IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 28, 2019, accepted January 16, 2020, date of publication January 31, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970608

An Efficient MQ-Signature Scheme Based on Sparse Polynomials

KYUNG-AH SHIM[1], CHEOL-MIN PARK[1], AND NAMHUN KOO[2]
[1]National Institute for Mathematical Sciences, Daejeon 34047, South Korea
[2]Applied Algebra and Optimization Research Center, Sungkyunkwan University, Seoul 16419, South Korea

Corresponding author: Kyung-Ah Shim (kashim@nims.re.kr)

This work was supported by the National Institute for Mathematical Sciences through the Ministry of Science and ICT of Korea under Grant B20720000.

ABSTRACT Multivariate quadratic (MQ) equations-based cryptography is one of the most promising alternatives for currently used public-key cryptographic algorithms in the post-quantum era. It is important to design practical public-key signature schemes on embedded processors and resource-constrained devices for emerging applications in Internet of Things. The MQ-signature schemes are suitable for low-cost constrained devices since they require only modest computational resources. In this paper, we propose an efficient MQ-signature scheme, SOV, using sparse polynomials with a shorter secret key and give its security analysis against known algebraic attacks. Compared to Rainbow, the secret key of SOV has reduced by a factor of 90% without increasing the public key size. In particular, SOV requires signatures of 52 bytes, while ECDSA-256 requires signatures of 64 bytes.

INDEX TERMS Equivalent key, good key, isomorphism of polynomials problem, key recovery attack, multivariate-quadratic problem, sparse polynomial.

I. INTRODUCTION

It is known that if a large scale quantum computer capable of implementing Shor's algorithm [41] is developed then the discrete logarithm problem (DLP) and the integer factorization problem (IFP) are solved in polynomial time. Thus, currently used public-key cryptographic algorithms based on the these problems such as RSA, DSA and ECDSA could be broken by the quantum computer. There are public-key cryptographic algorithms believed to remain secure against a quantum computer: lattice-based, code-based, hash-based, multivariate quadratic (MQ) equations-based and supersingular Isogeny-based. Although they have been resist classical and quantum cryptanalysis, most of them suffer from large key sizes, signature sizes and/or slow performance compared to the currently used public-key cryptographic algorithms. Recently, NIST have initiated Post-Quantum Cryptography Standardization for public-key encryption, key exchange and digital signature.

Multivariate quadratic (MQ) equations-based cryptography relies on the intractability of solving large multivariate quadratic systems called the MQ-problem. The MQ-problem is proven to be NP-hard even for quadratic polynomials defined over $\mathbb{F}_2$. To build an MQ-scheme, one has to find an easily invertible quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The selection of candidates for the quadratic map $\mathcal{F}$ with a special structure is a basic idea for constructing the MQ-schemes. The MQ-schemes requires an additional structure to hide a trapdoor, called the affine-substitute-affine (ASA) structure: it needs two invertible affine maps $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to destroy the special structure of $\mathcal{F}$. Then a public key is given by $\mathcal{P} = S \circ \mathcal{F} \circ T$ and a secret key is $(S, \mathcal{F}, T)$ that allows to invert the public key. This ASA structure is related to some variants of the Isomorphism of Polynomials (IP) problem [34].

Since Imai and Matsumoto [33] introduced the first MQ-encryption scheme, a number of MQ-schemes have been proposed. MQ-schemes are suitable for low-cost constrained devices like smart cards [8], [11] since they require simple operations on matrices and vectors in small fields without multiple-precision arithmetic. Due to the special structure related to the IP problem, most of the MQ-schemes were broken remaining few schemes including variants of Unbalanced Oil-and-Vinegar (UOV) [17], [30] and HFEv- [35], [38]. Despite advantages of fast performance and short signature, the MQ-signature schemes using the ASA structure

The associate editor coordinating the review of this manuscript and approving it for publication was Kaigui Bian.

suffer from large key sizes. There is the Fiat-Shamir type MQ-signature scheme converted from Sakumoto *et al.*'s identification scheme [39] using the Fiat-Shamir transform. The resulting scheme, MQDSS [2], [12], has a security reduction to a random instance of the MQ-problem and short key sizes, but lose the advantages of the MQ-schemes, short signature size and fast performance.

Due to emerging applications in Internet of Things (IoTs), more than 98 % of all microprocessors sold worldwide are used in embedded devices and will continue to increase. Thus, it is important to design practical public-key schemes suitable for embedded processors and resource-constrained IoT devices. In terms of efficiency, it is known that the MQ-signature schemes using the ASA structure are superior to others. At CHES 2012, Czypek *et al.* [16] demonstrated feasibility of MQ-signature schemes on 8-bit AVR microprocessor. It is shown that the signing speed of Rainbow and enTTS outperform RSA and ECDSA.

In the MQ-schemes, there is still room for improvements in key sizes, signature size and performance depending on the selection of central maps. For constrained devices, the faster the better, and the shorter the better. There are several proposals for constructing MQ-signature schemes with shorter key size and higher performance for practical purposes. Gligoroski *et al.* [27] presented a new signature scheme, MQQ-SIG, using multivariate quadratic quasigroups. They succeeded in reducing the secret key and improving signing performance significantly, but required a larger public key. It was broken by polynomial-time key-recovery attacks by Faugère *et al.* [22] at PKC 2015. TTS [14], [15] and enhanced TTS (enTTS) [44], [45] used sparse polynomials to reduce the secret key and signing cost, but had lager public key than other MQ-schemes. In this paper, we propose an efficient MQ-signature scheme with a shorter secret key and signatures maintaining the public key size. Our scheme is suitable for specific applications where the existing signature schemes cannot be used due to their slow performance and large signature size.

Our Contributions. We propose an efficient MQ-signature scheme, SOV, based on sparse polynomials.

- **An Efficient MQ-Signature Scheme.** Our central map uses sparse polynomials for reducing the secret key size and signing cost without increasing the public key size.
- **Shorter Secret Key Size and the Shortest Signature Size.** Compared to Rainbow, the secret key of SOV has reduced by a factor of 90% without increasing the public key. In particular, the signature size of SOV is the shortest among pre-quantum schemes and post-quantum schemes: SOV requires signatures of 52 bytes, while ECDSA-256 requires signatures of 64 bytes.

The rest of the paper is composed as follows. In Section II, we construct an efficient MQ-signature scheme, SOV, using sparse polynomials. In Section III, we give security analysis of SOV against known algebraic attacks and compare our scheme to existing signature schemes in Section IV. We conclude this paper in Section V.

II. A NEW EFFICIENT MQ-SIGNATURE SCHEME

Original TTS was proposed in [14] and later refined in [15]. Afterwards, Yang and Chen [44], [45] revealed some weaknesses of TTS against the MinRank attack and the High-Rank attack and then proposed the Enhanced TTS (enTTS). enTTS based on sparse polynomials reduces the secret key size and its signing cost, but its public key is about 2 times lager than that of Rainbow. Now, we construct an efficient MQ-signature scheme using sparse polynomials with a shorter secret key and signatures.

Notations.

