IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 August 2025, accepted 24 August 2025, date of publication 8 September 2025, date of current version 12 September 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3607474

RESEARCH ARTICLE

Hybrid KEM-QKD Integration With Parameter Optimization for Secure Underwater Networks via NetSquid Simulations

D. JEYA MALA, (Member, IEEE), ACHINTYA KANT RASTOGI, AYUSH RAJ, AND VAIDIK MANORI

Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India

Corresponding author: D. Jeya Mala (jeyamala.d@vit.ac.in)

This work was supported in part by the Department of Science and Technology (DST), India, through the Fund for Improvement of Science and Technology (S&T) Infrastructure in Universities and Higher Educational Institutions (FIST) Program, under Grant SR/FST/ET-I/2022/1079; and in part by VIT University.

ABSTRACT Quantum cryptography, especially quantum key distribution (QKD), is significant for shielding communications against the dangers of quantum computing by providing information-theoretic security established in quantum mechanics. To securely generate and distribute cryptographic keys between two parties, several quantum safe protocols were proposed. Even though the BB84 protocol is a more trusted, widely implemented and standardized protocol for QKD, it suffers from 50% key loss during sifting. The next version B92 protocol is the lighter version of BB84, has critical issues such as: less tolerance to noise and photon loss and is specifically applicable for short range, lower security scenarios and as B92 has only two non-orthogonal states, it makes it more vulnerable to certain Unambiguous State Discrimination (USD) attacks. Hence, this work has taken the most widely adopted protocol BB84 as it has more advantages for underwater networks by proposing a novel hybrid approach to mitigate the fundamental efficiency challenge of key losses during the sifting phase due to basis mismatches. As this inefficiency is a significant barrier to practical deployment, particularly in resource-constrained environments like underwater networks, we propose a novel hybrid KEM-QKD protocol that eliminates the sifting process of BB84 entirely. Our primary contributions are: (i) integration of a post-quantum key encapsulation mechanism (KEM), CRYSTALS-Kyber, to securely transmit basis information prior to measurement which allows for 100% basis alignment between communicating parties, preserving the entire raw key; (ii) benchmarked our modified protocol against traditional BB84 using NetSquid, a quantum network simulator and (iii) optimized the proposed protocol's parameters using Bayesian Optimization (BO) and Genetic Algorithms (GA). Our results demonstrate two major performance enhancements: (i) a 100% raw key generation rate, a significant improvement over BB84's 50% efficiency and (ii) an increase in the maximum secure distance of up to 42% in existing optic fiber cables, with BO proving superior for parameter optimization. Further, our rigorous experimentation results showcase the potential of the proposed hybrid quantum-classical framework to enhance the practical efficiency of QKD, advancing its viability for robust, high-performance underwater quantum networks.

INDEX TERMS Quantum key distribution (QKD), BB84 protocol, post quantum cryptography (PQC), key encapsulation mechanisms (KEM), CRYSTALS-Kyber, Bayesian optimization (BO), genetic algorithm (GA).

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su.

I. INTRODUCTION

Quantum computers are advancing rapidly and threaten to break the encryption systems that protect most of the

internet today. Current methods like RSA and ECC, which secure everything from online banking to messaging apps, rely on mathematical problems that quantum computers could solve quickly. For example, a quantum algorithm called Shor's algorithm can crack these codes in minutes, while traditional computers would take thousands of years. It is especially worrying because hackers are already stealing encrypted data, such as emails or financial records, and storing it to decrypt later once quantum computers become powerful enough. Experts warn that by 2029, these encryption methods may no longer be safe, pushing governments and companies to adopt quantum-resistant solutions now.

Quantum Key Distribution (QKD) offers a way to share encryption keys that even quantum computers cannot hack. Instead of relying on math problems, QKD uses the laws of physics—like how light particles (photons) behave—to create unbreakable keys. Here is how it works: Two parties send photons encoded with secret information. If a hacker tries to intercept them, measuring the photons changes their properties, alerting the users to the breach.

Challenges to be addressed in this work include:

• BB84 Challenges: Inherent sifting inefficiency in BB84, where approximately 50% of transmitted qubits are discarded due to basis mismatch, leading to resource wastage in constrained environments like under- water networks.

• Quantum Network Challenges: Limitations in secure communication distance and performance in quantum networks, exacerbated by factors such as latency, attenuation, and computational overhead.

• Parameter Optimization Challenges: Need for efficient parameter optimization in high- dimensional, noisy spaces to maximize protocol distance between nodes.

• Underwater Communication Challenges: The underwater communication cables which handle over $10 trillion in daily transactions, face unique challenges in the era of quantum computing. These cables connect continents and are critical for global communications, but they are vulnerable for three main reasons:

- **Latency:** The delay in sending signals through water (over 300 milliseconds round-trip) makes it hard to update encryption keys quickly, giving hackers more time to steal data.
- **Outdated Infrastructure:** Many underwater cables, like signal boosters, use old hardware that cannot easily support new quantum-safe upgrades.
- **Hybrid Systems:** Mixing old and new encryption methods during upgrades can create weak spots that hackers could exploit.

• Underwater Key-Update Challenges: Additionally, underwater systems rely on pre-shared keys for communication, which are difficult to update regularly. Although laser-based QKD has demonstrated effectiveness in short underwater experiments, practical issues, such as light obstruction from murky water, continue to hinder its effectiveness.

To address these challenges, this research work focuses on the improvement of BB84 as it is a more trusted and standardized protocol for QKD, and has several advantages while facing some performance issues. Even though B92 protocol is the next version of BB84, it has critical issues such as: less tolerance to noise and photon loss and is specifically applicable for short range, lower security scenarios and as B92 has only two non-orthogonal states, it makes it more vulnerable to certain Unambiguous State Discrimination (USD) attacks.

The proposed, KEM-BB84 approach differs fundamentally from B92. Instead of modifying the number of quantum states, our method retains the robust four-state structure of BB84 but addresses the sifting inefficiency directly. By using a post-quantum KEM to securely exchange basis information, we eliminate the sifting step entirely, achieving a 100% raw key rate without the trade-offs in noise tolerance associated with B92. This makes our approach particularly advantageous for noisy channels, such as those in underwater networks.

In our approach to improve the BB84 algorithm, Alice encodes her randomly chosen basis (rectilinear or diagonal) into a ciphertext using a post-quantum KEM, such as NIST-standardized CRYSTALS-Kyber. This encapsulated basis is transmitted to Bob alongside the qubits. Bob then decapsulates the ciphertext using his private key, recovering Alice's basis choice before measuring the qubits. All transmitted qubits contribute directly to the final key by aligning their bases prior to measurement, bypassing the wasteful sifting step. This theoretically eliminates basis mismatch errors, preserving the entire raw key for privacy amplification. While KEM encapsulation introduces computational overhead, this trade-off is justified in resource-constrained settings. For underwater networks, where photon generation is costlier than computation, reducing optical transmissions outweighs marginal increases in processing latency.

To evaluate the performance of KEM-enhanced BB84 in underwater environments, we modelled the protocol using NetSquid, a quantum network simulator designed for high-fidelity simulations of quantum communication systems. We integrated CRYSTALS-Kyber for basis encapsulation, transmitting ciphertexts alongside qubits over a hybrid quantum-classical channel. By eliminating the sifting process, the protocol retained 100% of transmitted qubits, improving raw key rates significantly compared to traditional BB84. However, KEM processing may introduce latency overheads due to ciphertext transmission and decapsulation steps, highlighting a critical trade-off between efficiency and computational load. To maximize the operational range of KEM-BB84, we employed Genetic Algorithms (GAs) and Bayesian Optimization (BO) to identify optimal parameter configurations. The goal is to find the maximum distance between two nodes under realistic channel modeling for underwater networks.

The integration of classical cryptography technique in the proposed work has two-fold benefits: (a) The Quantum security principles (Heisenberg uncertainty, no-cloning

theorem) remain intact for the quantum channel, while the post-quantum KEM (Kyber) provides cryptographically secure basis transmission over the classical channel as KEM helps resist attacks, side-channel vulnerabilities from quantum computers by adding redundancy if QKD channels are disrupted or compromised; (b) KEMs integration helps in embedding of QKD into larger classical infrastructure and can bridge the gaps where Quantum Repeaters are not viable for secure classical key transport over the communication network.

The above benefits makes the proposed work to achieve the 100% basis alignment which eliminates the 50% sifting waste without sacrificing information-theoretic security, representing a net security and efficiency gain rather than a compromise.

Further, the paper is organized as follows: Section I provides introduction to our proposed work with an extensive analysis on QKD protocols and various Key Exchange Mechanisms (KEMs); Section II elaborates related works in this area; Section III provides a detailed discussion on proposed methodology with explanation about all the phases; Section IV discusses the results and challenges in the proposed work; Section V throws light on the benefits, challenges and threat to validity and finally Section VI concludes with the advantages of the proposed work and future research directions.

A. QKD PROTOCOLS - AN EXTENSIVE ANALYSIS

The most common QKD protocol, BB84, has been tested in real-world scenarios, such as securing fiber-optic cables over long distances. QKD provides 'future-proof' security, unlike software-based encryption, because it is based on physics, not just complex math. The BB84 protocol, developed in 1984, enables secure key exchange using quantum principles. Alice encodes random bits into photons polarized in one of two bases (rectilinear: 0° or 90°; diagonal: 45° or 135°) and sends them to Bob. Bob measures these photons in randomly chosen bases. After transmission, they publicly compare bases (not the actual bits), retaining only bits where the bases matched—a process called sifting. Any eavesdropping disrupts the photon states, exposing intrusion via elevated error rates. BB84's sifting step discards approximately 50% of transmitted bits due to mismatched bases. For example, if Alice sends 1,000 photons, only approximately 500 survive sifting (assuming random basis selection). This inefficiency doubles the required number of photon transmissions to achieve a target key length, putting a strain on bandwidth and energy resources.

Recent advancements that address this issue is the application of Predetermined Key Bit Positioning. PRNG-based basis alignment represents a significant advancement in addressing sifting inefficiencies in QKD protocols. This technique employs pseudo random number generators to predetermine the basis choices for both the sender and receiver, eliminating the need for post-transmission basis reconciliation [1]. But this approach has it's own set of disadvantages such as it requires precise synchronization of PRNG seeds between communicating parties. It may introduce security vulnerabilities if the PRNG implementation is compromised. It requires additional computational resources for PRNG operations and security proofs may need revision to account for non-random basis selection.

There is also Adaptive Basis Reconciliation, which dynamically adjusts the reconciliation process based on observed channel conditions and error patterns. However, this approach presents different challenges and drawbacks such as increase in computational complexity, It may require additional protocol overhead for adaptation mechanisms, the performance benefits may vary depending on channel characteristics and requires careful implementation to maintain security guarantees.

On the other hand Hybrid Discrete Variable-Continuous Variable (DV-CV) QKD protocols represent a significant advancement in addressing the fundamental limitations of both DV and CV approaches independently [2]. In the hybrid DV-CV implementation, the transmitter simultaneously performs discrete modulation-based encoding for the CV-QKD subsystem and time-phase encoding for DV-QKD. This approach allows for efficient utilization of photons, addressing the inefficiency of discarding bits in traditional protocols. However, similar to other algorithms, it increases system complexity requiring both DV and CV components, more sophisticated post-processing algorithms, higher implementation cost due to dual subsystems and requires precise calibration and synchronization between subsystems on top the added complexity.

Other significant advancements have produced hybrid encoder implementations that can efficiently toggle between discrete and continuous variable working modes. A notable innovation is the iPOGNAC modulator-based hybrid encoder, which ensures compatibility with both DV and CV-QKD systems using commercial-off-the-shelf components. This approach is particularly significant as it supports DV polarization protocols, making it an appealing candidate for space nodes in future quantum networks [3]. It's disadvantages requires more complex modulation hardware, it introduces additional sources of errors during mode switching, Higher power consumption compared to single-mode systems and calibration must be maintained for both operational modes.

These optimizations are critical for underwater deployments, where experimental BB84 implementations already operate at marginal key rates, such as 563 kbps in lab settings, which may be inadequate for practical applications. Without these improvements, sifting inefficiencies could render underwater QKD impractical for real-time applications such as naval communications or seismic monitoring. Another notable protocol aimed at improving BB84's efficiency is B92, proposed by Bennett in 1992. The B92 protocol simplifies key distribution by using only two non-orthogonal quantum states instead of BB84's four. While this reduces the complexity of state preparation, it inherently yields a lower

key rate and is more susceptible to noise and specific types of attacks compared to BB84.

B. KEY ENCAPSULATION MECHANISMS - AN EXTENSIVE ANALYSIS

Key Encapsulation Mechanisms (KEMs) address the vulnerabilities of traditional key exchange methods by enabling secure transmission of cryptographic keys even in quantum-threatened environments. Alice generates a random symmetric key in a KEM-based system and securely ''encapsulates'' it using Bob's publicly available encryption parameters. This process produces a ciphertext—a scrambled version of the key—that Alice transmits to Bob. Bob then ''decapsulates'' the ciphertext using his private key to recover the original symmetric key. Unlike classical methods such as Diffie-Hellman or RSA, which rely on integer factorization or discrete logarithm problems vulnerable to quantum attacks, modern KEMs leverage mathematical frameworks believed to resist both classical and quantum computational assaults.

The U.S. National Institute of Standards and Technology (NIST) initiated a multi-year standardization process to identify quantum-resistant algorithms, culminating in the 2022 selection of four KEM finalists from over 80 submissions. These include CRYSTALS-Kyber, NTRU, SABER, and Classic McEliece, each grounded in distinct mathematical foundations. Kyber and SABER rely on variants of the Learning With Errors (LWE) problem, which involves solving noisy linear equations—a task proven intractable for quantum algorithms. NTRU, first proposed in 1996, employs polynomial ring-based equations, while Classic McEliece uses error-correcting codes, a methodology unbroken since its 1978 inception. NIST prioritized these algorithms due to their rigorous security proofs, extensive cryptanalysis, and performance benchmarks across diverse hardware platforms.

