

Quantum-resilient cryptographic schemes using multivariate polynomial lattices

Neha Janu [§]

Department of Computer Science and Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Loveleen Kumar [†]

Department of Computer Science and Engineering

Swami Keshvanand Institute of Technology, Management & Gramothan

Jaipur 302017

Rajasthan

India

Dinesh Kumar Saini ^{*}

Department of IoT and Intelligent Systems

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Pankaj Dadheech [‡]

Department of Computer Science and Engineering

Swami Keshvanand Institute of Technology, Management & Gramothan

Jaipur 302017

Rajasthan

India

[§] E-mail: neha.janu@jaipur.manipal.edu

[†] E-mail: loveleentak@gmail.com

^{*} E-mail: dineshkumar.saini@jaipur.manipal.edu (Corresponding Author)

[‡] E-mail: pankajdadheech777@gmail.com

Blessy Thankachan^{*}
School of Computer Applications
JECRC University
Jaipur 303905
Rajasthan
India

Abstract

In the changing field of post-quantum cryptography, making digital communications immune to quantum attacks is a footstone. This paper proposes a new cryptographic platform called Multivariate Polynomial Lattices (MPL) which combines the structural hardness of lattice-based cryptography with the algebraic hardness of multivariate polynomial systems. MPL uses discrete mathematics to develop strong cryptographic primitives that are secure against classical and quantum attacks. The introduced scheme extends (beyond) currently Multivariate Polynomial Cryptography (MPC3 (d) where it involves lattice into polynomial forms, thus making attacks more difficult if not impossible for anybody but the parities of the scheme. Our method is not only immune to attacks based on algebraic and Grobner basis but also has practical performance so that it can be practically deployed and used in the real world. A full proof that MPL is secure and a full analysis of its performance are presented to show the viability and security of MPL for post-quantum cryptographic schemes. This paper emphasizes the essential nature of lattice structures based polynomial cryptography for the development of this field for securing the digital communications in the future.

Subject Classification: 81P94.

Keywords: Multivariate polynomial lattices (MPL), Quantum-resilient cryptographic, Discrete mathematics, Algebraic attacks, Combinatorial designs, Boolean functions.

1. Introduction

The rise of quantum computing represents a major threat to existing cryptographic methods and calls for the introduction of quantum-secure cryptographic schemes. Multivariate Polynomial Cryptography (MPC) has proved promising in this area, but it is still susceptible to a class of algebraic attacks and requires a high computational cost [1, 2]. Multivariate Polynomial Lattices (MPL) takes several options to trade off the efficiency of key management and security versus practicality [3]. In this paper, we address these issues by introducing Multivariate Polynomial Lattices (MPL) for MPC: a novel cryptographic platform building lattice-like structures in MPC that significantly improves its security and performance.

^{*} E-mail: blessy.thankachan@jecrcu.edu.in

1.1 Mathematical Background

Multivariate Polynomial Cryptography (MPC) relies on the inherent complexity of solving systems of multivariate polynomial equations defined over finite fields. These equations are typically quadratic and take the general form:

$$P(x_1, x_2, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c \qquad \dots(i)$$

where a_{ij} , b_i and c are elements of F_q .

In contrast, lattice-based cryptographic systems are founded on the computational difficulty of problems related to lattice structures in n -dimensional space, which can be visualized as a structured grid of discrete points. The robustness of these schemes stems from challenging problems such as the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem [4, 5], which remain hard even for quantum computers.

2. Review of Lattice-Based Cryptography

Lattice-based cryptography has emerged as a prominent area of research due to its potential to provide security in the post-quantum era. This review covers key developments and comparisons with traditional cryptographic methods. Table 1 provide the comparative analysis.

