Decoding the CRYSTALS-Kyber attack using artificial intelligence: Examination and strategies for resilience

Maksim Iavich[1,*,†], Sergiy Gnatyuk[2,†] and Assel Mukasheva[3,†]

[1] Caucasus University, 1 Paata Saakadze str., 0102 Tbilisi, Georgia
[2] National Aviation University, 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine
[3] Kazakh-British Technical University, 59 Tole Bi str., 050000 Almaty, Kazakhstan

Abstract

The recent advancements in artificial intelligence and quantum computing pose a significant threat to traditional public key cryptosystems. In this context, Kyber, a post-quantum encryption technique relying on lattice problem hardness, has been standardized. Despite thorough testing by the National Institute of Standards and Technology (NIST), recent investigations expose vulnerabilities in CRYSTALS-Kyber, demonstrating its susceptibility to attacks in non-controlled environments using AI. This study delves into the susceptibility of CRYSTALS-Kyber to side-channel attacks. Based on the study of the reference implementation of Kyber512, it becomes clear that the use of selected ciphertext allows additional functions to be compromised. The successful implementation of the last allows for real-time recovery of the entire secret key in various attack scenarios.

Keywords

post-quantum cryptography, machine learning, recursive learning, lattices, NIST, Kyber

1. Introduction

The impending rise of quantum computing heralds a transformative era in computing capabilities. Post-quantum cryptography, or quantum encryption, offers mechanisms to protect classical computers from potential threats posed by quantum computers. These systems provide defense mechanisms against the exponential speed advantage of quantum computers, which exploit the distinctive properties of quantum mechanics. The urgency of this transition is underscored by the stark contrast between the rapid quantum computing of complex problems and the prolonged execution times required by traditional computers.

The development of quantum computing raises concerns about the viability of current cryptographic methodologies, particularly those reliant on RSA. RSA, a widely used public key cryptosystem, relies on the complexity of mathematical problems such as integer factorization. However, the advent of large-scale quantum computers equipped with Shor's algorithm poses a significant threat to the security of existing public key cryptographic systems by rapidly solving these mathematical challenges [1–3].

In response to this impending challenge, post-quantum cryptosystems are being developed to withstand and thwart quantum attacks. The evolution of quantum technology necessitates the continuous pursuit of resilient post-quantum systems, as conventional asymmetric methods like RSA may prove inadequate in safeguarding private data.

To anticipate the impact of quantum computers on cryptographic security, the National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography Standardization Initiative (NIST PQC) in 2016. This initiative aims to establish robust cryptographic algorithm standards capable of withstanding quantum computer attacks and protecting confidential data in the post-quantum computing era. The project's approach involves soliciting, evaluating, and standardizing quantum-resistant cryptographic algorithms.

NIST initiated the process by selecting a group of potential algorithms submitted by the cryptography community. Rigorous testing ensued, focusing on the resilience of these candidates against quantum attacks. The chosen primitives are grounded in linear error-correcting code decoding and lattices, addressing mathematical challenges deemed formidable for quantum computers.

In a significant development, NIST announced in July 2022 that CRYSTALS-Kyber would become the new standard for key setup and public key encryption (PKE). This decision underscores its identification as a key encapsulation mechanism (KEM) securing IND-CCA2 in both classical and quantum models of random oracles. CRYSTALS-Kyber's security is rooted in the complexity of the module learning with errors (M-LWE) problem, introducing unknown noise into linear equations [4, 5].

Furthermore, the prompt inclusion of CRYSTALS-Kyber by the National Security Agency (NSA) in its recommended cryptographic algorithms for national security applications

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
miavich@cu.edu.ge (M. Iavich);
s.gnatyuk@nau.edu.ua (S. Gnatyuk);
a.mukasheva@gmail.com (A. Mukasheva)

0000-0002-3109-7971 (M. Iavich);
0000-0003-4992-0564 (S. Gnatyuk);
0000-0001-9890-4910 (A. Mukasheva)
© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3826/short26.pdf

highlights its significance in protecting cryptographic systems from emerging quantum threats.

CRYSTALS-Kyber, renowned for its IND-CCA2 security, operates as a KEM in classical and quantum random oracle models, making it immune to adaptive chosen ciphertext attacks. Its security derives from the severe problem of learning with errors (M-LWE), introducing unknown noise into linear equations. Despite the robust theoretical security foundations of CRYSTALS-Kyber and other post-quantum Public Key Encryption (PKE)/Key Encapsulation Mechanism (KEM) algorithms, vulnerabilities have surfaced in protected software implementations. Advanced side-channel analysis techniques, particularly those rooted in deep learning, have successfully compromised various versions of CRYSTALS-Kyber. These vulnerabilities encompass higher-order masked implementations, first-order software implementations with mask and shuffle, and first-order mask implementations. Identifying these susceptibilities prompted the development of enhanced defenses against side-channel attacks, leading to the refinement of CRYSTALS-Kyber implementations.

