IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 November 2024, accepted 23 January 2025, date of publication 5 February 2025, date of current version 24 February 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3539178

RESEARCH ARTICLE

A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection

NOOR UL AIN[1], MUHAMMAD WAQAR[2], ANAS BILAL[3], (Senior Member, IEEE), AJUNG KIM[4], HAIDER ALI[5], UMAIR ULLAH TARIQ[6], AND MUHAMMAD SHAHROZ NADEEM[2]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan
[2]School of Technology, Business and Arts, University of Suffolk, IP4 2QJ Ipswich, U.K.
[3]College of Information Science and Technology, Hainan Normal University, Haikou, Hainan 570100, China
[4]Department of Optical Engineering, Sejong University, Seoul 05006, South Korea
[5]Department of Computing, University of Derby, DE22 3AW Derby, U.K.
[6]School of Engineering and Technology, Central Queensland University, Rockhampton, QLD 4701, Australia

Corresponding author: Ajung Kim (akim@sejong.ac.kr)

This work was supported by MSIP and NRF of South Korea under Grant RS-2024-00396999 and Grant RS-2024-00437191.

ABSTRACT Quantum cryptography is anticipated to drive substantial advancements in cybersecurity. The impending arrival of quantum cryptography compromises current encryption methods, possibly compromising the effectiveness of traditional key management-based security protocols. One fundamental Quantum Key Distribution (QKD) protocol, BB84, encounters challenges when operating with fewer Quantum bits (Qubits) and bases that only support up to 8 Qubits. This limitation weakens the system's security, making brute force, intercept, and resend attacks less challenging. Consequently, this study proposes a method to enhance the security of the BB84 protocol, to reduce susceptibility to attacks and eavesdropping. The improved BB84 protocol utilizes 9, 12, and 16 quantum bits along with two, and three bases to significantly bolster security. This allows authorized parties to eliminate the use of compromised keys. Additionally, the study implements the E91 QKD protocol utilizing the Entanglement Pair Generation (EPR) method to produce secure keys. While the existing E91 protocol ensures security through Bell's theorem and Bell's inequality, it overlooks the impact of noise, leading to inaccuracies in eavesdropper detection. To address this, the study introduces an additional security measure. Whenever an eavesdropper attempts to measure the quantum state, the proposed E91 protocol collapses its state from $|10\rangle$ to $|11\rangle$, setting the first Qubit to $|1\rangle$ and the other Qubit to $|0\rangle$, thus providing the eavesdropper with incorrect information, accompanied by a phase angle of $15\pi/8$. This leads to a misconception, preventing eavesdroppers from obtaining useful details about transferred quantum states. Additionally, considering that the proposed E91 protocol relies on entangled particles and utilizes double Qubit gates, which are inherently noisier than single Qubit gates and more susceptible to quantum decoherence, this study employs error mitigation techniques during the final measurement to predict outcomes more efficiently.

INDEX TERMS Quantum cryptography, quantum key distribution, eavesdropper detection, quantum entanglement.

I. INTRODUCTION

Traditional cryptographic techniques have long been used to encode original content into cipher text, which is then transmitted through a channel secured by a key. When

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

the recipient possesses the correct key, they can retrieve the original content. To strengthen security in conventional cryptography, several measures must be implemented, with confidentiality, authenticity, and accountability being the most valuable. These are achieved through symmetric and asymmetric cryptography, the primary techniques used in classical cryptography. Algorithms such as Rivest Shamir Adleman (RSA) [1], Advanced Encryption Standard (AES), and Data Encryption Standard (DES) [2] rely on number theory and mathematical assumptions to prevent third parties from accessing encrypted messages. One of the most widely used algorithms is AES, deployed globally and offers different key lengths—128, 192, and 256 bits. Later, the Triple Data Encryption Standard (3DES) [2] was introduced by expanding the key length to address the vulnerabilities in DES. Elliptic Curve Cryptography (ECC) [3] is considered one of the most stable and efficient cryptographic techniques but remains susceptible to quantum computing attacks. If key management methods are ineffective, the system becomes vulnerable to security breaches, potentially leading to devastating attacks. The majority of encryption techniques in use today are considered highly secure. However, their resilience against emerging threats, particularly quantum computing, remains a significant concern.

Conversely, Quantum computers pose a threat to traditional encryption schemes, potentially making some of them untrustworthy. Algorithms such as Grover's and Shor's algorithms [4], [5] can break symmetric and asymmetric cryptographic schemes. Quantum cryptography ensures that information cannot be copied by transferring millions of photons over a fiber optic cable. Each photon maintains its unique state, and together, all photons generate a binary data stream composed of zeros and ones [6]. From a physics perspective, quantum cryptography's key attraction is its ability to share a secret key between two remote users in a way that makes it unthinkable for a third party to eavesdrop without disrupting the quantum transmission. In this way, the eavesdropper is detected by both parties [7]. Utilizing quantum computing for QKD is exceptionally promising. For specific protocols, it relies on both the Heisenberg uncertainty principle and the no-cloning theorem [8]. In place of concealing data, QKD takes advantage of quantum mechanics to distribute information between two locations. Several advantages of utilizing QKD are relevant to security and can replace mathematical approaches that are prone to being broken. The central thought is to detect an eavesdropper when a key exchange happens on the quantum channel. To eliminate the likelihood of Man-In-The-Middle (MITM) attacks, these systems require an authenticated public channel [9]. The polarization states are used to encrypt information in two manners: Rectilinear at 0° and 90° and Diagonal at 45° and 135° as shown in FIGURE 1.

Despite several advantages, there is finite research on the unreliability of secret keys and their consequences on the quantum systems, which are not stable enough. These systems drop information if not stored properly, making it tricky

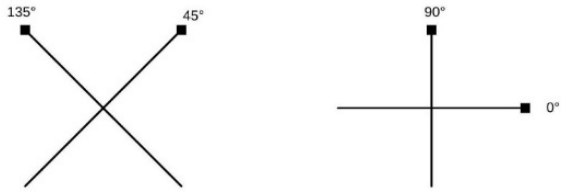


FIGURE 1. Photon polarization: diagonal and rectilinear.

to maintain these photon's positions and entanglement for a long duration [8] and [10]. The first and most widely used QKD protocol named BB84 was presented by Bennett and Brassard [11] which are based on two means of communication. The initial channel or quantum channel that is utilized to travel quantum bits between remote users is based on two polarization states and the other one is an authenticated classical channel used for transferring the encoded message as shown in FIGURE 2. They had to choose whether to scan every bit using a rectilinear or diagonal polarization state when they obtained the photon key. In some cases, both Alice and Bob will accurately measure the polarization. However, if Bob uses inappropriate polarization photons, he will receive inappropriate outcomes. At this point, they established a vulnerable channel that others could watch. As per reference [12] improvements in quantum computing algorithms would render almost half of the encryption schemes in use obsolete. It is necessary to uncover vulnerabilities' of these protocols to protect against future quantum attacks. In quantum cryptography, secure communication depends on the robustness of QKD protocols, with BB84 and E91 being the most commonly used. Despite being popular, existing methodologies [13], [14], [15] face significant challenges, such as noise sensitivity, quantum errors, and vulnerabilities in key generation due to eavesdropping. These challenges are highlighted when a limited number of Qubits and bases are used.

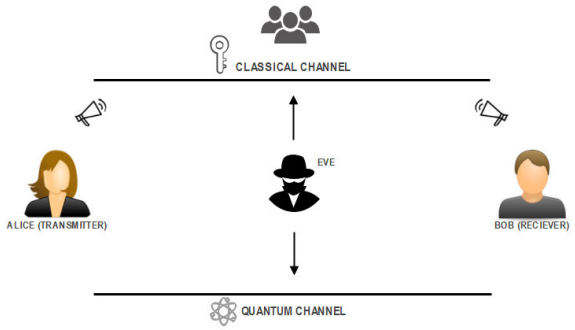


FIGURE 2. Basic workflow of quantum key distribution.

This research aims to enhance the reliability and robustness of quantum communication by addressing these challenges, mainly the secure generation of quantum keys for practical use. We enhance previous studies by implementing the BB84 protocol with Qubit lengths of 9, 12, and 16 and testing it

across two and three bases. This approach enables a detailed analysis of the impact of Qubit length on key generation security. Additionally, the E91 protocol was examined under various configurations, including simulated eavesdropping scenarios and reverse quantum gate configurations. To mitigate the effects of noise, error correction techniques are integrated, providing a framework to enhance the reliability of QKD protocols in real-world quantum communication systems. While the two protocols differ in their methodologies, as BB84 employs individual Qubits and E91 relies on entanglement, their common goal is to ensure secure key distribution. Both protocols aim to detect eavesdropping using different physical phenomena: BB84 relies on the disturbance in quantum states caused by measurement, whereas E91 takes advantage of violations of Bell's inequality. Although their underlying mechanics differ, both protocols play an important role in advancing the security of quantum communications. Additionally, comparing these two protocols provides crucial information into the evolution and diversity of QKD approaches. While BB84 offers simplicity and practical options with available technology, E91, despite its higher complexity, promises robust security in future scalable quantum networks. Understanding the strengths and limitations of both helps define ongoing efforts in quantum cryptography, which aim to develop upon these foundational protocols to develop more advanced and efficient quantum communication systems [14], [16].

