GeMSS **and** DualModeMS
Two Multivariate Submissions to the NIST Standardization Process

Talk given by Rachel Player
Contributors : A. Casanova, J.-C. Faugère, G. Macario-Rat, Ludovic Perret, J. Patarin and J. Ryckeghem

Sorbonne Université, INRIA Paris, CNRS
LIP6, PolSyS Project, Paris, France

First PQC Standardization Conference

NIST

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

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

- DualModeMS : *A Dual Mode for Multivariate-based Signature*
  - J.-C. Faugère, L. Perret and J. Ryckeghem
  - A mode of operation for multivariate signature schemes : larger signature, much smaller public-key (root of a Merkle Tree)

Multivariate Public-Key Cryptography : 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
- Good signature schemes emerged : variants of HFE such as QUARTZ.
  - Candidate to NESSIE portfolio (New European Schemes for Signatures)

General Structure

Private-Key

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

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

$(\mathbf{S}, \mathbf{T}) \in \mathrm{GL}_{n+v}(\mathbb{F}_2) \times \mathrm{GL}_m(\mathbb{F}_2)$.

Public-Key

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

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

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

DualModeMS **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:

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

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.

DualModeMS **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:

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

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 $(v_1, \ldots, v_v)$:

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

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 :

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

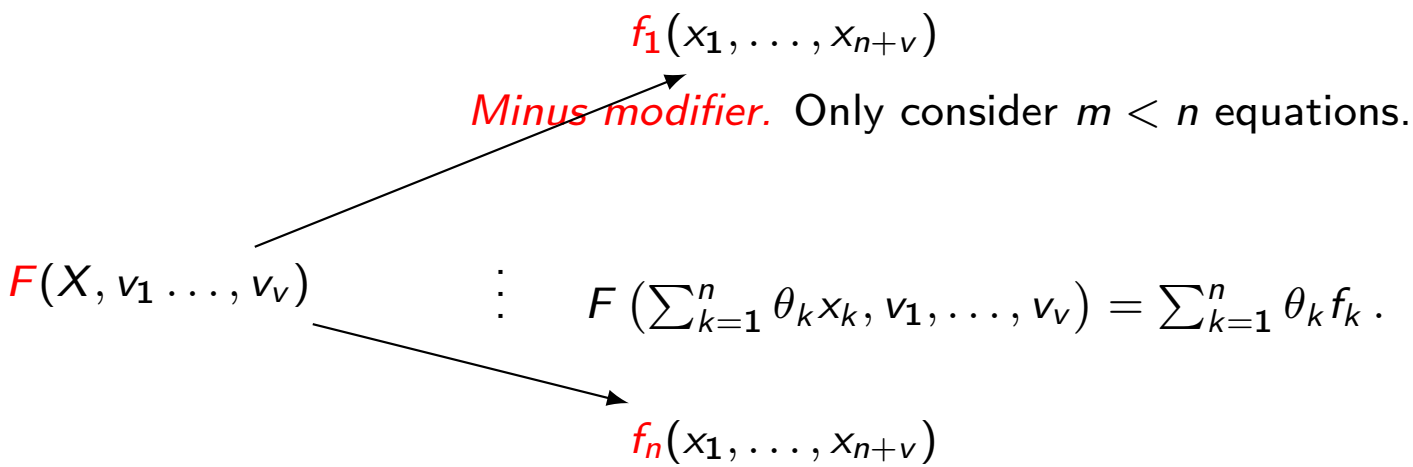
J. von zur Gathen, J. Gerhard:
Modern Computer Algebra (3. ed.).
Cambridge University Press 2013.

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.