Given the well-established vulnerabilities, it is essential to assess and enhance the resilience of CRYSTALS-Kyber implementations against side-channel attacks. These attacks exploit data obtained from physically available channels, such as the timing or power consumption of the device running the application, posing a significant threat to the security of cryptographic implementations.

Significant progress has been made in the field of side-channel analysis, exemplified by Kocher et al.'s development of Differential Side-Channel Analysis, which utilizes differences in physical data. Another noteworthy advancement is the introduction of Deep Learning-Based Side-Channel Analysis, enabling attacks on a diverse array of cryptographic systems. Existing defense mechanisms prove inadequate against these sophisticated attacks. Additionally, Wang et al.'s Error Injection Method has demonstrated effectiveness in dismantling robust targets, including CRYSTALS-Kyber's hardware implementations, by transforming non-differential attacks into differential ones.

To mitigate the risks associated with side-channel attacks, various countermeasures have been deployed. These measures include masking, shuffling, randomized clock, random delay insertion, constant-weight encoding, and code polymorphism. These countermeasures aim to prevent information leakage through physically measurable channels such as time, power consumption, or electromagnetic radiation, thereby protecting cryptosystems [6, 7].

In conclusion, the development of AI and by means of it the escalating sophistication of side-channel attacks underscores the critical need for continuous evaluation and enhancement of cryptographic implementation security [8]. This imperative is particularly pronounced in the domain of post-quantum cryptography algorithms like CRYSTALS-Kyber. As the cryptographic landscape evolves, proactive measures must be taken to stay ahead of emerging threats and fortify the security posture of these vital encryption techniques.

2. Kyber encryption system

Kyber is recognized as a secure Key Encapsulation Mechanism (KEM) with IND-CCA2 security, stemming from its ability to address the learning-with-errors (LWE) problem within module lattices [9]. It has emerged as a prominent contender in the NIST Post-Quantum Cryptography Project. The proposal outlines three distinct parameter sets, meticulously crafted to achieve specific security levels. Specifically, Kyber-512 aims to provide security comparable to AES-128, Kyber-768 targets a level roughly equivalent to AES-192, and Kyber-1024 aims to match the security level of AES-256 [10].

An effective strategy involves leveraging Kyber in a hybrid mode by integrating it with established "pre-quantum" security protocols. For instance, combining Diffie-Hellman with an elliptic curve capitalizes on the strengths of both classical and post-quantum cryptography, thereby enhancing overall security [11–13].

Particular emphasis is placed on recommending the use of the Kyber-768 parameter set. This selection is grounded in a thorough analysis indicating that it provides more than 128 bits of security against all recognized conventional and quantum attacks. The decision is underpinned by a highly conservative assessment, wherein 128 bits of security are deemed exceptionally robust, offering resilience against a spectrum of both known and unforeseen threats in the cryptographic landscape.

In the summer of 2022, the NIST selected a candidate proposal based on Post-Quantum Cryptography (PQC) for standardization, specifically, the CRYSTALS-Kyber. This innovative quantum-safe key encapsulation technique falls under the acronym CRYSTALS, representing the Cryptographic Suite for Algebraic Lattices.

Kyber, an integral component of CRYSTALS-Kyber, stands out as a chosen ciphertext attack (CCA) secure Key Encapsulation Mechanism (KEM). Its foundation lies in the selected plaintext attack (CPA) secure Public Key Encryption (PKE) technique, resulting in a CCAKEM. Figs. 1 and 2 illustrate the utilization of an adapted version of the Fujisaki-Okamoto (FO) transform in CPAPKE. The security level of CRYSTALS-Kyber is determined by the rank of the module k, with the scheme utilizing vectors of ring elements in CRYSTALS-Kyber encompasses three variants for different values of k: Kyber-512, Kyber-768, and Kyber-1024, corresponding to k=2,3, and 4. Given that the target implementations support Kyber-512, this version takes precedence. To achieve efficient multiplications in R_q, CRYSTALS-Kyber employs the Number-Theoretic Transform (NTT).

