Key recovery attack on Hufu-UOV

Yasufumi Hashimoto\(^1\)*

\(^1\)Department of Mathematical Science, University of the Ryukyus, 1 Senbaru, Nishihara-cho, Okinawa 903-0213, Japan
*Corresponding author: hashimoto@math.u-ryukyu.ac.jp

Received October 21, 2021, Accepted November 10, 2021

Abstract

The unbalanced oil and vinegar signature scheme (UOV) is a signature scheme whose public key is a set of quadratic polynomials over a finite field. This scheme has been considered to be secure and efficient enough under suitable parameter selections. However, its key size is relatively large, and then various arrangements of UOV with smaller keys have been proposed. Hufu-UOV proposed by Tao in 2019 is one of such variants of UOV, whose keys are generated by circulant and Toeplitz matrices. In the present paper, we study the security of Hufu-UOV and propose an attack on it.

Keywords multivariate public-key cryptosystems, UOV, Hufu-UOV

1. Introduction

UOV, the unbalanced oil and vinegar signature scheme [1, 2], is a signature scheme whose public key is a set of multivariate quadratic polynomials over a finite field. This signature scheme has been highly regarded since the original UOV has been secure enough against known attacks in this two decades and the signature generation of UOV is efficient enough under suitable parameter selections. In fact, UOV [3], a variant of UOV, was selected as a second round candidate and Rainbow [4], a multi-layer UOV, is a finalist of NIST’s Post-Quantum Cryptography Standardization Program [5]. On the other hand, UOV has the disadvantage that the sizes of secret and public keys are relatively large, and then reducing key sizes of UOV is one of the most important issues in multivariate cryptography. Until now, there have been various arrangements of UOV (and Rainbow) with smaller keys, e.g. [3, 6–9]. Unfortunately, some of them are much less secure than expected, since the special structures in these arrangements for reducing the keys yield vulnerabilities [10–14].

Hufu-UOV [15] proposed by Tao at 2019 is one of such variants of UOV with smaller keys. In this scheme, the quadratic polynomials in the secret and public keys are generated by circulant matrices and Toeplitz matrices. However, its vulnerability is included in the “Toeplitz” and “circulant” structures. In the present paper, we propose an attack on Hufu-UOV and reduce its security drastically.

2. UOV

We first describe the original unbalanced oil and vinegar signature scheme (UOV) [1, 2].

2.1 Basic construction

Let \( n, o, v \geq 1 \) be integers with \( v \geq o \), \( n = o + v \), \( q \) be a power of prime and \( \mathbb{F}_q \) a finite field of order \( q \). Define the quadratic polynomials \( g_1(x), \ldots, g_o(x) \) of \( x = t(x_1, \ldots, x_n) \) by

\[
g_l(x) = \sum_{1 \leq i \leq o} x_i \cdot (\text{linear form of } x_{o+i}, \ldots, x_n)
\]

\[
+ (\text{quadratic form of } x_{o+i}, \ldots, x_n)
\]

\[
= t\left(\begin{array}{c}
0 \\
* \\
* \\
* \\
* \\
* \\
\end{array}\right)x + (\text{linear form}),
\]

for \( 1 \leq l \leq o \), where the coefficients of the polynomials above are elements of \( \mathbb{F}_q \), and the map \( G : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^o \) by \( G(x) = t(g_1(x), \ldots, g_o(x)) \). Then the unbalanced oil and vinegar signature scheme (UOV) [2] is constructed as follows.

Secret Key. An invertible affine map \( S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \) and the quadratic map \( G \) defined above.

Public key. The quadratic map \( F := G \circ S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^o \).

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

\[
g_1(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_1,
\]

\[
\vdots
\]

\[
g_o(y_1, \ldots, y_o, u_1, \ldots, u_v) = m_o.
\]

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

Signature verification. The signature \( z \) is verified if \( F(z) = m \) holds.

2.2 Security

We now give a short survey on the security of UOV.

