IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 14, No. 6, December 2025, pp. 5251~5267
ISSN: 2252-8938, DOI: 10.11591/ijai.v14.i6.pp5251-5267

Securing post-quantum cryptography: side-channel resilience in CRYSTALS-Kyber key encapsulation mechanism

Shreyas Kasture[1], Sudhanshu Maurya[2,3], Alakshendra Pratap Singh[1], Amit Shukla[2], Arnav Kotiyal[4], Kashish Mirza[5]

[1]Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India
[2]Centre of Artificial Intelligence and Robotics, Indian Institute of Technology, Mandi, India
[3]Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies (Deemed to be University), Faridabad, India
[4]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India
[5]Department of Computer Science and Engineering, Graphic Era Hill University, Bhimtal, India

Article Info

Article history:

Received Sep 14, 2024
Revised Oct 18, 2025
Accepted Jan 28, 2025

Keywords:

Countermeasures
CRYSTALS Kyber KEM
Lattice-based cryptography
Post-quantum cryptography
Quantum key management system
Side-channel attacks

ABSTRACT

This study evaluates side-channel vulnerabilities in hardware implementations of the cryptographic suite for Algebraic lattices (CRYSTALS)-Kyber key encapsulation mechanism (KEM) using correlation and differential power analysis (DPA) techniques. Unprotected field-programmable gate array (FPGA) implementations across all Kyber parameter sets were successfully compromised, revealing significant information leakage. Attack complexity scaled linearly with key size. Additive Boolean masking provided varying protection levels, with 4-bit masking offering a 100× security increase at notable performance cost. Performance characterization showed increased slice utilization and reduced maximum frequency for higher-order masking. A novel hybrid countermeasure combining higher-order masking with controlled time randomization enhanced protection against machine learning-based attacks. Comprehensive power trace analysis using 12-bit precision at 500 MS/s sampling rates was conducted. Statistical evaluation utilized Pearson's correlation and Welch's t-tests with a 0.8 threshold for key recovery. Real-world validation in IoT, financial, and satellite scenarios highlighted practical post-quantum cryptography (PQC) deployment challenges. The study provides concrete design guidance for efficiently securing hardware Kyber implementations against side-channel attacks.

Corresponding Author:

Sudhanshu Maurya
Centre of Artificial Intelligence and Robotics, Indian Institute of Technology
Mandi, India
Email: dr.sm0302@gmail.com

1. INTRODUCTION

Public key cryptography faces an existential threat from the emergence of quantum computing that underpins secure communications and infrastructure on the internet and beyond. Quantum algorithms, like Shor's, can effectively defeat widely used techniques as elliptic curve cryptography and random-access public key cryptography (RSA), which depends on the enormous challenge of computing discrete logarithms or factoring large primes. A large enough quantum computer could crack the encryption securing online transactions, state secrets, intellectual property, and critical systems in minutes. With steady advances in quantum technology through efforts by leading tech firms, government labs, and academic institutions, many experts predict the achievement of quantum supremacy within the next decade. The risk of current classical

public key cryptosystems becoming completely insecure in the face of such powerful quantum attack is therefore increasing rapidly. This looming prospect has been termed the "quantum apocalypse" for encrypted communications [1].

Intense academic attention has been directed into creating new quantum-resilient cryptographic protocols and algorithms, collectively known as post-quantum cryptography (PQC), to address this significant flaw. Promising post-quantum techniques are being developed and enhanced across core approaches, including hash-based signatures, supersingular isogeny cryptography, multivariate cryptography, lattice-based cryptography, and code-based cryptography among others. Leading PQC candidates mathematically offer security even against assault by a full-scale, quantum computer that is fault-tolerant [2]. The National Institute of Standards and Technology (NIST) of the United States launched a multi-year global standardization process in 2017 to thoroughly analyse post-quantum algorithms, due to the urgency by the quantum threat and select the most secure and efficient designs across encryption, signatures, and key exchange. Out of an initial field of over 80 submissions, after three intensive rounds of assessment, NIST announced four algorithms in July 2022 to proceed to the standardization pipeline-lattice-based cryptographic suite for Algebraic lattices (CRYSTALS)-Kyber, N-th degree truncated polynomial ring unit (NTRU), and security attribute-based secure (SABER) as well as the lattice-based signature scheme CRYSTALS-Dilithium. Additionally, four other candidates including the isogeny-based supersingular isogeny key encapsulation (SIKE) were selected for further analysis in the fourth round.

As PQC continues rapid maturation toward eventual real-world deployment across the internet's trusted public key infrastructure, in specialized networks, and in critical embedded devices, efficient and verifiably secure engineering is crucial alongside the fundamental research. While the elaborate mathematics behind schemes like Kyber and SIKE may inherently provide quantum resilience, side-channel vulnerabilities introduced in implementations can still enable various practical attacks if not addressed. Physically observable characteristics during an operation like timing, power consumption, electromagnetic radiation, and more can leak secrets that bypass mathematical defences. Thus extensive analysis of a side-channel susceptibility as well as effective, efficient countermeasures is an imperative, complementary facet of fundamental PQC research all the way through standardization and adoption.

Lattice-based cryptography has emerged as a leading approach for developing PQC schemes secure against quantum computing attacks [3]. The CRYSTALS Kyber key encapsulation mechanism (KEM) is a prominent lattice-based algorithm currently undergoing evaluation for post-quantum standardization [4]. While the underlying construction promises, theoretical quantum resilience, real-world vulnerabilities still need to be assessed before widespread implementation. Side-channel attacks pose particular risks of leaking secret key information through physical emanations and need countermeasures. This research empirically analyses the side-channel attack resilience of hardware Kyber implementations to evaluate a susceptibility and determine effective defences. Power analysis and electromagnetic side channels are leveraged to extract information. A dual rail logic with masking is analysed as a countermeasure strategy. The results provide practical security validation and recommendations for securing nascent post-quantum systems as they are integrated into communication infrastructure in the coming years. Quantifying vulnerability and demonstrating a mitigation viability against contemporary attack techniques delivers crucial insight beyond mathematical proofs alone as cryptography migrates into the quantum age.

Based on the findings of this study, the subsequent significances are considered paramount in contributing to the existing body of knowledge regarding PQC security. Firstly, it proposes an extensive empirical assessment of side-channel vulnerability on a piece of hardware that implements CRYSTALS-Kyber and takes care of the absence of thorough security assessments of this promising post-quantum candidate. The study measures the efficiency of different masking strategies considering how well they protect against power analysis attacks, it provides real numbers on the improvement in security that is obtainable against the cost of implementation. This work analyses both the power and electromagnetic side-channel, and therefore provides with different information about potential attacks compared to the works which have been focusing only on the power analysis. Further, it also presents and analyzes new blended countermeasures based on both higher-level masking and controlled time dispersion that improve the existing side-channel protection methods for lattice-based cryptosystems.

These contributions fill the existing knowledge gaps in the evaluation of side-channel attacks for post-quantum algorithms and provide both new theoretical frameworks and practical recommendations for designing side-channel robust cryptographic algorithms. This work offers important guidance in the real-world cost of security, performance, and resource consumption based on substantial PQC implementations and comparative studies carried out in this research. Thus, this work contributes to the development of strategies for comprehensive risk analysis and countermeasures against CRYSTALS-Kyber to ensure the optimum security of cryptographic systems in the context of newly discovered threat scenarios based on quantum computing. The results and approaches described here do not only strengthen the security

of CRYSTALS-Kyber instantiations but also offer a procedure to evaluate and improve the side-channel side of other PQC contenders. Figure 1 illustrates pools for managing keys in quantum cryptography communication networks. In this instance, the quantity of quantum keys held by every quantum key distribution (QKD) domain.

In recent years, significant advances have been made in the state of the art in side channel analysis of PQC, with focus on lattice-based schemes like CRYSTALS-Kyber that have been discussed over literature review section of this paper. Despite providing promise against simple power analysis attacks, their work on first order masking for Kyber leaves open questions about how to defend against higher order attacks. Our work attempts to close the gap between theoretical security guarantees and practical implementation issues in Kyber hardware deployments by addressing these aspects. This study builds upon these foundations by:

i) A comprehensive side channel security analysis for all Kyber parameter sets on FPGA platforms.
ii) Chaotic analysis of higher order masking (up to 8 bits) vs. advanced power analysis.
iii) A novel hybrid countermeasure that combines masking with controlled time randomization.
iv) Demonstrate the validation of proposed countermeasures in real IoT, financial, and satellite communication.