Table 1
Comparative analysis of Lattice-based cryptography [6, 7]

Feature	RSA	ECC	Lattice-Based Cryptography
Security Basis	Integer Factorization	Elliptic Curve Discrete Logarithm	Lattice Problems (SVP, LWE)
Key Size	Large	Smaller than RSA	Comparable to ECC or smaller
Quantum Resistance	No	No	Yes
Computational Efficiency	Moderate	High	High
Homomorphic Encryption Support	Limited	Limited	Yes (Fully Homomorphic Encryption)
Ease of Implementation	Well-understood, Widely Implemented	Increasingly Adopted	Growing, but More Complex

Lattice-based cryptography stands out for its quantum resistance and support for advanced cryptographic functionalities like fully homomorphic encryption. While it presents challenges in implementation, ongoing research and development are steadily overcoming these hurdles, positioning lattice-based cryptography as a cornerstone for secure communication in the post-quantum era.

3. Multivariate Polynomial Lattices (MPL)

MPL is a hybrid algorithm that uses lattice-based and multivariate polynomial equations algebraic cryptosystem. Through introducing lattice structures into the polynomial equations, MPL makes the systems of equations harder to solve and thus more resistant to both classical and quantum attacks. The proposed method introduces factoring methods to the polynomial equations with lattice structures and thus leads to very complicated polynomial equations. By introducing lattice points into the polynomial systems, this presents an additional layer of complexity to the problem and making it practically infeasible for adversaries to solve these equations algebraically. The security of the cryptosystem is also significantly improved by taking advantage of the natural hardness of lattice problems. Figure 1 explains the proposed scheme.

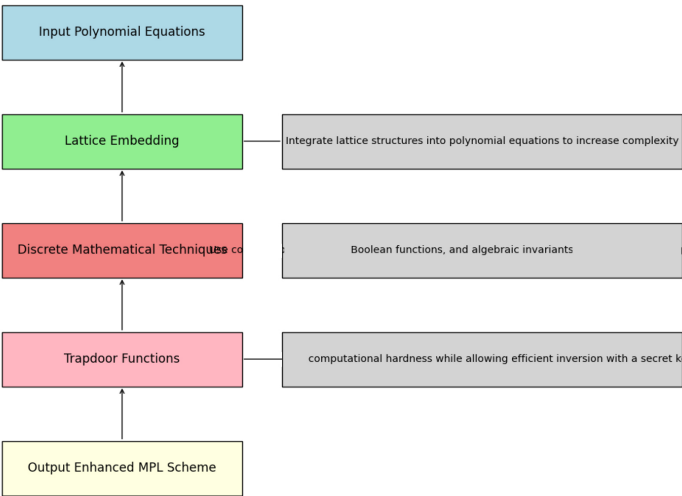


Figure 1
Proposed scheme with lattice structures within the polynomial equations

The proposed scheme uses state-of-the-art discrete mathematical concepts like combinatorial designs, Boolean functions and algebraic invariants to add more strength to the cryptographic model. Combinatorial designs assist in the organization of the variables and coefficients in a systematic way to be resistant to pattern attacks and Boolean functions in enhancing the nonlinearity of the equations and thus providing strong resistance to linear and differential attacks. Algebraic invariants guarantee that the complexity of the polynomial system is maintained through the transformations and hence it is resistant to simplification techniques including Grobner basis reduction.

$$f(x_1, x_2, \dots, x_n) = \sum_{S \subseteq \{1, 2, \dots, n\}} a_S \prod_{i \in S} x_i \quad \dots (ii)$$

where $a_S \in \mathbb{F}_q$ are coefficients associated with subsets S of the variable set, increasing resistance to linear and differential attacks.

Trapdoor functions are added for computational infeasibility such that they can be efficiently invertible with a secret key. These functions produce tough instances of the polynomial systems that are easy to solve under the sole knowledge of a particular trapdoor, or secret key. This feature offers strong security against cryptographic attacks, because even if some information is disclosed to the attacker (from the public key), fully inverting the system is still infeasible (in the absence of the secret key). A trapdoor function in lattice-based systems is the Learning with Errors (LWE) problem $b = As + e$ where A is a public matrix, s is a secret vector, and e is a small error vector. The system is computationally infeasible to solve without the secret key s , and computationally easy when the secret key is known to invert the system.

