electronics

MDPI

Article

Lightweight and Efficient Post Quantum Key Encapsulation Mechanism Based on Q-Problem

Mostefa Kara [1], Konstantinos Karampidis [2], Spyros Panagiotakis [2,*], Mohammad Hammoudeh [3], Muhamad Felemban [1,3,4] and Giorgos Papadourakis [2]

[1] Interdisciplinary Research Center for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; mostefa.kara@kfupm.edu.sa (M.K.); mfelemban@kfupm.edu.sa (M.F.)
[2] Department of Electrical and Computer Engineering, Hellenic Mediterranean University, 71410 Heraklion, Greece; karampidis@hmu.gr (K.K.); papadour@hmu.gr (G.P.)
[3] Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; mohammad.hammoudeh@kfupm.edu.sa
[4] Computer Engineering Department, ICS, IRC for ISS, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
* Correspondence: spanag@hmu.gr

Abstract: The Q-problem is a new lightweight and hard mathematical problem that resists quantum attacks. It depends on putting one known value and two unknown values per equation; whatever the operator, the Q-problem defines certain conditions between equations. This paper presents a new key exchange protocol based on the Q-problem. To protect secure end-to-end communication over a public transmission channel, the proposed mechanism consists of two rounds of exchanging totally random numbers, which ensure a shared secret key between two parties at the end. Security analysis proves the robustness of the proposal and experiments prove its lightness during implementation, making it a promising protocol of hybrid solutions and an assistive technique for the transition to the quantum era.

Keywords: Q-problem; key exchange protocol; secure communication; lightweight cryptography; quantum attacks

Academic Editor: Zbigniew Kotulski

Received: 8 January 2025
Revised: 10 February 2025
Accepted: 11 February 2025
Published: 13 February 2025

Citation: Kara, M.; Karampidis, K.; Panagiotakis, S.; Hammoudeh, M.; Felemban, M.; Papadourakis, G. Lightweight and Efficient Post Quantum Key Encapsulation Mechanism Based on Q-Problem. *Electronics* **2025**, *14*, 728. https://doi.org/10.3390/electronics14040728

1. Introduction

In the contemporary digital landscape, secure communication has become a cornerstone of global connectivity [1,2]. The exponential growth of online services, cloud computing, Internet of Things (IoT) devices, and critical infrastructure systems has amplified the demand for cryptographic mechanisms to ensure confidentiality, integrity, and authenticity of data exchanges [3]. Every interaction, be it financial transactions, healthcare records, or government communication, relies on the robustness of cryptographic protocols to safeguard sensitive information from adversaries. Despite significant advances in cryptographic science, the advent of quantum computing introduces formidable challenges to the existing paradigms of secure communication [4]. This has intensified the search for innovative, lightweight, and quantum-resistant cryptographic solutions, which can operate efficiently across diverse environments [5].

Among the foundational elements of secure communication are key exchange protocols, which enable parties to establish a shared secret key over an insecure channel [6,7]. These protocols are critical for ensuring that subsequent encrypted communication remains secure against eavesdropping and tampering [8,9]. Classical key exchange mechanisms, such as the Diffie–Hellman (DH) protocol and its elliptic curve variant (ECDH), rely on mathematical problems like the Discrete Logarithm Problem (DLP) or the Elliptic Curve Discrete Logarithm Problem (ECDLP) [10]. However, with the rapid advancements in quantum computing, these problems are no longer considered secure, as quantum algorithms, notably Shor's algorithm, are capable of solving them in polynomial time. Consequently, the cryptographic community is actively seeking key exchange mechanisms that are resistant to quantum attacks while maintaining efficiency and scalability [11].

A promising avenue for post-quantum cryptography is the development of protocols based on mathematically hard problems that remain intractable even for quantum computers [12]. Among these, the Q-problem emerges as a novel, lightweight, and computationally challenging problem, which demonstrates strong resistance to quantum attacks. The Q-problem is characterized by its unique structure: each equation involves one known value and two unknown values, combined through an operator, which is subject to specific inter-equation conditions [13]. This intrinsic complexity creates a cryptographic foundation that is lightweight and suitable for resource-constrained environments, and it is resistant to the computational capabilities of quantum systems. By leveraging the Q-problem, new cryptographic protocols can address the dual challenges of efficiency and security in the post-quantum era [14].

Quantum computing represents a paradigm shift in computational power, posing an existential threat to traditional cryptographic systems [12]. Algorithms, such as Shor's and Grover's, exploit the parallelism inherent in quantum systems to solve classical cryptographic problems with unprecedented speed. For instance, Shor's algorithm can efficiently factorize large integers and compute discrete logarithms, rendering RSA, DH, and ECDH insecure. Furthermore, Grover's algorithm accelerates brute-force attacks, weakening the security of symmetric-key cryptography by effectively halving the key length [15]. The looming prospect of quantum attacks necessitates a transition to the cryptographic systems that can withstand such computational advances, which are commonly referred to as post-quantum or quantum-resistant cryptography [16].

While addressing quantum resistance is paramount, another pressing concern is the need for lightweight cryptography, especially in the context of IoT, wearable devices, and other resource-constrained systems [17,18]. These environments require cryptographic protocols that minimize computational overhead, memory usage, and energy consumption without compromising security. Traditional post-quantum cryptographic schemes, often based on lattice problems, code-based cryptography, or multivariate polynomials, can be computationally intensive, which makes them impractical for lightweight applications [19,20]. The Q-problem, with its inherently simple yet hard mathematical structure, presents an ideal candidate for lightweight and efficient cryptographic solutions that cater to both quantum resistance and resource efficiency [21].

1.1. Contributions

This paper introduces a "Lightweight and Efficient Post-Quantum Key Encapsulation Mechanism Based on Q-Problem: QP-KEM", a novel protocol designed to address the dual challenges of quantum resistance and lightweight operation. The proposed protocol leverages the unique properties of the Q-problem to establish secure key exchange mechanisms that are resilient to quantum attacks while maintaining minimal computational and resource requirements. The key contributions of this research are as follows:

- Proposal of a Q-problem-based key exchange protocol: A detailed description and analysis of the protocol, which highlights its design principles and operational mechanics.
- Quantum resistance: A comprehensive security analysis demonstrating the protocol's resilience against quantum attacks, including its immunity to Shor's and Grover's algorithms.