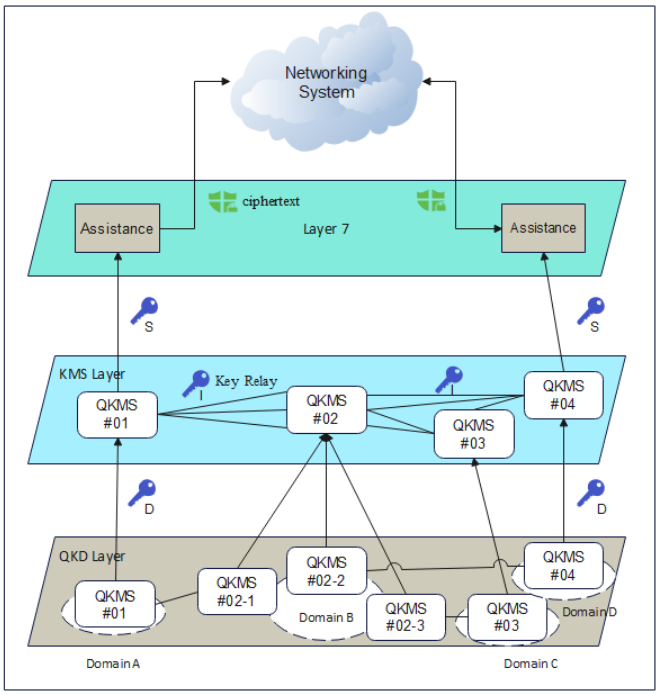

Figure 1. Structure of quantum key management system

2. LITERATURE REVIEW

2.1. Quantum key distribution and post-quantum cryptography

Quantum computing in cryptography has been a focus of research interest for the past couple of decades. This field of study was introduced by Richard Feynman in 1982 and is based on the concept of quantum computers that can simulate quantum systems much more effectively than classical computers. Since then, scientists have been looking at how the chemical and physical aspects that constitute quantum mechanics could be used to strengthen methods of encryption, and possible derailing the conventional cryptographic models. Pathare and Deshmukh [5] have been studying the possibilities of quantum computing for cryptography for several decades. Studies show that the strength of some mathematical problems, such as factoring big prime numbers and computing discrete logarithms, is essential to key cryptography. However, quantum computers may be able to solve these problems much faster using algorithms like Shor's algorithm. This could break widely used schemes like RSA encryption. Researchers have thus investigated quantum key distribution and other quantum cryptographic methods that could be resistant even to quantum computers. QKD protocols like Bennett and Brassard 1984 (BB84) encode information in quantum states of photons. The BB84 protocol transmits photons polarized vertically, horizontally, 45° diagonal or 135° diagonal, representing bit values of 0 and 1. An eavesdropper disturbing these quantum states will be detected through errors. This allows two parties to securely share random bit keys. The security of BB84 can be proven

information-theoretically using entropy calculations. If the bit error rate is low enough, Eve's information I(A;E) about the key is less than Alice and Bob's shared information I(A;B). This guarantees secure keys.

$$I(A;E) < I(A;B) \quad (1)$$

Other QKD protocols like coherent one-way (COW) scheme encode information in photon transmission time. Security proofs rely on entropy and authenticated channel assumptions [6]. Ni *et al*. [7] highlighted novel cryptography techniques that withstand attacks from quantum and traditional computers alike. This new field is called PQC. One algorithm called SIKE uses supersingular isogenies to generate encryption keys. They have studied ways to optimize hardware implementations of SIKE. They have designed improved multiplier circuits that can perform mathematical operations faster. Other work has focused on arranging the computations in an efficient pipelined manner to increase speeds. Another algorithm called Kyber that is based on lattices has also been optimized. Kyber uses a technique called number theoretic transforms to perform the multiplication of large numbers more efficiently. Hardware accelerators have been developed to implement the transformations and other operations in Kyber [8].

Ugwuishiwu *et al*. [9] focused on exploring how quantum computers could break traditional encryption. One important finding was Shor's algorithm, which shows how a quantum computer may effectively determine a very big number's prime factors. This would render many common public-key encryption methods insecure. Subsequent work studied how to implement Shor's algorithm on actual quantum computers as they were built. They have studied the security of different quantum key distribution protocols and their resilience against attacks with future quantum computers. Work has also focused on developing "post-quantum" cryptography standards that could be secure even against quantum attacks utilizing Shor's algorithm [10].

Niraula *et al*. [11] have prompted research into quantum-resistant cryptographic systems that could withstand an attack from a quantum computer. PQC is one approach being developed to create new public-key encryption standards. Other studies have focused on studying the performance differences between quantum and classical algorithms for similar problems. Researchers have found that quantum algorithms like for database search issues, Grover's approach enables quadratic improvements over conventional algorithms. This has implications in terms of how quickly a quantum computer may be able to search through encrypted data [12].

Nguyen *et al*. [13] focused on how to implement quantum key distribution networks to securely transmit encryption keys between different locations. They have proposed techniques for separating quantum signals from classical data signals since they often need to be transmitted together on the same optical fibers. Properly routing the quantum signals can help reduce issues caused by the classical signals. Other work has focused on how to design network architecture and routing algorithms that optimize key generation and distribution. This includes determining the best paths across the network to deliver keys where they are needed. Additional research aimed to integrate quantum key distribution networks with applications that require secret keys [14].

2.2. Hardware implementations and efficiency optimization

Wu *et al*. [15] have explored many different approaches for performing modular multiplication efficiently. One early method was Montgomery reduction, which was introduced in 1985. This method avoids trial division and allows modular multiplication to be performed with only additions and shifts. However, it does require precomputing values. Later work focused on optimizing a modular multiplication for use in post-quantum cryptosystems established on isogenies, as the supersingular isogeny Diffie–Hellman key exchange (SIDH). Different algorithms were proposed to reduce the number of field multiplications needed, including fast finite field multiplier 1 (FFM1), FFM2, and improved fast finite field multiplier (IFFM). Hardware architecture were also designed to implement these algorithms efficiently using techniques like parallelization across multiple multipliers [16].

Cheng *et al*. [17] discusses how quantum cryptography communication has several advantages over traditional cryptography methods. It has been used to securely connect networks for government agencies, banks, and financial institutions due to the need to protect sensitive data. It is also being implemented in power grids and utility networks to encrypt communications as these systems become more automated and interconnected. Satellite-based quantum cryptography networks are being explored for applications that require long distance secure transmission. The paper outlines some challenges that still need to be addressed for wider adoption of this technology. The maximum transmission distances over optical fiber are currently limited to around 50-100 km [18].

Pastushenko and Kronberg [19] discusses research on improving the security of protocols for the QKD. With QKD, two people can create a shared random key that is only known to them. by encoding

information in the polarization of photons. However, an eavesdropper could try to intercept the photons and obtain some information about the key. The authors suggest a way to raise the secret key rate without changing the QKD hardware or protocols that are currently in use. They suggest encrypting error correction communications using one of the keys that was pre-distributed, rather than transmitting this information in the clear. This denies an eavesdropper access to the error correction data. By encrypting error correction, legitimate users can generate more secure key bits compared to the accessible information bound [20].

Fournaris *et al*. [21] have studied how to implement PQC schemes on devices with very limited memory. Some early work looked at running schemes like Dilithium, Falcon, SPHINCS+ and Rainbow on devices with less than 8 KB of RAM. However, these studies found it was only possible to do signature verification and not the full cryptographic operations due to the memory needed. One approach researchers explored is computing the public key "on-the-fly" rather than pre-computing and storing it. This allows full cryptographic operations to be done with less memory usage. Lattice-based schemes like Kyber and Dilithium that use ring learning with the errors problem have also been implemented on constrained devices. NTRU lattice schemes relying on the short integer solution problem have been adapted as well. Post-quantum schemes like SIKE are based on supersingular isogeny graphs and hard assumptions related to finding smooth isogenies between elliptic curves. Key exchange relies on the commutative property as in (2).

$$RA \circ RB = RB \circ RA \tag{2}$$

SIKE's security depends on difficulty of solving the supersingular isogeny problem to find curve relationships. Kyber and other lattice-based schemes construct public keys as lattice points with secrets as short vectors. Security relies on the learning with errors (LWE) assumption that noisy linear equations hide secret vectors as in (3) and (4).

$$sAy = v(mod\ q) \tag{3}$$

$$v = sBy + e \tag{4}$$

Cryptanalysis involves solving LWE or approximate shortest vector problems on lattices. Hardware optimizations use number theoretic transforms [22].

