degree l over $\mathbf{F}_q$. For $h \in \mathbf{F}_q[x]/(g)$, define the matrix $\Phi_h^g \in \mathbf{F}_q^{l \times l}$ by $(1, x, \cdots, x^{l-1})\Phi_h^g = (h, xh, \cdots, x^{l-1}h)$ and set $A_g := \{\Phi_h^g \mid h \in \mathbf{F}_q[x]/(g)\}$. One can easily check that

$$A_g = \left\{ a_0 I_l + a_1 C + \cdots + a_{l-1} C^{l-1} \;\middle|\; a_0, a_1, \ldots, a_{l-1} \in \mathbf{F}_q \right\},$$

where $C = C^g := \Phi_x^g = \begin{pmatrix} & & -a_0 \\ 1 & & -a_1 \\ & \ddots & \vdots \\ & & 1 \; -a_{l-1} \end{pmatrix}$ is the companion matrix of $g(x)$. Choose a non-zero linear map $\phi : \mathbf{F}_q[x]/(g) \to \mathbf{F}_q$ and put $W := \left(\phi(x^{i+j-2})\right)_{1 \leq i,j \leq l}$. It is known that $W\Phi$ is symmetric for any $\Phi \in A_g$ (see Theorem 1 in [5]). For $1 \leq i \leq m$, and $0 \leq j \leq l-1$, let

$F_{ij} \in \mathbf{F}_q^{N\times N}$ be a symmetric matrix with $F_{ij} = \left(\begin{smallmatrix} 0_O & * \\ * & *_V \end{smallmatrix}\right)$, $S_j \in \mathbf{F}_q^{N\times N}$ a matrix with $S_j = \left(\begin{smallmatrix} I_O & \\ * & I_V \end{smallmatrix}\right)$ and

$$\begin{aligned} F_i :=& W \otimes F_{i0} + (WC) \otimes F_{i1} + \cdots + (WC^{l-1}) \otimes F_{i,l-1}, \\ S :=& I_l \otimes S_0 + C \otimes S_1 + \cdots + C^{l-1} \otimes S_{l-1}. \end{aligned}$$

Define the polynomials $f_i(\mathbf{x}), p_i(\mathbf{x})$ by $f_i(\mathbf{x}) := {}^t\mathbf{x}F_i\mathbf{x}$ and $p_i(\mathbf{x}) = f_i(S\mathbf{x})$ for $1 \le i \le m$, and the maps $F, P : \mathbf{F}_q^n \to \mathbf{F}_q^m$ by $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$, $P(\mathbf{x}) = (p_1(\mathbf{x}), \ldots, p_m(\mathbf{x}))$. Note that the polynomial $p_i(\mathbf{x})$ is written by

$$p_i(\mathbf{x}) = {}^t\mathbf{x}P_i\mathbf{x} = {}^t\mathbf{x}\left(W \otimes P_{i0} + (WC) \otimes P_{i1} + \cdots + (WC^{l-1}) \otimes P_{i,l-1}\right)\mathbf{x},$$

for some symmetric $P_{ij} \in \mathbf{F}_q^{N\times N}$. We then see that the set of maps (S, F, P) defined above is equivalent to an $(\mathbf{F}_q, o, v, m)$-UOV map. Such a variant of UOV is called QR-UOV.

3 An elementary construction of QR-UOV

In this section, we show that the maps S, F, P are described by a UOV map over an extension field. We first prepare the following lemma.