The contributions of this study are summarized as follows:

1) This research enhances the BB84 QKD protocol by testing it across two and three bases with Qubit lengths of 9, 12, and 16. The choice of these quantum bit lengths ensures that the protocol remains computationally feasible while providing an adequate level of security. If the Quantum Bit Error Rate (QBER) and information leakage rate exceed permissible thresholds, privacy amplification is employed to eliminate any correlations that could potentially be exploited by an eavesdropper, ensuring the security of the final key. This step addresses potential vulnerabilities in the BB84 protocol by making it resistant to both noise-induced errors and eavesdropping attempts.
2) This study also incorporates the E91 protocol, which relies on entangled particle pair generation for secure communication. In this work, we introduce a reverse quantum gate configuration that transforms quantum states to obscure information being transmitted between users. This additional security layer examines the quantum states of entangled particles to assess interference based on Qubit states and phase angles, further complicating an eavesdropper's ability to extract useful information. By employing this method, even if an eavesdropper captures data, the information retrieved will be misleading and unusable.
3) The study also addresses the excessive noise prevalent in the E91 protocol, which arises from quantum gate operations susceptible to decoherence. Quantum noise can cause gates to collapse, thereby compromising the integrity of the communication. To counteract this, we implement error mitigation techniques during the final measurement phase, thereby reducing the impact of noise and enabling more accurate predictions of the final output. These corrective measures make the enhanced E91 protocol more resilient to eavesdropping and quantum noise, ensuring a higher degree of security in practical implementations.

The remainder of this study includes the following sections: Section II presents a literature review that compares and contrasts existing research, unifies the findings, and provides an introspection on the available knowledge in the specified domain. Section III explains the research methodology, procedures, and techniques. Section IV analyzes the proposed method and compares it to similar protocols. Lastly, Section V presents the conclusion.

II. LITERATURE REVIEW

Utilizing the basic principles of quantum mechanics to protect communication mediums, QKD represents a significant advancement in cryptographic research. The importance of reliable and immutable encryption techniques continues to grow as modern technology evolves. Consequently, this literature review comprehensively analyzes many of the recent innovations in QKD protocols. In anticipation of this phase, a study [17] analyzed the effects of QKD and Post-Quantum Cryptography (PQC) on Distributed Energy Resources (DER) networks. The study identified concerns about performance and installation cost when these methods were used concurrently. As a result, they proposed an innovative DER network configuration that minimizes the key distribution delay due to QKD's lower transfer rate compared to conventional networks. Currently, QKD networks are costly, and future research will focus on developing server-based QKD and lightweight PQC quantum-safe DER networks that are affordable and high-performing. A study [13] simulates the BB84 protocol using the IBM quantum computing platform, executing it with and without eavesdropper interference. They used both the ''qasm simulator'' as a local simulator and the ''ibmqx2'' quantum simulator with N quantum and classical registers corresponding to Alice and Bob's quantum circuits (in their case, N=4). They established the presence of an eavesdropper in the communication channel due to the transformed probability distributions, as some probabilities that are higher with an eavesdropper become lower without one. As a result, they discard the key and repeat the process because the key exchange has been compromised. A study [18] proposed Quantum Key Secure Communication (QKSC) which employs a dynamic key and super-dense coding system. They claimed that their QKSC protocol is the first to use a dynamic key in quantum cryptography. Additionally, it is easy to develop, affordable, and a low-maintenance option where keys and messages

remain secure. If QKSC operated at a single-photon level instead of using a key, and an eavesdropper deployed a photon number-splitting attack, then Bob might notice the disruption in communication and inform Alice to terminate the entire transmission. The primary reason for adding a dynamic key is to maintain message reliability. They observed that the problem arises when results obtained from the 16-Qubit Processor indicate a 40% error due to a large number of C-NOT gates. A study [19] showed that merging QKD with a traditional encryption algorithm significantly boosts data transmission security. The evaluation of encryption, decryption, throughput, and avalanche effect was estimated for algorithms incorporating and excluding quantum key distribution. Their results illustrate that this is achieved by minimizing the encryption and decryption time while increasing throughput over records between 500 and 3500 KB. They found that traditional encryption algorithms, including QKD, obtained 56.8%, 58.6%, and 54.3% shorter durations. A study [20] experimentally demonstrated a side-channel attack via misaligned sources over free-space QKD applications. They further conducted a proof-of-principle attack, which shows that minimal angular misalignment among the origin is theoretically dangerous because of this attack. They suggested two defenses to shield QKD systems from the outlined attack: using a single laser to eliminate spatial discriminability of sources and single-mode optical fiber. Lastly, they highlighted the security considerations that need to be taken into account for the safe transfer of keys. This study [21] provides solutions to conventional encryption protocols, starting with quantum key distribution protocols employing two, three, and four state methods. They identify eavesdropper presence by evaluating errors that occur after transmission across a quantum channel. Their results demonstrate that the QKD protocol featuring four-state systems is quite effective in the case of intercept-resend attacks. A study [22] proposed a verification technique using unitary quantum gate reversibility and quantum teleportation. Their core concept revolves around stabilizing the quantum state after the procedure, permitting quantum teleportation to preserve the position of quantum information before the interpretation process. They performed the technique by employing gates in reverse order—Controlled-Not (CX) and Hadamard Gate. The final result must match the initial input, typically $|0\rangle$. If they match, the computation result is verified and gains more credibility. Further, they eliminated 18.848% of results containing errors and utilized the remaining data as an outcome. This study [23] implements the B92 protocol on actual quantum hardware and explores its handling of key length variations with several eavesdropping techniques. They executed the program a specified number of times for each key length and eavesdropping technique, then analyzed the original key length with three cases: lost, compromised, or damaged. From each experiment, they calculated the standard deviation. They pointed out that using a higher number of Qubits ensures the security of the B92 protocol, however, with a shorter key length, the protocol becomes insufficiently secure.

The authors in [24] use case studies to ensure the sustainability of 7E through the IBM software. They also rely on Kyber and Dilithium strategies to improve existing encryption methods to post-quantum versions. They pointed out the operational aspects necessary to execute 7E and proposed a revised version for professionals. The results illustrate that only slight modifications are needed, and the 7E strategy adequately anticipates future development toward ongoing software security protections. This study [25] looks into the use of deep learning algorithms to identify and mitigate malware in real time. However, quantum-powered malware might bypass existing detection methods, leading researchers to explore quantum cryptographic techniques for improving malware detection security. A study [26] offers post-quantum cryptography and quantum attack resistance for online voting systems. They anticipate that the Blockchain-Based Voting System Powered by Post-Quantum Cryptography (BBVSP-PQC) platform will allow activities through inactive blockchain or a potential off-chain strategy. They found that 51% of attacks, or the majority of attacks, cannot be deployed in BBVSP-PQC since it uses the Practical Byzantine Fault Tolerant (PBFT) method. They also used electronic equipment to ensure that voting could not occur during a power outage. However, the system could be modified in the future to run effectively on quantum computers. The rapid deployment of 5G networks [27] increased connectivity but introduced security concerns, as existing encryption techniques such as RSA and ECC may be compromised by quantum computing. This has led to the development of quantum-safe solutions to protect 5G networks from quantum-based cyber-attacks.

The study [28] developed Enhanced BB84 Quantum Cryptography Protocol (EBB84QCP) for healthcare purposes, securely allocating encrypted credentials among communication entities by utilizing bitwise functions and quantum concepts to protect patients' sensor data in wireless environments. This provides an effective way of remotely monitoring patients. Their proposed EBB84QCP involves the following steps: quantum bit generation, check bit generation, analysis on a public communication channel, key generation using the bitwise operator, and analysis with Bob about the quantum key generation process. This process protects the network's medical information from attackers, particularly in the case of a potential MITM attack, preventing the key information from being acquired. They provide a time analysis with different file sizes through nine experiments. Compared to DES and RC4, their enhanced BB84 protocol provides faster key generation time measured in milliseconds. The study [29] examined two specific cases among all quantum key distribution protocols and proposed methods for preparing and measuring QKD techniques. The optimality shows the effectiveness of these techniques, presenting an optimal secure QBER for orthogonal Qubits (expanding

the BB84 Protocol) around 27.28% in terms of memory and memoryless Controlled-NOT threats. In contrast, secure restraints are improved to about 22.73% and 28.69% with non-orthogonal Qubits for memory and memoryless Controlled-NOT protocols such as the expanding B92 and SARG04 protocols. They also discussed collective attacks, where Controlled-NOT attacks serve as suitable eavesdropping strategies. A study [30] analyzes a simple approach to improving an entanglement source with access control by utilizing phase randomization, where all individuals can be controlled using improved entanglement resources to conduct quantum cryptography. The conventional collective attack is individually handled because the detected entanglement visibility in their system is above 96%. A study [31] evaluates privacy and effectiveness following the NIST post-quantum standardization approach, focusing on isogeny. They performed security inspection of shared key protocols leveraging certain post-quantum encryptions, and they analyzed discrete logarithm and integer factorization quantum encryptions, as well as discrete logarithm and integer factorization problems. Then, they compared their complexity with well-known attacks on IFP, DLP, SSI, ISD, and RLWE with the complexity of brute-force attacks. Their finding shows that, compared to post-quantum methods, SSI utilizes smaller keys than RLWE and the code-based algorithm. Regarding performance, RLWE-based postquantum algorithms perform the best, followed by SSI and code-based algorithms.

