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

Outline

Overview

- GeMSS : A *Great Multivariate Short Signature*
  - A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret and J. Ryckeghem
  - short signature, fast verification, large public-key given by multivariate polynomials

General Structure [T. Matsumoto, H. Imai, EC'88]

$m < n$: #equations, $n + v$: #variables, $\mathrm{nb\_ite}$: #iterations

Private-Key

$\mathbf{f} : (\mathbb{F}_2)^{n+v} \mapsto (\mathbb{F}_2)^m$ easy to invert.

$$f_1(x_1, \ldots, x_{n+v}),$$
$$\vdots$$
$$\vdots$$
$$f_m(x_1, \ldots, x_{n+v}).$$

$(\mathbf{S}, \mathbf{T}) \in \mathrm{GL_{n+v}}(\mathbb{F}_2) \times \mathrm{GL_m}(\mathbb{F}_2)$.
Signature : $\mathrm{nb\_ite}$ roots finding and inversion of the matrices.

Public-Key

$\mathbf{p} : (\mathbb{F}_2)^{n+v} \mapsto (\mathbb{F}_2)^m$

$$p_1(x_1, \ldots, x_{n+v}),$$
$$\vdots$$
$$\vdots$$
$$p_m(x_1, \ldots, x_{n+v}).$$

$$\mathbf{p} = \mathbf{T} \circ \mathbf{f} \circ \mathbf{S}.$$

Verification : $\mathrm{nb\_ite}$ evaluation of polynomials, i.e. $\mathbf{p}(\mathbf{s})=\mathbf{d}$.

GeMSS Trapdoor – HFEv Vinegar Modifier

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 $F(X, v_1 \ldots, v_v) \in \mathbb{F}_{2^n}[X, v_1 \ldots, v_v]$ such that:

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

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.

GeMSS Trapdoor – HFEv Vinegar Modifier

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 $F(X, v_1 \ldots, v_v) \in \mathbb{F}_{2^n}[X, v_1 \ldots, v_v]$ such that:

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

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.

- Guess vinegar variables $(v_1, \ldots, v_v)$:

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

HFE polynomial

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

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

Roots Finding (Las-Vegas)

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

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

J. von zur Gathen, J. Gerhard:
"Modern Computer Algebra (3. ed.)".
Cambridge University Press 2013.

Outline

NIST Status Report on Round-2 Candidates

"GeMSS *offers the smallest signatures of any digital signature candidate, supports a reasonably fast verification algorithm* [...]".

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 $\mathbb{F}_2^n$ 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 $\mathbb{F}_2^n$ 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

operation	NIST R1	NIST R2	NIST R2 (V2)	NIST R3
Keygen	118 MC	$\times$ 3.07	$\times$ 3.05	$\times$ 6.03
Sign	1270 MC	$\times$ 1.69	$\times$ 2.39	$\times$ 2.09
Verif	0.166 MC	$\times$ 2.03	$\times$ 1.57	$\times$ 1.57

Table: Evolution of GeMSS128 during the process.

Timings

	key gen. (MC)	sign (MC)	verify (KC)
GeMSS128	51.9	1080	163
BlueGeMSS128	51.5	154	174
RedGeMSS128	41.1	4.37	183
GeMSS192	274	3170	495
BlueGeMSS192	262	445	509
RedGeMSS192	221	12	514
GeMSS256	915	5300	1120
BlueGeMSS256	856	658	1130
RedGeMSS256	765	19.5	1140
WhiteGeMSS128	52.9	815	112
CyanGeMSS128	54.4	119	116
MagentaGeMSS128	41.9	3.51	125
WhiteGeMSS192	287	2380	388
CyanGeMSS192	289	339	396
MagentaGeMSS192	223	9.38	401
WhiteGeMSS256	960	3910	914
CyanGeMSS256	963	529	911
MagentaGeMSS256	750	15.6	936

Outline

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.
J. Complexity, 2013.

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

New Results for $\texttt{PoSSo}_2$

M. Bardet, J.-C. Faugère, B. Salvy, P.-J. Spaenlehauer.
On the Complexity of Solving Quadratic Boolean Systems.
J. Complexity, 2013.

- 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) : $\tilde{O}(2^{0.6943\,n})$
  - 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."
Cryptology ePrint Archive, 2020.

- 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.