- Efficiency and lightweight design: Evaluation of the protocol's performance metrics, which showcases its suitability for resource-constrained environments.
- Comparison with existing protocols: Benchmarking the proposed protocol against classical and post-quantum key exchange schemes in terms of security, efficiency, and practical applicability.

1.2. Structure of the Paper

The rest of this paper is organized as follows. Section 2 reviews related work in the domain of post-quantum cryptography and key exchange protocols, identifying gaps addressed by our research. Section 3 provides research design and an overview of the Q-problem, presenting its mathematical formulation and properties. Section 4 introduces the proposed Q-problem-based key exchange protocol, outlining its design, algorithms, and operational flow. Section 5 presents a thorough security analysis, including resistance to classical and quantum attacks. Section 6 evaluates the protocol's performance, highlighting its lightweight nature and efficiency. Finally, Section 7 concludes the paper with a summary of findings and directions for future research.

By integrating the Q-problem into a lightweight, post-quantum key exchange protocol, this research aims to contribute a robust and efficient solution to the evolving challenges of secure communication in the quantum era.

2. Related Work

The Diffie–Hellman (DH) protocol is a foundational cryptographic method that allows two parties to securely establish a shared secret over an insecure communication channel [22]. Introduced by Whitfield Diffie and Martin Hellman in 1976 [23], the protocol is based on the mathematical difficulty in solving the discrete logarithm problem. In DH, each party generates a private key and computes a public key derived from a shared base and modulus. By exchanging their public keys, both parties use their private keys to compute a shared secret, which remains confidential even if an eavesdropper intercepts the public keys. This shared secret can then be used to derive cryptographic keys for secure communication. Despite its effectiveness, the protocol is vulnerable to quantum attacks due to Shor's algorithm, prompting the need for post-quantum alternatives.

In [24], the authors introduced an anonymous authentication and key exchange protocol for communication between smart meters and the AMI Head-End in smart grid systems. This protocol was built on elliptic curve cryptography, with its security demonstrated using the random oracle model and BAN logic.

In [25], a multiparty key exchange protocol was proposed for handover authentication, emphasizing the privacy preservation of transfer tickets via the Diffie–Hellman method. The protocol aimed to minimize authentication delays during handover operations, achieving efficiency by relying solely on symmetric key-based operations to reduce computational overhead.

Gupta et al. [26] developed a model combining the RSA public-key cryptosystem with the Diffie–Hellman key exchange to mitigate man-in-the-middle (MITM) attacks. The effectiveness of this integrated approach was validated by comparing its performance against the standalone Diffie–Hellman key exchange algorithm and the RSA cryptosystem.

Mishri et al. [27] presented an end-to-end anonymous key exchange protocol leveraging self-blindable signatures. In this scheme, vehicles blind their private certificates for communication outside the mix-zone and generate an anonymously shared key using zero-knowledge proofs of knowledge (PoK). These proofs authenticate the ephemeral values used to derive a shared key through the Diffie–Hellman protocol. This design eliminated the need for external information to establish a secure shared key.

In [28], a novel key exchange protocol tailored for IoT environments was proposed, enabling secure communication between gateways and IoT devices over open channels. The protocol enhanced security by leveraging noncommutative structures and polynomials over noncommutative rings. Its foundation lies in solving the generalized decomposition problem associated with these rings. Additionally, the authors addressed how the protocol ensures key certification and forward secrecy.

In [29], a lattice-based explicit authenticated key exchange protocol was developed by integrating a Chosen Plaintext Attack (IND-CPA) key encapsulation mechanism with an EUF-CMA digital signature in the message-recovery mode. Parameter specifications were provided for 102-bit and 218-bit post-quantum security. Compared to implicit authenticated key exchange protocols derived directly from key encapsulation mechanisms, this approach reduced communication costs by 21.7% and 25.7%, respectively, under the same security levels.

Kundu et al. [30] introduced Rudraksh, a CCA-secure post-quantum key encapsulation mechanism (KEM) based on hard lattice problems. The authors optimized critical design elements, including polynomial size, field modulus structure, reduction algorithms, and secret/error distributions, to create a lightweight solution. The proposed design achieves 100-bit post-quantum security and demonstrates a threefold improvement in area efficiency compared to the state-of-the-art Kyber KEM.

In [31], code-based key encapsulation mechanisms designed for post-quantum cryptography were analyzed. These mechanisms, presented during the NIST PQC competition, were evaluated for their cryptographic properties and performance, providing a comprehensive comparative analysis of their effectiveness and practical implementation.

Kyber [32] is a module-based key encapsulation mechanism (KEM) built on the Learning With Errors (LWE) problem in module settings. It employs the LP-style public key encryption (PKE) framework, with its security grounded in the module-LWE assumption. Similarly, Saber [33] replaces Gaussian sampling, commonly used in key generation and encapsulation, with a rounding process. Saber's security is based on the module-Learning With Rounding (module-LWR) assumption, providing an efficient alternative to module-LWE-based schemes.

Lee et al. [34] introduced RLizard, a key encapsulation mechanism whose security relies on ring Learning With Errors (ring-LWE) and ring Learning With Rounding (ring-LWR) problems. By operating on a specialized type of ring, RLizard achieves greater efficiency than the original Lizard scheme, reducing both the clock cycles required for key generation and the overall key size.

Bernstein et al. [35] proposed NTRU Prime, a variant of the original NTRU encryption scheme. This design replaces cyclotomic rings with alternative rings that lack certain mathematical structures, enhancing security by mitigating potential vulnerabilities to future cryptanalysis. NTRU Prime also eliminates decryption failures and employs a constant-time implementation to bolster resistance against side-channel attacks.

All these proposals are not without one of two main drawbacks: the first is that they are not resistant to quantum attacks [23–27], or they are resistant to quantum but have a high computational and/or communication cost [28–35]. Therefore, this paper presents a new KEM that overcomes these obstacles, as it provides a lightweight and quantum-resistant protocol.

