GeMSS : A Great Multivariate Short Signature

Ludovic Perret (CryptoNext Security)
joint work with A. Casanova (CS), J.-C. Faugère (CryptoNext Security), G. Macario-Rat (Orange), J. Patarin (UVSQ) and J. Ryckeghem (SU/INRIA)

NIST Third PQC Standardization Conference
Plan

1. Introduction
2. Round-3 Updates
3. Third Party Analysis
Outline

1  Introduction

2  Round-3 Updates

3  Third Party Analysis
Overview

- **GeMSS : A Great Multivariate Short Signature**
  - short signature, fast verification, large public-key given by multivariate polynomials
General Structure [T. Matsumoto, H. Imai, EC’88]

\[ m < n : \#\text{equations}, \; n + \nu : \#\text{variables}, \; \text{nb}_\text{ite} : \#\text{iterations} \]

**Private-Key**

\[ f : (F_2)^{n+\nu} \leftrightarrow (F_2)^m \text{ easy to invert.} \]

\[ f_1(x_1, \ldots, x_{n+\nu}), \]

\[ \vdots \]

\[ \vdots \]

\[ f_m(x_1, \ldots, x_{n+\nu}). \]

\((S, T) \in \text{GL}_{n+\nu}(F_2) \times \text{GL}_m(F_2).\)

**Signature** : \text{nb}_\text{ite} roots finding and inversion of the matrices.

**Public-Key**

\[ p : (F_2)^{n+\nu} \leftrightarrow (F_2)^m \]

\[ p_1(x_1, \ldots, x_{n+\nu}), \]

\[ \vdots \]

\[ \vdots \]

\[ p_m(x_1, \ldots, x_{n+\nu}). \]

\[ p = T \circ f \circ S. \]

**Verification** : \text{nb}_\text{ite} evaluation of polynomials, i.e. \( p(s) = d. \)
Jacques Patarin.
“Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms”.

**HFE\textsuperscript{v} polynomial**

Let $D \in \mathbb{N}$. We define $F(X, v_1 \ldots, v_v) \in \mathbb{F}_{2^n}[X, v_1 \ldots, v_v]$ such that:

$$\sum_{0 \leq i < j \leq n \atop 2^i + 2^j \leq D} A_{i,j} X^{2^i + 2^j} + \sum_{0 \leq i < n \atop 2^i \leq D} \beta_i(v_1, \ldots, v_v) X^{2^i} + \gamma(v_1, \ldots, v_v),$$

where $\beta_i : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is linear and $\gamma(v_1, \ldots, v_v) : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is quadratic.
Jacques Patarin.
“Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms”.
EUROCRYPT ’96.

**HFEv polynomial**

Let $D \in \mathbb{N}$. We define $F(X, \nu_1 \ldots, \nu_v) \in \mathbb{F}_2^n[X, \nu_1 \ldots, \nu_v]$ such that:

$$
\sum_{0 \leq i < j < n \atop 2^i + 2^j \leq D} A_{i,j} X^{2^i+2^j} + \sum_{0 \leq i < n \atop 2^i \leq D} \beta_i(\nu_1, \ldots, \nu_v) X^{2^i} + \gamma(\nu_1, \ldots, \nu_v),
$$

where $\beta_i : \mathbb{F}_2^v \rightarrow \mathbb{F}_2^n$ is linear and $\gamma(\nu_1, \ldots, \nu_v) : \mathbb{F}_2^v \rightarrow \mathbb{F}_2^n$ is quadratic.

- **Guess vinegar variables** $(\nu_1, \ldots, \nu_v)$:

$$
\sum_{0 \leq i < j < n \atop 2^i + 2^j \leq D} A'_{i,j} X^{2^i+2^j} + \sum_{0 \leq i < n \atop 2^i \leq D} B'_i X^{2^i} + C' \in \mathbb{F}_2^n[X].
$$
HFE polynomial

Let $D \in \mathbb{N}$.

$$F(X) = \sum_{0 \leq i < j < n}^{2^i + 2^j \leq D} A'_{i,j}X^{2^i + 2^j} + \sum_{0 \leq i < n}^{2^i \leq D} B'_i X^{2^i} + C' \in \mathbb{F}_{2^n}[X].$$

Roots Finding (Las-Vegas)

We can find all the roots of $F \in \mathbb{F}_{2^n}[X]$ in quasi-linear time:

$$\tilde{O}(n \cdot D).$$

J. von zur Gathen, J. Gerhard:
Outline

1 Introduction

2 Round-3 Updates

3 Third Party Analysis
“GeMSS offers the smallest signatures of any digital signature candidate, supports a reasonably fast verification algorithm [...]”.
“The drawbacks of the scheme include extremely large public keys, difficulty implementing the algorithm on low-end devices, and signing times ranging from slow to very slow. [...], GeMSS seems to be a good and appropriate tool for applications in which offline signing and no transmission of the public key are acceptable and expected”.

