Volume 11, Issue 7, July – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

Noise-Aware Adaptive Quantum Secure Communication Using Decoy-State Encoding

Podinala Sharonjyoshna[1]; S. Surekha[2]

[1,2]Department of Computer Science and Engineering, UCEK (A), JNTU Kakinada, Andhra Pradesh, India-533003.

Publication Date: 2026/08/05

Abstract: Quantum Key Distribution is theoretically possible secure communication through the use of quantum-mechanical principles, such as superposition, measurement disturbance, and others. The BB84 and E91 protocols provide security by leveraging quantum principles against classical eavesdropping; nevertheless, the current implementation of QKD is vulnerable to photon-number-splitting attacks, imperfections in the devices used, and environmental quantum noise. Improving practical resistance to all of those is crucial for providing secure real-life use of QKD. Extending the current state-of-the-art through further development of research on eavesdropper detection and improvement of qubit-based security mechanisms, this research aims to develop the state-of-the art further by introducing a decoy-state BB84 framework and analyzing the behavior of such a system under realistic quantum noise. To find solutions to these problems, the current research will try to adopt the decoy-state BB84 model and analyze the system behavior under realistic quantum noise scenarios. So, the proposed approach, a standard BB84 protocol, will first be formulated and then further enhanced with decoy-state pulse generation to handle the vulnerabilities due to multi-photon pulses. Models like depolarizing noise, amplitude damping, and measurement errors will be used as real-world quantum channels. The model performance will be measured in terms of various performance metrics such as Key agreement ratio, Quantum Bit Error rate, and secure key rate for different qubit lengths. Scalability analysis and validation based on IBM quantum hardware will also be performed in order to measure the impact of real-world device noise on the reliability of generated keys.

Keywords: *Quantum Key Distribution, E91 Protocol, Photon Number Splitting Attack, BB84 Protocol, Eavesdropping Detection.*

How to Cite: Podinala Sharonjyoshna; S. Surekha (2026) Noise-Aware Adaptive Quantum Secure Communication Using Decoy-State Encoding. *International Journal of Innovative Science and Research Technology*, 11(7), 2891-2897. https://doi.org/10.38124/ijisrt/26jul1740

I. INTRODUCTION

QKD allows two legitimate users to create a common cryptographic key utilizing the principles of Quantum mechanics, thus providing security from any form of eavesdropping. Unlike traditional systems, which rely on security due to the computational complexities involved, QKD ensures information security based on quantum mechanical principles such as disturbance caused by the measurement process and the inability to clone quantum states [3], [5].

Protocols like BB84 and E91 have been widely used for generating keys securely and form the foundation of QKD systems [4]. But practical implementations are different from theoretical models because of flaws in the devices, photon losses, and environmental noise. These factors deteriorate the system performance and limit real-world deployment [6].

In this regard, PNS attacks leverage multi-photon pulse emissions from real-life photon sources, whereas channel noise such as depolarizing effects, amplitude damping, and measurement errors increases the QBER. This makes it hard and difficult to make sure both high security and efficient key generation in real communication systems [3].

To mitigate these challenges, decoy state and quantum noise modelling have been introduced. By introducing pulses with different levels of signal, the decoy-state method makes it possible to detect PNS attacks. However, most existing methods and models treat security and noise analysis separately without a single unified model that combines the two aspects practically [5], [6].

This work proposes a decoy-state BB84-based QKD framework that includes realistic quantum noise modelling. The efficiency of the suggested algorithm is measured through QBER, SKR, and KAR, considering different qubit lengths and scalability tests.

II. RELATED WORK

The study of QKD is carried out efficiently as an essential method of ensuring secure transfer of information in both traditional and fiber-optic networks in order to establish the efficiency and reliability of the Cryptographic Protocols.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

Lee et al. [1] proposed an enhanced eavesdropping detection mechanism for BB84 quantum key distribution systems by analysing statistical disturbances introduced during interception, demonstrating that deviations in measurement outcomes can be effectively used to identify potential eavesdropping activities, thereby improving protocol reliability under attack conditions. In Begimbayeva and Zhaxalykov et al. [2], various quantum key distribution protocols such as BB84, B92, and E91 have been investigated to reveal the effectiveness of the BB84 protocol in terms of its simplicity and security despite practical difficulties in its implementation. This literature review highlights the importance of eavesdropping detection and the proper selection of protocols for quantum communication systems.

