HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations

November 30, 2017

1. Algorithm Specification
2. Analysis of HiMQ-3 with respect to Known Attacks
3. Existential Unforgeability of HiMQ-3
4. Description of the Expected Security Strength of HiMQ-3
5. A Family of HiMQ-3: HiMQ-3F and HiMQ-3P
6. Performance Analysis
7. A Statement of Advantages and Limitations

1 Algorithm Specification

1.1 General Structure of MQ-Signature Schemes

We first describe a general structure of multivariate quadratic (MQ)-signature schemes. Let $\mathbb{F}_q$ be a finite field with elements q.

- A system $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$ of multivariate quadratic polynomials with m equations and n variables is defined by

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

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

- A main idea for the construction of MQ-signature schemes is to choose a system $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ (called a central map) of m multivariate quadratic polynomials in n variables which can be easily inverted.

- After that one chooses two affine or linear invertible maps $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to hide the structure of the central map $\mathcal{F}$ in a public key.

- A public key is the composed quadratic map $\mathcal{P} = S \circ \mathcal{F} \circ T$ which is supposed to be hardly distinguishable from a random system and therefore be difficult to invert.

- A secret key consists of $(S, \mathcal{F}, T)$ which allows to invert $\mathcal{P}$.

Signature generation and verification of the MQ-signature scheme are depicted in Fig. 1.

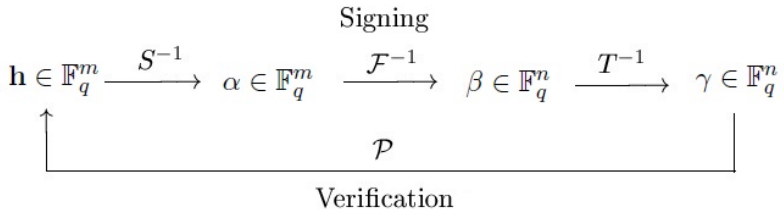

Figure 1: Signing and Verification of MQ-Signature Schemes.

1.2 Building Blocks

In general, if we can find a system of multivariate quadratic equations solvable in an efficient way, then we can construct an MQ-signature scheme. Now, we use a very simple solvable quadratic system.

A Solvable System of Quadratic Equations: Suppose that $char(\mathbb{F}_q) = 2$ and l is odd. We use a special system of quadratic equations $\mathcal{Q}$ defined by

$$\mathcal{Q} : \alpha_1 x_1 x_2 = \beta_1, \quad \alpha_2 x_2 x_3 = \beta_2, \cdots, \quad \alpha_l x_l x_1 = \beta_l,$$

where α_i and β_i are non-zero elements of $\mathbb{F}_q$. We need the following Lemma to find a solution $(x_1, \cdots, x_l)$ of $\mathcal{Q}$.

Lemma 1. Let l be an odd number and $char(\mathbb{F}_q) = 2$. Let $A = \prod_{i=1}^{l} X_i$, $B = \prod_{i=1}^{l} x_i$ and $C = \prod_{i:even} X_i = \prod_{i=2}^{l} x_i$, where $X_i = x_i x_{i+1}$ for $i = 1, \cdots, l-1$ and $X_l = x_l x_1$. Suppose that $B \neq 0$. Then the quadratic system $\mathcal{Q}$ has a unique solution $(x_1, \cdots, x_l)$ from the given $(X_1, \cdots, X_l)$, where x_i is given by

$$x_i = \begin{cases} B/C, & i = 1 \\ X_{i-1}/x_{i-1}, & i = 2, \cdots l-1 \\ X_i/x_1, & i = l. \end{cases}$$

Proof. We observe that $A = \prod_{i=1}^{l} X_i = B^2$, so $B = \prod_{i=1}^{l} x_i = \sqrt{A}$. Thus, we get $x_1 = B/C$ since $B \neq 0$, and then $x_i = X_i/x_{i-1}$, recursively for $i = 2, \cdots l-1$, and $x_l = X_l/x_1$. □

A Central Map. For a new MQ-signature scheme, we need the following four index sets as

$$V = \{1, \cdots, v\},\ O_1 = \{v+1, \cdots, v+o_1\},\ O_2 = \{v+o_1+1, \cdots, v+o_1+o_2\},$$
$$O_3 = \{v+o_1+o_2+1, \cdots, v+o_1+o_2+o_3\},$$

where $|V| = v$ and $|O_i| = o_i$, for $i = 1, 2, 3$. Let $v_i = v_{i-1} + o_i$ for $i = 1, 2$, where $v_0 = v$. A secret central map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$, a system of multivariate quadratic polynomials with $m = o_1 + o_2 + o_3$ equations and $n = v + m$ variables, is defined by

$$\begin{cases} \mathcal{F}^{(1)}(\mathbf{x}) = \Phi_1(\mathbf{x}) + \delta_1 x_{v+1} x_{v+2}, \\ \mathcal{F}^{(2)}(\mathbf{x}) = \Phi_2(\mathbf{x}) + \delta_2 x_{v+2} x_{v+3}, \\ \qquad \vdots \\ \mathcal{F}^{(o_1)}(\mathbf{x}) = \Phi_{o_1}(\mathbf{x}) + \delta_{o_1} x_{v+o_1} x_{v+1}, \end{cases}$$
$$\begin{cases} \mathcal{F}^{(o_1+1)}(\mathbf{x}) = \Psi_1(\mathbf{x}) + \delta_{o_1+1} x_{v_1+1} x_{v_1+2}, \\ \mathcal{F}^{(o_1+2)}(\mathbf{x}) = \Psi_2(\mathbf{x}) + +\delta_{o_1+2} x_{v_1+2} x_{v_1+3}, \\ \qquad \vdots \\ \mathcal{F}^{(o_1+o_2)}(\mathbf{x}) = \Psi_{o_2}(\mathbf{x}) + \delta_{o_1+o_2} x_{v_1+o_2} x_{v_1+1}, \end{cases}$$
$$\begin{cases} \mathcal{F}^{(o_1+o_2+1)}(\mathbf{x}) = \sum_{v+1 \le i \le j \le v_1} \beta_{i,j}^{(1)} x_i x_j + \Theta_1(\mathbf{x}) + \Theta_1'(\mathbf{x}) + \epsilon_1 x_{o_1+o_2+1}, \\ \qquad \vdots \\ \mathcal{F}^{(o_1+o_2+o_3)}(\mathbf{x}) = \sum_{v+1 \le i \le j \le v_1} \beta_{i,j}^{(o_3)} x_i x_j + \Theta_{o_3}(\mathbf{x}) + \Theta_{o_3}'(\mathbf{x}) + \epsilon_{o_3} x_{o_1+o_2+o_3}, \end{cases}$$

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

- $\Phi_i(\mathbf{x})$ $(i = 1, \cdots, o_1)$ is a quadratic equation in variables $(x_1, \cdots, x_v)$ defined by

$$\Phi_i(\mathbf{x}) = \sum_{j=1}^{v} \alpha_{i,j} x_j x_{1+(i+j-1)(\mathrm{mod}\ v)}$$

so that all the quadratic terms in $\Phi_i(\mathbf{x})$ don't overlap with those in $\Phi_j(\mathbf{x})$ for $i \neq j$ in the first layer and the $v \times v$ part of the symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ given in Fig. 1 has rank v for $i = 1, \cdots, o_1$, where $\alpha_{i,j} \in_R \mathbb{F}_q^*$.

- We choose random nonzero $\delta_i \in \mathbb{F}_q^*$ for $i = 1, \cdots, o_1$ such that an $o_1 \times o_1$ matrix Δ_1 is invertible, where

$$\Delta_1 = \begin{pmatrix} \delta_1 & \cdots & \cdots & 0 \\ 0 & \delta_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \delta_{o_1} \end{pmatrix}, \quad \Delta_1^{-1} = \begin{pmatrix} \delta'_1 & \cdots & \cdots & 0 \\ 0 & \delta'_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \delta'_{o_1} \end{pmatrix},$$

and $\delta'_i = \delta_i^{-1}$. The related part of δ_i in the first layer is written as

$$\begin{pmatrix} \mathcal{F}^{(1)}(\mathbf{x}) - \Phi_1(\mathbf{x}) \\ \mathcal{F}^{(2)}(\mathbf{x}) - \Phi_2(\mathbf{x}) \\ \cdots \\ \mathcal{F}^{(o_1)}(\mathbf{x}) - \Phi_{o_1}(\mathbf{x}) \end{pmatrix} = \Delta_1 \cdot \begin{pmatrix} x_{v+1}x_{v+2} \\ x_{v+2}x_{v+3} \\ \cdots \\ x_{v+o_1}x_{v+1} \end{pmatrix}.$$

- In the second layer, $\Psi_i(\mathbf{x})$ $(i = 1, \cdots, o_2)$ is a quadratic equation in variables $(x_1, \cdots, x_{v+o_1})$ defined by

$$\Psi_i(\mathbf{x}) = \sum_{j=1}^{v} \alpha'_{i,j} x_j x_{v+(i+j-1)(\mathrm{mod}\ o_1)},$$

so that all the quadratic terms of $\Psi_i(\mathbf{x})$ don't overlap with those of $\Psi_j(\mathbf{x})$ for $i \neq j$ in the second layer and the $v \times o_1$ part of the symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ given in Fig. 1 has rank $2o_1$ for $i = 1, \cdots, o_2$, where $\alpha'_{i,j} \in_R \mathbb{F}_q^*$.

- We choose random nonzero $\delta_{o_1+i} \in \mathbb{F}_q^*$ for $i = 1, \cdots, o_2$ such that an $o_2 \times o_2$ matrix Δ_2 is invertible, where

$$\Delta_2 = \begin{pmatrix} \delta_{o_1+1} & \cdots & \cdots & 0 \\ 0 & \delta_{o_1+2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \delta_{o_1+o_2} \end{pmatrix}, \quad \Delta_2^{-1} = \begin{pmatrix} \delta'_{o_1+1} & \cdots & \cdots & 0 \\ 0 & \delta'_{o_1+2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \delta'_{o_1+o_2} \end{pmatrix},$$

and $\delta'_{o_1+i} = \delta_{o_1+i}^{-1}$. The related part of δ_{o_1+i} in the second layer is written as

$$\begin{pmatrix} \mathcal{F}^{(o_1+1)}(\mathbf{x}) - \Psi_1(\mathbf{x}) \\ \mathcal{F}^{(o_1+2)}(\mathbf{x}) - \Psi_2(\mathbf{x}) \\ \cdots \\ \mathcal{F}^{(o_1+o_2)}(\mathbf{x}) - \Psi_{o_1}(\mathbf{x}) \end{pmatrix} = \Delta_2 \cdot \begin{pmatrix} x_{v_1+1}x_{v_1+2} \\ x_{v_1+2}x_{v_1+3} \\ \cdots \\ x_{v_1+o_2}x_{v_1+1} \end{pmatrix}.$$

- In the third layer, we choose $\beta_{i,j}^{(k)} \in \mathbb{F}_q$ for $\sum_{v+1 \leq i \leq j \leq v_1} \beta_{i,j}^{(k)} x_i x_j$ for $k = 1, \cdots, o_3$ in $\mathcal{F}^{(l)}$ for $l = o_1 + o_2 + 1, \cdots, m$.

- $\Theta_i(\mathbf{x})$ and $\Theta'_i(\mathbf{x})$ $(i = 1, \cdots, o_3)$ are quadratic equations in variables $(x_1, \cdots, x_n)$ defined by

$$\Theta_i(\mathbf{x}) = \sum_{j=1}^{v_1} \gamma_{i,j} x_i x_{v_1+(i+j-1)(\mathrm{mod}\ o_3)}, \quad \Theta'_i(\mathbf{x}) = \sum_{j=1}^{v_2} \gamma'_{i,j} x_i x_{v_2+(i+j-1)(\mathrm{mod}\ o_3)},$$

  so that all the quadratic terms in $\Theta_i(\mathbf{x})$ and $\Theta'_i(\mathbf{x})$ $(i = 1, \cdots, o_3)$ in the third layer don't overlap and the symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ has full rank for $i = o_1 + o_2 + 1, \cdots, m$, where $\gamma_{i,j}, \gamma'_{i,j} \in_R \mathbb{F}_q^*$.