Lemma 3.1. *Let $\theta \in \mathbf{F}_{q^l}$ be a root of $g(x)$ and $\Theta := \left(\theta^{(j-1)q^{i-1}}\right)_{1\le i,j\le l}$. Then, for any $\Phi \in A_g$, there exist $\alpha, \beta \in \mathbf{F}_{q^l}$ such that*

$$\Theta\Phi\Theta^{-1} = \alpha \oplus \alpha^q \oplus \cdots \oplus \alpha^{q^{l-1}}, \tag{2}$$

$${}^t\Theta^{-1}(W\Phi)\Theta^{-1} = \beta \oplus \beta^q \oplus \cdots \oplus \beta^{q^{l-1}}. \tag{3}$$

Proof. Since $\Theta C\Theta^{-1} = \theta \oplus \theta^q \oplus \cdots \oplus \theta^{q^{l-1}}$, we can easily check that (2) holds for some $\alpha \in \mathbf{F}_{q^l}$. Next, fix $c_0, \ldots, c_{l-1} \in \mathbf{F}_q$ by

$${}^t(c_0, \ldots, c_{l-1}) = \left(\mathrm{Tr}(\theta^{i+j-2})\right)^{-1}_{1\le i,j\le l} {}^t\left(\phi(1), \phi(x), \ldots, \phi(x^{l-1})\right)$$

and put $\gamma := c_0 + c_1\theta + \cdots + c_{l-1}\theta^{l-1} \in \mathbf{F}_{q^l}$. Then γ satisfies

$${}^t\Theta\left(\gamma \oplus \gamma^q \oplus \cdots \oplus \gamma^{q^{l-1}}\right)\Theta = \left(\mathrm{Tr}\left(\gamma\theta^{i+j-2}\right)\right)_{1\le i,j\le l} = \left(\phi(x^{i+j-2})\right)_{1\le i,j\le l} = W, \tag{4}$$

since

$$\mathrm{Tr}(\gamma\theta^k) = c_0\mathrm{Tr}\left(\theta^k\right) + c_1\mathrm{Tr}\left(\theta^{k+1}\right) + \cdots + c_{l-1}\mathrm{Tr}\left(\theta^{k+l-1}\right) = \phi(x^k)$$

holds for $k \ge 0$. The equation (3) with $\beta = \gamma\alpha$ follows from (2) and (4) immediately. □

Let $X_i := x_i + x_{i+l}\theta + \cdots + x_{i+(l-1)N}\theta^{l-1}$ for $1 \le i \le N$, $X = {}^t(X_1, \ldots, X_N)$ and $\Theta_N := \Theta \otimes I_N$. It then holds $\Theta_N\mathbf{x} = {}^t\left({}^tX, {}^tX^{(q)}, \ldots, {}^tX^{(q^{l-1})}\right) =: \mathcal{X}$. Due to Lemma 3.1, we see that the

polynomials $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})$ in QR-UOV are written as follows.

$$\begin{aligned} f_i(\mathbf{x}) =& {}^t\mathbf{x}F_i\mathbf{x} = {}^t\mathcal{X}({}^t\Theta_N^{-1}F_i\Theta_N^{-1})\mathcal{X} \\ =& {}^t\mathcal{X}\left(({}^t\Theta^{-1}W\Theta^{-1}) \otimes F_{i0} + \cdots + ({}^t\Theta^{-1}WC^{l-1}\Theta^{-1}) \otimes F_{i,l-1}\right)\mathcal{X} \\ =& {}^t\mathcal{X}\left(\left(\gamma \oplus \cdots \oplus \gamma^{q^{l-1}}\right) \otimes F_{i0} + \cdots + \left(\gamma\theta^{l-1} \oplus \cdots \oplus (\gamma\theta^{l-1})^{q^{l-1}}\right) \otimes F_{i,l-1}\right)\mathcal{X} \\ =& {}^t\mathcal{X}\left(\mathcal{F}_i \oplus \mathcal{F}_i^{(q)} \oplus \cdots \oplus \mathcal{F}_i^{(q^{l-1})}\right)\mathcal{X} \\ =& {}^tX\mathcal{F}_iX + \left({}^tX\mathcal{F}_iX\right)^q + \cdots + \left({}^tX\mathcal{F}_iX\right)^{q^{l-1}} = \mathrm{Tr}\left(\mathcal{F}_i(X)\right), \end{aligned}$$

where

$$\mathcal{F}_i := \gamma F_{i0} + \gamma\theta F_{i1} + \cdots + \gamma\theta^{l-1}F_{i,l-1} = \begin{pmatrix} 0_O & * \\ * & *_V \end{pmatrix}$$