- GeMSS Round-3. Faster software implementation (improved key-generation, improved constant-time gcd, ...)
- GeMSS Round-3. New parameters sets to improve arithmetic in $\mathbb{F}_2^n$ for low-end devices
NIST Status Report on Round-2 Candidates

“The drawbacks of the scheme include extremely large public keys, difficulty implementing the algorithm on low-end devices, and signing times ranging from slow to very slow. [...] GeMSS seems to be a good and appropriate tool for applications in which offline signing and no transmission of the public key are acceptable and expected”.

- GeMSS **Round-3**. Faster software implementation (improved key-generation, improved constant-time gcd, ...)
- GeMSS **Round-3**. New parameters sets to improve arithmetic in $\mathbb{F}_2$ for low-end devices

“The second-round inclusion of the RedGeMSS and BlueGeMSS parameter sets offers additional flexibility in the performance properties [...] and appropriately addresses the concerns raised in the previous round. It is possible that there may yet be additional trade-offs to further improve performance”.

- GeMSS **Round-3**. Smaller number of iterations in the Feistel-Patarin construction, leading to WhiteGeMSS(variant of GeMSS), CyanGeMSS (variant of BlueGeMSS) and MagentaGeMSS (variant of RedGeMSS)
  - Signing and verif are 25% faster
Parameter Sets for WhiteGeMSS, CyanGeMSS and MagentaGeMSS

|                | $D$  | $|pk|$ (KB) | $|sk|$ (bits) | sign (bits) |
|----------------|------|------------|--------------|-------------|
| WhiteGeMSS128  | 513  | 358.17     | 128          | 235         |
| WhiteGeMSS192  | 513  | 1293.85    | 192          | 373         |
| WhiteGeMSS256  | 513  | 3222.69    | 256          | 513         |
| CyanGeMSS128   | 129  | 369.72     | 128          | 244         |
| CyanGeMSS192   | 129  | 1320.80    | 192          | 382         |
| CyanGeMSS256   | 129  | 3272.02    | 256          | 522         |
| MagentaGeMSS128| 17   | 381.46     | 128          | 253         |
| MagentaGeMSS192| 17   | 1348.03    | 192          | 391         |
| MagentaGeMSS256| 17   | 3321.72    | 256          | 531         |
Improved Implementation

J.-C. Faugère, L. Perret and J. Ryckeghem
“Software Toolkit for HFE-based Multivariate Schemes”.
CHES’19.

Multivariate Quadratic Software (MQsoft)

- An efficient C library exploiting SSE/AVX2 instructions set.
- Matsumoto-Imai-based schemes: QUARTZ, Gui, GeMSS, ...
- Fast arithmetic in $\mathbb{F}_2[X], \mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n}[X]$ (with root finding), multivariate quadratic systems in $\mathbb{F}$ (evaluation, change of variables, ...), mostly constant-time implementation against timing attacks.
- https://www-polsys.lip6.fr/Links/NIST/MQsoft.html

<table>
<thead>
<tr>
<th>operation</th>
<th>NIST R1</th>
<th>NIST R2</th>
<th>NIST R2 (V2)</th>
<th>NIST R3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keygen</td>
<td>118 MC</td>
<td>$\times$ 3.07</td>
<td>$\times$ 3.05</td>
<td>$\times$ 6.03</td>
</tr>
<tr>
<td>Sign</td>
<td>1270 MC</td>
<td>$\times$ 1.69</td>
<td>$\times$ 2.39</td>
<td>$\times$ 2.09</td>
</tr>
<tr>
<td>Verif</td>
<td>0.166 MC</td>
<td>$\times$ 2.03</td>
<td>$\times$ 1.57</td>
<td>$\times$ 1.57</td>
</tr>
</tbody>
</table>