1. Key recovery. It is easy to see that, if

\[
S(x) = \left(\begin{array}{c}
o \\
0 \\
* \\
* \\
* \\
* \\
\end{array}\right)x + (\text{const.}),
\]

\[
F(x) = \left(\begin{array}{c}
o \\
0 \\
* \\
* \\
* \\
* \\
\end{array}\right)x + (\text{line}),
\]

then $x \in \mathbb{F}_q^n$ and \( y \in \mathbb{F}_q^o \) are recovered. The problem is how to find $x$ and $y$.
one can generate dummy signatures easily, since
\[ f_l(x) = g_l(S(x)) = \frac{1}{x} \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} x + \text{(linear form)} \]
for \( 1 \leq l \leq o \). This means that recovering an invertible linear map \( S_1 : F_q^n \rightarrow F_q^n \) with
\[
(S \circ S_1)(x) = \frac{1}{x} \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} x + \text{(const.)}
\]
is enough to break UOV.

The most famous attack is to recover such an \( S_1 \) is Kipnis-Shamir's attack [1]. This attack is available for \( o \geq v \) and can recover \( S_1 \) in polynomial time. It is generalized in [2] to be available for \( v > o \) with the complexity \( O(q^{\max(0,v-o)})(\text{polyn.}) \). Thus, on UOV and its variants, \( o, v \) are usually taken \( v \gg 2o \).

2. Direct attacks. The direct attack is to generate a dummy signature by solving the system of \( o \) quadratic equations
\[ f_1(x) = m_1, \ldots, f_o(x) = m_o \quad (2) \]
of \( n \) variables directly. The most standard approach to solve (2) is by using the hybrid approach [16] of the Gröbner basis algorithm and the exhaustive search. Fix a small integer \( k \), choose \( u_1, \ldots, u_{v+k} \in F_q \) randomly and solve the system of \( o \) quadratic equations
\[ f_1(x_1, \ldots, x_{o-k}, u_1, \ldots, u_{v+k}) = m_1, \]
\[ \vdots \]
\[ f_o(x_1, \ldots, x_{o-k}, u_1, \ldots, u_{v+k}) = m_o \quad \text{(3)} \]
of \( o-k \) variables by the Gröbner basis algorithm. If solutions of (3) do not exist, change \( u_1, \ldots, u_{v+k} \) and try to solve (3) again. Its complexity is estimated by \( O(q^{k(o-k+d_{\text{reg}}(k))}w) \), where \( 2 \leq w < 3 \) is the exponent of the Gaussian elimination and \( d_{\text{reg}}(k) \) is the “degree of regularity” of the system (3) [17].

Note that, when the number \( n \) of variables is much larger than the number \( o \) of equations, one can transform the system (2) of equations to a smaller system of equations [18,19]. For example, if \( n > o \alpha \) with small \( \alpha > 1 \), one can transform (2) to a system of \( o - \lfloor \alpha \rfloor + 1 \) quadratic equations of \( o - \lfloor \alpha \rfloor + 1 \) variables. Especially, it is known that (2) can be solved in polynomial time if \( n \geq \frac{1}{2}o(o+1) \) [19,20].

3. Hufu-UOV

Hufu-UOV [15] is a variant of UOV, whose quadratic polynomials are constructed by circulant matrices and Toeplitz matrices respectively given in the following forms.
\[
\begin{pmatrix}
  a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\
  a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\
  \vdots & \ddots & \ddots & \ddots & \ddots \\
  a_2 & a_3 & \cdots & a_0 & a_1 \\
  a_1 & a_2 & \cdots & a_{n-1} & a_0 \\
\end{pmatrix}
\]
We call the matrices above by the \( n \)-circulant and the \( n \)-Toeplitz matrices respectively.

Define the quadratic map \( G(x) = (g_1(x), \ldots, g_o(x)) \) and the invertible linear map \( S : F_q^n \rightarrow F_q^n \) by
\[
g_l(x) = x \begin{pmatrix} \lambda_1 & \cdots & \lambda_o \\
 U_1 & \cdots & U_o \\
 W_1 & \cdots & W_o \\
\end{pmatrix} x \quad (1 \leq l \leq o),
\]
where \( \lambda_1, \ldots, \lambda_o \in F_q \) are scalars, \( A \) is an \( o \)-Toeplitz matrix, \( W_1, \ldots, W_o \) are \( v \)-circulant matrices and \( M, U_1, \ldots, U_o \) are \( v \times o \) matrices generated by the first \( o \) columns of \( v \)-circulant matrices. Note that \( A \) and \( W_1 \) can be taken to be symmetric. Then the Hufu-UOV is constructed as follows.