- m Number of equations
- n Number of variables
- $\mathbb{F}_q$ Finite field of q elements
- $\mathcal{M}_{m\times n}(\mathbb{F}_q)$ Set of $m \times n$ matrices defined on $\mathbb{F}_q$
- $GL_n(\mathbb{F}_q)$ General linear group of degree n defined on $\mathbb{F}_q$, the set of $n \times n$ invertible matrices
- $\mathcal{F}$ Invertible central map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$
- S Affine or linea map $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$
- T Affine or linea map $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- $\widetilde{S}, \widetilde{T}$ Denote $\widetilde{S} = S^{-1}$ and $\widetilde{T} = T^{-1}$

A. OUR CONSTRUCTION

A main idea to construct an MQ-scheme is to find a easily invertible quadratic map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ (called a central map) consisting of m multivariate quadratic polynomials with n variables. It needs to select two linear or affine invertible maps $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to destroy the special structure of $\mathcal{F}$. A public key is $\mathcal{P} = S \circ \mathcal{F} \circ T$ that seems to be indistinguishable from a random system. Then, $(S, \mathcal{F}, T)$ is a secret key. The public key is a system of m quadratic equations with n variables, $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$, defined by

$$\mathcal{P}^{(k)}(x_1, \cdots, x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)},$$

where $p_{ij}^{(k)}, p_i^{(k)}, p_0^{(k)} \in_R \mathbb{F}_q$ for $k = 1, \cdots, m$.

■ **A New Central Map.**

For a new central map, we need the following four index sets as

$$\begin{aligned} V_1 &= \{1, \cdots, v\},\ V_2 = \{1, \cdots, v + o_1\}, \\ O_1 &= \{v + 1, \cdots, v + o_1\}, \\ O_2 &= \{v + o_1 + 1, \cdots, v + o_1 + o_2\}, \end{aligned}$$

where $|V_1| = v$, $|V_2| = v + o_1$ and $|O_i| = o_i$ for $i = 1, 2$. A secret central map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$ is a system of m multivariate quadratic equations with n variables defined by

$$\begin{cases} \mathcal{F}^{(1)}(x) &= \sum_{i=1}^{v} \alpha_{i,v+1+(i-1 (\mathrm{mod}\ o_1))} x_i x_{v+1+(i-1 (\mathrm{mod}\ o_1))}, \\ \mathcal{F}^{(2)}(x) &= \sum_{i=1}^{v} \alpha_{i,v+1+(i-2 (\mathrm{mod}\ o_1))} x_i x_{v+1+(i-2 (\mathrm{mod}\ o_1))}, \\ &\vdots \\ \mathcal{F}^{(o_1)}(x) &= \sum_{i=1}^{v} \alpha_{i,v+1+(i (\mathrm{mod}\ o_1))} x_i x_{v+1+(i (\mathrm{mod}\ o_1))}, \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x) & = \Phi_1(x) + \Theta_1(x) + \epsilon_1 x_{o_1+1}, \\ & \vdots \\ \mathcal{F}^{(o_1+o_2)}(x) & = \Phi'_{o_2}(x) + \Theta_{o_2}(x) + \epsilon_{o_2} x_{o_1+o_2}. \end{cases}$$

where $x = (x_1, \cdots, x_n)$, $m = o_1 + o_2$ and $n = m + v$. We call $\mathcal{F}^{(i)}$ for $i = 1, \cdots, o_1$ a secret polynomial in the first layer, $\mathcal{F}^{(i)}$ for $i = o_1 + 1, \cdots, o_1 + o_2$ a secret polynomial in the second layer. Our central map is designed so that all quadratic terms in the central polynomials don't overlap and the symmetric matrix of each central polynomial has a designated rank. Each polynomial in the central map is selected as follows:

- Choose random $\alpha_{i,j} \in \mathbb{F}_q^*$ so that all quadratic terms in $\mathcal{F}^{(i)}$ don't overlap with those in $\mathcal{F}^{(j)}$ for $i \neq j$ in the first layer and the symmetric matrix corresponding to the quadratic part of each $\mathcal{F}^{(i)}$ $(i = 1, \cdots, o_1)$ has rank $2 \cdot o_1$.
- $\Phi_j(x)$ is a quadratic polynomial in variables $(x_1, \cdots, x_{v+o_1})$ defined by

$$\Phi_j(x) = \sum_{i=1}^{v} \beta_{j,i} x_i x_{1+(i+j-1 (\mathrm{mod}\ v))},$$

  so that all quadratic terms of $\Phi_i(x)$ don't overlap with those of $\Phi_j(x)$ for $i \neq j$ $(i, j = 1, \cdots, \lceil \frac{o_2}{2} \rceil + 1)$ and the $v \times v$ part of the symmetric matrix corresponding to the quadratic part of each $\mathcal{F}^{(i)}$ has rank v for $i = o_1 + 1, \cdots, o_1 + \lceil \frac{o_2}{2} \rceil + 1$, where $\beta_{i,j} \in \mathbb{F}_q^*$.
- $\Phi'_j(x)$ is a quadratic polynomial in variables $(x_1, \cdots, x_{v+o_1})$ defined by

$$\Phi'_j(x) = \sum_{i=v+1}^{v+o_1} \beta'_{j,i} x_i x_{v+1+(i+j-v-1 (\mathrm{mod}\ o_1))},$$

  so that all quadratic terms of $\Phi'_i(x)$ don't overlap with those of $\Phi'_j(x)$ for $i \neq j$ $(i, j = \lceil \frac{o_2}{2} \rceil + 2, \cdots, o_2)$ and the $v \times v$ part of the symmetric matrix corresponding to the quadratic part of each $\mathcal{F}^{(i)}$ has rank v for $i = o_1 + \lceil \frac{o_2}{2} \rceil + 2, \cdots, m$, where $\beta'_{i,j} \in \mathbb{F}_q^*$.
- $\Theta_j(x)$ is a quadratic polynomial in variables $(x_1, \cdots, x_n)$ defined by

$$\Theta_j(x) = \sum_{i=1}^{v+o_1} \gamma_{j,i} x_i x_{v+o_1+1+(i-j (\mathrm{mod}\ o_2))},$$

  so that all quadratic terms in $\Theta_i(x)$ don't overlap with those in $\Theta_j(x)$ for $i \neq j$ and the symmetric matrix corresponding to the quadratic part of each $\mathcal{F}^{(i)}$ has full rank for $i = o_1 + 1, \cdots, o_1 + o_2$, where $\gamma_{i,j} \in \mathbb{F}_q^*$.
- Lastly, select random $\epsilon_i \in \mathbb{F}_q^*$ for the linear part of $\mathcal{F}^{(i)}$ $(i = o_1 + 1, \cdots, o_1 + o_2)$.
- To satisfy the above conditions, the parameter $(\mathbb{F}_q, v, o_1, o_2)$ is guaranteed to be selected as $v \geq o_1 \geq o_2$.

Now, we propose an efficient MQ-signature scheme using our central map.

■ **SOV**(**S**parse Polynomials-based **O**il and **V**inegar Signature Scheme).