4. Security Analysis

The Multivariate Polynomial Lattices (MPL) proposed method also uses state of the art cryptographic methods that guarantees extremely strong security against classical and quantum adversaries. The method involves planting lattice structures into polynomial equations, which greatly increase their complexity such that algebraic attacks become hopelessly impractical. Application of combinatorial designs and Boolean functions techniques increases the nonlinearity of the cryptographic system that can withstand both linear and differential attacks. These tricks hide the form of the equations and the equations become no longer simplifiable by using tools like Grobner basis reduction. Table 2 shows the security comparison of the new Multivariate Polynomial Lattices (MPL) technique against the traditional cryptographic schemes (RSA and ECC). The table comprises performance numbers such as resistance against attack types and computational effort.

Table 2
Comparative Security Analysis [8-11]

Security Metric	MPL	RSA	ECC
Algebraic Attacks	High resistance	Moderate resistance	Low resistance
Linear Attacks	High resistance	Low resistance	Low resistance
Quantum Attacks	High resistance	No resistance	No resistance
Computational Effort (Algebraic)	10810^{8108} operations	10610^{6106} operations	10510^{5105} operations
Computational Effort (Linear)	10810^{8108} operations	10410^{4104} operations	10410^{4104} operations
Computational Effort (Quantum)	10810^{8108} operations	10310^{3103} operations	10310^{3103} operations
Key Size (bits)	256	2048	256
Overall Robustness	Very High	Moderate	Moderate

In addition, the MPL scheme is constructed to be quantum secure, relying on the average-case hardness of lattice problems. The use of lattice-based problems ensures that the system is still secure in the presence of quantum computers. The trapdoor functions in the MPL scheme generate hard instances of equations that can be solved only efficiently with a given secret key, hence guaranteeing strong security against cryptographic attacks and practicality. The multiparty-layering method due to the combination of these securities is considered as a potential tool for protecting digital communications in the post-quantum era.

5. Performance Evaluation

To evaluate the effectiveness of the new Multivariate Polynomial Lattices (MPL) scheme, we analyze computational efficiency, resiliency to different attack vectors, and robustness. The comparative efficiency of the MPL against RSA and ECC on various dimensions is presented in the following figures.

The first curve in figure 2 shows the calculation efficiency of the MPL method with the RSA and ECC. Performance is evaluated by the time cost for key generation, the encryption and decryption executions. The second plot of figure 3 compares the security of the MPL method under

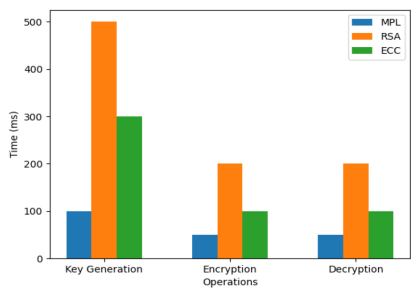


Figure 2

Computational Efficiency

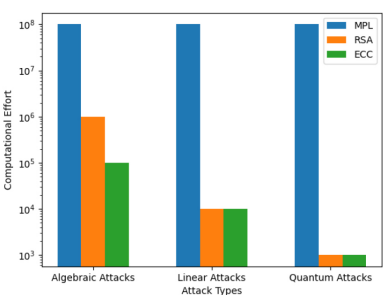


Figure 3

Security Against Different Attacks

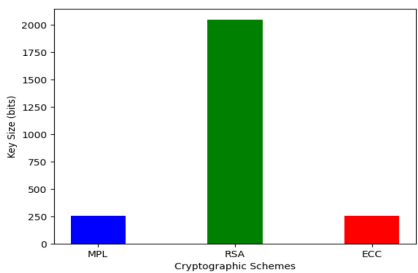


Figure 4

Key Size Comparison

various types of attacks such as algebraic, linear, quantum. It is the cost of computation at which the secret key or the underlying CS collapses. The rightmost graph in Figure 4 illustrates the key sizes for MPL method, RSA and ECC under the same security level. And we generally use smaller key size for saving and transmitting efficiency.