- To satisfy the above conditions, the parameter $(\mathbb{F}_q, v, o_1, o_2, o_3)$ is guaranteed to be selected as $v \geq o_1 + 1$ and $o_1 \geq o_2 \geq o_3$.

- Lastly, we choose random $\epsilon_i \in \mathbb{F}_q^*$ for the linear part of $\mathcal{F}^{(i)}$ $(i = o_1 + o_2 + o_3, \cdots, m)$.

Note that a similar construction using l-cycles in the mixed field case in [16] was proposed, but it was also broken by key recovery attacks [24]. We will show that our combination of solvable quadratic systems and the third layer with full rank allow us to construct more efficient and secure MQ-signature schemes.

How to Invert the Central Map. Given $\xi = (\xi_1, \cdots, \xi_m)$, to compute $\mathcal{F}^{-1}(\xi) = \mathbf{s}$, i.e., to find $\mathbf{s}$ such that $\mathcal{F}(\mathbf{x}) = \xi$.

- In the first layer, choose a random vector of Vinegar values $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$, plug $\mathbf{s_v} = (s_1, \ldots, s_v)$ into the polynomials $\mathcal{F}^{(i)}$ $(1 \leq i \leq o_1)$ and get a quadratic system of o_1 equations with o_1 variables as

$$\begin{cases} \delta_1 x_{v+1} x_{v+2} = \xi_1 - \Phi_1(\mathbf{s_v}), \\ \qquad\qquad \vdots \\ \delta_{o_1} x_{v+o_1} x_{v+1} = \xi_{o_1} - \Phi_{o_1}(\mathbf{s_v}). \end{cases}$$

  Find a solution $(s_{v+1}, \cdots, s_{v+o_1})$ by using Lemma 1. If $\xi_i - \Phi_i(\mathbf{s_v}) = 0$ then choose another Vinegar values $\mathbf{s}'_v = (s'_1, \cdots, s'_v)$ and try again.

- In the second layer, plug $(s_1, \ldots, s_{v+o_1})$ into the polynomials $\mathcal{F}^{(i)}$ $(o_1 + 1 \leq i \leq o_1 + o_2)$ and get a solution $(s_{v+o_1+1}, \cdots, s_{v+o_1+o_2})$ as in the first layer.

- In the third layer, plug $(s_1, \ldots, s_{v+o_1+o_2})$ into the polynomials $\mathcal{F}^{(i)}$ $(o_1+o_2+1 \leq i \leq m)$ and get a linear system of o_3 equations with o_3 variables. Find a solution $(s_{v+o_1+o_2+1}, \cdots, s_n)$ by solving the linear system from Gaussian elimination. Then $\mathbf{s} = (s_1, \cdots, s_n)$ is a solution of $\mathcal{F}(\mathbf{x}) = \xi$. If the linear system is not solvable then choose another Vinegar values $\mathbf{s}'_v = (s'_1, \cdots, s'_v)$ and try again.

1.3 HiMQ-3

Now, we specify our MQ-signature scheme with the three layers, HiMQ-3, based on our central map.

■ **High Speed MQ-Signature Scheme: HiMQ-3**

- **KeyGen**(1^λ). For a security parameter λ, generate a public/secret key pair $< PK, SK >=< \mathcal{P}, (\widetilde{S}, \mathcal{F} = (\Phi, \delta, \Psi, \Theta, R), \widetilde{T}) >$ as
  - Choose randomly two affine maps $\widetilde{S}$ and $\widetilde{T}$. If neither $\widetilde{S}$ nor $\widetilde{T}$ is invertible then choose again, where $\widetilde{S} = S^{-1}$ and $\widetilde{T} = T^{-1}$
  - Choose randomly $\Phi = (\Phi_1, \cdots, \Phi_{o_1})$, $\delta = (\delta'_1, \cdots, \delta'_{o_1+o_2})$, $\Psi = (\Psi_1, \cdots, \Psi_{o_2})$, $\Theta = (\Theta_1, \cdots, \Theta_{o_3}, \Theta'_1, \cdots, \Theta'_{o_3})$ and $R = \{\beta_{i,j}^{(k)}, \epsilon_k\}_{k=1}^{o_3})$ for the central map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$ so that they satisfy the conditions specified in the construction of the central map.
  - Compute $\mathcal{P}$ from $\mathcal{P} = S \circ \mathcal{F} \circ T$.
- **Sign**$(SK, \mathtt{m})$. Given a message $\mathtt{m}$,
  - Compute $h(\mathtt{m})$ and $\widetilde{S}(h(\mathtt{m})) = \xi$, where $\xi = (\xi_1, \cdots, \xi_m)$.
  - To compute $\mathcal{F}^{-1}(\xi) = \mathbf{s}$, i.e., to find $\mathbf{s}$ such that $\mathcal{F}(\mathbf{s}) = \xi$,
    * Choose a random vector of Vinegar values $\mathbf{s_v} = (s_1, \cdots, s_v)$. After plugging $\mathbf{s_v}$ into $\mathcal{F}^{(i)}$ for $i = 1, \cdots, o_1$, get a quadratic system of o_1 equations with o_1 variables and compute the following matrix multiplication
$$\begin{pmatrix} x_{v+1}x_{v+2} \\ x_{v+2}x_{v+3} \\ \cdots \\ x_{v+o_1}x_{v+1} \end{pmatrix} = \Delta^{-1} \cdot \begin{pmatrix} \xi_1 - \Phi_1(\mathbf{s_v}) \\ \xi_2 - \Phi_2(\mathbf{s_v}) \\ \cdots \\ \xi_{o_1} - \Phi_{o_1}(\mathbf{s_v}) \end{pmatrix}.$$
      By using Lemma 1, find a solution $(s_{v+1}, \cdots, s_{v+o_1})$.
    * After plugging $(s_1, \cdots, s_{v+o_1})$ into $\mathcal{F}^{(i)}$ for $i = o_1 + 1, \cdots, o_1 + o_2$, get a solution $(s_{v+o_1+1}, \cdots, s_{v+o_1+o_2})$ by using the same way in the first layer.
    * After plugging $(s_1, \cdots, s_{v+o_1+o_2})$ into $\mathcal{F}^{(i)}$ for $i = o_1 + o_2 + 1, \cdots, m$, get a solution $(s_{v+o_1+o_2+1}, \cdots, s_{v+m})$ by solving a linear system of o_3 equations with o_3 variables. Then $\mathbf{s} = (s_1, \cdots, s_n)$ is a solution of $\mathcal{F}(\mathbf{x}) = \xi$.
  - Compute $\widetilde{T}(\mathbf{s}) = \tau$. Then τ is a signature of $\mathtt{m}$.
- **Verify**$(PK, \mathtt{m}, \tau)$ Given a signature τ on $\mathtt{m}$ and a public key $\mathcal{P}$, check $\mathcal{P}(\tau) = h(\mathtt{m})$. If it holds, accept τ, otherwise, reject it.

Remark. 1. In signing, HiMQ-3 requires only one Gaussian Elimination in the third layer.
2. We explain how the public key and secret key sizes of HiMQ-3 are calculated.

- The public key requires $\dfrac{m(n+1)(n+2)}{2}$ field elements.
- The secret maps S and T require $m(m+1)$ and $n(n+1)$ field elements, respectively. In first layer, it requires $v+1$ field elements for each polynomial. In second layer, it requires $v+1$ field elements for each polynomial. In the third layer, v_1o_2 and v_2o_3 field elements for Θ and Θ', respectively, and $\dfrac{o_3o_1(o_1+3)}{2}$ for the other parts. Thus, the secret key requires
$$\frac{o_1o_3(o_1+3)}{2} + (v+1)(o_1+o_2) + v_1o_2 + v_2o_3 + m(m+1) + n(n+1)$$
field elements.

2 Analysis of HiMQ-3 with respect to Known Attacks

Here, we provide security analysis of HiMQ-3 against all the known attacks. The security of all MQ-schemes in the MQ+IP paradigm is not only based on the MQ-Problem, but also on some variant of the Isomorphism of Polynomials (IP) problem. Furthermore, layered MQ-signature schemes requires the hardness of the MinRank problem. The underlying problems are defined as follows:

- **Polynomial System Solving (PoSSo) Problem:** Given a system $\mathcal{P} = (P^{(1)}, \cdots, P^{(m)})$ of m nonlinear polynomial equations defined over $\mathbb{F}_q$ with degree of d in variables $x_1, \cdots, x_n$ and $\mathbf{y} = (y_1, \cdots, y_m) \in \mathbb{F}_q^m$, find values $(x'_1, \cdots, x'_n) \in \mathbb{F}_q^n$ such that $P^{(1)}(x'_1, \cdots, x'_n) = y_1, \cdots, P^{(m)}(x'_1, \cdots, x'_n) = y_m$.
- **EIP (Extended Isomorphism of Polynomials) Problem:** Given a nonlinear multivariate system $\mathcal{P}$ such that $\mathcal{P} = S \circ \mathcal{F} \circ T$ for linear or affine maps S and T, and $\mathcal{F}$ belonging to a special class of nonlinear polynomial system $\mathcal{C}$, find a decomposition of $\mathcal{P}$ such that $\mathcal{P} = S' \circ \mathcal{F}' \circ T'$ for linear or affine maps S' and T', and $\mathcal{F}' \in \mathcal{C}$.
- **MinRank Problem:** Let $m, n, r, k \in \mathbb{N}$ and $r, m < n$. The MinRank(r) problem is, given $(M_1, \cdots, M_l) \in \mathbb{F}_q^{m \times n}$, find a non-zero k-tuple $(\lambda_1, \cdots, \lambda_k) \in \mathbb{F}_q^k$ such that $Rank(\sum_{i=1}^{k} \lambda_i M_i) \leq r$.

The PoSSo problem is proven to be NP-complete [25]. For efficiency, MQ-PKC restrict to quadratic polynomials. The PoSSo problem with all polynomials $P^{(1)}, \cdots, P^{(m)}$ of degree 2 is called the MQ-Problem for multivariate quadratic. The IP-problem was first described by Patarin at Eurocrypt'96 [38], there is not much known about the difficulty of the IP-problem in contrast to the MQ-problem. The problem of finding a low rank linear combination of matrices was originally introduced in [45] as one of the natural questions in linear algebra, and the authors proved its NP-completeness.

A feature of MQ-schemes in the MQ+IP paradigm is that there exist a large number of different secret keys corresponding to a public key [49]. Suppose that $< \mathcal{P}, (S, \mathcal{F}, T) >$ is a public/secret key pair of an MQ-scheme. Then we call $(S', \mathcal{F}', T')$ is an equivalent key of $(S, \mathcal{F}, T)$ if $\mathcal{P} = S \circ \mathcal{F} \circ T = S' \circ \mathcal{F}' \circ T'$, where S' and T' are invertible affine maps, and $\mathcal{F}'$ preserves all zero coefficients of $\mathcal{F}$. Concept of equivalent keys plays a major role in the cryptanalysis of MQ-schemes. If an attacker can find any of the equivalent keys then he can forge signatures on any messages. Thus, the attacker tires to find equivalent keys with a simple structure. Known attacks can be divided into the following classes:

- **Direct Attack.** Given a public key $\mathcal{P}$ and $\mathbf{y} \in \mathbb{F}_q^m$, find a solution $\mathbf{x} \in \mathbb{F}_q^n$ of $\mathcal{P}(\mathbf{x}) = \mathbf{y}$.
- **Key Recovery Attack (KRA) using Equivalent keys and Good Keys.** Given $\mathcal{P} = S \circ \mathcal{F} \circ T$, find equivalent keys $(S', \mathcal{F}', T')$ of $(S, \mathcal{F}, T)$ s.t. $\mathcal{P} = S \circ \mathcal{F} \circ T = S' \circ \mathcal{F}' \circ T'$.
- **Rank-based Attacks.** Find linear combinations associated matrices at some given rank, nontrivial invariant subspaces of linear combinations associated matrices and so on: MinRank attack, HighRank attack, Kipnis-Shamir attack.