• **KeyGen**(1^λ). Given a security parameter λ, output a secret/public key $< SK, PK > = < (\widetilde{S}, \mathcal{F}, \widetilde{T}), \mathcal{P} >$ as follows:

- Select two invertible affine maps $\widetilde{S}$ and $\widetilde{T}$ at random, where $\widetilde{S} = S^{-1}$ and $\widetilde{T} = T^{-1}$
- Choose randomly $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$ so that it satisfies the conditions specified in the above construction of the central map.
- Compute $\mathcal{P} = S \circ \mathcal{F} \circ T$.

• **Sign**(SK, $\mathtt{m}$). For a collusion-resistant hash function $h : \{0,1\}^* \rightarrow \mathbb{F}_q^m$ and a message $\mathtt{m}$, calculate $h(\mathtt{m})$ and $\widetilde{S}(h(\mathtt{m})) = \xi$, where $\xi = (\xi_1, \cdots, \xi_m)$.

- To calculate $\mathcal{F}^{-1}(\xi) = s$: to find s such that $\mathcal{F}(s) = \xi$.
  - Choose a random vector of Vinegar values $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$. After plugging $\mathbf{s_v}$ into $\mathcal{F}^{(i)}$ $(i = 1, \cdots, o_1)$, get a linear system of o_1 equations in o_1 variables. Compute a solution $(s_{v+1}, \cdots, s_{v+o_1})$ of the linear system by using Gaussian elimination.
  - After plugging $(s_1, \cdots, s_{v+o_1})$ into $\mathcal{F}^{(i)}$ $(i = o_1 + 1, \cdots, o_1 + o_2)$, get a linear system of o_2 equations in o_2 variables and find a solution $(s_{v+o_1+1}, \cdots, s_{v+o_1+o_2})$ of the resulting linear system. Then $\mathbf{s} = (s_1, \cdots, s_n)$ is a solution of $\mathcal{F}(x) = \xi$.
  - If one of the two linear systems has no solution then choose another vector of Vinegar values $s_v{}' = (s'_1, \cdots, s'_v)$ and try again.
- Calculate $\widetilde{T}(s) = \sigma$ and output σ as a signature on $\mathtt{m}$.

• **Verify**(PK, σ, $\mathtt{m}$). From a public key $\mathcal{P}$ and a signature σ on $\mathtt{m}$, check the equality $\mathcal{P}(\sigma) = h(\mathtt{m})$. If it holds, output valid.

Key Sizes. The public key of SOV requires $\frac{m(n+1)(n+2)}{2}$ field elements. The secret affine maps T and S require $n(n+1)$ and $m(m+1)$ field elements, respectively. In the first layer, it requires $v \cdot o_1$ field elements. In the second layer, it requires $(v + o_1) \cdot o_2 + v \cdot (\lceil \frac{o_2}{2} \rceil + 1) + o_1 \cdot (\lceil \frac{o_2}{2} \rceil)$ field elements for quadratic terms and o_2 field elements for linear terms. Thus, the secret key requires $o_1 v + o_2(v + o_1 + 1) + v \cdot (\lceil \frac{o_2}{2} \rceil + 1) + o_1 \cdot \lceil \frac{o_2}{2} \rceil + m(m+1) + n(n+1)$ field elements.

III. SECURITY ANALYSIS OF SOV AGAINST KNOWN ALGEBRAIC ATTACKS

The MQ-schemes using the ASA structure require two hard problems for security: the MQ-Problem and the Extended Isomorphism of Polynomials problem. Moreover, the MQ-schemes with multiple layers need the intractability of the MinRank problem. We introduce the underlying hard problems.

- **Multivariate Quadratic (MQ) Problem:** Given a system of m quadratic equations, $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$, on $\mathbb{F}_q$ in variables $(x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_m) \in \mathbb{F}_q^m$, compute a solution $(x'_1, \cdots, x'_n) \in \mathbb{F}_q^n$ such that $\mathcal{P}^{(1)}(x'_1, \cdots, x'_n) = y_1, \cdots, \mathcal{P}^{(m)}(x'_1, \cdots, x'_n) = y_m$.

- **Extended Isomorphism of Polynomials (EIP) Problem:** For a nonlinear multivariate system $\mathcal{P} = S \circ \mathcal{F} \circ T$ for affine or linear maps S and T, and $\mathcal{F}$ in a certain class of nonlinear system $\mathcal{SC}$, find $(S', \mathcal{F}', T')$ such that $\mathcal{P} = S' \circ \mathcal{F}' \circ T'$ for affine or linear maps S' and T', and $\mathcal{F}' \in \mathcal{SC}$.
- **MinRank Problem:** For $k, m, n, r \in \mathbb{N}$ such that $m, r < n$. The MinRank(r) problem is, given $(M_1, \cdots, M_l) \in \mathcal{M}_{m\times n}(F_q)$, find a non-zero k-tuple $(\lambda_1, \cdots, \lambda_k) \in \mathbb{F}_q^k$ satisfying $Rank(\sum_{i=1}^{k} \lambda_i M_i) \leq r$.

The MQ-problem is proven to be NP-complete [26] even for the quadratic equations defined on $\mathbb{F}_2$. Patarin [34] describe the IP-problem and there exist not much known about its hardness compared to the MQ-problem [9], [23]. The MinRank problem was described in [40] and proven its NP-completeness.

It is known that a public key of the MQ-scheme has many distinct secret keys (called equivalent keys) [43]. For a secret/public key, $< (S, \mathcal{F}, T), \mathcal{P} >$, of an MQ-scheme, if $\mathcal{P} = S' \circ \mathcal{F}' \circ T' = S \circ \mathcal{F} \circ T$ and $\mathcal{F}'$ preserves the special structure of $\mathcal{F}$, then $(S', \mathcal{F}', T')$ is an equivalent key of $(S, \mathcal{F}, T)$, where $S' \in GL_m(\mathbb{F}_q)$ and $T' \in GL_n(\mathbb{F}_q)$. If an adversary can find any of the equivalent keys then the adversary can invert the public key, so forge signatures on any message for the public key.

In the MQ-schemes, there exist the two types of attacks as:

- **Direct Attack.** For a public key $\mathcal{P} = S \circ \mathcal{F} \circ T$ and $y \in \mathbb{F}_q^m$, compute a solution $s \in \mathbb{F}_q^n$ of $\mathcal{P}(x) = y$.
- **Key Recovery Attack.** For $\mathcal{P} = S \circ \mathcal{F} \circ T$, find an equivalent key of $(S, \mathcal{F}, \mathcal{T})$.