Kyber emerged as NIST's primary recommendation due to its optimal balance of security and efficiency, with key sizes under one kB and encryption speeds comparable to classical RSA. Classic McEliece, despite its bigger 260 kB public keys, was retained as a backup standard due to its unparalleled resistance to cryptanalytic attacks. NTRU and SABER serve as alternatives, offering hardware-friendly designs and decades of security analysis. NIST's selection criteria emphasized crypto-agility—the ability to adapt if vulnerabilities emerge—ensuring interoperability in systems like underwater networks, where infrastructure updates are logistically challenging.

II. RELATED WORK

Bennett and Brassard [4] used quantum cryptography to propose a novel algorithm for coin tossing, in which the two participants would exchange quantum messages. Known as the BB84 algorithm, they demonstrated how messages cannot be read by even a third party with unlimited computing power. However, these messages cannot be amplified, making them unusable for long-distance communication. Also, the participants could cheat in the exchange by applying the Einstein–Podolsky–Rosen(EPR) paradox. Ekert [5] extended their theorem by applying the generalized Bell's Theorem to the key distribution process. Here, he used the EPR paradox to prove the security of the proposed encrypted key. However, it still suffered challenges over long-distance communications and potential loss of data noise or losses in the quantum channel.

Scarani et al. [6] reviewed the security of quantum key distribution. In their analysis, they provided a detailed analysis of the various protocols used in QKD, including BB84, continuous variable, and distributed reference phased protocols. They emphasize that it is the first information task to have reached technological maturity, allowing it to be used commercially. They also speak about the current challenges, such as the difficulty of scaling up a network or the vulnerability to side-channel attacks.

Xu et al. [7] have analyzed the security of QKD from a real-world perspective. They attempted to find out how practical it is to apply QKD in practice and explored the application's vulnerabilities and challenges due to device limitations. While algorithms such as Measurement-Device-Independent QKD (MDI-QKD) and Twin-field QKD are significantly more robust and practically viable, the adoption of these protocols is severely limited due to the lack of hardware.

Eisaman et al. [8] provided a detailed analysis of various single photon sources and detectors. Sources generate photon particles, while detectors detect and analyze photon particles with high accuracy and precision. These devices are crucial for generating quantum encrypted messages, and improving their efficiency and scalability would have a direct effect on improving quantum communication technology.

Khalid et al. [9] tried to analyze the viability of lattice-based cryptographic protocols in IoT device networks. They tested and evaluated various lattice-based networks on embedded devices and benchmarked them against various metrics to ensure a fair result. They found that different protocols offer different advantages. Kyber and Saber offered an excellent trade-off in memory usage, security, and latency. Others, like FrodoKEM, offer higher security, but the large key sizes make them less suitable for practical applications.

Key Encapsulation is a secure exchange of symmetric keys between two parties in a communication system. Attempts have been made to secure this exchange from quantum attacks. In their paper, Bos et al. [10] introduced KYBER, a key encapsulation method that is secure against both classical and quantum attacks. Its security is based on Model-LWE(Learning with Errors), a complex problem in lattice-based cryptography. The researchers measured the efficiency of their algorithms and showed that the algorithm outperforms other existing schemes, such as NewHope and Frodo, in benchmark testing. However, it suffers from challenges such as complex implementations. Also, the key and ciphertext size is larger than that of other traditional systems like RSA. This makes the algorithm impractical in bandwidth-constrained environments.

Alkim et al. [11] presented NewHope as a lattice-based cryptographic measure to guard against quantum attacks in the TLS layer. The authors improved Peikart's Ring-LWE-based key exchange while keeping it robust against quantum attacks. The algorithm was designed with practical implications, but the reliance on optimization measures such as NTT and polynomial arithmetic made it unviable for resource-constrained environments.

Hoffstein et al. [12] presented NTRU, a public key cryptographic system built using a lattice-based cryptographic system. Like other lattice-based systems, the scheme is resistant to quantum-based attacks. In addition, its small key sizes and computationally efficient operations make it suitable for resource-constrained environments. However, encrypted messages can be longer than plaintexts, making the scheme unviable for bandwidth-constrained environments.

Diamanti et al. [13] explored the challenges of quantum key distribution practically. QKD systems are slower than conventional cryptographic systems in key generation, thus leading to a slower key rate. Also, while the protocols are theoretically secure, malicious actors in the real world can target the vulnerabilities in detectors or hardware to crack the ciphertext. They concluded by listing the various advances and avenues which are being currently explored to make QKD protocols easier to implement in real-world situations.

Another quantum-proof cryptographic scheme is FrodoKEM (Alkim et al. [14]), which, unlike KYBER, uses unstructured lattices for key Encapsulation. This makes it secure against attacks that exploit the mathematical properties of structured lattices. The scheme is also viable for hardware implementation since significant advancements have been made in matrix-multiplication architectures. However, the size of ciphertexts is significantly larger than that of other algorithms.

Boyer et al. [15] explored the possibility of a semi-quantum key distribution protocol. In the experiment, one participant used classical means to encrypt the data, while the other party possessed quantum capabilities. They proved that the protocol is completely robust, making it ideal for resource-constrained (for example, IOT or embedded systems) devices and environments.

Weedbrook et al. [16] have done a comprehensive analysis of Gaussian continuous-variable quantum information processes. They have given a detailed description of the various QKD continuous-variable protocols and have also performed security analysis on these protocols by simulating various Gaussian attacks. The authors concluded the section by listing areas where further research and innovation are required. However, there is no analysis of non-gaussian processes.

Bonato et al. [17] explored the feasibility of applying QKD between a ground station and a (low-key orbiting) satellite. This is a complex task since atmospheric noise, radiation, and different attenuation levels at the ground station and satellite levels make communication difficult. The study experimented with BB84, BB84 decoy state, and Ekert91 (entanglement-based). BB84 displayed the best results out of the three, with a secure key rate of 1 kbit/s for a satellite at 500-600 km.

There are few large-scale implementations of quantum key distribution. One such implementation is SwissQuantum, whose performance over 21 months is analyzed by Stucki et al. [18]. The network consisted of three nodes, Unige, CERN, and hepia, which were linked via three point-to-point QKD links. These devices were running under SARG, a variant of the BB84 protocol. While the long-term deployment proved the reliability and robustness of QKD for the real world, there were no mentions of any vulnerability tests against side-channel attacks, which malicious actors can utilize to hijack communications.

Pirandola et al. [19] reviewed the available literature comprehensively and described the current advances in quantum cryptography in their work. They gave a detailed analysis of various protocols, including device-independent QKD and hybrid protocols, along with their security proofs. They also mentioned the key areas where improvement is needed, such as scalability, implementation complexity, etc.

In recent times, there have been various advancements in the field. Li et al. [20] achieved a secret key rate (SKR) of 115.8 Mb/s over a range of 10 km. They were also able to extend the range of the communication to over 328 km. However, it was possible due to ultra-low-loss fibre cables. These cables were made of superconducting materials, making them unsuitable for real-world deployment. Liu et al. [21] performed a Twin-Field Quantum Key Distribution (TF-QKD) over 1002 km of optical fibre. However, with a low secret key rate and very sensitive infrastructure, it is unviable for real-world deployment. Nevertheless, it demonstrated the possibility of using QKD for long-distance communication shortly.

Vazirani and Vidick [22] presented an entanglement-based QKD protocol that is fully independent of the hardware devices it operates on. This makes the protocol immune to any hardware tampering, thus enhancing communication security. As a trade-off, the protocol has lower key rates than device-dependent protocols. It demands more advanced technologies like high-quality entangled photon sources and precise detection systems.

Chen et al. [23] constructed a 46-node quantum network in the metropolitan city of Hefei, China. The intended purpose was to test if Quantum Key Distribution is viable in urban settings. Operating on BB84 protocol, the system functioned continuously for 31 months. They managed to integrate it with other existing technologies and were still able to maintain flexibility for different user requirements.

A. RESEARCH PROBLEM AND CONTRIBUTION OF THE RESEARCH WORK

The standard BB84 protocol suffers from inherent inefficiencies in its sifting process. Alice and Bob must discard approximately 50% of all transmitted qubits due to basis mismatch. In this process, both parties publicly compare

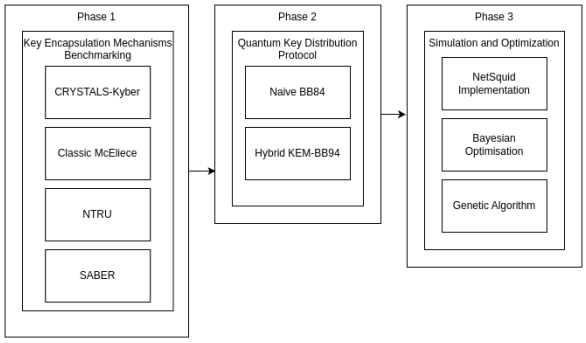

FIGURE 1. Overview of the proposed methodology.

their randomly chosen measurement bases, retaining only the bits where their bases aligned—typically only half of the transmitted bits. This fundamental inefficiency represents significant resource wastage, particularly problematic in resource-constrained environments such as underwater channels.

Key Encapsulation Mechanisms (KEMs) represent a promising avenue for enhancing the BB84 protocol's efficiency. KEMs are cryptographic protocols that allow two parties to securely establish a shared secret key over a public channel through three primary algorithms: key generation, encapsulation, and decapsulation. The proposed research investigates how incorporating KEM principles into the BB84 protocol could fundamentally redesign the sifting process, potentially eliminating or substantially reducing the 50% resource wastage.

The specific research question becomes ''How can the incorporation of KEMs in BB84 overcome the inefficiencies associated with sifting, and what is the impact on the protocol's performance and maximum distance?''

Moving forward to our simulation, we also tackle maximizing Protocol distance between 2 nodes. To address the problem, we need some optimization algorithms. Genetic Algorithms (GAs) and Bayesian Optimization (BO) are employed for their complementary strengths in addressing complex optimization challenges. GAs excels in global search across high-dimensional, noisy, or non-differentiable problem spaces through population-based evolution, leveraging mutation and crossover to avoid local optima. BO, by contrast, prioritizes sample efficiency in low-dimensional spaces using probabilistic surrogate models and acquisition functions, making it ideal for expensive-to-evaluate functions. While GAs handle discrete variables and constraints robustly but require extensive computational resources, BO rapidly converges in moderate dimensions but struggles with scalability. We choose these contrasting algorithms as the dimensions of the problem have not been specified yet.

III. PROPOSED METHODOLOGY

The proposed methodology consists of three distinct phases: The first phase is Key Encapsulation Mechanisms Benchmarking. This phase involves evaluating and benchmarking various post-quantum cryptographic algorithms to assess their performance and security. The mechanisms considered include:

- **CRYSTALS-Kyber**: A lattice-based algorithm known for its efficiency and strong security guarantees.
- **Classic McEliece**: Based on code-based cryptography, offering long-standing security.
- **NTRU**: Another lattice-based algorithm with a focus on performance and compactness.
- **SABER**: A lattice-based mechanism emphasizing simplicity and efficiency.

The second phase focuses on BB84. In this phase, quantum key distribution (QKD) protocols are explored to ensure secure communication in the presence of quantum threats. The tasks include:

- **Naive BB84**: Implementation of the BB84 protocol, which is a foundational QKD method based on quantum mechanics principles.
- **Hybrid KEM-BB84**: Integration of post-quantum key encapsulation mechanisms (KEMs) with the BB84 QKD protocol for enhanced security.

The last phase includes Simulation and Optimization. This phase focuses on simulating the quantum protocols and optimizing their performance using advanced computational techniques:

- **NetSquid Implementation**: Simulating the naive and our Hybrid KEM-BB84 protocol using NetSquid, a specialized platform for modeling quantum systems.
- Optimization and comparison between Bayesian Optimization and Genetic Algorithm for finding the maximum distance between 2 nodes.

A. PHASE 1: COMPARATIVE ANALYSIS AND IMPLEMENTATION OF KEY ENCAPSULATION MECHANISMS

In the first phase of the study, we will compare the algorithms selected by the Post-Quantum Cryptographic (PQC) standardization process held by National Institute of Standards and Technology (NIST) [24] in terms of their speed. NIST defines security levels for cryptographic algorithms in terms of the computational resources required to break them, allowing for standardized comparison between different approaches. These levels are anchored to the security strengths of well-established symmetric cryptographic primitives, which are considered relatively resistant to quantum attacks compared to their asymmetric counterparts mentioned in the Table 1. The formal security proofs of each KEM algorithm are presented in the research works [12], [25], [26], [27], [28], [29].

The finalist of round 3 that was selected for standardization at the end of round 3 was CRYSTALS-Kyber [25]. Besides CRYSTALS-Kyber, some algorithms including Classic McEliece, NTRU and SABER were identified for further evaluation in round 4. These algorithms were designed for

TABLE 1. Security levels comparison.

Security Level	Reference Algorithm	Classical Security (bits)	Quantum Security (bits)
Level 1	AES-128	128	64
Level 2	SHA3-256	128	85
Level 3	AES-192	192	96
Level 4	SHA3-384	192	128
Level 5	AES-256	256	128

secure key encapsulation against both classical and quantum attacks.

