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)

The Second PQC Standardization Conference

Multivariate Cryptography : More than 30 Years of History

T. Matsumoto and H. Imai.
"Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption".
EUROCRYPT '88.

J. Patarin.
"Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms".
EUROCRYPT'96.

J. Patarin, N. Courtois, L. Goubin.
"QUARTZ, 128-Bit Long Digital Signatures".
CT-RSA 2001.

- Classical candidate for post-quantum cryptography
- Many schemes proposed (44% of second round signature candidates)
- HFE and variants have been extensively studied
  - NESSIE EU standardization process (1999-2003).

GeMSS Trapdoor – HFE Vinegar

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:

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

each $\beta_i : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is linear and $\gamma(v_1, \ldots, v_v) : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is quadratic.

GeMSS Trapdoor – HFE Vinegar

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:

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

each $\beta_i : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is linear and $\gamma(v_1, \ldots, v_v) : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is quadratic.

- Guess vinegar variables $(v_1, \ldots, v_v) \in \mathbb{F}_2^v$:

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

Signature Generation

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 :

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

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

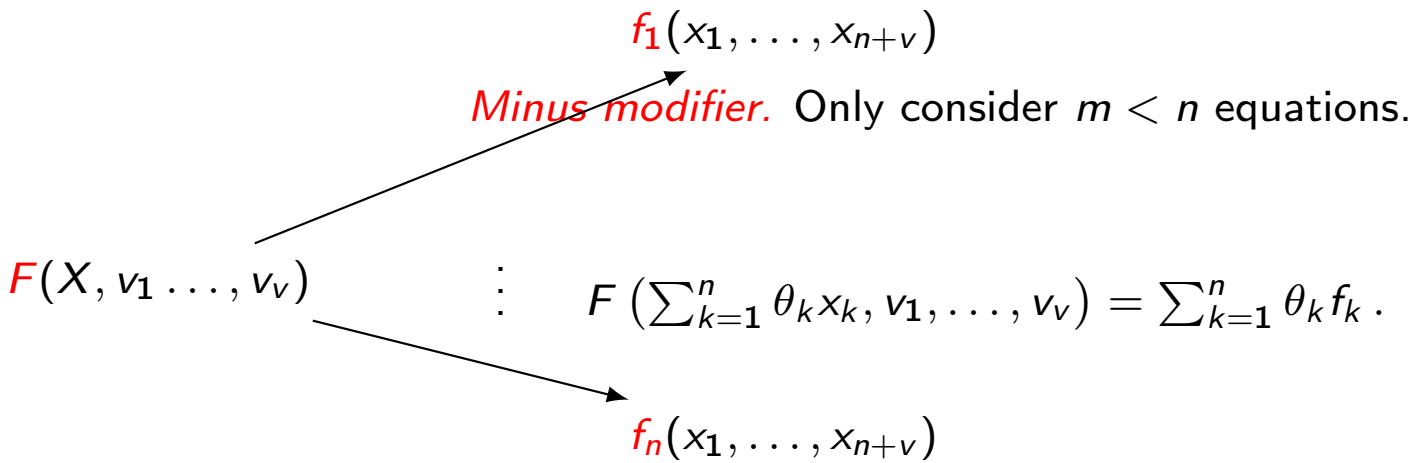
GeMSS KeyGen

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:

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

each $\beta_i : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is linear and $\gamma(v_1, \ldots, v_v) : \mathbb{F}_2^v \to \mathbb{F}_{2^n}$ is quadratic.



General Structure

$m < n$: number of equations, $n + v$: number of variables

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 : Roots finding and invertion 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 : evaluation of polynomials, i.e. $\mathbf{p}(\mathbf{s})=\mathbf{d}$.

Security Analysis

J.-C Faugère, A. Joux.
"Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Groebner Bases".
CRYPTO '03.

$O\left(\binom{n}{D_{\text{reg}}}^2\right)$, Row-echelon form on matrices up to degree D_{reg}

$p_1 = \cdots = p_m = 0$

- B. Buchberger (1965)
- D. Lazard (1983)
- F_4 (J.-C. Faugère, 1999)
- F_5 (J.-C. Faugère, 2002)
- FGLM (J-.C. Faugère, P. Gianni, D. Lazard, T. Mora, 1993)
- ...