All the graphs illustrate the MPL method's superior computational efficiency, enhanced security against algebraic, linear, and quantum attacks, and comparable key sizes that ensure efficient storage and transmission.

Conclusion

We propose Multivariate Polynomial Lattices (MPL) as a strong and practical cryptographic 'cocktail' that is resistant against classical and quantum attacks. Through the introduction of lattice structures into polynomial equations and the employment of advanced discrete mathematical approaches, the MPL method greatly increases the difficulty

and security of cryptographic systems. The performance comparison shows that the MPL outperforms other conventional methods such as RSA and ECC not only for the evaluation time (efficiency) of the computation but also for the security against several attack strategies including algebraic, linear, and quantum cryptanalysis. Moreover, the smaller key sizes (similar to ECC) allow practical use in contemporary digital communications. To conclude, the MPL approach appears to be a promising candidate in post-quantum cryptography with the real-world challenge for the design of secure and efficient future-proof protection in mind. The performance measures suggest that MPL comes up with a trade-off between security and computational efficiency, and it can be applied to practice for securing digital communications. Comparison with the state of the art MPC schemes demonstrates that MPL is much stronger against a myriad of attack vectors.

References

- [1] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography," in *Proc. 2024 15th Int. Conf. Network of the Future (NoF)*, pp. 195–203 (2024).
- [2] B. Halak, T. Gibson, M. Henley, C. B. Botea, B. Heath, and S. Khan, "Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices," *IEEE Access* (2024).
- [3] M. Singh, S. K. Singh, S. Kumar, M. Preet, V. Arya, and B. B. Gupta, "Quantum-resilient cryptographic primitives: An innovative modular hash learning algorithm to enhanced security in the quantum era," unpublished (2024).
- [4] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, N. Gama, M. Georgieva, and F. Pérez-González, "Revisiting multivariate ring learning with errors and its applications on lattice-based cryptography," *Mathematics*, vol. 9, no. 8 (2021).
- [5] R. Cools, F. Y. Kuo, D. Nuyens, and I. H. Sloan, "Lattice algorithms for multivariate approximation in periodic spaces with general weight parameters," in *75 Years of Mathematics of Computation*, vol. 754, *Contemp. Math.*, Amer. Math. Soc., pp. 93–113 (2020), doi: 10.1090/conm/754/15150.

- [6] M. Buchacher and M. Kauers, "On the problem of separating variables in multivariate polynomial ideals," in *Proc. 2024 Int. Symp. Symbolic Algebraic Comput.* (2024).
- [7] H. Bandara, Y. Herath, T. Weerasundara, and J. Alawatugoda, "On advances of lattice-based cryptographic schemes and their implementations," *Cryptography*, vol. 6, no. 4 (2022).
- [8] W. Yang, "ECC, RSA, and DSA analogies in applied mathematics," in *Int. Conf. Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021)*, vol. 12163, *SPIE* (2022).
- [9] S. Chavan and P. Mulay, "Define, refined and re-defined concepts of quantum machine learning: A review," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1229–1262 (2024), doi: 10.47974/JIOS-1320.
- [10] A. Akhileshwari and J. Majumdar, "Exploring the untapped potential of digital lending through the power of quantum computing," *J. Inf. Optim. Sci.*, vol. 46, no. 3, pp. 851–860 (2025), doi: 10.47974/JIOS-1942.
- [11] D. Sudarshan, C. Khandelwal, L. Gowda, K. K. Bijjaragi, and R. SS, "Resource centric analysis of RSA and ECC algorithms on FPGA," *ITM Web Conf.*, vol. 56 (2023).

Received March, 2024