Digital Signatures in a Quantum World: Evaluating The Trade-off Between Performance and Security for GeMSS

Paulo Ricardo Reis[1]
Fábio Borges[1]

[1]National Laboratory for Scientific Computing (LNCC)
25651-075 – Petrópolis – RJ – Brazil
{paulorbr,borges}@lncc.br

Abstract. *With the advent of quantum computing, it urges the definition of a cryptographic standard algorithm that can resist attacks from a quantum computer. Inside this context is GeMSS, a multivariate quadratic signature scheme based on the HFEv- construct. Schemes of this type have shown great potential throughout the last two decades. This paper traces a comparison of performance and security between GeMSS and other relevant digital signature schemes, showing that despite of its slow signature generation and large key pair, it has a very quick verification process and tiny signatures. It also proposes a method for deriving the size of keys from the security parameter evaluated.*

1. Introduction

In 1995, Peter Shor [Shor 1995] published an algorithm to run on a quantum computer capable of solving, in polynomial time, the Integer Factorization Problem (IFP) and the Discrete Logarithm Problem (DLP). These are considered hard mathematical problems for classical computers and are the most used in today cryptosystems. Another enemy of modern cryptography is Grover's quantum algorithm [Grover 1996] that can speed up the searching for cryptographic keys. Although quantum computers are not an immediate threat, their power is unavoidable as soon as they have evolved enough, therefore it is needed that quantum-safe cryptosystems are constructed and properly evaluated.

Given that scenario, cryptosystems based on the Multivariate Quadratic Problem (MQ) are a great bet. Patarin and Goubin [Patarin and Goubin 1997] showed that this problem is NP-complete and that there is no known, classical or quantum, algorithm that can solve it in polynomial time [Bernstein 2009][Nielsen and Chuang 2002]. This credits a potential security for such systems.

Our object of interest in this work is the usage of Multivariate Quadratic Public-Key Cryptosystems (MPKC) for digital signatures as an efficient and reliable quantum-safe alternative. We will be giving special attention to the Hidden Field Equations class of MPKC with vinegar and minus modifiers (HFEv-). HFEv- is the base of the Great Multivariate Signature Scheme (GeMSS) [Casanova et al. 2017], a candidate at NIST's Post-Quantum Cryptography Standardization process [Moody et al. 2019].

In the next section we present a theoretical overview of HFEv- as a digital signature scheme, presenting its basic characteristics and introducing some aspects of GeMSS. In the third section, we show some characteristics of performance and security of GeMSS. In the fourth section we present a comparison to other relevant cryptosystems. In the final section some conclusions are drawn.

2. Great Multivariate Signature Scheme - GeMSS

The Hidden Field Equations scheme was first proposed by Patarin [Patarin 1996] after he broke the security of the Matsumoto Imai Scheme A (MIA) [Patarin 1995]. HFE generalizes the central map F, substituting the monomials for polynomials.[Andrade 2013].

With the finding that some basic MQ-trapdoors were insecure, some changes in the basic formulations were proposed. A list of modifiers was then elaborated in order to make the trapdoors faster and/or more secure. For the HFE family, the Vinegar (v) and Minus (-) modifiers can turn it into a more secure version. Minus modifier acts getting rid of some equations of the public-key while Vinegar modifier defines some extra variables, called vinegar variables, parametrizing the central map F [Petzoldt et al. 2015]. Both modifiers can grant more security to the scheme, although they make the encryption process slower [Andrade 2013]. With this, we can now build a trapdoor HFEv-.

The most famous HFEv- based scheme is QUARTZ, proposed by [Patarin et al. 2001] to be a new alternative with greater security and very small signatures. The disadvantage of QUARTZ is the really slow signing process of the order of 10 seconds [Petzoldt et al. 2015]. This is due to the high order d of the polynomial used (for QUARTZ $d = 129$), which leads to a very costly inversion of the central map.

