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

Multivariate Cryptography

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j &+& \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j &+& \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
& & \vdots & \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j &+& \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$

The security of multivariate schemes is based on the

Problem MQ: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}),\ldots,p^{(m)}(\mathbf{x})$, find a vector $\bar{\mathbf{x}} = (\bar{x}_1,\ldots,\bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Multivariate Cryptography (2)

Advantages

- resistant against attacks with quantum computers
- modest computational requirements
  $\Rightarrow$ 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).

Multivariate Cryptography (3)

Drawbacks

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

Multivariate Cryptography (4)

Construction

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

Multivariate Cryptography (5)

(Big Field) Signature Schemes ($m \leq n$)

Signature Generation

$$\begin{tikzcd}
 & X \in \mathbb{E} \arrow[rr, "\mathcal{F}^{-1}"] & & Y \in \mathbb{E} \arrow[d, "\phi^{-1}"] & \\
\mathbf{h} \in \mathbb{F}^m \arrow[r, "\mathcal{S}^{-1}"] & \mathbf{x} \in \mathbb{F}^n \arrow[u, "\phi"] & & \mathbf{y} \in \mathbb{F}^n \arrow[r, "\mathcal{T}^{-1}"] & \mathbf{z} \in \mathbb{F}^n \arrow[llll, bend left, "\mathcal{P}"]
\end{tikzcd}$$

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

Signature Generation

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

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

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

Signature Verification

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

- Compute $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^{n-a}$
- If $\mathbf{h}' = \mathbf{h}$, the signature is accepted, otherwise rejected.

QUARTZ

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

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

- 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 $\mathbf{h}$, $\mathcal{H}(\mathbf{h}|00)$, $\mathcal{H}(\mathbf{h}|01)$ and $\mathcal{H}(\mathbf{h}|11)$)
$\Rightarrow$ signature length: $(n - a) + 4 \cdot (a + v) = 128$ bit

Main attacks

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

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

Efficiency

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

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

  of degree D over the extension field $\mathbb{E}$ by Berlekamps 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 *HFEv*− schemes with low degree central maps ($D \in \{9, 17\}$)
- Implementation of *HFEv*− 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)

$D = 9$

number of equations		20	25	30	32
$a = v = 4$	theoretical degree of regularity ≤ 7				
	(n,D,a,v)	(24,9,4,4)	(29,9,4,4)	(34,9,4,4)	(36,9,4,4)
	d_{reg}	5	6	6	6
	time (s)	2.7	244	31,537	102,321
$a = v = 5$	theoretical degree of regularity ≤ 8				
	(n,D,a,v)	(25,9,5,5)	(30,9,5,5)	(35,9,5,5)	(37,9,5,5)
	d_{reg}	5	6	6	7
	time (s)	2.8	255	32,481	ooM
for comparison: random system					
	d_{reg}	5	6	6	7
	time (s)	3.5	310	32,533	ooM

Experiments (3)

$D = 17$

number of equations		20	25	30	32
$a = v = 3$	theoretical degree of regularity ≤ 7				
	(n,D,a,v)	(23,17,3,3)	(28,17,3,3)	(33,17,3,3)	(35,17,3,3)
	d_{reg}	5	6	6	6
	time (s)	2.4	245	28,768	87,726
$a = v = 4$	theoretical degree of regularity ≤ 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

Results

- 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 $d_{\mathrm{reg}} \geq 7$
$\Rightarrow$ For $n = 90 + a$ we get

$$\begin{aligned}\mathrm{Complexity}_{\mathrm{direct\ attack}} &\geq 3 \cdot \binom{n-a+2}{2} \cdot \binom{n-a+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^2 \\ &= 3 \cdot \binom{92}{2} \cdot \binom{97}{7}^2 \geq 2^{81}\end{aligned}$$