2.1 Direct Attacks

An attacker mounting direct attacks tries to find a solution $\mathbf{x} \in \mathbb{F}_q^n$ of $\mathcal{P}(\mathbf{x}) = \mathbf{y}$. For it, the attacker use algorithms like XL and Gröbner basis algorithms such as Buchberger, F4 and F5 for solving the MQ-problem. Complexity of the MQ-Problem is determined by that of HybridF5 (HF5) algorithm [7] which is currently the fastest algorithm to solve the problem. The basic idea is to guess some of the variables to create overdetermined systems before applying Faugère's F5 algorithm [21]. When doing so, one has to run F5 algorithm several times to find a solution of the original system. When guessing k variables over $\mathbb{F}_q$, this number is given by q^k. Complexity of solving a semi-regular (random) system of m quadratic equations in n variables over $\mathbb{F}_q$ by HF5 algorithm can be estimated as

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

where the degree of regularity d_{reg} is the index of the first non-positive coefficient in the $S_{m,n} = \frac{(1-z^2)^m}{(1-z)^n}$ and $2 \leq \alpha \leq 3$ is the linear algebra constant of solving a linear system. The internal equations used by HF5 are very sparse and thus $\alpha = 2$ can be used to obtain a lower bound on the complexity. If we really want to break a scheme, we either calculate the correct α or use $\alpha = 2.8$ as an upper bound [48].

To analyze the security of HiMQ-3 against the direct attacks, we perform a number of experiments using F4 algorithm (the details of F5 algorithm are not publicly known) with MAGMA v2.19-10 on Intel Core i5-6600 3.3 GHz. We compare experimental results of solving quadratic systems derived from a public key of HiMQ-3 with random quadratic systems on $\mathbb{F}_{2^8}$ 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. It is an evidence that our system behave like random ones, i.e., we can use the estimation of complexity of solving a random system of m quadratic equations in n variables over $\mathbb{F}_q$ by HF5.

(v, o_1, o_2, o_3)	(7,3,3,2)	(7,3,3,3)	(9,3,3,3)	(11,5,3,2)	(11,5,4,3)	(11,5,4,4)	(11,5,5,4)
Random System	0.415	0.620	0.618	3.003	112.861	639.576	5753.369
HiMQ-3	0.134	0.593	0.57	3.203	109.823	756	5712.19

Table 1. Running Time (Second) for Solving Two Types of Quadratic Systems over $\mathbb{F}_{2^8}$.

Using HF5 algorithm ($\alpha = 2$), we summarize the lower bounds of the numbers of equations (m) for solving determined systems defined over $\mathbb{F}_{2^8}$ required to achieve given security levels in Table 2. It will be used to select a secure parameter of HiMQ-3 against the direct attacks for a given security level λ.

λ	80	96	128	160	192	256
m	26	31	43	55	68	93

Table 2. Lower Bounds of the Numbers of Quadratic Equations for Determined Systems over $\mathbb{F}_{2^8}$ at Each Security Level.

2.2 Key Recovery Attacks

Key recovery attacks (KRAs) exploit the special structure of the central map, i.e., zero entries at certain known places, to obtain equations with variables in S and T. A first improvement of the complexity of solving the above system can be achieved by using equivalent keys. If we can find an equivalent key (S', T') then we have to solve a large structured system of quadratic equations in many unknowns to recover (S', T') by reducing the number of variables. Complexity of solving such systems heavily relies on the number of unknowns and thus we would like to reduce them further.

The KRAs on UOV signature scheme were presented as Reconcilation attacks [17]. In 2008, Ding *et al.* [17] presented Rainbow Band Separation (RBS) attacks on Rainbow signature scheme. Later, Thomae [48] applied the attacks to other MQ-schemes using the concept of good keys which is a generalization of the RBS attacks. In our central map, it significantly increases quadratic terms with zero coefficients due to the use of sparse polynomials. Thus, the security of our scheme with these increased quadratic terms with zero coefficients against KRAs should be guaranteed. Now, we analyze security of HiMQ-3 against KRAs using equivalent keys and good keys.

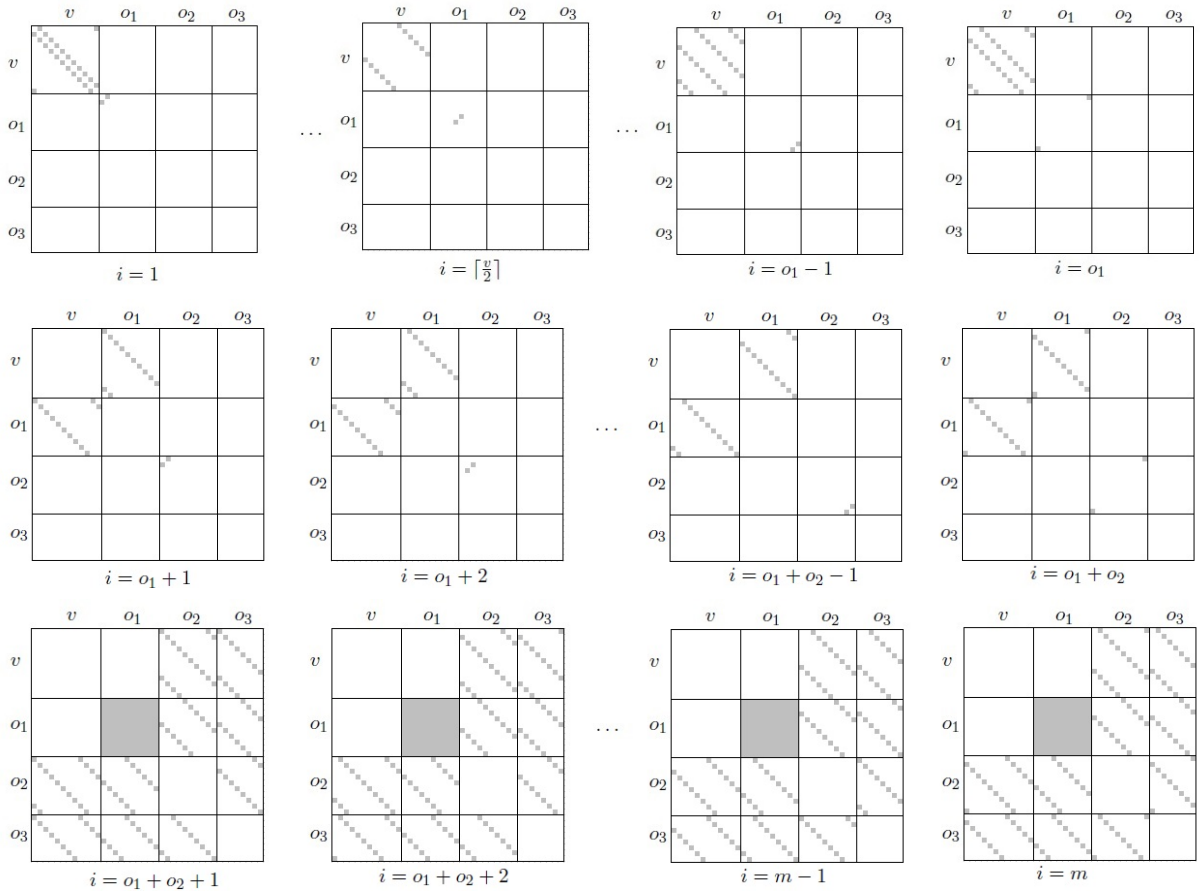

Figure 2: Symmetric Matrices associated to the Quadratic Parts of $\mathcal{F}$ for HiMQ-3.

KRAs on HiMQ-3. Let $F^{(k)}$ $(1 \leq k \leq m)$ be symmetric matrices associated to the homogeneous quadratic part of the k-th component of the central map $\mathcal{F}$. The matrices $F^{(k)}$ are depicted in Fig. 2, where white parts denote zero entries and gray parts denote arbitrary entries. Analogously, let $P^{(k)}$ $(1 \leq k \leq m)$ be symmetric matrices representing the quadratic part of the k-th component of the public key $\mathcal{P}$. Due to the structure of the secret map $\mathcal{F}$, we know that certain coefficients in $\mathcal{F}^{(k)}$ are systematically zero. Since $\mathcal{P} = S \circ \mathcal{F} \circ T$, we get $\mathcal{F} = \widetilde{S} \circ \mathcal{P} \circ \widetilde{T}$, where $\widetilde{S} = S^{-1}$ and $\widetilde{T} = T^{-1}$. From this, we get the following equality:

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

The corresponding system of equations is:

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

for some coefficients $c_{yz}^{(x)}$, as we have already known that $f_{ij}^{(k)} = 0$ for some i, j, k by construction of $\mathcal{F}$. Since the number of equations obtained by (1) equals the number of zeros in all the $\mathcal{F}^{(k)}$, we get $\frac{mn(n+1) - o_1 o_3(o_1+1)}{2} - (o_1+o_2)(v+1) - o_2(v+o_1) - o_3(n-o_3)$ cubic equations. The number of variables in $\widetilde{S}$ and $\widetilde{T}$ is $n^2 + m^2$. The complexity of solving such a system using HF5 is very large.

KRAs using Equivalent Keys on HiMQ-3. To improve this complexity, we use the concept of equivalent keys [49]. Let $\mathbb{GL}_m(\mathbb{F}_q)$ be a general linear group of degree n over $\mathbb{F}_q$.

Definition 1. **[Equivalent Key]** Let $S, S' \in \mathbb{GL}_m(\mathbb{F}_q)$ and $T, T' \in \mathbb{GL}_n(\mathbb{F}_q)$ and $\mathcal{F}, \mathcal{F}' \in \mathbb{F}_q[x_1, ..., x_n]^m$. We say that $(\mathcal{F}, S, T)$ is *equivalent* to $(\mathcal{F}', S', T')$ if and only if $S \circ \mathcal{F} \circ T = S' \circ \mathcal{F}' \circ T'$ and $\mathcal{F}|_I = \mathcal{F}'|_I$, that is, $\mathcal{F}$ and $\mathcal{F}'$ share the same structure when restricted to a fixed index set $I = \{I^{(1)}, \cdots I^{(m)}\}$.

When $(S, \mathcal{F}, T)$ is a secret key corresponding to the public key $\mathcal{P}$, i.e., $\mathcal{P} = S \circ \mathcal{F} \circ T$, we call S' and T' equivalent keys if $S \circ \mathcal{F} \circ T = \mathcal{P} = S' \circ \mathcal{F}' \circ T'$, where $\mathcal{F}'$ preserves all systematic zero coefficients of $\mathcal{F}$. Thus, an attacker who has any of equivalent keys can forge signatures on any messages. If we can find simpler equivalent keys, we can reduce the number of variables in S and T. If there are two invertible linear maps $\Sigma \in \mathbb{GL}_m(\mathbb{F}_q)$ and $\Omega \in \mathbb{GL}_n(\mathbb{F}_q)$ such that

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

and $\mathcal{F}$ and $\mathcal{F}'(= \Sigma \circ \mathcal{F} \circ \Omega)$ have the same structure, then S' and T' are equivalent keys, where $S' = S \circ \Sigma^{-1}$ and $T' = \Omega^{-1} \circ T$ ($\widetilde{S}' = \Sigma \circ \widetilde{S}$ and $\widetilde{T}' = \widetilde{T} \circ \Omega$).

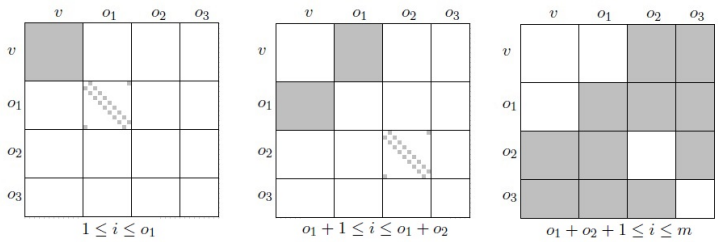

Figure 3: Generalized version of Quadratic Parts of the Central Map for HiMQ-3.

To find simpler equivalent keys, we consider the generalized version of our central map, $\overline{\mathcal{F}}^{(k)}$ for $1 \leq k \leq m$, given in Fig. 3.

Lemma 2. For the generalized central map given in Fig. 3, we can find equivalent keys S' and T' of the form given in Fig. 4 with high probability, where gray parts denote arbitrary entries and white parts denote zero entries and there are ones at the diagonal.

