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
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

- $\mathcal{F}: F_q^n \rightarrow F_q^m$ by $\mathcal{F}(X) = (\mathcal{F}^{(1)}(x), \ldots, \mathcal{F}^{(m)}(x))$ for $X = (x_1, x_2, \ldots, x_n)$

- $\mathcal{T}: F_q^n \rightarrow F_q^n$, $S: F_q^m \rightarrow F_q^m$ invertible affine maps

- $\mathcal{P} = S \circ \mathcal{F} \circ \mathcal{T}: F_q^n \rightarrow F_q^m$

- Public key: $\mathcal{P}$, Secret key: $S, \mathcal{F}, \mathcal{T}$
Building Blocks of $F$

- **Solvable System of Quadratic Equations** $Q$
  - $\text{char}(F_q) = 2$, is odd.
  - $Q : (x_1 x_2, x_2 x_3, \ldots, x x_1) = (\beta_1, \beta_2, \ldots, \beta)$ for $\beta_i \in F_q$

(1)  

$$(x_1 x_2) \times (x_2 x_3) \times \cdots \times (x x_1) = \left( \prod_{i=1}^{n} x_i \right)^2 = \left( \prod_{i=1}^{n} \beta_i \right)$$

(2)  

$$\left( \prod_{i=1}^{n} x_i \right) = \sqrt{\left( \prod_{i=1}^{n} \beta_i \right)}$$

(3)  

$$(x_2 x_3) \times (x_4 x_5) \times \cdots \times (x -1 x) = \left( \prod_{i=2}^{n} x_i \right) = \left( \prod_{i: \text{even}} \beta_i \right)$$

Using E.q. (2) and E.q. (3), we can obtain $x_1$ and so $x_2, \ldots, x$. 
Central map $\mathcal{F}$

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

\[
\begin{align*}
\mathcal{F}^{(1)}(x) &= \Phi_1(x_v) + \delta_1 x_{v+1} x_{v+2} \quad (x_v = (x_1, ..., x_v)) \\
\mathcal{F}^{(2)}(x) &= \Phi_2(x_v) + \delta_2 x_{v+2} x_{v+3} \\
& \quad \vdots \\
\mathcal{F}^{(o_1)}(x) &= \Phi_{o_1}(x_v) + \delta_{o_1} x_{v+o_1} x_{v+1} \\
\mathcal{F}^{(o_1+1)}(x) &= \Psi_1(x_{v_1}) + \delta_{o_1+1} x_{v_1+1} x_{v_1+2} \quad (x_{v_1} = (x_1, ..., x_{v+o_1})) \\
\mathcal{F}^{(o_1+2)}(x) &= \Psi_2(x_{v_1}) + \delta_{o_1+2} x_{v_1+2} x_{v_1+3} \\
& \quad \vdots \\
\mathcal{F}^{(o_1+o_2)}(x) &= \Psi_{o_2}(x_{v_1}) + \delta_{o_1+o_2} x_{v_1+o_2} x_{v_1+1} \\
\mathcal{F}^{(o_1+o_2+1)}(x) &= \sum_{v+1 \leq i \leq j \leq v_1} \beta_{j,i}^{(1)} x_i x_j + \Theta_1(x) + \Theta_1(x) + x_{o_1+o_2+1} \\
\mathcal{F}^{(o_1+o_2+2)}(x) &= \sum_{v+1 \leq i \leq j \leq v_1} \beta_{j,i}^{(2)} x_i x_j + \Theta_2(x) + \Theta_2(x) + 2 x_{o_1+o_2+2} \\
& \quad \vdots \\
\mathcal{F}^{(o_1+o_2+o_3)}(x) &= \sum_{v+1 \leq i \leq j \leq v_1} \beta_{j,i}^{(o_3)} x_i x_j + \Theta_{o_3}(x) + \Theta_{o_3}(x) + o_3 x_{o_1+o_2+o_3}
\end{align*}
\]
Central map $\mathcal{F}$ of HiMQ 3F

- $\Phi_k(x) = \sum_{1 \leq i \leq j \leq v} \alpha_{i,j}^{(k)} x_i x_j$,  
  $\Psi_k(x) = \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} \alpha_{i,j}^{(o_1+k)} x_i x_j$

- $\Theta_i(x) = \sum_{j=1}^{v_1} \gamma_{i,j} x_i x_{v_1} + (i+j-1)(\text{mod } o_3)$,
  
- $\Theta_i(x) = \sum_{j=1}^{v_2} \gamma_{i,j} x_i x_{v_2} + (i+j-1)(\text{mod } o_3)$

All the quadratic terms in $\Theta_i(x)$ and $\Theta_i(x)$ ($i = 1, \cdots, o_3$) don’t overlap and
symmetric matrix of the quadratic part of each $\mathcal{F}^{(i)}$ has full rank for
$i = o_1 + o_2 + 1, \cdots, m$.