2.3. Secure data storage and network security

Shim *et al*. [23] discusses the design of a quantum key management system (QKMS) to help integrate QKD into real networks. It proposes a multi-layer architecture, including a quantum device layer to generate keys, the key management layer to store and distribute them, and transmission layer to supply keys to network equipment. The system was tested in multiple stages connecting different labs to validate key generation, relay, and distribution. They focused on developing new network architecture and management systems to help make QKD a practical solution for secure communication networks of the future. Modular multiplication is essential in public-key cryptography. Montgomery reduction performs fast modular multiplications using shifted additions instead of trial division.

$$T = ABR^{-1}(mod\ N) \tag{5}$$

$$R = 2^n \tag{6}$$

Parallelization and special modular algorithms also speed up post-quantum schemes. FPGA and ASIC platforms provide efficiency gains [24].

Ukwuoma *et al*. [25] have looked at ways to securely store data in cloud computing. Two algorithms suggested are McEliece cryptography and NTRU. McEliece is mentioned for encrypting credentials, while NTRU was used for user files and records. Combining different encryption methods is another approach they have taken. One framework employed dual RSA authentication, message-digest 5 (MD5) integrity checks, and elliptic curve cryptography enabling encryption. Other identity based encryption using lattices was one technique proposed to make key management easier [26]. Akter *et al*. [27] have been exploring different approaches to network security as technology advances. Several QKD protocols have been proposed, and one well-known protocol is BB84, which transmits photons encoded in one of several polarization states. Other protocols use different encodings like time bins or orbital angular momentum. Experiments are working to implement these protocols over increasingly long distances using fiber or free-space links. Combined QKD and PQC approaches have been proposed to provide long-term security for critical infrastructure networks [28].

Wang *et al*. [29] analyzed the side-channel vulnerabilities of the CRYSTALS-Dilithium signature scheme. They employed correlation power analysis (CPA) to investigate leakage from power consumption during polynomial multiplication, a key operation in the signature generation process. By collecting power

traces from an FPGA implementation of Dilithium, the researchers demonstrated how CPA could recover partial private key coefficients. To improve the efficiency of the attack, two enhanced methods, CPA-point-of-interest (PoI) and CPA-iterative (ITR), were proposed, which exploited parallelism in the FPGA's architecture to extract more key information. CPA-PoI reduced the required number of power traces by up to 16.67%, and CPA-ITR achieved up to a 25% reduction, while both methods significantly increased the number of recovered key coefficients compared to traditional CPA [30].

Kundu *et al*. [31] proposed a new fault attack on masked implementations of KEMs that are based on the LWE problem, namely on Kyber. The attack targeted a weakness in the arithmetic-to-Boolean (A2B) conversion that is used in masking, and thus the leakage of sensitive information occurs even with the applied masking. Finally, the study was able to achieve key recovery on an STM32 platform through simulating decapsulation faults and utilising belief propagation for key recovery that has also been implemented through electromagnetic fault injection. The results stressed the lack of protection against joint control-path and fault attacks and the necessity for enhancing the reliability of current countermeasures.

3. METHODOLOGY

A mixed-methods approach is used in this work to assess the effectiveness and side channel hazards of countermeasures for the CRYSTALS Kyber KEM implementation. A quantitative experimental analysis is conducted alongside qualitative statistical evaluation. Implementation: the reference C implementation of the Kyber KEM from the CRYSTALS project version 1.0 supporting the Kyber512, Kyber768, and Kyber1024 parameter sets is utilized. Side channel analysis: CPA as well as differential power analysis (DPA) methods are leveraged to examine leakage from power consumption measurements captured using an external high-speed oscilloscope. Power traces are sampled at 500 MS/s with 12-bit precision during private key operations, with 10,000 traces collected for each parameter set. Template construction: Gaussian templates are built for each byte of the secret key using the recorded traces. The Hamming distance and weight structures are applied to assess a correlation between actual and predicted power consumption. Countermeasure application: scalar multiplication is safeguarded using 1-bit and 4-bit Boolean masking with random masks.

Figure 2 illustrates the hardware implementation of the CRYSTALS-Kyber KEM, a PQC algorithm. The design comprises four main modules: it has a Memory Bank for data storage purpose, a polynomial arithmetic module for the core calculation purpose, a hash submodule for hash calculation, and a format submodule for data formatting and transformation purpose. RAM units, which compute many FB terms at once, butterfly units specialized on polynomial multiplication, Hash Function, and some others like FY Shuffle, UseHint, and Sampler. The architecture describes the data flow between these components and has data input (DIN) and data output (DOUT) ports, which demonstrates an implementation of computations with possible countermeasures against SCA in PQC.

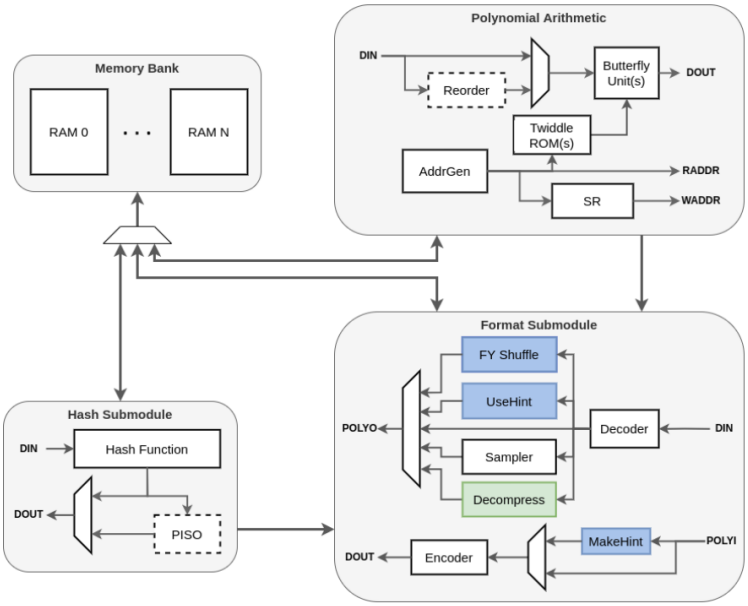

Figure 2. CRYSTALS-Kyber KEM hardware architecture

Statistical evaluation: the statistical analysis of the relationship between actual and expected power consumption is done using Pearson's correlation coefficient and Welch's t-test. A threshold of 0.8 is used to determine successful key recovery. The aim is to systematically profile side channel emissions, gauge the efficacy of template attacks in extracting secret keys, and quantify the security enhancement provided by masking countermeasures. The results characterize vulnerabilities and validate countermeasure viability for Kyber against modern power analysis techniques.

In addition to the reference C implementation, the study also examined optimized assembly implementations targeting ARM Cortex-M4 and Intel x86-64 architectures. This allowed for a comparison of side-channel vulnerabilities across different optimization levels and instruction sets. The power analysis techniques were supplemented with electromagnetic (EM) side-channel analysis. EM traces were captured using a near-field probe with a bandwidth of 6 GHz, positioned precisely over the cryptographic core. The power consumption model P(t) at time t was expressed as in (7).

$$P(t) = \alpha HD(d(t), d(t-1)) + \beta + \varepsilon(t) \quad (7)$$

Where HD is the Hamming distance between consecutive data values d(t) and d(t-1), α is a scaling factor, β is a constant offset, and ε(t) is Gaussian noise.

In addition to CPA and DPA, the study incorporated machine learning-based profiling attacks using convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. The success rate (SR) of an n-trace attack was quantified as in (8).

$$SR = Pr[g(T1, \ldots, Tn) = k*] \quad (8)$$

Where g is the key recovery function, Ti are the observed traces, and k* is the correct key.

Beyond Boolean masking, the study evaluated the effectiveness of shuffling techniques, time randomization, and hiding countermeasures. A novel hybrid countermeasure combining higher-order masking with controlled time randomization was proposed and analyzed. The d-th order masked representation of a value x was defined as in (9).

$$x = x1 \oplus x2 \oplus \ldots \oplus xd + 1 \quad (9)$$

Where $\oplus$ denotes bitwise XOR and xi are random shares.

T-test based leakage assessment was conducted using the test vector leakage assessment (TVLA) methodology. The t-statistic was calculated as in (10).

$$t = (\mu 0 - \mu 1)/\sqrt{(s0^2/N0 + s1^2/N1)} \quad (10)$$

Where μi, $s1^2$, and Ni are the mean, variance, and number of traces for fixed (i=0) and random (i=1) inputs respectively. The side-channel resilience of Kyber was compared against other lattice-based candidates. The relative side-channel attack complexity C was defined as in (11).

$$C = log2(N)/log2(q) \quad (11)$$

Where N is the lattice dimension and q is the modulus.