In response to the resource-related and efficiency problems discussed by earlier studies, additional research has been conducted towards the Optimal Performance of Quantum Systems under Practical Constraints. Chen & Wang et al. [5] provided an extensive overview of the various eavesdropping detection strategies in quantum cryptography systems, discussing different attack models and the approaches used for their detections, while underscoring the necessity of efficient error estimation to provide a secured channel under noisy conditions, Efficiency gains in key generation and transmission were examined by Gupta & Sharma et al. [6], who discussed the compromise between the improvement of security and the resources required for its implementation. In line with the aforementioned body of literature, the framework introduced in the current study is based on implementing the Decoy-state BB84 protocol, along with realistic Quantum Noise Modelling in Qiskit & Streamlit, under simulated communication conditions.

Many works have studied the security behaviour and the performance of the channel of QKD systems in realistic communication scenarios. For example, Nojun and Lauri et al. [3] studied the strength and robustness of BB84 in relation to intercept-resend attacks, in which it has been observed that any kind of illegal measurement definitely has an impact on the transmitted particles' state and results in variations of QBER. However, this study reveals that noise in the channels can cover up such attacks, making it very difficult to detect any type of attack. Kim and Park et al. [4] studied the performance of various QKD protocols in fibre optic communication networks and found that channel losses and noise have a significant impact on the key generation rate and overall system performance, especially for long-distance transmissions.

III. METHODOLOGY

The research presented proposes an enhanced QKD framework built upon the decoy-state BB84 approach integrated with realistic quantum noise modelling and attack simulation. The proposed system adopts a noise-aware modelling strategy by dynamically incorporating depolarizing noise, amplitude damping, and measurement disturbances during quantum transmission and is implemented using the Qiskit quantum simulation framework and evaluated under practical communication conditions including channel noise and eavesdropping attacks. The methodology consists of quantum state preparation, decoy-state generation, noisy quantum transmission, eavesdropping simulation, key sifting, error correction, and secure key generation. Figure 1 illustrates the workflow of this simulation, which is of 4 different phases – Quantum State Preparation and Environment Setup, Pulse Generation and Secure Transmission, Measurement and Key Generation, and Security and Performance Analysis.

- *Phase 1: Setup and Quantum State Preparation*

The System begins with this first phase, which is the establishment of the communication framework between two legitimate participants, where Alice performs the transmission, and Bob receives the quantum information. The participants then establish the QKD scheme to be followed, like BB84, and define the encoding rules for representing binary information using Quantum States. [7] A secure Classical Authenticated Channel is also established. Initially, all generated Qubits are initialized to the |0> state before Quantum State Preparation. An entangled pair is created using two gates – the Hadamard Gate (H), which creates Superposition(0 or 1), and the CX (CNOT) Gate, which makes the next bit flip when the first bit is 1. A Quantum entangled pair must be created to get the same key for both sender and receiver. If someone tries to measure the key, then the key changes and the Superposition will get destroyed, thus detecting Eavesdropping.[11] Once the system is ready with the setup, Alice generates a random binary sequence that forms the basis of the secret key. She then encodes each bit into Quantum states (qubits) using randomly selected polarization bases, such as rectilinear and diagonal bases. These Quantum States represent the actual carriers of information that will be transmitted through the Quantum Channel.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