Recently, researchers have studied different challenges of quantum cryptography and the way the QKD process ensures confidentiality and detection of third-party presence. Based on the above literature review, it is concluded that QC is still an emerging field that demands further study and evaluation to validate its reliability. Many of the QKD protocols experienced difficulties with fewer Qubits which could threaten security and eavesdroppers are less likely to be discovered. Moreover, existing quantum protocols deal with eavesdropping and neglect the effect of noise.

III. RESEARCH METHODOLOGY

In QKD protocols such as BB84 and E91 [32], the primary focus is on the secure exchange of cryptographic keys between Alice and Bob over a quantum channel. Unlike traditional encryption methods, QKD does not involve the direct encryption or decryption of information. Instead, it facilitates the secure generation and distribution of cryptographic keys, which are then used for conventional encryption. The effectiveness of QKD lies in its ability to securely distribute these keys, ensuring that the information encrypted with them remains protected from eavesdropping attempts. This section provides an in-depth overview of our proposed work which comprises BB84 and E91 protocol.

A. BB84 PROTOCOL

The proposed work evaluates the BB84 protocol with longer Qubit sequences (9, 12, and 16) while focusing on the complexities that arise during eavesdropping attempts. By employing three different quantum bases, Computational, Hadamard, and Diagonal, on a 16-Qubit configuration, this approach increases the difficulty for an eavesdropper to intercept and accurately measure the quantum states. As each Qubit exists in a superposition [33] an eavesdropper must not only predict the state but also the correct measurement basis, which significantly complicates their ability to extract useful information. This multi-base approach goes beyond typical two-base implementations, providing an extra layer of security, particularly under realistic conditions of noise and hardware imperfections. Moreover, this study acknowledges the limitations of current IBM quantum devices, which restrict the implementation of longer key lengths. However, this work aims to bridge the gap between theoretical security and practical implementation. While theoretically secure for longer keys, validating BB84 under real-world conditions is crucial, as noise and device imperfections can affect security. Using IBM's quantum simulators, we simulate realistic conditions and evaluate the protocol's performance across configurations. The findings offer practical insights into the challenges of scaling BB84 to larger Qubit systems and contribute to optimizing its robustness against noise and eavesdropping in future quantum communication systems.

The Proposed BB84 protocol is based on the following phases:

I. Exchange of raw keys

During the quantum phase, both legitimate users utilize quantum channel and measurements according to the BB84 protocol. The bases for Qubit generation in the distribution of quantum keys are typically referred to as the X-basis and the Z-basis. The Z-basis represents the conventional computational basis, via Qubits aligned across the 0° and 90° directions ($|0\rangle$, $|1\rangle$ states). The Qubits on the X-basis are superposition states ($|-\rangle$, $|+\rangle$), representing Qubits angles at 45° and 135° [11]. First, Alice constructs a random sequence of Qubits with their associated bases measurement and transfers it across the quantum channel toward Bob. Bob is unaware of the measurements of each Qubit, she receives the measurements and then randomly selects their measurement bases to figure out the quantum state, with or without the eavesdropper's existence.

II. Key Shifting

In the classical phase, to derive a confidential key following the protocols, both parties communicate over a classical channel about the bases they have used for transmitting and receiving. Both users can transfer their selected bases used for measurement and then disclose some information to detect the eavesdropper. Sometimes Bob selects the accurate bases and other times Bob selects the incorrect ones, like Alice selects each base at random. Bob's measurement would be imperfect if he had selected the incorrect bases, after bases comparison, the sequence of bits is considered to generate a Shifted Key ($K^{shifted}$) also referred to as basis reconciliation.

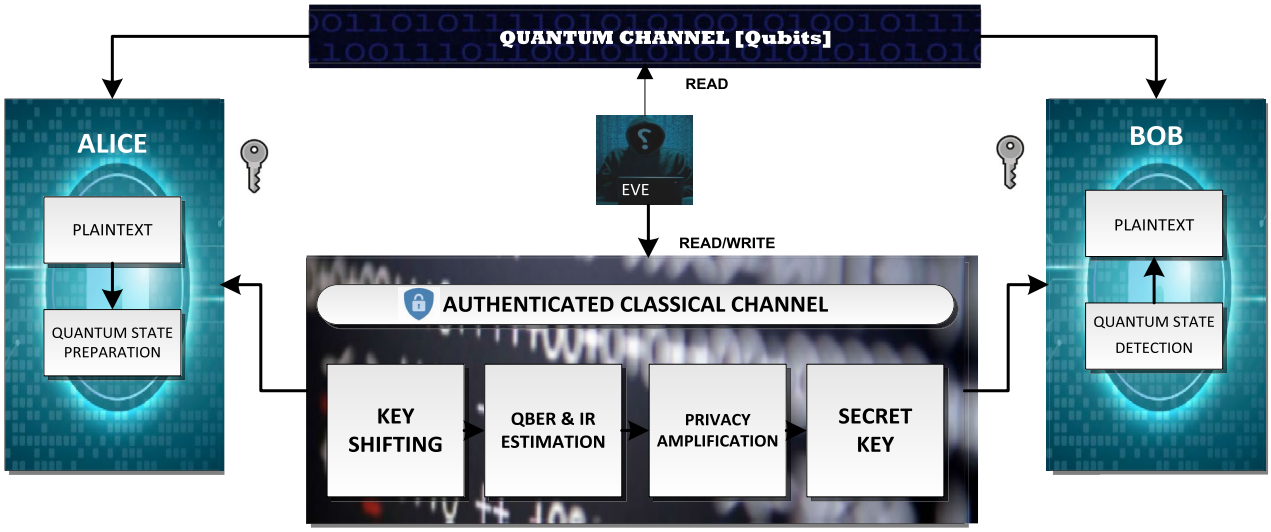


FIGURE 3. Quantum key exchange in proposed BB84 protocol.

III. Error Detection and Information Leakage Estimation

Error detection plays a crucial role in ensuring the security and reliability of the protocol. It allows Alice and Bob to determine whether Qubits have been intercepted by comparing specific portions of their measurements. The QBER is calculated as an approximation of the error rate in the communication, accounting for errors caused by eavesdropping, noise, and other factors. The error rate is determined using (1).

$$QBER = \frac{No\ of\ Bits\ Intercepted\ By\ Eaves}{Total\ No\ of\ Transmitted\ Bits} \tag{1}$$

If the estimated QBER based on the Shifted Key is high, it indicates the eavesdropper's presence in the quantum channel. To evaluate how the proposed protocol should proceed, the QBER is checked against the predefined threshold. When the QBER approaches 85% or above, it becomes problematic as it reveals a high possibility of being detected or environmental challenges. In such a case, the key becomes insecure, and both of them discard it and proceed again. While analyzing errors, Alice and Bob evaluated the possibility of data leaks within an acceptable range. They predicted how much information might be imposed on an eavesdropper that can be estimated using (2).

$$IR = \frac{Right\ Basis\ Selection}{Total\ no\ of\ Bits\ Attacked} \tag{2}$$

IV. Privacy Amplification

After completing the above phases, privacy amplification is performed by eliminating information that an eavesdropper might discover. This is an optional step, however, it is essential if there's the risk that the majority of the information is intercepted by an eavesdropper. It minimizes the total length of the raw key, this alteration in key length is acceptable which guarantees the secrecy of the obtained key. Because of unconditional security, QKD does not require classical channels to be confidential. However, they must be authenticated in terms of raw key exchange, basis shifting, and error detection.

As depicted in FIGURE 3, the protocol encapsulates various phases of the key exchange and demonstrates how quantum properties inherently ensure secure key generation and distribution throughout the transmission process. By incorporating additional Qubit pairs and bases into the key exchange, the BB84 protocol enhances its robustness against eavesdroppers. In particular, by increasing the raw key length, Alice and Bob can eliminate error-prone Qubits while preserving reliable Qubits for secure communication. Since Qubits are highly sensitive to disturbances, so eavesdropping introduces detectable errors, allowing Alice and Bob to discard compromised bits and keep the secure ones.

1) BB84 IMPLEMENTATION ON IBM QX (CASE 2: WITH EAVESDROPPER)

This study evaluates the performance of the BB84 protocol on the IBM Quantum Experience [34], analyzing its response to variations in key length and the presence of an eavesdropper. The proposed study utilized the 9, 12, and 16 Qubit configurations of the BB84 protocol. TABLE 1 presents the quantum operations that Alice and Bob executed on 9 Qubits without eavesdropper interceptions, the initial bit value of every Qubit can be kept unchanged (expressed as '-') or set to 1 (expressed as 'X'). According to the bit value, Alice deploys a Hadamard (H) gate [12] to certain Qubits, turning them from the computational basis to the diagonal basis or vice versa. To be more precise, Alice sets Q[0], Q[0], Q[1], Q[3], Q[6], and Q[7] in the superposition state essential for encoding in the diagonal basis by employing the Hadamard gate to them. Meanwhile, Bob integrates Hadamard (H) gates with measurement (M) operations. For instance, Bob measures Qubits Q[1], Q[2],

Q[4], and Q[8], whereas he performs Hadamard (H) gates and then a measurement on Qubits Q[0], Q[3], and Q[6] which expresses Bob's choice. The comparison between Alice and Bob is whether a Qubit is preserved or discarded, if their bases align, the Qubit is accepted (A), otherwise, it is discarded (D). The resulting key is derived from the accepted Qubits, in this case, the key is '1111' and gets generated from Alice and Bob's corresponding bases. TABLE 1 shows how Alice and Bob employ these functions for encoding and measuring Qubits to generate a shared key.