1) CRYSTALS-KYBER

CRYSTALS-Kyber is a lattice-based KEM cryptographic protocol that offers security from chosen ciphertext attacks (CCA) and chosen plain text attacks (CPA) [10]. Based on the mathematical hardness of the Learning with Errors problem(LWE), it offers more efficient key size and computational efficiency against other similar algorithms such as NEWHOPE. The key equations of Kyber are given below:

Key Generation:

The public key is computed as:

$$t = \text{Compress}_q\left(A \cdot s + e\right) \tag{1}$$

where:

- $A \in \mathbb{R}_q^{\kappa \times \kappa}$ is a public matrix deterministically generated from seed ρ.
- $s, e \in \mathbb{R}_q^{\kappa}$.
- t is a public key component.
- q is a large modulus.

Encapsulation:

The ciphertext components are:

$$u = \text{Compress}_q\left(A^T \cdot r + e_1\right) \tag{2}$$

$$v = \text{Compress}_q\left(t^T \cdot r + e_2 + \left\lfloor \frac{q}{2} \right\rfloor \cdot m\right) \tag{3}$$

where:

- r, e_1, e_2 are noise polynomials sampled using a hash of the message m.
- u, v are ciphertext components. The pair (u, v) is the ciphertext sent to the recipient.
- m is an encoded random message.

Decapsulation:

Recover the message using:

$$m' = \text{Decompress}_q\left(v - s^T \cdot u\right) \tag{4}$$

where:

- m' is the decrypted message.
- $s \in \mathbb{R}_q^{\kappa}$ is the secret key.

To prevent attacks (CCA), the receiver verifies the message, i.e., Bob re-encrypts the decrypted message m. If the computed ciphertext matches the ciphertext sent by Alice, then he proceeds to derive the shared key.

$$\text{If } (u', v') = \text{ReEnc}(m') \tag{5}$$

$$K = H\left(\hat{K}, H(c)\right) \tag{6}$$

If they do not match, then Bob generates a pseudo-random key, which uses a fallback value z instead of K, having no relation with Alice's key.

$$\text{Else If } (u', v') \neq \text{ReEnc}(m') \tag{7}$$

$$K = H\left(z, H(c)\right) \tag{8}$$

2) CLASSIC MCELIECE

The Classic McEliece cryptosystem distinguished by its proven resistance to quantum attacks and reliance on the NP-hard decoding problem for general linear codes [26], [27]. As a conservative choice for standardization, it employs binary Goppa codes in its Niederreiter variant to achieve IND-CCA2 security while addressing historical concerns about key sizes through parameter optimization. Its mathematical foundation combines algebraic coding theory with randomized error vectors to create a lattice-based alternative vulnerable only to classical information-set decoding attacks. The Key generation, Encapsulation and Decapsulation Equations are given below.

Key Generation:

1) Generate a uniform random seed $\delta \in \mathbb{F}_2^l$ (a random bitstring of length l).
2) Use a SHAKE256-based pseudo-random generator $G(\delta)$ to derive:
   a) A bitstring $s \in \mathbb{F}_2^n$.
   b) A Goppa polynomial $g(x) \in \mathbb{F}_q[x]$ of degree t.
   c) A sequence of distinct field elements $\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_q$.
3) Form the Goppa code: $\Gamma = (g, \alpha_1, \ldots, \alpha_n)$.
4) Compute the matrix reduction via the algorithm MatGen to obtain a parity-check matrix in systematic form, i.e.,
$$H = (I_{n-k} \mid T)\,.$$
5) Output:
   - Public key: pk $= T$.
   - Private key: sk $= (\delta, c, g, \alpha, s)$.

Encapsulation:

Given the public key T:

1) Generate a random error vector $e \in \mathbb{F}_2^n$ of weight t using FixedWeight().
2) Compute $C_0 = \text{Encode}(e, T)$.
3) Compute $C_1 = H(2, e)$ using a SHAKE256-based hash.
4) Form the ciphertext $C = (C_0, C_1)$.
5) Derive the shared session key: $K = H(1, e, C)$.

Output: ciphertext C and shared key K.

Decapsulation:

Given ciphertext $C = (C_0, C_1)$ and private key sk:

1) Split C into $C_0 \in \mathbb{F}_2^{(n-k)}$ and $C_1 \in \mathbb{F}_2^l$.
2) Set a flag $b \leftarrow 1$.

3) Extract $s \in \mathbb{F}_2^n$ and the permuted code description $\Gamma' = (g, \alpha'_1, \ldots, \alpha'_n)$ from sk.
4) Compute $e = \text{Decode}(C_0, \Gamma')$. If decoding fails (i.e., $e = \perp$), set $e \leftarrow s$ and $b \leftarrow 0$.
5) Recompute $C'_1 = H(2, e)$. If $C'_1 \neq C_1$, set $e \leftarrow s$ and $b \leftarrow 0$.
6) Derive the session key: $K = H(b, e, C)$.

Output: session key K.

3) NTRU

NTRU is a public-key cryptosystem that is based on polynomial algebra and the mathematical properties of convolution in difficulty to break the key encryption [12]. This allows it to reduce key sizes in comparison to other protocols such as RSA or ECC. In addition, the lack of dependence on factoring makes it resistant to common quantum-based attacks such as Shor's Algorithm. The key equations of NTRU are given below:

Key Generation:
The user selects two polynomials, f and g from $\mathcal{L}_g$. Then their inverses will be calculated with respect to q and p, denoted as:

$$F_q \otimes f \equiv 1 \pmod{q} \tag{9}$$
$$F_p \otimes f \equiv 1 \pmod{p} \tag{10}$$

Then, the user computes:

$$h \equiv F_q \otimes g \pmod{q} \tag{11}$$

Encryption:

$$e \equiv p\phi \otimes h + m \pmod{q} \tag{12}$$

where:

- m is the message.
- ϕ is a randomly chosen polynomial for encryption.
- p is a small integer used to ensure correct decryption.
- e is the encrypted message.

Decryption:

$$a \equiv f \otimes e \pmod{q} \tag{13}$$

where:

- a is an intermediate value.
- f is the private key.

$$m \equiv F_p \otimes a \pmod{p} \tag{14}$$

where:

- m is the recovered message.

4) SABER

SABER [28], [29] is a structured lattice-based key encapsulation mechanism (KEM). It is based on the Module Learning With Rounding (Mod-LWR) problem - a deterministic variant of the Learning With Errors (LWE) problem - it offers IND-CCA2 security while optimizing for implementation efficiency. The key equations of NTRU are given below:

Key Generation:
The public key is computed as:

$$b = \text{bits}(A \cdot s + h, \bar{q}, \bar{p}) \mod p \tag{15}$$

where:

- $A \in \mathbb{R}_q^{l \times l}$ is the public matrix generated using SHAKE-128 from a seed.
- $s \in \mathbb{R}_q^{l \times 1}$ is the secret vector sampled from a centered binomial distribution β_μ.
- h is a fixed rounding constant vector.
- The result is compressed from modulus q to p via bit extraction.

The public key is:

$$\text{pk} = (\text{seed}_A, b) \tag{16}$$

The secret key is:

$$\text{sk} = (s, z, \text{pkh}) \tag{17}$$

where:

- $z \in \{0, 1\}^{256}$ is a random string.
- $\text{pkh} = F(\text{pk})$ is a hash of the public key.

Encapsulation:
The key encapsulation process is as follows:

$$m \leftarrow \{0, 1\}^{256} \tag{18}$$
$$(\hat{K}, r) = G(F(\text{pk}), m) \tag{19}$$
$$c = \text{Saber.PKE.Enc}(\text{pk}, m; r) \tag{20}$$
$$K = H(\hat{K}, c) \tag{21}$$

where:

- G: SHA3-512-based hash function deriving both encapsulation randomness and pre-key.
- H: SHA3-256-based function which derives the shared key.
- c: Ciphertext encapsulating message m.
- K: Final shared key.

Decapsulation:
The key decapsulation process is as follows:

$$m' = \text{Saber.PKE.Dec}(\text{sk}, c) \tag{22}$$

Here, the plain-text message m' is derived by decrypting the ciphertext c using the secret key (sk) using Saber's Public-Key Encryption (PKE) Scheme. The retrieved message m' is combined with the hashed public key (pkh) and fed into a hash function G.

$$(\hat{K}', r') = G(\text{pkh}, m') \tag{23}$$

The hashed function G outputs two values: an intermediate secret key $\hat{K}'$, and a random value r', which is used for re-encryption in the next step.

$$c' = \text{Saber.PKE.Enc}(\text{pk}, m'; r') \tag{24}$$

Using the previously obtained values, the obtained plain-text is re-encrypted using the Saber Public-Key Encryption

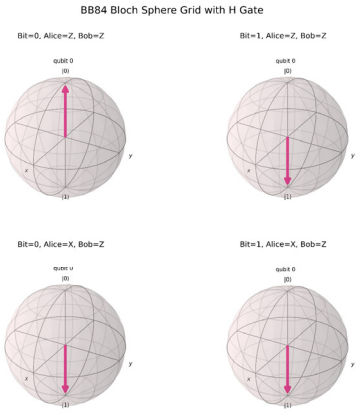

FIGURE 2. BB84 Bloch sphere with H gate.

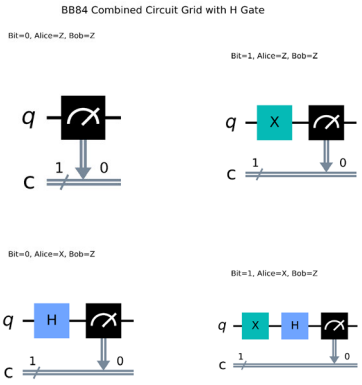

FIGURE 3. BB84 combined circuit with H gate.

scheme. The output c' is compared with the original ciphertext for consistency.

The consistency of the ciphertext is verified by re-encryption:

$$\text{If } c = c' \Rightarrow K = H(\hat{K}', c) \text{ else } K = H(z, c) \tag{25}$$

B. PHASE 2: ENHANCEMENT OF THE BB84 PROTOCOL USING KEMS

The BB84 protocol is the foundational quantum key distribution (QKD) method for securely exchanging cryptographic keys between two parties named Alice and Bob over a quantum channel. Its security relies on principles of quantum mechanics, making it theoretically immune to computational attacks, even by quantum computers. Fig.2 denotes the Bloch grid formed by the superposition caused by the H gates. Fig.3 represents the circuit grid for each possible combination.

The BB84 security derives from two quantum principles, Heisenberg Uncertainty Principle- Measuring a quantum state disturbs it unless the correct basis is used. Eavesdroppers introduce detectable errors by guessing bases incorrectly and No-Cloning Theorem- Eavesdroppers cannot perfectly copy unknown quantum states, preventing undetected interception. The below algorithm illustrates the brief overview of BB84.

1) **Initialization**
   - Alice and Bob agree on two orthogonal bases:
     - **Rectilinear basis** (+): 0° (bit 0) and 90° (bit 1).
     - **Diagonal basis** (×): 45° (bit 0) and 135° (bit 1).
2) **Key Generation and Encoding**
   - Alice generates two random binary strings:
     - **Data bits** (a): A sequence of n bits (e.g., 0101…).
     - **Basis selection bits** (b): A sequence of n bits determining the encoding basis for each data bit ($0 = +, 1 = \times$).
   - For each bit a_i, Alice prepares a photon polarized in:
     - 0° or 90° if $b_i = 0$.
     - 45° or 135° if $b_i = 1$.
3) **Quantum Transmission**
   - Alice transmits the encoded photon sequence to Bob via a quantum channel (e.g., optical fiber).
4) **Measurement**
   - Bob generates a random basis selection string (b') and measures each photon using his chosen basis (+ or ×).
   - Bob records results as raw key bits (a').
5) **Sifting**
   - Alice and Bob publicly compare b and b' via a classical channel.
   - They retain only bits where $b_i = b'_i$, discarding mismatched bases. The remaining bits form the sifted key.

We propose that a KEM encapsulate the basis Alice chose to be quantum attack resistant and then send these to Bob for decapsulation, eliminating the need for sifting and discarding bits. The security of KEM, especially CRYSTALS-Kyber, stems from its foundation in lattice-based cryptography, specifically the Module Learning With Errors (M-LWE) problem, a variant of the Learning With Errors (LWE) problem. This mathematical framework is believed to resist attacks from classical and quantum computers. The modified KEM-BB84 algorithm is defined below:

1) **Initialization**
   - Alice and Bob agree on two orthogonal bases:
     - **Rectilinear basis** (+): 0° (bit 0) and 90° (bit 1).
     - **Diagonal basis** (×): 45° (bit 0) and 135° (bit 1).
2) **Key Generation and Encoding**
   - Alice generates two random binary strings:
     - **Data bits** (a): A sequence of n bits (e.g., 0101…).
     - **Basis selection bits** (b): A sequence of n bits determining the encoding basis for each data bit ($0 = +, 1 = \times$).
   - For each bit a_i, Alice prepares a photon polarized according to:

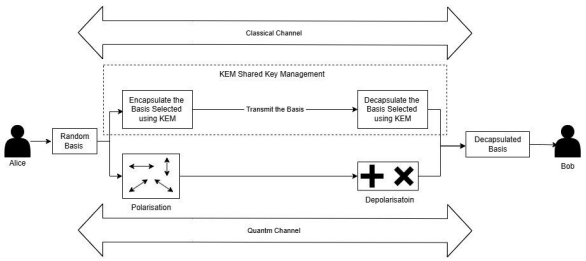

FIGURE 4. Hybrid KEM-BB84 proposed architecture.

- $0°$ or $90°$ if $b_i = 0$.
- $45°$ or $135°$ if $b_i = 1$.

3) **Basis Encapsulation**
- Alice encapsulates the basis using a Key Encapsulation Mechanism (KEM), in our case, CRYSTALS-Kyber.
- The encapsulated basis is transmitted to Bob.

4) **Quantum Transmission**
- Alice transmits the encoded photon sequence to Bob via a quantum channel (e.g., optical fiber).

5) **Decapsulation**
- Bob decapsulates the basis, obtaining the same basis as Alice.