A. DIRECT ATTACKS

An adversary for mounting direct attacks on the MQ-schemes wants to find a solution $s \in \mathbb{F}_q^n$ of $\mathcal{P}(x) = y$, i.e. solve the MQ-problem. For it, the adversary uses Gröbner basis algorithms like F4 and F5 for solving the MQ-problem. The complexity for solving the MQ-problem can be estimated as the HybridF5 (HF5) algorithm [6] to solve the problem. A main idea is to guess k variables to get overdetermined systems and then runs the F5 algorithm [21] for solving the overdetermined systems. Then, the number is given by q^k when guessing k variables over $\mathbb{F}_q$. The complexity for solving a semi-regular quadratic system of m equations with n variables on $\mathbb{F}_q$ by the HF5 algorithm is be determined by

$$C_{HF5}(q, n) = min_{k\geq 0}\mathcal{O}\left(q^k \left[m \cdot \binom{n-k-1+d_{reg,k}}{d_{reg,k}}\right]^{\alpha}\right),$$

where $d_{reg,k}$ is the degree of regularity of the quadratic system after fixing the values of k variables. The linear algebra constant $2 \leq \alpha \leq 3$ is for solving a linear system. Since the internal equations utilized by the HF5 algorithm are very sparse, $\alpha = 2$ can be used to get a lower bound on the complexity.

For security of SOV against the direct attacks, we perform a number of experiments using the F4 algorithm (the details of the F5 algorithm are not publicly known) with MAGMA v2.19-10 on Intel Core i5-6600 3.3 GHz. We compare experimental results for solving quadratic systems derived from a public key of SOV with random quadratic systems on $\mathbb{F}_{31}$ in Table 1. These results are averages of 100 measurements for each system. According to these results, it makes a little difference in complexities for solving two types of quadratic systems.

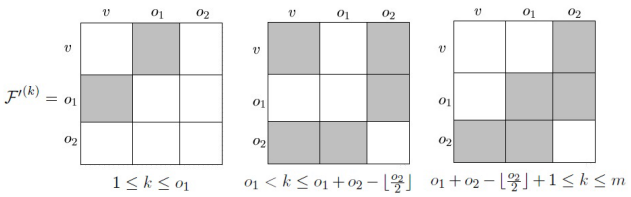

FIGURE 1. Generalized Version of the Central Map for SOV.

TABLE 1. Running Time (Second) for Solving Two Types of Quadratic Systems on $\mathbb{F}_{31}$.

(v, o_1, o_2)	(6,5,3)	(6,5,4)	(7,6,4)	(7,6,5)	(8,6,5)	(8,7,6)
Random System	0.098	0.43	2.4	16.58	107.07	839.9
SOV	0.089	0.44	2.59	14.67	119.52	850.61
deg_{reg}	10	11	12	13	14	15

For given security levels, we can determine the required numbers of equations for solving the determined systems on $\mathbb{F}_{31}$ by using HF5 algorithm ($\alpha = 2$) given in Table 2. It will be used to select a secure parameter of SOV against the direct attacks for a given security level λ.

TABLE 2. Numbers (m) of Quadratic Equations for Determined Systems over $\mathbb{F}_{31}$ associated to Security Levels.

m/λ	80	96	112	128	160	192	256
m	28	35	41	48	62	75	103

B. KEY RECOVERY ATTACKS

The goal of key recovery attacks (KRAs) is to find the secret key S and T. The KRAs use the special structure of the central map, i.e. quadratic terms with zero coefficients at certain known places, to get a systems of equations with variables in S and T. In our central map, since it significantly increases quadratic terms with zero coefficients due to the use of sparse polynomials, the security of our scheme against the KRAs should be guaranteed. The complexity of solving the above system can be improved by using equivalent keys. If one can find an equivalent key (S', T') then one can reduce the number of variables in the resulting system with many unknowns to recover (S', T'). Complexity of solving such systems depends on the number of unknowns and thus one would like to reduce them further.

Wolf and Preneel [43] introduced the concept of equivalent keys and Thomae [42] generalized the notion of equivalent keys to good keys. The KRAs on UOV were presented as

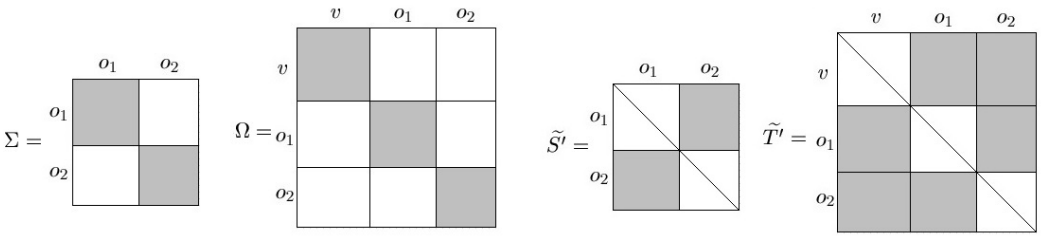

FIGURE 2. Equivalent Keys of SOV.

Reconcilation attacks [18]. Ding *et al.* [18] extended the Reconcilation attacks to Rainbow Band Separation (RBS) attacks on Rainbow. The KRAs using good keys are the generalization of the RBS attacks. Now, we give security analysis of SOV against KRAs using equivalent keys and good keys.

1) BASIC KRAS

For $1 \le k \le m$, let $F^{(k)}$ be symmetric matrices related to the quadratic part of $\mathcal{F}^{(k)}$ in the secret central map. For $1 \le k \le m$, let $P^{(k)}$ be symmetric matrices associated to the quadratic part of $\mathcal{P}^{(k)}$ in the public key. From $\mathcal{F} = \widetilde{S} \circ \mathcal{P} \circ \widetilde{T}$, we have the equality

$$\mathcal{F}^{(k)} = \widetilde{T}^{\mathsf{T}} \left(\sum_{j=1}^{m} \widetilde{s}_{ij} P^{(j)} \right) \widetilde{T}, \quad 1 \le k \le m,$$

and the corresponding system of equations as

$$f_{ij}^{(k)} = \sum_{x=1}^{m} \sum_{y=1}^{n} \sum_{z=1}^{n} c_{yz}^{(x)} \widetilde{s}_{kx} \widetilde{t}_{yi} \widetilde{t}_{zj} \tag{1}$$

with coefficients $c_{yz}^{(x)}$. Since certain quadratic terms in $\mathcal{F}^{(k)}$ have zero coefficients, we get $f_{ij}^{(k)} = 0$ for some i, j, k. For SOV, we get a system of

$$\frac{mn(n+1)}{2} - vo_1 - o_2(v + o_1 + \lfloor \frac{o_2}{2} \rfloor (o_1 - v) + vo_2)$$

cubic equations with $(n^2 + m^2)$ variables. The complexity for solving the cubic system using the HF5 algorithm is large.

2) KRAS USING EQUIVALENT KEYS

To reduce this complexity, one can use the notion of equivalent keys [42], [43].

Definition 1: Let $S, S' \in GL_m(\mathbb{F}_q)$ and $T, T' \in GL_n(\mathbb{F}_q)$. We call S' and T' equivalent keys to S and T, if and only if $S' \circ \mathcal{F}' \circ T' = S \circ \mathcal{F} \circ T$ and $\mathcal{F}|_I = \mathcal{F}'|_I$, i.e. both $\mathcal{F}$ and $\mathcal{F}'$ have the same structure for an index set $I = \{I^{(1)}, \cdots I^{(m)}\}$ for $I^{(k)} \subseteq \{x_i x_j | 1 \le i \le j \le n\}$.