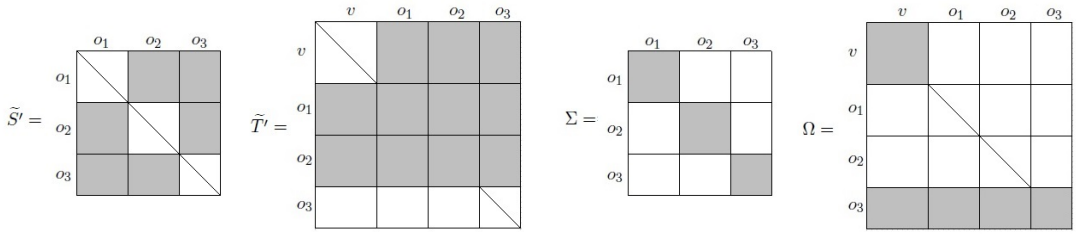

Figure 4: Equivalent Key of HiMQ-3.

Proof. As in [48], we can find Σ and Ω given in Fig. 4 with high probability. Then there exist equivalent keys (S', T') of the form given in Fig. 4. □

From the equivalent keys given in Fig. 4, we get a system of

$$\frac{mn(n+1) - o_1 v(v+1) - o_1 o_3(o_1+1)}{2} - o_2(vo_1 + o_2(v+o_1)) - o_1^2 - o_2^2 - o_3^2(n-o_3)$$

cubic equations and with $n(n-o_3) + m^2 - (v^2 + o_1^2 + o_2^2 + o_3^2)$ variables. However, complexity of solving such a system is still large: for $\text{HiMQ}(\mathbb{F}_q, v_1, o_1, o_2, o_3) = (\mathbb{F}_{2^8}, 31, 15, 15, 14)$, lower bound on the complexity of solving the system by HF5 is 2^{3330}.

KRAs using Good Keys on HiMQ-3. To further decrease this complexity, we use the notion of good keys which is a generalization of equivalent keys. Good keys don't preserve all the zero coefficients of $\mathcal{F}$, but just some of them. Hence, we can choose Σ and Ω more widely and further reduce the number of variables.

Definition 2. [Good Key] Let $S, S'' \in \mathbb{GL}_n(\mathbb{F}_q)$ and $T, T'' \in \mathbb{GL}_m(\mathbb{F}_q)$ and $\mathcal{F}, \mathcal{F}'' \in \mathbb{F}_q[x_1, ..., x_n]^m$, and $J = \{J^{(1)}, \cdots, J^{(m)}\} \subset I = \{I^{(1)}, \cdots, I^{(m)}\}$ for all k with at least one $J^{(k)} \neq \phi$. We say that $(\mathcal{F}'', S'', T'')$ is a *good key* for $(\mathcal{F}, S, T)$ if and only if $S \circ \mathcal{F} \circ T = S'' \circ \mathcal{F}'' \circ T''$ and $\mathcal{F}|_J = \mathcal{F}''|_J$.

Lemma 3. Let S' and T' be equivalent keys for HiMQ-3 of the form given in Fig. 4. Then there are good keys S'' and T'' of the form given in Fig. 5. Only the last column of $\widetilde{T''}$ contains arbitrary values in the first $v + o_1 + o_2$ rows, which are equal to the corresponding values in $\widetilde{T'}$. Respectively, only $o_2 + o_3$ values of the o_1-th row of $\widetilde{S''}$ contain arbitrary values, which are equal to the corresponding values in $\widetilde{S'}$.

Proof. We can find Σ' and Ω' given in Fig. 5 with high probability. Then there exist equivalent keys (S', T') of the form given in Fig. 5. □

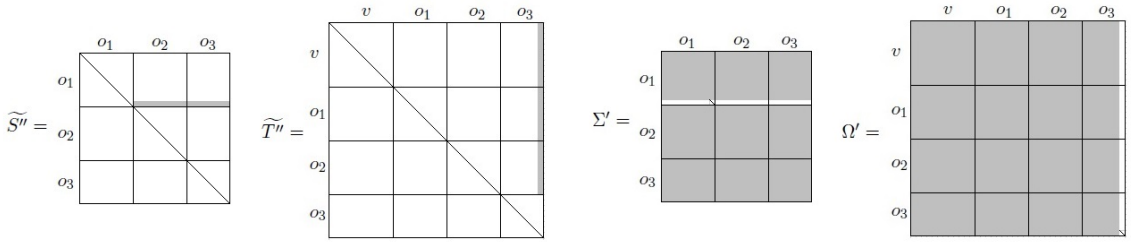

Figure 5: Good Keys of HiMQ-3.

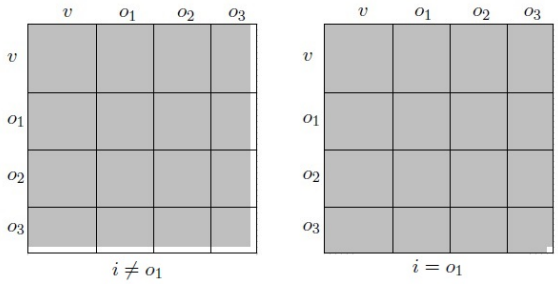

Figure 6: Quadratic Parts of $\mathcal{F}''^{(i)}$.

Finally, we get the central map $\mathcal{F}''$ in Fig. 6 after applying the transformations Σ' and Ω'. Thus, we obtain the following Theorem.

Theorem 1. The main complexity of the key recovery attack using good keys on HiMQ-3 is determined by solving $n-1$ bihomogeneous equations and m quadratic equations with $n + \min(o_1, o_2)$ variables.

After obtaining one column of T' and one row of S', all the other parts of T' and S' are revealed by linear equations as in [48]. Consequently, we recover the equivalent keys T' and S'.

In Rainbow, complexity of the KRAs with good keys is determined by solving $n-1$ bihomogeneous equations and m quadratic equations with n variables. In our scheme, since the number of variables for solving the resulting system is increased, it allows us to select the number of variables, n, less than that of Rainbow to achieve the same security level.

HiMQ-3	# of Equations	# of Variables	d_{reg}	Complexity
KRAs	115,223(Cubic)	7,325	494	2^{5337}
KRAs with Equi. Keys	82,498(Cubic)	4,711	304	2^{3330}
KRAs with Good Keys	116(Quad.)	88	21	2^{160}

Table 3. Lower-bound on the Complexity of the KRAs using Equivalent Keys and Good Keys for HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)

Table 3 shows improvements of lower bounds ($\alpha = 2$) on the complexities of solving the resulting systems by HF5 achieved by the KRAs using equivalent keys and good keys for HiMQ($\mathbb{F}_{2^8}, 31, 15, 15, 14$). In general, only the number of variables is reduced, as we find simpler equivalent keys maintaining the number of equations. However, the number of equations in our KRAs with equivalent keys is also changed, as we use the equivalent keys for the generalized central map given in Fig. 2. The reason of the selection of this parameter will be presented in §4.

Key Recovery Attacks using linear part of $\mathcal{F}$. It is also known that some coefficients of linear terms in the central map are zero. This does not significantly affect the KRAs since the number of quadratic terms with zero coefficients is much larger than that of linear terms with zero coefficients. When we reduce the number of variables in good key recovery, we use Ω' where each coordinate function has at least $n-1$ linear terms (see Lemma 3). Even if $\mathcal{F}'^{(k)}$ has only one linear term for each k, $\mathcal{F}'^{(k)} \circ \Omega'$ has at least $n-1$ linear terms. However, we cannot replace the structure of Ω', because this attack depends on the number of variables more than the number of equations and this replacement may increase the number of variables and so complexity. Nevertheless, if there is no linear term in $\mathcal{F}$, we can get nm linear terms with zero coefficients of $\mathcal{F}' \circ \Omega'$ and n variables in constant part of $\widetilde{T''}$ by choosing Ω and Ω' carefully satisfying Lemma 2 and Lemma 3. Then we reset $\Sigma' = \left(\widetilde{S'}\right)^{-1} = S'$ so that the variables in $\widetilde{S''}$ are removed. Finally, we get a system of $(n+1)m$ quadratic equations with $n+v_1+o_1$ variables. If HiMQ-3 has no linear term in $\mathcal{F}$ then, for HiMQ($\mathbb{F}_{2^8}, 31, 15, 15, 14$), the complexity of solving this system by HF5 is 2^{61}. Thus, it must have a proper amount of linear terms.

2.3 MinRank attack

In MinRank attacks, one tries to find linear combinations $M = \sum_{i=1}^{m} \mu_i P^{(i)}$ of the matrices $P^{(i)}$, where M has a minimal rank r. Underlying idea of an algorithm to solve this MinRank problem [45] is to search for a vector lying in the kernel of the desired linear combination M. Complexity of the MinRank attack is determined by that of finding the linear combinations. We get the complexity of HiMQ-3 against the MinRank attack by using the technique in [8] as in Proposition 2.

Proposition 2. Complexity of HiMQ-3 against the MinRank attack is $o_1 \cdot q^{v-o_1+3}$.

Proof. In MinRank attacks, we must find a vector $v \in \mathbb{F}_q^n$ such that $v \in \ker P$, where P is a matrix with the minimal rank in Span$\{P^{(i)}\}$. The probability is the same as that of finding $v' \in \mathbb{F}_q^n$ such that $v' \in \ker Q$, where Q is a matrix with the minimal rank in Span$\{F^{(i)}\}$. Note that $F^{(i)} \cdot v'$ has at most $v_1 + 2$ non-zero component for a random vector v' and $i = 1, \cdots, o_1$. Let $w_i = Q_i \cdot v'$ for $i = 1, \cdots, o_1$. Then the probability that w_i are linearly dependent is

$$1 - \prod_{i=0}^{o_1-1} (1 - \frac{q^i}{q^{v_1+2}}) > 1/q^{v_1-o_1+3}$$

Note that $\sum_{i=1}^{o_1} \lambda_i F^{(i)}$ has minrank. Hence the probability of $v' \in \ker(\sum_{i=1}^{o_1} \lambda_i F^{(i)})$ for a random vector v' and non-trivial λ_i is $1/q^{v_1-o_1+3}$. By finding o_1 linear independent matrices $M = \sum_{i=1}^{m} \lambda_i P^{(i)}$, we can extract the first layer of HiMQ-3. This step costs approximately $o_1 \cdot q^{v-o_1+3}$ as in [41]. After separating all the layers of HiMQ-3, an attacker can generate its signatures. □

2.4 HighRank Attack

In HighRank attacks, one tries to identify the variables appearing the lowest number of times in the central polynomials. The variables $x_{v+o_1+o_2+1}, \cdots, x_n$ appear only in the quadratic terms of the central polynomials $(\mathcal{F}^{(o_1+o_2+1)}, \cdots, \mathcal{F}^{(o_1+o_2+o_3)})$ of the third layer of HiMQ-3. As in Rainbow [41], the complexity of HiMQ-3 against the HighRank attacks is determined by the

number of matrices with full rank in the third layer, thus, we get its complexity against the HighRank attacks is $q^{o_3} \cdot \frac{n^3}{6}$.

2.5 Kipnis-Shamir Attack

Kipnis-Shamir attack (UOV attack) [33] was originally used to break the balanced Oil and Vinegar signature scheme [39]. We consider the generalization to the unbalanced case. We first define four index sets as

$$D_1 = \{i | 1 \leq i \leq v\},\ D_2 = \{i | v+1 \leq i \leq v+o_1\},$$

$$D_3 = \{i | v+o_1+1 \leq i \leq v+o_1+o_2\},\ D_4 = \{i | v+o_1+o_2+1 \leq i \leq n\}.$$

Definition 3. We define meaningful two subspaces of $\mathbb{F}_q^n$ as

$$V_{0001} = \{(x_1, \cdots, x_n) | x_i = 0, i \notin D_4\},\ V_{1110} = \{(x_1, \cdots, x_n) | x_i = 0, i \in D_4\}.$$

The goal of the attack is to find the preimage of the above subspaces under an equivalent key T'. We use the following property: any linear combinations of the matrices $F^{(1)}, \cdots, F^{(m)}$ is of the form $\begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & P & 0 \end{pmatrix} \cdots (*)$ from Fig. 1. The following Theorems show why invariant subspaces exist with a certain probability.

Lemma 4. Let $\psi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a linear transformation of the form $(*)$. Then we get that $\psi(V_{0001})$ is a subspace of V_{1110}.

Note that $\psi(V) = \mathbb{F}_q^n$ for the other subspaces of $\mathbb{F}_q^n$ except V_{0001}.

