G*e*MSS: A Gr*e*at Multivariate Short Signature

Principal submitter

This submission is from the following team, listed in alphabetical order:

- A. Casanova, CS
- J.-C. Faugère, CryptoNext, INRIA and Sorbonne University
- G. Macario-Rat, Orange
- J. Patarin, University of Versailles
- L. Perret, CryptoNext, Sorbonne University and INRIA
- J. Ryckeghem, Sorbonne University and INRIA

E-mail address: `ludovic.perret@lip6.fr`

Telephone : +33-1-44-27-88-35

Postal address:
Ludovic Perret
Sorbonne Université
LIP6 - Équipe projet INRIA/SU POLSYS
Boite courier 169
4 place Jussieu
F-75252 Paris cedex 5, France

Auxiliary submitters: There are no auxiliary submitters. The principal submitter is the team listed above.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: Same as submitter.

Signature: $\times$. See also printed version of "Statement by Each Submitter".

1 Changes for the second round

The goal of this part is to summarize the modifications done on GeMSS for the second round.

1.1 Large set of parameters

The parameters proposed for GeMSS in the first round were very conservative in term of security. In [5], it was suggested to explore different parameters in order to improve efficiency. We address this comment as follows.

- We added a new Section 9 to discuss the parameters.
- In Section 9.6, we present an exhaustive table including possible parameters and the corresponding timings.
- In Section 9.5, we explore the use of sparse polynomials in GeMSS to improve the efficiency of the signing process.
- We then suggest 3 sets of parameters for each security level with several trade-offs. This includes the initial parameters of GeMSS proposed in the first round, and two new more aggressive parameters (BlueGeMSS and RedGeMSS).
  - RedGeMSS128 is 269 times faster than GeMSS128.
  - BlueGeMSS128 is 7.08 times faster than GeMSS128.
- We design a family of possible values that depends on only one parameter n. We call this family FGeMSS(n) (Section 9.4).

1.2 Further details on known attacks

The paper [2] was published at about the same time than the deadline for the first round. In this revision, we further details [2] in Section 8 (Analysis of known attacks). We added two new sub-sections (8.3.4 and 8.4.2) to explain the attacks from [2]. This attack permits to give more insight on how to balance the number of modifiers. These attacks tend to confirm that taking the same number of minus and same number of vinegar variables is a safe choice.

1.3 Implementation and Performance

Since the submission, we also drastically improved the keypair generation, the signing process as well as the root finding. These are key steps for the efficiency of GeMSS. We have a paper accepted at CHES on this topic [4, 1]. This paper presents also `MQsoft`, an efficient library which permits to implement HFE-based multivariate schemes submitted to the NIST PQC process such as GeMSS, Gui and DualModeMS. The library is implemented in `C` targeting Intel 64-bit processors and using avx2 set instructions. `MQsoft` permits, in partiular, to

- perform an efficient constant-time arithmetic in $\mathbb{F}_{2^n}$.

- to find the roots of a univariate polynomial in $\mathbb{F}_{2^n}[X]$. We have specialized algorithms for the `HFE` polynomials.
- to evaluate efficiently multivariate quadratic systems in $\mathbb{F}_2$ (in constant-time and in variable-time).
- to implement the dual mode of Matsumoto-Imai based multivariate signature schemes (cf. DualModeMS [3]).

Our new submitted implementations are more secure against timing attacks.

- We have removed `NTL` in the optimized and additional implementations. We have added a constant-time implementation of the inverse in $\mathbb{F}_{2^n}$ (which replaces the use of `NTL`).
- During the keypair generation, the determinant and the inversion of matrices in $M_n(\mathbb{F}_2)$ are achieved in constant-time. In particular, we have implemented a constant-time Gaussian elimination. Now, the keypair generation is immune against timing attacks.
- During the signing process, the Frobenius map is achieved in constant-time. We assume the degree of the current polynomial in $\mathbb{F}_{2^n}[X]$ is $D-1$ and its square has a degree $2D-2$. In particular, we compute the square of the zero coefficients.

Our practical sizes are shorter.

- We have added an algorithm to compress and uncompress the signature. Now, the theoretical size is the same than the practice size.
- When the public-key has 324 equations, we have added "an hybrid representation" which permits to have a practice size similar to the theoretical size. The practical size of the 320 first equations is exactly the theoretical size.

Several algorithms are improved:

- The computation of the components of F is faster. When $v=0$, the old complexity was $O(n^2\log_2(D)^2)$ multiplications in $\mathbb{F}_{2^n}$. The new complexity is $O(n\log_2(D)(n+\log_2(D)))$ multiplications in $\mathbb{F}_2[X]$ and $O(n(n+\log_2(D)))$ modular reductions.
- When n is large compared to D, we compute the Frobenius map by using multi-squaring tables.

Our implementations use only the `ranbombytes` function for the random generation. In particular, we have modified the equal-degree factorization algorithm from `NTL`, for using `ranbombytes`.

References

[1] MQsoft: a fast multivariate cryptography library, December 2018. https://www-polsys.lip6.fr/Links/NIST/MQsoft.html.

[2] Jintai Ding, Ray A. Perlner, Albrecht Petzoldt, and Daniel Smith-Tone. Improved cryptanalysis of hfev- via projection. In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 375–395, 2018.

[3] Jean-Charles Faugère, Ludovic Perret, and Jocelyn Ryckeghem. DualModeMS: A Dual Mode for Multivariate-based Signature. Research report, UPMC - Paris 6 Sorbonne Universités ; INRIA Paris ; CNRS, December 2017.

[4] Jean-Charles Faugère, Ludovic Perret, and Jocelyn Ryckeghem. Software toolkit for hfe-based multivariate schemes. 2019 (forthcoming).

[5] NIST. Status report on the first round of the nist post-quantum cryptography standardization process.