Parameters

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

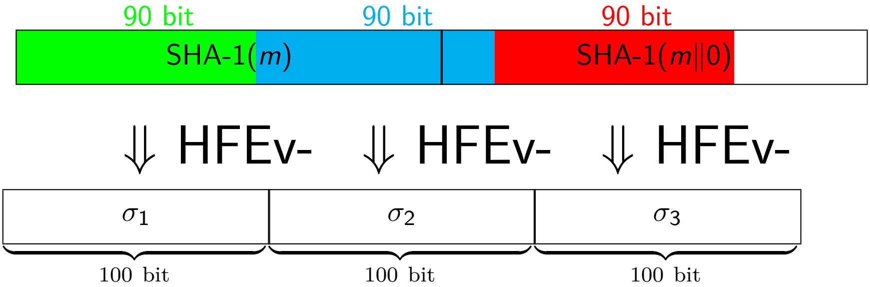
Avoiding birthday attacks

- Input size of HFEv- maps is short (in our case 90 - 123 bit)
  $\Rightarrow$ 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.

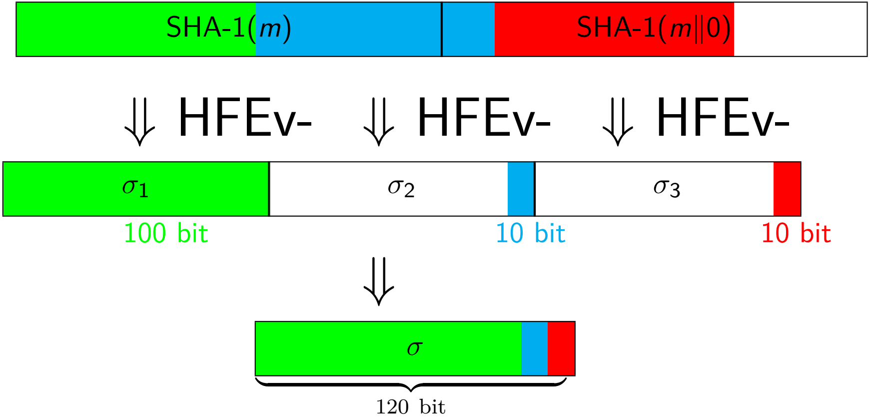
Gui-95

$$\overbrace{\boxed{\text{SHA-1}(m)}}^{160\ \text{bit}}\overbrace{\boxed{\text{SHA-1}(m\|0)}}^{160\ \text{bit}}$$

Gui-95


90 bit
90 bit
90 bit
SHA-1(m)
SHA-1(m||0)
⇓ HFEv-
⇓ HFEv-
⇓ HFEv-
σ1
σ2
σ3
100 bit
100 bit
100 bit

Gui-95


SHA-1(m)
SHA-1($m \| 0$)
⇓ HFEv-
⇓ HFEv-
⇓ HFEv-
σ_1
σ_2
σ_3
100 bit
10 bit
10 bit
⇓
σ
120 bit

Parameters and Key Sizes

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

Arithmetic over large fields

We use the fields

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

Furthermore we use

- pclmuldqd 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 $\mathrm{Gcd}(\mathcal{F}(Y), Y^{2^n} - Y)$.
- How to compute $Y^{2^n} - Y \bmod \mathcal{F}(Y)$ efficiently?
- direct computation is infeasible
  $\Rightarrow$ Recursively square the lower degree polynomial Y^{2^m}

  $$(Y^{2^m} \bmod \mathcal{F}(Y))^2 \bmod \mathcal{F}(Y) =$$
  $$\left(\quad {}_{i<2^m} b_i Y^i \right)^2 \bmod \mathcal{F}(Y) = \left(\quad {}_{i<2^m} b_i^2 Y^{2i} \right) \bmod \mathcal{F}(Y)$$

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

Comparison

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

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 ($D \in \{9, 17\}$)

$\Rightarrow$ very short signatures (120 bit)
$\Rightarrow$ 150 times faster than QUARTZ
$\Rightarrow$ Efficiency comparable to standard schemes (RSA, ECDSA)

The end

THANK YOU

Questions?