3. Research Design and Q-Problem

3.1. Research Design

Derived from the literature review, this study aims to address the following research questions:

- How does the proposed KEM ensure security against quantum attacks compared to existing post-quantum cryptographic schemes?
- How does the computational and communication efficiency of the proposed scheme compare to other post-quantum KEMs?
- Can the proposed mechanism maintain lightweight performance while ensuring secure key exchange in resource-constrained environments (e.g., IoT applications)?

To answer these research questions, we designed and implemented a novel post-quantum key encapsulation mechanism based on the Q-problem. After explaining the proposal in detail and stating the required settings for implementation, our methodology consists of the following steps. We analyze the cryptographic strength of the proposed mechanism against both classical and quantum adversaries, demonstrating its resistance to known attacks. The proposed KEM is implemented and tested while considering constrained environments in real-world scenarios, such as IoT devices, to evaluate its efficiency. The protocol undergoes experimental testing, where execution time and memory usage are measured to validate its lightweight properties. We compare the performance of our protocol against existing post-quantum KEMs (e.g., lattice-based and code-based schemes) in terms of computational complexity, key sizes, and communication overhead.

To assess the effectiveness of the proposed scheme, some metrics are used, including resistance to classical and quantum attacks; execution time for key generation, encapsulation, and decapsulation; and size of exchanged messages. By addressing these aspects, this research aims to demonstrate that the proposed KEM provides quantum resistance while maintaining lightweight efficiency, making it a viable solution for future cryptographic applications.

3.2. Q-Problem

The security of the proposed scheme is rooted in a novel post-quantum computational challenge known as the Q-problem, which was introduced by Laouid et al. [13]. This problem establishes a robust mathematical foundation that is considered resistant to the advanced computational capabilities of quantum computers, ensuring the security of our approach. The Q-problem (QP) is formally defined as follows:

$$\text{QP} \Leftrightarrow \begin{cases} \triangleright\, F() = \{Qe_1, Qe_2, \ldots, Qe_n\} \\ \triangleright\, Qe_i : x_i \star y_i \mod p \mid \star\ is : +, \times, or\ exp \\ \triangleright\, Both\ x_i\ and\ y_i\ are\ hidden \\ \triangleright\, \forall\ (Qe_i, Qe_j)\ Qe_i\ \theta\ Qe_j = \perp \\ \triangleright\, \forall\ Qe_i,\ (x_i, y_i)\ \theta\ p = \perp \\ \triangleright\, Given\ z, \forall\ Qe_i : \\ \ \#Sols_{Eq.}(\ z = x \star y \mod p) >> 1 \end{cases}$$

Qe refers to Post Quantum expression, Laouid et al. [13] have coined this term to refer to a mathematical equation in which the number of unknowns is greater than one, i.e., a single equation -linear or not- containing two or more unknown variables such that a quantum computer cannot solve it except by using of a brut force attack (BFA). Values x and y are unknown numbers or composed of arithmetic expressions of unknown numbers, i.e., $x = x_1 \star x_2$ and so on; $\perp$ means that neither x nor y has any relation with the public parameter p or part of it, i.e., the attacker cannot infer any information, neither partial nor complete, about the unknowns x, y from p. For more details, see Section 5.

The Q-problem was designed in reverse, which is to give the attacker many solutions instead of a single solution issue. For example, $z = x + y$ where z is known and (x, y) is unknown. This is shown as follows: $\#Sols_{Eq.}(\ z = x \star y \mod p) >> 1$. Many other assumptions are based on the difficulty of finding a single solution. Take, for example, the discrete logarithm problem $z = x^y$ where z and x are given. Using Shor's algorithm, the attacker can find y. Therefore, the Q-problem takes into account the future advancements in quantum computing, where it does not matter how advanced it is as long as there is always a set of solutions for each Q-problem instance.

3.3. Cryptographic Assumptions

The core idea of the Q-problem aligns with hidden subgroup problems and collision-resistant properties found in existing post-quantum cryptographic schemes, yet it generalizes beyond them by ensuring that an attacker always faces an exponential number of potential solutions rather than a single hard-to-compute one.

3.3.1. Q-Problem and the Hidden Subgroup Problem (HSP)

The Hidden Subgroup Problem (HSP) is a well-studied problem in quantum computing, which generalizes computational problems such as factoring and discrete logarithms. It is formally defined as follows: given a function $f : G \to X$ that hides a subgroup H, the goal is to determine H. Shor's algorithm efficiently solves HSP for abelian groups, which underlies quantum attacks on RSA and discrete logarithm-based cryptosystems. The Q-problem exhibits properties that make it difficult to reduce to HSP.

In traditional cryptographic problems, an equation often has a unique solution (e.g., discrete logarithm: given $z = x^y \mod p$, finding y uniquely). In the Q-problem, we ensure that for any given z, the number of solutions satisfies the following:

$$\#Sols_{\text{Eq.}}(z = x \star y \mod p) \gg 1 \tag{1}$$

This prevents an adversary from applying quantum period-finding techniques to extract a single valid solution. Moreover, in HSP, when the group G is non-abelian, quantum algorithms fail to efficiently recover the hidden subgroup H. The Q-problem is analogous to such non-abelian settings, as the attacker faces an exponentially large space of solutions, rendering quantum period-finding methods ineffective.

3.3.2. Q-Problem and Collision Resistance in Post-Quantum Cryptography

Collision-resistant hash functions are fundamental to post-quantum cryptography. A hash function $H(x)$ is collision-resistant if it is hard to find two distinct inputs $x_1 \neq x_2$ such that the following holds:

$$H(x_1) = H(x_2) \tag{2}$$

This property is essential for security in hash-based cryptographic schemes such as SPHINCS+. The Q-problem establishes a similar concept. Instead of relying on a function with low collision probability, the Q-problem guarantees that multiple valid solutions exist for every instance. Given $z = x \star y \mod p$, an adversary cannot determine a unique pair (x, y), mimicking the behavior of collision-resistant hashes. Even if a quantum algorithm efficiently finds one solution, it cannot verify its correctness due to the existence of multiple valid solutions.

A comparison between the Q-problem and collision-resistant hashes is given in Table 1.