Let $H = \sum_{i=1}^m \lambda_i F^{(i)}$ be a linear combination of the matrices $F^{(i)}$ associated to the quadratic part of the i-th central map. Note that H has the form of $(*)$. Then we get the following Theorem as in [33].

Theorem 2. Assume that, for some k $(1 \leq k \leq m)$, the matrix $F^{(k)}$ is invertible. Then, the map $(F^{(k)})^{-1} \cdot H$ has a nontrivial invariant subspace $\psi(V_{0001})$ with probability not less than $q^{-v-o_1-o_2+o_3}$.

Proof. They are obtained from the following facts: $[(F^{(k)})^{-1} \cdot F^{(i)}](V_{0001}) \subset (F^{(k)})^{-1}(V_{1110})$ and $V_{0001} \subset (F^{(k)})^{-1}(V_{1110})$, let $\Phi = (F^{(k)})^{-1} \cdot F^{(i)}$, then as in [32], we have

$$Pr[\Phi(V_{0001}) \subset V_{1110}] \geq q^{-v-o_1+o_2},$$

where $o_3 = dim(V_{0001})$ and $v+o_1+o_2 = dim(V_{1110})$. Thus, we get a nontrivial invariant subspace V_{0001} with probability not less than $q^{-v-o_1-o_2+o_3}$. □

Theorem 3. Let $W = \sum_{i=1}^m \lambda_i P^{(i)}$ be a linear combination of the matrices $P^{(i)}$ and let $P^{(k)}$ (for some k, $1 \leq k \leq m$) be invertible. Then the map $(P^{(k)})^{-1} \cdot W$ has a nontrivial invariant subspace V_{1110} which is a subspace of $T^{-1}(V_{1110})$ with probability not less than $q^{-v-o_1-o_2+o_3}$.

Proof. They are obtained from the Theorem 2 and the following:

$$(P^{(k)})^{-1} \cdot W = (P^{(k)})^{-1} \cdot \sum_{i=1}^{m} \lambda_i P^{(i)} = (T^T \cdot F^{(k)} \cdot T)^{-1} \cdot \sum_{i=1}^{m} \lambda_i \cdot (T^T \cdot F^{(i)} \cdot T)$$
$$= T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (F^{(k)})^{-1} \cdot F^{(i)}) \cdot T.$$
$$(P^{(k)})^{-1} \cdot W(T^{-1}(V_{0001})) = (T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (F^{(k)})^{-1} \cdot F^{(i)}) \cdot T)(T^{-1}(V_{0001}))$$
$$= T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (F^{(k)})^{-1} \cdot F^{(i)})(V_{0001}) \subset T^{-1}(V_{1110}).$$

Thus, we get a nontrivial invariant subspace V_{0001} with probability not less than $q^{-v-o_1-o_2+o_3}$. □

From Theorem 3, we get that the complexity of HiMQ-3 against the Kipnis-Shamir attacks is $q^{v+o_1+o_2-o_3}$.

2.6 Design Rationale

Now, we describe our design rationale for HiMQ-3. One may design a signature scheme using only the first layer of HiMQ-3 as a single-layer MQ-signature scheme. Suppose that HiMQ-1 is a single-layer signature scheme with only the first layer of HiMQ-3, where $n = v + o_1$ and $m = o_1$. Now, we demonstrate how such a single-layer structure affects the security of known cryptanalytic attacks. First, it is insecure against the HighRank attack identifying the variables appearing the lowest number of times in the central polynomials. The variables $x_{v+1}, \cdots, x_{v+o_1}$ appear only twice in the quadratic terms of the central polynomials. Thus, the HighRank attack is successful since there is no symmetric matrix with full rank. Second, it is also insecure against the Kipnis-Shamir attack: it has invariant subspaces as V_1 and V_2, where $V_1 = \{(x_1, \cdots, x_v, 0, \cdots, 0) | x_i \in_R \mathbb{F}_q\}$ and $V_2 = \{(0, \cdots, 0, x_{v+1}, \cdots, x_{v+o_1}) | x_i \in_R \mathbb{F}_q\}$ as in the cryptanalysis of Oil and Vinegar scheme [33]. Therefore, we can say that it is entirely broken by these attacks without explaining the KRAs using good keys. In fact, a similar construction in the mixed field case as in [16] was proposed, but it was also broken by key recovery attacks [24].

We can construct a signature scheme consisting of the first layer and the third layer of HiMQ-3 as a two-layer MQ-signature scheme. Suppose that HiMQ-2 is a two-layer signature scheme with the first layer and the third layer of HiMQ-3, where $n = v + o_1 + o_3$ and $m = o_1 + o_3$. In this case, we can analyze its security against all the known attacks and select secure parameters against the attacks. However, good keys of HiMQ-2 have the same form as those of Rainbow, i.e., complexity of the KRAs on HiMQ-2 is determined by solving $n-1$ bihomogeneous equations and m quadratic equations with n variables as in Rainbow. Thus, compared to Rainbow, HiMQ-2 dramatically reduces the secret key size due to their solvable quadratic systems and sparse polynomials, but HiMQ-2 cannot achieve any improvement on the public key size reduction since the parameter selection of HiMQ-2 is the same as that of Rainbow.

Finally, HiMQ-3 consisting of two layers with simple solvable quadratic systems and the last layer with missing oil×oil structure resists all the known attacks and induces higher complexity against the KRAs using good keys resulting in the reduction of the number of variables, n (so, the public key size reduction). These are the reason why we propose HiMQ-3 as a three-layer MQ-signature scheme.

2.7 Quantum Security Analysis

Now, we give quantum security analysis of HiMQ-3 against the direct attacks and KRAs. Although there is no dedicated quantum algorithm for solving the MQ-problem, we can use Grover's algorithm [27] to the guessing (searching) part of the classical HF5 algorithm [7] since the basic idea of HF5 algorithm is to guess some of the variables to create overdetermined systems before applying F5 algorithm. Thus, we use both HF5 algorithm and Grover's algorithm for quantum security analysis of HiMQ-3 against the direct attacks as in [12].

Unlike the case of $m = n$ in [12], our case is underdetermined, $m < n$. Since $\lambda = q^{n-m}$ is relatively large, the Poisson distribution in this case is difficult to deal with. But, our system has $\lambda = q^{n-m}$ solutions on average, we can expect that a new quadratic system that assumes and assigns $n-m$ variables have one solution on average. The process of guessing and assigning $n-m$ variables is much less complex than solving a quadratic system with m equations and variables. So, we consider quantum complexity of a determined quadratic system of m equations and variables, i.e., $m = n$.

Here, we point out a missing point of Chen *et al.*'s quantum security analysis [12]. They directly used the method in [7] to determine k (the number of variables to guess in HF5 algorithm). However, Grover's algorithm should be applied to the method. Then its complexity is computed by

$$\min_{1 \le k \le m} G(q,k,m) \cdot O\left(\left[m \cdot \binom{m-k+d_{reg}-1}{d_{reg}}\right]^{\alpha}\right),$$

where $G(q,k,m)$ is complexity of Grover's algorithm to guess k variables in a determined quadratic system of m equations and variables over $\mathbb{F}_q$, and d_{reg} is the degree of regularity for solving quadratic systems of m equations in $m-k$ variables using F5 algorithm. Table 4 shows that the least number m such that a determined quadratic system of m equations and variables is required to achieve each quantum security 2^{λ} when $\alpha = 2$.

λ	112	128	160	192	256
m	44	51	66	81	110
k	9	11	11	16	18

Table 4. Lower Bounds of Numbers of Quadratic Equations for Determined Systems on $\mathbb{F}_{2^8}$ at Each Quantum Security Level.

Unlike MQDSS in [12], we need to solve an overdetermined system with $n+m-1$ equations and $n+min(o_1,o_2)$ variables to find good keys of HiMQ-3 to mount the KRAs using good keys. The number of equations in this system is almost twice the number of variables. In this case, complexity for guessing one variable and solving a system with one less equation is much less than $\sqrt{q}$, which is complexity of guessing one variable with Grover's algorithm. Thus, there is no benefit obtainable from using Grover's algorithm.

3 Existential Unforgeability of HiMQ-3

Here, we prove existential unforgeability of HiMQ-3 against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of HiMQ-3.

3.1 Formal Security Model and Complexity Assumption

Now, we describe formal security models of signature schemes. The most general security notion of signature schemes is existential unforgeability against an adaptive chosen-message attack. Its formal security model is defined as follows:

Existential Unforgeability against Adaptive Chosen-Message Attacks (EUF-acma). An adversary $\mathcal{A}$'s advantage $Adv_{\mathcal{PKS},\mathcal{A}}$ is defined as its probability of success in the following game between a challenger $\mathcal{C}$ and $\mathcal{A}$:

- **Setup.** The challenger runs `Setup` algorithm and its resulting system parameters are given to $\mathcal{A}$.
- **Sign Queries.** $\mathcal{A}$ issues the following queries: adaptively, $\mathcal{A}$ requests a signature on a message $\mathtt{m}_i$, $\mathcal{C}$ returns a signature σ_i.
- **Output.** Eventually, $\mathcal{A}$ outputs σ^* on a message $\mathtt{m}^*$ and wins the game if
  i) $\mathtt{Verify}(\mathtt{m}^*, \sigma^*) = 1$,
  ii) $\mathtt{m}^*$ has never requested to the `Sign` oracle.

Definition 4. A forger $\mathcal{A}(t, g_H, q_S, \epsilon)$-breaks a signature scheme if $\mathcal{A}$ runs in time at most t, $\mathcal{A}$ makes at most q_H queries to the hash oracle, q_S queries to the signing oracle and $Adv_{\mathcal{PKS},\mathcal{A}}$ is at least ϵ. A signature scheme is (t, q_E, q_S, ϵ)-EUF-acma if no forger (t, q_H, q_S, ϵ)-breaks it in the above game.

Next, we need to define the following set as:

- $\mathcal{MQ}_{HiMQ-3}(\mathbb{F}_q, m, n)$: a set of all quadratic equations defined over $\mathbb{F}_q$ with m equations and n variables induced by all public keys of HiMQ-3$(\mathbb{F}_q, v, o_1, o_2, o_3)$, where $m = o_1 + o_2 + o_3$ and $n = v + m$.

Definition 5. We say that the MQ-problem in $\mathcal{MQ}_X(\mathbb{F}_q, m, n)$ is (t, ϵ)-hard if no t-time algorithm has advantage at least ϵ in solving the MQ-problem in $\mathcal{MQ}_X(\mathbb{F}_q, m, n)$.

3.2 Existential Unforgeability

To prove existential unforgeability of HiMQ-3 against an adaptive chosen-message attack, we want to find a reduction to the hardness of MQ-problem in $\mathcal{MQ}_{HiMQ-3}(\mathbb{F}_q, m, n)$. The hardness of the MQ-problem for a system of m quadratic equations with n variables mainly depends on the selection of $\mathbb{F}_q$, m and n. However, the security of HiMQ-3 against the attacks presented in §3 depends on the selection of the specific parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ such that $m = o_1 + o_2 + o_3$ and $n = v + m$ due to the special structure of the central map. If the parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ is chosen to be secure against the MinRank attack, HighRank attack and Kipnis-Shamir attack, then it remains only two attacks to consider: the direct attack and KRAs using good keys. In Theorem 1, we have shown that the security of KRAs using good keys for HiMQ-3 is still reduced to the intractability of the MQ-problem, i.e., its complexity is determined by solving $n - 1$ bihomogeneous equations and m quadratic equations with n variables. In fact,

the MinRank attack, HighRank attack, Kipnis-Shamir attack and the KRAs using good keys are related to the MinRank problem and the IP problem. Therefore, if the parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ is chosen to be secure against the MinRank attack, HighRank attack, Kipnis-Shamir attack and KRAs using good keys, we can prove that existential unforgeability of HiMQ-3 is reduced to the hardness of the MQ-problem induced by a public key of the scheme as in [46]. Asiacrypt 2017, we proved existential unforgeability of an MQ-signature scheme, ELSA, against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of ELSA with a secure parameter set in the random oracle model [46]. In fact, the result can be applied to any MQ-signature scheme in the MQ+IP paradigm if the selection of the detailed parameter set depending on the special structure of the central map to be secure against the MinRank attack, HighRank attack, Kipnis-Shamir attack and KRAs using good keys is guaranteed.