If one can find two linear maps $\Sigma \in GL_m(\mathbb{F}_q)$ and $\Omega \in GL_n(\mathbb{F}_q)$ so that

$$\mathcal{P} = (S \circ \Sigma^{-1}) \circ (\Sigma \circ \mathcal{F} \circ \Omega) \circ (\Omega^{-1} \circ T),$$

and $\mathcal{F}'$ preserves all quadratic terms with zero coefficients in $\mathcal{F}$, then S' and T' are equivalent keys, where $\mathcal{F}' = \Sigma \circ \mathcal{F} \circ \Omega$, $T' = \Omega^{-1} \circ T$ and $S' = S \circ \Sigma^{-1}$.

To find the equivalent key of SOV, we consider a generalized version of our central map, $\overline{\mathcal{F}} = (\overline{\mathcal{F}}^{(1)}, \cdots, \overline{\mathcal{F}}^{(m)})$, given in Fig. 1, where gray parts represent arbitrary values and white parts represent zero values.

Lemma 1: For the generalized central map $\overline{\mathcal{F}}^{(k)}$ in Fig. 1, there exist equivalent keys S' and T' of the forms in Fig. 2, where white parts represent zero values, gray parts represent arbitrary values and there exist ones at the diagonal.

Proof: One can select Ω and Σ of the forms in Fig. 2 so that $\mathcal{F}'^{(k)}$ preserves the quadratic terms with zero coefficients in the generalized central map $\overline{\mathcal{F}}^{(k)}$ in Fig. 1 as in [42]. Then $T' = \Omega^{-1} \circ T$ and $S' = S \circ \Sigma^{-1}$ are the equivalent key of the forms in Fig. 2. □

When we apply the transformations Ω and Σ to the generalized central map $\overline{\mathcal{F}}^{(k)}$, we get $\mathcal{F}'$ as in Fig. 1. To recover the equivalent key, we need to solve a system of

$$\frac{o_1 n(n+1) + o_2 v(v+1) + \lfloor \frac{o_2}{2} \rfloor (v - o_1)(v + o_1 + 1)}{2} + vo_1(o_2 - o_1)$$

cubic equations with $(4\, o_1\, o_2 + 2vm)$ variables. The complexity for solving this cubic system is still large: the complexity for solving the cubic system by HF5 is 2^{4218} for the parameter SOV($\mathbb{F}_{31}$, 29, 28, 26).

3) KRAs USING GOOD KEYS

To further improve this complexity, one can use good keys, a generalized notion of equivalent keys [42]. Good keys preserve some of quadratic terms with zero coefficients in $\mathcal{F}$ not all these quadratic terms. Thus, one further reduces the numbers of variables and equations by selecting Σ and Ω more generally.

Definition 2: Let $S, S'' \in GL_n(\mathbb{F}_q)$ and $T, T'' \in GL_m(\mathbb{F}_q)$ and $I^{(k)} \subseteq \{x_i x_j | 1 \le i \le j \le n\}$ for $1 \le k \le m$ fixed. Let $J^{(k)} \subseteq I^{(k)}$ for $1 \le k \le m$ with at least one $J^{(k)} \ne \phi$. We call S'' and T'' gook key of S and T if and only if $S'' \circ \mathcal{F}'' \circ T'' = S \circ \mathcal{F} \circ T$ and $\mathcal{F}|_J = \mathcal{F}''|_J$ for the fixed index set $J = \{J^{(1)}, \cdots, J^{(m)}\}$.

Let S' and T' be the equivalent key of SOV. If one can find two linear maps $\Sigma' \in GL_m(\mathbb{F}_q)$ and $\Omega' \in GL_n(\mathbb{F}_q)$ so that

$$\mathcal{P} = (S' \circ \Sigma'^{-1}) \circ (\Sigma' \circ \mathcal{F}' \circ \Omega') \circ (\Omega'^{-1} \circ T')$$

and $\mathcal{F}''$ preserves all quadratic terms with zero coefficients in the subset J of I, then $(\mathcal{F}'',\ S'',\ T'')$, are good keys of

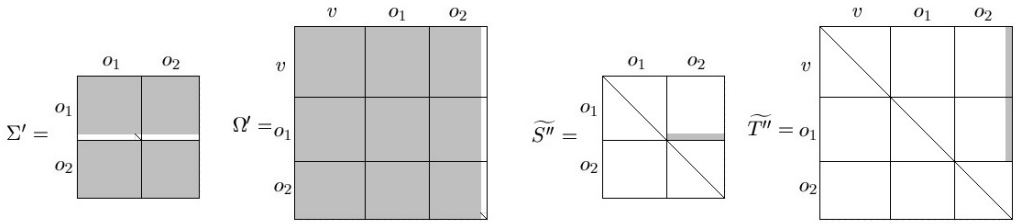

FIGURE 3. Good keys for SOV.

TABLE 3. Complexities of the KRAs using Equivalent Keys and Good Keys for SOV($\mathbb{F}_{31}$, 29, 28, 26).

SOV	# of Equations	# of Variables	d_{reg}	Complexity
KRAs	166,684(Cubic)	9,805	628	2^{6871}
KRAs with Equivalent Keys	106,917(Cubic)	6,044	384	2^{4218}
KRAs with Good Keys	136(Quad.)	83	15	2^{128}

$(S, \mathcal{F}, T)$, where $\mathcal{F}'' = \Sigma' \circ \mathcal{F}' \circ \Omega'$, $S'' = S' \circ \Sigma'^{-1}$ and $T'' = \Omega'^{-1} \circ T'$. We can get the good keys for SOV as in Lemma 2.

Lemma 2: For the equivalent key for SOV, S' and T' of the forms in Fig. 2, there exist good keys S'' and T'' of the forms in Fig. 3. In the good keys, only o_2 values of the o_1-th row in $\widetilde{S''}$ are arbitrary, equal to the corresponding values in $\widetilde{S'}$ and only the last column of $\widetilde{T''}$ are arbitrary values in the first $(v + o_1 + o_2)$ rows, equal to the corresponding values in $\widetilde{T'}$.

Proof: One can select Σ' and Ω' of the forms in Fig. 3 so that $\mathcal{F}''$ preserves the quadratic terms with zero coefficients in the designated index set as in [42]. Then, $S'' = S' \circ \Sigma'^{-1}$ and $T'' = \Omega'^{-1} \circ T'$ of the form given in Fig. 3 are good keys associated to the equivalent key (S', T'). □

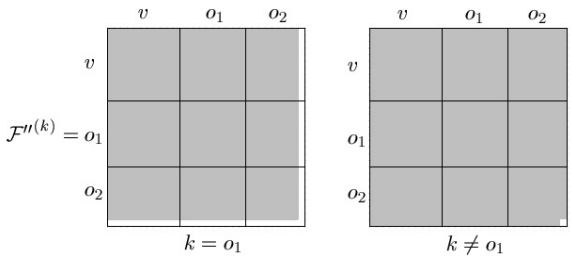

FIGURE 4. Form of $\mathcal{F}'' = \Sigma' \circ \mathcal{F}' \circ \Omega'$ of SOV.