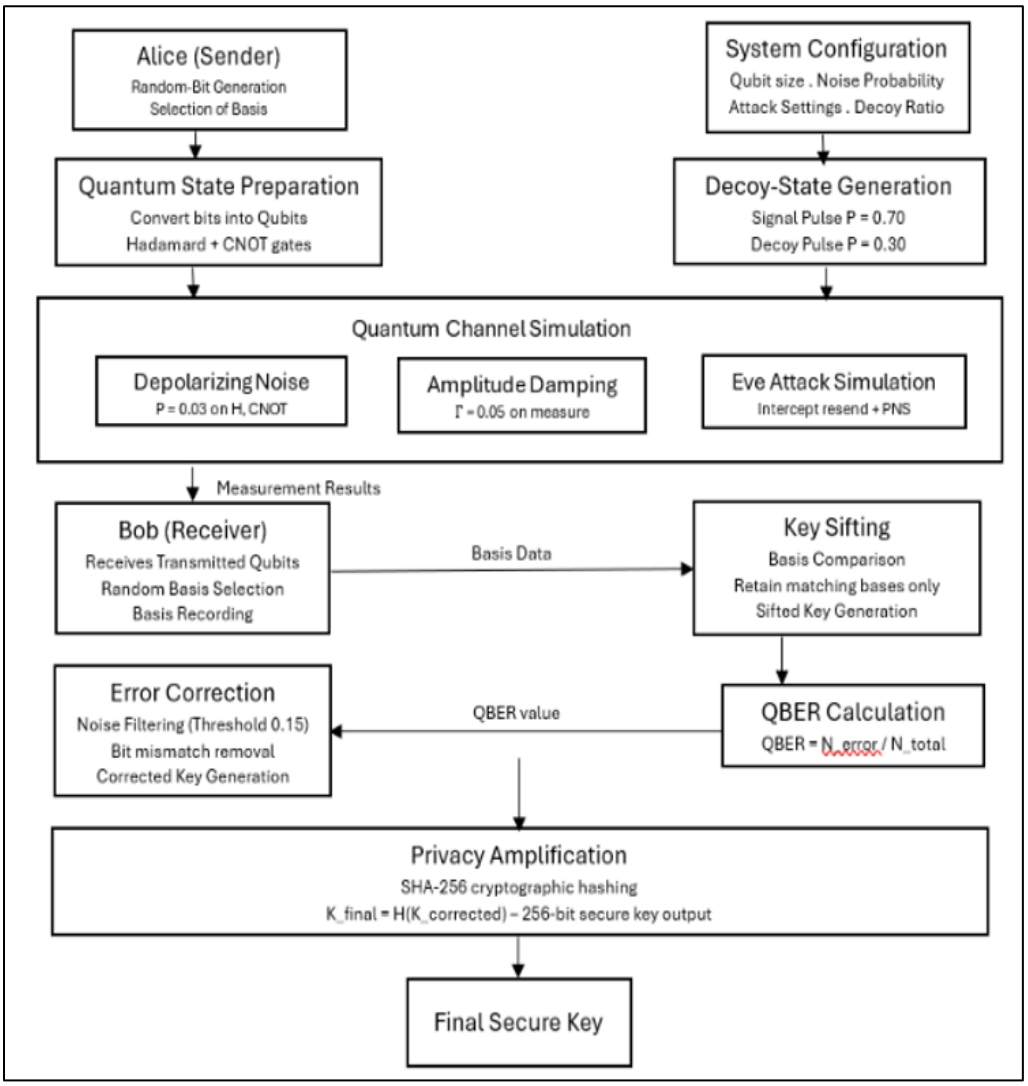

Fig 1 Workflow of QKD

➢ *Phase 2: Pulse Generation and Secure Transmission*

Decoy States are also used here to identify and mitigate PNS attacks while making the system secure in real-world conditions.[9] Every Pulse has a single photon, but some pulses do have Multiple Photons, which makes it interesting. For a single photon in a Pulse, when Eve (Attacker) tries to intercept it, she must measure it; then the state will get destroyed, and Eve gets caught. But in Multi-Photon Pulses, there will be two Photons – Photon A and Photon B (Both are identical to each other). When transmitting, Eve keeps Photon A, and Photon B will be sent to Bob(Receiver); thus, eavesdropping will be easier, and no one can detect. In this case, Eve tries to be smart and focuses only on Multi-Photon Pulses. To address this issue, decoy states have been introduced, which means instead of sending all pulses the same way, Alice randomly chooses between: Signal State – Normal Pulses used for Key generation and Decoy State – Weaker or sometimes vacuum pulses used only for testing.[14] For each Qubit, Alice randomly chooses, and she then converts a bit in the BB84 basis and transmits it over the Quantum channel. Bob does not know which one is signal or decoy. But then he measures all incoming photons and records detections and results. At this point, he does not separate signal or decoy yet. Later, Alice tells Bob over the classical channel which pulses were signal and which were decoy. This technique does not help for Eavesdropping. Meanwhile, Eve targets multi-photon pulses without knowing they may be Signal or Decoy Pulses since both look physically identical in form. So, the attack strategy that targets multi-photon pulses distorts the statistical correlations between Signal and Decoy states, revealing her presence.[1] These do not directly prevent eavesdropping; instead, they make eavesdropping detectable.

