High Speed MQ Signature: HiMQ 3

Cheol-Min Park (NIMS)

Joint work with Kyung-Ah Shim, Aeyoung Kim (NIMS) and Namhun Koo (SKKU)

The First PQC Standardization Conference
April 12, 2018

Presentation Outline

1. Algorithm Specification
2. Security Analysis of HiMQ-3
3. Key feature of HiMQ-3
4. Implementation and Comparison
5. Advantages and limitations

General Structure of MQ Signature

- F_q: finite field with q elements
- $\mathcal{F} : F_q^n \to F_q^m$ by $\mathcal{F}(X) = (\mathcal{F}^{(1)}(x), ..., \mathcal{F}^{(m)}(x))$ for $X = (x_1, x_2, ..., x_n)$
- $\mathcal{T} : F_q^n \to F_q^n$, $\mathcal{S} : F_q^m \to F_q^m$ invertible affine maps
- $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : F_q^n \to F_q^m$
- Public key: $\mathcal{P}$, Secret key: $\mathcal{S}, \mathcal{F}, \mathcal{T}$

Building Blocks of $\mathcal{F}$

- Solvable System of Quadratic Equations $\mathcal{Q}$
  - char(F_q)=2, is odd.
  - $\mathcal{Q} : (x_1x_2,\ x_2x_3,\ \ldots\ ,\ x\ x_1) = (\beta_1, \beta_2, \ldots, \beta\ )$ for $\beta_i \quad F_q$

$$(x_1x_2) \times (x_2x_3) \times \cdots \times (x\ x_1) = (\prod_{i=1} x_i)^2 = (\prod_{i=1} \beta_i) \qquad (1)$$

$$(\prod_{i=1} x_i) = \sqrt{(\prod_{i=1} \beta_i)} \qquad (2)$$

$$(x_2x_3) \times (x_4x_5) \times \cdots \times (x_{\ -1}x\ ) = (\prod_{i=2} x_i) = (\prod_{i:even} \beta_i) \qquad (3)$$

Using E.q. (2) and E.q. (3), we can obtain x_1 and so $x_2, \ldots, x\ $.

Central map $\mathcal{F}$

- $\mathcal{F}(X) = (\mathcal{F}^{(1)}(x), \ldots, \mathcal{F}^{(m)}(x))$ where

$$\begin{cases} \mathcal{F}^{(1)}(x) = \Phi_1(\mathbf{x_v}) + \delta_1 x_{v+1} x_{v+2} & (\mathbf{x_v} = (x_1, \ldots, x_v)) \\ \mathcal{F}^{(2)}(x) = \Phi_2(\mathbf{x_v}) + \delta_2 x_{v+2} x_{v+3} & \\ \qquad \vdots \qquad\qquad \vdots & \\ \mathcal{F}^{(o_1)}(x) = \Phi_{o_1}(\mathbf{x_v}) + \delta_{o_1} x_{v+o_1} x_{v+1} & \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x) = \Psi_1(\mathbf{x_{v_1}}) + \delta_{o_1+1} x_{v_1+1} x_{v_1+2} & (\mathbf{x_{v_1}} = (x_1, \ldots, x_{v+o_1})) \\ \mathcal{F}^{(o_1+2)}(x) = \Psi_2(\mathbf{x_{v_1}}) + \delta_{o_1+2} x_{v_1+2} x_{v_1+3} & \\ \qquad \vdots \qquad\qquad \vdots & \\ \mathcal{F}^{(o_1+o_2)}(x) = \Psi_{o_2}(\mathbf{x_{v_1}}) + \delta_{o_1+o_2} x_{v_1+o_2} x_{v_1+1} & \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+o_2+1)}(x) = \sum\limits_{v+1 \le i \le j \le v_1} \beta_{j,i}^{(1)} x_i x_j + \Theta_1(x) + \Theta_{1}(x) + \ {}_1 x_{o_1+o_2+1} \\ \mathcal{F}^{(o_1+o_2+2)}(x) = \sum\limits_{v+1 \le i \le j \le v_1} \beta_{j,i}^{(2)} x_i x_j + \Theta_2(x) + \Theta_{2}(x) + \ {}_2 x_{o_1+o_2+2} \\ \qquad \vdots \qquad\qquad \vdots \\ \mathcal{F}^{(o_1+o_2+o_3)}(x) = \sum\limits_{v+1 \le i \le j \le v_1} \beta_{j,i}^{(o_3)} x_i x_j + \Theta_{o_3}(x) + \Theta_{o_3}(x) + \ {}_{o_3} x_{o_1+o_2+o_3} \end{cases}$$