$v \geq 2o_1 + 1$ and $o_2 \geq o_3$. 
Central map $\mathcal{F}$ of HiMQ 3

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

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

- $\Theta_i(x), \Theta'_i(x)$ is the same as HiMQ-3F

All the quadratic terms in $\Phi_i(x)$ ($i = 1, \cdots, o_1$) and $\Psi_i(x)$ ($i = 1, \cdots, o_2$) 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
Symmetric Matrices of the Quadratic Parts of $\mathcal{F}$ for HiMQ 3
Given $\xi = (\xi_1, \ldots, \xi_m)$, find $s$ such that $F(s) = \xi$

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

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

Find solution $(s_{v+1}, \ldots, s_{v+o_1})$ by using E.q. (2) and E.q. (3).
3. To Invert $F^{(i)} (o_1 + 1 \leq i \leq o_1 + o_2)$ in the 2nd layer is similar to Step 1 and Step 2.
4. Plug $(s_1, \ldots, s_{v+o_1+o_2})$ into the polynomials $F^{(i)} (o_1 + o_2 + 1 \leq i \leq m)$.
5. Solve a linear system of $o_3$ equations with $o_3$ variables and find solution $(s_{v+o_1+o_2}, \ldots, s_n)$ 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 \( \mathcal{P} = (P^{(1)}, \ldots, P^{(m)}) \) of \( m \) nonlinear polynomial equations defined over \( \mathbb{F}_q \) with degree of \( d \) in variables \( x_1, \ldots, x_n \) and \( y = (y_1, \ldots, y_m) \in \mathbb{F}_q^m \), find values \( (x_1, \ldots, x_n) \in \mathbb{F}_q^n \) such that \( P^{(1)}(x_1, \ldots, x_n) = y_1, \ldots, P^{(m)}(x_1, \ldots, x_n) = y_m \).

- **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 \( (M_1, \ldots, M_l) \in \mathbb{F}_q^{m \times n} \), find a non-zero \( k \)-tuple \( (\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k \) such that \( \text{Rank}(\sum_{i=1}^k \lambda_i M_i) \leq r \).
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 $\mathbb{F}_{2^8}$.

<table>
<thead>
<tr>
<th>$(\nu, o_1, o_2, o_3)$</th>
<th>$(7,3,3,2)$</th>
<th>$(7,3,3,3)$</th>
<th>$(9,3,3,3)$</th>
<th>$(11,5,3,2)$</th>
<th>$(11,5,4,3)$</th>
<th>$(11,5,4,4)$</th>
<th>$(11,5,5,4)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random System</td>
<td>0.145</td>
<td>0.602</td>
<td>0.618</td>
<td>3.003</td>
<td>112.861</td>
<td>639.576</td>
<td>5753.369</td>
</tr>
<tr>
<td>HiMQ-3</td>
<td>0.134</td>
<td>0.593</td>
<td>0.57</td>
<td>3.203</td>
<td>109.823</td>
<td>756</td>
<td>5712.19</td>
</tr>
</tbody>
</table>
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

\[ C_{HR}(q, o_3, n) = q^{o_3} \cdot \frac{n^3}{6} \]
Complexity of HiMQ-3 against the Kipnis-Shamir Attacks is

\[ C_{KS}(q, \nu, o_1, o_2, o_3) = q^{\nu+o_1+o_2-o_3} \]

Figure: \( S \circ F \) of HiMQ-3
Key recovery attack (KRA)

- Complexity of HiMQ-3 against the KRAs using good keys is
  \[ C_{KRAg}(q, m, n) = C_{MQ}(q, m + n - 1, n + \min(o_1, o_2)) \]

\[ \mathcal{P} = (S \circ \Sigma^{-1}) \circ (\Sigma \circ \mathcal{F} \circ \Omega) \circ (\Omega^{-1} \circ \mathcal{T}) \]
\[ = S \circ \mathcal{F} \circ \mathcal{T} \quad ((S, \mathcal{F}, \mathcal{T}) \text{: equivalent key}) \]

\[ \text{Figure: Equivalent Key of HiMQ-3} \]

\[ \text{Figure: Good Key of HiMQ-3} \]
Existential unforgeability of HiMQ 3

**Theorem**

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

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

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 $n = \nu + m$ if the parameter set ($\mathbb{F}_q, \nu, o_1, o_2, o_3$) is chosen to be secure against the MinRank attack, HighRank attack, Kipnis-Shamir attack and KRAs using good keys.
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 $O_i \times O_i$ 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**: $\text{char}(F_q)=2$, $o_1, o_2$ are odd and $o_2 \geq o_3, v \geq 2o_1 + 1$
- **HiMQ-3**: $\text{char}(F_q)=2$, $o_1, o_2$ 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**