The Great Multivariate Signature Scheme (GeMSS) is a multivariate scheme proposed by [Casanova et al. 2017] based on QUARTZ [Patarin et al. 2001] and Gui [Petzoldt et al. 2015]. Whilst cryptanalysis of multivariate schemes is constantly studied, QUARTZ remains not having practical attacks against it. The attack using Gröbner bases remains as the best known attack, and GeMSS exploits this in order to set its parameters, delivering improved security and efficiency [Casanova et al. 2017].

2.1. Mathematical Foundations

Multivariate Cryptosystems objects are systems of multivariate quadratic polynomials, as in Eq. (1)

$$\begin{cases} p^{(1)}(x_1,\ldots,x_n) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum\limits_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\ p^{(2)}(x_1,\ldots,x_n) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum\limits_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} \\ \quad\vdots \\ p^{(m)}(x_1,\ldots,x_n) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum\limits_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}. \end{cases} \tag{1}$$

The security of those schemes relies on the MQ Problem, which might be read as: Given m multivariate quadratic polynomials $p^{(1)}(x),\ldots,p^{(m)}(x)$ in n variables $x_1,\ldots,x_n$, find a vector $\vec{\mathbf{x}}(x_1,\ldots,x_n)$ such that $p^{(1)}(\vec{\mathbf{x}}) = \cdots = p^{(m)}(\vec{\mathbf{x}}) = 0$.

It also relies on the Extended Isomorphism of Polynomials (EIP) Problem, due to the process of composition involved in the public-key generation. In an MPKC the public-key P is created by composing the three private-keys: two affine invertible transformations $S : \mathbb{F}^n \mapsto \mathbb{F}^n$ and $T : \mathbb{F}^m \mapsto \mathbb{F}^m$ with a central easily invertible quadratic map $F : \mathbb{F}^n \mapsto \mathbb{F}^m$. We thus have

$$P = T \circ F \circ S. \tag{2}$$

To sign $w \in \mathbb{F}^n$ a message $x \in \mathbb{F}^m$ one uses the inverse functions of private-keys F, S e T, thus computing, recursively, $y = T^{-1}(x) \in \mathbb{F}^m$, $z = F^{-1}(y) \in \mathbb{F}^n$ and $w = S^{-1}(y) \in \mathbb{F}^n$

$$w = S^{-1}\left(F^{-1}\left(T^{-1}(x)\right)\right). \tag{3}$$

To verify a signature one simply analyses if the vector of polynomials P generates the signature w, i.e., verify the validity of $P(w) = x$. If it holds, then it is a valid signature.

The signature schemes focused on this paper belongs to the BigField family of multivariate schemes. In this type of scheme, the central map is chosen to be an easily invertible map over a degree n extension field $\mathbb{E}$ of $\mathbb{F}$, i.e., $\mathbb{E} = \mathbb{F}_{q^n}$. In order to transform F into a quadratic map, one has to use an isomorphism $\varphi : \mathbb{F}^n \to \mathbb{E}$ and its inverse φ^{-1} to map $\mathbb{F}^n \to \mathbb{F}^n$ [Petzoldt et al. 2015]. One then makes a composition

$$\bar{F} = \varphi^{-1} \circ F \circ \varphi. \tag{4}$$

For the HFE scheme we use $\mathbb{E} = \mathbb{F}_{q^n}$ where q has a prime characteristic p, such that $q = p^k$, $k \in \mathbb{N}$. HFE is therefore characterized by

$$\mathbb{F}^n \overset{S}{\mapsto} \mathbb{F}^n \overset{\varphi^{-1}}{\mapsto} \mathbb{E}^n \overset{F}{\mapsto} \mathbb{E}^n \overset{\varphi}{\mapsto} \mathbb{F}^m \overset{T}{\mapsto} \mathbb{F}^m. \tag{5}$$

The central map can be defined by [Patarin 1996]

$$f(x) = \sum_{i,j}^{d} \xi_{ij} x^{q^{\theta_{ij}} + q^{\sigma_{ij}}} + \sum_{i}^{d} \psi_i x^{q^{\gamma_i}} + \mu \tag{6}$$

where $i, j \in \mathbb{N}$; $\xi_{ij}, \psi_i, \mu \in \mathbb{E}$; $\theta, \sigma, \gamma \in \mathbb{Z}$. In Eq. (6), $\xi_{ij} x^{q^{\theta_{ij}} + q^{\sigma_{ij}}}$ are the quadratic terms, $\psi_i x^{q^{\gamma_i}}$ are the linear terms and μ are the constant terms. Thus $f(x)$ is a polynomial in x over $\mathbb{E}_{q^n}$, with degree d, where $0 \leq \theta_{ij}, \sigma_{ij}, \gamma_i \leq d$.