Central map $\mathcal{F}$ of HiMQ 3F

- $\Phi_k(x) = \sum_{1\le i\le j\le v} \alpha_{i,j}^{(k)} x_i x_j, \quad \Psi_k(x) = \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} \alpha_{i,j}^{(o_1+k)} x_i x_j$
- $\Theta_i(\mathbf{x}) = \sum_{j=1}^{v_1} \gamma_{i,j} x_i x_{v_1+(i+j-1) \pmod{o_3}}$,

  $\Theta_{i}(\mathbf{x}) = \sum_{j=1}^{v_2} \gamma_{i,j} x_i x_{v_2+(i+j-1) \pmod{o_3}}$
- All the quadratic terms in $\Theta_i(\mathbf{x})$ and $\Theta_{i}(\mathbf{x})$ $(i = 1, \cdots, o_3)$ don't overlap and

  symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ has full rank for $i = o_1 + o_2 + 1, \cdots, m$.

  $v \ge 2o_1 + 1$ and $o_2 \ge o_3$.

Central map $\mathcal{F}$ of HiMQ 3

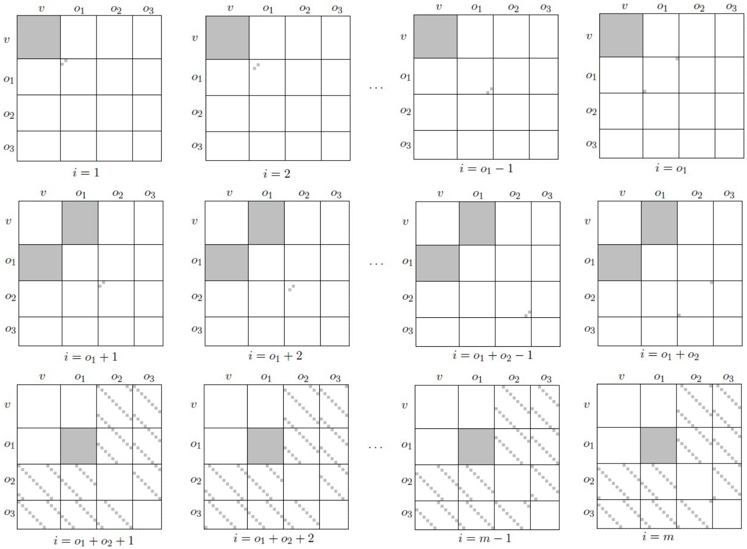
- $$\Phi_i(\mathbf{x}) = \sum_{j=1}^{v} \alpha_{i,j} x_j x_{1+(i+j-1)(\text{mod } v)},$$
  $$\Psi_i(\mathbf{x}) = \sum_{j=1}^{v} \alpha_{i,j} x_j x_{v+(i+j-1)(\text{mod } o_1)}.$$

- $\Theta_i(\mathbf{x})$, $\Theta_i(\mathbf{x})$ is the same as HiMQ-3F

- All the quadratic terms in $\Phi_i(\mathbf{x})$ $(i = 1, \cdots, o_1)$ and $\Psi_i(\mathbf{x})$ $(i = 1, \cdots, o_2)$ don't overlap and
  symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ has full rank for $i = o_1 + o_2 + 1, \cdots, m$.

  $v \geq 2o_1 + 1$ and $o_1 \geq o_2 \geq o_3$.