The variable K is derived by combining the message and the hash of the public key with the hash of the CPAPKE.Enc function output, utilizing a key derivation function. In simpler terms, the encryption key (K) is generated by incorporating additional information related to the message and public key, along with encryption function outputs (CPAPKE.Enc).

This approach is described in detail in the definition of the Kyber.Encaps function.

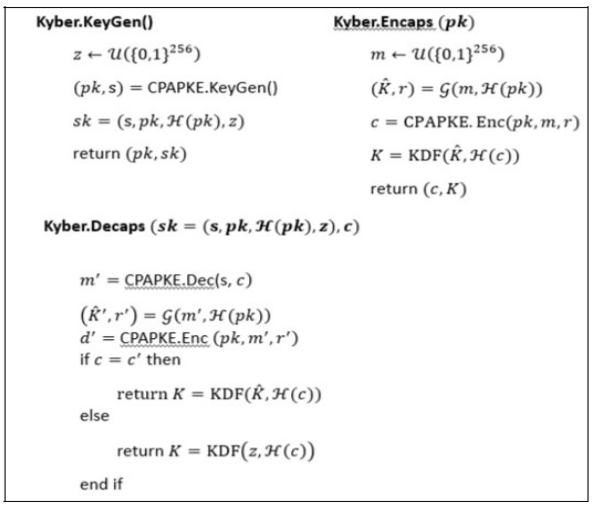

Figure 1: CCAPKE algorithms

The encryption process produces a value of K, and after decryption (Kyber.Decaps), the returned value of K may remain unchanged after encryption or be a deceptive value, depending on the assessment of the potentially malicious ciphertext (c).

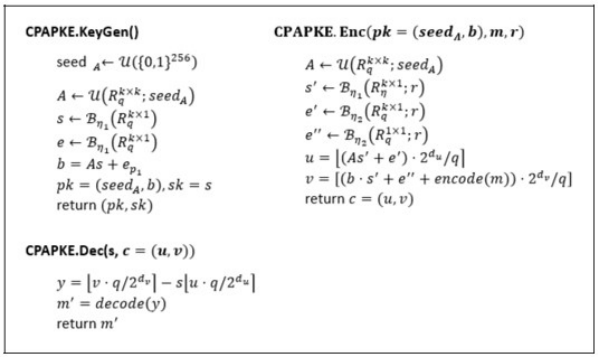

Figure 2: CCAKEM algorithms

A modification has been implemented to the input r for CPAPKE.Enc, which is the result of the message and public key hashing as opposed to being an arbitrary value. The objective of this adjustment is to enhance security.

Error-Based Learning systems, as examples in cases like Kyber, are vulnerable to decryption failures. The intentional manipulation of these failures by adversaries could potentially result in the exposure of sensitive information. Instances of decryption failures become more pronounced when attackers manipulate covert vectors and error values, causing them to surpass the defined parameters in the CPAPKE.Enc scheme.

By employing a modified variant of the Fujisaki-Okamoto transform, the procedures of encapsulation and decapsulation (Kyber.Encaps and Kyber.Decaps) ensure the legitimate generation of random secret and error values, with verification incorporated into the decryption process.

In terms of ensuring CCA2 security, the CRYSTALS-Kyber algorithm employs the Fujisaki-Okamoto transformation. The process is initiated by decrypting the ciphertext using CPA. Subsequently, a new ciphertext ′is generated through "re-encryption" using CPA encryption on the message. The process then assesses the equality between ′and the public ciphertext c. The algorithm outputs True if c=′and False otherwise. The session key K is generated depending on this Boolean result. The Fujisaki-Okamoto-transform is executed to verify the absence of any alterations made by a potential adversary.

Generally, the Kyber mechanism safeguards against attackers attempting to exploit vulnerabilities of encryption-decryption procedures.

3. Side-channel attacks

One-time signature schemes are very inconvenient to use because to sign each message, we need to use a different key pair. The problem with such schemes is that they require storing *n* digesting. For everyday use it is impractical, and we would like a scheme that allows us to store a uniform-sized digest, no matter how many files we have. Merkle Tree was proposed to solve this problem. By using a binary tree as the root, this approach can replace a large number of verification keys with a single public key. A cryptographic hash function and a one-time Lamport or Winternitz signature scheme are used in this system.

