GeMSS: A Great Multivariate Short Signature

Principal submitter

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

- A. Casanova, CS
- J.-C. Faugère, INRIA and Sorbonne Universities/UPMC Univ Paris 06
- G. Macario-Rat, Orange
- J. Patarin, University of Versailles
- L. Perret, Sorbonne Universities/UPMC Univ Paris 06 and INRIA
- J. Ryckeghem, Sorbonne Universities/UPMC Univ Paris 06 and INRIA

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

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

Postal address:
Ludovic Perret
Université Pierre et Marie Curie
LIP6 - Équipe projet INRIA/UPMC POLSYS
Boite courier 169
4 place Jussieu
F-75252 Paris cedex 5, France

1 Introduction

sparkling GeMSS *spring up from the night sky*
a dazzling splendor to ever beautify
sequined glories that verily eye smack
sparkling GeMSS *spring up from night sky*
studding the vast backdrop of black

The purpose of this document is to present GeMSS : a Great Multivariate Signature Scheme. As suggested by its name, GeMSS is a multivariate-based [14, 22, 4, 2, 20, 19] signature scheme producing small signatures. It has a fast verification process, and a medium/large public-key. GeMSS is in direct lineage from `QUARTZ` [18] and borrows some design rationale of the `Gui` multivariate signature scheme [5]. The former schemes are built from the *Hidden Field Equations* crypotsystem (`HFE`) [17, published in 1996] by using the so-called minus and vinegar modifiers, i.e. `HFEv-` [12]. It is fair to say that `HFE`, and its variants, are the most studied schemes in multivariate cryptography. `QUARTZ` produces signatures of 128 bits for a security level of 80 bits and was submitted to the *Nessie Ecrypt* competition [15] for public-key signatures. In contrast to many multivariate schemes, no practical attack has been reported against `QUARTZ`. This is remarkable knowing the intense activity in the cryptanalysis of multivariate schemes, e.g. [16, 13, 7, 8, 11, 10, 6, 9, 4, 2, 3, 1, 19, 21]. The best known attack remains [8] that serves as a reference to set the parameters for GeMSS.

GeMSS is a faster variant of `QUARTZ` that incorporates the latest results in multivariate cryptography to reach higher security levels than `QUARTZ` whilst improving efficiency.

Acknowledgement. G*e*MSS has been prepared with the support of the french Programme d'Investissement d'Avenir under national project RISQ[1] P141580.

2 Advantages and limitations (2.B.6)

Since the first scheme of Mastumoto and Imai [14] in 1988, almost 30 years ago, multivariate-based cryptosystems have been extensively analysed in the literature. We have designed G*e*MSS using this knowledge and taking conservative choices for deriving parameters. We also performed practical experiments using the best known tools for computing Gröbned bases.

From a practical point of view, the main drawback of G*e*MSS is the size of the public-key. However, we mention that the generation of a (public-key,secret-key) remains rather efficient in G*e*MSS. The main advantages of G*e*MSS are the size of the signatures generated, about 2λ bits, and the fast verification process.

References

[1] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. *Des. Codes Cryptography*, 69(1):1–52, 2013.

[2] Olivier Billet and Jintai Ding. *Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography*, pages 263–283. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[3] Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat. Practical key-recovery for all possible parameters of SFLASH. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer, 2011.

[4] Jintai Ding and Bo-Yin Yang. *Multivariate Public Key Cryptography*, pages 193–241. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[5] Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFEv-. In Philippe Gaborit, editor, *Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings*, volume 7932 of *Lecture Notes in Computer Science*, pages 52–66. Springer, 2013.

[6] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. Practical cryptanalysis of SFLASH. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

[7] Jean-Charles Faugère. Algebraic cryptanalysis of HFE using Gröbner bases. Reasearch report RR-4738, INRIA, 2003.

[1] https://risq.fr/?page_id=31&lang=en

[8] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

[9] Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, and Jacques Stern. Total break of the l-ic signature scheme. In Ronald Cramer, editor, *Public Key Cryptography - PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, March 9-12, 2008. Proceedings*, volume 4939 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2008.

[10] Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 44–57. Springer, 2000.

[11] Louis Granboulan, Antoine Joux, and Jacques Stern. Inverting HFE is quasipolynomial. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 345–356. Springer, 2006.

[12] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.

[13] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[14] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynominal-tuples for efficient signature-verification and message-encryption. In *EUROCRYPT*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer, 1988.

[15] NESSIE. New european schemes for signatures, integrity, and encryption, 2003.

[16] Jacques Patarin. Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt'88. In Don Coppersmith, editor, *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Springer, 1995.

[17] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[18] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Quartz, 128-bit long digital signatures. In David Naccache, editor, *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track*

at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, Proceedings, volume 2020 of *Lecture Notes in Computer Science*, pages 282–297. Springer, 2001.

[19] Ludovic Perret. *Bases de Gröbner en Cryptographie Post-Quantique. (Gröbner bases techniques in Quantum-Safe Cryptography)*. 2016.

[20] ETSI ISG QSC. Quantum-safe cryptography (QSC); quantum-safe algorithmic framework. http://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf.

[21] Jeremy Vates and Daniel Smith-Tone. Key recovery attack for all parameters of HFE-. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 272–288. Springer, 2017.

[22] Christopher Wolf. *Multivariate quadratic polynomials in public key cryptography*. Univ. Leuven Heverlee, 2005.