Combining Detection-Based and Arithmetic Masking Countermeasures Against Side-channel Attacks on Post-quantum Cryptography

Xiyana Figuera *

***Abstract*— Quantum computing is a highly invested area of research with vast potential across disciplines. At the same time, Quantum computers pose a potential threat for the current classical cryptographic techniques. The National Institute of Standards and Technology (NIST) has addressed potentials risks by selecting optimal post-quantum cryptography (PQC) methods for standardization. However, the meticulous testing of these methods, particularly their susceptibility to side-channel attacks, remains crucial. For this reason, NIST has prioritized evaluating the resilience of candidate algorithms against such attacks. Recent demonstrations of side-channel attacks on PQC methods employing deep learning have surfaced exploiting vulnerabilities. To mitigate these threats, we propose the implementation of combined detection-based and arithmetic masking-based countermeasures designed to safeguard PQC algorithms against side-channel attacks.**

I. INTRODUCTION

Quantum computing is a major focus of current research [1]. This increased attention in the field brings with it the imminent possibility of entering an era where quantum computers can be fully developed [2]. The promise of unprecedented computational power underscores a profound need for reevaluating security, particularly in the field of classical cryptographic techniques [3]. These techniques heavily rely on the difficulty posed to classical computers in solving mathematical problems—a challenge easily overcome by quantum computers [4].

In post-quantum cryptography (PQC) literature, current efforts to offer safety against quantum-based attacks can be categorized into five main groups: Lattice-based [5], Code-based [6], Hash-based [7], Multivariate-based [8], and Isogeny-based cryptography [9]. In these classifications, Lattice-based Post-Quantum Cryptography (PQC) emerges as the favored option, due to its perceived resilience against both classical and quantum-based attacks [10].

In response to the potential quantum-based attacks on encrypted systems, the National Institute of Standards and Technology (NIST) is actively involved in selecting and standardizing PQC methods [11]. At present, three out of the four chosen candidates for standardization fall within the Lattice-based PQC category [11]. Lattice-based PQC is further segmented into three schemes: Lattice-based encryption [12], lattice-based signature schemes [13], and lattice-based key exchanges [14]. Notably, CRYSTALS-Kyber, an algorithm selected as a candidate following the third round of NIST evaluations, belongs to the lattice-based key exchanges [15]. CRYSTALS-Kyber is a key encapsulation mechanism (KEM), whose security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices.

The effort to establish secure post-quantum cryptographic methods is filled with challenges. Deep learning techniques, increasingly common in various fields, present a unique difficulty in the context of cryptographic security. An example of this, is the introduction of recursive learning, a method that has shown success in side-channel attacks against finalists like CRYSTALS-Kyber, selected by NIST. This emphasizes that even the most promising post-quantum cryptographic solutions have vulnerabilities, requiring a thorough reassessment of security measures in the face of evolving threats. As researchers strive to strengthen cryptographic protocols against the capabilities of quantum computers, countering deep learning-based side-channel attack methods becomes primordial to ensuring the safety of post-quantum cryptographic solutions

Given its status as one of the finalist candidates for NIST standardization, it becomes imperative to scrutinize the robustness of CRYSTALS Kyber implementations against side-channel attacks [16]. These attacks leverage information gleaned from physically measurable, non-primary channels like timing or power consumption of the device running the implementation. Consequently, the quest for effective techniques to safeguard hardware implementations becomes crucial in ensuring the reliability of CRYSTALS Kyber as a potential frontrunner in the NIST Post-Quantum Cryptography (PQC) Standardization Process.

Our method aims to contribute in the following ways:

1) We provide an enhanced defense against side-channel attacks by integrating Ciphertext and Message Polynomial Sanity Checks improving post-quantum cryptographic systems as an effective measure to prevent attacks.
2) strengthened security through the strategic application of arithmetic masking in both encryption and decryption processes. By injecting random masks, our method significantly raises the difficulty for potential attackers, ensuring the robustness of post-quantum cryptographic systems.

II. RELATED WORKS

A. Attack Techniques

In [17], a novel single-step message recovery method is presented, allowing for the direct retrieval of the message without the explicit recovery of individual shares. This

* Computer Science and Technology, Ulsan National Institute of Science and Technology. Ulsan, South Korea. xyin@unist.ac.kr.

innovative approach utilizes a neural network trained during the profiling stage on traces that encompass both shares, with each labeled by the value of the corresponding message bit. This method has been applied to first order masking.