Secret Key. The invertible linear map \( S \), the quadratic map \( G \) defined above and an invertible affine map \( T : F_q^n \rightarrow F_q^n \).

Public key. The quadratic map \( F := T \circ G \circ S : F_q^n \rightarrow F_q^n \).

Signature generation. If \( A = 0 \), it is same as the original UOV. If \( A \neq 0 \), signatures are generated as follows. For a message \( m \in E_q^n \) to be signed, compute \( z = (z_1, \ldots, z_o) := T^{-1}(m) \). Choose \( u_1, \ldots, u_o \in F_q \) randomly, and find \( (y_1, \ldots, y_o) \in F_q^n \) with
\[
g_1(y_1, \ldots, y_o, u_1, \ldots, u_o) = z_1, 
\]
\[
g_2(y_1, \ldots, u_o) = \lambda_2 \lambda_1^{-1} g_1(y_1, \ldots, u_o) = z_2 - \lambda_2 \lambda_1^{-1} z_1, 
\]
\[
\vdots 
\]
\[
g_o(y_1, \ldots, u_o) = \lambda_o \lambda_1^{-1} g_1(y_1, \ldots, u_o) = z_o - \lambda_o \lambda_1^{-1} z_1. 
\]
Since the first equation in (4) is quadratic and the later \( o-1 \) equations are linear, one can find \( (y_1, \ldots, y_o) \) efficiently. The signature for \( m \) is \( s := S^{-1}(y_1, \ldots, y_o, u_1, \ldots, u_o) \).

Signature verification. The signature \( s \) is verified if \( F(s) = m \) holds.

Let \( f_1(x), \ldots, f_o(x), \bar{g}_1(x), \ldots, \bar{g}_o(x) \) be the quadratic polynomials with \( F(x) = (f_1(x), \ldots, f_o(x)) \) and \( (T \circ G)(x) = (\bar{g}_1(x), \ldots, \bar{g}_o(x)) \). We see that, similarly to \( g_l(x) \), the polynomials \( f_l(x), \bar{g}_l(x) \) (1 \( \leq l \leq o \)) are written by
\[
f_l(x) = x \begin{pmatrix} A_l & B_l \\
 V_l & U_l \\
 W_l & W_l \\
\end{pmatrix} x, \quad \bar{g}_l(x) = x \begin{pmatrix} V_l & U_l \\
 W_l & W_l \\
\end{pmatrix} x 
\]
for \( o \times o \) symmetric matrices \( A_l, V_l, v \times o \) matrices \( B_l, U_l \) and \( v \times v \) symmetric matrices \( C_l, W_l \).
4. Proposed attack

By the definition of $T$ and $G$, we see that there exist $\mu_1, \ldots, \mu_o \in \mathbb{F}_q$ such that $V_i = \mu_i A$. Since

$$f_1(S^{-1}(x)) = \bar{y}_i(x),$$

we have

$$A_1 - B_1 M - M B_1 + M C_1 M = \mu_1 A,$$

$$B_1 - C_1 M = \bar{U}_1, \quad C_1 = W_i. \tag{5}$$

Recall that $M, \bar{U}_1, \mu, A$ are secret and $A_1, B_1, C_1$ are public. Furthermore, note that $A_1$ is an $o \times o$ symmetric Toeplitz matrix, $C_1$ is a $v \times v$ symmetric circulant matrix and $B_1$ is the first $o$ column of a $v \times v$ circulant matrix. It is easy to see that there exist $v \times v$ circulant matrices $A^c, A_1^c, B_1^c, M^c$ such that

$$A = (I_o, 0_{v, o})A^c \left( I_o \begin{array}{c} 0 \end{array} \right), \quad A_l = (I_o, 0_{v, o})A_l^c \left( I_o \begin{array}{c} 0 \end{array} \right),$$

$$B_l = B_l^c \left( I_o \begin{array}{c} 0 \end{array} \right), \quad M = M^c \left( I_o \begin{array}{c} 0 \end{array} \right),$$

where $0_{v, o}$ is the $o \times v$ zero matrix. For example, when $o = 2, v = 5$ and