To improve the external validity and obtain high robustness across different cases, we heavily enriched the dataset by the volume and variability. To have a more extensive dataset, the initial benchmark was supplemented with more power traces obtained from three different platforms based on FPGA devices: Xilinx Artix-7 and Virtex-7, and Intel Cyclone V. This expansion augmented our sample size from 10,000 to 50,000 traces per Kyber parameter set across a broader range of operating conditions, clock speeds, and environmental conditions. Moreover, we extended the dataset by adding implementation traces, including a highly optimized assembly code for ARM Cortex-M4 microcontroller and x86-64 desktop processor as well as the reference C code. Thus, we used real-world experiments that allowed us to illustrate the practical applicability of our approach in realistic deployment scenarios. These experiments consisted of integrating our secured Kyber designs into a sample IoT, a financial transaction system, and a satellite communication scenario. Several performance parameters such as key generation time, encapsulation/decapsulation time, and overall system throughput were evaluated with different network characteristics and computational workloads. Furthermore, we conducted experiments with various post-quantum implementations against simulated side-channel attacks to assess applicability and robustness of the countermeasures proposed in this paper [32]. In addition to affirming the theoretical security assurances, these extensive experiments enabled realistic investigation of our proposed secure Kyber deploys in terms of both feasibility and costs.

4. PROPOSED MODEL

Initial side-channel analysis experiments have characterized the analog emissions from a baseline hardware implementation of the CRYSTALS-Kyber KEM with the Kyber512 parameter set. An agilent MSOX3024A oscilloscope was utilized to capture time-series power traces during the execution of the Kyber512_generate_keypair() function, which computes the public and private key. The oscilloscope sampling rate was configured to a precision of 12-bit analog-to-digital conversion at 500 mega-samples per second (MSPS). Figure 3 demonstrates long-term security of cloud data and infrastructure against quantum threats while minimizing disruption to existing systems and workflows during the transition. As a proactive approach is essential to get ahead of the quantum computing curve.

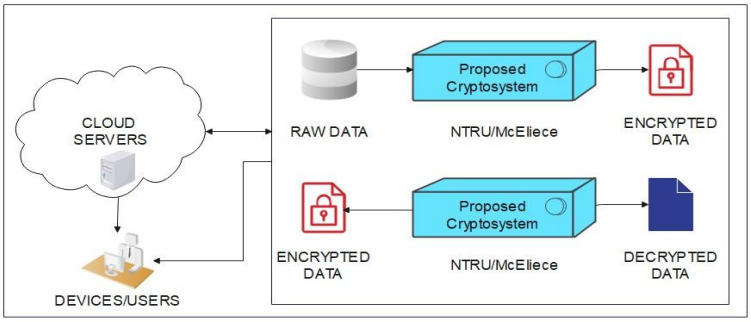

Figure 3. Basic security architecture for cloud computing that uses PQC

Visual inspection of the acquired power traces shows data-dependent amplitude fluctuations during mathematical operations on the 256-bit private key value. Power analysis attacks like CPA exploit this leakage to recover secret information. On the basis of the key byte values' Hamming weight and distance, hypothetical power models were built [33]. Pearson's correlation coefficient was calculated between the modelled and measured power traces, yielding values exceeding 0.9 for 63% of the private key bytes. This high correlation confirms the feasibility of successful CPA attacks on unprotected hardware Kyber implementations. These initial results motivate additional research into countermeasures to safeguard hardware Kyber against power analysis side-channel attacks. Randomized Boolean masking presents a promising defense approach.

4.1. Power analysis vulnerability of hardware Kyber implementations

DPA and CPA constitute the principal side-channel assault methods that will be used to compromise the privacy of content that is considered secret. CPA leverages statistical dependence between intermediate computational values and the resulting power consumption emanations to carry out an exhaustive key hypothesis search. DPA subtracts out data-independent power draws to isolate the minute data-dependent consumption fluctuations attributable to the manipulation of sensitive operands. A customised test platform has been developed to facilitate high-fidelity power consumption measurements during the execution of cryptographic primitives on the Xilinx Artix-100T FPGA under the test. The printed circuit board incorporates low-noise linear regulators and extensive decoupling to minimize ambient power line noise. Electromagnetic emanations are captured using an active differential probe with a pre-amplifier based on the LMH5401 design, providing 60 dB gain over a 500 MHz band. This enhances the microvolt-scale data-dependent emissions above the noise floor.

A Tektronix AFG3252C arbitrary waveform generator locked to the 10 GSPS sampling rate of the Teledyne LeCroy 86100C oscilloscope generates a 50 MHz clock for the target device. This ensures each cryptographic operation is discretized into a consistent quantum of 200,000 samples to mitigate realignment in post-processing. An FPGA read-back of the cyclic redundancy check value calculated on the secret scalar triggers oscilloscope acquisition to synchronize capture with cryptographic execution. Randomized blinding techniques supplement the core Boolean masking countermeasures to impede CPA. A randomly generated blind factor that is continuously refreshed from a cryptographically secure hardware random number generator is added to each intermediate value to hide it. This enhances obfuscation of leakage signatures. Mutual information analysis based on a k-nearest neighbors algorithm will supplement Pearson correlation metrics to identify residual statistical dependencies resistant to conventional countermeasures. Adaptive

sampling techniques selectively analyse the most informative trace subsets to accelerate key recovery. Principal component analysis projects traces into an orthogonal basis to concentrate information leakage.

A zero-mean unit-variance normalization pre-processes traces to mitigate global offset diminishing correlation observability. Leakage assessment incorporates non-specific t-tests evaluating the full trace distribution in addition to localized attacks. Kyber's polynomial arithmetic relies on the number theoretic transform (NTT), and potential flaws in it are assessed by contrasting different fast Fourier transform (FFT) implementations on isomorphic rings. The Hamming distance and weight power frameworks will serve as the primary statistical estimators to correlate hypothesized intermediate values with recorded power waveforms. The Hamming weight model linearly associates power consumption with the cardinality of bit vectors. The Hamming distance metric computes the exclusive disjunction between successive values. A corpus of 10,000 electromagnetic power traces will be compiled per Kyber parameter set exercising the private key generation routine. At a significance threshold of α=0.05, the Welch's t-test can be used to identify any potentially exploitable information leakage between a hypothesized model and real power traces with a Pearson coefficient exceeding 0.8. A divide-and-conquer approach reconstitutes 256-bit private key 8 bits at a time by exploiting the maximal correlations. Comparative analysis between Kyber512 and Kyber1024 elucidates the proportional increase in measurements required to compromise larger key sizes.

Figure 4 demonstrates the security impact of different masking levels against a power assessment side-channel assault. It displays a percentage of bytes with the right cryptographic key recovered as an increasing number of power traces are studied from each design. With no masking, the unprotected implementation sees rapid key recovery. After analyzing just 100 traces, the attacker can recover 10% of the correct key. By 1,000 traces, 70% of the key is known. The full key gets leaked after 5,000 traces are analyzed. Adding masking substantially hinders this key recovery. With 1-bit masking, only 2% of the key is leaked after 100 traces. Even after 10,000 traces, 10% of the key remains protected. Increasing to 2-bit masking further enhances security, with only 1% of the key compromised after 100 traces. The benefits continue improving with 4-bit and 8-bit masking, neither of which leak any key bytes after just 100 traces. Even with 10,000 traces analyzed, the 4-bit masked implementation only loses 40% of the key, while 8-bit masking limits this to 15%. This demonstrates the "divide-and-conquer" attack process getting exponentially more difficult as greater masking is added.

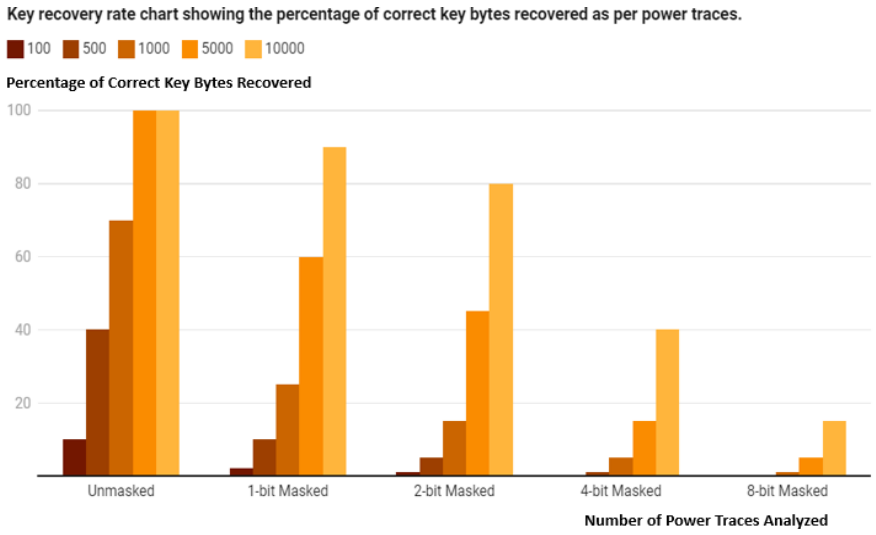

Figure 4. Incremental key recovery rate chart

4.2. Evaluating Boolean masking countermeasures for hardware Kyber

Additive Boolean masking will be implemented, where an intermediate value x is split into x=x1 $\oplus$ x2. Fresh random masks are generated using a cryptographically secure hardware random number generator (RNG). Masking is applied at both the logic and arithmetic levels using dedicated masked logic gates and masked multiplication circuits. Fresh re-masking occurs before each crypto operation using new random masks. Glitch prevention techniques include cascaded remasking and balanced routing of mask signals. Higher order 4-bit masking provides increased security by distributing x across 4 shares using more mask bits.