2.2. Design Rationale

The parameters chosen to GeMSS are listed below

- D, positive integer, degree of a secret polynomial, such that $D = 2^i$ for $i \geq 0$, or $D = 2^i + 2^j$ for $i \neq j$, and $i, j \geq 0$
- K, output size of hash function, in bits
- λ, security level
- m, number of equations in the public-key
- nb_ite > 1, number of iterations in the verification and signature processes
- n, the degree of a field extension of $\mathbb{F}_2$
- v, the number of vinegar variables
- Δ, the number of minus ($m = n - \Delta$)

The secret-keys in GeMSS are composed by two invertible matrices $(\mathbf{S}, \mathbf{T}) \in GL_{n+v}(\mathbb{F}_2) \times GL_n(\mathbb{F}_2)$ and a polynomial $F \in \mathbb{F}_{2^n}[X, v_1 \ldots, v_v]$ with structure given by Eq. (7)

$$\sum_{\substack{0 \leq j < i < n \\ 2^i + 2^j \leq D}} \left(A_{i,j} X^{2^i + 2^j}\right) + \sum_{\substack{0 \leq i < n \\ 2^i \leq D}} \left(\beta_i(v_1, \ldots, v_v) X^{2^i} + \gamma(v_1, \ldots, v_v)\right), \tag{7}$$

where $A_{i,j} \in \mathbb{F}_{2^n}, \forall i, j, 0 \leq j < i < n$, each $\beta_i : \mathbb{F}_2^v \mapsto \mathbb{F}_{2^n}$ is linear and $\gamma(v_1, \ldots, v_v) : \mathbb{F}_2^v \mapsto \mathbb{F}_{2^n}$ is quadratic and $v_1, \ldots, v_v$ are the vinegar variables. The degree of F is D, the maximum degree of its HFE polynomials.

Let $(\theta_1, \ldots, \theta_n) \in (\mathbb{F}_{2^n})^n$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Set $\varphi : E = \sum_{k=1}^{n} e_k \cdot \theta_k \in \mathbb{F}_{2^n} \longrightarrow \varphi(E) = (e_1, \ldots, e_n) \in \mathbb{F}_2^n$. We can now define a set of multivariate polynomials $\mathbf{f} = (f_1, \ldots, f_n) \in \mathbb{F}_2[x_1, \ldots, x_{n+v}]^n$ derived from the HFEv polynomial $F \in \mathbb{F}_2^n[X, v_1, \ldots, v_v]$ by:

$$F\left(\sum_{k=1}^{n} \theta_k x_k, v_1, \ldots, v_v\right) = \sum_{k=1}^{n} \theta_k f_k. \tag{8}$$

The public key in GeMSS is a set of m quadratic equations in $n + v$ variables, that is, $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{F}_2\left[x_1, \ldots, x_{n+v}\right]^m$ where we denote the vinegar variables as $(v_1, \ldots, v_v) = (x_{n+1}, \ldots, x_{n+v})$. The public-key is obtained from the secret-key by taking the first $m = n - \Delta$ polynomials of:

$$\Big(f_1\big((x_1, \ldots, x_{n+v})\,\mathbf{S}\big), \ldots, f_n\big((x_1, \ldots, x_{n+v})\,\mathbf{S}\big)\Big)\mathbf{T}, \tag{9}$$

and reducing it modulo $\left\langle x_1^2 - x_1, \ldots, x_{n+v}^2 - x_{n+v}\right\rangle$.

