Mitigating Bucket Brigade Attacks in Quantum Networks Using Photon Polarization and Quantum Cloning Constraints

Ms.L. Thanga Palani[1] Dr.K. Bala[2]

1. Research Scholar, Department of Computer Science and Engineering, School of Computing, Bharath Institute of Higher Education and Research, Tamil Nadu, India

2. Professor, Department of Computer Science and Engineering, School of Computing, Bharath Institute of Higher Education and Research, Tamil Nadu, India.

Email : lthangamsaran@gmail.com

ABSTRACT Quantum communication systems, particularly those employing Quantum Key Distribution (QKD) protocols like BB84, are designed to leverage the principles of quantum mechanics to ensure secure information transfer. However, they remain susceptible to certain types of attacks, such as the **Bucket Brigade Attack (BBA)**, where an adversary intercepts and retransmits quantum signals to eavesdrop without detection. This abstract explores the potential of utilizing **quantum cloning** and **photon polarization techniques** to detect and mitigate such attacks. The no-cloning theorem in quantum mechanics prohibits the creation of perfect copies of unknown quantum states. Nonetheless, approximate quantum cloning machines (QCMs) can produce imperfect copies with a fidelity less than one. In the context of a BBA, an adversary might employ QCMs to intercept and clone quantum states, aiming to extract information without introducing detectable anomalies. By understanding the limitations of quantum cloning, legitimate parties can design systems that are sensitive to the disturbances introduced by such cloning attempts, thereby detecting potential eavesdropping. **Photon polarization** is a fundamental property utilized in encoding information within quantum communication protocols. Techniques that manipulate and measure the polarization states of photons are crucial for both transmitting information and detecting anomalies.

INDEX TERMS Quantum Symmetric Key Distribution (QSKD), Decoy State Protocols, Quantum Teleportation, Quantum Random Access Memory (qRAM), Heralded Noiseless Amplification

I. INTRODUCTION

Quantum communication, particularly through Quantum Key Distribution (QKD) protocols like BB84, offers unparalleled security by leveraging the principles of quantum mechanics. However, these systems are not immune to sophisticated threats such as the Bucket Brigade Attack (BBA), a variant of the man-in-the-middle attack. In a BBA, an adversary intercepts and retransmits quantum signals between communicating parties, potentially compromising the security of **the key exchange.** The inherent properties of quantum mechanics, notably the no-cloning theorem and the disturbance caused by measurement, provide natural defences against such attacks. The no-cloning theorem prohibits the creation of an exact copy of an arbitrary unknown quantum state, ensuring that any eavesdropping attempt introduces detectable anomalies. Furthermore, the use of photon polarization states to encode information means that any measurement by an eavesdropper alters these states, signalling a potential breach.

To enhance the resilience of quantum communication systems against BBAs, advanced techniques in **quantum cloning and photon polarization** are employed in QSKD of symmetric key. While perfect cloning is impossible, understanding the limitations of approximate quantum cloning machines (QCMs) allows for the development of protocols that can detect and mitigate cloning-based eavesdropping attempts. Additionally, precise control and monitoring of photon polarization states enable the detection of unauthorized interventions in the

communication channel reducing the risk of interception inherent in BBAs.

This paper explores the integration of quantum cloning and photon polarization techniques as a comprehensive strategy to detect and mitigate Bucket Brigade Attacks in quantum communication systems to safeguard QSKD. By analysing the vulnerabilities exploited in BBAs and the quantum mechanical principles that can counteract them, we aim to propose robust solutions to enhance the security of quantum key distribution protocols.

II. RELATED WORKS

Recent advancements in quantum communication have increasingly focused on the use of photons and atoms to transmit quantum information. This review begins by examining photonic and atomic protocols and concludes with their potential integration. QSKD has traditionally relied on well-characterized devices. However, device-independent. QSKD presents a promising avenue for security without this dependency, despite the implementation challenges, particularly in photonic systems. In [14], the authors verified device-independent QSKD using a photonic setup that enhanced loss tolerance. They developed a polarization-entangled photon source with a heralded detection efficiency of 87.5%, achieving a positive key rate over 220min the fiber. Additionally, the authors in [16] demonstrated a modified Ekert QSKD protocol using a coherently driven quantum dot over 250 m of single-mode fiber and free space, successfully connecting two buildings at Sapienza University in Rome. This study indicates that quantum dot-entangled photon sources are well suited for practical quantum communication applications. Despite significant advances in photonic systems, relying on well-characterized devices remains a challenge.