A cryptographic system relies on highly intricate mathematics, which may give the impression of being impervious to mathematical attacks. However, it remains susceptible to side-channel attacks, first identified by Paul Kocher in 1996, which exploit data leakage while the cryptographic device is operational. This leaked information can manifest in various forms, such as electromagnetic radiation, power consumption, sound waves, or execution time. Systems employing cryptography are vulnerable to side-channel attacks. While many contenders in post-quantum cryptography (PQC) are engineered to withstand direct timing attacks, certain techniques like power and electromagnetic analysis can still expose vulnerabilities. Researchers are actively engaged in exploring and addressing these weaknesses, with NIST stressing the importance of integrating side-channel resistance into PQC. The ongoing research endeavors to fortify PQC's resilience against diverse side-channel attacks [14–17].

Extensive scholarly research has focused on examining the susceptibility of lattice-based Key Encapsulation Mechanisms (KEMs) to various side-channel attacks, with particular attention on side-channel-assisted chosen-ciphertext attacks (CCAs). CCAs are designed to acquire the secret key and have been the subject of multiple studies. These investigations delve into CCAs targeting different operations within lattice-based KEMs. The scrutinized operations include the Fujisaki–Okamoto (FO) transform, message encoding/decoding, error-correcting codes, and inverse NTT. Side-channel attacks exploit non-primary channels, such as power usage or timing, to unveil vulnerabilities. Researchers employed vertical side-channel leakage detection to scrutinize the decryption mechanism of CRYSTALS-Kyber to identify potential weaknesses in the electrical signals generated during cryptographic operations.

KYBER-512 exhibits vulnerabilities that enable an attacker to completely recover the key using simple queries, as they can access the content of decrypted messages. The investigation focused on the clean and m4 scheme elements, specifically message encoding and the inverse Number

Theoretic Transform (NTT). It is notable that for both clean and m4 schemes, the secret key can be recovered in just four and eight searches, respectively. Additionally, researchers have proposed message recovery techniques involving cyclic message rotation and targeted permutation of message bits. Even though these methods required (w+1) traces in the presence of a side-channel weighted Hamming classifier, it was emphasized that applications employing anti-masking and anti-shuffling measures could still be vulnerable. Conversely, launching attacks on secure implementations with shuffling and obfuscation necessitated a strong assumption that the attacker could disable countermeasures to create patterns.

Furthermore, the researchers proposed a key recovery attack based on recovered messages, which would require a set of six specific ciphertexts. It is essential to note that the noise value for KYBER-512 has been increased, and the CRYSTALS-KYBER specification has been adjusted. This implies that a more meticulous preparation of ciphertexts is now necessary.

4. Masking

Verkle trees are a powerful upgrade to Merkle trees (Fig. 3) that allow for much smaller verifications and are more efficient. The structure of the Verkle tree (Fig. 4) is very similar to the Merkle Patricia tree [15, 18, 19].

To enhance the resistance of CRYSTALS-Kyber against side-channel attacks, masking will be implemented as a countermeasure. This strategy involves partitioning a secret into multiple partially randomized shares, with "fifth-order" indicating that the secret is divided into five shares. Masking obscures the underlying arithmetic behavior of cryptographic algorithms, offering additional protection against side-channel threats.

Masking serves as a prominent defense mechanism against power and electromagnetic side-channel investigations. Essentially, this method entails randomly dividing a concealed value into several shares, each processed independently at every stage of the algorithm. Their outcomes are then combined to generate the final result. Operating within the masking domain prevents the leakage of sensitive variable x's information, as it is never directly utilized. In an ω-order masking scheme, a sensitive variable x is divided into ω+1 share, denoted as x=1 ∘ 2 ∘ …∘+1. The choice between arithmetic and Boolean masking depends on the specific technique, where "∘" represents different operations. For instance, in arithmetic masking, "∘" signifies addition, while in Boolean masking, it denotes XOR.

The variable x does not directly partake in the computation, as operations are conducted independently on shared resources, theoretically preventing information leakage about x through side channels. Each time a share is processed, it is randomly assigned. Randomization is typically achieved by distributing random masks 1, 2, …, across shares ω, and then computing arithmetic masking as—(1+2+ ⋯ +) or logical masking as ⊕ 1 ⊕ 2 ⊕ … ⊕.

5. The analysis of the Attacks using AI against CRYSTALS-Kyber

To standardize post-quantum encryption, CRYSTALS-Kyber has been officially endorsed by NIST as a public-key algorithm. Despite initial beliefs in its resilience against side-channel attacks, researchers have successfully identified a vulnerability in its implementation. Utilizing machine learning techniques, the attack specifically focused on power usage as a key element of its strategy [20–25]. The increasing accessibility of measuring and analyzing computer hardware power usage has raised concerns about side-channel attacks as a significant security concern. These attacks exploit energy fluctuations during certain circuits or processes to obtain detailed information about the system or processed data [26].