Since $\mathcal{F}'' = \Sigma' \circ \mathcal{F}' \circ \Omega'$, $\mathcal{F}''$ is of the form in Fig. 4, which is the same as those of Rainbow [42]. It shows that the forms of the good keys for SOV are the same as those for Rainbow although the equivalent keys for SOV is different from those of Rainbow. Consequently, we get the following Theorem.

Theorem 1: The complexity of SOV against the KRAs using good keys is determined by solving m quadratic equations and $(n-1)$ bihomogeneous equations with n variables.

All the remaining parts of S' and T' are retrieved by linear equations as in [42] after recovering one row of S' and one column of T'. Therefore, we can retrieve the entire equivalent keys S' and T'.

In Table 3, we summarize improvements of lower bounds ($\alpha = 2$) on the complexities for solving the resulting systems by the HF5 algorithm from the KRAs using equivalent keys and good keys for SOV($\mathbb{F}_{31}$, 29, 28, 26). The reason of the selection of this parameter will be presented in the Section IV. In general, only the number of variables is reduced to find the equivalent keys. Since we utilize the equivalent keys corresponding to the generalized central map given in Fig. 1 instead of the original central map to get complexity as low as possible, the number of equations in our KRAs with equivalent keys is also changed,

C. RANK-BASED ATTACKS

Now, we analyze our scheme against known rank-based attacks. Our central map is designed so that all the quadratic terms in the central polynomials don't overlap and each symmetric matrix of each central polynomial has a designated rank. In particular, each symmetric matrix of each central polynomial in the second layer has full rank. This property plays an important role in preventing the rank-based attacks.

• **MinRank attack.** An adversary for mounting the MinRank attack wants to find linear combinations $R = \sum_{i=1}^{m} \lambda_i P^{(i)}$ of the matrices $P^{(i)}$, where R has a minimal rank r. A basic idea to solve the MinRank problem [40] is to find a vector in the kernel of R. The following Proposition determines the complexity of SOV against the MinRank attack by using the technique in [7].

Proposition 1: The complexity of SOV against the MinRank attack is $o_1 \cdot q^{o_1+1}$.

Proof: In this attack, one tries to find a vector $v \in \mathbb{F}_q^n$ in the $\ker P$, where P is a matrix of the minimal rank in Span$\{P^{(i)}\}$. The probability of finding such v is the same as that of finding $v' \in \mathbb{F}_q^n$ in the $\ker Q$, where Q is a matrix of the minimal rank in Span$\{F^{(i)}\}$. More precisely, $F^{(i)}$ in the first layer is of the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. Then $F^{(i)} \cdot (*, 0)^T = (0, *)^T$ and $F^{(i)} \cdot (0, *)^T = (*, 0)^T$. Let $w_i = F^{(i)} \cdot (*, 0)^T$ and $w_i' = F^{(i)} \cdot (0, *)^T$ for $i = 1, \cdots, o_1$. Then the probability that w_i (resp., w_i') are

TABLE 4. Complexities of SOV($\mathbb{F}_{31}$, 29, 28, 26) against All the Attacks.

$(\mathbb{F}_q, v, o_1, o_2)$	Direct	KRAs	Kipnis-Shamir	MinRank	HighRank
$(\mathbb{F}_{31}, 29, 28, 26)$	2^{145}	2^{128}	2^{172}	2^{148}	2^{145}

TABLE 5. Comparison of Signature Sizes, Key Sizes of Ours, Pre-Quantum Schemes and Post-Quantum Schemes.

Scheme (λ)	**Signature Size** (Bytes)	**Public Key** (Bytes)	**Secret Key** (Bytes)
Classical ones			
RSA-3072 (128) [5]	361	384	3072
ECDSA-256 (128) [5]	64	64	96
Lattice-based			
TESLA-416 (128) [3]	1,280	1,331,200	1,011,744
TESLA-768 (128) [3]	2,336	4,227,072	3,293,216
ring-TESLA-II (128) [1]	1,568	3,328	1,920
BLISS-BI (128) [19], [20]	1,559	7,168	2,048
Hash-based			
XMSS [10], [28] (256)	1,332	14,951	8,500
XMSS-T [29] (256)	66	14,951	8,500
SPHINCS 256 (256) [4]	41,000	1,056	1,088
Code-based			
Parallel-CFS (80) [32]	20,968,300	4,194,300	75
Isogeny-based			
GPS (128) [25]	22,528	96	32
CSIDH^{SS} (128) [24]	978	4,194,304	16
CSIDH^{SP} (128) [24]	3136	32	1,048,576
MQ-based			
MQDSS-31-64 (>128) [12]	40,952	72	64
Gui(2,240,9,16,16,3) (100) [13], [38]	68	921,088	64,409
enTTS($\mathbb{F}_{28}$, 15, 60, 88) (128) [16], [44]	88	234,960	13,051
Rainbow($\mathbb{F}_{31}$, 28, 28, 28) [13], [17]	53	127,925	100,415
SOV($\mathbb{F}_{31}$, 29, 28, 26) (128)	**52**	**120,487**	**8,145**

CSIDH^{SS} is a smaller signature version of CSIDH in [24].
CSIDH^{SP} is a smaller public key version of CSIDH in [24].

linearly dependent is

$$1-\prod_{i=0}^{o_1-1}(1-\frac{q^i}{q^{o_1}}) > 1/q \ \ (resp.,\ 1-\prod_{i=0}^{o_1-1}(1-\frac{q^i}{q^{v}}) > 1/q^{v-o_1+1}).$$

Then, $\sum_{i=1}^{o_1}\lambda_i F^{(i)}$ has a minimal rank. The probability of $v' \in \ker(\sum_{i=1}^{o_1}\lambda_i F^{(i)})$ with a random vector v' and non-trivial λ_i is $1/q^{o_1}\cdot 1/q = 1/q^{o_1+1}$: the probability that the vector v' has of the form $(*, 0)$ is $1/q^{o_1}$. Similarly, the probability for $v' = (0, *)$ is

$$1/q^{v}\cdot 1/q^{v-o_1+1} = 1/q^{2v-o_1+1}.$$

In our case, since $v \geq o_1 \geq o_2$, $min\{q^{o_1+1},\ q^{2v-o_1+1}\}$ is q^{o_1+1}. By finding o_1 linear independent matrices $M = \sum_{i=1}^{m}\lambda_i P^{(i)}$, one can extract the first layer of SOV. This step costs approximately $o_1\cdot q^{o_1+1}$ as in [37]. □

• **HighRank Attack.** An adversary for mounting the HighRank attack wants to identify the variables appearing the lowest number of times in the central polynomials. The variables $x_{v+o_1+1}, \cdots, x_n$ appear only in the quadratic terms of $\mathcal{F}^{(o_1+1)}, \cdots, \mathcal{F}^{(o_1+o_2)}$ in the second layer of SOV. Thus, it is similar to that of Rainbow. As in [37], the complexity of SOV against the HighRank attack is $q^{o_2}\cdot\frac{n^3}{6}$.