These generated pulses are forwarded via the quantum communication channel to the receiver. During transmission, practical communication channels may introduce disturbances and losses that affect the quantum states.[10] Real-world communication conditions have been simulated through noise models such as Depolarizing Noise and Amplitude Damping. The first noise model, Depolarizing Noise, randomly changes the state of transmitted Qubits, while Amplitude Damping signifies energy loss while transmitting.

To further evaluate the performance of the system, an eavesdropping attack simulation is introduced. Eve tries to measure and attempts to obtain information by intercepting

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

the exchanged quantum states during transmission.[3] The laws of Quantum physics state that such measurements modify the quantum states being transmitted, resulting in inconsistencies in the exchanged information.[11] Such disturbances can be identified during the Key generation and error estimation stages.

➢ *Phase 3: Measurement and Key Generation*

This Phase deals with receiving, measuring, and processing the transmitted information to generate the Key. The transmitted Quantum States are received by Bob. Since Bob doesn't know the basis selected by Alice during Quantum State Preparation, he randomly chooses either the rectilinear basis or the diagonal basis for every incoming qubit.[7] The Quantum mechanical properties imply that a Qubit measured using the correct basis yields the original encoded bit with high probability, whereas measurement in the incorrect basis produces a random outcome [11]. Once the measurement process is finished, both Sender and Receiver communicate via an authenticated classical channel to compare only the measurement bases selected for each transmitted qubit. The correct bit values should never be revealed during the exchange. Any qubits that correspond to the incorrect bases are removed, and those that are measured using matching bases should be kept. This process is called Key Sifting, generating the Sifted Key, which is the first shared key between the sender and the receiver.

The generated sifted key can still include errors arising from quantum channel noise, transmission impairments, or unauthorized interception.[4] Therefore, an Error Correction procedure is performed to correct the differences occurring between the sender's and receiver's sifted key sequences.[5] Following error correction, the QBER is calculated by evaluating the differences present in a sample of the error-corrected key bits.[1] This step makes sure that both sender and receiver possess identical copies of the shared key while preserving its confidentiality.

Once the keys have been successfully reconciled, [12] Privacy Amplification improves the confidentiality of the generated key by applying a key reduction process that limits the impact of any information leakage caused by possible interception. By applying Cryptographic Hash Functions, the final key is compressed into a shorter but highly secure one. SHA-256 has been used to generate a highly secure Key. SHA-256 relies on Five Fundamental Properties. These properties of SHA-256 ensure that the final Secure Key generated cannot be feasibly reversed or predicted, thereby strengthening the overall security, confidentiality, and integrity of the QKD process.

➢ *Phase 4: Security and Performance Evaluation*

Security evaluation of the proposed approach is performed by verifying the quality and protection level of the generated secret key after its propagation through the Quantum Channel. This assessment is conducted using key performance metrics such as QBER, KAR, and SKR. Collectively, these parameters assess both the security and efficiency of the proposed quantum communication framework.

The primary security metric which is used is QBER, which represents the fraction of Bit errors among all the compared key bits after Key Sifting and Error Correction.[3] A low QBER indicates that the transmitted Quantum States have experienced minimal disturbance, suggesting Secure Communication. Conversely, a rise in the QBER value indicates degradation in transmission quality and may also reveal the possibility of an intrusion attempt on the quantum communication channel.

- *Quantum Bit Error Rate (QBER) is Computed as:*

$$QBER = \frac{N\_error}{N\_total} \quad (1)$$

KAR indicates the proportion of usable keys successfully established during the quantum transmission process from the generated raw or sifted key material.[12] It estimates the capability of the Quantum channel to generate valid key material and is further refined through Error Correction and Privacy Amplification techniques.

- *Key Agreement Ratio (KAR) is Computed as:*

$$KAR = \frac{\sum(A_i = B_i)}{N} \quad (2)$$

SKR represents the final rate at which secure cryptographic keys are generated after all post-processing steps.[6] It indicates the actual usable secret key output of the system. A higher SKR implies an efficient and secure QKD system, while a reduction in SKR compared to KAR demonstrates the role of Error Correction and Privacy Amplification, performed during the post-processing stage, in ensuring a secure and consistent key exchange.