A successful side-channel attack was carried out on CRYSTALS-Kyber, revealing details about the encryption key, which is one step before decrypting the data. Exploiting machine learning to enable the system to capitalize on the side-channel facilitated the attack. Considering that machine learning is not commonly used in security research, this achievement is remarkable. Thus, it's notable that machine learning can be misused, and businesses must be vigilant about the potential security threats it may pose. Even though the attack on CRYSTALS-Kyber was successful, this does not mean that it is completely unusable. We need to be aware of the possible security threats that machine learning can pose to use these types of attacks. The algorithm remains secure.

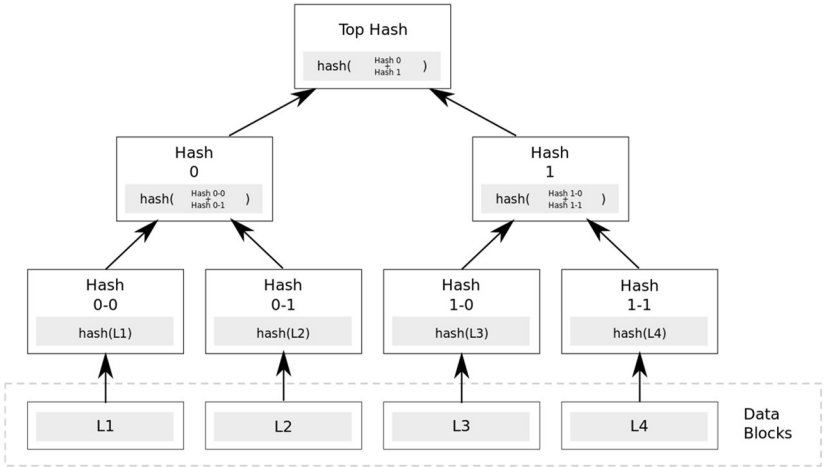

Figure 3: Merkle Tree example

Earlier research has utilized artificial intelligence (AI) to compromise first, second, and third-order masked Kyber implementations. However, breaking higher-order masked implementations using traditional AI training and profiling techniques proved challenging. Dubrova et al. overcame this challenge by employing a novel form of deep learning and rotations on intercepted messages, thereby increasing the leakiness of the bits and enhancing the likelihood of a successful attack [25–28].

The initial presentation of the attack by Dubrova et al. focused on Kyber's first-order masking, extending the function masked_poly_frommsg() to incorporate higher-order masking. Further exploration is intended to assess the power consumption of the presented method, particularly during Kyber's re-encryption phase. This phase targets the decapsulation stage, where the shared key is retrieved and undergoes a re-encapsulation process for verification of any alterations in the ciphertext.