Although advances in device-independent QSKD are promising, more research is needed to enhance its practical implementation. Atomic protocols are particularly compelling because of their potential for high-fidelity entangled photon generation. A notable study on cavity-based quantum networks [10] emphasized the importance of efficient interfaces between stationary quantum nodes, such as single atoms, and flying carriers, such as optical photons. This research proposes various protocols for generating entangled photons and reversibly mapping quantum states between photons and atoms, underscoring their significance in scalable quantum networks. Another significant contribution involved the experimental realization of heralded atom‑photon quantum correlations. Research on **single- and entangled-photon pair generation** using atomic vapors [9] has demonstrated that atomic vapours can effectively generate both single-photon and entangled photon pairs, which is crucial for secure quantum communication. This study highlighted Symmetry 2025, 17, 458 5 of 20 the potential for enhanced photon production rates and improved entanglement fidelity, thereby strengthening quantum networks. Furthermore, the study in [17] introduced a new protocol for controlled secure direct quantum communication, which allows simultaneous authentication between Alice and Bob with the help of a **third party, Charlie,** through entanglement swapping. This protocol exhibited resilience against various attacks, including impersonation and intercept-and-resend attacks, and was favourable compared to existing protocols. The study in [18] showcased multiplexing-enhanced atom‑photon quantum correlations over a fiber length of 12 km, indicating that integrating atom‑photon systems could significantly improve the efficiency of the entanglement distribution over long distances, which is essential for large-scale quantum networks. Furthermore, [19] introduced dual field QSKD over optical fibers as a promising method for secure long-distance communication. By leveraging atomic clock technologies, including narrow-linewidth lasers and photon polarisation optical pulse distribution, this study details the integration of these technologies into a dual field QSKD setup on an extended metropolitan fiber network and reports the anticipated performance outcomes of the QSKD system.

These studies illustrate the complementary roles of photons and atoms in quantum channels, highlighting the potential of hybrid systems to leverage the strengths of both modalities. As research grows, integrating these approaches is expected to result in more robust and efficient quantum communication protocols. In this

context, a new hybrid technology is proposed that harnesses the unique advantages of both Photons and Cloning of atoms, enhances security while improving key distribution efficiency, and strengthens the QSKD against eavesdropping. This integration not only improves security through entanglement swapping but also increases the robustness of QSKD through error correction and privacy amplification of eavesdropping attempts by monitoring for disturbances in quantum states.

III PROPSED METHODOLGY

A sophisticated form of man-in-the-middle attack where an adversary intercepts and retransmits quantum signals between communicating parties, aiming to extract information without detection. Quantum mechanics prohibits the creation of an exact: Any attempt by an eavesdropper to clone quantum information introduces detectable anomalies, serving as a natural defence mechanism. While perfect cloning is impossible, adversaries might attempt approximate cloning, resulting in imperfect copies. In Fig(1) by analysing the fidelity of received quantum states, legitimate parties can identify discrepancies indicative of cloning attempts. Information is encoded in the polarization states of photons (e.g., horizontal, vertical, diagonal). Any unauthorized measurement or interception alters the polarization state, signalling a potential breach. An additional non-information-carrying photons (decoy states) alongside actual data-carrying photons which helps detect and prevent photon number splitting attacks, which are related to BBAs.

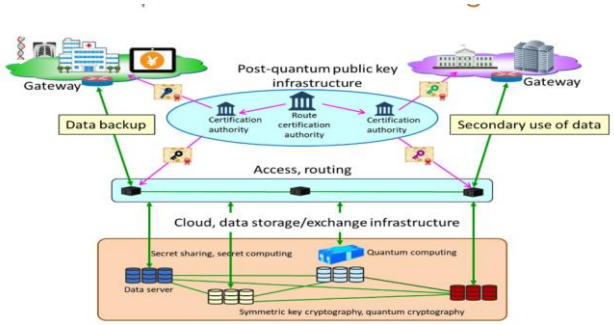

Fig-1- Architecture of safe quad QSKD in QN using Third Party constraint

A. PRELIMINARIES - Differently from classical information, quantum information (e.g., qubits) cannot be copied due to the no-cloning theorem. Hence, quantum networks rely on the quantum teleportation process as the unique feasible solution to transmit a qubit without the need of physically moving the physical particle storing such a qubit. The quantum teleportation of a single qubit between two different nodes requires: i) a classical communication channel capable of sending two classical bits, and ii) the generation of a pair of maximally entangled qubits, referred to as QSK (quantum Symmetric Key) pair, with each qubit stored at each remote node. In the following, the generation of an QSK pair at two different nodes is referred to as remote entanglement generation. In a nutshell, the process of teleporting an arbitrary qubit, say qubit j'i, from quantum node vi to quantum node vj can be summarized as follows:

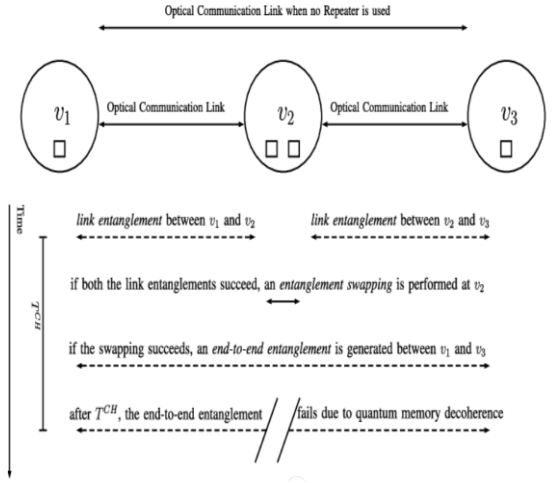

Fig-2- QSKD using Quantum Memories (Squares)

Nodes v_1 and v_3: These are the end-user nodes (e.g., Alice and Bob) aiming to establish entanglement for secure quantum communication. Quantum Repeater v_2 an intermediary node facilitating entanglement between v_1 and v_3 by performing entanglement swapping and purification processes. Using Quantum Memories (Squares) each node is equipped with quantum memory units, depicted as squares, which store quantum states (qubits) temporarily to manage synchronization and mitigate decoherence effects. T_{CH} **(Decoherence Time)** This denotes the characteristic time over which quantum information in the memory degrades due to interactions with the environment. Efficient entanglement distribution must occur within this timeframe to maintain fidelity. Time Proportions

of operations are not to scale in this schematic; they are adjusted for clarity and illustrative purposes.

B. QUANTUM SYMMETRIC KEY DISTRIBUTION (QSKD)

After analysing the current state-of-the-art in quantum network security, privacy, and trust, it is clear that QSKD is a promising cryptographic technique that allows for secure key generation over a quantum channel. However, several key challenges must be addressed to enable the realization of secure and trustworthy quantum networks:

Enabling Secure and Trustworthy Quantum Networks

1) Implementation complexity: The practical implementation of QSKD is complex and requires precise control of the quantum communication channels and equipment.

2) Channel loss and noise: QSKD is sensitive to channel loss and noise, which can cause errors and reduce the range of the communication.

3) Eavesdropping attacks: While QSKD is theoretically secure against eavesdropping attacks, practical implementations are vulnerable to attacks such as side channel attacks and Trojan horse attacks.

4) Limited range: QSKD is currently limited to relatively short distances due to the attenuation of the quantum signals over long distances.

5) Scalability: QSKD systems must be scalable to support large-scale quantum networks, which requires the development of new technologies and protocols.

6) Cost: The cost of QSKD systems is currently high compared to classical cryptographic systems, which may limit their adoption in some applications. Considering the current state-of-the-art and the identified key challenges for QSKD, the following potential solutions can be explored and implemented to address these challenges and enable the realization of secure and trustworthy quantum networks:

1) Improving QSKD protocols: One potential solution is to develop more efficient and robust QSKD protocols that can overcome the current limitations of channel loss, noise, and eavesdropping attacks. This can involve the use of novel techniques such as multi-photon sources, entangled photon pairs, and quantum memories to improve the rate and range of QSKD.

2) Developing practical QSKD systems: Another potential solution is to develop practical QSKD systems that can be easily integrated into existing communication infrastructures. The commercial availability of plug and- play protocols for QSKD has already made strides in this direction, simplifying integration and deployment. Looking ahead, there are also some promising avenues for further reducing costs and enhancing the practicality of QSKD systems such as utilizing **silicon photonics to integrate** QSKD components or researching quantum dot sources for reliable photon generation.