Symmetric Matrices of the Quadratic Parts of $\mathcal{F}$ for HiMQ 3F

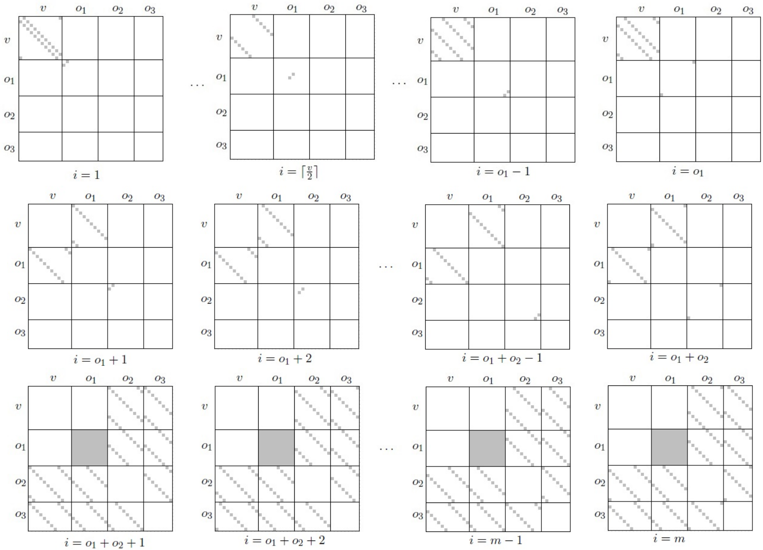


$i = 1$ $i = 2$ $\dots$ $i = o_1 - 1$ $i = o_1$

$i = o_1 + 1$ $i = o_1 + 2$ $\dots$ $i = o_1 + o_2 - 1$ $i = o_1 + o_2$

$i = o_1 + o_2 + 1$ $i = o_1 + o_2 + 2$ $\dots$ $i = m - 1$ $i = m$

Symmetric Matrices of the Quadratic Parts of $\mathcal{F}$ for HiMQ 3


$i = 1$ … $i = \lceil \frac{v}{2} \rceil$ … $i = o_1 - 1$ $i = o_1$

$i = o_1 + 1$ $i = o_1 + 2$ … $i = o_1 + o_2 - 1$ $i = o_1 + o_2$

$i = o_1 + o_2 + 1$ $i = o_1 + o_2 + 2$ … $i = m - 1$ $i = m$

How to invert $\mathcal{F}$

- Given $\xi = (\xi_1, ..., \xi_m)$, find s such that $\mathcal{F}(s) = \xi$

1. Choose a random Vinegar vector $s_v = (s_1, ..., s_v)$ and plug it into $\mathcal{F}^{(i)}$ $(1 \leq i \leq o_1)$.
2. Solve a quadratic system of o_1 equations with o_1 variables

   $$(\delta_1 x_{v+1} x_{v+2},\ \dots\ ,\ \delta_{o_1} x_{v+o_1} x_{v+1}) = (\xi_1 - \Phi_1(s_v), ..., \xi_{o_1} - \Phi_{o_1}(s_v))$$

   Find solution $(s_{v+1}, ..., s_{v+o_1})$ by using E.q. (2) and E.q. (3).
3. To Invert $\mathcal{F}^{(i)}$ $(o_1 + 1 \leq i \leq o_1 + o_2)$ in the 2nd layer is similar to Step 1 and Step 2.
4. Plug $(s_1, ..., s_{v+o_1+o_2})$ into the polynomials $\mathcal{F}^{(i)}$ $(o_1 + o_2 + 1 \leq i \leq m)$.
5. Solve a linear system of o_3 equations with o_3 variables and find solution $(s_{v+o_1+o_2}, ..., s_n)$ by Gaussian elimination.

