Gui: Revisiting Multivariate Digital Signature Schemes based on HFEv-

Jintai Ding

joint work with A. Petzoldt, M. Chen, B. Yang

PQC Workshop
Gaithersburg, Maryland, USA

02.04.2015
Why this name?

Gui

- Chinese pottery from Longshan period
- more than 4000 years old
- 3 legs: one in front, 2 in the back
- front leg: HFE
- back legs: Minus + Vinegar
Outline

1. Multivariate Cryptography
2. HFEv- based Signature Schemes
3. The new multivariate signature scheme Gui
4. Implementation and Results
Multivariate Cryptography

The security of multivariate schemes is based on the

**Problem MQ:** Given \( m \) multivariate quadratic polynomials \( p^{(1)}(x), \ldots, p^{(m)}(x) \), find a vector \( \bar{x} = (\bar{x}_1, \ldots, \bar{x}_n) \) such that

\[
p^{(1)}(\bar{x}) = \ldots = p^{(m)}(\bar{x}) = 0.
\]
Advantages

- resistant against attacks with quantum computers
- modest computational requirements
  \[ \Rightarrow \text{can be implemented on low cost devices} \]
- Many practical signature schemes:
  - UOV 1999; Rainbow (Multi-layer UOV) 2004
  - QUARTZ 2001
- Very Fast in computations (Except Quartz).
Drawbacks

- Large size of the public and private keys
- Provable security?
  - though Security is strongly supported by experiments and related theory.
- No explicit parameter choices known to meet given levels of security for Quartz.
Construction

- Easily invertible quadratic map $\mathcal{F}: \mathbb{F}^n \to \mathbb{F}^m$
- Two invertible affine (or linear) maps $S: \mathbb{F}^m \to \mathbb{F}^m$ and $T: \mathbb{F}^n \to \mathbb{F}^n$
- Public key: $\mathcal{P} = S \circ \mathcal{F} \circ T$ supposed to look like a random system
- Private key: $S$, $\mathcal{F}$, $T$ allows to invert the public key
(Big Field) Signature Schemes ($m \leq n$)

**Signature Generation**

\[
\begin{align*}
X & \in \mathbb{E} & \mathcal{F}^{-1} & \quad Y \in \mathbb{E} \\
\phi & \quad \phi^{-1} \\
\mathbf{h} & \in \mathbb{F}^m & S^{-1} & \quad \mathbf{x} \in \mathbb{F}^n \\
\mathbf{y} & \in \mathbb{F}^n & \mathcal{T}^{-1} & \quad \mathbf{z} \in \mathbb{F}^n
\end{align*}
\]

**Signature Verification**
HFEv− - Key Generation

- finite field $\mathbb{F}$, extension field $\mathbb{E}$ of degree $n$
- isomorphism $\phi : \mathbb{F}^n \to \mathbb{E}$, $\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \cdot X^{i-1}$
- central map $\mathcal{F} : \mathbb{E} \to \mathbb{E}$,

$$
\mathcal{F}(X) = \sum_{0 \leq i \leq j}^{q^i + q^j \leq D} \alpha_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \leq D} \beta_{i}(v_1, \ldots, v_v) \cdot X^{q^i} + \gamma(v_1, \ldots, v_v)
$$

where $\beta_{i}$ is a linear map from $\mathbb{F}^v$ to $\mathbb{E}$ and $\gamma$ is quadratic
- public key: $\mathcal{P} = S \circ \phi^{-1} \circ \mathcal{F} \circ \phi \circ \mathcal{T}$ with two affine (or linear) maps $S : \mathbb{F}^n \to \mathbb{F}^{n-a}$ and $\mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ of maximal rank
- private key: $S$, $\mathcal{F}$, $\mathcal{T}$, $\phi$
Signature Generation

Given: message $h \in \mathbb{F}^{n-a}$

1. Compute $x = S^{-1}(h) \in \mathbb{F}^n$ and $X = \phi(x) \in \mathbb{E}$
2. Choose random values for the vinegar variables $v_1, \ldots, v_v$
   Solve $F_{v_1,\ldots,v_v}(Y) = X$ over $\mathbb{E}$ via Berlekamp’s algorithm
3. Compute $y = \phi^{-1}(Y) \in \mathbb{F}^n$ and $z = T^{-1}(y || v_1 || \ldots || v_v)$