3) Hybrid QSKD solutions: A hybrid QSKD solution, combining the best of classical cryptography and quantum key distribution, can be considered to overcome the challenges in implementing QSKD at a large scale. Such hybrid solutions can use classical encryption techniques to ensure the security of the message, while using QSKD to distribute and refresh the keys.

4) QSKD network architectures: Another potential solution is to develop QSKD network architectures that can support long-distance QSKD over multiple hops. This can involve the use of quantum repeaters, which can amplify and regenerate quantum signals over long distances, or the use of satellite-based QSKD to enable global QSKD networks. In addition, the potential solutions identified above can help address the key challenges in implementing QSKD and enable the realization of secure and trustworthy quantum networks. However, further research is required to fully explore the feasibility and effectiveness of these solutions in practical quantum network deployments.

C. QUANTUM CLONING:

While perfect cloning is prohibited, approximate quantum cloning machines (QCMs) can produce imperfect copies of quantum states. Understanding the limitations and effects of such cloning is crucial for detecting and mitigating potential eavesdropping strategies. **Decoy State Protocols** - A technique in QSKD where additional non-information-carrying photons (decoy states) are sent alongside actual data-

carrying photons. This approach helps detect and prevent photon number splitting attacks, which are related to BBAs. **Entanglement Swapping** -A process where two particles that have never interacted become entangled through the entanglement of their partners. This technique is useful in extending the range of quantum communication and can aid in detecting and mitigating BBAs by ensuring the integrity of entangled states across the network

D. PHOTON POLARIZATION- A property of photons used to encode information in quantum communication. By manipulating the polarization states (e.g., horizontal, vertical, diagonal), information can be securely transmitted. Any unauthorized measurement or interception alters the polarization, signalling a potential breach.

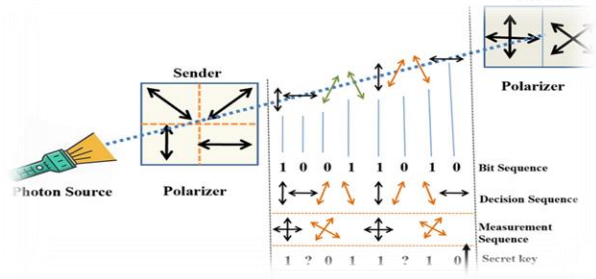

Fig (3)

Heralded Noiseless Amplification -A technique that amplifies quantum signals without introducing additional noise, preserving the integrity of quantum information. This method can be employed to strengthen weak signals and detect anomalies indicative of BBAs.

Quantum Error Correction- A set of methods used to protect quantum information against errors due to decoherence and other quantum noise. Implementing robust error correction protocols is vital in maintaining the security and reliability of quantum communication systems against BBAs.

E.QUANTUM-RESISTANT CRYPTOGRAPHY

Quantum-Resistant Cryptography faces significant challenges in the realization of secure and trustworthy quantum networks. Some of the key challenges for Quantum-Resistant Cryptography include:

1) *Lack of standardized algorithms*: Though the NIST has announced the first four algorithms for post-quantum cryptography, there is still no consensus on a standardized set of quantum-resistant cryptographic algorithms.

2) *Post-quantum security analysis*: Many proposed quantum-resistant cryptographic algorithms have not yet undergone sufficient analysis to confirm their security in a post-quantum computing environment.

3) *Interoperability with existing systems*: Quantum resistant cryptography must be compatible with existing systems and protocols, which may require significant modifications or updates.

4) *Performance overhead:* Many quantum-resistant cryptographic algorithms are computationally intensive and may require significant computational resources, which could affect the performance of systems and applications.

5) *Quantum computing progress*: The progress of quantum computing itself presents a challenge, as the development of more powerful quantum computers could eventually render current quantum-resistant cryptographic algorithms obsolete. To address these challenges and enable the realization of secure and trustworthy quantum networks, several potential solutions are being explored:

1) *Standardization of quantum resistant algorithms*: Efforts are underway, led by organizations like NIST, to identify and standardize the most promising quantum-resistant cryptographic algorithms.

2) *Post-quantum cryptography (PQC):* As a promising solution to address the limitations of QKD, PQC has garnered significant attention. PQC is designed to offer resilience against attacks from both classical and quantum computers, making it a compelling choice for securing modern communication networks.