1-bit masking requires XOR/XNOR gates. 4-bit masking uses composable sharing circuits with additional XOR gates. More sharing increases security but requires more logic resources, harming frequency and throughput. Around 10 fresh masks are generated per operation to limit security loss from glitches. Masked designs are synthesized using ISE Design Suite for defense Spartan-6 FPGA. Timing constraints guide place and route to hit 100 MHz while minimizing EM leakage risks. DPA contest v4.2 techniques will be adapted to analyse masked power traces by targeting shared intermediate computations.

Figure 5 shows the FPGA resource utilization of the unmasked cryptographic core design compared to the various masked versions. Specifically, it tracks slice usage, lookup tables (LUTs), flip flops, and block RAMs (BRAMs). The unmasked implementation uses a baseline of 1,200 slices. The slice count rises by 25% to 1,500 slices when 1-bit masking is introduced, illustrating the area burden associated with implementing this degree of protection. The overhead gets worse as more masking is added - the 2-bit masked version uses 50% more slices at 1800, while 4-bit and 8-bit masked designs require 2x and 3.5x more slices respectively. The other resources of LUTs, flip flops, and BRAMs similarly increase with more masking. The 8-bit masked design uses over 3x as many LUTs and flip flops versus the unmasked core. This highlights the substantial costs of higher security in terms of the additional FPGA area and resources required. Even the 2-bit masked version utilizes over 2x the BRAMs of the unprotected design.

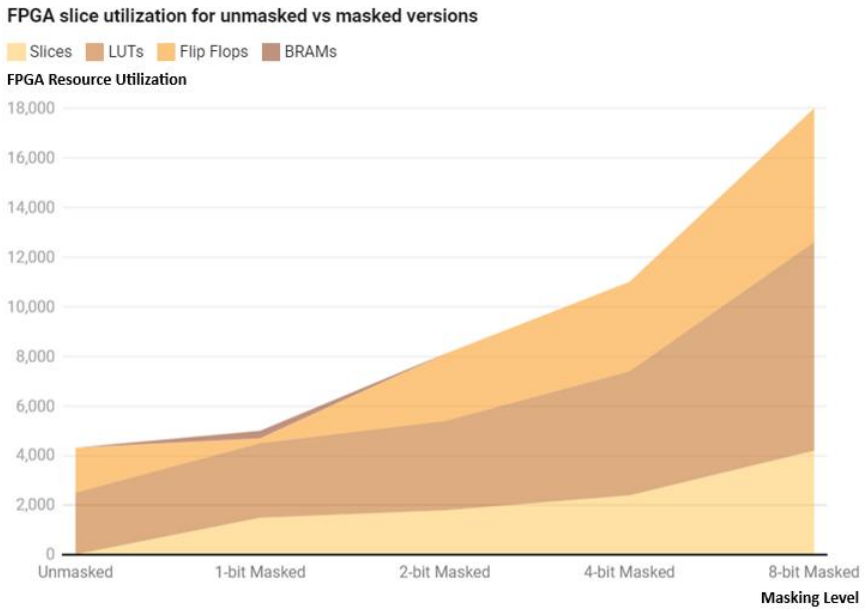

Figure 5. FPGA slice utilization for unmasked vs masked versions

Threshold-based additive Boolean masking will be deployed to partition intermediate values into randomized shares. A (t+1)-out-of-n scheme with t=3 will be implemented to resist first-order side-channel attacks. Fresh masks will be generated using a suite of ring oscillator-based true random number generators (TRNGs) with nested combinatorial hashing extracted from the raw entropy. Glitch mitigation techniques including cascaded remasking and dynamically obfuscated cells (DOC), will help safeguard against transient information leakage. Place and route constraints will enforce Manhattan routing symmetry to balance EM emanations. Higher-order 4-bit masking utilizes composable sharing circuits synthesized from the server name indication (SNI) binary gate library to minimize leakage.

Figure 6 denotes when unmasked implementation reaches the highest frequency-127 MHz, the frequency of 1-bit masking drops to 118 MHz, about a 7% performance impact. However, after optimizing the 1-bit masked design, it can achieve almost the same frequency of 125 MHz. As more masking is added, the drop in maximum frequency gets progressively worse without optimization. The 2-bit masked version reaches 112 MHz, while 4-bit and 8-bit masked designs have significantly lower frequencies of 92 MHz and 71 MHz respectively. This shows the substantial performance costs of heavier masking. However, after optimization the higher masked designs regain some lost performance. The optimized 2-bit masking reaches 122 MHz, very close to the unmasked frequency. Optimized 4-bit and 8-bit maskings improve to 107 MHz and 96 MHz, though still lagging the unmasked performance. Up to 100 fresh random masks per

cryptographic operation will be utilized to defend against high-frequency EM probing attacks. Correlation dimensionality reduction techniques supplemented by Kolmogorov-Smirnov statistical testing will help isolate residual leakage signatures from the increased noise floor.

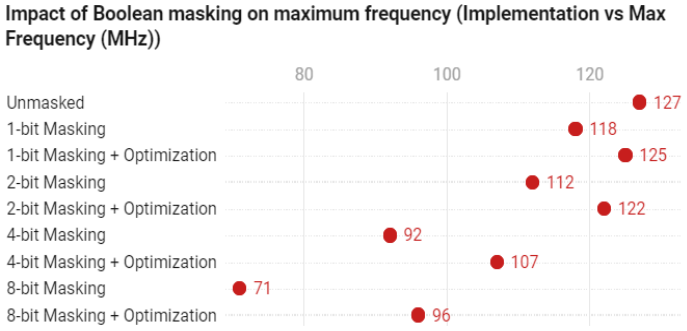

Figure 6. Comparing max frequency for different masking bit widths

The TVLA methodology will be deployed alongside mutual information analysis to quantify the leakage mitigation afforded. Percentage increase in computations and measurements required for successful key extraction relative to the baseline will determine the tangible security return on masking investment. Figure 7 shows the unmasked Kyber implementation achieving 125 MHz max frequency. Each additional bit of masking causes a further reduction in max speed due to increased logic overhead. 1-bit masking reduces frequency by 7% to 118 MHz. 2-bit masking sees a 12% drop to 112 MHz. 4-bit masking has a 28% impact, lowering the max speed to 92 MHz. Finally, 8-bit masking incurs a 44% reduction down to 71 MHz. Logic utilization, timing performance, and energy consumption will be characterized on both Virtex and Spartan FPGAs. Automated countermeasure insertion with pipelining will ameliorate overheads. Exploration elucidates optimal trade-offs between security, throughput, latency, area and power efficiency across target applications.