The signature of the message $h$ is $z \in \mathbb{F}^{n+v}$. 
Signature Verification

Given: signature $z \in \mathbb{F}^n$

- Compute $h' = P(z) \in \mathbb{F}^{n-a}$

- If $h' = h$, the signature is accepted, otherwise rejected.
QUARTZ

- standardized by Courtois, Patarin in 2002
- HFEv\(^{-}\) with \(\mathbb{F} = \text{GF}(2)\), \(n = 103\), \(D = 129\), \(a = 3\) and \(v = 4\)
  \(\Rightarrow \mathbb{E} = \text{GF}(2)^{103} = \text{GF}(2)[x]/(x^{103} + x^9 + 1)\)

\[\mathcal{F}(X) = \sum_{0 \leq i \leq j}^{2^i + 2^j \leq 129} \alpha_{ij} X^{2^i + 2^j} + \sum_{i=0}^{2^i \leq 129} \beta_i(v_1, \ldots, v_4) \cdot X^{2^i} + \gamma(v_1, \ldots, v_4)\]

- public key: quadratic map \(\mathcal{P} : \mathbb{F}^{107} \rightarrow \mathbb{F}^{100}\)
- To avoid birthday attacks, the signature generation step is performed four times (for \(h, \mathcal{H}(h|00), \mathcal{H}(h|01)\) and \(\mathcal{H}(h|11)\))
  \(\Rightarrow\) signature length: \((n - a) + 4 \cdot (a + v) = 128\) bit
Main attacks

- **MinRank Attack**
  \[ \text{Rank}(Q) = r + a + v \]
  \[ \Rightarrow \text{Compl}_{\text{MinRank}} \approx 2^n \cdot (r+a+v) \cdot (n-a)^3 \]

- **Direct attack**
  Recent breakthrough (result by Ding and Yang)
  \[ d_{\text{reg}} \leq \begin{cases} \frac{(q-1) \cdot (r-1+a+v)}{2} + 2 & q \text{ even and } r + a \text{ odd}, \\ \\ \frac{(q-1) \cdot (r+a+v)}{2} + 2 & \text{otherwise}. \end{cases} \]
  with \( r = \lfloor \log_q(D-1) \rfloor + 1. \)
Efficiency

- Signature generation time $\approx 10$ seconds
- Bottleneck: Inversion of the univariate polynomial equation

$$\mathcal{F}_{(v_1, \ldots, v_v)}(Y) = X \quad (1)$$

of degree $D$ over the extension field $\mathbb{E}$ by Berlekamp's algorithm: Complexity $\mathcal{O}(D^3 + n \cdot D^2)$

- equation (1) solvable with probability $\approx \frac{1}{e}$
- we have to solve (1) for 4 different values of $X \Rightarrow$ we have to perform Berlekamp's algorithm about 11 times
Research Questions

- Is the upper bound on the degree of regularity given by Ding and Yang reasonably tight?

- Can we decrease the degree $D$ of the central $HFEv$ polynomial to speed up the scheme?
How should we choose $D$?

- $D \in \{2, 3\}$ would lead to central maps of rank 2 (Matsumoto-Imai case)
- For $D \in \{5, 7\}$ one can get central maps of rank 2 by linear transformation

$\Rightarrow D \in \{9, 17\}$ (central maps of rank 4 and 6 respectively)
Experiments

- Experiments with $HFE_v$— schemes with low degree central maps ($D \in \{9, 17\}$)
- Implementation of $HFE_v$— in MAGMA code
- Fixing of $a + v$ variables to create determined systems
- Adding field equations
- Systems were solved with $F_4$ integrated in MAGMA
# Experiments (2)

\[ D = 9 \]

<table>
<thead>
<tr>
<th>number of equations</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a = v = 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d_{\text{reg}})</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>time (s)</td>
<td>2.7</td>
<td>244</td>
<td>31,537</td>
<td>102,321</td>
</tr>
</tbody>
</table>

| \(a = v = 5\)      |      |      |      |      |
| \(d_{\text{reg}}\) | 5    | 6    | 6    | 7    |
| time (s)            | 2.8  | 255  | 32,481 | ooM |