The Q-problem ensures quantum resistance by leveraging two key principles. Avoiding unique solution structures, which prevents the use of quantum algorithms such as Shor's algorithm, ensures an exponentially large solution space, similar to the non-abelian HSP, making it infeasible for quantum solvers to extract useful information. Thus, the Q-problem generalizes the hardness of non-abelian HSP while also mimicking the unpredictability of collision-resistant hash functions.

Table 1. Comparison between Q-problem and collision-resistant hashes.

Property	Collision-Resistant Hashes	Q-Problem
Hardness Assumption	Hard to find two inputs with same output	Hard to find the exact (x, y) pair when many exist
Vulnerability to Quantum Algorithms	Grover's algorithm weakens security ($O(\sqrt{N})$ speedup)	No quantum speedup due to large solution space
Impact on Cryptanalysis	Resistance depends on function complexity	Resistance is intrinsic due to problem design

4. Proposed Mechanism

Post-quantum KEMs are essential for securing communication in real-world applications, especially in IoT and critical infrastructure. In IoT networks, post-quantum KEMs enable secure key exchange between resource-constrained devices, such as smart meters and industrial sensors, protecting data transmission from quantum-enabled attacks. In critical infrastructure, including power grids and transportation systems, these KEMs safeguard communication between control centers and remote monitoring devices, ensuring resilience against advanced cyber threats.

As illustrated in Figure 1, the proposed QP-KEM consists of two rounds. The first one uses random numbers and linear equations to transmit them. The second round between Alice and Bob introduces Hash calculation to check mutually exchanged values' correctness. Therefore function f_4 (respectively, f_8) can be any exponential or Hash safe calculation, the same thing for f_9 (respectively, f_{10}).

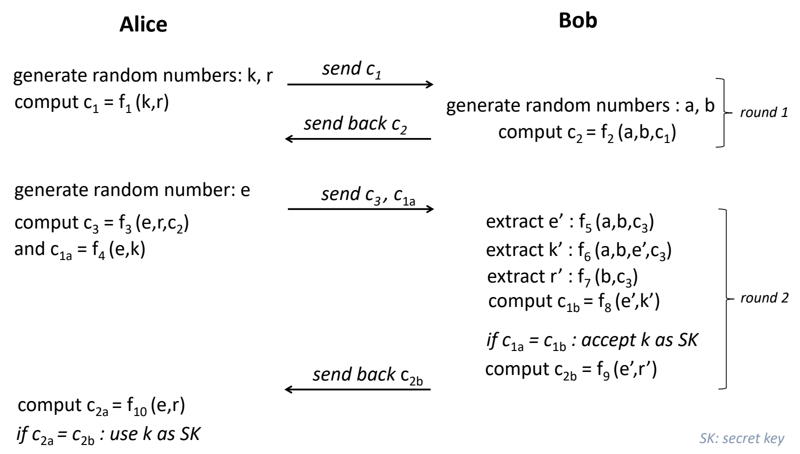

Figure 1. A general representation of the proposed mechanism.

First, Alice generates two random numbers k and r, where k will be the secret key. f_1 represents the multiplication of k and r and returns c_1 as follows: $f_1 : c_1 = k \times r \mod p$, where p is a public prime number. Alice sends c_1 to Bob via an insecure channel. Upon receiving c_1, Bob generates two random numbers a and b, then computes c_2 by f_2. f_2 represents a linear calculation that returns c_2 using the received c_1 and the generated values, $f_2 : c_2 = c_1 \times a + b \mod p$. By sending c_2 from Bob to Alice, round 1 is ended.

In round 2, Alice generates a new random number e and computes c_3 via f_3, using c_2, the previous generated number r, and the new one e. f_3 is the linear function that eliminates r from c_2, adds e, and returns c_3 as follows $f_3 : c_3 = c_2 \times r^- + e \mod p$, where r^- denotes the multiplicative inverse of r. In this stage, Alice also computes c_{1a} via f_4 as $f_4 : c_{1a} = Hash(e \times k)$; c_{1a} will be used by Bob to check data integrity and Alice's legitimacy. In reality, Alice sends the signature of c_{1a} using a post-quantum signature.

Upon receiving c_3 and c_{1a}, Bob extracts Alice's values e, k, r by f_5, f_6, f_7, respectively. f_5 is the function that recovers e from c_3 by using a and b as the following equation shows $f_5 : e' = (c_3 \mod b) \mod a$. f_6 is the function that recovers k from c_3 by using a, b, and e'

as the following calculation shows $f_6 : k' = (((c_3 - e') \mod b) \times a^-) \mod p$. f_7 is the function that returns r from c_3 by using b as follows $f_7 : r' = (c_3\mathfrak{b})^-$. Via f_8, Bob computes c_{1b} using the new calculated values e' and k' same as the function f_4 of Alice does (which outputs c_{1a}), $f_8 : c_{1b} = Hash(e' \times k')$. If $c_{1a} = c_{1b}$, Bob accepts the secret key k.

Until Bob proves to Alice that he obtained the right value of the secret key k and proves his legitimacy (against a man-in-the-middle attack), he sends her a new token c_{2b} with a different calculation than the first one ($f_9 \neq f_8$ i.e., $c_{1b} \neq c_{2b}$). f_9 returns c_{2b} and it is defined as follows $f_9 : c_{2b} = Hash(e' \times r')$. Then Bob sends c_{2b} to Alice to check the integrity of messages. In reality, Bob sends the signature of c_{2b} using a post-quantum signature in order to prove his legitimacy to Alice. Via f_10, Alice calculates c_{2a} by using her own numbers e and r as follows $f_10 : c_{2a} = Hash(e \times r)$. Finally, if $c_{2a} = c_{2b}$, Alice uses k as a secret key.

Parameter Picking

The following conditions should be satisfied to ensure the correct progress of the key exchange process. Any breach of these settings will affect the security or the validity of the proposed mechanism.