Presentation Outline

1. Algorithm Specification
2. Security Analysis of HiMQ-3
3. Key feature of HiMQ-3
4. Implementation and Comparison
5. Advantages and limitations

Underlying problems for security of HiMQ 3

- **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 $\mathbf{y} = (y_1, \cdots, y_m) \quad \mathbb{F}_q^m$, find values $(x_1, \cdots, x_n) \quad \mathbb{F}_q^n$ 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 $\mathcal{F} \quad \mathcal{C}$.

- **MinRank Problem:** Let $m, n, r, k \quad \mathbb{N}$ and $r, m < n$. The MinRank(r) problem is, given $(M_1, \cdots, M_l) \quad \mathbb{F}_q^{m \times n}$, find a non-zero k-tuple $(\lambda_1, \cdots, \lambda_k) \quad \mathbb{F}_q^k$ such that $Rank(\sum_{i=1}^{k} \lambda_i M_i) \leq r$.

Direct attack

- 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.

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

(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	0.145	0.602	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

Rank attack

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

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

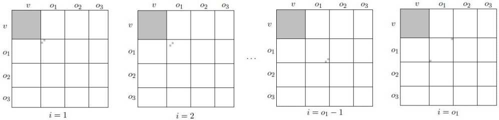


Figure: 1st layer of HiMQ-3

- 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

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

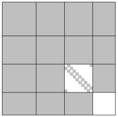


Figure: $\mathcal{S} \circ \mathcal{F}$ of HiMQ-3

Key recovery attack(KRA)

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

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

$$\begin{aligned}\mathcal{P} &= (S \circ \Sigma^{-1}) \circ (\Sigma \circ \mathcal{F} \circ \Omega) \circ (\Omega^{-1} \circ T) \\ &= S\ \circ \mathcal{F}\ \circ T \qquad ((S\ , \mathcal{F}\ , T\ ) : \text{ equivalent key})\end{aligned}$$

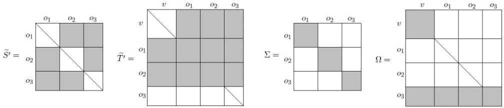


Figure: Equivalent Key of HiMQ-3

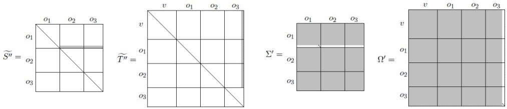


Figure: Good Key of HiMQ-3

Existential unforgeability of HiMQ 3

Theorem

If the MQ-problem in $\mathcal{MQ}_{HiMQ-3}(\mathbb{F}_q, m, n)$ is $(t\ ,\varepsilon\ )$-hard, HiMQ-3$(\mathbb{F}_q, v, o_1, o_2, o_3)$ is $(t, q_H, q_S, \varepsilon)$-EUF-acma, for any t and ε satisfying

$$\varepsilon \geq \mathrm{e} \cdot (q_S + 1) \cdot \varepsilon\ , \quad t\ \geq t + q_H \cdot c_V + q_S \cdot c_S,$$

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.

Presentation Outline

1 Algorithm Specification

2 Security Analysis of HiMQ-3

3 Key feature of HiMQ-3

4 Implementation and Comparison

5 Advantages and limitations

Key feature of HiMQ 3

- Smaller public key size (compared to other MQ-signatures)
  - Use an easily solvable system of quadratic equations in Oil × Oil parts of 1st and 2nd layers

    Good keys of HiMQ-3 in KRA are different from that of Rainbow.

    Increase the complexity of key recovery attack

    Reduce the number of variables

    Smaller public key size, signature size and faster verification.

Key feature of HiMQ 3

- Smaller secret key size (compared to other MQ-signatures)
    - HiMQ-3 and HiMQ-3F use sparse quadratic polynomials in the 3rd layer.
    - HiMQ-3 also use sparse quadratic polynomials in the 1st and 2nd layer
    - In HiMQ-3P, we use a small random seed for secret key and recover the entire secret key from the seed in signing via PRNG.