6) **Measurement**
- Bob generates a random basis selection string (b') and measures each photon using his chosen basis ($+$ or $\times$).
- Bob records results as raw key bits (a').

7) **Sifting**
- Alice and Bob publicly compare b and b' via a classical channel.
- They retain only bits where $b_i = b'_i$, discarding mismatched bases. The remaining bits form the sifted key.

Based on the above algorithm, our proposed system architecture is illustrated in Fig.4.

C. PHASE 3: SIMULATION AND OPTIMIZATION

1) QUANTUM NETWORK SETUP

Without accessible quantum hardware, our research employs simulation tools to model and analyze quantum key distribution (QKD) protocols. Specifically, we utilize NetSquid to simulate quantum networks and liboqs from the Open Quantum Safe (OQS) project to implement quantum-resistant cryptographic algorithms.

NetSquid (Network Simulator for Quantum Information using Discrete events) is a discrete-event simulation platform designed to model and simulate scalable quantum networks and modular quantum computing systems. It is used here to simulate a quantum network consisting of two nodes (Alice and Bob). This network includes bidirectional classical and quantum channels from Alice to Bob. The quantum channel is simulated as a fiber optic link between Alice and Bob. The transmission delays are modelled using the FiberDelayModel, while the signal attenuation is accounted for through the FiberLossModel.

OQS's liboqs is an open-source C library that implements various quantum-resistant cryptographic algorithms, including support for key exchange mechanisms and digital signature schemes for quantum-resistant algorithms. We use a Python wrapper of this library to implement CRYSTALS-Kyber.

2) PROTOCOL IMPLEMENTATION

AliceProtocol()

The node Alice generates a random bit string and randomly assigns bases (either X or Z) to each character. These bases are converted into a byte array and then encrypted using Bob's public KYBER key. The encrypted bases are then transmitted via the classical channel, using the corresponding Kyber encapsulated key for Bob to decapsulate. For each bit, the Hadamard operation is applied if the assigned basis is X (if Z, then no operation is applied, and the raw bit is transmitted). These transformed qubits are then sent over the quantum channel to Bob. The whole operation is repeated (up to MAX_RETRIES) if there is no acknowledgment signal from Bob in 1s. This is also called timeout further on in the optimization phase.

BobProtocol() – Using this, the protocol is initiated when Bob receives the encrypted bases and the KYBER encapsulated key. The protocol is initiated when Bob receives the encrypted bases and the KYBER encapsulated key. The node decapsulates the encapsulated key to retrieve the shared secret, which is then used to decrypt Alice's basis selection. Bob applies the Hadamard operation for each incoming qubit if the basis is X (otherwise ignored). It then measures the qubit in the correct basis. Then, it sends an acknowledgment signal to Alice for each successfully received bit.

3) SEARCH SPACE

In our parameter-optimization framework, whether employing a genetic algorithm or Bayesian Optimization, we define a search space comprising three key parameters:

1. Distance (d) – the maximum separation (in meters) between the two communicating nodes in an underwater quantum channel.

2. Timeout (t) – the allowable time window (in nanoseconds) for each qubit exchange before triggering a retry or abort condition.

3. Max Retries (r) – the number of attempts permitted when qubits fail to be received or measured accurately within the given time window.

Formally, we represent the search space S as:

$$S = \langle d, t, r \rangle \quad \text{where} \quad \begin{cases} d \in [d_{\min}, d_{\max}] \\ t \in [t_{\min}, t_{\max}] \\ r \in \mathbb{Z}^+ \cap [r_{\min}, r_{\max}] \end{cases} \tag{26}$$

4) GENETIC ALGORITHM

A Genetic Algorithm (GA) is a search heuristic that is inspired by the principles of natural selection and genetics in nature. It is widely used in optimization problems to find approximate solutions by mimicking evolutionary processes such as selection, crossover, and mutation. Here, we try to optimize the variable parameters (distance between the two parties, timeout and maximum retries per bit) in the experiment using the genetic algorithm. The condensed flow is illustrated in Fig. 5.

Each individual chromosome in the genetic algorithm represents a possible configuration of QKD parameters:

$$C = \langle d, t, r \rangle \tag{27}$$

where:

- $d \in [1, 200]$ km (inter-node distance)
- $t \in [1, 10^{10}]$ ns (timeout duration)
- $r \in \{1, 2, \ldots, 10\}$ (maximum retry attempts)

The initial population consists of 50 individuals, each with randomly generated values for d, t, and r, ensuring coverage of the entire parameter space. The fitness function evaluates how well the individual chromosome performs in terms of key agreement accuracy. The fitness function is defined as:

$$F(d, t, r) = \begin{cases} d & \text{if success rate} \geq 95\% \\ d \times \dfrac{\text{success rate}}{100} & \text{otherwise} \end{cases} \tag{28}$$

where the success rate is obtained via the avg_100_runs() function, which runs 100 simulations of the custom protocol and computes the percentage of successful key exchanges. To speed up fitness evaluations, multiprocessing was implemented, which reduces execution time through simultaneous evaluation of multiple chromosomes.

To ensure the best candidates propagate, we rank all individuals by their fitness and select the top 50% to act as parents for the next generation. We then implement the crossover by selecting two parents and swapping a portion of their genes at a random crossover point as depicted in Fig.6, thus allowing exploration of new combinations:

$$\begin{aligned} \text{Offspring}_1 &= \left(d_{\text{parent}_1}, t_{\text{parent}_2}, r_{\text{parent}_2}\right) \\ \text{Offspring}_2 &= \left(d_{\text{parent}_2}, t_{\text{parent}_1}, r_{\text{parent}_1}\right) \end{aligned} \tag{29}$$

For example, suppose we have two parents:

$$\text{Parent}_1 = \left(30, 5 \times 10^2, 10\right) \tag{30}$$

$$\text{Parent}_2 = \left(20, 7 \times 10^1, 5\right) \tag{31}$$

If the crossover point is chosen between the first and second gene, then:

Offspring 1 inherits the distance from Parent 1 but takes the timeout and max_retries from Parent 2:

$$(30, 7 \times 10^1, 5) \tag{32}$$

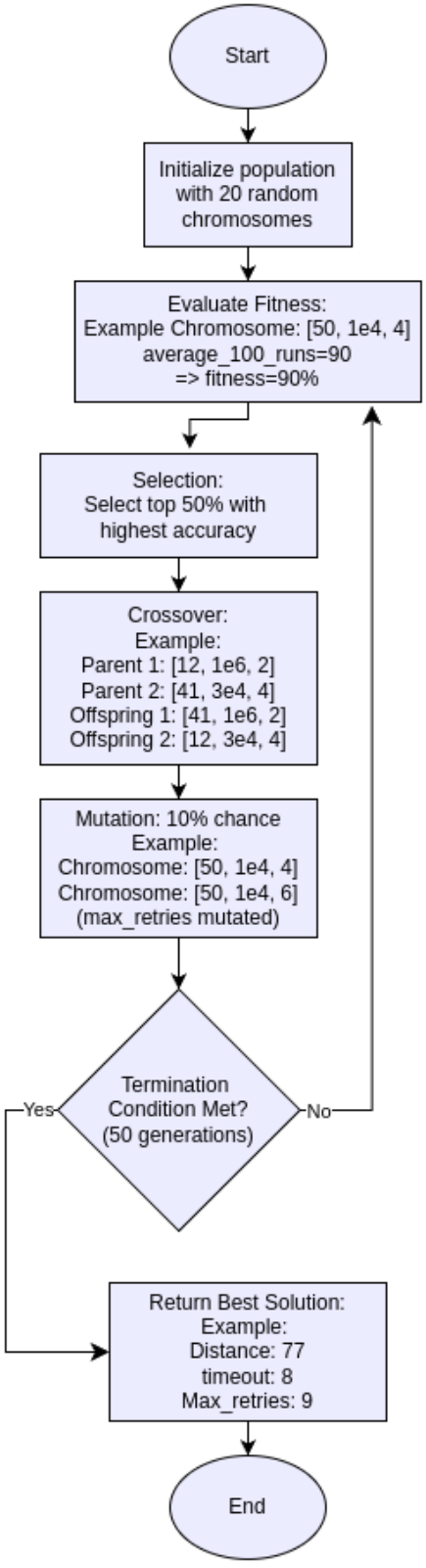

FIGURE 5. Genetic algorithm flowchart.

Offspring 2 inherits the distance from Parent 2 but takes the timeout and max_retries from Parent 1:

$$(20, 5 \times 10^2, 10) \tag{33}$$

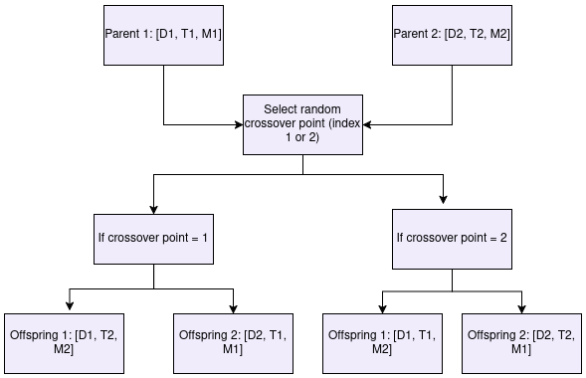

FIGURE 6. Cross over operation of genetic algorithm.

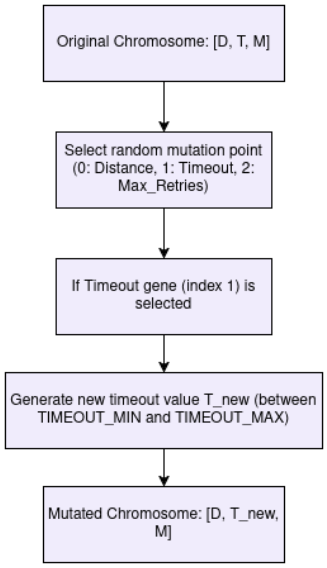

FIGURE 7. Mutation operation in genetic algorithm.

With a different crossover point (between the second and third gene), you would see a different swap pattern. We also enable a random mutation rate for 10% of the off-springs to maintain genetic diversity. This prevents the premature convergence of the parameters and encourages broader exploration of the search space as illustrated in Fig.7.

These equations describe how a new (mutated) value is chosen for each parameter in the genetic algorithm. The mutations can be represented as:

$$d_{\text{mutated}} = d_{\min} + \text{rand}\,(d_{\max} - d_{\min}) \tag{34}$$

The mutated distance thus lies between the maximum and minimum distance. Similarly for, the mutated time and the mutated logic.

$$t_{\text{mutated}} = t_{\min} + \text{rand}\,(t_{\max} - t_{\min}) \tag{35}$$

$$r_{\text{mutated}} = r_{\min} + \text{rand}\,(r_{\max} - r_{\min}) \tag{36}$$

In each case, the mutation step randomly resets that parameter to a new valid value in [min,max][min,max]. This preserves genetic diversity in the population and helps the genetic algorithm avoid converging prematurely on suboptimal solutions.

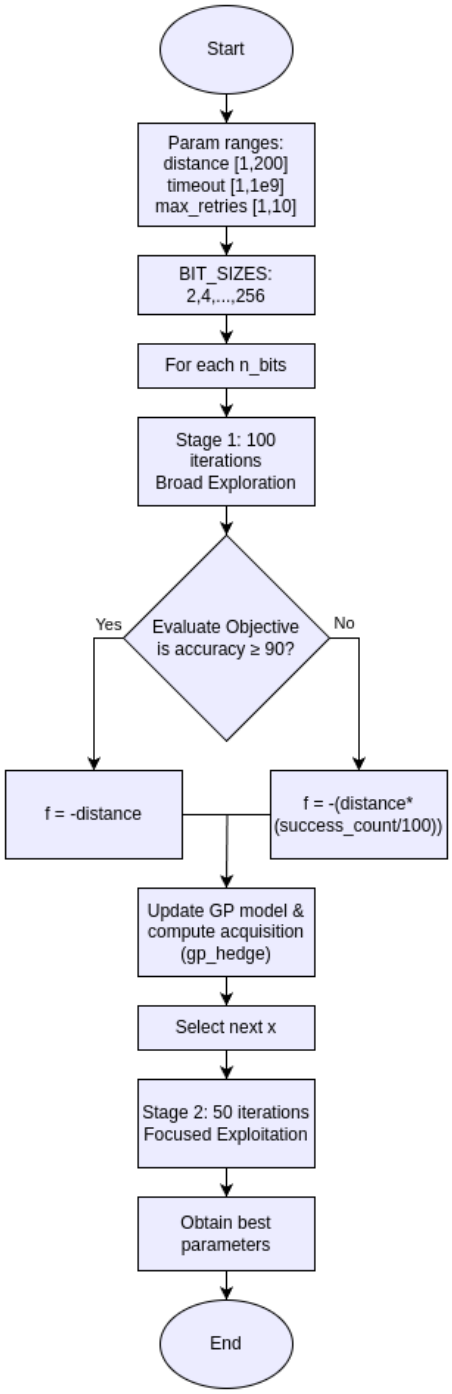

FIGURE 8. Bayesian optimization flowchart.

5) BAYESIAN OPTIMIZATION

Bayesian Optimization is a probabilistic approach used to efficiently find the maximum or minimum value of an objective function—typically one that's costly, noisy, or lacks a clear analytical form. We have applied the following to see if we are able to improve our results.

The three key parameters were the same that we used in genetic algorithm (distance, timeout, max retries). The search space is covered over:

$$S = \left\{(d, t, r) \mid d \in [1, 200],\ t \in [1, 10^9],\ r \in [1, 10]\right\} \tag{37}$$

where d, t, and r were optimized using a combination of log-uniform sampling (for distance and timeout) and integer sampling (for max retries).