We have $c_1 = k \times r$ and $c_2 = c_1 \times a + b$, so

$$c_2 = k \times r \times a + b \tag{3}$$

If $c_3 = c_2 \times r^- + e \mod p$, then

$$c_3 = k \times a + b \times r^- + e \tag{4}$$

1. $r^- <<$: since we have a strict condition on r^- and not in r (setting: 4), Alice must pick r^- then computes r; in another word, we need for r^- to be relatively small and r to be large. If r is large, then $c_1 = k \times r$ would be greater than p, and this will make $k \times r \mod p$ secure.
2. $e < a$: if $k \times a + e < b$ in c_3, then $c_3 \mod b = k \times a + e$; and if $e < a$, then $(c_3 \mod b) \mod a = e$.
3. $a \times k < b$: to extract first $k \times a + e$ from c_3, this condition must be satisfied, so we need $c_3 \mod b$ to give exactly $k \times a + e$.
4. $b \times r^- < p$: after multiplying c_2 by r^- to calculate c_3, Alice obtains $k \times a + b \times r^- + e$. Bob needs these values to be exactly less p in order to be able to extract e, k, and r using a and b. Since $a \times k < b$ and $b \times r^- < p$, so $k \times a + b \times r^- + e < p$.
5. $p < k \times r$: as aforementioned, $c_1 = k \times r$ must be greater than p in order to hide k and r and protect them against factorization.
6. Public parameters : since the random values k, r, e, a, and b are unknown, there must be public parameters so that Alice and Bob can generate their random numbers. Let us call K, R, E, A, and B spaces for random values. These public parameters satisfy the conditions mentioned above.

Algorithms 1 and 2 summarize the proposed QP-KEM. In Algorithm 1, the multiplication in line 3 is to hide k by a random number r. After sending c_1, Alice waits for c_2 from Bob. In a failure case, Alice waits for a while and resends c_1 again. In line 9, a new random is added to hide k. After computing c_3 and c_{1a}, Alice sends them to Bob and waits for c_{2B} as shown in lines 9 to 13. In a failure case, Alice waits for a while and resends c_3 and c_{1a} again. If there is an interruption at this point, Alice returns to line 2. In Algorithm 2, two random numbers are included in line 6 and are used later to extract Alice numbers. In a failure case in line 9, Bob came back to line 7. In lines 11, 12, and 13, Bob uses his values to obtain Alice's values. c_{1b} is used so that Bob can confirm to Alice that he obtained the correct numbers.

Algorithm 1 Alice

Require: p, K, R, E

function F
  $k, r \leftarrow$ random
  $c_1 \leftarrow k \times r \mod p$
  send c_1
  —
  wait for $c_2 \ldots$
  —
  – Round 2 –
  $e \leftarrow$ random
  $c_3 \leftarrow c_2 \times r^- + e \mod p$
  $c_{1a} \leftarrow Hash(e \times k) \mod p$
  send c_3 and c_{1a} ▷ In practice, Alice sends Sig(c_{1a})
  —
  wait for $c_{2b} \ldots$
  —
  $c_{2a} \leftarrow Hash(e \times r) \mod p$
  if $c_{2a} = c_{2b}$ **then**
    return k
  else
    return *err*
  end if
end function

Algorithm 2 Bob

Require: p, A, B

function F
  —
  wait for $c_1 \ldots$
  —
  $a, b \leftarrow$ random
  $c_2 \leftarrow c_1 \times a + b \mod p$
  send c_2
  – Round 2 –
  —
  wait for c_3 and $c_{1a} \ldots$
  —
  $e' \leftarrow (c_3 \mod b) \mod a$
  $k' \leftarrow (((c_3 - e') \mod b) \times a^-) \mod p$
  $r' \leftarrow (\frac{c_3}{b})^- \mod p$
  $c_{1b} \leftarrow Hash(e' \times k') \mod p$
  if $c_{1a} = c_{1b}$ **then**
    $c_{2b} \leftarrow Hash(e' \times r') \mod p$
    send c_{2b} ▷ In practice, Bob sends Sig(c_{2b})
    return k'
  else
    return *err*
  end if
end function

5. Security Analysis

This section presents a formal security proof for the proposed key encapsulation mechanism (KEM) based on the hardness of the Q-problem.

We start by tracking the values exchanged between Alice and Bob to search in the Q-problem assumption for any loophole through which an attacker can penetrate the system or obtain any information or part of sensitive information.

Alice computes $c_1 = k \times r \mod p$; c_1 is of the form $c_1 = x \times y$, where x and y are unknown and chosen uniformly at random without relation between them, so the attacker cannot obtain any of them from c_1. To compute c_2, Bob multiplies c_1 by a and adds b, so c_2 is of the form $c_2 = x + y$ where x and y are unknown and chosen uniformly at random without relation between them; no information the attacker can extract from c_2. The same thing occurs in the next step when Alice computes and sends $c_3 = c_2 \times r^- + e$; it is of the form $c_3 = x + y$. The attacker still cannot obtain any useful information from the exchanged messages.

The other exchanged messages are c_a and c'_b, where $c_{1a} = Hash(e \times k) \mod p$ and $c_{2b} = Hash(e \times r) \mod p$. We note that both c_{1a} and c_{2b} are of the form $c = x \times y$ where x and y are unknown and chosen uniformly at random without relation between them. In addition, there is no way to use them simultaneously in order to recover the secret k, r, or e because the base in one is the exponent in the other. Sohr's algorithm is not efficient at all due to blinding both the base and exponent. Thus, the proposed protocol respects the Q-problem rules.

As defined by Recommendations for Key-Encapsulation Mechanisms [36] in security considerations for composite schemes, the proof covers two key security properties:

- Indistinguishability under IND-CPA: Ensures that the encapsulated key k is indistinguishable from a random key.
- Indistinguishability under Chosen Ciphertext Attack (IND-CCA): Ensures that even with access to a decapsulation oracle, an adversary cannot gain any information about the key.

The protocol involves values $c_1, c_2, c_3, c_{1a}, c_{2b}$ and operations mod p, with the security grounded in the post-quantum hardness of the Q-problem.

5.1. Security Assumptions

The security of the protocol relies on the following assumptions:

- **Hardness of the Q-Problem**: Given $c_1, c_2, c_3, c_{1a}, c_{2b}$, it is computationally infeasible to deduce k, r, e, a, b.
- **Randomness**: The values k, r, e, a, b are chosen uniformly at random and are independent.

5.2. IND-CPA Security Proof

Game-Based Approach: The proof proceeds through a sequence of games, where each game modifies the protocol slightly. We show that the adversary's advantage in distinguishing between games is negligible.