Researchers are actively developing and refining quantum-resistant cryptographic schemes, including lattice-based cryptography, code-based cryptography, Enabling Secure and Trustworthy Quantum Networks and hash-based cryptography. These innovative cryptographic techniques are tailored to withstand the unique threats posed by quantum computers.

3) *Hardware-based Solutions*: Beyond software-based approaches, there is also research into hardware-based solutions for quantum-resistant cryptography. These solutions, such as hardware

security modules and quantum-resistant smart cards [46], aim to provide secure and efficient implementations of post-quantum cryptographic algorithms in practical settings. In addition, to enable the realization of secure and trustworthy quantum networks, it is crucial to continue research efforts in developing and standardizing post-quantum cryptographic algorithms, integrating them into existing network protocols and architectures, and exploring efficient hardware-based implementations.

IV RESULTS AND ANALYSIS:

A. Mathematical Validation -

The proposed method (polarisation & Cloning) integrates high-speed photonic transmission with resilient atomic-state encoding, facilitating effective error correction and robust eavesdropping detection. In addition, it incorporates mechanisms for authentication and privacy amplification, thereby reinforcing the overall security architecture. This section presents a formal mathematical justification of the protocol's enhanced security properties.

4.1. Security Advantages of Entanglement swapping in QSKD: Entanglement swapping offers superior security for QSKD protocols compared to traditional entanglement. In traditional entangled photon systems, Alice and Bob share an entangled state established using a Bell state, which is represented as

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|HH\rangle_{AB} + |VV\rangle_{AB}).$$

In quantum security, if an eavesdropper, often referred to as Eve, intercepts photon A and measures it, she alters the state of the entire system. Although photon A is collapsed by this measurement, photon B is not directly revealed to Eve. This causes uncertainty in the correlation between Alice and Bob, increasing the quantum bit error rate (QBER), which is defined as

$$QBER = \frac{E\prime}{N\prime\prime}$$

where E' accounts for the errors introduced by Eve, and N' is the total number of bits following Charlie's measurement. The enhanced sensitivity to eavesdropping in entanglement swapping QSKD leads to a more robust security framework. Any attempt by Eve to measure photons C or D will introduce detectable errors in the correlation between photons A and B. This illustrates that entanglement swapping provides superior security for QKD protocols compared to traditional entanglement, enabling the more effective detection of eavesdropping attempts

4.2. Authenticity and Integrity in Privacy Amplification: Here The privacy amplification process reduces any partial information that an eavesdropper may have about the key, ensuring that the final key is secure. Specifically, the use of a secret key K in conjunction with the BLAKE2 hash function to generate an integrity tag ensures that even if Eve has access to the cipher text, she cannot produce a valid tag without knowing K.

Statement 1 : The BLAKE2 hash function used in privacy amplification has several characteristics [27,28,30]:

- Pre-image resistance: Given a hash output h, it is computationally infeasible to find any input x such that BLAKE2(x) = h.
- Second pre-image resistance: Given an input x1, it is computationally infeasible to find a different input x2 such that BLAKE2(x1) = BLAKE2(x2).
- Collision resistance: It is computationally infeasible to find two distinct inputs x1 and x2 such that BLAKE2(x1) = BLAKE2(x2).

***Assumption** 1:* Assume Eve intercepts the Symmetric key C but does not know the secret key K. She has access to the cipher text and the corresponding integrity tag. Furthermore, assume Eve modifies the Symmetric key to C'. In this case, Eve attempts to generate a new tag, denoted as tag' such that $tag' = BLAKE2(K||C')$.

To produce a valid tag that matches the original tag, Eve must find K or create a collision

Proof. By the pre-image resistance property of BLAKE2, Eve cannot feasibly compute K from tag since

$tag \neq BLAKE2(K||C')$ for all $C' \neq C$

If Eve tries to find a K' such that

$BLAKE2(K||C) = BLAKE2(K'||C')$

then this is infeasible due to the second pre-image resistance property of BLAKE2. As Eve cannot generate a valid tag tag' for the modified

symmetric key C' without knowing K, it can be concluded that the integrity tag effectively amplifies privacy. Integrity tags guarantee that any modifications made to the cipher text can be identified, giving the recipient confidence in the authenticity of the message they have received. The use of BLAKE2 in conjunction with a secret key K in the integrity tag generation process guarantees that an eavesdropper, even with access to the cipher text, is prevented from forging a valid tag. This mechanism reinforces data integrity and enhances privacy through strong cryptographic principles.