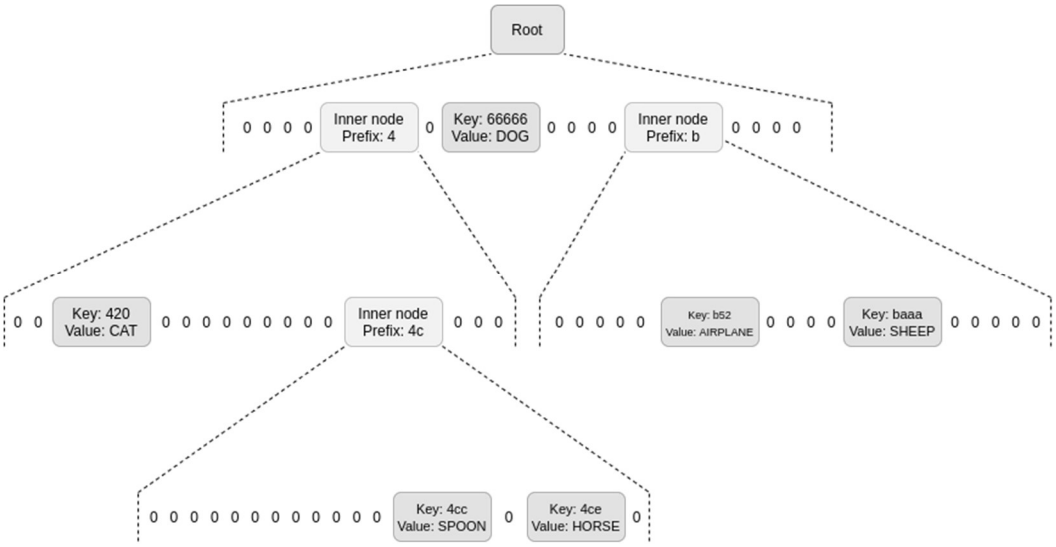

Figure 4: Verkle Tree example

In this re-encryption process, the secret or the antecedent of the shared key is meticulously stored bit by bit into a polynomial. Specifically, the 256-bit secret is transformed into a polynomial modulo q = 3329 with 256 coefficients. In this transformation, the i^{th} coefficient is $(q+1)/2$ if the i^{th} bit is 1, and 0 otherwise. Although the function may seem simple, creating a masked version poses a challenge due to the inherent method of generating shares of the secret, involving xor-ing together, and adding shares to form the hypothetical polynomial.

In contrast to previous studies, the AI incorporates recursive learning at the profiling stage. Training an implementation with a w-order mask involves replicating the weights of the input batch normalization layer from the −1 model trained on the implementation with a $(w-1)$-order mask. Subsequently, the layer is expanded to introduce an additional share, creating the initial network. Recursive learning comes into play when w>3, and the AI undergoes training using a network with a standard random weight distribution when w≤3.

By utilizing cut-and-join training traces byte-wise, two universal models, 0 and 1, are derived. These models capture the most powerful leaks, paying special attention to the first two bits of each message byte. Furthermore, the labels "0" and "1" are assigned to message bits, and the AI is trained to directly recover the message without eliminating the random masks.

As detailed in the attacks described in this paper, after rotating the message three times, the last six bits of each byte are moved to the positions of the initial two bits. This approach increases the probability of success of the attack by utilizing "more leakage" of bit locations, extracting bit values with a higher probability.

The attack employs the cyclic rotation method due to the uneven distribution of leakage from Masked_poly_frommsg(). This irregularity is evidenced by a 9% dissimilarity in the successful recovery probability between 0 and 7 bits. Furthermore, this approach is facilitated by the fact that modular LWEs are ring LWEs extensions, enabling the alteration of encrypted texts by cyclically alternating messages. By changing the last 6 bits to the first and second bits in each byte, the attack non-cyclically modifies the message three times to 2 bits. This strategy allows for more efficient transmission of information by bits without excessive time consumption compared to other looping approaches.

By manipulating the corresponding ciphertext, it becomes possible to perform a message rotation. In CRYSTALS-Kyber, a ciphertext c=(u,v) is composed of polynomials in the ring $\mathbb{Z}[\ ]/(256+1)$. To obtain a negacyclic rotation of the message, it is necessary to multiply u and v by the indeterminate X, under the condition that c is constructed accurately. However, it's important to note that the Decode (-y) and Decode (y) operations may yield dissimilar values, introducing the possibility of errors, particularly with specific ciphertexts employed in attempts to recover the secret key [29].

The code iterates over the portions of the two shares, generating a mask for each bit: 0xffff for 1, and 0 for 0. This mask can be applied to increase the polynomial share by (q+1)/2, requiring slightly more energy to treat a 1. This function will leak information without the need for AI. This vulnerability in the pattern was recognized as problematic

in 2016, raising concerns about a potential risk to Kyber in 2020. To mitigate this [30], processing multiple bits simultaneously is a recommended countermeasure.

Dubrova et al., the authors, do not assert that this is a radically innovative approach to the attack. Instead, they increase the attack's effectiveness by training the neural network and optimizing the utilization of numerous traces through alterations in the sent ciphertext.

Dubrova et al. conducted the proposed attack using an ARM Cortex-M4 CPU together with STM32F415-RGT6 device, a CW308 UFO board, and a 24MHz target board-CW308T-STM32F4. Power consumption measurements were carried out with high accuracy up to 10 bits at a frequency of 24 MHz.

To train the neural networks, Dubrova et al. collected 150,000 power traces to decrypt various ciphertexts using the same KEM keypair. While this approach is somewhat unusual for a real-world attack, as KEM key pairs for key agreements are typically non-durable, nevertheless it has valid applications for long-term KEM key pairs, as well as ECH, HPKE, and authentication [31].

Training is a crucial step as devices of the same make and model may exhibit significantly different power traces even when executing identical code. Neural networks undergo training to target "shares", representing implementations with varying security levels. The progression begins with attacking a five-share implementation as the initial step to a six-share implementation. Executing their methodology requires extracting one-fifth of the 150,000 power traces against a six-share execution, then repeating the process with a five-share execution, and so forth. The scenario where a device permits an attacker to manipulate share numbers appears improbable. The authors initiate the actual attack by asserting that, under optimal conditions, there is a 0.127% probability of recovering the shared key. However, they do not furnish specific figures for single-trace assaults involving more than two shares.