**Table:** Evolution of GeMSS128 during the process.
## Timings

<table>
<thead>
<tr>
<th>GeMSS128</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>51.9</td>
<td>1080</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>BlueGeMSS128</td>
<td>51.5</td>
<td>154</td>
<td>174</td>
</tr>
<tr>
<td>RedGeMSS128</td>
<td>41.1</td>
<td>4.37</td>
<td>183</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GeMSS192</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>274</td>
<td>3170</td>
<td>495</td>
<td></td>
</tr>
<tr>
<td>BlueGeMSS192</td>
<td>262</td>
<td>445</td>
<td>509</td>
</tr>
<tr>
<td>RedGeMSS192</td>
<td>221</td>
<td>12</td>
<td>514</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GeMSS256</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>915</td>
<td>5300</td>
<td>1120</td>
<td></td>
</tr>
<tr>
<td>BlueGeMSS256</td>
<td>856</td>
<td>658</td>
<td>1130</td>
</tr>
<tr>
<td>RedGeMSS256</td>
<td>765</td>
<td>19.5</td>
<td>1140</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WhiteGeMSS128</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.9</td>
<td>815</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>CyanGeMSS128</td>
<td>54.4</td>
<td>119</td>
<td>116</td>
</tr>
<tr>
<td>MagentaGeMSS128</td>
<td>41.9</td>
<td>3.51</td>
<td>125</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WhiteGeMSS192</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>287</td>
<td>2380</td>
<td>388</td>
<td></td>
</tr>
<tr>
<td>CyanGeMSS192</td>
<td>289</td>
<td>339</td>
<td>396</td>
</tr>
<tr>
<td>MagentaGeMSS192</td>
<td>223</td>
<td>9.38</td>
<td>401</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WhiteGeMSS256</th>
<th>key gen. (MC)</th>
<th>sign (MC)</th>
<th>verify (KC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>960</td>
<td>3910</td>
<td>914</td>
<td></td>
</tr>
<tr>
<td>CyanGeMSS256</td>
<td>963</td>
<td>529</td>
<td>911</td>
</tr>
<tr>
<td>MagentaGeMSS256</td>
<td>750</td>
<td>15.6</td>
<td>936</td>
</tr>
</tbody>
</table>
Outline

1  Introduction

2  Round-3 Updates

3  Third Party Analysis
New Results for PoSSo$_2$

PoSSo$_2$

**Input.** Quadratic non-linear polynomials $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$

**Question.** Find $(z_1, \ldots, z_n) \in \mathbb{F}_2^n$ such that:

$$p_1(z_1, \ldots, z_n) = 0, \ldots, p_m(z_1, \ldots, z_n) = 0.$$  

M. Bardet, J.-C. Faugère, B. Salvy, P.-J. Spaenlehauer.

On the Complexity of Solving Quadratic Boolean Systems.


- Asymptotic complexity $O(2^{0.792m})$
  - GeMSS: derived parameters with $2^{0.792m}$
New Results for PoSSo₂

M. Bardet, J.-C. Faugère, B. Salvy, P.-J. Spaenlehauer.
On the Complexity of Solving Quadratic Boolean Systems.

- Asymptotic complexity $O(2^{0.792m})$
  - GeMSS: derived parameters with $2^{0.792m}$

Itai Dinur.
“Improved Algorithms for Solving Polynomial Systems over GF(2) by Multiple Parity-Counting.”
SODA 2021.

Itai Dinur.
“Cryptanalytic Applications of the Polynomial Method for Solving Multivariate Equation Systems over GF(2).”
EC’2021.

- New asymptotic bound (SODA’21): $\tilde{O}(2^{0.6943n})$
  - Large constant
  - Concrete variant (EC’21) with complexity $m^2 2^{0.815m}$
    - No impact on the parameters proposed for GeMSS
Improved Key-Recovery Attack on GeMSS

C. Tao, A. Petzoldt, J. Ding.
“Improved Key Recovery of the HFEv- Signature Scheme.”

- New modelling of the key-recovery
  - MinRank-based
- Use a new approach for solving MinRank
- Major impact on the security (details, next session)
New Proposal for GeMSS

- (White)GeMSS128 parameter sets less impacted
- Add a new modifier (projection)

M. Oygarden, D. Smith-Tone, J. A. Verbel.
“On the Effect of Projection on Rank Attacks in Multivariate Cryptography.”
Cryptology ePrint Archive, 2021.

- About the same parameter sets, signing time increased.