- *Secure Key Rate (SRK) is Computed as:*

$$SKR = Lsifted \cdot (1 - QBER) \quad (3)$$

Overall, the combined analysis of QBER, KAR, and SKR ensures that the system maintains both security against eavesdropping and efficiency in Key Generation. The final secure key is accepted only when QBER remains below the predefined threshold and a non-zero SKR is achieved.

IV. RESULTS AND ANALYSIS

The proposed decoy-state BB84 Quantum Key Distribution (QKD) framework was evaluated under different communication conditions, including ideal transmission, noisy quantum channels, eavesdropping attacks, and combined attack-noise environments. The system was implemented using Qiskit Aer Simulator with integrated depolarizing and amplitude damping noise models. Performance evaluation was carried out using metrics such as QBER, SKR, and KAR.

➢ *Performance Under Ideal Conditions :*

The performance of the proposed scheme was initially studied without noise and eavesdropping. Under the best communication conditions, the sifted keys generated by Alice

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

and Bob were highly correlated with low bit errors. The QBER values, which were measured to be low, indicate that the communication was secure. The keys that were transmitted were absolutely the same even after the reconciliation because that process eliminates the bits that are not matched by using Key sifting. Therefore, SKR was close to its optimal value while KAR was 1. Finally, this states that the proposed framework is working properly under ideal communication conditions.

➢ *Performance Under Quantum Noise :*

To simulate the Quantum Noise, models like depolarizing noise and amplitude damping were introduced to analyze the communication behavior, which will be introduced into the Quantum Channel. After observing the metrics, it is observed that Noise affected the qubit states during transmission and measurement. Since depolarizing noise is included in the framework, it has led to a lot of disturbances in the quantum states, whereas amplitude damping results in the photon's energy loss during their transmission. The following table shows various values under different qubit sizes.

Table 1 QBER, KAR and SKR Values Before (Under Noise Conditions)

Qubits	QBER before	KAR	SKR	QBER after
2	0.000	1.0000	1	0.00
4	0.500	0.5000	1	0.00
8	0.667	0.3333	1	0.00
16	0.222	0.8000	8	0.00
32	0.176	0.8235	14	0.00
64	0.162	0.8378	31	0.00
128	0.065	0.9355	58	0.00
256	0.090	0.9104	122	0.00

As the noise probability increases, QBER also increases because of the mismatched bits between the sender and the receiver. But the proposed noise filtering and error correction mechanisms reduced the ratio of the mismatched bits after the post-processing. This improves the efficiency and reliability of the keys generated and maintains metric values under moderate noise conditions.

The above results shown confirm that the proposed framework improves the QKD robustness in realistic communication environments.

➢ *Performance Under Eavesdropping Attacks :*

In this case, the framework was evaluated under eavesdropping conditions by introducing the attacker into the Quantum channel. Eve attempts to intercept the qubits and perform unauthorized measurements before the qubits have been forwarded to Bob. This attack simulation evaluated the effect of eavesdropping by allowing Eve to intercept the qubits and attempt to get the information from them, which enables the security of the Quantum communication system. The following are the values of the metrics under different qubit sizes.

Table 2 QBER, KAR and SKR Values Before (Under Eve Attacks)

Qubits	QBER before	KAR	SKR	QBER after
2	0.20	1.000	1.00	0.00
4	0.145	1.000	3.00	0.00
8	0.500	0.500	1.00	0.00
16	0.222	0.7778	7.00	0.00
32	0.118	0.8824	15.00	0.00
64	0.088	0.9118	31.00	0.00
128	0.077	0.9231	48.00	0.00
256	0.068	0.9316	109.00	0.00

As a result, the QBER increased significantly compared to the normal communication conditions. The increased QBER enabled successful identification of eavesdropping in that communication channel. The proposed mechanism improved further attack detection by analysing variations in photon pulses. Abnormal behaviour is observed during the transmission of the qubits, which indicates that there are attempts at photon extraction by the attacker.

The outcomes obtained here indicated that the approach successfully recognized the security threats by utilizing QBER variations and behavior.