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 3 & 2 \\ 1 & 3 \\ 1 & 1 \\ 0 & 1 \\ 2 & 0 \end{pmatrix},$$

the 5-circulant matrices $A^c, M^c$ are given by

$$A^c = \begin{pmatrix} 1 & 2 & y & y & 2 \\ 2 & 1 & 2 & y & y \\ y & 2 & 1 & 2 & y \\ y & y & 2 & 1 & 2 \\ 2 & y & 2 & 1 \end{pmatrix},$$

$$M^c = \begin{pmatrix} 3 & 2 & 0 & 1 & 1 \\ 1 & 3 & 2 & 0 & 1 \\ 1 & 1 & 3 & 2 & 0 \\ 0 & 1 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 & 3 \end{pmatrix},$$

for some $y \in \mathbb{F}_q$. Remark that $A^c$ cannot be fixed uniquely when $v \geq 2o$ and we remain such unfixed parameters to be unknown. Since $A^c$ is symmetric and $v$-circulant, we see that the number of unknowns in $A^c$ is $\lceil (v + 1)/2 \rceil = o$.

The first equation of (5) is rewritten by

$$t M^c C_1 M^c - t B_1^c M^c - M^c B_1^c + A_1^c = \mu_1 A^c. \tag{6}$$

Since the multiplication between circulant matrices is commutative, we have

$$C_1^t M^c M^c - t B_1^c M^c - B_1^c M^c + A_1^c = \mu_1 A^c \tag{6}$$

for $1 \leq l \leq o$. We will study how to recover $M^c$ from the matrix equation (6).

4.1 The case $A \neq 0$

We first study the case $A = 0$ for simplicity. Let

$$H_l := C_1^t M^c M^c - t B_1^c M^c - B_1^c M^c + A_1^c,$$

for $1 \leq l \leq o$ and

$$H_l := C_1 H_l - C_1 H_1$$

for $2 \leq l \leq o$. It is easy to see that the matrix $H_l$ is a symmetric $v$-circulant matrix and the unknowns in (7) are included in $A_1^c, M^c$ linearly. Then the matrix equations

$$H_2 = 0, \ldots, H_K = 0$$

yield a system of $(K - 1)((v + 1)/2)$ linear equations of $v + K \lceil (v + 1)/2 \rceil - o$ unknowns. Since the number of unknowns is larger than that of linear equations when $K \geq (3v + 1)/2o$, we can expect that one can solve its system and can recover the secret key $M^c$. Table 1 gives experimental results to recover $M^c$ for the parameter selection in [15] by Magma ver.2.24-5 under macOS Mojave ver.10.14.16, Intel Core i5, 3 GHz. Note that “Security” is the security expected by Tao [15], and “Attack” is the computational times (in seconds) of our attack to recover $M^c$. This table shows that our attack can recover the secret key quite effectively.

4.2 The case $A \neq 0$

Let

$$H_l := C_1 t M^c M^c - t B_1^c M^c - B_1^c M^c + A_1^c - \mu_1 A^c$$

for $1 \leq l \leq o$, and

$$H_l(\delta_1, \delta_2) := (C_2 - \delta_2 C_1)H_l - (C_1 - \delta_1 C_1)H_2 + (\delta_2 C_1 - \delta_1 C_2)H_1$$

(4)

$$= ((C_1 t B_1^c - C_1 t B_1^c) + \delta_2(C_1 t B_1^c - C_1 t B_1^c) + \delta_1(C_1 t B_1^c - C_1 t B_1^c)) M^c + (C_2 B_1^c - C_2 B_1^c) M^c + (C_2 B_1^c - C_2 B_1^c) M^c + (C_2 B_1^c - C_2 B_1^c) M^c$$

for $2 \leq l \leq o$. It is easy to see that the matrix $H_l$ is a symmetric $v$-circulant matrix and the unknowns in (7) are included in $A_1^c, M^c$ linearly. Then the matrix equations