Side-channel attacks demonstrate increased success when multiple traces of the same decapsulation are employed. The authors introduce a clever twist by rotating the ciphertext instead of using identical traces of the message. This strategic rotation, particularly when four identical traces are involved, elevates the likelihood of success to 78%, compared to a two-share implementation. Even with a 0.5% chance, the six-share implementation remains strong. Remarkably, 87% of the shared key can be recovered with 20 traces from the six-share implementation. For each w-order masked realization, 2500 messages are randomly selected, resulting in a total of 10,000 traces for each message, including three 2-bit cyclic message rotations in each trace. In the absence of cyclic rotations, the likelihood of message recovery is 0.127%. However, this probability significantly increases to 78.866% with the introduction of cyclic rotations. For a single trace on a fifth-order masked implementation using cyclic rotations, the recovery probability is 0.56%, rising to 54.53% with three traces, and peaking at 87.085% with five traces respectively [31, 32].

In hardware terms, the device may resemble a smart card in some aspects, but it is quite different from high-end devices such as desktops, servers, and mobile phones. Even with 1 GHz embedded processors, performing simple side-channel attacks to analyze power consumption becomes an extremely complex task, requiring thousands of traces and a high-performance oscilloscope placed directly next to the processor. This physical access to the server provides broader attack vectors, simply connecting the oscilloscope to the memory bus.

Power-side channel attacks are typically considered impractical, except for highly sensitive applications. However, under specific circumstances, throttling can potentially transform an exceptionally potent power side-channel attack into a remote timing attack. It's important to note that the current situation is far from resembling such an attack [33].

Moreover, this attack is neither particularly potent nor surprising. In practical terms, whether a masked implementation reveals its secrets or not is inconsequential. The critical question is the level of difficulty involved in executing such attacks in real-world scenarios. Articles such as this one help manufacturers in assessing the number of countermeasures needed to make such attacks prohibitively expensive.

6. Protection measures

Minimizing the exposure duration of the application's secret key serves as the most effective defense against a majority of existing attacks. The attack becomes more challenging as the secret key is disclosed fewer times. If a secret key is used only once, the attacker can only utilize the message recovery attack once. However, this approach may introduce other challenges, such as the need to generate a substantial number of secret keys or the elimination of secret key usage altogether.

The success of the given attack relies on the repeated execution of the decapsulation procedure. The attack can be hindered by limiting the number of decryptions of the same ciphertext with a single secret key. It may be necessary to allow multiple retries to accommodate occasional communication errors.

Alternatively, stronger defenses against power analysis attacks, such as the proposed duplication by clock randomization approach, can be considered. This approach involves two identical cores: a main cryptographic core and a dummy cryptographic core, constituting the protected realization. Despite using different private and public key pairs, these cores operate on two different random clocks while receiving identical input data. This technique offers several camouflage benefits, including fault immunity, zero clock cycle overhead, universal coverage, and increased resistance to replay attacks.

7. Conclusions

Because of the increased power of AI technologies, the CRYSTALS-Kyber key encapsulation system faces increasing challenges from sophisticated side-channel attacks. Recent research reveals vulnerabilities even in environments with strong security measures, highlighting the necessity for ongoing defensive improvements. Essential countermeasures to bolster cryptographic systems

include Masking and shuffling. As we transition into the post-quantum era, evaluating algorithms for both mathematical robustness and resistance to external attacks becomes crucial.

Rather than completely disrupting a new encryption system, AI serves as a valuable tool for managing noisy data and detecting its weaknesses. There is a fundamental difference between a power side-channel attack and a direct cryptographic violation. The actual attack is based on a surprisingly small number of traces; however, it is still possible to effectively use extremely noisy traces for deep learning training. An intriguing aspect of this debate is the limited availability of feasible, simple, affordable, and effective defenses to counter these attacks through channels of power. We plan to improve the existing scheme, using provided by us recommendations.

Acknowledgments

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSF) [STEM – 22 –1076].

References

[1] D. Aggarwal, U. Maurer, Breaking RSA Generically is Equivalent to Factoring, Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (2009).

[2] D. R. L. Brown, Breaking RSA May Be as Difficult as Factoring, J. Cryptology, 29 (2016) 220–241. doi: 10.1007/s00145-014-9192-y.