<table>
<thead>
<tr>
<th>$(F_q, v, o_1, o_2, o_3)$</th>
<th>Direct</th>
<th>KRA</th>
<th>Kipnis-Shamir</th>
<th>MinRank</th>
<th>HighRank</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiMQ-3($F_{28}, 31, 15, 15, 14$)</td>
<td>$2^{131}$</td>
<td>$2^{166}$</td>
<td>$2^{368}$</td>
<td>$2^{155}$</td>
<td>$2^{128}$</td>
</tr>
<tr>
<td>HiMQ-3F($F_{28}, 24, 11, 17, 15$)</td>
<td>$2^{129}$</td>
<td>$2^{140}$</td>
<td>$2^{280}$</td>
<td>$2^{131}$</td>
<td>$2^{135}$</td>
</tr>
</tbody>
</table>
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)

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

- Key size and Signature size (Byte)

<table>
<thead>
<tr>
<th>MQ-Scheme</th>
<th>Signature</th>
<th>PK</th>
<th>SK</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiMQ-3((\mathbb{F}_{2^8}), 31, 15, 15, 14)</td>
<td>75</td>
<td>128,744</td>
<td>12,074</td>
</tr>
<tr>
<td>HiMQ-3F((\mathbb{F}_{2^8}), 24, 11, 17, 15)</td>
<td>67</td>
<td>100,878</td>
<td>14,878</td>
</tr>
<tr>
<td>HiMQ-3P((\mathbb{F}_{2^8}), 24, 11, 17, 15)</td>
<td>67</td>
<td>100,878</td>
<td>32</td>
</tr>
<tr>
<td>Scheme</td>
<td>Sig. Size (Bytes)</td>
<td>PK (Bytes)</td>
<td>SK (Bytes)</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>RSA-3072e 128</td>
<td>361</td>
<td>384</td>
<td>3072</td>
</tr>
<tr>
<td>ECDSA-256e 128</td>
<td>64</td>
<td>64</td>
<td>96</td>
</tr>
<tr>
<td>TESLA-416f 128</td>
<td>1,280</td>
<td>1,331,200</td>
<td>1,011,744</td>
</tr>
<tr>
<td>TESLA-768f &gt; 128</td>
<td>2,336</td>
<td>4,227,072</td>
<td>3,293,216</td>
</tr>
<tr>
<td>BLISS-Bi 128</td>
<td>700</td>
<td>875</td>
<td>250</td>
</tr>
<tr>
<td>XMSS (h = 20) 256</td>
<td>3,584</td>
<td>1,536</td>
<td>2,662</td>
</tr>
<tr>
<td>XMSS-Tf (h = 60) 256</td>
<td>2,969</td>
<td>66</td>
<td>2,252</td>
</tr>
<tr>
<td>SPHINCS 256s 256</td>
<td>41,000</td>
<td>1,056</td>
<td>1,088</td>
</tr>
<tr>
<td>Parallel-CFS 80</td>
<td>75</td>
<td>20,968,300</td>
<td>4,194,300</td>
</tr>
<tr>
<td>MQDSS-31-64 &gt; 128 enTTS (F_{28},15,60,88) 128</td>
<td>40,952</td>
<td>72</td>
<td>64</td>
</tr>
<tr>
<td>Rainbow (F_{28},36,21,22) 128</td>
<td>88</td>
<td>234,960</td>
<td>13,051</td>
</tr>
<tr>
<td>HiMQ-3 (F_{28},31,15,15,14) 128</td>
<td>79</td>
<td>139,320</td>
<td>105,006</td>
</tr>
<tr>
<td>HiMQ-3F (F_{28},24,11,17,15) 128</td>
<td>128,744</td>
<td>12,074</td>
<td>21,594</td>
</tr>
<tr>
<td>HiMQ-3P (F_{28},24,11,17,15) 128</td>
<td>67</td>
<td>100,878</td>
<td>14,878</td>
</tr>
</tbody>
</table>

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.