In [18], demonstrated successful message and secret key recovery attacks on the second- and third-order masked implementations running on a different device than the profiling one. In [19], attacks on the second masked implementations have been also demonstrated by employing the error-injection method as the chosen attack strategy.

In [16], a side-channel attacks on up to the fifth-order masked software implementations of CRYSTALS-Kyber exploiting a vulnerability was demonstrated. The attacks were performed using a new neural network training method called recursive learning and cyclic rotation-based message recovery method. During the profiling stage, 30,000 power traces were gathered from the decapsulation process involving various ciphertexts for the same Key Encapsulation Mechanism (KEM) pair and a known keypair. The outcomes demonstrated that the likelihood of recovering a message bit from a lone trace of a first-order masked implementation, excluding cyclic rotations, was 0.127%. However, incorporating cyclic rotations substantially elevated the success rate to 87%.

B. Defense mechanisms

Numerous Side-Channel Analysis countermeasures have been suggested, and some of them have being successfully implemented. One of the preferred methods to protect against Side-Channel Analysis is masking, especially for differential power analysis attacks is a widely used method [20] [21]. [20] presented a protected binomial sampler which provides protection against a side-channel analysis at any order. This relies on a new conversion between Boolean and arithmetic (B2A) masking schemes for prime moduli which can be implemented to CRYSTALS-Kyber.

In [22], Introduced an alternative method centered on detection. Countermeasures based on detection assess whether a received ciphertext exhibits malicious characteristics. Upon detecting malicious intent, the device under test (accessible to the attacker) can promptly reject the ciphertext and initiate a change or refresh of the public-private key pair by rerunning the key-generation procedure. This approach guarantees that, upon detection, the risk of prolonged exposure of the secret key is effectively mitigated.

III. METHODOLOGY

As the attack vectors to encrypted systems evolve, securing post-quantum cryptography systems against side-channel attacks (SCAs) requires a multifaceted approach. In this work we propose a robust combination of detection-based countermeasures and arithmetic masking to improve the security of cryptographic algorithms, specifically focusing on Chosen-Ciphertext Attacks (CCAs) within the Kyber Key Encapsulation Mechanism (KEM).

A. Detection-Based Countermeasure Integration

Ciphertext Sanity Check: Implemention of the Ciphertext Sanity Check involves a meticulous analysis of ciphertext coefficients to identify irregularities. This detection mechanism aims to detect malicious ciphertexts based on their statistical characteristics, specifically focusing on the distribution of coefficients. When integrated into our methodology, this countermeasure can be used as an initial defense method against specific side-channel attacks.

Message Polynomial Sanity Check: By analyzing the coefficients of the noisy message polynomial during decryption, we can enhance our ability to detect potential attacks that exploit vulnerabilities in the decryption process. This countermeasure acts as a complementary strategy, focusing on the subtle variations introduced during cryptographic operations.

B. Arithmetic Masking Integration

Arithmetic masking is introduced to mitigate the impact of potential side-channel attacks. This technique involves injecting randomness into intermediate computations during cryptographic operations, obscuring the true values being processed. In our methodology, arithmetic masking is strategically applied to both the encryption and decryption processes.

Encryption Phase: During encryption, random masks are introduced to the intermediate values of the cryptographic algorithm. The incorporation of masks prevents an attacker from extracting meaningful information even if side-channel leakage occurs during this phase. This countermeasure disrupts the correlation between the sensitive data and observable side-channel information, enhancing the security of the encryption process.

Decryption Phase: Arithmetic masking is also applied to the decryption phase, ensuring that the intermediate computations are consistently obfuscated. By introducing randomness into the decryption process, our methodology aims to minimize the effectiveness of side-channel attacks attempting to exploit the information leaked during this critical stage. The unpredictability introduced by masking would increase the level of complexity for malicious attacker.