TABLE 1. Gates chosen by alice and bob.

Qubits	Q[0]	Q[1]	Q[2]	Q[3]	Q[4]	Q[5]	Q[6]	Q[7]	Q[8]
Initial Bit	X	-	X	X	X	-	-	X	-
Alice's Operation	H	H	-	H	-	-	H	H	H
Bob's Operation	H, M	M	M	H, M	H, M	H, M	M	H, M	M
Comparison	A	D	A	A	D	D	D	A	D
Final Key	1	-	1	1	-	-	-	1	-

TABLE 2. Theoretically expected results, 100% probability of obtaining the encryption key.

Qubits	Theory Expected Results
Q[0]	100% probability of 1
Q[1]	50% probability of each1 and 0
Q[2]	100% probability of 1
Q[3]	100% probability of 1
Q[4]	50% probability of each1 and 0
Q[5]	50% probability of each1 and 0
Q[6]	50% probability of each1 and 0
Q[7]	100% probability of 1
Q[8]	50% probability of each1 and 0

TABLE 2 summarizes the theoretically expected results, it represents the probability of every Qubit remaining in state 0 or 1 upon processing. For instance, the Qubits Q[0], Q[2], Q[3], and Q[7] are expected to be in state 1 with 100% probability, however, the remaining Qubits have a 50% chance to remain in state 0 or 1. After determining the Qubit values, the gates that Alice and Bob selected are evaluated with the expected outcomes. FIGURE 4 illustrates a quantum circuit that begins with the generation of a bit-string, which is encoded into quantum states. Alice prepares and transmits these Qubits to Bob via the quantum channel. Bob then applies specific quantum gates based on his chosen basis, after which both parties measure their respective Qubits. Then these measurements generate a result, which is then compared to the expected outcomes observed in TABLE 2 This study provided a detailed explanation of the implementation of the proposed BB84 protocol with two bases and 9 Qubits, including the processes of gate application and basis selection. The focus was on theoretically predicted outcomes, which serve as a foundation for the measured results. Likewise, FIGURE 4 illustrates the process of key generation using Qubits, where both users perform encoding and decoding across quantum and classical channels. The proposed protocol was also executed with 12 and 16 Qubits using two bases, however, these configurations are not extensively discussed, as the 9-Qubit implementation serves as the foundational basis for protocol analysis.

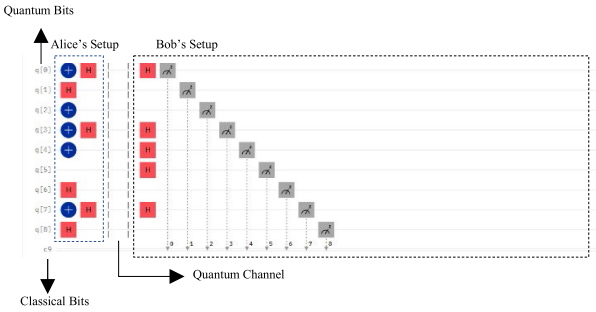


FIGURE 4. An illustration of quantum key generation by deploying 9-Qubits from IBM's QX platform.

2) BB84 IMPLEMENTATION ON IBM QX (CASE 2: WITH EAVESDROPPER)

This section presents an in-depth illustration concerning how key distribution was carried out in case of eavesdropper presence by utilizing 9, 12, and 16 Qubits. Because there is no cloning property, an eavesdropper can only sniff the Qubits but cannot duplicate them. The measurements made in the actual transmission by the eavesdropper using a separate basis are also selected at random like Alice/Bob measurements. There are thus two eavesdropper scenarios: either the Eavesdropper appropriately guesses the basis as chosen by Alice and Bob, or the eavesdropper selects a basis that has no impact on the measurement outcomes on Bob's side. As a result, neither party can identify the eavesdropper because the values remain constant. In contrast, when an eavesdropper guesses the basis inaccurately, Alice and Bob notice an alteration in the values. Due to the 50% chance of getting "0" and 50% chance of getting "1," both communication parties discard it. TABLE 3 and FIGURE 5 illustrate the implementation of an eavesdropper in both scenarios, considering that the eavesdropper attacked Q[0], Q[1], Q[3], Q[4], Q[6], and Q[7].

TABLE 3. Eavesdropper attack on 9 qubits.

Qubits	Alice's Sequence	Alice's Basis	Eave's Basis	Bob's Basis	Final Outcome
Q[0]	1	R	D	R	
Q[1]	0	D	D	R	
Q[2]	1	D		D	
Q[3]	**1**	**R**	**R**	**R**	**1**
Q[4]	1	R	D	D	
Q[5]	0	R		D	
Q[6]	0	D	R	R	
Q[7]	**1**	**R**	**R**	**R**	**1**
Q[8]	0	R	D	D	

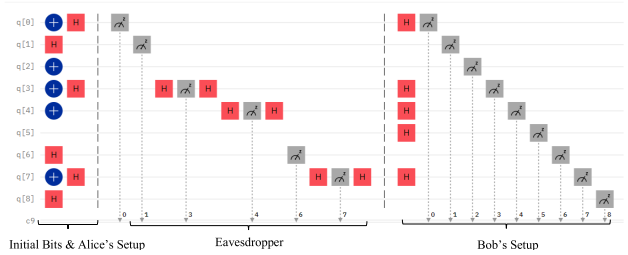


FIGURE 5. Eavesdropper attack based on 9 qubits.

The influence of eavesdropping can be observed in FIGURE 5, which shows the way errors are dispersed over the attacked Qubits. It is evident from the figure that the attack on the quantum channel which is between the first and second barrier makes observable fluctuations. Further analysis of these implementation insights is provided in the results and discussion section for more clarity. After that, we evaluate the variations of quantum states for 12 and 16 Qubits while considering the interruption from eavesdroppers in the quantum channel. As shown in FIGURE 5 and FIGURE 6, the evident fluctuations in quantum states when an eavesdropper is there. Despite Eve's interception, just a pair of Qubits states seemed appropriately predicted, indicating their capability for interpreting information was quietly restricted. The accurate predictions of certain Qubit states over the eavesdropper's interference are made clear through the comparison of Alice's Qubit preparation to Bob's measurement decisions. If the states line up with how gates are configured, it reveals whether eavesdropping is successful or unsuccessful for those specific Qubits. Considering this approach corresponds to a 9-Qubit implementation methodology, we do not elaborate more details here. The results and discussions section presents an extensive discussion of the findings and evaluations.

Furthermore, the 16 Qubit configuration utilizes three bases, including Computational, Hadamard, and Diagonal to promote reliability by making it trickier for an eavesdropper to figure things out. The probable outcomes of productive eavesdropping are restricted by the diversity of bases, concentrating on how significant they are to sustaining the stability and security of quantum communication exchange. FIGURE 6 illustrates an experimental configuration involving an eavesdropper who randomly selects 12 among 16 Qubits for measurements. The configuration becomes clear in FIGURE 6, which sets apart between Alice, Bob, and Eavesdropper. The region in the circuit that is between the second and third barrier represents where eavesdropper attack on Q[0], Q[1], Q[2], Q[5], Q[6], Q[7], Q[8], Q[9], Q[10], Q[12], Q[13], Q[14], and Q[15]. In particular, eavesdroppers accurately determine the states of Q[1] and Q[8], but not the remaining Qubits. When the count of Qubits rises to 16, the difficulty of quantum states increases exponentially. As every Qubit can exist in a superposition containing multiple states, the eavesdropper has to predict the entire quantum state and every Qubit's basis with accuracy. However, the possibility of properly predicting all these minimizes with more Qubits. Therefore, just two-Qubit configurations are normally anticipated by eves precisely, but, ten-Qubit configurations are inaccurate.

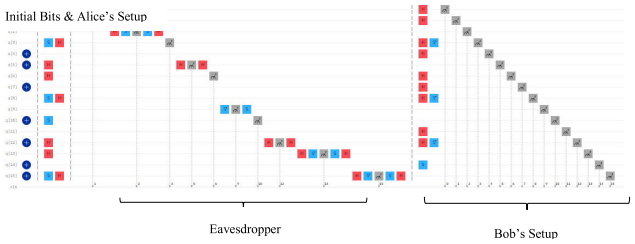


FIGURE 6. Eavesdropper attack based on 16 qubits.

B. E91 PROTOCOL

Existing implementations of the QKD protocols such as E91, which rely on quantum entanglement and Bell's theorem [35], [36] for security, have been demonstrated to be effective under theoretical conditions and through the application of Quantum Error-Correcting Codes (QECC) and classical Error Correction Codes (ECC). However, practical implementations on real quantum devices introduce noise and imperfections that can compromise security in more subtle ways. Noise fluctuations, imperfect hardware, and gate errors can degrade the quality of entanglement and make it easier for an eavesdropper to acquire partial information without being detected. This study proposes novel enhancements to the E91 protocol, targeting real-world noise and potential eavesdropping threats that arise specifically in practical settings. Our approach incorporates reverse gate configurations as an additional layer of security and ensures the protocol's compatibility with noisy quantum devices.