[3] M. Sharma, et al., Leveraging the Power of Quantum Computing for Breaking RSA Encryption, Cyber-Physical Systems 7(2) (2021) 73–92.

[4] R. Avanzi, et al., Crystals-Kyber, NIST, Tech. Rep. (2017).

[5] E. Dubrova, et al., Breaking a Fifth-Order Masked Implementation of Crystals-Kyber by Copy-Paste, in: 10th ACM Asia Public-Key Cryptography Workshop (2023).

[6] F.-X. Standaert, Introduction to Side-Channel Attacks, Secure Integrated Circuits and Systems (2010) 27–42.

[7] M. Randolph, W. Diehl, Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman, Cryptography, 4(2) (2020).

[8] O. Mykhaylova, et al., Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 239–251.

[9] J. Bos, et al., CRYSTALS-Kyber: a CCA-Secure Module-Lattice-based KEM, IEEE European Symposium on Security and Privacy (EuroS&P) (2018).

[10] W. Guo, S. Li, L. Kong, An Efficient Implementation of Kyber, IEEE Transactions on Circuits and Systems II: Express Briefs, 69(3) (2021) 1562–1566.

[11] A. Bessalov, V. Sokolov, S. Abramov, Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves, Cryptography 8(3), iss. 38 (2024) 1–17. doi:10.3390/cryptography8030038.

[12] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10

[13] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[14] M. Iavich, et al., Use of Content-Filtering Method for Hardware Vulnerabilities Identification System, in: IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT) (2021).

[15] R. Megrelishvili, et al., Post-Quantum Key Exchange Protocol using High Dimensional Matrix, in: International Conference on Information Technologies, vol. 2145 (2018) 83–87/

[16] Z.-D. Zhang, et al., Study on the Convective Heat Transfer Characteristics of Supercritical CO2 in Mini-Channels under Unilateral Heating Conditions for Application in a Compact Solar Receiver, Int. J. Heat Mass Transfer. 219 (2024) 124839.

[17] M. Iavich, et al., Lattice based Merkle, in: International Conference on Information Technologies, vol. 2470 (2019) 13–16.

[18] V. Kharchenko, I. Chyrka, Detection of Airplanes on the Ground using YOLO Neural Network, International Conference on Mathematical Methods in Electromagnetic Theory (2018) 294–297.

[19] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[20] O. Solomentsev, M. Zaliskyi, Method of Sequential Estimation of Statistical Distribution Parameters in Control Systems Design, in: IEEE 3rd International Conference on Methods and Systems of Navigation and Motion Control (2014) 135–138.

[21] S. Tynymbayev, et al., Modular Reduction based on the Divider by Blocking Negative Remainders, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences 2(434) (2019) 238–248. doi: 10.32014/2019.2518-170x.60.

[22] S. Gnatyuk, et al., New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing (2020) 93–104.

[23] A. Celik, et al., Implementation of CRYSTALS-Kyber Post-Quantum Algorithm using RISC-V Processor, 30th IEEE International Conference on Electronics, Circuits and Systems (ICECS) (2023) 1–4.

[24] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

[25] S. Gnatyuk, et al., Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, in: 16th International Conference on Control, Automation and

Systems (2016) 1476–1479. doi: 10.1109/iccas.2016.7832498.

[26] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187 (2022) 302–309.

[27] O. Solomentsev, et al., Sequential Procedure of Changepoint Analysis during Operational Data Processing, in: IEEE Workshop on Microwave Theory and Techniques in Wireless Communications (2020) 168–171.

[28] S. Jendral, et al., Breaking SCA-Protected CRYSTALS-Kyber with a Single Trace, IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (2024) 70–73.

[29] C. Papamanthou, et al., Streaming Authenticated Data Structures, Advances in Cryptology—EUROCRYPT (2013) 353–370. doi: 10.1007/978-3-642-38348-9_22.

[30] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

[31] Y. Ji, etb al., A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber, IEEE European Test Symposium (ETS) (2023) 1–5.

[32] D. S. Hegde, et al, Rapid Prototyping of CRYSTALS-Kyber Primitives on FPGA using Python-only HW-SW Flow, 28th International Symposium on VLSI Design and Test (VDAT) (2024) 1–6.

[33] J. Zhang et al., Super-K: A Superscalar CRYSTALS-KYBER Processor based on Efficient Arithmetic Array, IEEE Transactions on Circuits and Systems II: Express Briefs, 71(9) (2024) 4286–4290. doi: 10.1109/TCSII.2024.3382772.