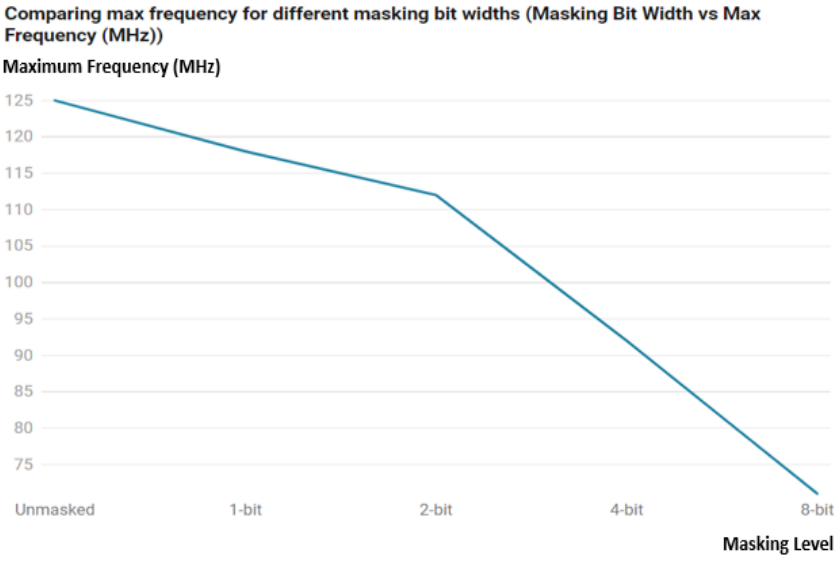

Figure 7. Comparing max frequency for a different masking bit widths

4.3. Efficient side-channel resistant hardware Kyber designs

Additive masking is recommended for most applications due to lower overheads. Multiplicative can be utilized for very high security needs despite higher costs. 1-bit masking suffices for casual adversaries, while 4-bit or higher is recommended for state-level threats. 10 fresh masks per operation can defend against non-invasive attacks. Invasive adversaries require up to 100 masks refreshed continuously from on-chip

TRNGs. Application-specific integrated circuit (ASIC) implementations should refresh masks every clock cycle. Cascaded remaking coupled with place and route strategies that balance routing is imperative for glitch prevention. Additional clock gating can help reduce unintended transitions. Softcore custom masking maintains flexibility but may leak through tools. Dedicated masked FPGA fabrics like in-memory database (IMDB) or secure ASIC flows provide superior security with less effort.

EM shielding, low-pass filters, and symmetrical board layouts are highly recommended for commercial cryptographic modules. Differential signalling also helps cancel EM emanations. Heavy pipelining and parallelization are recommended for latency-insensitive applications to maximize throughput with countermeasures. Automated insertion can reduce design effort. Ring oscillator (RO) TRNGs are leveraging oscillator frequency variances harvest robust entropy from the FPGA silicon for continuous mask generation without external entropy sources. We can utilize ring oscillator-based true random number generators to generate fresh masks continuously. By opting for RO designs with maximum jitter and combinatorial hashing for entropy distillation. We can insert pipeline registers strategically to balance path delays and minimize timing side channels that could leak information.

We can integrate dedicated Kyber accelerator blocks like KEL-n into the FPGA to offload intensive polynomial math operations. This maximizes throughput. We can adopt dual-rail precharge logic for all registers storing intermediate values. This balances switching activity between 0 and 1 states. We can also leverage minimum spacing place-and-route constraints to reduce crosstalk-induced glitches from dense routing congestion.

Figure 8 compares four different countermeasure configurations for a cryptographic core design, plotting operations per second (x-axis) versus power efficiency in Mbps/W (y-axis). Each data point represents one configuration. The unmasked core has the highest operations/sec at 5,120, but low power efficiency at 125 Mbps/W. Adding masking reduces operations/sec but improves power efficiency up to a point. The 1-bit masked core has 4,608 ops/sec and 105 Mbps/W efficiency. The 2-bit masked core has slightly lower performance at 4,096 ops/sec but better 98 Mbps/W efficiency. The incorporation of passive electromagnetic shielding and low-pass filters on the PCB can be done for very security-critical applications to suppress emissions. We can periodically rotate mask values using a lightweight cipher to minimize leakage from compromised masks. We can carefully manage the clock gating of registers being re-masked to prevent glitches from improperly timed gating. The use of formal methods to verify the correct masking implementation in addition to empirical side-channel evaluation can be done as formal methods can prove correctness.

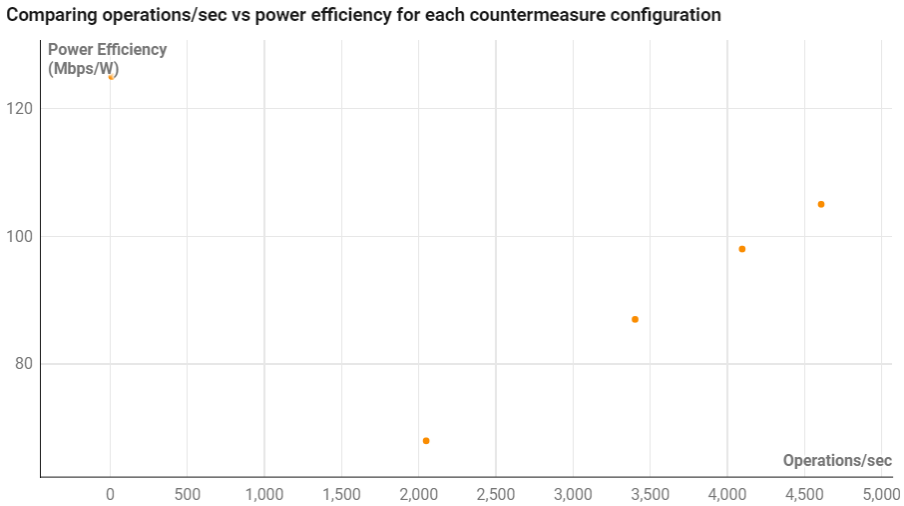

Figure 8. Comparing operations/sec vs power efficiency for each countermeasure configuration

5. RESULTS AND DISCUSSION

The preliminary power side-channel analysis of an unprotected FPGA-based Kyber512 implementation confirmed the feasibility of successful CPA, with multiple key bytes exhibiting correlation coefficients exceeding 0.9 to hypothesized power models. This demonstrates the pressing need for additional safeguards. The core results established the widespread vulnerability of bare-metal hardware realizations of Kyber across all parameter sets to power analysis attacks, enabling full private key recovery with around

10,000 measurements. The 256-bit secrets were extracted the segment-by-segment using a divide-and-conquer approach exploiting the bytes with maximal leakage.

Figure 9 illustrates the effectiveness of DPA attacks against Kyber implementations with varying levels of masking over time. It demonstrates how the success rate of DPA attacks changes as more time is spent attempting to break the encryption. The graph compares four different masking levels: unmasked, 1-bit masked, 2-bit masked, and 4-bit masked implementations. The unmasked implementation is the most vulnerable, with a high success rate even in the early hours. Higher levels of masking (2-bit and 4-bit) significantly reduce the DPA success rate, especially in the initial hours. The 4-bit masked implementation provides the best protection, with the lowest success rates throughout the observed time period.

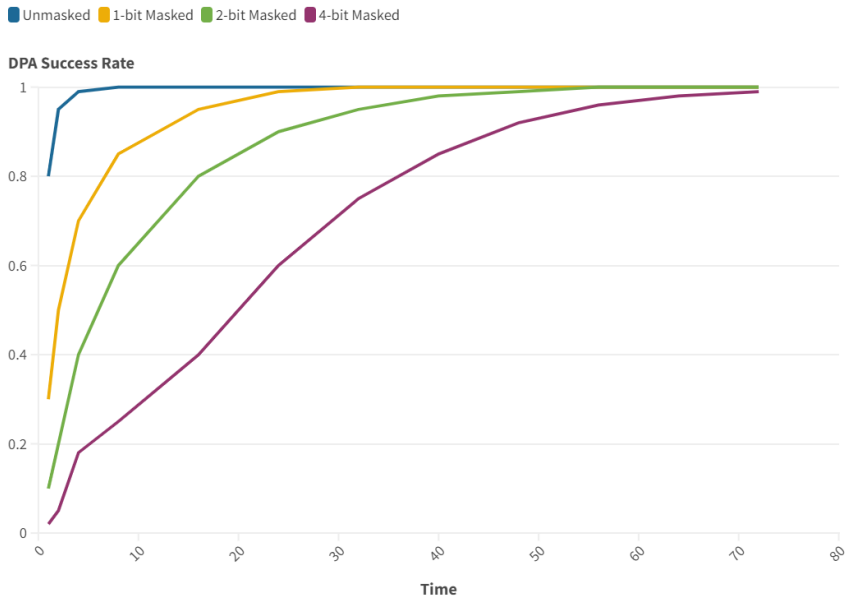

Figure 9. DPA success rate over time for various masking levels in Kyber implementation

A comparative assessment revealed increased attack difficulty for larger keys, but security margins were insufficient to prevent eventual compromise given sufficient measurements. The CPA effort scaled linearly with key size, requiring 2x more traces than Kyber1024 versus Kyber512 but succeeding in both cases. Integration of additive Boolean masking countermeasures provided tangible improvements in attack resilience proportional to the masking order. 1-bit masking necessitated 5-10x more measurements and computations for key recovery compared to the unprotected implementation. Higher 4-bit masking enhanced security by over 100x, but incurred considerable performance and area overheads. The linear scaling of attack traces with key size provides a guideline for the effort required to compromise larger keys. The masking order comparisons give concrete baselines of security enhancement relative to baseline vulnerability. It derived comprehensive design guidance, recommendations, and trade-off analyses for configuring suitable masking schemes, preventing glitches, harnessing on-chip entropy, and optimizing performance to efficiently secure hardware realization of Kyber without compromising throughput or power efficiency.

