FPGA Implementation of Post-Quantum DME Cryptosystem

José L. Imaña
Department of Computer Architecture and Automation
Faculty of Physics, Complutense University
28040 Madrid, Spain
Email: jluimana@ucm.es

Ignacio Luengo
Department of Algebra, Geometry, and Topology
Faculty of Mathematics, Complutense University
28040 Madrid, Spain
Email: iluengo@ucm.es

The rapid development of quantum computing constitutes a significant threat to modern Public-Key Cryptography (PKC). The use of Shor's algorithm [1] with potential powerful quantum computers could easily break the two most widely used public key cryptosystems, namely, RSA and Elliptic Curve Cryptography (ECC), based on integer factorization and discrete logarithm problems. For this reason, Post-Quantum Cryptography (PQC) [2] based on alternative mathematical features has become a fundamental research topic due to its resistance against quantum computers. The National Institute of Standards and Technology (NIST) has even opened a call for proposals of quantum-resistant PKC algorithms in order to standardize one or more PQC algorithms. Cryptographic systems that appear to be extremely difficult to break with large quantum computers are *hash-based cryptography*, *lattice-based cryptography*, *code-based cryptography*, and *multivariate-quadratic cryptography* [3]. Furthermore, efficient hardware implementations are highly required for these alternative quantum-resistant cryptosystems [4].

Multivariate Public-Key Cryptosystems (MPKCs) are cryptosystems for which the public key is a set of polynomials $P(X) = (p_1, \ldots, p_m)$ in variables $X = (x_1, \ldots, x_n)$ where all the variables and coefficients are in a finite field. Their security relies on the difficulty of the problem of solving a set of multivariable quadratic polynomial equations over $GF(q)$, which is in general NP-hard. Different schemes of MPKCs have been proposed in the literature. TTS (*Tame Transformation Signature*) schemes, such as *amended* TTS (amTTS) and *enhanced* TTS (enTTS) were based on the *Tame Transformation Method* (TTM). The Oil-Vinegar family of MPKCs consists of three families, named balanced Oil-Vinegar, unbalanced Oil-Vinegar (UOV) and Rainbow [5], that is a multilayer construction using UOV at each layer. Rainbow has great potential in terms of its efficiency and applications in ubiquitous computing. Furthermore, Rainbow is a candidate for the NIST PQC Standardization Process that has moved on to the second round of the competition. DME-(m,n,e) [6] is a new proposal of quantum-resistant PKC algorithm that was presented for NIST PQC Standardization competition. Although DME could not move on to the second round, its high performance and security properties make its study and implementation of great interest. DME is a multivariate public key, signature and Key Encapsulation Mechanism (KEM) system based on a double exponentiation with matrix exponents.

In this paper, a high-throughput pipelined architecture of DME-(3,2,48), with m = 3, n = 2, and $q = 2^e = 2^{48}$, has been presented and hardware implementations over Xilinx FPGAs Artix-7 have been performed. These settings correspond with the reference implementation given in the NIST proposal [7], where the finite field $GF(2^{48})$ is generated by the *type I irreducible pentanomial* [8] $f(y) = y^{48}+y^{28}+y^{27}+y+1$ over $GF(2)$. The proposed pipelined scheme, that is valid for any DME-(m, n, e) cryptosystem, only requires five clock cycles for performing computations. Experimental results show that the architecture here presented exhibits the lowest execution time and highest throughput when it is compared with other PQC multivariate implementations. Furthermore, the Area×Time metrics for DME-(3,2,48) presents the third best result among the other multivariate schemes here considered.

ACKNOWLEDGMENT

This work has been supported by the Spanish MINECO and CM under grants S2018/TCS-4423, TIN 2015-65277-R and RTI2018-093684-B-I00.

REFERENCES

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1997.

[2] D.J. Bernstein, J. Buchmann and E. Dahmen, "Post-Quantum Cryptography", Springer, 2009.

[3] J. Ding and D. Schmidt, "Multivariate public key cryptosystems", *Advances in Information Security*, vol. 25, 2006.

[4] S. Tang, H. Yi, J. Ding, H. Chen and G. Chen, "High-speed hardware implementation of rainbow signature on fpgas", *Fourth Int'l. Conf. on post-Quantum Cryptography, PQCCrypto 2011*, LNCS 7071, pp. 228-243, 2011.

[5] J. Ding and D. Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme", *Applied Cryptography and Network Security, ACNS 2005*, LNCS 3531, pp. 164-175, 2005.

[6] I. Luengo, "DME: a public key, signature and KEM system based on double exponentiation with matrix exponents", *Tech. Rep.*, 2017.

[7] I. Luengo, M. Avendaño and M. Marco, "DME a public key, signature and KEM system based on double exponentiation", *NIST proposal*, 2017. *https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions*.

[8] J.L. Imaña, "Fast Bit-Parallel Binary Multipliers Based on Type-I Pentanomials", *IEEE Trans. Computers*, vol. 67, no. 6, pp. 898-904, Jun. 2018.