The main goal in the signing process is to solve:

$$p_1\left(x_1, \ldots, x_{n+v}\right) - d_1 = 0, \ldots, p_m\left(x_1, \ldots, x_{n+v}\right) - d_m = 0 \tag{10}$$

for $\mathbf{d} = (d_1, \ldots, d_m) \in \mathbb{F}_2^m$. This is done by randomly sampling $\mathbf{r} = (r_1, \ldots, r_{n-m}) \in \mathbb{F}_2^{n-m}$ and appending it do $\mathbf{d}$, which gives $(\mathbf{d}, \mathbf{r}) \in \mathbb{F}_2^n$. One then computes $D' = \varphi^{-1}(\mathbf{d}' \times \mathbf{T}^{-1}) \in \mathbb{F}_{2^n}$ and try to find a root $(Z, z_1, \ldots, z_v) \in \mathbb{F}_{2^n} \times \mathbb{F}_2^v$ of the multivariate equation:

$$F(Z, z_1, \ldots, z_v) - D' = 0 \tag{11}$$

If a root $Z \in \mathbb{F}_{2^n}$ is found, then return $(\varphi(Z), \mathbf{v}) \times \mathbf{S}^{-1} \in \mathbf{F}_2^{n+v}$. The process of find the roots of Eq. (11) uses the Berlekamp algorithm [von zur Gathen and Gerhard 2003], which leads to an estimated $\tilde{\mathcal{O}}(D \log(q)) = \tilde{\mathcal{O}}(nD)$ (for $q = 2^n$) number of operations in $\mathbb{F}_q$.

3. Performance and Security

3.1. Performance

Any digital signature scheme based on HFEv- will have a very costly step that is the inversion of the polynomial equation. This step is usually accomplished by the Berlekamp algorithm. In GeMSS, this step has estimated complexity of $\tilde{\mathcal{O}}(nD)$ operations in $\mathbb{F}_{2^n}$.

Given this,the most expensive part of GeMSS is the multiplication in $\mathbb{F}_{2^n}$. The generation of keys requires $\mathcal{O}(n^2 \log{(D)}^2 + nv \log{(D)})$ multiplications and the signature process requires $\tilde{\mathcal{O}}(nD)$ multiplications.

3.2. Security

Accordingly to [Petzoldt et al. 2015], the most important attacks against HFEv- signature schemes to be considered are direct algebraic attacks, as the ones using Gröbner bases, and Kipnis-Shamir attack [Shamir and Kipnis 1999], a key-recovery attack. One can also try a direct signature forgery attack, essentially, try solving the system of non-linear equations:

$$\begin{cases} p_1(x_1, \dots, x_{n+v}) - d_1 = 0 \\ p_2(x_1, \dots, x_{n+v}) - d_2 = 0 \\ \qquad\quad \vdots \\ p_m(x_1, \dots, x_{n+v}) - d_m = 0 \\ x_1^2 - x_1 = 0 \\ \qquad\quad \vdots \\ x_{n+v}^2 - x_{n+v} = 0 \end{cases} \tag{12}$$

An exhaustive search method is described in [Bouillaguet et al. 2010] in which to recover a solution of Eq. (12) requires $4\log_2(m)2^m$ binary operations. A Quantum Exhaustive Search [Schwabe and Westerbaan 2016] can solve m binary quadratic equations in m binary variables using $\mathcal{O}(m)$ qubits, and evaluating $\mathcal{O}(2^{m/2}m^3)$ quantum gates.
An approximation method (AM) is described in [Lokshtanov et al. 2017] which leads to an asymptotic complexity (lower-bounded) of

$$\mathcal{O}^*(2^{0.8765m}) \tag{13}$$

A hybrid approach (HA) that combines exhaustive search and Gröbner bases techniques is found in BooleanSolve [Bardet et al. 2011], which is the fastest asymptotic algorithm for solving system of non-linear Boolean equations. The Las-Vegas variant has expected complexity of