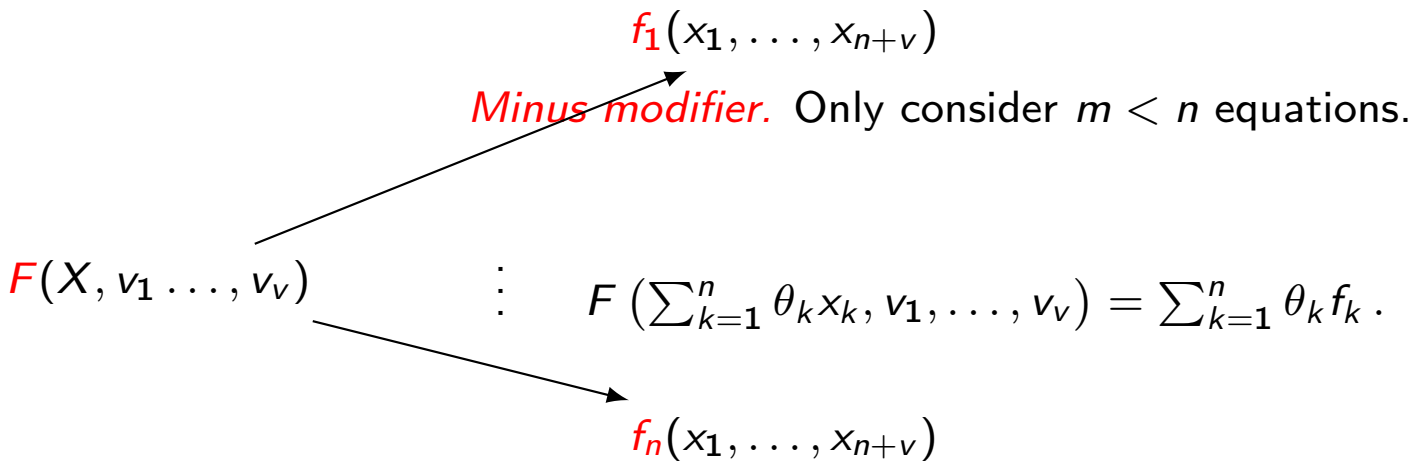


HFEv polynomial

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.



- J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt and Bo-Yin Yang, "Gui".

Signing/Verification Process

GeMSS.Sig(M)

$\mathbf{H} \leftarrow \mathrm{SHA3}(\mathbf{M})$
$\mathbf{S}_0 \leftarrow \mathbf{0} \in \mathbb{F}_2^m$
For i from 1 to nb_ite **do**
  $\mathbf{D}_i \leftarrow$ first m bits of $\mathbf{H}$
  $(\mathbf{S}_i, \mathbf{X}_i) \leftarrow \mathrm{GeMSS.Inv}_{\mathbf{p}}(\mathbf{D}_i \oplus \mathbf{S}_{i-1})$
    $\triangleright\ \mathbf{S}_i \in \mathbb{F}_2^m, \mathbf{X}_i \in \mathbb{F}_2^{n-m}$, and $\mathbf{p}(\mathbf{S}_i, \mathbf{X}_i) = \mathbf{D}_i \oplus \mathbf{S}_{i-1}$
  $\mathbf{H} \leftarrow \mathrm{SHA3}(\mathbf{H})$
EndFor
Return $(\mathbf{S}_{\mathrm{nb\_ite}}, \mathbf{X}_{\mathrm{nb\_ite}}, \ldots, \mathbf{X}_1)$

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

Signing/Verification Process

GeMSS.Verif($\mathbf{M}$,($\mathbf{S}_{\mathrm{nb\_ite}}, \mathbf{X}_{\mathrm{nb\_ite}}, \ldots, \mathbf{X}_1$))

$\mathbf{H} \leftarrow \mathrm{SHA3}(\mathbf{M})$
For i from 1 to $\mathrm{nb\_ite}$ **do**
  $\mathbf{D}_i \leftarrow$ first m bits of $\mathbf{H}$; $\mathbf{H} \leftarrow \mathrm{SHA3}(\mathbf{H})$
EndFor
For i from $\mathrm{nb\_ite} - 1$ to 0 **do**
  $\mathbf{S}_i \leftarrow \mathbf{p}(\mathbf{S}_{i+1}, \mathbf{X}_{i+1}) \oplus \mathbf{D}_{i+1}$
EndFor
Return VALID if $\mathbf{S}_0 = \mathbf{0}$ and INVALID otherwise.

Number of iterations ($\mathrm{nb\_ite} = 4$ in GeMSS.)

Let λ be the sec. parameter. The number of iterations $\mathrm{nb\_ite}$ is s.t.:

$$2^{m \frac{\mathrm{nb\_ite}}{\mathrm{nb\_ite}+1}} \geqslant 2^{\lambda}.$$

N. Courtois.
"Generic Attacks and the Security of QUARTZ".
Public Key Cryptography 2003.

Direct Signature Forgery Attack – Generic Techniques

We can fix $n + v - m$ variables

Input. Non-linear public-key polynomials $p_1, \ldots, p_m \in \mathbb{F}_2[x_1, \ldots, x_m]$
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],
- `BooleanSolve` $O(2^{0.792m})$ [M. Bardet, J.-C. Faugère, B. Salvy, P-J. Spaenlehauer, Journal of Complexity, 2013],
- ...