1) E91 PROTOCOL IMPLEMENTATION ON IBM QX

The protocol examined in [14], highlights challenges related to noise and errors in real quantum devices that can compromise its security. In our work, we introduce a novel reverse operation technique during eavesdropping scenarios in the E91 protocol as shown in Algorithm 1 and FIGURE 7. Initially, the two-Qubit operation is performed on an IBM Quantum Experience based on Entanglement. By applying the Hadamard gate which rotates the states $|0\rangle$ and $|1\rangle$ to $|+\rangle$ and $|-\rangle$ and Controlled-NOT (CX) gate whenever control is in state $|1\rangle$, CX creates entanglement. Where both parties publicly share their findings to evaluate the channel's performance which is designed to determine whether eavesdroppers exist or not. By reversing the input sequence at the final stage, we preserve the quantum states, ensuring that any intercepted information remains misleading to the eavesdropper. This approach was not explored in [14] and [16] where the focus was on standard implementations of the protocol. Our reverse operation technique is a significant advancement, offering a practical solution to the security vulnerabilities identified in

previous works. Moreover, this method ensures that eavesdroppers obtain deceptive information, even if they believe they have accurately captured the data.

Algorithm 1 Entanglement-based Proposed E91 Protocol

Input: Initialize Number of Qubits N = 2;
Initialize Quantum register [Q^r], & Classical register [C^r] with size 2
Initialize Q[0] and Q[1] to $|1\rangle$
Perform Hadamard operation with CX operation on Q[0], Q[1]
▶ **Entanglement Generation**
If Control State = $|1\rangle$ **then**
    Gate creates Entanglement
End if
Perform Hadamard or H, S, T operation on Q[0] and Q[1]
Store and measure the output in the Classical register, C[0]
Perform Hadamard or H, $T^{\uparrow}$or Tdg, S on Q[0] and Q[1]
Store and measure the output in the Classical register, C[1]
Configure the initial steps 3 and 4 in reverse order
▶ **Verification Process**
Measure the stored information in the Classical register, C^r
▶**Observe the correlation**
If the value ≈ expected correlation **then**
    Finalize the key
Else
    Discard the key
End if
The Final key is ready
End procedure

FIGURE 7. Quantum circuit with eavesdropping and some reverse operations to show the effect.

2) ERROR MITIGATION IN THE E91 PROTOCOL

Artur Ekert's E91 protocol is not as extensively used as others like the BB84 protocol, as the E91 protocol is susceptible to channel noise and loss. Without preventives, the protocol's strength and reliability may be threatened as the transmission of quantum states can be affected by channel noise and loss due to the inadequacy of error mitigation techniques, where these errors can result in illegitimate key generation or quantum states may be distracted and interrupted by an eavesdropper. However, most of the quantum communication protocols deal with eavesdropping and neglect the effect of noise that causes imprecisions in eavesdropper exposure. Noise and errors from real quantum devices have been a recurring challenge, as demonstrated in [12] and [13] where discrepancies between theoretical predictions and experimental results were attributed to quantum coherence and environmental noise. While these studies acknowledged the impact of noise, they did not propose practical methods to address it. In contrast, our study applies advanced error mitigation techniques derived from quantum error correction codes, which are specifically designed to reduce the noise generated by double-Qubit gates and other imperfections on real quantum hardware. By integrating these techniques into the E91 protocol, we significantly reduce error rates and ensure more accurate results. This practical contribution addresses a critical challenge in the field and represents a significant improvement over previous studies that primarily focused on theoretical results under idealized conditions.

IV. RESULTS AND DISCUSSIONS

This section illustrates the results of our proposed protocol, incorporating BB84 and E91 mechanisms. They exhibit improved eavesdropper ability and attain optimal key lengths, to emphasize their efficiency as they generate reliable and trustworthy keys. This study utilizes the IBM Quantum Experience Platform to execute the circuit in Section III, the local simulator virtual machine for prototyping quantum algorithms, protocols, and circuits up to a limit. The below figures express the probabilities of the occurrence of output states after the measurement.

A. BB84 PROTOCOL

1) BB84 IMPLEMENTATION ON IBM QX (CASE 1: NO EAVESDROPPER)

Through the use of ibmq_qasm_simulator [34], FIGURE 10 shows the BB84 protocol's implementation by utilizing 9-Qubits with 1024 shots representing the theoretically calculated outcome presented in TABLE 4. Where Q[0] is 1 in output, indicating a 100% chance of getting 1. Similar to this, the likelihood of measuring Q[4] and obtaining 0 is 50.3%, while the likelihood of gaining 1 is 49.4%. It is possible to detect a small difference between the theoretically expected probabilities and the results of implementation. TABLE 4 displays the Qubits Q[1], Q[4], Q[5], Q[6], and Q[8] in computational basis state with different result probabilities. These probabilities represent the possibility, as a percentage, of determining each particular basis state when our circuit is tested 1024 times (Shots). Also, reflect on determining how frequently each Qubit turns out in a certain state ($|0\rangle$ or $|1\rangle$) after measurement. According to a simulation of 9 Qubits, the outcome "1111" displays every Qubit that was determined in the state $|1\rangle$.

TABLE 4. Theoretically calculated outcomes for 9 Qubits (Case: No Eavesdropper).

Qubits	Probability of 0 (%)	Probability of 1(%)
Q[0]	0	1
Q[1]	0.01	0.9982
Q[2]	0	1
Q[3]	0	1
Q[4]	0.5039	0.4944
Q[5]	0.4962	0.502
Q[6]	0.507	0.4912
Q[7]	0	1
Q[8]	0.4982	0.5

The proposed protocol is tested on 12 and 16 Qubits with two base counts. As more quantum bits are incorporated, the protocol constructs a safe key with minimal errors, emphasizing its effectiveness. FIGURE 8 reflects the results of the BB84 protocol by using 12 Qubits with 1024 shots. The simulation resulted in the key ''10111'', indicating that some challenges remain to be addressed. In contrast, FIGURE 9 presents the outcomes of the 16-Qubit execution, which significantly outperforms the 9-Qubit and 12-Qubit configurations. The key ''1011011'' was retrieved over 16 Qubit configurations in which the observed Qubits formed a combination of both states $|0\rangle$ and $|1\rangle$. The corresponding Qubits denote either the Qubit collapse to state $|0\rangle$ or $|1\rangle$, representing the results of the Qubit measurements on the computational basis. Likewise, employing more Qubits promotes error resilience, resulting in less challenge for the system to identify and eradicate errors. These conclusions underline the prospect of 16-Qubit execution for quantum communication systems and underscore the worth of scaling the Qubit count in quantum key distribution.

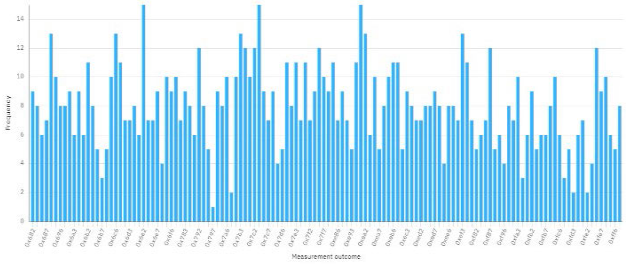


FIGURE 8. Results of BB84 protocol implementation utilizing 12 Qubits obtained using IBM QX with 1024 shots.

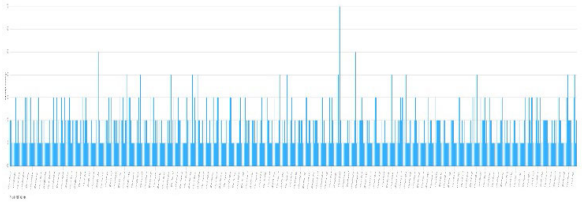


FIGURE 9. Results of BB84 protocol implementation utilizing 16 Qubits obtained using IBM QX with 1024 shots.

2) BB84 IMPLEMENTATION ON IBM QX (CASE 2: WITH EAVESDROPPER)

Furthermore, this study analyzes the performance of the BB84 protocol by employing an eavesdropping scenario, gathering evidence from the same number of shots. Our findings from the 9-Qubits BB84 protocol execution without an eavesdropper are represented in FIGURE 10 (Case 1), whereas FIGURE 10 (Case 2) represents an eavesdropper using 9-Qubits. When Bob notifies Alice about his measurements they discover an eavesdropper, as a fluctuation in the results. These frequency fluctuations from a specific range reflect that measurements that were attempted to intercept the quantum channel are inaccurate.

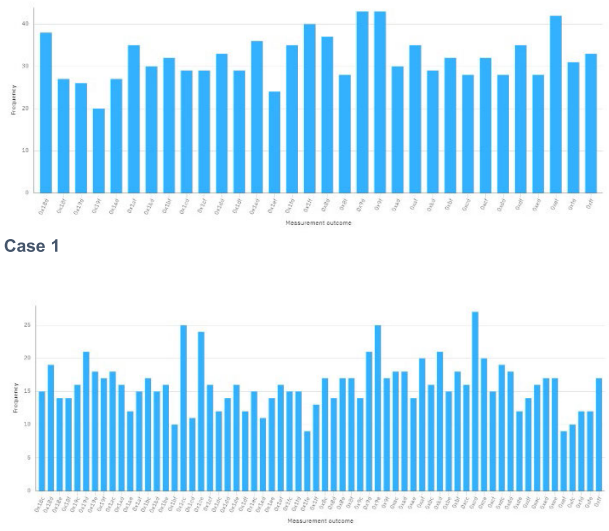


FIGURE 10. Results of BB84 protocol implementation utilizing 9 qubits with and without eavesdropper presence in the quantum channel.