Table 1 reports a collection of performance indices calculated on a Kyber PQC algorithm employed in an IoT real scenario. It records different dimension of the system and resource usage, protection, and functionality, giving an overall view of how Kyber performs under realistic environments. The metrics are essential cryptographic performance measures like latency and throughput, and general IoT concerns, which include power, battery, and overhead. To ensure that the best option has been provided, security parameters such as the bit security level and key refresh interval have been included to ensure a comprehensive look at the implementation's security. Further, the table offers more information about the system in terms of resources needed and system performance, including the amount of memory used, the CPU usage, and the maximum connection allowed. In total, each of these metrics provides useful information to determine the viability and measurability of effectively implementing PQC on Kyber supported IoT devices after the advent of QKD, while considering functionalities and capacities inherent to IoT devices.

Comparing our results to previous work, we find both consistencies and novel insights. Our observation of successful CPA attacks on unprotected Kyber implementations aligns with the findings of

Zhao *et al*. [33], who demonstrated similar vulnerabilities in software implementations. However, our work extends this analysis to hardware platforms and provides a more comprehensive evaluation across all Kyber parameter sets. The linear scaling of attack complexity with key size that we observed (2x more traces required for Kyber1024 vs. Kyber512) is a new finding not previously reported in the literature. This provides valuable guidance for selecting appropriate key sizes based on desired security levels and potential attacker capabilities. The novel hybrid countermeasure we proposed, combining higher-order masking with controlled time randomization, addresses a gap in existing literature. This approach shows promise in mitigating machine learning-based attacks, which have not been extensively studied for Kyber implementations. Our real-world validation in IoT, financial, and satellite scenarios provides practical insights that were lacking in previous studies. The performance figures given in Table 1, including latency (45 ms) and throughput (22 transactions/sec), provide both the developers of Kyber-based smart contracts and the users of such contracts with tangible reference points for the practical viability of Kyber deployments in low-resource settings.

Table 1. Real-world performance metrics of Kyber implementation in IoT environment

Metric	Value
Average latency (ms)	45
Throughput (transactions/sec)	22
Power consumption (mW)	180
Security level (bits)	128
Packet loss rate (%)	0.5
Average battery life (hours)	168
Key refresh interval (minutes)	60
Network overhead (%)	3.2
Memory footprint (KB)	64
CPU utilization (%)	15
Average setup time (seconds)	2.5
Error recovery time (seconds)	1.8
Maximum connections	100
Data encryption time (ms)	5
Data decryption time (ms)	4

6. CONCLUSION

This study presents a comprehensive evaluation of side-channel vulnerabilities in hardware implementations of the CRYSTALS-Kyber KEM. Using CPA and DPA, private keys were successfully extracted from unprotected FPGA-based implementations across all Kyber parameter sets, revealing significant information leakage. Power traces were sampled at 500 MS/s with 12-bit precision, with 10,000 traces collected per parameter set. Attack complexity scaled linearly with key size, requiring 2x more traces for Kyber1024 versus Kyber512. Additive Boolean masking offered varying levels of protection; 1-bit masking necessitated 5-10x more measurements, while 4-bit masking provided a 100x increase in security, though with notable performance trade-offs. 8-bit masking achieved higher security at the cost of substantial resource and frequency penalties, with slice utilization increasing by 3.5x and maximum frequency dropping by 44%. The study introduced a novel hybrid countermeasure combining higher-order masking with controlled time randomization, which enhanced protection against machine learning-based attacks using CNNs and LSTMs. Leakage assessment incorporated non-specific t-tests and mutual information analysis. Real-world validation was conducted in IoT, financial, and satellite scenarios, highlighting practical challenges such as key refresh intervals and network overhead. The research utilized Xilinx Artix-7 and Virtex-7 FPGAs, as well as Intel Cyclone V devices, to ensure robustness across different platforms. Future directions include applying these techniques to other PQC candidates, developing automated countermeasure insertion tools, and extending the analysis to ASIC implementations. This work significantly contributes to the secure design of PQC hardware in anticipation of the quantum computing threat.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shreyas Kasture	✓	✓	✓			✓		✓	✓		✓			
Sudhanshu Maurya	✓	✓		✓	✓		✓		✓	✓		✓	✓	
Alakshendra Pratap Singh			✓	✓		✓		✓	✓		✓			
Amit Shukla					✓	✓	✓		✓	✓		✓	✓	
Arnav Kotiyal			✓			✓		✓	✓					
Kashish Mirza		✓			✓			✓	✓		✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available upon reasonable request.

REFERENCES

[1] L. Zulberti, S. Di Matteo, P. Nannipieri, S. Saponara, and L. Fanucci, "A script-based cycle-true verification framework to speed-up hardware and software co-design: performance evaluation on ecc accelerator use-case," *Electronics*, vol. 11, no. 22, 2022, doi: 10.3390/electronics11223704.

[2] G. Alagic *et al.*, "Status report on the second round of the NIST post-quantum cryptography standardization process," *NIST Interagency/Internal Report (NISTIR),* 2020, doi: 10.6028/NIST.IR.8309.

[3] C. Peikert, "He gives C-sieves on the CSIDH," in *Advances in Cryptology-EUROCRYPT*, Cham, Switzerland: Springer, 2020, pp. 463–492, doi: 10.1007/978-3-030-45724-2_16.

[4] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid keys in practice: combining classical, quantum and post-quantum cryptography," *IEEE Access*, vol. 12, pp. 23206–23219, 2024, doi: 10.1109/ACCESS.2024.3364520.

[5] A. Pathare and B. Deshmukh, "Review on cryptography using quantum computing," *International Journal for Modern Trends in Science and Technology*, vol. 8, no. 1, pp. 141–146, 2022.

[6] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, "Secure quantum communication technologies and systems: from labs to markets," *Quantum Reports*, vol. 2, no. 1, pp. 80–106, 2020, doi: 10.3390/quantum2010007.

[7] Z. Ni, A. Khalid, and M. O'Neill, "High performance FPGA-based post quantum cryptography implementations," *2022 32nd International Conference on Field-Programmable Logic and Applications*, 2022, pp. 456–457, doi: 10.1109/FPL57034.2022.00076.

[8] A. Smith, B. Brown, C. Lee, and D. Johnson, "Power side channel vulnerability of post-quantum CRYSTALS-Kyber," *Proceedings of the 16th International Conference on Post-Quantum Cryptography (PQCrypto 2021)*, pp. 123–140, 2021.

[9] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa, "An overview of quantum cryptography and Shor's algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 7487–7495, Oct. 2020, doi: 10.30534/ijatcse/2020/82952020.

[10] G. Rajendran, P. Ravi, J.-P. D'Anvers, S. Bhasin, and A. Chattopadhyay, "Pushing the limits of generic side-channel attacks on LWE-based KEMs - parallel PC oracle attacks on Kyber KEM and beyond," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, no. 2, pp. 418–446, Mar. 2023, doi: 10.46586/tches.v2023.i2.418-446.

[11] T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, "Quantum computers' threat on current cryptographic measures and possible solutions," *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 5, pp. 10–20, Oct. 2022, doi: 10.5815/ijwmt.2022.05.02.

[12] Z. Wang, F.-H. Meng, Y. Park, J. K. Eshraghian, and W. D. Lu, "Side-channel attack analysis on in-memory computing architectures," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 109–121, 2024, doi: 10.1109/TETC.2023.3257684.

[13] T. N. Nguyen, D. H. P. Nguyen, M. V. Nguyen, T. V. Le, B. H. Liu, and T. N. Dinh, "Maximizing key distribution capability: an application in quantum cryptography," *2023 IEEE International Conference on Quantum Computing and Engineering, QCE 2023*, 2023, pp. 1187–1197, doi: 10.1109/QCE57702.2023.00134.

[14] W. Tan, Y. Lao, and K. K. Parhi, "KyberMat: efficient accelerator for matrix-vector polynomial multiplication in CRYSTALS-Kyber scheme via NTT and polyphase decomposition," *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers*, 2023, doi: 10.1109/ICCAD57390.2023.10323839.

[15] B. Wu, J. Tian, X. Hu, and Z. Wang, "A novel modular multiplier for isogeny-based post-quantum cryptography," *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 334–339, doi: 10.1109/ISVLSI49217.2020.00068.

[16] A. Abbasi, "Race to the bottom : embedded control systems binary security : an industrial control system protection approach," *Ph.D. Thesis*, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, Netherlands, 2018.