Signature

Security Analysis

J.-C Faugère, A. Joux.
"Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Groebner Bases".
CRYPTO '03.

Complexity is driven by the maximal degree D_{reg} reached.

$O\left(\binom{n}{D_{\text{reg}}}^2\right)$, Row-echelon form on matrices up to degree D_{reg}

$p_1 = \cdots = p_m = 0$

- B. Buchberger (1965)
- D. Lazard (1983)
- F_4 (J.-C. Faugère, 1999)
- F_5 (J.-C. Faugère, 2002)
- FGLM (J-.C. Faugère, P. Gianni, D. Lazard, T. Mora, 1993)
- ...

Signature

Generic Techniques

We can fix $n + v - m$ variables

Input. Non-linear public-key polynomials $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_n]$
Question. Find $(z_1, \ldots, z_m) \in \mathbb{F}_2^m$ such that:

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

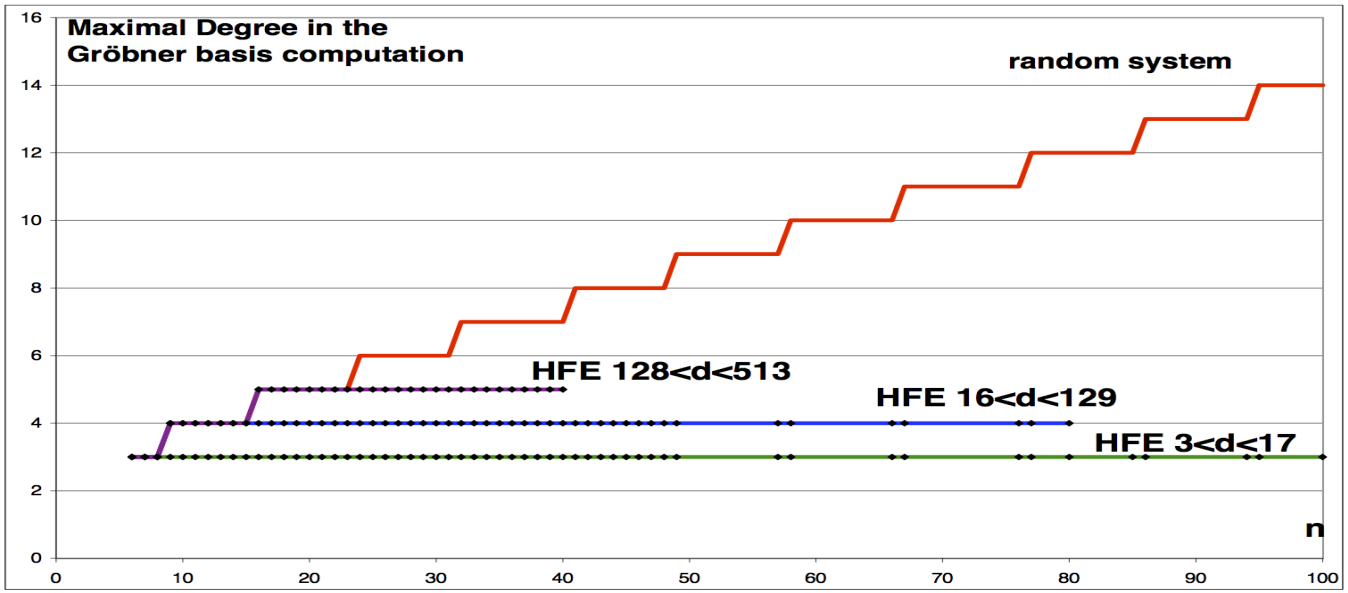
- exhaustive search in $4 \log_2 2^m$ [C. Bouillaguet, C.-Mou Cheng, T. Chou, R. Niederhagen, B-Y. Yang, SAC'2013]
- $O^*(2^{0.8765\, m})$ [D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, H. Yu, SODA'2017], no assumption
- `BooleanSolve` $O(2^{0.792m})$ [M. Bardet, J.-C. Faugère, B. Salvy, P-J. Spaenlehauer, Journal of Complexity, 2013], assumption on the input