For comparison: random system

| \(d_{\text{reg}}\) | 5    | 6    | 6    | 7    |
| time (s)            | 3.5  | 310  | 32,533 | ooM |
Experiments (3)

\( D = 17 \)

<table>
<thead>
<tr>
<th>number of equations</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a = v = 3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>theoretical degree of regularity ( \leq 7 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( (n,D,a,v) )</td>
<td>(23,17,3,3)</td>
<td>(28,17,3,3)</td>
<td>(33,17,3,3)</td>
<td>(35,17,3,3)</td>
</tr>
<tr>
<td>( d_{reg} )</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>time (s)</td>
<td>2.4</td>
<td>245</td>
<td>28,768</td>
<td>87,726</td>
</tr>
</tbody>
</table>

| theoretical degree of regularity \( \leq 8 \) |    |    |    |    |
| \( (n,D,a,v) \)     | (24,17,4,4) | (29,17,4,4) | (34,17,4,4) | (36,17,4,4) |
| \( d_{reg} \)       | 5  | 6  | 6  | 7  |
| time (s)            | 2.4| 248| 31,911| ooM|

for comparison: random system

| \( d_{reg} \)       | 5  | 6  | 6  | 7  |
| time (s)            | 3.5| 310| 32,533| ooM|
The theoretical result about the degree of regularity is relatively tight
(for $a = v = 3$ we can reach the upper bound both for $D = 9$ and $D = 17$)

For the parameter sets $(D, a, v) = (9, 5, 5)$ and $(D, a, v) = (17, 4, 4)$ and $n \geq 32$ we have $d_{\text{reg}} \geq 7$

$\Rightarrow$ For $n = 90 + a$ we get

\[
\text{Complexity}_{\text{direct attack}} \geq 3 \cdot \binom{n-a+2}{2} \cdot \binom{n-a+d_{\text{reg}}}{d_{\text{reg}}}^2
\]

\[
= 3 \cdot \binom{92}{2} \cdot \binom{97}{7}^2 \geq 2^{81}
\]
We propose three versions of Gui

- **Gui-95** with \((n, D, a, v) = (95, 9, 5, 5)\) providing a security level of 80 bit
- **Gui-94** with \((n, D, a, v) = (94, 17, 4, 4)\) providing a security level of 80 bit
  and
- **Gui-127** with \((n, D, a, v) = (127, 9, 4, 6)\) providing a security level of 123 bit
Avoiding birthday attacks

- Input size of HFEv- maps is short (in our case 90 - 123 bit) ⇒ Possibility of birthday attacks

- Solution:
  - Sign $k$ different hash values of the message $m$.
  - Combine the $k$ outputs to a single signature of size $(n - a) + k \cdot (a + v)$ bit.

- In the case of Gui we set
  - $k = 3$ for Gui-95,
  - $k = 4$ for Gui-94 and Gui-127.
Gui-95

\[ \text{160 bit} \quad \text{SHA-1}(m) \quad \text{SHA-1}(m||0) \quad \text{160 bit} \]
Multivariate Cryptography

HFEv-

Gui

Implementation

Gui-95

90 bit SHA-1(m) 90 bit SHA-1(m∥0) 90 bit

⇓ HFEv- ⇓ HFEv- ⇓ HFEv-

σ1 100 bit

σ2 100 bit

σ3 100 bit
Multivariate Cryptography

HFEv- Gui

SHA-1(m) → HFEv- → HFEv- → HFEv-

σ_1 100 bit  σ_2 10 bit  σ_3 10 bit

σ 120 bit
## Parameters and Key Sizes

<table>
<thead>
<tr>
<th>scheme</th>
<th>security level (bit)</th>
<th>input size (bit)</th>
<th>signature size (bit)</th>
<th>public key size (Bytes)</th>
<th>private key size (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gui-95</td>
<td>80</td>
<td>90</td>
<td>120</td>
<td>60,600</td>
<td>3,053</td>
</tr>
<tr>
<td>Gui-94</td>
<td>80</td>
<td>90</td>
<td>122</td>
<td>58,212</td>
<td>2,943</td>
</tr>
<tr>
<td>Gui-127</td>
<td>123</td>
<td>123</td>
<td>163</td>
<td>142,576</td>
<td>5,350</td>
</tr>
<tr>
<td>QUARTZ</td>
<td>80</td>
<td>100</td>
<td>128</td>
<td>75,514</td>
<td>3,774</td>
</tr>
<tr>
<td>RSA-1024</td>
<td>80</td>
<td>1024</td>
<td>1024</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>112</td>
<td>2048</td>
<td>2048</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>ECDSA P160</td>
<td>80</td>
<td>160</td>
<td>320</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>ECDSA P192</td>
<td>96</td>
<td>192</td>
<td>384</td>
<td>48</td>
<td>72</td>
</tr>
<tr>
<td>ECDSA P256</td>
<td>128</td>
<td>256</td>
<td>512</td>
<td>64</td>
<td>96</td>
</tr>
</tbody>
</table>
Arithmetic over large fields