$$H_2 = 0, \ldots, H_K = 0$$

yield a system of $(K - 1)((v + 1)/2)$ linear equations of $v + K \lceil (v + 1)/2 \rceil - o$ unknowns. Since the number of unknowns is larger than that of linear equations when $K \geq (3v + 1)/2o$, we can expect that one can solve its system and can recover the secret key $M^c$. Table 1 gives experimental results to recover $M^c$ for the parameter selection in [15] by Magma ver.2.24-5 under macOS Mojave ver.10.14.16, Intel Core i5, 3 GHz. Note that “Security” is the security expected by Tao [15], and “Attack” is the computational times (in seconds) of our attack to recover $M^c$. This table shows that our attack can recover the secret key quite effectively.

Table 1. Experiments of the proposed attack on Hufu-UOV.

| $(q, o, v)$ | Security | Attack |
|-----------|----------|--------|
| (16,64,192) | 128 bits | 48s. |
| (16,96,288) | 192 bits | 245s. |
| (16,128,384) | 256 bits | 757s. |
| (256,48,144) | 128 bits | 19s. |
| (256,64,192) | 128 bits | 59s. |
| (256,80,240) | 256 bits | 137s. |
for \( 3 \leq l \leq o \) and \( \delta_l \in \mathbb{F}_q \). It is easy to see that, if \( \delta_2 = \mu_1^{-1}\mu_2, \delta_l = \mu_1^{-1}\mu_l \), the matrix equation
\[
H_1(\delta_1, \delta_2) = 0
\]
generates a system of linear equations of unknowns in \( M^c, A_1^c, A_2^c, A_1 \). Since the numbers of linear equations derived from
\[
H_3(\delta_3, \delta_2) = 0, \ldots, H_K(\delta_K, \delta_2) = 0
\]
and their unknowns are respectively \([(v+1)/2](K-2)\) and \( v + (\lfloor (v+1)/2 \rfloor - \alpha)K \), we can recover \( M \) by solving its system of linear equations if \( K \geq (2v+1)/o \) and \( \delta_2, \ldots, \delta_K \) are chosen correctly. Thus the following attack is available on Hufu-UOV.

Step 1. Choose \( \delta_2, \ldots, \delta_K \in \mathbb{F}_q \) randomly.

Step 2. Solve the system of linear equations derived from
\[
H_3(\delta_3, \delta_2) = 0, \ldots, H_K(\delta_K, \delta_2) = 0.
\]
If there exists a solution, fix \( M \) by its solution. If not, go back to Step 1 and choose another \( (\delta_2, \ldots, \delta_K) \).

Step 3. If the quadratic forms of \( x_1, \ldots, x_o \) in
\[
f_2 \left( \begin{pmatrix} I_o & I_v \end{pmatrix} x \right), \ldots, f_m \left( \begin{pmatrix} I_o & I_v \end{pmatrix} x \right)
\]
are constant multiples of the quadratic form of \( x_1, \ldots, x_o \) in
\[
f_1 \left( \begin{pmatrix} I_o & I_v \end{pmatrix} x \right),
\]
output \( M \) as the correct secret key. If not, return to Step 1 and change \( \delta_2, \ldots, \delta_K \).

Since the number of candidates of \( (\delta_2, \ldots, \delta_K) \) are \( q^{K-1} = q^{\lfloor (2v+1)/o \rfloor - 1} \), the complexity of this attack is \( O(q^{\lfloor (2v+1)/o \rfloor - 1}) \). (polyn.). It is much less than the complexities of the Kipnis-Shamir’s attack and the direct attack on the original UOV.

5. Conclusion

While the structure of Hufu-UOV using circulant and Toeplitz matrices reduces the key size of UOV, it weakens the security. One should be careful not to weaken the security when he/she tries to improve the efficiency.

Acknowledgments

The author would like to thank the anonymous reviewer(s) for reading the previous draft carefully and giving helpful comments. He was supported by JST CREST no. JPMJCR2113 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

[1] A. Kipnis and A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in: Proc. of CRYPTO 1998, H. Krawczyk ed., LNCS Vol. 1462, pp. 257–267, Springer, Heidelberg, 1998.