Minimal Condition

λ : security parameter:

$$m \geqslant 1.26 \cdot \lambda.$$

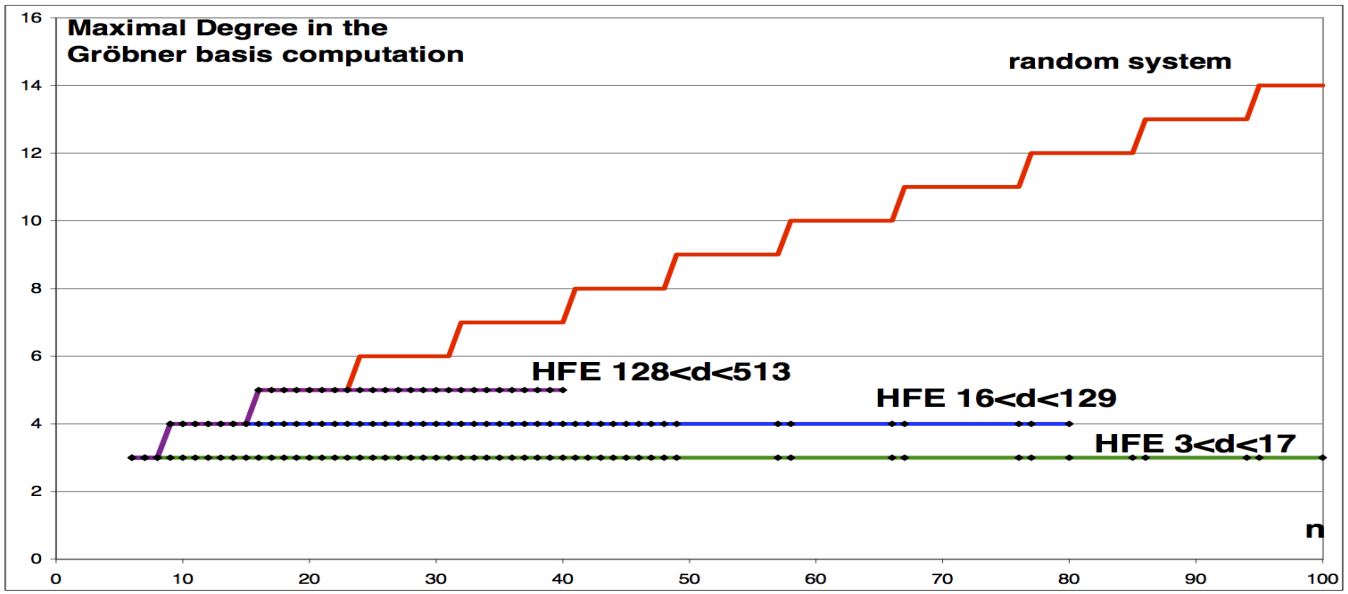
Message Recovery Attack : Nude HFE



Upper bound [Faugère, Joux; L. Granboulan, A. Joux, J. Stern; V. Dubois, N. Gamma; J. Ding, T. Hodges]

$$D_{\text{reg}} \approx \mathcal{O}\big(\log_2(D)\big).$$

Message Recovery Attack : Nude HFE



Experimental approximation

$$D_{\text{reg}} \approx 2.03 + 0.36 \log_2(D).$$

Setting Parameters

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.

Solving a system of $m = n - \Delta$ equations in $n + v$ variables:

$$\binom{m}{D_{\text{reg}}}^2 \geqslant 2^{\lambda}.$$

Nude HFE

$$D_{\text{reg}}^{\text{init}} \approx 2.03 + 0.36 \log_2(D).$$

Setting Parameters

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.

Solving a system of $m = n - \Delta$ equations in $n + v$ variables:

$$\binom{m}{D_{\text{reg}}}^2 \geqslant 2^{\lambda}.$$

Nude `HFE`

$$D_{\text{reg}}^{\text{init}} \approx 2.03 + 0.36 \log_2(D).$$

3 modifiers allow to increase the degree of regularity of nude `HFE` by one (heuristic/experiment rule).

$$\Delta + v \approx \frac{3\lambda}{\log_2(m^2)} - 6.06 - 1.08 \log_2(D).$$

Setting Parameters

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.