Game 0: Real Protocol. This is the real protocol interaction, where the adversary observes $c_1, c_2, c_3, c_{1a}, c_{2b}$ and tries to distinguish between the real key k and a random key k'.

Game 1: Replace c_{1a} with Random. In this game, we replace c_{1a} with a value computed from a random key k' instead of the actual k. All other values c_1, c_2, c_3, c_{2B} remain unchanged.

Transition Analysis: The adversary's advantage in distinguishing Game 0 from Game 1 is negligible, assuming the Q-problem is hard. The computation of c_{1a} involves $Hash(e \times k) \mod p$, which is indistinguishable from random due to the randomness of e, k.

Game 2: Replace All Values with Random. In this game, all transmitted values $c_1, c_2, c_3, c_{1a}, c_{2b}$ are replaced with random values.

Transition Analysis: The adversary's advantage in distinguishing Game 1 from Game 2 is negligible as $c_1, c_2, c_3, c_{1a}, c_{2b}$ depend on random combinations of k, r, e, a, b, and the

Q-problem ensures these are indistinguishable from random values. Since the adversary's advantage in each game transition is negligible, we conclude that the adversary cannot distinguish between the real key k and a random key k'. This proves IND-CPA security.

5.3. IND-CCA Security Proof

Reduction to the Q-Problem: To prove IND-CCA security, we assume an adversary $\mathcal{A}$ can break the protocol and construct a simulator $\mathcal{S}$ that solves the Q-problem.

1. Simulator $\mathcal{S}$ receives $c_1, c_2, c_3, c_{1a}, c_{2b}$ as input and acts as a decapsulation oracle for $\mathcal{A}$.
2. For each decapsulation query from $\mathcal{A}$, $\mathcal{S}$ computes k, r, e, a, b using its knowledge of the protocol equations.
3. $\mathcal{S}$ returns the decapsulated value to $\mathcal{A}$.

If $\mathcal{A}$ succeeds in distinguishing k from a random key, it provides $\mathcal{S}$ with sufficient information to solve the Q-problem. Thus, $\mathcal{A}$'s advantage is bounded by the probability of solving the Q-problem, which is negligible. We have shown that the proposed protocol achieves IND-CPA and IND-CCA security under the assumption that the Q-problem is computationally hard. The adversary's advantage in breaking the protocol is negligible in both cases.

As for the man-in-the-middle attack (MIMA), it cannot be detected in the first round because the attacker can easily impersonate Bob and generate two forged numbers a and b without Alice detecting it. On the other hand, Bob cannot be sure that the sender of c_1 is Alice. In the second round, Alice signs c_{1a} using a post-quantum signature and sends the signature instead of c_{1a}. When Bob receives signed c_{1a}, he will be able to verify Alice's identity as well as data integrity. After that, Bob signs c_{2b} and sends the signature to Alice. Now Alice can verify Bob's legitimacy as well as data integrity and then use the secret key k for data exchange.

Improper choice of p can expose k and r to factorization attacks or brute force. Therefore, in our protocol, p is intended to be a sufficiently large prime number, at least 256 bits, to mitigate these risks and ensure that brute-force attacks are computationally infeasible. Safe prime selection where $p = 2q + 1$, with q also a prime, is essential for enhancing security. The random selection of k, r, and the other numbers further complicates these attacks by increasing entropy.

6. Results and Performance

There are six parameters: K, A, E, B, R, and p. In the following, we show the smooth sequence of choosing the sizes of these parameters so that the conditions imposed on them are all met, and the key exchange process is correct and secure at the same time.

To achieve 128-bit security, the first parameter that would be selected is $\mid K \mid$ = 128 bits, then $\mid A \mid$ can equal 110 bits. According to setting #2 ($A > E$), we put $\mid E \mid$ = 100 bits. Upon satisfying setting #3 ($B > A \times K$), it is enough to put $\mid B \mid$ = 250 bits and $\mid R^- \mid$ = 40 bits for setting #1. Here, it is expressed by R^- instead of R because choosing R as a large number and producing R^- a small number from it is difficult. Therefore, Alice will calculate R^- first, then compute $R = (R^-)^-$. Finally, $\mid p \mid$ = 300 bits for setting #4 is chosen ($p > B \times R^-$). Since $R = (R^-)^-$, so $\mid R \mid \approx \mid p \mid$, and $K \times R > p$ (setting #5 is verified).

Now, Settings 1 to 5 are satisfied. Instances from public parameters could be randomly selected. Alice: $k^- \leftarrow random_K$, $r^- \leftarrow random_{R^-}$, and $e^- \leftarrow random_E$; Bob: $a^- \leftarrow random_A$ and $b^- \leftarrow random_B$.

Here, r^- should not be too small so that c_2 can be hidden in the equation f_3 using mod when calculating c_3, $c_3 = c_2 \times r^- + e \mod p$. Thus, $c_2 \times r^-$ must be greater than p and r^- would not be a large number. On the one hand, that is not needed, as it is just to hide c_2 in the calculation of c_3. On the other hand, the larger r^{-}'s size the larger p's size is, and thus the encrypted text size will increase. Certainly, c_1 is hidden in $c_2 = c_1 \times a + b$ because by default, $c_1 \times a$ is greater than p due to $\mid c_1 \mid \approx = \mid p \mid$.

In our simulation (see https://github.com/karamostefa/KEM), we neglected to handle time which includes transmission (message/bandwidth e.g., 1500/10 Mbps) and propagation delay (e.g., 10–50 ms). The execution time also does not take into account the signature time of c_{1a} and c_{2b}. For the proposal, quantum 128-bit security is considered, the key generation time is negligible, and i7-10610U CPU-2.30 GHz is used. For the other techniques, RSA: $\mid n \mid$ = 2048 bits, Diffie–Hellman: $\mid p \mid$ = 256 bits, Ref. [24]: $\mid p \mid$ = 256 bits, Ref. [26]: $\mid p \mid$ = 256 bits, Ref. [27]: $\mid q \mid$ = 128 bits, Ref. [28]: $\mid p \mid$ = 128 bits.