TABLE 2 represents anticipated results and serves as a baseline for practical measurements. By extracting information from these simulation results, the discrepancies reveal the potential of eavesdropping as evidenced in TABLE 5. For instance, the probability for Q[1] is considerably unbalanced, with 0.4615 for 0 and 0.5322 for 1, whereas without eavesdropper anticipated probabilities for 0.01 for 1 and 0.99 for 1. Similar to this, the Qubits Q[0], Q[4], and Q[6] exhibit significant variations, corresponding to probabilities of 0 and 1. If a significant portion of information has been compromised, it is essential to discard the generated key because of confidentiality concerns. Conversely, the privacy amplification step can tackle the compromised bits if only a small portion is captured. This approach ensures the generated key that is secure against possibilities including intercepting and eavesdropping.

TABLE 5. Theoretically calculated outcomes for 9 qubits.

Qubits	Probability of 0 (%)		Probability of 1 (%)	
	Without Eavesdropper	With Eavesdropper	Without Eavesdropper	With Eavesdropper
Q[0]	0	0.4971	1	0.4966
Q[1]	0.01	0.4615	0.9982	0.5322
Q[2]	0	-	1	-
Q[3]	0	0	1	1
Q[4]	0.5039	0.4831	0.4944	0.5106
Q[5]	0.4962	-	0.502	-
Q[6]	0.507	0.5056	0.4912	0.4803
Q[7]	0	0	1	1
Q[8]	0.4982	-	0.5	-

After that, the proposed BB84 protocol is on a 12 Qubits configuration as seen in FIGURE 11, where Eve intercepts 8 Qubits via two bases utilization. The resulting fluctuations in the measurement frequencies indicate the effects induced by eavesdropping. Unusually low and high measurement frequencies are signs of potential eavesdropping in quantum systems. Low frequencies reflect alterations or errors imposed by eavesdropping, while high frequencies signify that an eavesdropper negatively affects the system by over-representing some states.

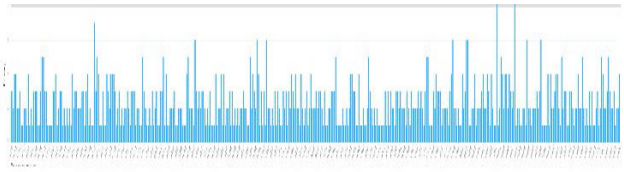


FIGURE 11. Results of implementation of BB84 protocol with eavesdropper attack based on 12 Qubits.

In the last, 16 Qubits were tested on the proposed BB84 protocol under an eavesdropper attack where Eve made attempts to intercept 13 of them. However, she correctly identified the state of 2 Qubits with 100% accuracy on the measurement outcome of Q[1] and Q[8]. Despite her minimum achievement, Eve was unsuccessful in getting the remaining 11 Qubits, proving the proposed protocol's resilience. It becomes trickier for Eve to precisely estimate the states due to the 16 Qubits are configured using three different bases, contributing to the system's complexity and uncertainty. As presented in TABLE 6, Q[0], Q[2], and Q[9] reflect probabilities for both 0 and 1 which are roughly 50%, revealing that Eve's interception caused noise and uncertainty in the measurement process. These inaccurate measurements point out Eve's challenges, as Qubits are in superposition states and are extremely sensitive to measurements. This configuration works more efficiently as opposed to the 9 and 12 Qubits structure due to its more complexity and deployment of three bases. The added bases ensure a more reliable key generation process by making it exceptionally difficult for an eavesdropper to remain quiet.

Previous studies such as [15] have implemented the BB84 protocol using 8 Qubits with two bases, both with and without the presence of an eavesdropper. While these studies demonstrated the effectiveness of the BB84 protocol in controlled environments, they did not explore the impact of increased Qubit lengths on security. In contrast, we extend the BB84 protocol by implementing longer Qubit lengths of 9, 12, and 16. The selection of Qubits ensured that they remained manageable while sustaining an adequate degree of security. TABLE 7 presents the proposed BB84 protocol simulation results which confirms that increasing Qubits also improves the security and chances of eavesdropping detection. The QBER reflects the eavesdropper's key length interception that helps detect and mitigate intercepted Qubits. For instance, the QBER is 0.62 and the information leakage

TABLE 6. Theoretically Calculated Outcomes for 16 Qubits (Case 2: With Eavesdropper).

Qubits	Probability of 0 (%)	Probability of 1 (%)
0	0.4853	0.5146
1	0	100
2	0.5078	0.4921
3	-	-
4	-	-
5	0.5068	0.4931
6	0.5087	0.4912
7	0.5156	0.4843
8	100	0
9	0.5234	0.4765
10	0.5117	0.4882
11	-	-
12	0.4931	0.5068
13	0.4951	0.5048
14	0.5039	0.496
15	0.5	0.5

is 0.2 with 8 Qubits adjustments. Among the configurations, the 16 Qubit configuration shows the most effective performance with a minimal information leakage rate of 0.15, resulting in an ideal choice for resilient quantum key distribution.

TABLE 7. Proposed BB84 protocol.

	Existing Work [15]	.	.	Proposed Work
Qubits	8	9	12	16
Final Key Length	5	4	5	7
Attack on Bits by Eaves	5	7	8	13
Right Basis Selection	1	2	2	2
Wrong Basis Selection	4	5	6	11
Information Leakage	0.2	0.28	0.25	0.15
QBER	0.62	0.77	0.66	0.81

The results and analysis show that increasing the Qubit length significantly enhances the security of the protocol by making it more difficult for eavesdroppers to intercept bits without detection. This is particularly important because, as noted in [13] and [14] shorter Qubit lengths make the protocol more susceptible to intercept-resend and brute force attacks. By demonstrating how increased Qubit lengths improve security, we address a gap in the literature and offer a novel contribution to the field of QKD.

B. E91 PROTOCOL

1) E91 PROTOCOL IMPLEMENTATION ON IBM QX

The Initial phase angle of $|10\rangle$ is determined to be $9\pi/8$ which acts appropriately with no disruptions. However, the calculated $9\pi/8$ rotates to $15\pi/8$, revealing an unauthorized attempt to access the key. While the simple execution and

eavesdropping are theoretically discussed, this study concentrates on the result of the E91 protocol deploying the reverse operation technique. Building on the security provided by Bell's theorem, we introduce reverse gate configurations to further complicate any potential eavesdropping attempts. By setting gate inputs in reverse order at the final stage, the protocol obfuscates the quantum states, making it difficult for an eavesdropper to gain useful information. The FIGURE 12 reflects the E91 protocol was successfully executed according to our proposed E91 algorithm. To prevent such eavesdropping, this study configures reverse gates [22]. By intentionally disrupting the computational basis state, such configuration transfers it from state $|10\rangle$ to $|11\rangle$. This technique does not replace traditional security measures but adds a layer of defense, particularly in noisy environments. Unlike traditional approaches that focus solely on correcting transmission errors, this study introduces a mechanism that actively transforms intercepted information into deceptive data. This ensures that even if an eavesdropper acquires some information, the data they obtain will be misleading and effectively useless.

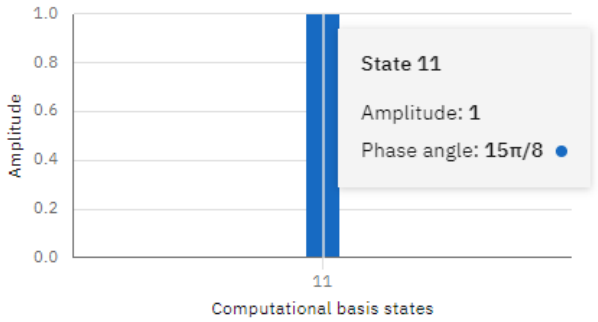


FIGURE 12. Results of Implementation of Eavesdropping and Some Reverse Operations to Show the Effect, where computational basis state from $|10\rangle$ to $|11\rangle$ are depicted.

In addition to using traditional QECC and ECC methods, this research applies advanced error mitigation techniques designed specifically for real-world quantum devices, which experience higher noise levels. By reducing the impact of noise from quantum gates, our approach ensures the fidelity of the entangled states and enhances the overall security and reliability of the key generation process.