Key feature of HiMQ 3

- Fast signature generation (compared to other MQ-signatures)
  - Use an easily solvable system of quadratic equations instead of Oil-Vinegar system.
  - No Gaussian elimination in 1st and 2nd layers.
  - In 3rd layer, Gaussian elimination for equations with smaller number of variables than UOV or Rainbow.

Parameter Selection and Expected Security

- HiMQ-3F: char(F_q)=2, o_1, o_2 are odd and $o_2 \geq o_3, v \geq 2o_1 + 1$
- HiMQ-3: char(F_q)=2, o_1, o_2 are odd and $o_1 \geq o_2 \geq o_3, v \geq 2o_1 + 1$

- Complexities of HiMQ-3 and HiMQ-3F against All Known Attacks at 128 security level

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

Presentation Outline

1. Algorithm Specification
2. Security Analysis of HiMQ-3
3. Key feature of HiMQ-3
4. Implementation and Comparison
5. Advantages and limitations

Implementation results of HiMQ 3 and HiMQ 3F at the 128 bit Security Level.

- Implementation results (cycle)

MQ-Scheme	KeyGen	Sign	Verify	
HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)	50,593,934	21,594	17,960	AVX2
	69,104,986	44,703	237,999	ANSI C
HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$)	79,256,175	25,613	14,645	AVX2
	107,559,999	64,773	184,402	ANSI C

- Key size and Signature size (Byte)

MQ-Scheme	Signature	PK	SK
HiMQ-3($\mathbb{F}_{2^8}, 31, 15, 15, 14$)	75	128,744	12,074
HiMQ-3F($\mathbb{F}_{2^8}, 24, 11, 17, 15$)	67	100,878	14,878
HiMQ-3P($\mathbb{F}_{2^8}, 24, 11, 17, 15$)	67	100,878	32

Scheme λ	**Sig. Size** (Bytes)	**PK** (Bytes)	**SK** (Bytes)	**Sign** (Cycles)	**Verify** (Cycles)	**CPU**
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
TESLA-416^t 128	1,280	1,331,200	1,011,744	697,940	250,264	Intel Core i7-4770K(Haswell)
TESLA-768^t > 128	2,336	4,227,072	3,293,216	2,232,906	863,790	Intel Core i7-4770K(Haswell)
BLISS-BI 128	700	875	250	358,400	102,000	Intel Core i7 3.4 GHz
XMSS ($h = 20$) 256	3,584	1,536	2,662	12,488,458	–	Intel Core i7-4770 3.5GHz
XMSS-T^t ($h = 60$) 256	2,969	66	2,252	34,862,003	–	Intel Core i7-4770 3.5GHz
SPHINCS 256^s 256	41,000	1,056	1,088	51,636,372	1,451,004	Intel Xeon E3-1275 3.5 GHz
Parallel-CFS 80	75	20,968,300	4,194,300	4,200,000,000	–	Intel Xeon W3670 3.2GHz
MQDSS-31-64 > 128	40,952	72	64	8,510,616	5,752,616	Intel Core i7-4770K 3.5GHz
enTTS $(\mathbb{F}_{2^8}, 15, 60, 88)$ 128	88	234,960	13,051	–	–	–
Rainbow $(\mathbb{F}_{2^8}, 36, 21, 22)$ 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 $(\mathbb{F}_{2^8}$,24,11,17,15) 128	**67**	**100,878**	**32**	**25,613+** **20,011**^{P}	**14,645**	Intel Core i7-6700 3.4 GHz

Table Performance, Key Sizes and Signature Sizes of Schemes at the Classical Security Levels.

Presentation Outline

1. Algorithm Specification

2. Security Analysis of HiMQ-3

3. Key feature of HiMQ-3

4. Implementation and Comparison

5. Advantages and limitations

Advantages and limitations

- Advantages of HiMQ-3
  - High speed in signing and verifying

    Attractive in a small device with limited computational resources
    High speed after adapting countermeasure against side-channel attacks
  - Small signature size (comparable to ECDSA-256)
  - Small public key and secret key size compared to other MQ-signatures
- Need to reduce the public key size of HiMQ-3.