Table 2 highlights the performance and security characteristics of various KEM, showcasing notable differences in computation cost, communication cost, and quantum security. Classical methods such as RSA (6.08 ms) and Diffie–Hellman (8.83 ms) demonstrate moderate computational efficiency but lack quantum security, making them unsuitable for future-proof applications. In contrast, post-quantum cryptographic methods like Kyber (0.159 ms), NewHope (0.123 ms), and Saber (0.084 ms) are highly efficient, offering significantly lower computation costs while ensuring quantum resistance. In contrast, they generated large ciphertexts (6656, 8960, and 5888 bits, respectively). Techniques like Frodo AES and Classic-McEliece provide robust quantum security but exhibit higher computation costs (28.04 ms and 2.03 ms, respectively) and larger communication overheads. Notably, the proposed QP-KEM method achieves a balance between computational efficiency (0.161 ms) and communication cost (1500 bits) with quantum security, making it a competitive candidate for secure and efficient cryptographic applications in the post-quantum era.

Table 2. Comparison of various KEM.

Technique	Computation Cost (ms)	Ciphertext/Communication Cost (bits)	Quantum Secure
RSA	6.08	2048	N
Diffie–Hellman	8.83	512	N
Ref. [24], 2021	760	2048	N
Ref. [26] 2022	5.64	512	N
Ref. [27] 2022	3.58	1536	N
Ref. [28] 2022	192	512	Y
Ref. [34] 2018	3.47	6656	Y
Kyber [34,37]	0.159	6656	Y
NewHope [34,37]	0.123	8960	Y
Frodo AES [34,37]	28.04	77,888	Y
Saber [34,37]	0.084	5888	Y
NTRUEncrypt [34,37]	0.246	4888	Y
BIKE-L3 [37,38]	2.172	12,584	Y
Classic-McEliece [38]	2.03	1024	Y
Rudraksh [30] 2024	0.197	2771	Y
Proposed QP-KEM	0.161	1500	Y

Table 2 demonstrates the efficiency of QP-KEM in terms of time and size, demonstrating its potential for real-world applications. However, its advantages are most evident in resource-constrained environments, such as IoT devices, embedded systems, and mobile communications, where computational efficiency and low memory usage are critical. Unlike lattice-based alternatives, which may require higher computational power, the lightweight structure of QP-KEM makes it particularly suitable for scenarios demanding fast key exchanges with minimal overhead. Additionally, its simple mathematical operations enable seamless integration into hybrid cryptographic frameworks, facilitating a smoother transition to post-quantum security without significantly impacting performance. Therefore, the specific scenarios where QP-KEM is most advantageous appear in resource-constrained environments and hybrid cryptography.

7. Conclusions

This paper introduced a novel key exchange protocol based on the Q-problem, a lightweight mathematical problem specifically designed to resist quantum attacks. The proposed protocol ensures secure end-to-end communication through two rounds of random number exchange, leveraging linear calculations to establish a shared secret key. The comparative analysis demonstrated that the proposed protocol balanced computational efficiency and communication cost favorably, outperforming many post-quantum cryptographic schemes while maintaining quantum security. By achieving 0.161 ms in computation cost and 1500 bits in ciphertext size, experimental results further confirmed its lightweight nature, making it a viable candidate for resource-constrained environments. Additionally, its robustness against quantum threats positions it as a promising solution for hybrid cryptographic frameworks, thus facilitating a smooth transition into the quantum era. This work contributes to the ongoing development of efficient and secure cryptographic protocols, which aligns with the need for practical post-quantum security solutions. In future research, a formal side-channel resistance evaluation, energy consumption, and bandwidth efficiency will be taken into consideration.

Author Contributions: Conceptualization, M.K.; methodology, M.K. and K.K.; software, S.P.; validation, M.F. and S.P.; formal analysis, S.P., M.H. and G.P.; writing—original draft preparation, M.K. and K.K.; writing—review and editing, M.F., M.H. and G.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ashraf, Z.; Sohail, A.; Iqbal, M. Design and Implementation of Lightweight Certificateless Secure Communication Scheme on Industrial NFV-Based IPv6 Virtual Networks. *Electronics* **2024**, *13*, 2649. [CrossRef]
2. Santhosh Kumar, S.; Selvi, M.; Kannan, A. A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Comput. Intell. Neurosci.* **2023**, *2023*, 8981988. [CrossRef]
3. Merkle, R.C. Secure communications over insecure channels. *Commun. ACM* **1978**, *21*, 294–299. [CrossRef]
4. Torrieri, D.J. *Principles of Secure Communication Systems*; Artech House, Inc.: Norwood, MA, USA, 1992.
5. Feng, H.; Cai, B. A Provably Secure and Lightweight Two-Factor Authentication Protocol for Wireless Sensor Network. *Electronics* **2024**, *13*, 4289. [CrossRef]
6. Li, N. Research on Diffie-Hellman key exchange protocol. In Proceedings of the 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16–19 April 2010; IEEE: Piscataway, NJ, USA, 2010; Volume 4, p. V4-634.
7. Dharminder, D.; Reddy, C.B.; Das, A.K.; Park, Y.; Jamal, S.S. Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT. *IEEE Internet Things J.* **2022**, *10*, 2680–2692. [CrossRef]
8. AlShaikh, M.; Alzaqebah, M.; Gmati, N.; Alrefai, N.; Alsmadi, M.K.; Almarashdeh, I.; Mohammad, R.M.A.; Alamri, S.; Kara, M. Image encryption algorithm based on factorial decomposition. *Multimed. Tools Appl.* **2024**, *83*, 88447–88467. [CrossRef]
9. Kara, M.; Laouid, A.; Euler, R.; Yagoub, M.A.; Bounceur, A.; Hammoudeh, M.; Medileh, S. A homomorphic digit fragmentation encryption scheme based on the polynomial reconstruction problem. In Proceedings of the 4th International Conference on Future Networks and Distributed Systems, Alicante, Spain, 16–20 November 2020; pp. 1–6.
10. Rawat, A.S.; Deshmukh, M. Efficient extended diffie-hellman key exchange protocol. In Proceedings of the 2019 International Conference on Computing, Power and Communication Technologies (GUCON), NCR New Delhi, India, 27–28 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 447–451.
11. Park, H.; Son, S.; Park, Y.; Park, Y. Provably Quantum Secure Three-Party Mutual Authentication and Key Exchange Protocol Based on Modular Learning with Error. *Electronics* **2024**, *13*, 3930. [CrossRef]