In our study, we define a function $f(d, t, r)$ that returns a negative value because most solvers (e.g., `gp_minimize` in scikit-optimize) are designed to minimize an objective. To maximize distance, we take a negative sign. The objective function is defined as:

$$f(d,t,r) = \begin{cases} -d, & \text{if success rate} \geq 95\% \\ -d \times \left(\dfrac{\text{success rate}}{100}\right), & \text{otherwise} \end{cases} \tag{38}$$

where the success rate is obtained over an average of 100 iterations of the protocol and returning the percentage of successful key exchanges. The outline of the algorithm is defined in Fig.9.

IV. RESULTS AND DISCUSSION

A. CHALLENGES ADDRESSED AND EVALUATION FRAMEWORK

This subsection outlines the primary challenges targeted by the hybrid KEM-QKD protocol, the evaluation indicators used to assess resolution, and the methods for calculating these indicators. The framework is derived from the research problem and proposed methodology, focusing on inefficiencies in traditional BB84 and their mitigation through KEM integration and parameter optimization.

1) **Targeted Challenges:**
   - Inherent sifting inefficiency in BB84, where approximately 50% of transmitted qubits are discarded due to basis mismatch, leading to resource wastage in constrained environments like underwater networks.
   - Limitations in secure communication distance and performance in quantum networks, exacerbated by factors such as latency, attenuation, and computational overhead.
   - Need for efficient parameter optimization in high-dimensional, noisy spaces to maximize protocol distance between nodes.
2) **Evaluation Indicators:**
   - Key generation rate: Measures the percentage of retained bits post-transmission (target: 100% vs. BB84's 50%).
   - Maximum secure distance: The longest achievable distance between nodes while maintaining a success rate ≥95% over 100 simulation runs.

TABLE 2. Hardware components.

Hardware Component	Model/Specification	Manufacturer
Processor (CPU)	AMD Ryzen 7 4800HS	AMD
Graphics Processor Unit (GPU)	NVIDIA GeForce GTX 1650	NVIDIA
RAM	24 GB	Crucial Technology
Storage	1 TB NVMe SSD	SAMSUNG
Display	14" – 2560 x 1440	ASUS
Network Interface	MediaTek MT7921 Wi-Fi 6 Wireless Network Adapter	MediaTek, Inc.

TABLE 3. Software components.

Software Component	Version/Specification
Operating System	Arch Linux (2024.11.21-1)
Quantum Computing Framework	IBM Qiskit (0.43.0)
Simulation Software	Python (3.7.17)
KEM Libraries	Liboqs(0.12) and liboqs-python (0.12)
Development Environment	Visual Studio (1.98.2)
Version Control System	Git (2.49.0)

   - Computational efficiency: Latency in key generation, encapsulation, and decapsulation operations, benchmarked against NIST security levels.
   - Optimization convergence: Fitness scores from Genetic Algorithms (GA) and Bayesian Optimization (BO), including success rates and parameter stability.
3) **Calculation Methods:**
   - Key generation rate is calculated as (Retained bits / Total bits) × 100%, derived from NetSquid simulations comparing naive BB84 and hybrid KEM-BB84.
   - Maximum secure distance is optimized via GA (fitness as per Equation 28: d if success rate ≥95%, else d × (success rate / 100)) or BO (objective as -d if success rate ≥95%, else -d × (success rate / 100)), averaged over 30 runs with means $\pm n$ standard deviations.
   - Computational efficiency is computed as mean latency (in seconds) over 1000 repetitions per KEM variant, using liboqs benchmarks.
   - Resolution is confirmed if indicators show ≥95% success rate and improvements over baselines (e.g., 42% distance extension), with statistical reliability from repeated simulations.

B. EXPERIMENTAL SETUP

In our experimental methodology, all cryptographic benchmarks and simulation trials were repeated under the following specifications to guarantee statistical reliability.

Each KEM benchmark-for key-generation, encapsulation, and decapsulation latency-was executed 1000 times per variant, with the NumPy and Python RNGs reseeded (seed = 1493) at the outset of each script to ensure independence.

TABLE 4. Kyber variants specifications.

Kyber Variant	Public Key Size	Secret Key Size	Ciphertext Size	NIST Security Level
Kyber512	800 bytes	1632 bytes	768 bytes	1
Kyber768	1184 bytes	2400 bytes	1088 bytes	3
Kyber1024	1568 bytes	3168 bytes	1568 bytes	5

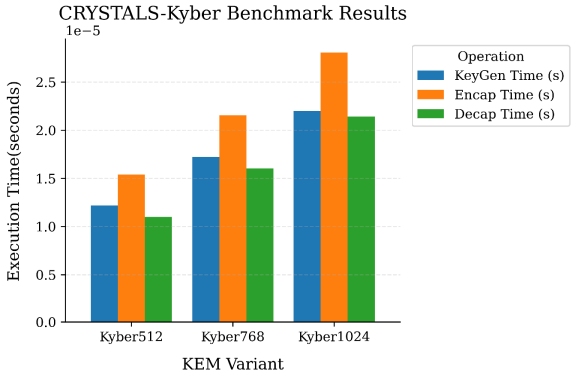

FIGURE 9. Performance analysis of CRYSTALS-Kyber variants.

TABLE 5. Kyber variant benchmarks results.

KEM Variant	KeyGen Time (s)	Encap Time (s)	Decap Time (s)
Kyber512	1.50×10^{-5}	1.60×10^{-5}	1.10×10^{-5}
Kyber768	1.80×10^{-5}	2.20×10^{-5}	1.60×10^{-5}
Kyber1024	2.30×10^{-5}	2.80×10^{-5}	2.10×10^{-5}

For the NetSquid-based hybrid KEM-BB84 protocol, every candidate parameter tuple evaluated by both the Genetic-Algorithm and Bayesian-Optimization frameworks was subjected to 100 independent simulation runs via the avg_100_runs routine, again reseeding before each run. The genetic and Bayesian optimization has 30 independent runs for each set of bits.

The Fiber testing script is also run 30 independent times. The reported values throughout the manuscript are expressed as arithmetic mean ± standard deviation over these repetitions.

C. PHASE 1 RESULTS

1) CRYSTALS-KYBER

Kyber has 3 different variants as mentioned in Table 4. Each variant has increasing NIST security level, Public Key size, Secret Key size, Ciphertext Size and Shared Secret Key size. All the KEM algorithm share the same secret key size which is 32 bytes. But with higher key sizes comes additional computation time as demonstrated in Fig. 9 and Table 5.

The Kyber Variant benchmarks results as shown in table 5, indicates that, the Kyber1024 has higher time than others due to the fact that it has higher key size of public key (1568 bytes), secret key (3168 bytes) and cipher text (1568).

TABLE 6. Classic McEliece variants specifications.

Classic McEliece Variant	Public Key Size	Secret Key Size	Ciphertext Size	NIST Security Level
348864 / 348864f	261,120 bytes	6,492 bytes	96 bytes	1
460896 / 460896f	524,160 bytes	13,608 bytes	156 bytes	3
6688128 / 6688128f	1,044,992 bytes	13,932 bytes	208 bytes	5
6960119 / 6960119f	1,189,888 bytes	14,592 bytes	232 bytes	5
8192128 / 8192128f	1,357,824 bytes	16,320 bytes	240 bytes	5

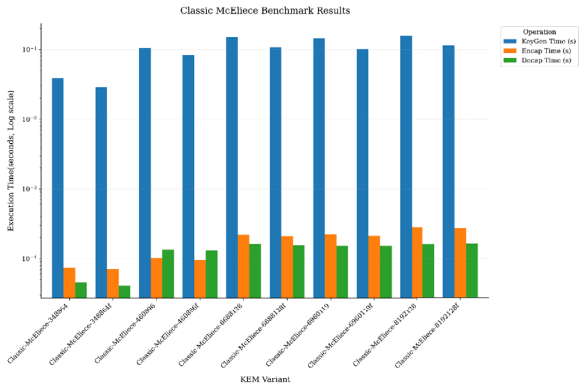

FIGURE 10. Performance analysis of classical McEliece variants.

2) CLASSIC MCELIECE

In the library liboqs, five different variants of Classic McEliece -quantum-safe key encapsulation mechanism (KEM) and digital signature algorithms are available as mentioned in Table 6.

Each variant has a 'f' version which uses Optimized Gaussian elimination with relaxed pivot conditions (32, 64) and higher success rates. The non-'f' variants use standard Gaussian elimination with stricter pivot conditions which lead to higher probability of key-generation failure, requiring multiple attempts.

Each variant has increasing NIST security level, Public Key size, Secret Key size, Ciphertext Size and Shared Secret Key size. But with higher key sizes comes additional computation time as demonstrated in Fig. 10 and Table 7.

3) NTRU

Compared to previous algorithms, NTRU only has a single variant in the liboqs library in Table 8. The average time of NTRU is mentioned in Fig. 11 and Table 8.

The benchmark results of NTRU based KEM variant is given in Table 9.

4) SABER

The SABER protocol uses three parameter sets (LightSaber, Saber, FireSaber). It is given in Table 10 with NIST security level of each variant.

TABLE 7. Classic McEliece benchmark results.

KEM Variant	KeyGen Time (s)	Encap Time (s)	Decap Time (s)
Classic-McEliece-348864	3.58×10^{-2}	4.60×10^{-5}	4.30×10^{-5}
Classic-McEliece-348864f	2.83×10^{-2}	3.70×10^{-5}	4.00×10^{-5}
Classic-McEliece-460896	1.06×10^{-1}	1.10×10^{-4}	1.35×10^{-4}
Classic-McEliece-460896f	8.35×10^{-2}	1.03×10^{-4}	1.35×10^{-4}
Classic-McEliece-6688128	1.52×10^{-1}	2.06×10^{-4}	1.50×10^{-4}
Classic-McEliece-6688128f	1.05×10^{-1}	2.00×10^{-4}	1.48×10^{-4}
Classic-McEliece-6960119	1.40×10^{-1}	2.07×10^{-4}	1.55×10^{-4}
Classic-McEliece-6960119f	1.01×10^{-1}	2.04×10^{-4}	1.43×10^{-4}
Classic-McEliece-8192128	1.58×10^{-1}	2.79×10^{-4}	1.53×10^{-4}
Classic-McEliece-8192128f	1.14×10^{-1}	2.85×10^{-4}	1.57×10^{-4}

TABLE 8. NTRU variant specifications.

NTRU Variant	Public Key Size	Secret Key Size	Ciphertext Size	NIST Security Level
sntrup761	766 bytes	842 bytes	766 bytes	2

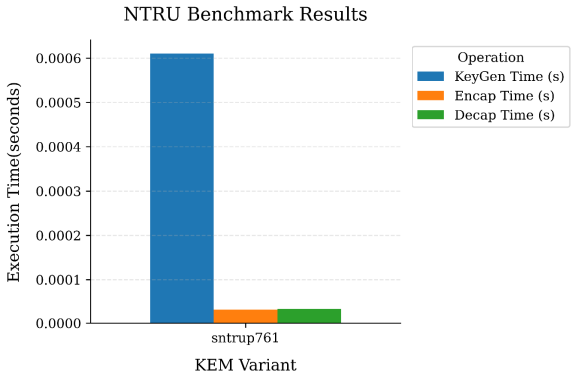

FIGURE 11. Performance analysis of NTRU variants.

TABLE 9. NTRU benchmark results.

KEM Variant	KeyGen Time (s)	Encap Time (s)	Decap Time (s)
sntrup761	3.10×10^{-4}	1.70×10^{-5}	1.70×10^{-5}

The average time of these parameters is mentioned in Fig. 12 and Table 11.

TABLE 10. Saber variants specifications.

Saber Variant	Public Key Size	Secret Key Size	Ciphertext Size	NIST Security Level
LightSaber	672 bytes	1,568 bytes	736 bytes	1
Saber	992 bytes	2,304 bytes	1,088 bytes	3
FireSaber	1,312 bytes	3,040 bytes	1,472 bytes	5

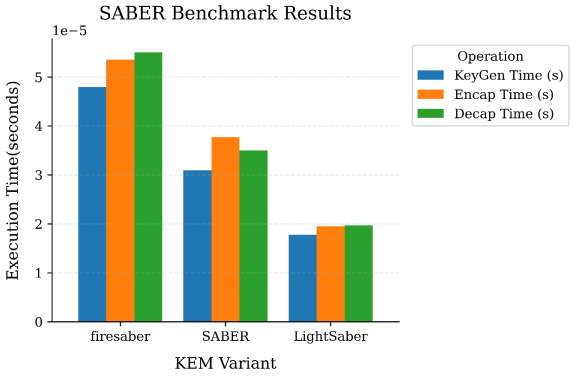

FIGURE 12. Performance analysis of SABER variants.

TABLE 11. Saber benchmark results.

KEM Variant	KeyGen Time (s)	Encap Time (s)	Decap Time (s)
FireSaber	4.79×10^{-5}	5.36×10^{-5}	5.50×10^{-5}
LightSaber	1.78×10^{-5}	1.95×10^{-5}	1.97×10^{-5}
SABER	3.09×10^{-5}	3.77×10^{-5}	3.50×10^{-5}

Further, the benchmark results of SABER variants is given in Table 11 provides the key generation time, Encapsulation time and Decapsulation time.

5) SUMMARY

CRYSTALS-Kyber, McEliece, NTRU and SABER are leading post-quantum cryptographic algorithms, each offering unique strengths. Since widespread quantum computers are not feasible yet, we will move forward with NIST Security level 1. Although the developed algorithms are compartmentalized and are swappable, for our demonstration we will go with the algorithm variant which is fastest i.e. CRYSTALS-kyber512 as observed in Table 12 and Fig. 13.