C. Parallel Operation

The integration of detection-based countermeasures and arithmetic masking is designed for synergistic operation. The Ciphertext Sanity Check and Message Polynomial Sanity Check serve as the initial filters, identifying potential threats based on statistical irregularities. If a malicious ciphertext is detected, the system triggers a response that includes rejecting the ciphertext and refreshing the cryptographic keys.

Arithmetic masking is parallel to the detection-based countermeasures, ensuring that even if a side-channel attack bypasses the initial detection, the leaked information remains unintelligible due to the presence of random masks. The unpredictability introduced by masking significantly raises

the dificulty for attackers attempting to exploit side-channel vulnerabilities.

IV. CONCLUSION

Our methodology combines sophisticated detection-based countermeasures with the robust protection offered by arithmetic masking. This integrated approach aims to provide a resilient defense against side-channel attacks, particularly in the context of CCAs targeting the Kyber KEM. By leveraging the strengths of both detection and masking, our methodology contributes to the ongoing efforts to enhance the security of post-quantum cryptographic systems in the face of evolving cyber threats.

REFERENCES

[1] Y. Kanamori and S.-M. Yoo, "Quantum computing: principles and applications," *Journal of International Technology and Information Management*, vol. 29, no. 2, pp. 43–71, 2020.

[2] D. Rosch-Grace and J. Straub, "Analysis of the likelihood of quantum computing proliferation," *Technology in Society*, vol. 68, p. 101880, 2022.

[3] P. Ravi, A. Chattopadhyay, and S. Bhasin, "Security and quantum computing: An overview," in *2022 IEEE 23rd Latin American Test Symposium (LATS)*. IEEE, 2022, pp. 1–6.

[4] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Springer, 2022, pp. 397–407.

[5] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[6] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[7] R. C. Merkle, *Secrecy, authentication, and public key systems.* Stanford university, 1979.

[8] J. Patarin, "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*. Springer, 1996, pp. 33–48.

[9] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4*. Springer, 2011, pp. 19–34.

[10] A. Wang, D. Xiao, and Y. Yu, "Lattice-based cryptosystems in standardisation processes: A survey," *IET Information Security*, vol. 17, no. 2, pp. 227–243, 2023.

[11] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *US Department of Commerce, NIST*, 2022.

[12] J. N. Ortiz, R. R. de Araujo, D. F. Aranha, S. I. Costa, and R. Dahab, "The ring-lwe problem in lattice-based cryptography: The case of twisted embeddings," *Entropy*, vol. 23, no. 9, p. 1108, 2021.

[13] J. Vakarjuk, N. Snetkov, and J. Willemson, "Dilizium: A two-party lattice-based signature scheme," *Entropy*, vol. 23, no. 8, p. 989, 2021.

[14] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.

[15] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023.

[16] E. Dubrova, K. Ngo, J. Gärtner, and R. Wang, "Breaking a fifth-order masked implementation of crystals-kyber by copy-paste," in *Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop*, 2023, pp. 10–20.

[17] K. Ngo, E. Dubrova, Q. Guo, and T. Johansson, "A side-channel attack on a masked ind-cca secure saber kem implementation," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 676–707, 2021.

[18] K. Ngo, R. Wang, E. Dubrova, and N. Paulsrud, "Side-channel attacks on lattice-based kems are not prevented by higher-order masking," *Cryptology ePrint Archive*, 2022.

[19] A.-M. E. Emanations, "A message recovery attack on lwe/lwr-based pke/kems using amplitude-modulated em emanations," in *Information Security and Cryptology–ICISC 2022: 25th International Conference, ICISC 2022, Seoul, South Korea, November 30–December 2, 2022, Revised Selected Papers*, vol. 13849. Springer, 2023, p. 450.

[20] T. Schneider, C. Paglialonga, T. Oder, and T. Güneysu, "Efficiently masking binomial sampling at arbitrary orders for lattice-based crypto," in *Public-Key Cryptography–PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II 22*. Springer, 2019, pp. 534–564.

[21] F. Bache, C. Paglialonga, T. Oder, T. Schneider, and T. Güneysu, "High-speed masking for polynomial comparison in lattice-based kems," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 483–507, 2020.

[22] P. Ravi, A. Chattopadhyay, J. P. D'Anvers, and A. Baksi, "Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, dilithium): Survey and new results," *ACM Transactions on Embedded Computing Systems*, 2022.