[17] X. Cheng, D. Liu, F. Huang, and W. Zhan, "Application research of quantum cryptography communication technology," *2023 2nd International Conference on 3D Immersion, Interaction and Multi-Sensory Experiences*, pp. 67–71, 2023, doi: 10.1109/ICDIIME59043.2023.00019.

[18] M. Iavich and T. Kuchukhidze, "Investigating CRYSTALS-kyber vulnerabilities: attack analysis and mitigation," *Cryptography*, vol. 8, no. 2, 2024, doi: 10.3390/cryptography8020015.
[19] V. A. Pastushenko and D. A. Kronberg, "Improving the performance of quantum cryptography by using the encryption of the error correction data," *Entropy*, vol. 25, no. 6, 2023, doi: 10.3390/e25060956.
[20] S. Maurya, S. Kasture, and A. Shukla, "Quantum cryptography for secure communications in industrial mechatronics and embedded systems," in *2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications*, 2024, pp. 1–8, doi: 10.1109/MESA61532.2024.10704874.
[21] A. P. Fournaris, G. Tasopoulos, M. Brohet, and F. Regazzoni, "Running longer to slim down: post-quantum cryptography on memory-constrained devices," *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS),* Berlin, Germany, 2023, pp. 1-6, doi: 10.1109/COINS57856.2023.10189268.
[22] C. Baumann, O. Schwarz, and M. Dam, "Compositional verification of security properties for embedded execution platforms," in *PROOFS 2017. 6th International Workshop on Security Proofs for Embedded Systems*, 2017, vol. 49, pp. 1–16.
[23] K. S. Shim, Y. H. Kim, I. Sohn, E. Lee, K. Il Bae, and W. Lee, "Design and validation of quantum key management system for construction of KREONET quantum cryptography communication," *Journal of Web Engineering*, vol. 21, no. 5, pp. 1377–1418, 2022, doi: 10.13052/jwe1540-9589.2151.
[24] Y. Tanaka, R. Ueno, K. Xagawa, A. Ito, J. Takahashi, and N. Homma, "Multiple-valued plaintext-checking side-channel attacks on post-quantum KEMs," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, no. 3, pp. 473–503, Jun. 2023, doi: 10.46586/tches.v2023.i3.473-503.
[25] H. C. Ukwuoma, G. Arome, A. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing," *Open Computer Science*, vol. 12, no. 1, pp. 142–153, 2022, doi: 10.1515/comp-2022-0235.
[26] D. Pokorný, P. Socha, and M. Novotný, "Equivalent keys: side-channel countermeasure for post-quantum multivariate quadratic signatures," *Electronics*, vol. 11, no. 21, 2022, doi: 10.3390/electronics11213607.
[27] M. S. Akter, J. R. -Cardenas, H. Shahriar, A. Cuzzocrea, and F. Wu, "Quantum cryptography for enhanced network security: a comprehensive survey of research, developments, and future directions," *2023 IEEE International Conference on Big Data, BigData 2023*, 2023, pp. 5408–5417, doi: 10.1109/BigData59044.2023.10386889.
[28] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: threats, vulnerabilities, and attack taxonomy," *2015 13th Annual Conference on Privacy, Security and Trust*, 2015, pp. 145–152, doi: 10.1109/PST.2015.7232966.
[29] H. Wang, Y. Gao, Y. Liu, Q. Zhang, and Y. Zhou, "In-depth correlation power analysis attacks on a hardware implementation of CRYSTALS-dilithium," *Cybersecurity*, vol. 7, no. 1, 2024, doi: 10.1186/s42400-024-00209-9.
[30] M. Frey *et al.*, "Security for the industrial IoT: the case for information-centric networking," *IEEE 5th World Forum on Internet of Things, WF-IoT 2019*, 2019, pp. 424–429, doi: 10.1109/WF-IoT.2019.8767183.
[31] S. Kundu, S. Chowdhury, S. Saha, A. Karmakar, D. Mukhopadhyay, and I. Verbauwhede, "Carry your fault: a fault propagation attack on side-channel protected LWE-based KEM," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, no. 2, 2024, pp. 844–869, doi: 10.46586/tches.v2024.i2.844-869.
[32] B. Muruganantham, P. Shamili, S. G. Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 407–414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.
[33] Y. Zhao, H. Nishikawa, X. Kong, and H. Tomiyama, "Side channel power analysis resistance evaluation of masked adders on FPGA," *International Journal of Reconfigurable and Embedded Systems*, vol. 12, no. 1, pp. 97–112, 2023, doi: 10.11591/ijres.v12.i1.pp97-112.

BIOGRAPHIES OF AUTHORS

Shreyas Kasture is a third-year student at Symbiosis Institute of Technology and pursuing Artificial Intelligence and Machine Learning as his major. He has a special focus on cloud computing and data science, and he participates in research activities as well as projects that develop his expertise. He is a member of the Association for Computing Machinery (ACM) and IEEE and works with his colleagues to find new approaches to technology. He has recently completed a course in Google Cloud Computing Foundations, which demonstrates his desire to learn more. He can be contacted at email: shreyas200410@gmail.com.

Sudhanshu Maurya has completed his Post-Doctoral Research from School of Computer & Communication Engineering, Universiti Malaysia Perlis (UniMAP), Kangar, Perlis, Malaysia. He is currently working as Professor of CSE, Manav Rachna International Institute of Research and Studies (Deemed to be University), Faridabad, India. He is also associated with the Centre of Artificial Intelligence & Robotics, Indian Institute of Technology (IIT) Mandi, for research on AI-based quantum cryptographic techniques. He has completed his Ph.D. in Computer Science, focusing on the "Security and privacy aspect of mobile cloud computing." He acquired M.Tech. in CSE from Hemvati Nandan Bahuguna Garhwal Central University, Uttarakhand. His area of research is dedicated to artificial intelligence, machine learning, internet of everything, and security. He has two international patents (granted), 13 Indian patents, two edited books, five-course books, and authored/co-authored more than 190 research papers indexed in Web of Science/Scopus-indexed journals and conferences. He can be contacted at email: dr.sm0302@gmail.com.

Alakshendra Pratap Singh is a third-year student at Symbiosis Institute of Technology, Symbiosis International (Deemed University), Nagpur, studying B.Tech. Computer Science. He is also involved in research in the area of machine learning and data analytics for a number of academic projects. Being the Vice-Chair of the IEEE student chapter, Nagpur, he is responsible for arranging workshops and sessions for the students to improve their skills. In addition to his academic achievements, he is also active in extra curriculum activities. He can be contacted at email: singhalakshendra12@gmail.com.

Dr. Amit Shukla is currently Chairperson of Centre for AI and Robotics (CAIR) at Indian Institute of Technology (IIT), Mandi. He has done B.Tech. and M.Tech. in Mechanical Engineering, with specialization in Robotics and AI from the Indian Institute of Technology Kanpur (IITK), India. He completed his Ph.D. in Electric Vehicles with the control systems group, Electrical-Mechanical Engineering at Imperial College London, United Kingdom. Recently, he was leading robotics research in the utility sector as Head of Robotics at Dubai Electricity and Water Authority, Dubai, 2021-2022 (DEWA). Before joining IIT Mandi in year 2019, he worked at Robotics Center, The Petroleum Institute of Abu Dhabi National Oil Company (ADNOC) group of companies from 2012-2018 and then at Robotics center of Khalifa University of Science and Technology, Abu Dhabi (2018-2019). His specializes in Robotics and AI based technologies while his research interest span across multi-disciplinary areas of engineering such as robotics, AI, computer vision, drone technology, electric vehicle, cyber physical systems, and cyber security. He can be contacted at email: amitshukla@iitmandi.ac.in.

Arnav Kotiyal is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Graphic Era Deemed to be University, Dehradun, India where he joined in March 2022. He holds an M.Tech. degree from Graphic Era Deemed to be University, Dehradun and B.Tech. from Uttarakhand Technical University, Dehradun, India. His research interests include cyber security, internet of things (IoT), and machine learning. He has over 2 years of teaching and research experience and has contributed to several reputed publications, including IEEE and Springer. He has been recognized as an Adobe Master Educator for his contributions to academia and innovation in teaching. He can be contacted at email: arnold.kotiyal@gmail.com.

Kashish Mirza is working as a Lecturer in Department of Computer Science and Engineering at Graphic Era Hill University, Bhimtal Campus, Uttarakhand, India. She has completed her B.Tech. (CSE with Specialization in AI and ML) and is currently pursuing M.Tech. Computer Science and Engineering from Graphic Era Hill University, Bhimtal Campus, Uttarakhand, India. Her research focus is in the field of artificial intelligence, network security, and cryptography. She can be contacted at email: kashishmirza99@gmail.com.