D. PHASE 2 RESULTS

The Table 13 and Fig. 14 denote the key rate vs distance graph made in ideal conditions i.e. no delay, no loss and a channel length of 1 meters to compare the algorithms head-to-head. We can conclude that we were able to improve and maintain 100% basis alignment via our improved KEM-BB84 algorithm and eliminate the need for sifting altogether.

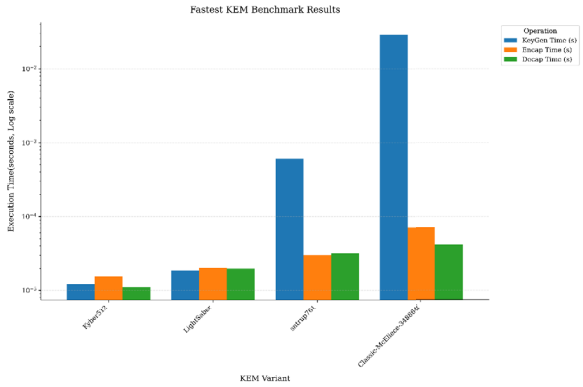

FIGURE 13. Performance analysis of all variants.

TABLE 12. KEM computational performance with NIST security level.

KEM Variant	KeyGen Time (s)	Encap Time (s)	Decap Time (s)	NIST Security Level
Kyber512	1.30×10^{-5}	1.50×10^{-5}	1.10×10^{-5}	1
LightSaber	1.78×10^{-5}	1.95×10^{-5}	1.97×10^{-5}	1
sntrup761	3.09×10^{-4}	1.60×10^{-5}	1.60×10^{-5}	2
Classic-McEliece-348864f	2.92×10^{-2}	6.90×10^{-5}	5.30×10^{-5}	1

TABLE 13. Key length efficiency comparison between naive BB84 and KEM-BB84 protocols.

Bits	Avg. Key Length (Naive BB84)	Avg. Key Length (KEM-BB84)
2	0.93	2.00
4	1.73	4.00
8	3.92	8.00
16	8.08	16.00
32	15.79	32.00
64	32.17	64.00
128	63.12	128.00
256	128.09	256.00

E. COMPUTATIONAL AND COMMUNICATION OVERHEAD ANALYSIS

In the Hybrid-KEM-BB84 protocol, each basis choice is encapsulated as a Kyber ciphertext (768 bytes for Kyber512) and transmitted over the classical channel, introducing a per-qubit classical communication overhead not present in standard BB84, which only requires 1 bit per basis for public reconciliation. For a session this results in a total classical overhead of 768 bytes. However, this increase in size is offset by the complete elimination of the sifting step, allowing all transmitted qubits to contribute to the final key and thus halving the required quantum transmissions. In underwater or high-latency environments, where quantum channel resources are far more constrained than classical bandwidth, this trade-off is favorable and enables practical deployment of QKD protocols at greater distances and higher key rates.

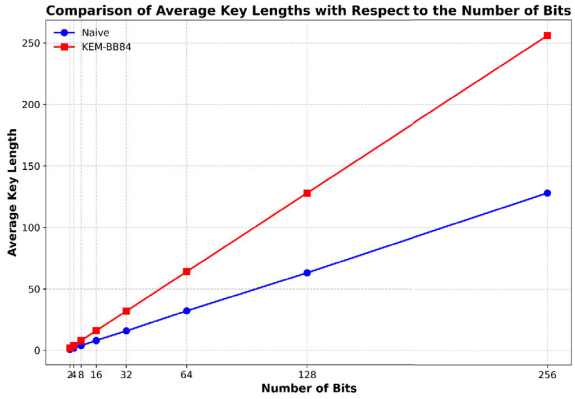

FIGURE 14. Comparison of average key length with respect to the number of bits.

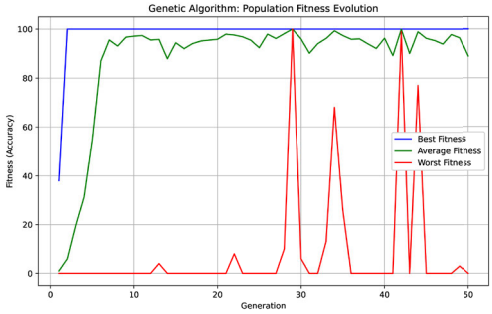

FIGURE 15. Genetic algorithm: Population fitness evolution.

F. PHASE 3 RESULTS

Fig. 15 shows the visualization of the fitness evolution over generations in the Genetic Algorithm, showing the progressive improvement of solutions. We can observe that the best fitness (blue line) starts and remains consistently high near 100% throughout all generations, indicating that excellent solutions are found early and preserved. The average fitness (green line) shows dramatic improvement in early generations (0-10), rising from approximately 10% to 90%, then stabilizing with fluctuations between 75-100%. The persistent fluctuations in worst fitness (red line) suggest the algorithm deliberately maintains diversity to avoid premature convergence and escape local optima. We can conclude that there appears to be a balance between exploitation (refining reasonable solutions) and exploration (trying new approaches). The narrowing gap between best and average fitness over time indicates adequate selection pressure driving population improvement. The periodic drops in worst fitness likely represent moments when new, exploratory individuals are introduced through mutation.

The convergence graph in Fig. 16 illustrates the progression of Bayesian optimization, showcasing the objective value (minimum f(x)) against the number of calls (n). The optimization process is divided into two stages: exploration and exploitation; the exploration runs for 300 runs. The first 100 points are the randomly sampled points for the initialization of the surrogate model. They are evaluated

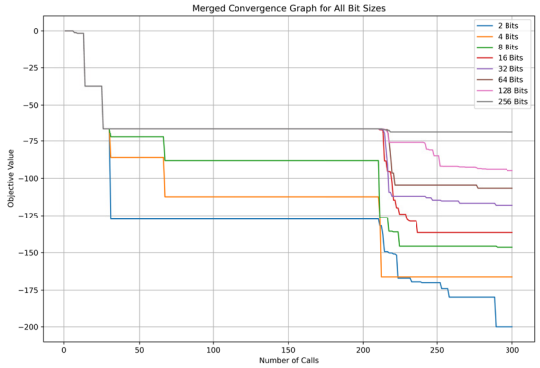

FIGURE 16. Optimization convergence with early stopping.

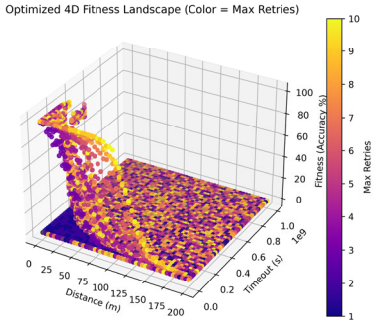

FIGURE 17. Fitness landscape visualization.

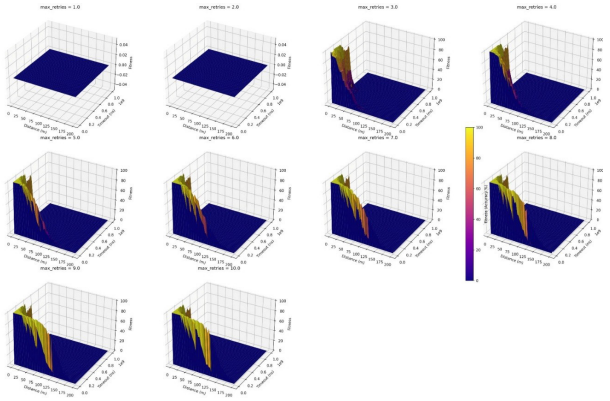

FIGURE 18. Fitness landscape by retry attempts.

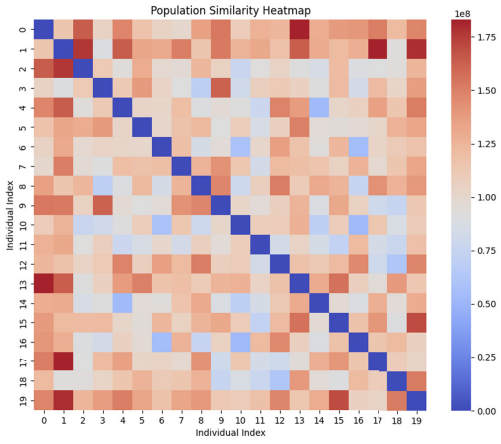

FIGURE 19. Population distribution heatmap.

before fitting the Gaussian Process. They also act as a burn-in period to prevent premature convergence to local minima. The following 100 iterations are for the exploration phase, and the final 100 for the exploitation phase.

In the exploration stage (up to n=100), the algorithm seeks to evaluate diverse regions of the search space, resulting in significant drops in the objective value as better solutions are discovered. After transitioning to the exploitation stage, the algorithm refines its search near promising regions identified earlier, leading to more minor but consistent improvements. The cumulative minimum curve demonstrates a steady convergence toward an optimal solution, with diminishing returns as n increases. This pattern reflects the efficiency of Bayesian optimization in balancing exploration and exploitation to achieve convergence within a limited number of function evaluations.

The Fig. 17 and 18 present a 4D fitness landscape that visualizes system performance for 32 bits across multiple parameters, using three spatial dimensions (distance, timeout, and fitness) and a color-coded fourth dimension (max retries).

The first image reveals that optimal performance (highest fitness) occurs at shorter distances, higher timeout values, and higher max retries, with color intensity highlighting this trend. The trend is confirmed by observing similar results in our Bayesian Optimization for 32 bits.

The Fig. 18 decomposes the landscape into a series of 3D plots for each max retries value (1)-(10), showing how retries influence performance. At lower retries, the fitness landscape is flat with minimal accuracy, but as retries increase, a ''performance cliff'' emerges in the low-distance, high-timeout region. Beyond retries of 7-8, diminishing returns are observed.

These visualizations highlight the inter-dependencies between parameters, showing that optimal system performance is achieved with shorter distances, higher timeouts, and sufficient retry attempts.

The Fig. 19 shows the Heatmap visualization of population distribution in the Genetic Algorithm, highlighting diversity and convergence trends. From the heatmap we can notice several individuals showing higher similarity with specific others, potentially indicating family relationships, shared ancestry, or demographic clustering. Also, the absence of clear, distinct clusters suggests a complex population structure rather than completely isolated groups.

The Table 14 contrasts the parameters (Bits, Distance, Timeout, Retries and Convergence Time) of our selected optimization algorithms.

We can hence conclude that due to BO prioritizing sample efficiency in low-dimensional spaces using probabilistic surrogate models and acquisition functions, it was able to adapt better to non-linear noise profiles making it suitable and outperform GA.

TABLE 14. Genetic algorithm Vs bayesian optimization performance comparison analysis.

Bits	Algorithm	Distance (km)	Timeout (s)	Retries
2	GA	167.50 ± 15.13	0.070 ± 0.016	9.83 ± 0.37
	BO	192.55 ± 20.79	0.073 ± 0.143	7.60 ± 1.88
4	GA	158.40 ± 18.68	0.028 ± 0.014	9.70 ± 0.65
	BO	186.45 ± 27.33	0.023 ± 0.016	6.80 ± 1.90
8	GA	125.26 ± 29.07	0.032 ± 0.017	9.63 ± 0.96
	BO	184.66 ± 26.33	0.022 ± 0.015	7.46 ± 2.04
16	GA	62.93 ± 18.50	0.044 ± 0.012	9.23 ± 0.77
	BO	172.21 ± 33.24	0.012 ± 0.010	7.70 ± 2.01
32	GA	79.06 ± 4.57	0.014 ± 0.0025	9.93 ±0.25
	BO	160.40 ± 38.40	0.0071 ± 0.010	8.76 ± 1.83
64	GA	52.36 ± 13.93	0.0055 ± 0.0071	8.33 ± 1.68
	BO	132.60 ± 39.57	0.0031 ± 0.0040	9.46 ± 1.19
128	GA	14.40 ± 10.15	0.016 ± 0.0019	6.40 ± 1.81
	BO	101.10 ± 34.93	0.0005 ± 0.0004	9.20 ± 0.76
256	GA	53.50 ± 1.13	0.0078 ± 0.00	9.03 ± 1.03
	BO	102.55 ± 33.17	0.0010 ± 0.0009	9.16 ± 0.69

G. PROTOCOL PERFORMANCE METRICS IN COMMON OPTICAL FIBER CABLES USED IN UNDERWATER DEPLOYMENT

The following Table 15 summarizes the measured transmission performance of various Corning single-mode fiber cables. Each fiber is identified by its refractive index, followed by the attenuation at specific wavelengths and the corresponding mean transmission distance (± standard deviation), averaged over thirty test runs.

Across all fibers, lower attenuation at 1550 nm consistently yields longer mean reach, with ULL variants, TXF and Vascade variants achieving the highest distances. But these commercial fibers are outperformed by the special Laboratory fiber by [31]. The standard deviations reflect stable performance over thirty repetitions, indicating reliable attenuation characteristics for each fiber type.

Submarine cables are engineered with multiple layers of protection to endure the harsh conditions of the ocean floor while maintaining reliable data transmission. Their design typically includes robust polymer sheathing for abrasion and chemical resistance, water-blocking gels or superabsorbent polymers to prevent moisture ingress, and steel armoring tailored to the cable's depth and environment. These features work together to shield the delicate optical fibers from physical damage caused by anchors, fishing gear, and geological events, as well as from mechanical stresses encountered during installation and operation.

However, over time, secondary effects such as microcracks in the sheathing, hydrogen ingress, and thermal cycling can compromise these defenses, leading to increased signal attenuation and gradual degradation of cable performance.

To counter these challenges, the industry continually innovates with advanced materials and monitoring technologies. Recent developments include hydrogen scavenging gel (HSG) technology and record-low attenuation levels of 0.1460 dB/km using silica-core fibers with large effective areas. Modern submarine systems leverage optimized C-band and L-band transmission windows, enabling repeater spacings exceeding 100 km across transoceanic distances.

TABLE 15. Attenuation and mean transmission distance of common underwater optical fiber cables.