Minimal (Conservative) Condition

λ : security parameter:

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

Quantum Setting

Quantum Exhaustive Search [P. Schwabe, B. Westerbaan, Solving Binary MQ with Grover's Algorithm. 2016]

- We can solve m binary quadratic equations in m binary variables using $O(m)$ qubits, and evaluating $O(2^{m/2}m^3)$ quantum gates

Quantum Setting

Quantum Exhaustive Search [P. Schwabe, B. Westerbaan, Solving Binary MQ with Grover's Algorithm. 2016]

- We can solve m binary quadratic equations in m binary variables using $O(m)$ qubits, and evaluating $O(2^{m/2}m^3)$ quantum gates

`QuantumBooleanSolve/GroverXL` (Hybrid approach+Grover's algorithm)

- $O(2^{0.462m})$, "*Fast Quantum Algorithm for Solving Multivariate Quadratic Equations*" [J.-C Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, L. Perret, 2017]
- When $q = 2$, $O(2^{0.472m})$, "*Asymptotically faster quantum algorithms to solve multivariate quadratic equations*" [D. J. Bernstein, B-Y. Yang, PQC 2018]

(Some) Structural Attacks

- Message recovery attack [J.-C. Faugère, A. Joux, 2003]
  - First HFE challenge broken ($n = 80, q = 2, D = 96$, 80 bits security)
  - Theoretical degree of regularity ([L. Granboulan, A. Joux, J. Stern, 2006], [V. Dubois, N. Gamma, 2011], [J. Ding, T. Hodges, 2012], [L. Bettale, J.-C. Faugère, and L. Perret, 2013)
- Key-recovery (MinRank) attack [A. Kipnis, A. Shamir, 1999, J. Ding, Schmidt, Werner, 2008]
- Weak keys [C. Bouillaguet, P.-A. Fouque, A. Joux, J. Treger, 2011]
- Differential properties [T. Daniels, D. Smith-Tone]
- Improved Cryptanalysis of `HFEv-` via Projection [J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone, PQC18]
- ...

(Some) Structural Attacks

- Message recovery attack [J.-C. Faugère, A. Joux, 2003]
  - First HFE challenge broken ($n = 80, q = 2, D = 96$, 80 bits security)
  - Theoretical degree of regularity ([L. Granboulan, A. Joux, J. Stern, 2006], [V. Dubois, N. Gamma, 2011], [J. Ding, T. Hodges, 2012], [L. Bettale, J.-C. Faugère, and L. Perret, 2013)
- Key-recovery (MinRank) attack [A. Kipnis, A. Shamir, 1999, J. Ding, Schmidt, Werner, 2008]
- Weak keys [C. Bouillaguet, P.-A. Fouque, A. Joux, J. Treger, 2011]
- Differential properties [T. Daniels, D. Smith-Tone]
- Improved Cryptanalysis of HFEv- via Projection [J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone, PQC18]
- ...

Conclusion

- All known attacks against HFEv-/ GeMSS are exponential in $O(\log_2(D))$, the number of equations removed, and the vinegar v.