and $\mathcal{F}_i(X) := {}^tX\mathcal{F}_iX$. Similarly, we have

$$\begin{aligned} \Theta_N S\Theta_N^{-1} =& \mathcal{S} \oplus \mathcal{S}^{(q)} \oplus \cdots \mathcal{S}^{(q^{l-1})}, \\ p_i(\mathbf{x}) =& {}^t\mathcal{X}\left(\mathcal{P}_i \oplus \mathcal{P}_i^{(q)} \oplus \cdots \oplus \mathcal{P}_i^{(q^{l-1})}\right)\mathcal{X} \\ =& {}^tX\mathcal{P}_iX + \left({}^tX\mathcal{P}_iX\right)^q + \cdots + \left({}^tX\mathcal{P}_iX\right)^{q^{l-1}} = \mathrm{Tr}\left(\mathcal{P}_i(X)\right), \end{aligned}$$

where

$$\begin{aligned} \mathcal{S} :=& S_0 + \theta S_1 + \cdots + \theta^{l-1}S_{l-1}, \\ \mathcal{P}_i :=& \gamma P_{i0} + \gamma\theta P_{i1} + \cdots + \gamma\theta^{l-1}P_{i,l-1} \end{aligned}$$

and $\mathcal{P}_i(X) := {}^tX\mathcal{P}_iX$. Furthermore, since $p_i(\mathbf{x}) = f_i(S(\mathbf{x}))$, we see that

$$\begin{aligned} p_i(\mathbf{x}) =& {}^t(S\mathbf{x})F_i(S\mathbf{x}) = {}^t(\theta_N S\theta_N^{-1}\mathcal{X})\left({}^t\Theta_N^{-1}F_i\Theta_N^{-1}\right)(\theta_N S\theta_N^{-1}\mathcal{X}) \\ =& {}^t(\mathcal{S}X)\mathcal{F}_i(\mathcal{S}X) + \left({}^t(\mathcal{S}X)\mathcal{F}_i(\mathcal{S}X)\right)^q + \cdots + \left({}^t(\mathcal{S}X)\mathcal{F}_i(\mathcal{S}X)\right)^{q^{l-1}} = \mathrm{Tr}\left(\mathcal{F}_i(\mathcal{S}(X))\right). \end{aligned}$$

Thus we can construct QR-UOV as follows.

An elementary construction of QR-UOV.

Keys. Generate an $(\mathbf{F}_{q^l}; O, V, m)$-UOV map $(\mathcal{S}, \mathcal{F}, \mathcal{P})$. The secret key is $(\mathcal{S}, \mathcal{F})$ and the public key is $\mathcal{P}$.

Signature generation. For a message $\mathbf{m} = {}^t(m_1, \ldots, m_m) \in \mathbf{F}_q^m$ to be signed, choose $U_1, \ldots, U_V \in \mathbf{F}_{q^l}$ randomly, and find $Y = {}^t(Y_1, \ldots, Y_O) \in \mathbf{F}_{q^l}^O$ with

$$\mathrm{Tr}\left(\mathcal{F}_i(Y_1, \ldots, Y_O, U_1, \ldots, U_V)\right) = m_i$$

for $1 \le i \le m$. The signature for $\mathbf{m}$ is $Z := \mathcal{S}^{-1}{}^t(Y_1, \ldots, Y_O, U_1, \ldots, U_V) \in \mathbf{F}_{q^l}^N$.

Signature verification. The signature Z is verified if $\mathrm{Tr}(\mathcal{P}_i(Z)) = m_i$ holds for $1 \le i \le m$.