➢ *Combined Noise and Attack Environment:*

The framework was also tested for its performance under the noise and eavesdropping conditions at the same time. Here, both channel disturbance and intentional interception were responsible for communication errors. The following table shows the metric's values under different qubit sizes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

Table 3 QBER, KAR and SKR Values Before (Under Both Noise and Eve Attacks)

Qubits	QBER before	KAR	SKR	QBER after
2	0.500	0.5000	1.00	0.00
4	0.000	1.0000	4.00	0.00
8	0.200	0.8000	4.00	0.00
16	0.364	0.6364	7.00	0.00
32	0.067	0.9333	14.00	0.00
64	0.129	0.8710	27.00	0.00
128	0.179	0..8209	55.00	0.00
256	0.163	0.8374	103.00	0.00

The observed QBER values were much higher compared to observed noise conditions and attack conditions separately. The system dynamically applied countermeasures to reduce the impact of disturbances.

Although SKR decreased significantly due to aggressive post-processing, the framework successfully generated secure keys that maintained optimal KAR values after correction. These results indicated that the framework remains functional and secure even under disturbed communication environments.

➢ *Scalability Analysis*

The proposed framework was tested under different qubit sizes. When more qubits are transmitted, the key length and SKR also increased.

But larger qubit transmissions introduced additional noise effects, which is slightly increased the QBER. Despite this, error correction and privacy amplification techniques maintained stable communication reliability.

The scalability study shows that the framework supports large-scale quantum communication with secure performance.

➢ *Comparative Analysis*

The proposed research provides several improvements compared to traditional ones, which include – More resilient towards PNS attacks, greater robustness under noisy channels, Noise-aware post-processing, reliable in key generation and better detection capability.

In comparison with conventional systems, the proposed protocol is more robust and offers practical security.

V. DISCUSSIONS

The experimental results show that by combining the decoy state with realistic noise modelling, the effectiveness of QKD systems can be enhanced. The proposed model was successful in detecting any attacks while ensuring that secure key generation is achieved under a noisy environment. Combining depolarizing noise, amplitude damping, error correction, and privacy amplification enables a more realistic evaluation of quantum communication systems than through the theoretical BB84 implementations.

Overall, the proposed system provides an effective and scalable approach for secure quantum key generation in real quantum communication networks.

VI. CONCLUSION

This paper presented an advanced decoy-state BB84 QKD framework with quantum noise and attack simulation integrated with decoy-state pulses, Quantum Noise and Eavesdropping attacks. The system was studied under noisy channels and different kinds of attacks, including intercept-resend and PNS attacks.

The results demonstrated that the decoy-state mechanism improved attack detection capability, while noise-aware modelling improved communication reliability under practical conditions. Performance analysis using QBER, SKR, and Kar showed that the framework maintained secure and stable key generation even under disturbed scenarios.

Thus, the introduced framework produced a practical and scalable way for improving the performance, security, and robustness of real-world quantum systems.

REFERENCES

[1]. C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in BB84 quantum key distribution protocols," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2689–2701, Sept. 2022.

[2]. Y. Begimbayeva and T. Zhaxalykov, "Research of quantum key distribution protocols: BB84, B92, E91," in *Proc. International Conference on Information and Communication Technologies*, 2022.

[3]. J. S. Nojun and D. S. Lauri, "Security analysis of BB84 QKD protocol under intercept-resend attack," *Journal of Quantum Communications*, vol. 5, no. 2, pp. 112–128, 2023.

[4]. H. J. Kim and S. M. Park, "Performance comparison of QKD protocols in fiber optic networks," *Quantum Network Review*, vol. 14, no. 1, pp. 45–59, 2021.

[5]. L. Chen and W. Wang, "Quantum cryptography: A review of eavesdropping detection methods," *Security and Communication Networks*, vol. 2024, p. e10245, 2024.

[6]. R. Gupta and A. Sharma, "Optimization of quantum resource consumption in QKD systems," *IEEE Communications Letters*, vol. 26, no. 8, pp. 1843–1847, 2022.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1740

[7]. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
[8]. D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.
[9]. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, 2005.
[10]. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, 2005.
[11]. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.
[12]. V. Scarani et al., "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, 2009.
[13]. M. Koashi, "Simple security proof of quantum key distribution based on complementarity," arXiv preprint, 2004.
[14]. H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states," *Quantum Information & Computation*, 2007.
[15]. M. Lucamarini et al., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, 2018.
[16]. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, 1992.