2) ERROR MITIGATION IN THE E91 PROTOCOL

This study considers the mechanism to mitigate the impact of noise and external disturbance by incorporating error correction codes. The proposed E91 protocol incorporates a noise calibration layer before the measurement procedure to overcome shortcomings, optimizing the precision and reliability of quantum systems. This implies estimating the inbuilt noise in the measuring devices where insignificant errors can accumulate and jeopardize the security of obtained keys. Throughout communication, stable probabilities are expected for quantum states including $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. However, because of noise and eavesdropping, these probabilities

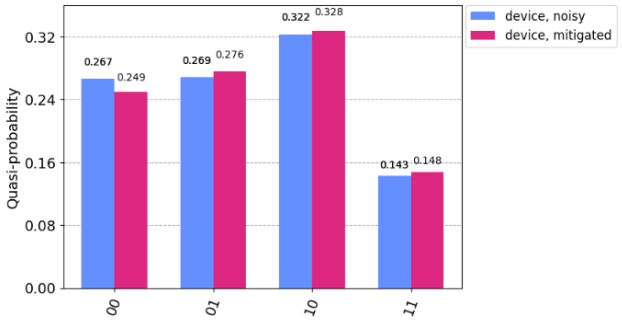


FIGURE 13. Error mitigation in real quantum device.

fluctuate which leads to errors. For instance, error mitigation resolves the system to bring it back in line if noise gives rise to state $|00\rangle$ getting a lower probability than expected as shown in FIGURE 13. As the mitigation can't recover the state to its exact, it aims to adjust it nearer to the precise value. For the remaining states $|01\rangle$, $|10\rangle$, and $|11\rangle$ their probabilities are nearly restored, assuring that the exchange of information is as stable as possible. The communication process is accelerated, error counts are reduced and more efficient key generation is made. The proposed E91 protocol as presented in TABLE 8, shows its durability and sophisticated safety measures.

TABLE 8. Proposed E91 protocol.

Cases	Simple	With Eavesdropper	With Reverse Operations and Error Mitigation Technique
States	$\|10\rangle$	$\|10\rangle$	$\|11\rangle$
Phase Angle	$9\pi/8$, Amplitude=1	$15\pi/8$, Amplitude=1	$15\pi/8$, Amplitude=1
State Probability (Noisy)	0.267	0.269	0.143
State Probability (Mitigated)	0.249	0.276	0.148
Information Leakage	-	High	Low

With $|10\rangle$ state and a phase angle of $9\pi/8$ at an amplitude of 1, the initial setting serves as a baseline without an eavesdropper. It pointed out the state probability reduction from 0.267 to 0.249 after error mitigation. The second setting showed substantial information leakage due to eavesdropping, with the state probability rising from 0.269 with noise to 0.276 after mitigation. Lastly, the eavesdropper substantially reduced the state probability from 0.143 to 0.148, causing unnecessary information leakage by deploying reverse operations and error mitigation on $|11\rangle$ state with the same phase angle. This strategy gives the eavesdropper inaccurate details, causing the data they capture to differ from the original.

V. CONCLUSION

In this study, a detailed analysis of QKD protocols, BB84 and E91, focusing on their resistance to eavesdropping has been evaluated. The main contribution involves the experimental realization of these protocols, which are modified to different bases and Qubit counts and evaluated on quantum simulators and devices. By comparing theoretical predictions with practical outcomes, mainly in the BB84 protocol, the study reveals key discrepancies that expose eavesdropping. Through simulations via Qiskit, insights were gathered under different configurations, especially in terms of error probabilities. The simulation results show fluctuations in probabilities from 0 to 0.4971% and 100 to 0.4966%, indicating eavesdropper measurements. As Qubit lengthens, guessing polarization configurations becomes more difficult, resulting in enhanced protocol security. In cases where Qubits are compromised, techniques such as error detection, information leakage, and privacy amplification ensure secure communication. Furthermore, the E91 protocol has been theoretically proposed to offer high resistance to errors, the experimental findings reveal its susceptibility to noise and eavesdropping. To address these vulnerabilities, this study adds a layer of security by incorporating reverse gate configurations and error mitigation techniques. These measures not only render any captured data worthless but also significantly minimize the impact of noise. Specifically, noise was reduced by filtering out inaccurate measurement results and recalibrating the quantum system using error mitigation techniques. These processes proved effective in optimizing the stability and privacy of the protocol, as demonstrated in experiments on real quantum devices. Notably, Qubit states are optimized from initial values of 0.267, 0.269, 0.322, and 0.143 to 0.249, 0.276, 0.328, and 0.148, respectively. In comparison to previous studies, which overlooked these critical enhancements, proposed research addresses these gaps by improving the protocol's resilience to both noise and eavesdropping. Future research will explore the potential of higher-dimensional quantum states, known as Qudits, as a replacement for binary quantum bits. Due to their ability to express multiple levels, Qudits can store significantly more information per particle, potentially increasing data transmission capacity and enhancing the overall efficiency of QKD networks.

ACKNOWLEDGMENT

The authors acknowledge the incorporation of the IBM Quantum Experience Platform for the execution of the experiments, which played an essential role in accomplishing the experimental results presented in this study.

REFERENCES

[1] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and critical review of RSA based public key cryptographic schemes: Past and present status," *IEEE Access*, vol. 9, pp. 155949–155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[2] A. Nurgaliyev and H. Wang, "Comparative study of symmetric cryptographic algorithms," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Lijiang City, China, Oct. 2021, pp. 107–112, doi: 10.1109/NaNA53684.2021.00026.

[3] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

[4] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa, "An overview of quantum cryptography and Shor's algorithm," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 7487–7495, Oct. 2020, doi: 10.30534/ijatcse/2020/82952020.

[5] N. Aquina, S. Rommel, and I. T. Monroy, "Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution," in *Proc. 24th Int. Conf. Transparent Opt. Netw. (ICTON)*, Bari, Italy, Jul. 2024, pp. 1–4, doi: 10.1109/icton62926.2024.10648124.

[6] A. A. Abushgra, "Variations of QKD protocols based on conventional system measurements: A literature review," *Cryptography*, vol. 6, no. 1, p. 12, Mar. 2022, doi: 10.3390/cryptography6010012.

[7] S. Subramani and S. K. Svn, "Review of security methods based on classical cryptography and quantum cryptography," *Cybern. Syst.*, vol. 56, no. 3, pp. 302–320, Jan. 2023, doi: 10.1080/01969722.2023.2166261.

[8] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Quantum key distribution: Modeling and simulation through BB84 protocol using Python3," *Sensors*, vol. 22, no. 16, p. 6284, Aug. 2022, doi: 10.3390/s22166284.

[9] V. Gaur, D. Mehra, A. Aggarwal, R. Kumari, and S. Rawat, "Quantum key distribution: Attacks and solutions," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3563118.

[10] M. A. Sharma and D. A. Kumar, "A survey on quantum key distribution," in *Proc. 2nd Int. Conf. Issues Challenges Intell. Comput. Techn. (ICICT)*, 2019, pp. 1–4.

[11] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3831–3868, Aug. 2021, doi: 10.1007/s11831-021-09561-2.

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

[13] M. H. Saeed, H. Sattar, M. H. Durad, and Z. Haider, "Implementation of QKD BB84 protocol in qiskit," in *Proc. 19th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Islamabad, Pakistan, Aug. 2022, pp. 689–695, doi: 10.1109/IBCAST54850.2022.9990073.

[14] I. Pedone, A. Atzeni, D. Canavese, and A. Lioy, "Toward a complete software stack to integrate quantum key distribution in a cloud environment," *IEEE Access*, vol. 9, pp. 115270–115291, 2021, doi: 10.1109/ACCESS.2021.3102313.

[15] A. Warke, B. K. Behera, and P. K. Panigrahi, "Experimental realization of three quantum key distribution protocols," *Quantum Inf. Process.*, vol. 19, no. 11, p. 407, Nov. 2020, doi: 10.1007/s11128-020-02914-z.

[16] Y. Begimbayeva and T. Zhaxalykov, "Research of quantum key distribution protocols: BB84, B92, E91," *Sci. J. Astana IT Univ.*, vol. 10, pp. 4–14, Jun. 2022, doi: 10.37943/qrkj7456.

[17] J. Ahn, H.-Y. Kwon, B. Ahn, K. Park, T. Kim, M.-K. Lee, J. Kim, and J. Chung, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD)," *Energies*, vol. 15, no. 3, p. 714, Jan. 2022, doi: 10.3390/en15030714.

[18] M. Mastriani, "Quantum key secure communication protocol via enhanced superdense coding," *Opt. Quantum Electron.*, vol. 55, no. 1, p. 10, Jan. 2023, doi: 10.1007/s11082-022-04303-5.

[19] A. Ahilan and A. Jeyam, "Breaking barriers in conventional cryptography by integrating with quantum key distribution," *Wireless Pers. Commun.*, vol. 129, no. 1, pp. 549–567, Mar. 2023, doi: 10.1007/s11277-022-10110-8.

[20] P. Arteaga-Díaz, D. Cano, and V. Fernandez, "Practical side-channel attack on free-space QKD systems with misaligned sources and countermeasures," *IEEE Access*, vol. 10, pp. 82697–82705, 2022, doi: 10.1109/ACCESS.2022.3196677.

[21] G. Mogos, "Intercept-resend attack on quantum key distribution protocols with two, three and four-state systems: Comparative analysis," in *Proc. 2nd Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2015, pp. 1–4, doi: 10.1109/ICISSEC.2015.7371010.

[22] C. Liu, "Reverse checking of quantum algorithm execution," *IEEE Access*, vol. 8, pp. 228702–228710, 2020, doi: 10.1109/ACCESS.2020.3043187.