In the process of signature generation, one should solve a system of m equations in the form

$$\left(A, A^{(q)}, \cdots, A^{(q^{l-1})}\right) \begin{pmatrix} Y \\ Y^{(q)} \\ \vdots \\ Y^{(q^{l-1})} \end{pmatrix} = \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}$$

for some $A \in \mathbf{F}_{q^l}^{m \times O}$ and $e_1, \ldots, e_m \in \mathbf{F}_q$. While it seems a system of high degree polynomial equations of O variables over $\mathbf{F}_{q^l}$, it is equivalent to a system of m linear equations of $o(= Ol)$ variables over $\mathbf{F}_q$ since $\Theta_O^{-1\,t}\left({}^tY, {}^tY^{(q)}, \ldots, {}^tY^{(q^{l-1})}\right) \in \mathbf{F}_q^o$ and $\left(A, A^{(q)}, \cdots, A^{(q^{l-1})}\right)\Theta_O \in \mathbf{F}_q^{m \times o}$. Then, if $o \geq m$, one can (expect to) solve its system efficiently.

Acknowledgments. The author was supported by JST CREST no. JPMJCR2113 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

[1] W. Beullens, B. Preneel, A. Szepieniec and F. Vercauteren, LUOV, an MQ signature scheme, `https://www.esat.kuleuven.be/cosic/pqcrypto/luov/`.

[2] M.-S.Chen, J. Ding, M. Kannwischer, J. Patarin, A. Petzoldt, D. Schmidt and B.-Y. Yang, Rainbow Signature, `https://www.pqcrainbow.org/`.

[3] J. Ding, J. Deaton, K. Schmidt, Vishakha and Z. Zhang, Cryptanalysis of the lifted unbalanced oil vinegar signature scheme, CRYPTO'20, LNCS **12172** (2020), 279–278.

[4] D.H. Duong, A. Petzoldt, Y. Wang and T. Takagi, Revisiting the cubic UOV signature scheme, ICISC'16, LNCS **10157** (2016), 223–238.

[5] H. Furue, Y. Ikematsu, Y. Kiyomura, T. Takagi, A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV, Asiacrypt'21, LNCS **13093** (2021), 187–217.

[6] H. Furue, K. Kinjo, Y. Ikematsu, Y. Wang, T. Takagi, A structural attack on block-anti-circulant UOV at SAC 2019, PQCrypto'20, LNCS **12100** (2020), 323–339.

[7] Y. Hashimoto, Weaknesses of cubic UOV and its variants, Ryukyu Math. J., **30** (2017), 1–7.

[8] Y. Hashimoto, Key recovery attack on Circulant UOV/Rainbow, JSIAM Lett., **11** (2019), 45–48.

[9] Y. Hashimoto, Key recovery attack on Hufu-UOV, JSIAM Lett., **14** (2022), 1–4.

[10] Y. Hashimoto, Y. Ikematsu and T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacrypt 2017, IWSEC'18, LNCS **11049** (2018), 3–18.

[11] A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), 206–222, extended in `http://www.goubin.fr/papers/OILLONG.PDF`.

[12] A. Kipnis and A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto'98, LNCS **1462** (1998), 257–267.

[13] K. Mus, S. Islam and B. Sunar, QuantumHammer: A practical hybrid attack on the LUOV signature scheme, Proc. of CCS'20 (2020), 1071–1084.

[14] J. Patarin, The Oil and Vinegar Signature Scheme, the Dagstuhl Workshop on Cryptography, 1997.

[15] Z. Peng and S. Tang, Circulant UOV: a new UOV variant with shorter private key and faster signature generation, KSII T. Internet Info., **12** (2018), 1376-1395.

[16] A. Petzoldt, S. Bulygin and J. A. Buchmann, CyclicRainbow - A multivariate signature scheme with a partially cyclic public key, Indocrypt'10, LNCS **6498** (2010), 33–48.

[17] K.-A. Shim, C.-M. Park and N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, Asiacrypt'17, LNCS **10624** (2017), 37–64.

[18] A. Szepieniec, B. Preneel, Block-anti-circulant unbalanced oil and vinegar, SAC'19, LNCS **11959** (2019), 574–588.

[19] C. Tao, A Method to Reduce the Key Size of UOV Signature Scheme, `https://eprint.iacr.org/2019/473`.