12. Giron, A.A.; Custódio, R.; Rodríguez-Henríquez, F. Post-quantum hybrid key exchange: A systematic mapping study. *J. Cryptogr. Eng.* **2023**, *13*, 71–88. [CrossRef]
13. Laouid, A.; Kara, M.; Hammoudeh, M. Toward Independent Key Encryption based on Q-Problem. *Cryptol. Eprint Arch.* **2024**. Available online: https://eprint.iacr.org/archive/2024/645/1729147498.pdf (accessed on 10 February 2025).
14. Ding, J.; Alsayigh, S.; Lancrenon, J.; Rv, S.; Snook, M. Provably secure password authenticated key exchange based on RLWE for the post-quantum world. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 14–17 February 2017; Springer: Cham, Switzerland, 2017; pp. 183–204.
15. Aydin, F.; Aysu, A.; Tiwari, M.; Gerstlauer, A.; Orshansky, M. Horizontal side-channel vulnerabilities of post-quantum key exchange and encapsulation protocols. *ACM Trans. Embed. Comput. Syst. (TECS)* **2021**, *20*, 1–22. [CrossRef]
16. Scalise, P.; Garcia, R.; Boeding, M.; Hempel, M.; Sharif, H. An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics* **2024**, *13*, 4258. [CrossRef]
17. Medileh, S.; Kara, M.; Laouid, A.; Bounceur, A.; Kertiou, I. A Secure Clock Synchronization Scheme in WSNs Adapted for IoT-based Applications. In Proceedings of the 7th International Conference on Future Networks and Distributed Systems, Dubai, United Arab Emirates, 21–22 December 2023; pp. 674–681.
18. Kebache, R.; Laouid, A.; Bounceur, A.; Kara, M.; Karampidis, K.; Papadourakis, G.; Hammoudeh, M. Reducing the Encrypted Data Size: Healthcare with IoT-Cloud Computing Applications. *Comput. Syst. Sci. Eng.* **2024**, *48*, 1055–1072. [CrossRef]
19. Fernández-Caramés, T.M. From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2019**, *7*, 6457–6480. [CrossRef]
20. Rana, M.; Mamun, Q.; Islam, R. Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. *Electronics* **2024**, *13*, 4325. [CrossRef]
21. Tanksale, V. Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices. *Electronics* **2024**, *13*, 3631. [CrossRef]
22. Ahmed, M.; Sanjabi, B.; Aldiaz, D.; Rezaei, A.; Omotunde, H. Diffie-Hellman and its application in security protocols. *Int. J. Eng. Sci. Innov. Technol. (IJESIT)* **2012**, *1*, 69–73.
23. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
24. Luo, Y.; Zheng, W.; Chen, Y.C. An anonymous authentication and key exchange protocol in smart grid. *J. Netw. Intell.* **2021**, *6*, 206–215.
25. Roy, A.K.; Nath, K.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Privacy preserving multi-party key exchange protocol for wireless mesh networks. *Sensors* **2022**, *22*, 1958. [CrossRef]
26. Gupta, C.; Reddy, N.S. Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. *J. Phys. Conf. Ser.* **2022**, *2161*, 012014. [CrossRef]
27. AlMarshoud, M.S.; Al-Bayatti, A.H.; Kiraz, M.S. Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures. *Veh. Commun.* **2022**, *36*, 100490. [CrossRef]
28. Kanwal, S.; Inam, S.; Ali, R.; Cheikhrouhou, O.; Koubaa, A. Lightweight noncommutative key exchange protocol for IoT environments. *Front. Environ. Sci.* **2022**, *10*, 996296. [CrossRef]
29. Xue, G.; Wang, B.; Qu, Q.; Zhang, W. Efficient lattice-based authenticated key exchange based on key encapsulation mechanism and signature. *IET Inf. Secur.* **2021**, *15*, 107–116. [CrossRef]
30. Kundu, S.; Ghosh, A.; Karmakar, A.; Sen, S.; Verbauwhede, I. Rudraksh: A compact and lightweight post-quantum key-encapsulation mechanism. *arXiv* **2025**, arXiv:2501.13799.
31. Kuznetsov, A.; Lutsenko, M.; Kiian, N.; Makushenko, T.; Kuznetsova, T. Code-based key encapsulation mechanisms for post-quantum standardization. In Proceedings of the 2018 IEEE 9th international conference on dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 24–27 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 276–281.
32. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 353–367.
33. D'Anvers, J.P.; Karmakar, A.; Sinha Roy, S.; Vercauteren, F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In Proceedings of the Progress in Cryptology—AFRICACRYPT 2018: 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, 7–9 May 2018; Proceedings 10; Springer: Cham, Switzerland, 2018; pp. 282–305.
34. Lee, J.; Kim, D.; Lee, H.; Lee, Y.; Cheon, J.H. RLizard: Post-quantum key encapsulation mechanism for IoT devices. *IEEE Access* **2018**, *7*, 2080–2091. [CrossRef]
35. Bernstein, D.J.; Chuengsatiansup, C.; Lange, T.; van Vredendaal, C. NTRU prime: Reducing attack surface at low cost. In Proceedings of the Selected Areas in Cryptography—SAC 2017: 24th International Conference, Ottawa, ON, Canada, 16–18 August 2017; Revised Selected Papers 24; Springer: Cham, Switzerland, 2018; pp. 235–260.
36. Alagic, G.; Barker, E.; Chen, L.; Moody, D.; Robinson, A.; Silberg, H.; Waller, N. *Recommendations for Key-Encapsulation Mechanisms*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025.

37. Roma, C.A.; Tai, C.E.A.; Hasan, M.A. Energy efficiency analysis of post-quantum cryptographic algorithms. *IEEE Access* **2021**, *9*, 71295–71317. [CrossRef]
38. Farooq, S.; Altaf, A.; Iqbal, F.; Thompson, E.B.; Vargas, D.L.R.; Díez, I.d.l.T.; Ashraf, I. Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms. *Sensors* **2023**, *23*, 5379. [CrossRef] [PubMed]