Comparison of Generated Key Rates in Quantum Networks

Parameter	**Photonic QKD**	**Atomic QKD**	**Quantum Symmetric Key Distribution (QSKD)**
Key Generation Rate	High (GHz-scale in advanced setups)	Moderate to Low (kHz to MHz range)	Variable (depends on implementation)
Speed	Very fast; limited mainly by detector efficiency and channel loss	Slower due to complex atomic state manipulation	Moderate; depends on symmetric operations and trusted setups
Scalability	Good over short to medium distances; challenging over long distances without quantum repeaters	Limited scalability; best suited for short-range secure storage and memory	Potentially high with trusted nodes or pre-shared keys
Coherence Time	Low; photons decohere quickly (μs scale)	High; atoms can store quantum states longer (ms to seconds)	N/A (not based on entanglement lifetime)
Error Rates	Higher in long-distance or lossy links	Lower due to stable state encoding	Depends on noise models and protocol design
Implementation Complexity	Mature; easier to integrate with current optical infrastructure	Technically complex; requires precise trapping and cooling	Relatively simple if relying on classical infrastructure with quantum-enhanced techniques
Best Use Cases	Long-distance QSKD with optical fibers or satellites	Quantum memory, local QSKD, or trusted-node networks	Hybrid quantum-classical systems or pre-shared symmetric key schemes
Security Against Eavesdropping	High, but vulnerable to photon loss and intercept-resend attacks	Very high due to better eavesdropping detection	Depends on key management and trust assumptions

B. Analysis: In QSKD simulation, MATLAB R2024a (24.1) serves as the primary tool due to its robust capabilities and flexibility. It effectively models various QSKD protocols, including photonic, atomic, and hybrid systems, using advanced matrices and vectors to represent quantum states and operations. The photonic and atomic protocols are employed as benchmarks to evaluate the performance of the proposed hybrid protocol. Comprehensive simulate key generation processes, incorporating critical parameters such as successful key rate, QBER, loss rates, and error rates for a thorough analysis. In addition, MATLAB's intuitive visualization features facilitate comparisons and allow a clearer understanding of performance differences between QSKD protocols. In practice, hardware limitations can impact hybrid QSKD system

performance, including lower efficiency, higher error rates, and sensitivity to environmental factors. Increased demand for QSKD may necessitate additional resources, such as quantum repeaters and entangled photon sources, which may not be readily available or economically feasible. Real-world noise and interference can reduce the quality of quantum signals. The simulation may overestimate protocol robustness by not taking into account all relevant factors.

Figure 4 below illustrates the key rates generated by the three QSKD protocols, revealing notable performance differences. The QSKD protocol demonstrates the highest key rate, indicating that integrating both photonic and atomic states enhances the overall key generation efficiency. This hybrid approach effectively harnesses the advantages of both quantum systems by utilizing a photonic subsystem for rapid transmission and an atomic subsystem to improve security and robustness. Specifically, the hybrid protocol benefits from the transmission capabilities of photons and the robust security

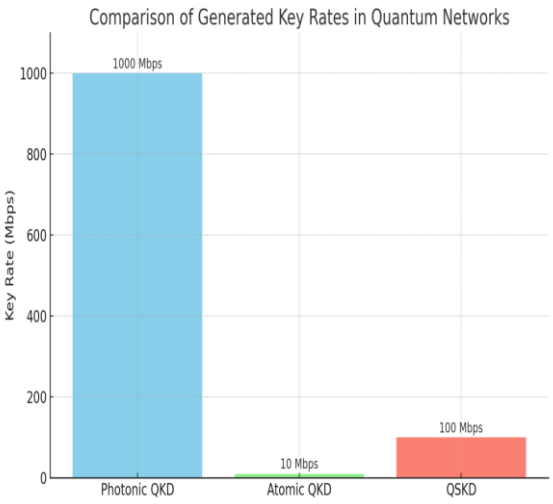

Fig 4- Comparison of generated key rates for photonic, atomic, and QSKD

features inherent in atomic states, supplemented by privacy amplification using BLAKE2, and error correction through LDPC codes. Privacy amplification with BLAKE2 transforms the raw key material generated during the QSKD process into a shorter secure key, thus reducing the likelihood of information leakage that could be exploited by potential eavesdroppers. LDPC codes further enhance the key rate by minimizing the overhead associated with error correction, thereby allowing a greater proportion of bits to contribute directly to the final key.