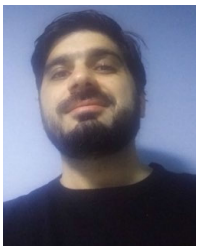
[23] A. Gopal, "Experiments with B92 quantum key distribution algorithm implementation," *Math. Comput. Sci.*, preprint, Jul. 2022, doi: 10.20944/preprints202207.0279.v1.
[24] L. Zhang, A. Miranskyy, W. Rjaibi, G. Stager, M. Gray, and J. Peck, "Making existing software quantum safe: A case study on IBM Db2," *Inf. Softw. Technol.*, vol. 161, Sep. 2023, Art. no. 107249, doi: 10.1016/j.infsof.2023.107249.
[25] M. Waqar, S. Fareed, A. Kim, S. U. R. Malik, M. Imran, and M. U. Yaseen, "Malware detection in Android IoT systems using deep learning," *Comput., Mater. Continua*, vol. 74, no. 2, pp. 4399–4415, 2023.
[26] S. Gupta, K. K. Gupta, P. K. Shukla, and M. K. Shrivas, "Blockchain-based voting system powered by post-quantum cryptography (BBVSP-PQC)," in *Proc. 2nd Int. Conf. Power, Control Comput. Technol. (ICPCT)*, Raipur, India, Mar. 2022, pp. 1–8, doi: 10.1109/ICPC2T53885.2022.9776966.
[27] M. Waqar, M. U. Mustafa, F. Jabeen, and S. A. Shah, "Performance improvement of time-sensitive fronthaul networks in 5G cloud-rans using reinforcement learning-based scheduling scheme," *IEEE Access*, vol. 12, pp. 59756–59770, 2024.
[28] V. Kalaivani, "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications," *Pers. Ubiquitous Comput.*, vol. 27, no. 3, pp. 875–885, Jun. 2023, doi: 10.1007/s00779-021-01546-z.
[29] H. Shu, "Asymptotically optimal prepare-measure quantum key distribution protocol," *Int. J. Theor. Phys.*, vol. 62, no. 8, p. 191, Aug. 2023, doi: 10.1007/s10773-023-05447-0.
[30] Q. Zeng, H. Wang, H. Yuan, Y. Fan, L. Zhou, Y. Gao, H. Ma, and Z. Yuan, "Controlled entanglement source for quantum cryptography," *Phys. Rev. Appl.*, vol. 19, no. 5, May 2023, Art. no. 054048, doi: 10.1103/physrevapplied.19.054048.
[31] F. Borges, P. R. Reis, and D. Pereira, "A comparison of security and its performance for key agreements in post-quantum cryptography," *IEEE Access*, vol. 8, pp. 142413–142422, 2020, doi: 10.1109/ACCESS.2020.3013250.
[32] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, "Quantum cryptography and US digital security: A comprehensive review: Investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security," *Comput. Sci. IT Res. J.*, vol. 5, no. 2, pp. 390–414, Feb. 2024, doi: 10.51594/csitrj.v5i2.790.
[33] S. Prajapat, P. Kumar, D. Kumar, A. K. Das, M. S. Hossain, and J. J. P. C. Rodrigues, "Quantum secure authentication scheme for Internet of Medical Things using blockchain," *IEEE Internet Things J.*, vol. 11, no. 23, pp. 38496–38507, Dec. 2024, doi: 10.1109/JIOT.2024.3448212.
[34] A. Das and A. Chakrabarti, "A comprehensive study of noise models simulation using various quantum simulators," in *Proc. Int. Conf. Trends Quantum Comput. Emerg. Bus. Technol.*, Pune, India, Mar. 2024, pp. 1–6, doi: 10.1109/tqcebt59414.2024.10545051.
[35] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: Applications and future prospects," *Frontiers Phys.*, vol. 12, Aug. 2024, Art. no. 1456491, doi: 10.3389/fphy.2024.1456491.
[36] L. Mariani, L. Salatino, C. Attanasio, S. Pagano, and R. Citro, "Simulation of an entanglement-based quantum key distribution protocol," *Eur. Phys. J. Plus*, vol. 139, no. 7, p. 602, Jul. 2024, doi: 10.1140/epjp/s13360-024-05337-2.

NOOR UL AIN received the bachelor's degree in computer science from the Federal Urdu University of Arts, Science and Technology, Islamabad, in 2021, and the master's degree in information security from COMSATS University Islamabad, Pakistan, solidifying her expertise in the field. Currently, she is actively pursuing certifications in both security and cloud computing. She has also completed the Certified Ethical Hacker (CEH) certification by EC-Council, further enhancing her proficiency in these critical domains. She represented her work on cyber security in International Conference on AI and the Digital Economy (CADE 2023), which focuses on machine learning and artificial intelligence algorithms to detect cyberbullying. Her research interests include cutting-edge realm of quantum cryptography and quantum key distribution protocols, reflecting her commitment to exploring innovative solutions and advancing secure communication methods in the quantum era.

MUHAMMAD WAQAR received the B.S. degree in computer engineering and the M.S. degree in computer networks from COMSATS University Islamabad (CUI), Islamabad Campus, Pakistan, in 2011 and 2015, respectively, and the Ph.D. degree in 5G cloud RANs and security from Sejong University, Seoul, South Korea, in 2020. He was an Assistant Professor with CUI. He is currently a Lecturer with the University of Suffolk, Ipswich, U.K. He is also with the DigiTech Centre, Digital Futures Institute (DFI), Adastral Park, a regional hub for technology-focused research, knowledge exchange, and innovation, in collaboration with the University of Suffolk. He has authored several research articles in peer-reviewed journals and international conferences. His research interests include computer networks, cryptography, penetration testing, malware analysis, image processing, and deep learning. He serves as a reviewer for esteemed journals and a member for multiple editorial boards. He actively participates in international conferences as a member of steering and technical program committees.

ANAS BILAL (Senior Member, IEEE) received the B.S. degree in telecommunication and networks from Iqra University, Pakistan, in 2013, the M.S. degree in electrical and electronic systems from the University of Lahore, Pakistan, in 2016, and the Ph.D. degree in electronics science and technology from Beijing University of Technology, Beijing, China, in 2021. Currently, he is an Assistant Professor and a Undergraduate Supervisor with the Software College, Hainan Normal University, Haikou, China. He has published more than 30 technical articles in scientific journals and conference proceedings. His current research interests include AI, computer vision, image processing, medical imaging, remote sensing, cyber security, and pattern recognition. His research work focuses on various image processing and computation communication methods through technology, developing new and innovative approaches for medical imaging, and remote sensing images. He is a member of the IEEE Computer Society Technical Community on Computer Architecture and the IEEE Young Professionals. He is the Program Chair of ICPPOE 2022 and ICAICT 2023 and a member of the Technical Program Committee at AIIPCC 2023. He is an Academic Editor of *PLOS One* and an Advisory Board Member of *Journal of Social Sciences Advancements*.

AJUNG KIM received the B.S. degree in physics from Seoul National University, South Korea, in 1988, and the M.S. and Ph.D. degrees majoring in information theory from Northwestern University, Evanston, USA. She was a Postdoctoral Research Fellow and a Research Associate with Northwestern University. She was with Samsung Electronics, and the School of Engineering and Applied Science, Harvard University, as an Exchange Professor. Since 2003, she has been a Professor with the Department of Optical Engineering, Sejong University, Seoul, South Korea. Her research interests include network communications, quantum computing, cryptography, information security, and optical networks.



HAIDER ALI received the master's degree in electronic systems design engineering from Manchester Metropolitan University (MMU), U.K., and the Ph.D. degree from the University of Derby (UoD), U.K. He is currently a Lecturer with the School of Computing, UoD. He was with COMSATS University Islamabad, Abbottabad Campus, Pakistan, as a Lecturer, from 2011 to 2016. He is currently working on energy-efficient algorithms for task mappings on modern embedded systems for real-time applications. His research areas of interests include biomedical systems design, the Internet of Things (IoT), algorithms design, and cybersecurity. He has received two best paper awards from international conferences. He has served as a member for the technical program committee for different workshops and serves many reputable journals and transactions as a reviewer.

UMAIR ULLAH TARIQ received the B.Sc. degree(Hons.) in computer engineering from the COMSATS Institute of Information Technology, Pakistan, in 2008, and the M.Sc. degree in computer engineering and the Ph.D. degree in computer science and engineering from the University of Engineering and Technology, Taxila, in 2013 and 2018, respectively. Currently, he is a Lecturer-ICT with the College of Information and Communication Technology, School of Engineering and Technology, CQUniversity Sydney. Before this, he was a Digital Transformation Engineer with BlueScope Steel Port Kembla and a Sessional Academician with CQUniversity Sydney. He has published two book chapters and more than 20 refereed papers that include high-impact journal and conference papers. His area of research interests include evolutionary computation, machine learning, energy-aware scheduling, the Internet of Things, and wireless sensor networks.

MUHAMMAD SHAHROZ NADEEM received the B.S. and M.S. degrees in computer science from the National University of Computer and Emerging Sciences (NUCES), Pakistan, in 2015 and 2017, respectively, and the Ph.D. degree in computer science (focused on computer vision) from the University of Derby, U.K., in 2023. He is currently a Lecturer in computing and cyber security with the University of Suffolk, U.K. He was a Research Associate with the Reveal Laboratories and Cyber Security Research Group, where he has published several research articles in peer-reviewed journals and conferences. His current research focus is on the detection of weapon-based violence utilizing synthetic data. His research interests include deep learning, data science, image restoration, computer vision, cyber security, and penetration testing. He is the General Chair of the NGH Workshop.