• **Kipnis-Shamir Attack (UOV Attack).** The balanced Oil and Vinegar signature scheme ($v = o$) [36] was broken by Kipnis-Shamir attack [31]. The attack can be generalized to the unbalanced schemes. It uses the property that any linear combinations of $F^{(1)}, \cdots, F^{(m)}$ has of the form $\begin{pmatrix} A_1 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & 0 \end{pmatrix}$ to find the preimage of the subspaces under an equivalent key T', It has the same form of Rainbow. As in [37], the complexity of SOV against the UV attack is $o_2^4\cdot q^{v+o_1-o_2-1}$.

IV. PARAMETER SELECTION AND COMPARISON

Now, we select a secure and optimal parameter for SOV and compare SOV and other signature schemes.

A. PARAMETER SELECTION

We want to select a secure and optimal parameter set $(\mathbb{F}_q, v, o_1, o_2)$ so that a SOV($\mathbb{F}_q, v, o_1, o_2$) instance over $\mathbb{F}_q$ achieves a security level of λ-bits against all known attacks. According to our security analysis, the complexities of SOV against all the known attacks are summarized as:

- Direct attacks: The complexity is the same as $C_{MQ}(q, m, n)$, where $C_{MQ}(q, m, n)$ denotes complexity for solving a random system of m quadratic equations with n variables defined on $\mathbb{F}_q$ by using the HF5 algorithm.
- KRAs: The complexity is the same as $C_{MQ}(q,\ m+n-1,\ n)$.
- MinRank Attacks: The complexity is $o_1\cdot q^{o_1+1}$.

- HighRank Attacks: The complexity is $q^{o_2} \cdot \frac{n^3}{6}$.
- Kipnis-Shamir Attacks: The complexity is $o_2^4 \cdot q^{v+o_1-o_2-1}$.

Finally, we select a secure and optimal parameter of SOV at a 128-bit security level as

- SOV($\mathbb{F}_{31}$, 29, 28, 26).

We summarize complexities of SOV($\mathbb{F}_{31}$, 29, 28, 26) against all the attacks in Table 4, where we take $\alpha = 2$ for computing the complexities against the KRAs using good keys and the direct attacks.

B. COMPARISON

We compare our scheme to pre-quantum schemes and post-quantum schemes in terms of signature sizes and key sizes in Table 5.

Signature Size. Signature size of SOV is also the shortest among pre-quantum schemes and post-quantum schemes. SOV($\mathbb{F}_{31}$, 29, 28, 26) results in signatures of 52 bytes, while ECDSA-256 requires signatures of 64 bytes. Signatures of BLISS-BI are about 30 times bigger than those of SOV.

Key Sizes. Compared to Rainbow, the secret key of SOV is reduced by a factor of about 90% without increasing public key size. Compared to enTTS, the public key size and secret key size of SOV are reduced by a factor of about 49% and 38%, respectively.

V. CONCLUSION

We constructed an efficient MQ-signature scheme, SOV, using the sparse polynomials. The secret key size of SOV is reduced by a factor of about 90% without increasing the public key size compared to Rainbow. Moreover, the signature size is the shortest among all known signature schemes resulting in 52 bytes, while ECDSA-256 requires signatures of 64 bytes. We believe that SOV is suitable for specific applications, where the existing signature schemes cannot be used due to their slow performance and large signature sizes.

REFERENCES

[1] S. Akleylek, N. Bindel, J. Buchmann, J. Krämer, and G. A. Marson, "An efficient lattice-based signature scheme with provably secure instantiation," in *AFRICACRYPT* (Lecture Notes in Computer Science), vol. 9646. Heidelberg, Germany: Springer, 2016, pp. 44–60.

[2] S. M. E. Y. Alaoui, O. Dagdelen, P. Véron, D. Galindo, and P.-L. Cayrel, "Extended security arguments for signature schemes," in *AFRICACRYPT* (Lecture Notes in Computer Science), vol. 7374. Heidelberg, Germany: Springer, 2012, pp. 19–34.

[3] E. Alkim, N. Bindel, J. Buchmann, O. Dagdelen and P. Schwabe, "TESLA: Tightly-secure efficient signatures from standard lattices," IACR, Cryptol. ePrint Arch., Tech. Rep. 2015/755, 2015.

[4] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "SPHINCS: Practical stateless hash-based signatures," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 9056. Heidelberg, Germany: Springer, 2015, pp. 368–397.

[5] D. J. Bernstein and T. Lange. *eBACS: ECRYPT Benchmarking of Cryptographic Systems*. Accessed: Sep. 30, 2016. [Online]. Available: http://bench.cr.yp.to

[6] L. Bettale, J.-C. Faugère and L. Perret, "Hybrid approach for solving multivariate systems over finite fields," *J. Math. Cryptol.*, vol. 3, no. 3, pp. 177–197, 2009.

[7] O. Billet and H. Gilbert, "Cryptanalysis of rainbow," in *Security and Cryptography for Networks* (Lecture Notes in Computer Science), vol. 4116. Heidelberg, Germany: Springer, 2006, pp. 336–347.

[8] A. Bogdanov, T. Eisenbarth, A. Rupp and C. Wolf, "Time-area optimized public-key engines: $\mathcal{MQ}$-cryptosystems as replacement for elliptic curves?" in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 5154. Heidelberg, Germany: Springer, 2018, pp. 45–61.

[9] C. Bouillaguet, P.-A. Fouque, A. Veber, and G.-T. A. F. the, "Graph-theoretic algorithms for the 'Isomorphism of polynomials' problem," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 7881. Heidelberg, Germany: Springer, 2013, pp. 211–227.

[10] J. Buchmann, E. Dahmen and A. Hülsing, "XMSS—A practical forward secure signature scheme based on minimal security assumptions," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 7071. Heidelberg, Germany: Springer, 2011, pp. 117–129.

[11] A.I.-T. Chen, M.S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E.L.-H. Kuo, F.Y.-S. Lee and B.-Y. Yang, "SSE implementation of multivariate PKCs on modern x86 CPUs," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 5747. Heidelberg, Germany: Springer, 2009, pp. 33–48.

[12] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe, "From 5-Pass $\mathcal{MQ}$-based identification to $\mathcal{MQ}$-based signatures," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 10032. Heidelberg, Germany: Springer, 2016, pp. 135–165.

[13] M.-S. Chen, W.-D. Li, B.-Y. Peng, B.-Y. Yang and C.-M. Cheng, "Implementing 128-bit secure MPKC signatures," IACR, Cryptol. ePrint Arch., Tech. Rep. 2017/636, 2017.

[14] J.-M. Chen and B.-Y. Yang, "Tame transformation signatures with topsy-yurvy hashes," IWAP, Taipei, Taiwan, Tech. Rep., 2002.

[15] J-M Chen and Bo-Yin Yang, "A more secure and efficacious TTS signature scheme," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, in Lecture Notes in Computer Science, vol. 2971. Heidelberg, Germany: Springer, 2003, pp. 320–338.