Fiber Type	Refractive Index	Wavelength / Attenuation		Distance (km)
		nm	dB/km	
Corning SMF-28e+	1.4674	1310	0.35	39.67 ± 2.05
		1383	0.35	39.67 ± 2.05
		1490	0.24	54.87 ± 2.85
		1550	0.20	65.53 ± 4.01
		1625	0.23	57.73 ± 3.62
Corning SMF-28 Ultra	1.4676	1310	0.32	42.7 ± 2.21
		1383	0.32	42.7 ± 2.21
		1490	0.21	62.17 ± 3.36
		1550	0.18	72.73 ± 4.26
		1625	0.20	66.23 ± 3.05
Corning SMF-28 Contour Fit	1.4673	1310	0.32	40.3 ± 2.48
		1383	0.32	40.3 ± 2.48
		1490	0.21	60.27 ± 3.24
		1550	0.18	65.46 ± 2.97
		1625	0.20	60.27 ± 3.24
Corning SMF-28 Contour Pro	1.4673	1310	0.32	40.3 ± 2.48
		1383	0.32	40.3 ± 2.48
		1490	0.21	60.27 ± 3.24
		1550	0.18	65.46 ± 2.97
		1625	0.20	60.27 ± 3.24
Corning SMF-28 ULL	1.4606	1310	0.30	45.67 ± 2.48
		1550	0.16	81.9 ± 3.81
		1625	0.18	72.67 ± 3.33
Corning SMF-28 ULL Ultra Bend	1.4606	1550	0.16	82.67 ± 3.5
		1625	0.18	72.87 ± 3.27
Corning SMF-28 ULL S+	1.4620	1550	0.17	77.0 ± 4.14
		1625	0.19	69.73 ± 2.87
Corning TXF	1.4650	1550	0.17	82.13 ± 4.23
		1625	0.19	74.07 ± 4.27
Corning LEAF	1.4693	1383	0.4	34.67 ± 1.64
		1410	0.32	43.33 ± 2.04
		1450	0.26	51.77 ± 3.0
		1550	0.19	68.97 ± 2.99
		1625	0.19	63.27 ± 2.66
Corning Vascade EX2000 / EX2500	1.4634	1550	0.16	80.87 ± 4.14
		1625	0.18	74.40 ± 2.79
Lab Tested	1.470	1550	0.116	112.57 ± 4.18

Submarine fiber-optic cables encounter varying levels of optical loss depending on the surrounding water's chemistry—primarily the concentration of dissolved hydrogen and hydroxyl ions. In freshwater environments, minimal hydrogen ingress yields attenuation increases typically below 0.1 dB/km. Brackish or coastal waters, where corrosion byproducts introduce moderate hydrogen levels, drive losses into the 0.1–0.3 dB/km range. For example, shallow marine deployments (30 ft depth) can experience interstitial hydrogen–induced attenuation of about 0.30 dB/km at 1310 nm. Low water-peak single-mode fibers further suppress hydroxyl absorption around 1383 nm, reducing water-peak loss to roughly 0.35 dB/km, while industry specifications cap allowable water-peak attenuation at 0.4 dB/km for OS2 fiber types. Waters inducing losses above this threshold—often in deeper, anoxic zones—necessitate hermetically sealed cable designs to preserve transmission performance. The impact on max node distance for possible values of attenuation from 0.1 db/km to 0.4 db/km is illustrated below in Fig.20 and Table 16.

We can observe that, for 32 bit size message, a fixed refractive index of 1.46, as attenuation increases, the max distance between nodes decreases.

H. OPTIMIZATION ALGORITHM PARAMETER SELECTION AND SENSITIVITY ANALYSIS

The genetic algorithm (GA) implementation adopts a population size of 50 and 50 generations, with a mutation rate

TABLE 16. Water type, increasing attenuation vs maximum distance between nodes.

Water Type	Attenuation (dB/km)	Max Distance (km)
Freshwater	0.10	127.20 ± 4.85
Brackish/Coastal	0.11	118.63 ± 4.33
	0.12	105.97 ± 5.43
	0.13	97.37 ± 4.89
	0.14	93.27 ± 4.22
	0.15	85.23 ± 4.84
	0.16	80.80 ± 4.31
	0.17	77.27 ± 3.46
	0.18	73.57 ± 3.84
	0.19	69.70 ± 3.29
	0.20	66.33 ± 3.51
	0.21	62.73 ± 3.50
	0.22	60.10 ± 4.38
	0.23	57.33 ± 2.59
	0.24	55.47 ± 2.00
	0.25	53.70 ± 2.95
	0.26	52.07 ± 2.76
	0.27	50.37 ± 2.37
	0.28	48.07 ± 2.78
	0.29	46.33 ± 2.10
Shallow Marine	0.30	45.07 ± 2.46
Low-Water-Peak Fiber	0.31	43.17 ± 2.10
	0.32	42.60 ± 2.32
	0.33	41.00 ± 2.25
	0.34	40.80 ± 2.14
	0.35	38.60 ± 2.65
Deep/Anoxic Zones	0.36	37.87 ± 2.09
	0.37	37.03 ± 1.87
	0.38	36.27 ± 1.90
	0.39	35.30 ± 1.64
	0.40	34.27 ± 1.77

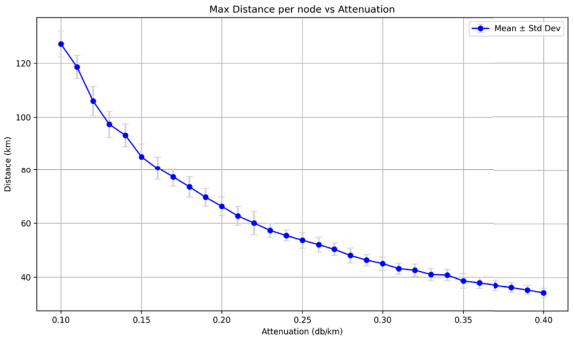

FIGURE 20. Max distance vs attenuation.

of 0.1, to ensure robust exploration and convergence in a large, mixed-integer search space defined by distance (1)–200 m), timeout (1)–1e9 ns), and max retries (1)–(10). The choice of a population size of 50 is grounded in the need to maintain sufficient genetic diversity across a broad parameter landscape, which is particularly important given the stochastic nature of the quantum simulation environment and the discrete-continuous hybrid of the optimization variables. Empirical evidence from the convergence plots in Fig. 16 shows that the average fitness rapidly improves in the first 10 generations and stabilizes thereafter, indicating that 50 generations suffice for the algorithm to approach convergence without excessive computational cost.

The mutation rate of 0.1 is selected to prevent premature convergence and the algorithm not to strike up at local optima, as evidenced by the persistent fluctuations in worst-case fitness across generations, which reflect ongoing exploration. Crossover is implemented at a random point between genes, enabling effective recombination of parameter subsets and further promoting exploration of the solution space. The selection strategy, which retains the top 50% of individuals by fitness, strikes a balance between exploitation of high-performing solutions and preservation of diversity. These choices are consistent with established practices in evolutionary computation for high-dimensional, noisy, or expensive-to-evaluate problems, and are validated by the observed convergence and diversity maintenance in the population heatmap Fig. 19.

I. JUSTIFICATION OF HYPERPARAMETER CHOICES AND CONVERGENCE BEHAVIOR

The Bayesian optimization (BO) framework employs a Gaussian Process surrogate, with the acquisition function set to 'gp_hedge', which adaptively chooses among multiple acquisition strategies (including Expected Improvement and Probability of Improvement) to balance exploration and exploitation. The search space mirrors that of the GA, with log-uniform priors on distance and timeout, and integer sampling for max retries. Each optimization run is initialized with 100 random samples (n_initial_points=100), providing broad coverage for the surrogate model and mitigating the risk of early convergence to suboptimal regions. This is followed by 100 exploitation calls, for a total of 200 function evaluations per bit size, as reflected in the staged optimization and convergence plots (Fig. 16).

The use of early stopping via DeltaYStopper (n_best=15, delta=0.01) ensures computational efficiency by terminating the search when improvements fall below 1% over the best 15 solutions, aligning with the diminishing returns observed in the objective value as the optimization progresses. The convergence plots demonstrate that the objective stabilizes well within the allocated budget, confirming the adequacy of these settings. The kernel for the Gaussian Process defaults to the Matérn kernel in scikit-optimize, which is well-suited for modeling moderately smooth, non-stationary objective functions typical in quantum network simulations.

The robustness of BO to kernel and acquisition function choices is supported by the consistent convergence behavior across all tested bit sizes (Table 14).

Both optimization strategies demonstrate reliable convergence: the GA achieves rapid initial improvement and maintains diversity, while BO consistently reaches stable optima within the specified evaluation budget. Sensitivity to population size, generation count, and mutation rate in GA, as well as kernel and acquisition function in BO, is implicitly addressed by the observed convergence and the stability of final solutions across multiple runs. However, for a more granular sensitivity analysis, future work could include systematic variation of these hyperparameter and statistical comparison of convergence rates and solution quality.

TABLE 17. Comparison of QKD protocols and hybrid approaches.

Protocol	Sifting Elimination	Device Indep.	Key Rate Efficiency	Max Distance	Security Assumption	Complexity	PQC Integration
Naive BB84	No	No	50%	Mod.	Standard quantum	Low	No
PRNG-Basis Align	Yes	No	100%	Mod.	PRNG, sync	Med.	No
Hybrid KEM-BB84 (this work)	Yes	No	100%	Mod.+	PQC, KEM	Med.	Yes
TF-QKD	Yes	Yes (MDI)	High (long)	V.High	Phase, MDI	High	No
MDI-QKD	Yes	Yes	Moderate	High	MDI, detectors	High	No
CV-QKD	Yes	No	High (short/med.)	Mod.	Gaussian, trusted	High	No

J. ANALYSIS OF SECURITY RISKS AND MITIGATION STRATEGIES

The proposed hybrid KEM-BB84 protocol is designed to enhance efficiency by eliminating the sifting step inherent in traditional BB84, thereby achieving 100% basis alignment and full utilization of transmitted qubits. This efficiency gain is particularly significant for resource-constrained environments such as underwater networks, where photon generation and transmission are costly and challenging.

However, this modification introduces a new dependency on the security of the underlying Key Encapsulation Mechanism (KEM), specifically CRYSTALS-Kyber, which is selected for its NIST-standardized, lattice-based security guarantees.

While the quantum physical principles of BB84-such as the Heisenberg uncertainty principle and the no-cloning theorem-continue to provide information-theoretic security against eavesdropping on the quantum channel, the overall security of the hybrid protocol also relies on the cryptographic hardness of the KEM against both classical and quantum attacks. Potential vulnerabilities may arise from the classical channel used to transmit the encapsulated basis information, as any compromise of the KEM (e.g., through implementation flaws, side-channel attacks, or future advances in cryptanalysis) could expose the basis choices and thus weaken the protocol's security.

To mitigate these risks, the protocol leverages KEMs that have undergone extensive cryptanalysis and standardization, employs authenticated classical channels to prevent man-in-the-middle attacks, and incorporates fallback mechanisms in the KEM decapsulation process to ensure robustness against active attacks.

Furthermore, the modular design enables crypto-agility, allowing for rapid substitution of alternative KEMs should vulnerabilities be discovered. Future work will focus on formal security proofs for the integrated protocol and on simulating advanced attack scenarios, such as side-channel and phase-remapping attacks, to further validate and strengthen the security posture of the proposed framework.

K. COMPARISON WITH PRNG-BASED AND NEXT-GENERATION QKD PROTOCOLS

While PRNG-based basis alignment and other hybrid QKD approaches have demonstrated the potential to eliminate sifting and improve efficiency, they introduce distinct challenges [1]. PRNG-based protocols require strict synchronization and the secure sharing of seeds, and their security may be compromised if the PRNG or seed exchange is attacked. In contrast, our KEM-based approach leverages post-quantum security assumptions and does not require ongoing synchronization, but does introduce computational overhead and relies on the security of the encapsulation mechanism. We did not include direct simulation comparisons with PRNG-based or other hybrid protocols, as our primary focus is on integrating PQC primitives and evaluating their performance in underwater scenarios; moreover, open-source and standardized implementations of these alternatives are limited.

Regarding next-generation QKD protocols, such as TF-QKD, MDI-QKD, and CV-QKD, these schemes address different challenges-namely, extending achievable distance and mitigating device vulnerabilities. TF-QKD and MDI-QKD offer measurement-device independence and improved key rates over long distances but require more complex infrastructure and are not yet widely deployable in resource-constrained or underwater environments. Our approach, by contrast, is tailored to scenarios where practical integration with PQC and efficient photon utilization are paramount. The Table 17 provides a comparative summary of the key trade-offs among these protocols.

L. PROGRESS SUMMARY

This subsection quantifies the advances made in addressing the identified challenges, comparing the proposed hybrid KEM-QKD protocol against state-of-the-art (SOTA) baselines.

Progress is measured through key metrics such as efficiency gains, distance extensions, and optimization performance, supported by simulation results.

The advances of the proposed work are listed below:

1) **Advances:**

- Achieved 100% raw key generation efficiency by eliminating sifting through KEM-based basis alignment, compared to BB84's 50%.
- Extended maximum secure distances by up to 42% in optic fiber simulations, with Bayesian Optimization (BO) outperforming Genetic Algorithms (GA) across bit sizes (160.40 km vs. 79.06 km for 32 bits).
- Demonstrated superior computational efficiency with Kyber512, achieving 26.97% faster key

generation, 23.08% quicker encapsulation, and 44.16% faster decapsulation than LightSaber.
- BO showed consistent outperformance in solution quality and efficiency, balancing exploration and exploitation for complex quantum network optimization.