We use the fields

- $\text{GF}(2^{95}) = \text{GF}(2)[x]/(x^{95} + x^{11} + 1)$ for Gui-95
- $\text{GF}(2^{94}) = \text{GF}(2)[x]/(x^{94} + x^{21} + 1)$ for Gui-94 and
- $\text{GF}(2^{127}) = \text{GF}(2)[x]/(x^{127} + x + 1)$ for Gui-127.

Furthermore we use

- pclmulqdq instruction set for carry-less multiplication
  (problem: long latency)
- karatsuba algorithm
Inverting the equation $\mathcal{F}(Y) = X$

- We need only the first step of Berlekamp’s algorithm, i.e. the computation of $\text{Gcd}(\mathcal{F}(Y), Y^{2^n} - Y)$.
- How to compute $Y^{2^n} - Y \mod \mathcal{F}(Y)$ efficiently?
- Direct computation is infeasible
  $\Rightarrow$ Recursively square the lower degree polynomial $Y^{2^m}$

\[
(Y^{2^m} \mod \mathcal{F}(Y))^2 \mod \mathcal{F}(Y) = (\sum_{i<2^m} b_i Y^i)^2 \mod \mathcal{F}(Y) = (\sum_{i<2^m} b_i^2 Y^{2i}) \mod \mathcal{F}(Y)
\]

- Prepare a table for $Y^{2i} \mod \mathcal{F}(Y)$
- Square all the coefficients $b_i$ of $Y^{2^m} \mod \mathcal{F}(Y) = \sum_{i<2^m} b_i Y^i$
- Multiply the squared coefficients to the $Y^{2i}$ from the table
Comparison

<table>
<thead>
<tr>
<th>scheme</th>
<th>security level (bit)</th>
<th>signing time (k-cycles)</th>
<th>verifying time (k-cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gui-95</td>
<td>80</td>
<td>1,479 / 1,186</td>
<td>325 / 230</td>
</tr>
<tr>
<td>Gui-94</td>
<td>80</td>
<td>4,945 / 5,421</td>
<td>357 / 253</td>
</tr>
<tr>
<td>Gui-127</td>
<td>123</td>
<td>1,966 / 1,249</td>
<td>707 / 427</td>
</tr>
<tr>
<td>QUARTZ</td>
<td>80</td>
<td>167,485 / 168,266</td>
<td>375 / 235</td>
</tr>
<tr>
<td>RSA-1024</td>
<td>80</td>
<td>2,080 / 2,115</td>
<td>74 / 64</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>112</td>
<td>8,834 / 5,347</td>
<td>138 / 76</td>
</tr>
<tr>
<td>ECDSA P160</td>
<td>80</td>
<td>1,283 / 1,115</td>
<td>1,448 / 1,269</td>
</tr>
<tr>
<td>ECDSA P192</td>
<td>96</td>
<td>1,513 / 1,273</td>
<td>1,715 / 1,567</td>
</tr>
<tr>
<td>ECDSA P256</td>
<td>128</td>
<td>1,830 / 1,488</td>
<td>2,111 / 1,920</td>
</tr>
</tbody>
</table>

time on AMD Opteron 6212, 2.5 GHz / Intel Xeon E5-2620, 2.0 GHz
Conclusion

- Proposal of a new multivariate signature scheme Gui
- Use of low degree HFEv- polynomials \((D \in \{9, 17\})\)

⇒ very short signatures (120 bit)
⇒ 150 times faster than QUARTZ
⇒ Efficiency comparable to standard schemes (RSA, ECDSA)
The end

THANK YOU

Questions?