Solving a system of $m = n - \Delta$ equations in $n + v$ variables:

$$\binom{m}{D_{\text{reg}}}^2 \geqslant 2^{\lambda}.$$

Nude `HFE`

$$D_{\text{reg}}^{\text{init}} \approx 2.03 + 0.36 \log_2(D).$$

3 modifiers allow to increase the degree of regularity of nude `HFE` by one (heuristic/experiment rule).

$$\Delta + v \approx \frac{3\lambda}{\log_2(m^2)} - 6.06 - 1.08 \log_2(D).$$

General formula for setting the parameters

$$2^{\text{SecRela}(n,\Delta,\log_2(D),v)} \geqslant 2^{\lambda}.$$

Parameters/Performance

NIST Status Report on Round 1 Candidates

"GeMSS *offers some of the* **smallest signature lengths** *among all submissions. GeMSS also benefits from the fact that the HFEv- construction is* **one of the most studied signature primitives** *in the literature. Aside from signature size and verification time, other performance characteristics of* GeMSS *raise some concerns. The* **signing time is quite high and the public keys are quite large**; *these properties may be features of* GeMSS *that are inherent to the HFEv- methodology.*"

- Decrease D and adapt the others parameters.
- Larger set of parameters : GeMSS, BlueGeMSS and RedGeMSS (faster signing and key-generation).

Parameters/Performance

scheme	key gen. (MCycles)	sign (MC)	verify (KC)	$\|pk\|$ (KBytes)	$\|sk\|$ (KB)	sign (bits)
GeMSS128	38.5	750	82	352.19	13.44	258
BlueGeMSS128	39.3	106	111	363.61	13.70	270
RedGeMSS128	39.2	2.79	109	375.21	13.10	282
GeMSS192	175	2320	239	1237.96	34.07	411
BlueGeMSS192	172	331	252	1264.12	35.38	423
RedGeMSS192	171	8.38	255	1290.54	34.79	435
GeMSS256	532	3640	566	3040.70	75.89	576
GeMSS256	529	545	583	3087.96	71.46	588
GeMSS256	523	12.9	588	3135.59	71.89	600

Fastest implementation (AVX2), Intel Core i7-6600U, Skylake, 3,40 GHz.

Multivariate Quadratic Software : MQsoft

J.-C. Faugère, L. Perret and J. Ryckeghem
"Software Toolkit for HFE-based Multivariate Schemes".
CHES'19.

Teaser

- 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

Speed-up

sign. scheme	sec. level	key gen.	sign.	verif.
GeMSS128	128	+220%	+100%	+95%
GeMSS192	192	+220%	+57%	+84%
GeMSS256	256	+240%	+110%	+75%
`Gui-184`	128	+1200%	+100%	+73%
`Gui-312`	192	+1600%	+95%	+56%
`Gui-448`	256	+2500%	+85%	+58%

Improvement of MQsoft w.r.t. fastest first round implementations.

Third-Party Analysis

Quantum analysis

J.-C Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, L. Perret.
"Fast Quantum Algorithm for Solving Multivariate Quadratic Equations".
2018, Under submission.

D. J. Bernstein, B-Y. Yang.
"Asymptotically faster quantum algorithms to solve multivariate quadratic equations".
PQCrypto 2018.

Third-Party Analysis

Improved analysis of the key-revovery

J. Ding, R. A. Perlner, A. Petzoldt, D. Smith-Tone:
"Improved Cryptanalysis of HFEv- via Projection".
PQCrypto 2018.

J. Verbel, J. Baena, D. Cabarcas, R. Perlner, D. Smith-Tone.
"On the Complexity of "Superdetermined" Minrank Instances".
PQCrypto 2019.

Conclusion

- No new attack
- Better understanding of the security
- Improved efficiency
  - Software
  - New parameters
- short signature (258 bits), fast verification ($\approx \mu$ seconds), and large public-key ($\approx$ 352 KBytes)

RISQ