2) **Measurement of Progress:**
- Efficiency and distance metrics are quantified via comparative benchmarks (Tables 13 and 14), with statistical validation over multiple runs.
- Progress is evident in reduced quantum transmission requirements and enhanced stability for underwater deployments, supporting crypto-agility and interoperability.

These quantifiable improvements highlight the protocol's progress toward practical, scalable quantum-secure communications.

V. BENEFITS AND DEPLOYMENT CHALLENGES ADDRESSED

A. BENEFITS

The proposed methodology represents a theoretically sound solution that leverages established cryptographic principles to address real-world quantum communication challenges. The systematic approach, from algorithm selection through optimization, provides a replicable framework for quantum-secure underwater networks with clear performance metrics and engineering constraints.

Even though the integrated protocol will increase complexity and potential implementation costs, as per 'No Free Lunch' theorem, the potential benefits it brings particularly in the context of post-quantum security and hybrid cryptographic systems that works on both quantum and classical, can outweigh these costs.

Some of the primary advantages of this work are:

- At the Post-Quantum Security layer, CRYSTAL-Kyber type of KEM helps resist attacks from quantum computers by adding redundancy if QKD channels are disrupted or compromised.
- It provides Hybrid Security as it combines the strengths of QKD and Post-Quantum classical security which will help in providing robust protection in uncertain environments.
- With KEM integration, key reuse and reduction in key wastage as in BB84 are discarded.
- The integration of KEM can mitigate side-channel vulnerabilities of physical QKD implementations.
- Using KEMs integration, the embedding of QKD into larger classical infrastructure can be easily done.
- As KEMs can bridge the gaps where Quantum repeaters are not yet viable, they provide secure classical key transport over the communication network.

B. DEPLOYMENT CHALLENGES

(i) This research work analyses the possibilities of challenges or overheads associated with 'Network Switch' in implementing this work. It confirms that no such overheads will occur due to the following reasons:

- As the process is going to be done at the quantum layer, it operates outside the traditional switches and it will be operated using dedicated fiber channels or free-space optics.
- The KEM processing is happening on edge devices or secure servers and not in switches directly.
- The only function of Switch will be to route encapsulated keys, quantum metadata and encrypted payloads across the network. Hence, the concern on Switch overloading is not arising for this proposed work.

(ii) Regarding the challenges related to the Engineering Insights during actual deployment, some of the suggested solutions to be incorporated are:

- Edge based encryption units near switches
- Software-Defined Networking (SDN) for dynamic routing of quantum key metadata and secure channels
- Integration of NIST approved Post-Quantum Cryptography libraries such as liboqs and PQClean on existing computing nodes and
- Deployment of trusted repeater nodes to extend QKD range.

C. THREAT TO VALIDITY

Due to several factors that influence our current analysis, the current stimulation conducted for the study may yield slightly different results, even with the same parameters.

NetSquid and liboqs, the simulation tools, should be compiled in identical configurations to obtain similar output. Any differences in software versions or parameter settings can lead to diverging results. It should also be noted that quantum states are sensitive to disturbances and can be unique.

Finally, there are differences between QKD hardware systems and software programs. This may lead to slight differences in the simulation results when run in real world settings.

VI. CONCLUSION AND FUTURE WORK

This research developed an integrated framework for quantum-secure communications by advancing post-quantum cryptography, quantum key distribution, and network optimization. A systematic evaluation of NIST Round 3 key encapsulation mechanisms (KEMs) identified CRYSTALS-Kyber as optimal for resource-constrained environments, demonstrating superior computational efficiency with Kyber512 achieving 26.97% faster key generation, 23.08% quicker encapsulation and 44.16% faster decapsulation compared to the runner up LightSaber while maintaining NIST Level 1 security. The protocol's compact key sizes and efficient lattice-based operations made it particularly suitable for practical implementations where computational overhead and bandwidth constraints are critical considerations.

The study significantly enhanced the efficiency of the BB84 protocol by integrating Kyber KEM, which eliminates basis mismatch and achieves near-perfect qubit utilization

through basis encapsulation. NetSquid simulations validated this approach, demonstrating 100% efficiency in key generation, compared to the approximately 50% efficiency of traditional BB84 under theoretical conditions. This Kyber-enhanced quantum key distribution method eliminates the need for public basis reconciliation while maintaining information-theoretic security through quantum physical principles.

To optimize quantum network node placement and maximize achievable distances, we implemented and compared two advanced techniques: Genetic Evolution algorithms and Bayesian optimization. Both methods were assessed for their ability to identify optimal node configurations under realistic physical constraints. Bayesian optimization consistently outperformed Genetic Evolution in terms of both solution quality and computational efficiency. While Genetic Evolution provided acceptable solutions, Bayesian optimization delivered superior results, making it particularly well-suited for computationally intensive quantum network simulations. The effectiveness of Bayesian optimization lies in its strategic balance between exploration and exploitation, achieved through a surrogate probabilistic model and an acquisition function that efficiently navigates the complex solution space. This approach proved especially valuable for quantum network optimization, where the relationship between node placement and achievable distances involves complex non-linear interactions.

The significance of the proposed hybrid KEM-QKD framework extends beyond theoretical improvements in quantum key distribution. By eliminating the sifting step through KEM-based basis alignment, the framework substantially enhances system stability and resource efficiency, which are critical for practical deployment in resource-constrained and high-latency environments such as underwater networks. Furthermore, by benchmarking and selecting NIST-standardized KEMs, the approach ensures compatibility with current and future standardization efforts, supporting crypto-agility and long-term interoperability. The resulting reduction in quantum transmission requirements directly addresses cost barriers, while the use of advanced optimization techniques enables robust, real-world parameter tuning. Collectively, these features make the framework not only a theoretical advancement but also a necessary step towards scalable, cost-effective, and standardized quantum-secure communication systems.

Future research in quantum-secure communications will focus on developing integrated simulation frameworks that combine quantum-classical network dynamics, utilizing tools like NetSquid for quantum channel modeling and NS-3/OMNeT++ for emulating classical infrastructure. This hybrid approach, inspired by cloud security simulations that demonstrated 75% faster encryption through co-simulation, will address real-world deployment challenges such as atmospheric turbulence effects and the need for hardware-software co-design in error correction. Enhanced noise modeling will incorporate photon number splitting attacks and Trojan-resistant KEM architectures, supported by ongoing standardization efforts for benchmarking metrics like adaptive LDPC coding and security certification frameworks. Bayesian optimization, which has already shown success in quantum annealing and network topology design, will be combined with quantum-inspired genetic algorithms to optimize decoy-state ratios and entanglement swapping protocols.

Future advancements will prioritize real-time adaptive strategies, leveraging machine learning for dynamic polarization control and CNN-based error correction to reduce quantum bit error rates (QBER). To enhance security, proofs for Kyber-BB84 integrations will be validated through Bell inequality checks and Monte Carlo simulations of phase-remapping attacks. Cross-shaped post-election protocols and ML-driven anomaly detection techniques will address QBER fluctuations in free-space channels, while entanglement-based monitoring may extend secure distances beyond 50 km. Standardization efforts must reconcile competing frameworks for QKD certification and hybrid post-quantum solutions, ensuring backward compatibility with existing infrastructure. These initiatives collectively aim to bridge the gap between theoretical security proofs and the practical challenges of deploying metropolitan-scale quantum networks.

ACKNOWLEDGMENT

The authors are grateful to DST-FIST and VIT management for their financial support and the resources provided for this work.

APPENDIX
IMPLEMENTATION DETAILS

The implementation code in NetSquid platform is available in the GitHub repository: https://github.com/jeyamala/QKD

REFERENCES

[1] A. Bhatia, S. Bitragunta, and K. Tiwari, "Enhanced lightweight quantum key distribution protocol for improved efficiency and security," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 926–943, 2025, doi: 10.1109/OJCOMS.2025.3528718.

[2] I. B. Djordjevic, "Hybrid DV-CV QKD outperforming existing QKD protocols in terms of secret-key rate and achievable distance," in *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, Angers, France, Jul. 2019, pp. 1–5, doi: 10.1109/ICTON.2019.8840467.

[3] M. Sabatini, T. Bertapelle, P. Villoresi, G. Vallone, and M. Avesani, "Hybrid encoder for discrete and continuous variable QKD," 2024, *arXiv:2408.17412*.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[7] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, no. 2, May 2020, Art. no. 025002.

[8] M. D. Eisaman et al., "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, 2011, Art. no. 071101.

[9] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based cryptography for IoT in a quantum world: Are we ready?" in *Proc. IEEE 8th Int. Workshop Adv. Sensors Interface (IWASI)*, Jun. 2019, pp. 194–199.
[10] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE EuroSP*, Apr. 2018, pp. 353–367.
[11] E. Alkim, "Post-quantum key exchange—A new hope," in *Proc. USENIX Secur.*, 2016, pp. 327–343.
[12] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. Int. Algor. Number Theory Symp.*, 1998, pp. 267–288.
[13] E. Diamanti et al., "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–14, 2016.
[14] E. Alkim. *FrodoKEM: Practical Quantum-secure Key Encapsulation From Generic Lattices*. Accessed: Mar. 30, 2025. [Online]. Available: https://frodokem.org/
[15] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical bob," in *Proc. 1st Int. Conf. Quantum, Nano, Micro Technol. (ICQNM)*, Jan. 2007, p. 10.
[16] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.
[17] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045017.
[18] D. Stucki, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, Dec. 2011, Art. no. 123001.
[19] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, p. 1012, 2020.
[20] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, "High-rate quantum key distribution exceeding 110 Mb s^{-1}," *Nature Photon.*, vol. 17, no. 5, pp. 416–421, May 2023.
[21] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, May 2023, Art. no. 210801.
[22] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Commun. ACM*, vol. 62, no. 4, p. 133, Mar. 2019.
[23] T.-Y. Chen, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Inf.*, vol. 7, no. 1, p. 134, Sep. 2021.
[24] National Institute of Standards and Technology. *Post-Quantum Cryptography*. Accessed: Mar. 30, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
[25] National Institute of Standards and Technology. *Post-Quantum Cryptography Standardization: Round 3 Submissions*. Accessed: Mar. 30, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
[26] Classic McEliece Team. *Classic McEliece: Implementation*. Accessed: Mar. 30, 2025. [Online]. Available: https://classic.mceliece.org/impl.html
[27] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Deep Space Netw. Prog. Rep.*, vol. 44, pp. 114–116, Jan./Feb. 1978.
[28] J. P. D'Anvers A. Karmakar, S. S. Roy, and F. Vercauteren, "SABER: Mod-LWR based KEM (round 2 submission)," NIST Computer Security Resource Center, Aug. 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/saberround-2-presentation/images-media/saber-danvers.pdf
[29] SABER Team. *SABER: LWR-based KEM*. Accessed: Mar. 30, 2025. [Online]. Available: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/
[30] S. C. G, L. Gokavi, C. H. Ravikumar, and R. G. Balarkishna, "Antibody-modified 2D MXene nanosheet probes for selective, picolevel detection of cancer biomarkers," *Biosensors Bioelectron.*, vol. 271, Mar. 2025, Art. no. 117028. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10761772/
[31] Y. Chen, "Hollow core DNANF optical fiber with $<$ 0.11 dB/km loss," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, San Diego, CA, USA, 2024, pp. 1–3.

D. JEYA MALA (Member, IEEE) is currently a Professor with the School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology. She has more than 25 years of experience in teaching, research, and industry. She has been granted a design patent and published two utility patents from the IP, Government of India. She completed a funded research project from the Government of India as the Principal Investigator. She has published four books and more than 65 articles in reputed and refereed SCI and Scopus-indexed journals and conferences and book chapters. Her research interests include quantum computing, AI/ML, explainable AI, TinyML, healthcare analytics, software engineering, and security. She is a member of the National Work Group on Quantum Computing formed by the Telecommunications Department, Government of India, and has contributed to the Technical Report ITU-T TR.UQKDN presented by India at the Geneva Meet, Switzerland, in 2024. She has served as an Expert Evaluation Committee Member of AICTE-NEAT, Government of India, and for the MoE's Innovation Council, Government of India, by AICTE. She is a member of ACM and other professional bodies. She is a Listee of the Who's Who List of SEBASE Repository of the University College of London, U.K., for her research work. She has received awards and honors from governments and industries.

ACHINTYA KANT RASTOGI is currently pursuing the bachelor's degree in computer science and engineering with Vellore Institute of Technology, Chennai. He has presented his research findings at the International Conference on Emerging Trends in Business Analytics and Management Science (BAMS-ORSI 2024) hosted at IIT Bombay. His research interests include quantum computing applications, specifically in quantum machine learning, quantum annealing, and post-quantum cryptography. His current research interests include reinforcement learning, vehicle dynamics, internal combustion engines, and automotive technologies.

AYUSH RAJ is currently pursuing the B.Tech. degree in computer science and engineering with Vellore Institute of Technology, Chennai.

He is an AI Engineer at Outlier, where he contributes to the reinforcement learning from human feedback (RLHF) projects, enhances AI coding models, and applies prompt engineering techniques to improve generative AI performance. His technical expertise spans C++, Python, Java, SQL, and JavaScript, with experience in frameworks, such as React, Django, and Express. He has worked on various projects, including CuteAI, an interactive chat application powered by OpenAI, and an animated gaming website using React and GSAP. He has presented research at the International Conference on Emerging Trends in Business Analytics and Management Science (BAMS-ORSI 2024) at IIT Bombay. He holds multiple certifications, including AWS Certified Solutions Architect-Associate and the AWS Certified Cloud Practitioner. His interests include artificial intelligence, reinforcement learning, cloud computing, and full-stack development.

VAIDIK MANORI is currently pursuing the B.Tech. degree in computer science and engineering with Vellore Institute of Technology, Chennai. His research interests include machine learning, generative artificial intelligence, and deep learning.