Now, we prove existential unforgeability of HiMQ-3 against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of HiMQ-3 in the random oracle model. Its existential unforgeability against an adaptive chosen-message attack is almost the same as that of ELSA in [46].

Theorem 4. If the MQ-problem in $\mathcal{MQ}_{HiMQ-3}(\mathbb{F}_q, m, n)$ is (t', ε')-hard, HiMQ-3$(\mathbb{F}_q, v, o_1, o_2, o_3)$ is $(t, q_H, q_S, \varepsilon)$-$\mathsf{EUF\text{-}acma}$, for any t and ε satisfying

$$\varepsilon \geq \mathsf{e} \cdot (q_S + 1) \cdot \varepsilon', \quad t' \geq t + q_H \cdot c_V + q_S \cdot c_S,$$

where e is the base of the natural logarithm, and c_S and c_V are time for a signature generation and a signature verification, respectively, where $m = o_1 + o_2 + o_3$, and $n = v + m$ if the parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ is chosen to be secure against the MinRank attack, HighRank attack, Kipnis-Shamir attack and KRAs using good keys.

Proof. The proof is almost the same as Theorem 4.1. in [46].

4 Description of the Expected Security Strength of HiMQ-3

Security of MQ-schemes is given by complexities against known attacks. Now, we show how a secure and optimal parameter set $(\mathbb{F}_q^*, v, o_1, o_2, o_3)$ should be selected so that a HiMQ-3 instance over $\mathbb{F}_q$ achieves a security level of λ-bits against all known attacks. We first have to determine a parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ of HiMQ-3 for a given security level such that

- $char(\mathbb{F}_q) = 2$, and o_1 and o_2 are odd,
- $m = o_1 + o_2 + o_3$ and $n = v + m$,
- $v \geq o_1 + 1$, $o_1 \geq o_2 \geq o_3$.

According to our security analysis of HiMQ-3, we summarize its complexities of HiMQ-3 against all the known attacks.

- Direct attacks: Complexity of HiMQ-3 against the direct attacks is estimated as

  $$C_{Direct}(q, m, n) = C_{MQ}(q, m, n),$$

  where $C_{MQ}(q, m, n)$ denotes complexity of solving a semi-regular system of m equations in n variables defined over $\mathbb{F}_q$ by using HF5 algorithm.

- KRAs: Complexity of HiMQ-3 against the KRAs using good keys is

$$C_{KRAg}(q,\ m,\ n) = C_{MQ}(q,\ m+n-1,\ n+min(o_1,o_2)).$$

- MinRank Attacks: Complexity of HiMQ-3 against the MinRank attacks is

$$C_{MR}(q,v,o_1,m) = o_1 \cdot g^{v-o_1+3}.$$

- HighRank Attacks: Complexity of HiMQ-3 against the HighRank attacks is

$$C_{HR}(q,o_3,n) = q^{o_3} \cdot \frac{n^3}{6}.$$

- Kipnis-Shamir Attacks: Complexity of HiMQ-3 against the Kipnis-Shamir Attacks is

$$C_{KS}(q,v,o_1,o_2,o_3) = q^{v+o_1+o_2-o_3}.$$

Finally, we select a secure and optimal parameter of HiMQ-3 at a 128-bit security level as

– HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$).

We summarize complexities of our selected parameter against the known attacks in Table 5. For computing of complexities against direct attacks and KRAs using good keys, we use HF5 algorithm with $\alpha = 2$. Moreover, based on our quantum security analysis, HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$) achieves a 112-bit quantum security.

$(\mathbb{F}_q, v, o_1, o_2, o_3)$	Direct	KRA	Kipnis-Shamir	MinRank	HighRank
HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)	2^{131}	2^{166}	2^{368}	2^{155}	2^{128}

Table 5. Complexities of HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$) against All Known Attacks.

5 A Family of HiMQ-3: HiMQ-3F and HiMQ-3P

A family of HiMQ-3 consists of HiMQ-3F and HiMQ-3P, the generalization of HiMQ-3 and HiMQ-3 using a small random seed as the secret key, respectively. HiMQ-3, HiMQ-3F and HiMQ-3P are optimized for signing performance, the public key size and the secret key size, respectively.

5.1 HiMQ-3F

HiMQ-3F is the generalization of HiMQ-3 replacing sparse polynomials with entire quadratic equations in the $v \times v$ parts in the first layer and the $v \times o_1$ parts in the second layer remaining the third layer of HiMQ-3.

A Central Map. A central map of HiMQ-3F is modified as follows: the central map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$, with $m = o_1 + o_2 + o_3$ equations and $n = v + m$ variables is defined by

$$\begin{cases} \mathcal{F}^{(1)}(\mathbf{x}) = \sum_{1\le i\le j\le v} \alpha_{i,j}^{(1)} x_i x_j + \delta_1 x_{v+1} x_{v+2} = \Phi_1^F(\mathbf{x}) + \delta_1 x_{v+1} x_{v+2}, \\ \mathcal{F}^{(2)}(\mathbf{x}) = \sum_{1\le i\le j\le v} \alpha_{i,j}^{(2)} x_i x_j + \delta_2 x_{v+2} x_{v+3} = \Phi_2^F(\mathbf{x}) + \delta_2 x_{v+2} x_{v+3}, \\ \quad\vdots \\ \mathcal{F}^{(o_1)}(\mathbf{x}) = \sum_{1\le i\le j\le v} \alpha_{i,j}^{(o_1)} x_i x_j + \delta_{o_1} x_{v+o_1} x_{v+1} = \Phi_{o_1}^F(\mathbf{x}) + x_{v+o_1} x_{v+1}, \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+1)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} \alpha_{i,j}^{(o_1+1)} x_i x_j + \delta_{o_1+1} x_{v_1+1} x_{v_1+2} = \Phi_{o_1+1}^F(\mathbf{x}) + \delta_{o_1+1} x_{v_1+1} x_{v_1+2}, \\ \mathcal{F}^{(o_1+2)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} \alpha_{i,j}^{(o_1+2)} x_i x_j + \delta_{o_1+2} x_{v_1+2} x_{v_1+3} = \Phi_{o_1+2}^F(\mathbf{x}) + \delta_{o_1+2} x_{v_1+2} x_{v_1+3}, \\ \quad\vdots \\ \mathcal{F}^{(o_1+o_2)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} \alpha_{i,j}^{(o_1+o_2)} x_i x_j + \delta_{o_1+o_2} x_{v_1+o_2} x_{v_1+1} = \Phi_{o_1+o_2}^F(\mathbf{x}) + \delta_{o_1+o_2} x_{v_1+o_2} x_{v_1+1}, \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+o_2+1)}(\mathbf{x}) = \sum_{v+1\le i\le j\le v_1} \beta_{i,j}^{(o_1+o_2+1)} x_i x_j + \Theta_1(\mathbf{x}) + \Theta_1'(\mathbf{x}) + \epsilon_1 x_{o_1+o_2+1}, \\ \quad\vdots \\ \mathcal{F}^{(o_1+o_2+o_3)}(\mathbf{x}) = \sum_{v+1\le i\le j\le v_1} \beta_{i,j}^{(m)} x_i x_j + \Theta_{o_3}(\mathbf{x}) + \Theta_{o_3}'(\mathbf{x}) + \epsilon_{o_3} x_{o_1+o_2+o_3}, \end{cases}$$

where $\mathbf{x} = (x_1, \cdots, x_n)$. Each equation in the central map is chosen as follows:

- We choose random $\alpha_{i,j}^{(k)} \in \mathbb{F}_q$ for $\Phi_k^F(\mathbf{x})$ $(k = 1, \cdots, o_1 + o_2)$.
- In the first layer, we choose random nonzero $\delta_i \in \mathbb{F}_q^*$ for $i = 1, \cdots, o_1$ as in HiMQ-3.
- In the second layer, we choose random nonzero $\delta_{o_1+i} \in \mathbb{F}_q^*$ for $i = 1, \cdots, o_2$ as in HiMQ-3.
- The third layer of HiMQ-3F is the same as that of HiMQ-3.

Secret Key Size of HiMQ-3F. The secret key of HiMQ-3F is $SK =< \widetilde{S}, \mathcal{F} = (\Phi^F, \delta, \Theta, R), \widetilde{T} >$, where $\Phi^F = (\Phi_1^F, \cdots, \Phi_{o_1+o_2}^F)$, $\delta = (\delta_1', \cdots, \delta_{o_1+o_2}')$, $\Theta = (\Theta_1, \cdots, \Theta_{o_3}, \Theta_1', \cdots, \Theta_{o_3}')$ and $R = \{\beta_{i,j}^{(k)}, \epsilon_k\}_{k=1}^{o_3})$ for the central map. The secret maps S and T require $m(m+1)$ and $n(n+1)$ field elements, respectively. In first layer, it requires $\dfrac{v(v+3)}{2}$ field elements for each polynomial. In second layer, it requires vo_1+1 field elements for each polynomial. In the third layer, $v_1o_2+v_2o_3$ field elements for Θ, and $\dfrac{o_3o_1(o_1+3)}{2}$ for the other parts. Thus, the secret key requires

$$\frac{o_1\left[v(v+3)+o_3(o_1+3)\right]}{2} + o_2(v+1)(o_1+1) + o_3v_2 + m(m+1) + n(n+1)$$

field elements.

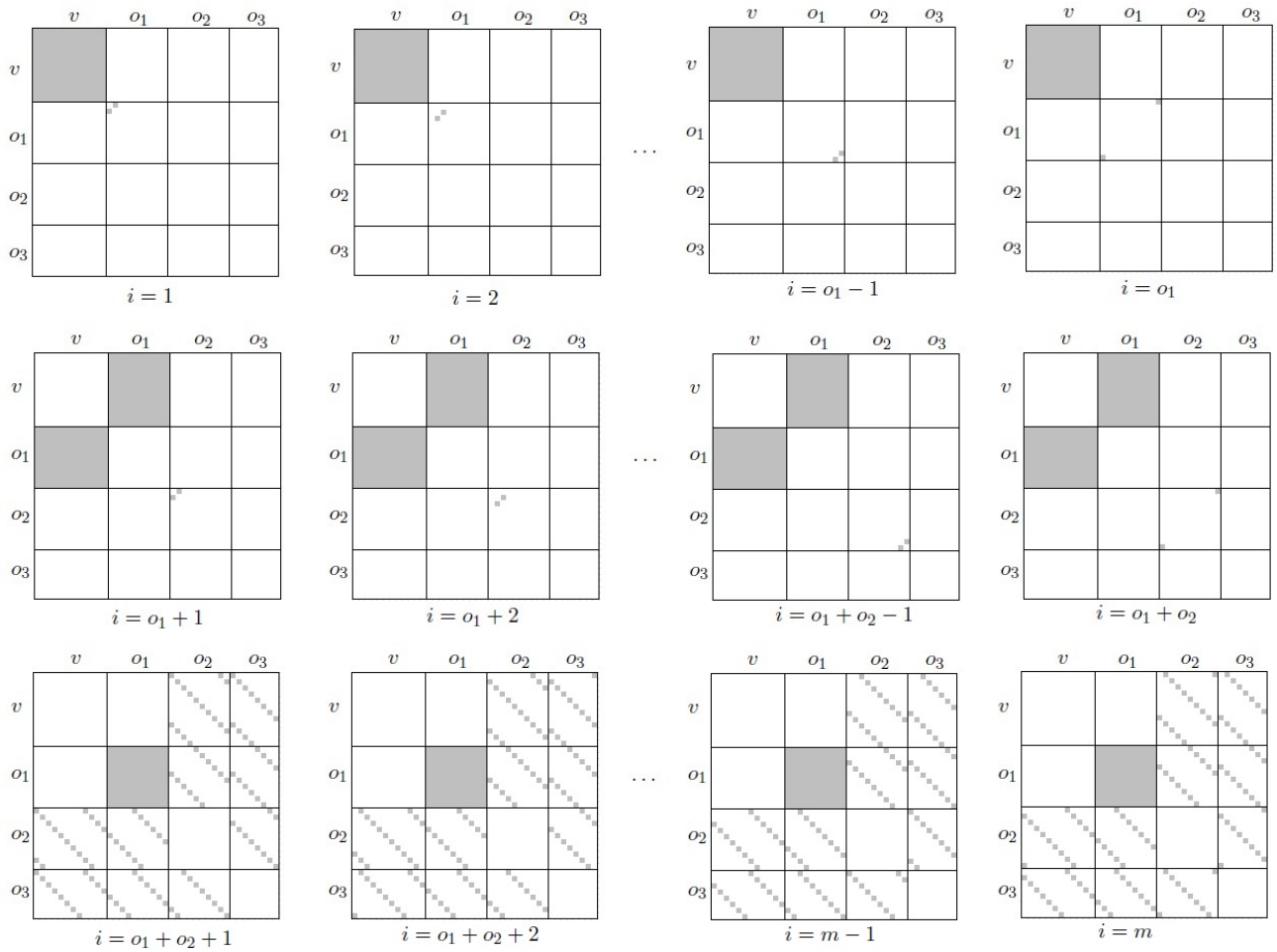

Figure 7: Symmetric Matrices associated to the Quadratic Parts of $\mathcal{F}$ for HiMQ-3F.