(Some) Structural Attacks

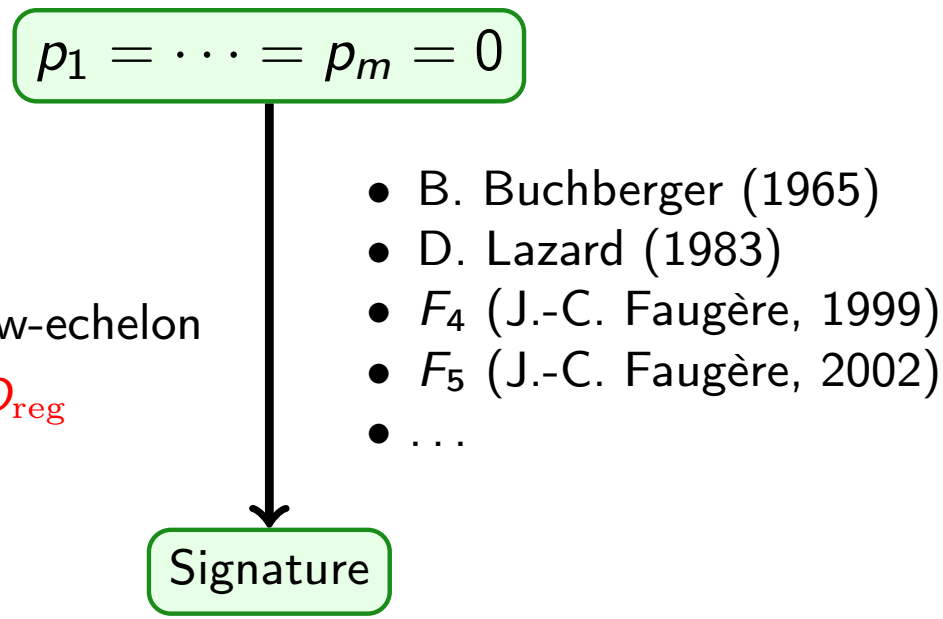
- Message recovery attack [J.-C. Faugère, A. Joux, 2003]
  - First HFE challenge broken ($n = 80, q = 2, D = 96$, 80 bits security)
  - Theoretical degree of regularity ([L. Granboulan, A. Joux, J. Stern, 2006], [V. Dubois, N. Gamma, 2011], [J. Ding, T. Hodges, 2012], [L. Bettale, J.-C. Faugère, and L. Perret, 2013)
- Key-recovery (MinRank) attack [A. Kipnis, A. Shamir, 1999, J. Ding, Schmidt, Werner, 2008]
- Weak keys [C. Bouillaguet, P.-A. Fouque, A. Joux, J. Treger, 2011]
- Differential properties [T. Daniels, D. Smith-Tone]
- Improved Cryptanalysis of HFEv- via Projection [J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone, PQC18]
- ...

Conclusion

- All known attacks against HFEv-/ GeMSS are exponential in $O(\log_2(D))$, the number of equations removed, and the vinegar v.
- How to set the parameters ?

Reference attack [J.-C. Faugère, A. Joux, 2003] – Computing a Gröbner Basis

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



- B. Buchberger (1965)
- D. Lazard (1983)
- F_4 (J.-C. Faugère, 1999)
- F_5 (J.-C. Faugère, 2002)
- ...

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

Setting Parameters – Predicting D_{reg}

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.
- GeMSS, $m = 1.26 \cdot \lambda$; Gui $m > 1.26 \cdot \lambda$
- Gui has a bigger public-key than GeMSS.

Setting Parameters – Predicting D_{reg}

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.
- GeMSS, $m = 1.26 \cdot \lambda$; Gui $m > 1.26 \cdot \lambda$
- Gui has a bigger public-key than GeMSS.

D_{reg} is a function of the modifiers Δ and v that has to verify:

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

Heuristic/experiment rule:

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

Setting Parameters – Predicting D_{reg}

- λ : security parameter, number of equations $m \geqslant 1.26 \cdot \lambda$.
- GeMSS, $m = 1.26 \cdot \lambda$; Gui $m > 1.26 \cdot \lambda$
- Gui has a bigger public-key than GeMSS.

D_{reg} is a function of the modifiers Δ and v that has to verify:

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

Heuristic/experiment rule:

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

- "On the Complexity of the Hybrid Approach on HFEv-" [A. Petzoldt]
- Gui has a faster signature generation : m is bigger but D is smaller.
  - Large choice of parameters proposed for GeMSS.

Great Multivariate Short Signature (GeMSS)

Sizes

sec. level	sec. key	pub. key	signature size
Level I	13.44 KBytes	352.19 KBytes	258 bits
Level II	34.07 KBytes	1,237.96 KBytes	411 bits
Level III	75.89 KBytes	3,040.70 KBytes	576 bits