[16] P. Czypek, S. Heyse and E. Thomae, "Efficient implementations of $\mathcal{MQ}$PKS on constrained devices," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 7428. Heidelberg, Germany: Springer, 2012, pp. 374–389.

[17] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 3531. Heidelberg, Germany: Springer, 2005, pp. 164–175.

[18] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, "New differential-algebraic attacks and reparametrization of rainbow," in *Applied Cryptography and Network Security*. Heidelberg, Germany: Springer, 2008, pp. 242–257.

[19] L. Ducas, "Accelerating bliss: The geometry of ternary polynomials," IACR, Cryptol. ePrint Arch., Tech. Rep. 2014/874, 2014.

[20] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 8042. Heidelberg, Germany: Springer, 2013, pp. 40–56.

[21] J.-C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, 2002, pp. 75–83.

[22] J.-C. Faugère, D. Gligoroski, L. Perret, S. Samardjiska, and E. Thomae, "A polynomial-time key-recovery attack on MQQ cryptosystems," in *Public-Key Cryptography*, (Lecture Notes in Computer Science), vol. 9020. Heidelberg, Germany: Springer, 2015, pp. 150–174.

[23] J.-C. Faugère and L. Perret, "Polynomial equivalence problems: Algorithmic and theoretical aspects," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 4004. Heidelberg, Germany: Springer, 2006, pp. 30–40.

[24] L. D. Feo, and S. D. Galbraith, "SeaSign: Compact isogeny signatures from class group actions," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 1147. Heidelberg, Germany: Springer, 2019, pp. 759–789.

[25] S. D. Galbraith, C. Petit and J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems," in *ASIACRYPT* (Lecture Notes in Computer Science), vol. 10624. Heidelberg, Germany: Springer, 2017, pp. 3–33.

[26] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. San Francisco, CA, USA: Freeman, 1990.

[27] D. Gligoroski, R. Steinsmo, R. E. Jensen, L. Perret, J-C. Faugere, S. J. Knapskog, and S. Markovski, "MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme," in *INTRUST* (Lecture Notes in Computer Science), vol. 7222. Heidelberg, Germany: Springer, 2011, pp. 184–203.

[28] A. Hülsing, D. Butin, and S. Gazdag, "XMSS: Extended hash-based signatures draftxmss-00," Crypto Forum Research Group, Internet Draft, Tech. Rep., 2015. Accessed: Sep. 1, 2019. [Online]. Available: https://tools.ietf.org/html/draft-huelsing-cfrg-hash-sig-xmss-00

[29] A. Hülsing, J. Rijneveld, and F. Song, "Mitigating multi-target attacks in hash-based signatures," in *Public-Key Cryptography* (Lecture Notes in Computer Science), vol. 9614. Heidelberg, Germany: Springer, 2016, pp. 387–416.

[30] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1592. Heidelberg, Germany: Springer, 1999, pp. 206–222.

[31] A. Kipnis and A. Shamir, "Cryptanalysis of the oil and vinegar signature scheme," in *CRYPTO* (Lecture Notes in Computer Science), vol. 1462. Heidelberg, Germany: Springer, 1998, pp. 257–266.

[32] G. Landais and N. Sendrier, "Implementing cfs," in *INDOCRYPT* (Lecture Notes in Computer Science), vol. 7668. Heidelberg, Germany: Springer, 2012, pp. 474–488.

[33] T. Matsumoto, and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 330. Heidelberg, Germany: Springer, 1998, pp. 419–453.

[34] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 1070. Heidelberg, Germany: Springer, 1996, pp. 33–48.

[35] J. Patarin, N. Courtois, and L. Goubin, "QUARTZ, 128-bit long digital signatures," in *CT-RSA* (Lecture Notes in Computer Science), vol. 2020. Heidelberg, Germany: Springer, 2001, pp. 282–297.

[36] J. Patarin, "The oil and vinegar signature scheme," in *Proc. Dagstuhl Workshop Cryptogr.*, Sep. 1997.

[37] A. Petzoldt, "Selecting and reducing key sizes for multivariate cryptography," Ph.D. dissertation, Technische Universität Darmstadt, Darmstadt, Germany, 2013.

[38] A. Petzoldt, M.-S. Chen, B.-Y. Yang, C. Tao, and J. Ding, "Design principles for HFEv- based multivariate signature schemes," in *ASIACRYPT* (Lecture Notes in Computer Science), vol. 9452. Heidelberg, Germany: Springer, 2015, pp. 311–334.

[39] K. Sakumoto, T. Shirai, and H. Hiwatari, "Public-key identification schemes based on multivariate quadratic polynomials," in *CRYPTO* (Lecture Notes in Computer Science), vol. 6841. Heidelberg, Germany: Springer, 2011, pp. 706–723.

[40] J.O. Shallit, G.S. Frandsen, and J. F. Buss, *The Computational Complexity of some Problems of Linear Algebra*, BRICS series report, Aarhus, Denmark. Accessed: Sep. 1, 2019. [Online]. Available: http://www.brics.dk/RS/96/33

[41] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 41, no. 2, pp. 1484–1509, 1997.

[42] E. Thomae, "About the security of multivariate quadratic public key schemes," Ph.D. dissertation, Ruhr-Univ. Bochum, Bochum, Germany, 2013.

[43] C. Wolf and B. Preneel, "Large superfluous keys in Multivariate Quadratic asymmetric systems," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3386. Heidelberg, Germany: Springer, 2005, pp. 275–287.

[44] B.-Y. Yang and J.-M. Chen, "TTS: Rank attacks in tame-like multivariate PKCs," IACR Cryptol. ePrint Arch., Lyon, France, Tech. Rep. 2004/061, 2004. [Online]. Available: http://eprint.iacr.org/2004/061

[45] B.-Y. Yang and J.-M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," in *Proc. Australas. Conf. Inf. Secur. Privacy* (Lecture Notes in Computer Science), vol. 3574. Heidelberg, Germany: Springer, 2005, pp. 518–531.

KYUNG-AH SHIM is currently a Senior Researcher with the National Institute for Mathematical Sciences. Her research interests include public-key cryptography, post-quantum cryptography, cryptographic protocols, and information security.

CHEOL-MIN PARK received the B.S. degree in mathematics education, the M.S. and Ph.D. degrees in mathematics from Seoul National University, Seoul, South Korea, in 1999, 2001, and 2006, respectively. He has been a Researcher with the National Institute for Mathematical Sciences, since 2011. His research interests include elliptic curves and multivariate public key cryptography.

NAMHUN KOO received the B.S., M.S., and Ph.D. degrees in mathematics from Sungkyunkwan University, Suwon, South Korea, in 2007, 2009, and 2014, respectively. From May 2014 to May 2017, he was a Postdoctoral Researcher with the National Institute for Mathematical Sciences (NIMS), Daejeon, South Korea. He is currently a Senior Researcher with the Applied Algebra and Optimization Center (AORC), Sungkyunkwan University. His research interests include post-quantum cryptography and cryptographic Boolean functions.