Symmetric Matrices for the Central Map of HiMQ-3F. Symmetric matrices $F^{(k)}$ ($1 \leq k \leq m$) associated to the homogeneous quadratic part of the k-th component of the central map of HiMQ-3F are depicted in Fig. 7.

5.1.1 Security Analysis of HiMQ-3F

Direct Attacks. As in HiMQ-3, we compare experimental results of solving quadratic systems derived from a public key of HiMQ-3F with random quadratic systems in Table 6. The result shows that our system behave like random ones.

(v, o_1, o_2, o_3)	(5,3,3,2)	(5,3,3,3)	(5,3,5,2)	(5,3,5,3)	(6,3,5,4)	(6,3,5,5)
Random System	0.137	0.565	3.111	18.372	117.65	707.12
HiMQ-3F	0.141	0.621	3.061	15.66	105.98	745.82

Table 6. Running Time (Second) for Solving Two Types of Quadratic Systems over $\mathbb{F}_{2^8}$.

Rank-based Attacks. Although the central map of HiMQ-3F is a generalization of that of HiMQ-3 (all the crossterms are added in the $v \times v$ parts in the first layer and the $v \times o_1$ parts in the second layer), there is no change to the rank of the symmetric matrix of each central

polynomial compared to HiMQ-3. Thus, the security of HiMQ-3 against rank-based attacks, the MinRank attack and HighRank attack, is preserved in HiMQ-3F. Also, any linear combinations of the matrices $F^{(1)}, \cdots, F^{(m)}$ in HiMQ-3F is the same as that in HiMQ-3 as in the form (*) of §2.5. Thus, the security analysis of HiMQ-3F against the Kipnis-Shamir attack is the same as that of HiMQ-3.

KRAs using Equivalent Keys and Good Keys. To investigate the security against the KRAs on HiMQ-3F, as in (1), we get

$$\frac{mn(n+1) - o_1\left(v(v+3) + o_3(o_1+3)\right)}{2} - o_2(v+1)(o_1+1) - o_3 v_2$$

cubic equations with $n^2 + m^2$ variables, which is different from the case of HiMQ-3. Compared to the basic KRAs on HiMQ-3, the number of equations is reduced since we start with the generalized central map. However, the KRAs using equivalent keys and good keys on HiMQ-3F is the same as those of HiMQ-3 since we have already used the generalized version in Fig. 3 to find equivalent keys and good keys for HiMQ-3 with the least complexities. So, the complexity of KRAs using good keys on HiMQ-3F with the generalized version is less than that of the attacks on HiMQ-3 with the original central map. Thus, both HiMQ-3 and HiMQ-3F use the same generalized version of the central map given in Fig. 2 resulting in the same forms of equivalent keys and good keys, and the same number of equations and variables. Table 7 shows improvements of lower bounds ($\alpha = 2$) on the complexities of solving the resulting systems by HF5 achieved by the KRAs using equivalent keys and good keys for HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$). The reason of the selection of this parameter will be presented in §5.3.

HiMQ-3F	# of Equations	# of Variables	d_{reg}	Complexity
KRA	87,619(Cubic)	6,338	462	2^{4892}
KRA with Equi. Keys	68,141(Cubic)	4,122	276	2^{2996}
KRA with Good Keys	109(Quad.)	78	18	2^{140}

Table 7. Lower-bound on Complexities of the KRAs using Equivalent Keys and Good Keys for HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$)

5.2 HiMQ-3P

In HiMQ-3P, we use a random seed as the secret key instead of entire secret key. Then signing requires additional cost for seed expansion using a pseudorandom generator (PRNG) to recover the entire secret key resulting in reducing the secret key size up to 32 Bytes at a 128-bit security level. Main differences between HiMQ-3F and HiMQ-3P are in **KeyGen** and **Sign** algorithms for generating a seed and recovering the secret key from the seed, respectively.

■ HiMQ-3P

- **KeyGen**(1^λ). For a security parameter λ, generate a public/secret key pair $< PK, SK >=< \mathcal{P}, se >$ as
  - Choose a λ-bit random seed se and compute $\widetilde{S}$, $\widetilde{T}$, $\Phi^F = (\Phi_1^F, \cdots, \Phi_{o_1+o_2}^F)$, $\delta = (\delta'_1, \cdots, \delta'_{o_1+o_2})$, $\Theta = (\Theta_1, \cdots, \Theta_{o_3}, \Theta'_1, \cdots, \Theta'_{o_3})$ and $R = \{\beta_{i,j}^{(k)}, \epsilon_k\}_{k=1}^{o_3}$ for the central map $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$ from se using the PRNG. If these don't satisfy the conditions specified in HiMQ-3F, choose another se and try again.

– Compute $\mathcal{P}$ from $\mathcal{P} = S \circ \mathcal{F} \circ T$.

- **Sign**$(SK, \mathtt{m})$. Given a message $\mathtt{m}$ and a secret key se,
  - **Recovery Phase.** Recover the entire secret key $SK =< \widetilde{S}, \mathcal{F} = (\Phi^F, \delta, \Theta, R), \widetilde{T} >$ from se using the PRNG.
  - **Signing Phase.** This is the same as that of HiMQ-3F.

5.3 Parameter Selection and Expected Security Strength of HiMQ-3F

We have to determine a parameter set $(\mathbb{F}_q, v, o_1, o_2, o_3)$ of HiMQ-3F for a given security level such that

- $char(\mathbb{F}_q) = 2$, and o_1 and o_2 are odd,
- $m = o_1 + o_2 + o_3$, $n = v + m$ and $o_2 \geq o_3$.

Compared to HiMQ-3, the condition $v \geq o_1 + 1$ can be removed due the elimination of the sparse structure of the first layer. According to our security analysis of HiMQ-3F, complexities of HiMQ-3F are the same as those of HiMQ-3. Finally, we select a secure and optimal parameter of HiMQ-3F at the 128-bit security level as

- HiMQ-3F$(\mathbb{F}_{2^8}, 24, 11, 17, 15)$,

The removal of the above condition allows us to select more optimal parameter than HiMQ-3. So, we reduce the number of n from 75 to 67 requiring additional costs for computing quadratic terms. We summarize complexities of our selected parameter against the known attacks in Table 8. For computing of complexities against direct attacks and KRAs using good keys, we use HF5 algorithm with $\alpha = 2$. Furthermore, HiMQ-3$(\mathbb{F}_{2^8}, 24, 11, 17, 15)$ achieves a 110-bit quantum security.

$(\mathbb{F}_q, v, o_1, o_2, o_3)$	Direct	KRA	Kipnis-Shamir	MinRank	HighRank
HiMQ-3F$(\mathbb{F}_{2^8}, 24, 11, 17, 15)$	2^{129}	2^{140}	2^{280}	2^{131}	2^{135}

Table 8. Complexities of HiMQ-3F$(\mathbb{F}_{2^8}, 24, 11, 17, 15)$ against All Known Attacks.

6 Performance Analysis

This section consists of two kinds of implementation results of HiMQ-3 and HiMQ-3F: one is performed on an Intel processor using AVX2 instructions and the other is based on source codes written in ANSI C for achieving NIST's requirements. Benchmarks are carried out on a single core of an Intel Core i7-6700 CPU. More specifically, we implement them on the following environment:

- Intel Core i7-6700 (Skylake) @3.4GHz, turbo boost disabled.
- Memory: 16GB
- OS: x86-64-linux-gnu 4.10.0-28-generic (ubuntu 5.4.0)-6ubuntu1 16.04.4
- gcc: 5.4.0 20160609

Our result is an average of 1,000 measurements for each function using the C programming language with gcc compiler.

Implementation results of HiMQ-3 and HiMQ-3F on Intel processor using AVX2. Implementation of HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$) and HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$) at the 128-bit security level have been optimized for the Intel processor using AVX2 instructions. For a fare comparison, we also implement Rainbow($\mathbb{F}_{2^8}, 36, 21, 22$) at the 128-bit security level on our platform using the codes in [11]. In [11], the authors claimed that Rainbow($\mathbb{F}_{2^8}, 28, 20, 20$) achieved 128-bit security, but its complexities for the direct attacks and the KRAs using good keys are 2^{120} and 2^{114}, respectively, when we use HF5 algorithm with $\alpha = 2$. Their implementation results are given in Table 9.

MQ-Scheme	Sig. Size	PK	SK	KeyGen	Sign	Verify
HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)	75	128,744	12,074	50,593,934	21,594	17,960
HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$)	67	100,878	14,878	79,256,175	25,613	14,645
Rainbow($\mathbb{F}_{2^8}, 36, 21, 22$)	79	139,320	105,006	641,010,138	66,179	23,942

Table 9. Key Sizes, Signature Size (Byte) and Performance (Cycle) of HiMQ-3, HiMQ-3F and Rainbow at the 128-bit Security Level.

Signing and verification of HiMQ-3 are 3.1 times and 1.3 times faster than those of Rainbow, respectively. The secret key and public key size of HiMQ-3 have reduced by a factor 88% and 7.5%, respectively. Signing and verification of HiMQ-3F are 2.6 times and 1.6 times faster than those of Rainbow, respectively. The secret key and public key size of HiMQ-3F have reduced by a factor 86% and 28%, respectively.

Implementation results of HiMQ-3 and HiMQ-3F based on source codes written in ANSI C. Implementation results of HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$) and HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$) at the 128-bit security level based on the submitted optimized codes written in ANSI C on the same platform are given in Table 10.

MQ-Scheme	Sig. Size	PK	SK	KeyGen	Sign	Verify
HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)	75	128,744	12,074	69,104,986	44,703	237,999
HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$)	67	100,878	14,878	107,559,999	64,773	184,402

Table 10. Performance (Cycle) of HiMQ-3 and HiMQ-3F at the 128-bit Security Level.