$$\mathcal{O}^*(2^{0.792m}) \tag{14}$$

Alternatively, a quantum variety (qHA) has estimated complexity of [Faugere et al. 2017]

$$\mathcal{O}(2^{0.462m}) \tag{15}$$

3.2.1. Kipnis-Shamir attack

The Kipnis-Shamir key-recovery attack exploits the MinRank problem, which consists in given a field $\mathbb{K}$ and $m, n \in \mathbb{N}$, $r < n$, considering m matrices $n \times n$ over $\mathbb{K}$: $M_1, \dots M_m$, find a linear combination $\alpha \in \mathbb{K}^m$ of minimal rank:

$$\text{Rank}\left(\sum_i \alpha_i M_i\right) \leq r. \tag{16}$$

For this given system, it is found an estimated complexity of [Petzoldt et al. 2015]

$$\mathcal{O}\binom{n + r + \Delta + v}{r + \Delta + v}^{\omega} \tag{17}$$

where $2 \leq \omega < 3$ is the linear algebra constant and $r = \lceil \log_2(D) \rceil$,

4. A security comparison

As we have seen in the previous section, the best attacks to GeMSS are intimate related to the number of equations in the public-key. Given this, we now try a comparison between this algorithm best attacks (HA and qHA) and other relevant cryptosystems used for digital signatures: RSA and ECDSA.

It is known that RSA relies on the Integer Factorization Problem. One uses the general number field sieve (GNFS) to solve it with subexponential complexity given by

$$\mathcal{O}\left(\exp\left(\left(\left(\frac{64}{9}\right)^{1/3}+O(1)\right)(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)\right), \tag{18}$$

where n is the number for factorization.

To solve the Discrete Logarithm Problem (DLP) in order to break ECDSA, one can use Pollard's Rho algorithm, which has complexity given by

$$\mathcal{O}\left(\sqrt{\frac{\pi o}{2}}\right), \tag{19}$$

where o is the order of the group.

For GeMSS we have used a parameter analysis as proposed by the authors in their reference implementation [Casanova et al. 2017], developing a mathematical evaluation of the key length based on the parameters involved in the keys. This gave a general overview of the algorithm behavior, although the lack of specific information made our results differ a little from the authors report.

Given the complexities for the best known attacks obtained in previous equations, we are able to evaluate the minimal key length, in bits, in order to achieve a given security level. For this comparison we have matched the complexity for a brute force attack, i.e. $\mathcal{O}(2^x)$ with a established level of security, thus retrieving the results shown in Table 1.

Table 1. Comparison between brute force and minimum key length.

Brute Force	DLP - Eq.(19)	GNFS - Eq.(18)	NIST	HA - Eq.(14)	qHA - Eq.(15)
80	160	851	1 024	34029	92401
112	224	1 853	2 048	71164	190521
128	256	2 538	3 072	95617	252316
192	384	6 707	7 680	226161	588828
256	512	13 547	15 360	412051	1064043

It can be noticed in a glance that GeMSS key size requirements are extremely large compared to the classical algorithms. This is indeed a drawback of this cryptosystem, although it has some quite interesting aspects that we mention in next section.

Another meaningful aspect to remember is that in face of a quantum computer, every cryptographic algorithm should at least have its key length doubled. That is due to Grover's algorithm, which is capable of finding a n-bits key with complexity $\mathcal{O}(\sqrt{n})$ through brute force. The performance is directly proportional to the key length. Figure 1 depicts a trade-off between security and key bit length, with the approximate interpolation polynomials from the data in Table 1.