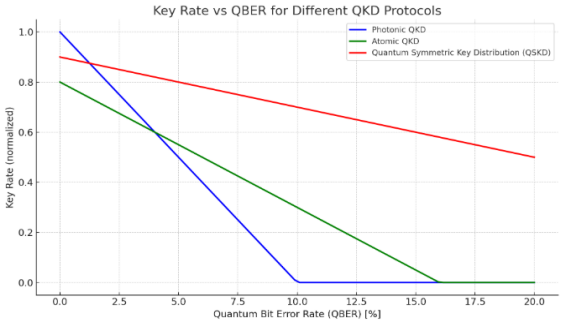

Fig-5 Comparison of the key rates in relation to QBER for photonic, atomic, and QSKD protocols.

Figure 5 shows the generated key rates versus QBER for the three QSKD protocols. All protocols exhibit a decrease in key generation rate as QBER increases, indicating that higher error rates negatively impact secure key generation. The hybrid protocol consistently achieves the highest key rate, suggesting greater resilience to errors and making it a strong candidate for practical quantum communication. In contrast, the atomic protocol, while showing a decrease in comparison to the hybrid, still it performs the photonic protocol at lower QBER levels. Although it performs reasonably well, it is less effective than the hybrid as error rates increase. The photonic protocol records the lowest key rate as QBER increases, highlighting its greater susceptibility to errors and reduced reliability under high noise or interference conditions

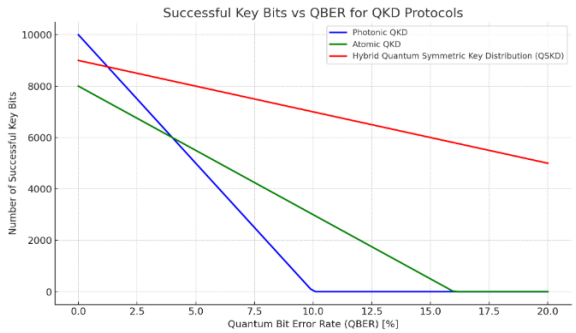

Fig-6 Comparison of successful key bits for photonic, atomic, and QSKD protocols

Figure 6 illustrates how the number of successful key bits (out of 10,000 transmitted bits) changes with increasing Quantum Bit Error Rate (QBER) for three types of quantum key distribution protocols:

- Photonic QKD: Suffers steep degradation in key generation as QBER increases.
- Atomic QKD: More resilient, maintaining higher key generation at moderate QBER.
- Hybrid QSKD: Combines advantages of both, providing the most consistent performance across varying QBER levels.

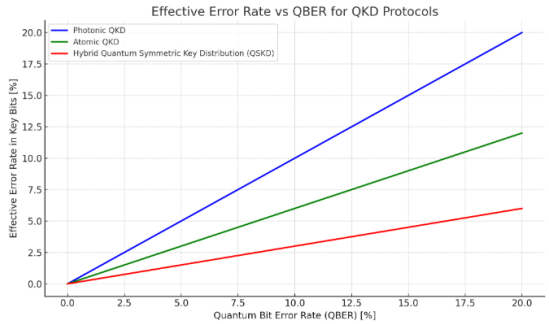

Fig 7 - Comparison of error rate for photonic, atomic, and QSKD protocol

Figures 7 show comparisons of error and loss rates for the three QSKD protocols based on distance. All three protocols exhibit negligible error and loss rates at short distances, thereby demonstrating their effectiveness for direct communication. However, as the distance increases, the photonic protocol shows the highest error and loss rates, indicating performance degradation. The atomic protocol outperforms the photonic protocol with increasing distance, demonstrating greater robustness against errors and losses. Meanwhile, the hybrid protocol consistently maintains the lowest error and loss rates at longer distances, underscoring its superior resilience in QSKD compared to the other two protocols. Additionally, there is a notable trade-off between the error and loss rates with distance in QSKD protocols, where longer distances generally lead to higher error and loss rates, impacting the overall key generation efficiency.