7 Advantages and limitations

Advantages. MQ-schemes require simplicity of operations (matrices and vectors) and small fields avoid multiple-precision arithmetic. So, they require only modest computational resources, which makes them attractive for the use on low cost devices such as smart cards [9, 10]. At CHES 2012, Czypek *et al.* [14] demonstrated feasibility of MQ-signature schemes on 8-bit AVR microprocessor ATxMega128a1 with 32 MHz, 128KB flash program memory and 8KB SRAM. They showed that the speed of Rainbow and enTTS outperform other signature schemes. In particular, MQ-signature schemes are competitive in terms of their speed and signature sizes. HiMQ-3 is suitable for very specific applications, where the cost of other signature schemes

Scheme λ	**Sig. Size** (Bytes)	**PK** (Bytes)	**SK** (Bytes)	**Sign** (Cycles)	**Verify** (Cycles)	**CPU**
Classical ones						
RSA-3072[e] 128	361	384	3072	8,802,242	87,360	Intel Core i5-6600 3.3 GHz
ECDSA-256[e] 128	64	64	96	163,994	310,048	Intel Core i5-6600 3.3 GHz
Lattice-based						
TESLA-416[t] [3] 128	1,280	1,331,200	1,011,744	697,940	250,264	Intel Core i7-4770K(Haswell)
TESLA-768[t] [3] > 128	2,336	4,227,072	3,293,216	2,232,906	863,790	Intel Core i7-4770K(Haswell)
BLISS-BI [19, 18] 128	700	875	250	358,400	102,000	Intel Core i7 3.4 GHz
Hash-based						
XMSS ($h = 20$) [31] 256	3,584	1,536	2,662	12,488,458	–	Intel Core i7-4770 3.5GHz
XMSS-T[t] ($h = 60$) [31] 256	2,969	66	2,252	34,862,003	–	Intel Core i7-4770 3.5GHz
SPHINCS 256[s] [5] 256	41,000	1,056	1,088	51,636,372	1,451,004	Intel Xeon E3-1275 3.5 GHz
Code-based						
Parallel-CFS [34] 80	75	20,968,300	4,194,300	4,200,000,000	–	Intel Xeon W3670 3.2GHz
MQ-based						
MQDSS-31-64 [12] > 128	40,952	72	64	8,510,616	5,752,616	Intel Core i7-4770K 3.5GHz
enTTS $(\mathbb{F}_{2^8}, 15, 60, 88)$ [14] 128	88	234,960	13,051	–	–	–
Rainbow $(\mathbb{F}_{2^8}, 36, 21, 22)$ [6] 128	79	139,320	105,006	60,361	48,079	Intel Core i5-6600 3.3 GHz
HiMQ-3 ($\mathbb{F}_{2^8}$,31,15,15,14) 128	**75**	**128,744**	**12,074**	**21,594**	**17,960**	Intel Core i7-6700 3.4 GHz
HiMQ-3F ($\mathbb{F}_{2^8}$,24,11,17,15) 128	**67**	**100,878**	**14,878**	**25,613**	**14,645**	Intel Core i7-6700 3.4 GHz
HiMQ-3P ($\mathbb{F}_{2^8}$,31,15,15,14) 128	**67**	**100,878**	**32**	**25,613+ 20,011**[P]	**14,645**	Intel Core i7-6700 3.4 GHz

Table 11. Performance, Key Sizes and Signature Sizes of Ours, Classical-Ones and Post-Quantum Ones at the Classical Security Levels.

Sig. Size, PK and SK represent signature size, public key and secret key, respectively.

> 128 means that the scheme achieves 2^λ security level, where $\lambda > 128$.

[t]The scheme has a tight security reduction to the underlying hard problem.

[s]The scheme is provably secure in the standard model.

[e]The result is given by the eBACS project [6].

[P]It requires at least 20,011 cycles for the recovery of the entire secret key from *se*.

becomes prohibitive: they are too slow or/and the signature size if too big. We expect that our schemes preserve their high speed after adapting countermeasures against side-channel attacks later. Our scheme is the fastest signature scheme in both signing and verification among classical ones and Post-Quantum ones. Table 10 provides comparisons between ours, classical ones and Post-Quantum ones in terms of performance, key sizes and signature sizes.

- Performance: Signing of HiMQ-3 is about 3.1 times faster than that of Rainbow. It takes 6.35 μs and 5.28 μs for signing and verification, respectively. Signing and verification of HiMQ-3 is about 7.6 times and 17.3 times faster than those of ECDSA, respectively. Signing and verification of HiMQ-3 is about 16.6 times and 5.68 times faster than those of BLISS-BI, respectively.
- Signature Size: HiMQ-3 requires signatures of 75 bytes. Signature size of HiMQ-3F is 67 bytes which is comparable to ECDSA-256 of 64 bytes. Signature size of BLISS-BI is about 10.45 times larger than that of HiMQ-3F.
- Key Sizes: Compared to Rainbow, the secret key size and public key size of HiMQ-3 are reduced by a factor of 88% and 7.5%, respectively. Compared to enTTS, the public key size and secret key size of HiMQ-3 have reduced by a factor of 45% and 7.5%, respectively. The secret key and public key size of HiMQ-3F have reduced by a factor 86% and 28%, respectively. The secret key size of HiMQ-3P is 32 bytes, while it requires additional costs for the recovery process of the secret key from a seed using the PRNG.

Limitations. The secret key sizes of HiMQ-3, HiMQ-3F and HiMQ-3P are 11.79KB, 14.53KB and 32B, respectively. In HiMQ-3 and HiMQ-3F, if we implement simper equivalent keys of them then 2KB to 3KB can be further reduced in the secret key sizes. However, their public key sizes are still large requiring about 125.73KB, 98.51KB and 98.51KB, respectively.

References

[1] S. M. E. Y. Alaoui, O. Dagdelen, P. Veron, D. Galindo, and P-L Cayrel, Extended Security Arguments for Signature Schemes, AFRICACRYPT 2012, LNCS 7374, pp. 19-34, 2012.

[2] M. R. Albrecht, J-C. Faugère, R. Fitzpatrick, L. Perret, Y. Todo and K. Xagawa, Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions, PKC 2014, LNCS 8383, pp. 446-464, 2014.

[3] E. Alkim, N. Bindel, J. Buchmann, O. Dagdelen and P. Schwabe, TESLA: Tightly-Secure Efficient Signatures from Standard Lattices, Cryptology ePrint Archive: Report 2015/755.

[4] D. J. Bernstein, Curve25519: New Diffie-Hellman Speed Records, PKC 2006, LNCS 3958, pp. 207-228, 2006.

[5] 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 Singatures, EUROCRYPT 2015, LNCS 9056, pp. 368-397, 2015.

[6] D. J. Bernstein and T. Lange, eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench.cr.yp.to. Accessed 30 September 2016.

[7] L. Bettale, J.-C. Faugére and L. Perret, Hybrid Approach for Solving Multivariate Systems over Finite Fields, Journal of Mathematical Cryptology, 3, pp. 177-197, 2009.

[8] O. Billet and H. Gilbert, Cryptanalysis of Rainbow, SCN 2006, LNCS 4116, pp. 336-347, 2006.

[9] A. Bogdanov, T. Eisenbarth, A. Rupp and C. Wolf, Time-area Optimized Public-key Engines: MQ-cryptosystems as Replacement for Elliptic Curves?, CHES'08, LNCS 5154, pp. 45-61, 2008.

[10] 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, CHES'09, LNCS 5747, pp. 33-48, 2009.

[11] M.S. Chen, W.-D. Li, B.-Y. Peng, B.-Y. Yang and C.-M. Cheng, Implementing 128-bit Secure MPKC Signatures, Cryptology ePrint Archive: Report 2017/636.

[12] M-S Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe, From 5-pass MQ-based Identification to MQ-based Signatures, to appear at Asiacrypt 2016.

[13] N. T. Courtois, Efficient Zero-knowledge Authentication based on a Linear Algebra Problem MinRank, ASIACRYPT 20001, LNCS 2248, pp. 402-421, 2001.

[14] P. Czypek, S. Heyse and E Thomae, Efficient Implementations of MQPKS on Con- strained Devices, CHES 2012, LNCS 7428, pp. 374-389, 2012.

[15] J. Ding and D. Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme, ACNS 2005, LNCS 3531, pp. 164-175, 2005.

[16] J. Ding, C. Wolf and B.Y. Yang, l-invertible cycles for multivariate quadratic (MQ) public key cryptography. PKC 2007, pp. 266-281, 2007.

[17] J. Ding, B-Y. Yang, C-H O. Chen, M-S. Chen, and C-M. Cheng, New Differential-algebraic Attacks and Reparametrization of Rainbow, ACNS'08, pp. 242-257, 2008.

[18] L. Ducas, Accelerating Bliss: the Geometry of Ternary Polynomials, Cryptology ePrint Archive: Report 2014/874.

[19] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, Lattice Signatures and Bimodal Gaussians, CRYPTO 2013, Part I, LNCS 8042, pp. 40-56, 2013.

[20] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez and P. Schwabe, High-speed Curve25519 on 8-bit, 16-bit and 32-bit microcontrollers, Designs, Codes and Cryptography, 77(2-3), pp. 493-514, 2015.

[21] J.-C. Faugére, A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5), ISSAC 2002, pp. 75-83, 2002.

[22] J.-C. Faugére, D. Gligoroski, L. Perret, S. Samardjiska, and E. Thomae, A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems, PKC 2015, LNCS 9020, pp. 150-174, 2015.

[23] J-C Faugére, F. Levy-dit-Vehel, and L. Perret, Cryptanalysis of MinRank, CRYPTO 2008, LNCS 5157, pp. 280-296, 2008.

[24] P-A Fouque, G. Macario-Rat, L. Perret and Jacques Stern, Total Break of the l-IC Signature Scheme, PKC 2008, pp. 1-17, 2008.

[25] M. R. Garey and D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, 1979.

[26] 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, INTRUST 2011, LNCS 7222, pp. 184-203, 2011.

[27] Lov K. Grover, A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC'96, pp. 212-219, ACM, 1996. https://arxiv. org/pdf/quant-ph/9605043v3.pdf.

[28] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, Transcript Secure Signatures Based on Modular Lattices, PQCrypto 2014, LNCS 8772, pp 142-159, 2014.

[29] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A Ring-based Public-Key Cryptosystem, ANTS 1998, pp. 267-288, 1998.

[30] Y.-J. Huang,F.-H. Liu and B.-Y. Yang, Public-Key Cryptography from New Multivariate Quadratic Assumptions, PKC 2012, LNCS 7293, pp. 190-205, 2012.

[31] A. Hülsing, J. Rijneveld and F. Song, Mitigating Multi-target Attacks in Hash-Based Signatures, PKC (1) 2016, LNCS 9614, pp. 387-416, 2016.

[32] A. Kipnis, J. Patarin, and L. Goubin, Unbalanced Oil and Vinegar Signature Schemes, CRYPTO'99, LNCS 1592, pp. 206-222, 1999.

[33] A. Kipnis and A. Shamir, Cryptanalysis of the Oil and Vinegar Signature Scheme, CRYPTO'98, LNCS 1462, pp. 257-266, 1998.

[34] G. Landais and N. Sendrier, Implementing CFS, Indocrypt 2012, LNCS 7668, pp. 474-488, 2012.

[35] T. Matsumoto, and H. Imai, Public Quadratic Polynomial-Tuples for efficient Signature-Verification and Message-Encryption, EUROCRYPT'88, LNCS 330, pp. 419-453, 1988.

[36] R. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN Progress Report 42-44, Jet Propulsion Laboratories, Pasadena, 1978.

[37] R. C. Merkle, A Digital Signature based on a Conventional Encryption Function, CRYPTO'87, LNCS 293, pp. 369-378, 1987.

[38] J. Patarin, Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, EUROCRYPT'96, LNCS 1070, pp. 33-48, 1996.

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

[40] J. Patarin, N. Courtois, and L. Goubin, QUARTZ, 128-bit Long Digital Signatures, CT-RSA 20001, LNCS 2020, pp. 282-297, 2001.

[41] A. Petzoldt, Selecting and Reducing Key Sizes for Multivariate Cryptography, PhD Thesis, 2013.

[42] A. Petzoldt, M-S Chen, B-Y Yang, C. Tao and J. Ding, Design Principles for HFEv- Based Multivariate Signature Schemes, ASIACRYPT 2015, Part I, LNCS 9452, pp. 311-334, 2015.

[43] T. Pöppelmann, T. Oder and T. Güneysu, High-Performance Ideal Lattice-Based Cryptography on 8-Bit ATxmega Microcontrollers, LatinCrypt 2015, LNCS 9230, pp. 346-365, 2015.

[44] K. Sakumoto, T. Shirai and H. Hiwatari, Public-Key Identification Schemes based on Multivariate Quadratic Polynomials, CRYPTO 2011, LNCS 6841, pp. 706-723, 2011.

[45] J. O. Shallit, G.S. Frandsen, and J.F. Buss, The Computational Complexity of some Problems of Linear Algebra, BRICS series report, Aarhus, Denmark, RS-96-33. (also at http://www.brics.dk/RS/96/33).

[46] K. A. Shim, C-M. Park and N.H. Koo, An Existential Unforgeable Signature Scheme based on Multivariate Quadratic Equations, Asiacrypt 2017, to appear.

[47] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. on Computing, pp. 1484-1509, 1997.

[48] E. Thomae, About the Security of Multivariate Quadratic Public Key Schemes, Dissertation Thesis by Dipl. math. E. Thomae, RUB, 2013.

[49] C. Wolf and B. Preneel, Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems, PKC 2005, LNCS 3386, pp. 275-287, 2005.

[50] B-Y Yang and J-M Chen, Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS, ACISP 2005, LNCS 3574, pp. 518.531, 2005.