[2] A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, in: Proc. of EUROCRYPT 1999, J. Stern ed., LNCS Vol. 1592, pp. 206–222, Springer, Heidelberg, 1999, extended in http://www.goubin.fr/papers/OILLONG.PDF (accessed 18 Oct. 2021).

[3] W. Beullens, B. Preneel, A. Selpenieie and F. Vercauteren, LUOV: an MQ signature scheme, https://www.essential.eu/cosic/pqcrypto/luov/ (accessed 18 Oct. 2021).

[4] M.-S. Chen, J. Ding, M. Kannwischer, J. Patarin, A. Petzoldt, D. Schmidt and B.-Y. Yang, Rainbow Signature, https://www.pqcrypto.org/ (accessed 18 Oct. 2021).

[5] NIST, Post-Quantum Cryptography. Round 3 submissions, https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed 18 Oct. 2021).

[6] A. Petzoldt, S. Bulygin and J. A. Buchmann, CyclicRainbow – A multivariate signature scheme with a partially cyclic public key, in: Proc. of INDOCRYPT 2010, G. Gong and K. C. Gupta eds., LNCS Vol. 6498, pp. 33–48, Springer, Heidelberg, 2010.

[7] D. H. Duong, A. Petzoldt, Y. Wang and T. Takagi, Revisiting the cubic UOV signature scheme, in: Proc. of ICISC 2016, S. Hong and J. H. Park eds., LNCS Vol. 10157, pp. 223–238, Springer, Cham, 2016

[8] K.-A. Shim, C.-M. Park and N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, in: Proc. of ASIACRYPT 2017, T. Takagi and T. Peyrin eds., LNCS Vol. 10624, pp. 37–64, Springer, Cham, 2017.

[9] Z. Peng and S. Tang, Circulant UOV: A new UOV variant with shorter private key and faster signature generation, KSII Trans. Internet Inf. Syst., 12 (2018), 1376–1395.

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

[11] Y. Hashimoto, Y. Ikematsu and T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacrypt 2017, in: Proc. of IWSEC 2018, A. Inomata and K. Yasuda eds., LNCS Vol. 11049, pp. 9–18, Springer, Cham, 2018.

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

[13] K. Mus, S. Islam and B. Sunar, QuantumHammer: A practical hybrid attack on the UOV signature scheme, in: Proc. of CCS’20, pp. 1071–1084, 2020.

[14] J. Ding, J. Deaton, K. Schmidt, Vishakha and Z. Zhang, Cryptanalysis of the lifted unbalanced oil vinegar signature scheme, in: Proc. of CRYPTO 2020, D. Micciancio and T. Ristenpart eds., LNCS Vol. 12172, pp. 279–287, Springer, Cham, 2020.

[15] C. Tao, A Method to Reduce the Key Size of UOV Signature Scheme, https://sprint.iacr.org/2019/473 (accessed 18 Oct. 2021).

[16] L. Bettale, J. C. Faugère and L. Perret, Solving polynomial systems over finite fields: Improved analysis of the hybrid approach, in: Proc of ISSAC’12, pp. 67–74, 2012.

[17] M. Bardet, J. C. Faugère, B. Salvy and B. Y. Yang, Asymptotic expansion of the degree of regularity for semi-regular systems of equations, in: Proc of MEGA’05, pp. 1–14, 2005.

[18] E. Thomae and C. Wolf, Solving underdetermined systems of multivariate quadratic equations revisited, in: Proc of PKC 2012, M. Fischlin et al. eds., LNCS Vol. 7293, pp. 156–171, Springer, Heidelberg, 2012.

[19] C.-M. Cheng, Y. Hashimoto, H. Miura and T. Takagi, A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics, in: Proc. of PQCRYPTO 2014, M. Mosca ed., LNCS Vol. 8772, pp. 40–58, Springer, Cham, 2014.

[20] H. Miura, Y. Hashimoto and T. Takagi, Extended algorithm for solving underdefined multivariate quadratic equations, in: Proc. of PQCRYPTO 2013, P. Gaboori ed., LNCS Vol. 7932, pp. 118–135, Springer, Heidelberg, 2013.