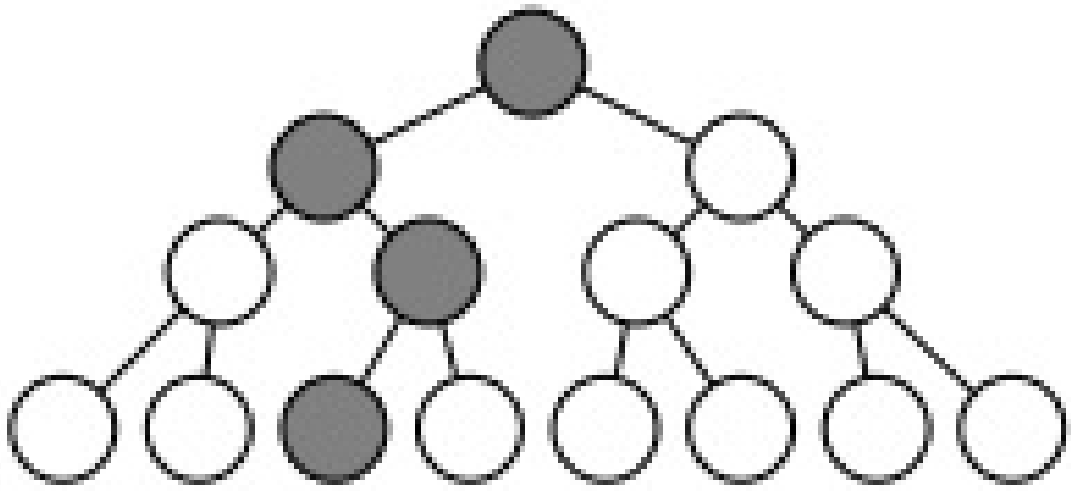
Benchmark results (Optimized version, AVX2)

sec. level	key gen.	signature gen.	signature verif.
I	76.51 MC/ 27ms	687.43 MC/245 ms	0.070M/25μs
II	377.31MC/134 ms	2,414.72MC/860ms	0.193MC/69μs
III	1,055.28 MC/376 ms	3,859.12MC/1,374 ms	0.498MC/177μs

Motivation

- Decrease the public-key size of GeMSS
  - Partially includes the public-key into the signature and the (new) secret-key,
  - New public-key is a Merkle tree; signature includes also an authentication path
  - General technique (Gui, and others multivariate sig. schemes)

A. Szepieniec, W. Beullens, Bart Preneel.
"MQ Signatures for PKI".
PQC, 2017.



A Dual Mode for Multivariate-based Signature (DualModeMS)

- On top of GeMSS
- Additional (Generalized) MinRank assumption

Sizes

sec. level (DualModeMS)	sec. key	pub. key	signature size
Level 1	1.8 MBytes	528 Bytes	32 KB

A Dual Mode for Multivariate-based Signature (DualModeMS)

- On top of GeMSS
- Additional (Generalized) MinRank assumption

Sizes

sec. level (DualModeMS)	sec. key	pub. key	signature size
Level 1	1.8 MBytes	528 Bytes	32 KB

sec. level (GeMSS)	sec. key	pub. key	signature size
Level 1	14 KBytes	352.18 KBytes	258 bits

sec. level (DualModeMS)	key gen.	signature gen.	signature verif.
Level 1	$1,988,572$MC/	$7,8$ MC	10 MC

Conclusion

- DualModeMS can be instantiated with LUOV, Gui, . . . (work in progress)
- EU-CMA variant of GeMSS described in the submission
- GeMSS is currently deployed into an industrial demonstrator of CS

RISQ Project

Idea

Let $\mathbf{p} \in \mathbb{F}_2[x_1, \ldots, x_{n+v}]^m$ be the pk of GeMSS.

$$\mathbf{p}(\mathbf{s_1}) = \mathbf{D_1}, \ldots, \mathbf{p}(\mathbf{s}_\sigma) = \mathbf{D}_\sigma, \text{ with } \mathbf{D_i} = \mathrm{Hash}(\mathbf{M} \,||\, i).$$

$\mathbf{t} \in \mathcal{M}_{m,\alpha}(\mathbb{F}_q)$ generated from $\mathbf{s_1}, \ldots, \mathbf{s}_\sigma$ and:

$$\mathbf{R} = \mathbf{p} \times \mathbf{t} \qquad \mathbf{R}(\mathbf{s_1}) = \mathbf{D_1} \times \mathbf{t}, \ldots, \mathbf{R}(\mathbf{s}_\sigma) = \mathbf{D}_\sigma \times \mathbf{t}$$

First attempt, new signature is $(\mathbf{s_1}, \ldots, \mathbf{s}_\sigma, \mathbf{R})$.

PKI for Multivariate Signatures

Problem

- How to check that $\mathbf{R} = \mathbf{p} \times \mathbf{t}$?
  - Simplified answer : evaluate the equality on several points; construct a Merkle tree with these points to authenticate it.