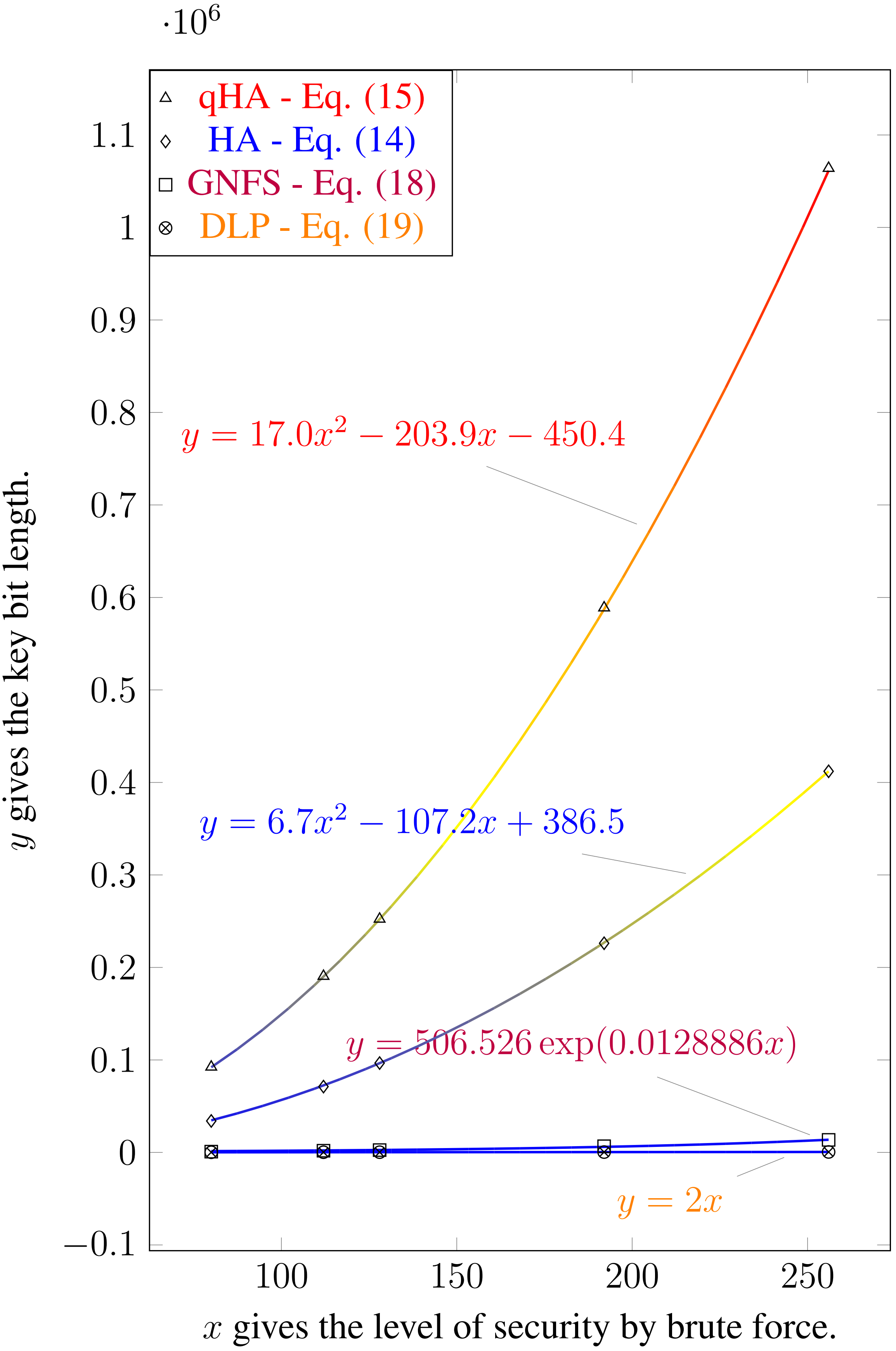

Figure 1. Comparison between brute force and minimum key length.

5. Conclusions

In this paper, we have discussed the trade-off between performance and security for GeMSS, a competitor in the second round of the post quantum standardization process promoted by the National Institute of Standards and Technology (NIST). This is already a great conquer for the cryptosystem, but does not take away its main problems.

GeMSS proves that HFEv- schemes continue to be a good bet regarding quantum-safe digital signature schemes, even after more that 20 years of constant and deep studies. The main reason for this is that it exploits the vulnerabilities found in QUARTZ in order to deliver a new adaptation with better performance and security, although the algorithm core, i.e, inversion of the central polynomial equation, continue to be a bottleneck for schemes of this type.

Despite GeMSS being a very prominent system for a quantum world, it has some really bothering drawbacks that are its very slow key pair and signature generation and the size of the keys, as we have shown in the previous section. This contrasts with its fast signature verification and tiny signature size. The best implementation, using an Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz processor gives the following results, accordingly to the security level [Casanova et al. 2017]

Security Level	**128 bits**	**192 bits**	**256 bits**
Key pair Generation	42 ms	166 ms	424 ms
Signing (mean values)	260 ms	694 ms	1090 ms
Verification	41 μs	117 μs	336 μs
Public key size	417408 bytes	1304192 bytes	3603792 bytes
Size of private key	14208 bytes	39440 bytes	82056 bytes
Size of signature	48 bytes	88 bytes	104 bytes

Table 2. Main aspects for each security level using an Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz processor

As the quantum era becomes closer, it is needed to focus on the research of cryptosystems that are capable of protecting our identity and privacy, with performance at least as good as the ones we use nowadays. Further investigation has to be done in order to determine better implementations and parameter choices in order to guarantee our security.

Acknowledgement

We would like to thank CNPq for supporting the development of this work.

References

Andrade, E. R. (2013). *Proposta de aprimoramento para o protocolo de assinatura digital Quartz*. PhD thesis, Universidade de São Paulo.

Bardet, M., Faugère, J., Salvy, B., and Spaenlehauer, P. (2011). On the complexity of solving quadratic boolean systems. *CoRR*, abs/1112.6263.

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer.

Bouillaguet, C., Chen, H.-C., Cheng, C.-M., Chou, T., Niederhagen, R., Shamir, A., and Yang, B.-Y. (2010). Fast exhaustive search for polynomial systems in f2. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 203–218. Springer.

Casanova, A., Faugère, J.-C., Macario-Rat, G., Patarin, J., Perret, L., and Ryckeghem, J. (2017). Gemss: A great multivariate short signature. *UPMC-Paris 6 Sorbonne Universités*.

Faugere, J.-C., Horan, K., Kahrobaei, D., Kaplan, M., Kashefi, E., and Perret, L. (2017). Fast quantum algorithm for solving multivariate quadratic equations. *arXiv preprint arXiv:1712.07211*.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM.

Lokshtanov, D., Paturi, R., Tamaki, S., Williams, R., and Yu, H. (2017). Beating brute force for systems of polynomial equations over finite fields. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2190–2202. SIAM.

Moody, D., Alagic, G., Alperin-Sheriff, J. M., Apon, D. C., Cooper, D. A., Dang, Q. H., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., et al. (2019). Status report on the first round of the nist post-quantum cryptography standardization process. Technical report, National Institute of Standards and Technology.

Nielsen, M. A. and Chuang, I. (2002). *Quantum computation and quantum information*. AAPT.

Patarin, J. (1995). Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt'88. In *Annual International Cryptology Conference*, pages 248–261. Springer.

Patarin, J. (1996). Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer.

Patarin, J., Courtois, N., and Goubin, L. (2001). Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference*, pages 282–297. Springer.

Patarin, J. and Goubin, L. (1997). Trapdoor one-way permutations and multivariate polynomials. In *International Conference on Information and Communications Security*, pages 356–368. Springer.

Petzoldt, A., Chen, M.-S., Yang, B.-Y., Tao, C., and Ding, J. (2015). Design principles for hfev- based multivariate signature schemes. In Iwata, T. and Cheon, J. H., editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 311–334, Berlin, Heidelberg. Springer Berlin Heidelberg.

Schwabe, P. and Westerbaan, B. (2016). Solving binary mq with grover's algorithm. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 303–322. Springer.

Shamir, A. and Kipnis, A. (1999). Cryptanalysis of the hfe public key cryptosystem. In *Advances in Cryptology, Proceedings of Crypto*, volume 99.

Shor, P. W. (1995). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

von zur Gathen, J. and Gerhard, J. (2003). *Modern Computer Algebra*. Cambridge University Press.