V CONCLUSIONS AND FUTURE ENHANCEMENT

This paper presents a novel hybrid quantum key distribution (QSKD) protocol that leverages both photonic and atomic systems to enhance security and reliability. The proposed architecture includes key stages such as encoding synchronization, state preparation, and secure message transmission, with an emphasis on robust eavesdropping detection and efficient error correction. Low-Density Parity-Check (LDPC) codes are employed to ensure high-performance error correction, maintaining the integrity of the transmitted key. By incorporating entanglement swapping and the BLAKE2 cryptographic hash function for privacy amplification, the protocol mitigates the risk of intercepted data being compromised, even in the presence of an adversary lacking the secret key. The synergy between photonic and atomic systems enables a balanced and resilient QSKD mechanism: photons offer rapid key generation with low decoherence, while atomic states provide long-term stability and improved error correction. This complementary interaction enhances the protocol's overall robustness.

Mathematical validation confirms the protocol's security guarantees, demonstrating the effectiveness of entanglement swapping and error correction in safeguarding communication channels. Comparative evaluations with existing QSKD schemes reveal that the hybrid model effectively combines the strengths of photonic speed and atomic stability, achieving secure key exchange with low error and loss rates over extended distances. While atomic QSKD is superior in detecting eavesdropping attempts, photonic QSKD, though simpler, is more susceptible to interception.

Looking ahead, future research should explore the scalability of hybrid QSKD systems across various operational environments and communication ranges. Additionally, Blockchain technology can be used to establish trust and security in quantum networks by creating a decentralized and tamper-proof ledger of network transactions. This can help to prevent malicious actors from compromising the network and ensure the integrity of the network's data. Overall, the above solutions can be used to address the key challenges of privacy-enhancing technologies in quantum networks and enable the realization of secure and trustworthy quantum networks.

Another key focus will be the development of trust models for the third-party node (Charlie), enabling flexible integration of partially trusted or untrusted intermediaries in the QSKD process, thus broadening the protocol's practical applicability in real-world network infrastructures

REFERENCES

[1] P. Arteaga-Díaz, D. Cano, andV. Fernandez, ‘‘Practical side-channel attack on free-space QKD systems with misaligned sources and countermeasures,’’ *IEEE Access*, vol. 10, pp. 82697–82705, 2022.

[2] A. Bach, ‘‘The concept of indistinguishable particles in classical and quantum physics,’’ *Found. Phys.*, vol. 18, no. 6, pp. 639–649, Jun. 1988.

[3] D. J. Bernstein, T. Lange, and C. Peters, ‘‘Attacking and defending the McEliece cryptosystem,’’ in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 5299, J. Buchmann and J. Ding, Eds. Cincinnati, OH, USA: Springer, Oct. 2008.

[4] C. H. Bennett and G. Brassard, ‘‘Quantum cryptography: Public key distribution and coin tossing,’’ in Proc. Int. Conf. Comput., Syst. Signal Process., 1984, pp. 175–179.

[5] V. Bhatia and K. R. Ramkumar, ‘‘An efficient quantum computing technique for cracking RSA using Shor’s algorithm,’’ in *Proc. IEEE 5th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Greater Noida, India, Oct. 2020, pp. 89–94.

[6] N. Bindel, U. Herath, M. McKague, and D. Stebila, ‘‘Transitioning to a quantum-resistant public key infrastructure,’’ in *Post-Quantum*

Cryptography (Lecture Notes in Computer Science), T. Lange and T. Takagi, Eds., vol. 10346. Utrecht, The Netherlands: Springer, Jun. 2017.

[7] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, ‘‘CRYSTALS–kyber: A CCA-secure module-lattice-based KEM,’’ in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2018, pp. 353–367.

[8] S. L. Braunstein and S. Pirandola, ‘‘Side-channel-free quantum key distribution,’’ *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130502.

[9] P. Busch, T. Heinonen, and P. Lahti, ‘‘Heisenberg’s uncertainty principle,’’ *Phys. Rep.*, vol. 452, no. 6, pp. 155–176, 2007.

[10] G. T. Byrd and Y. Ding, ‘‘Quantum computing: Progress and innovation,’’ *Computer*, vol. 56, no. 1, pp. 20–29, Jan. 2023.

[11] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, ‘‘The evolution of quantum key distribution networks: On the road to the qinternet,’’ *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.

[12] M. T. Dejpasand and M. S. Ghamsari, ‘‘Research trends in quantum computers by focusing on qubits as their building blocks,’’ *Quantum Rep.*, vol. 5, no. 3, pp. 597–608, Sep. 2023.

[13] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, ‘‘Practical challenges in quantum key distribution,’’ *npj Quantum Inf.*, vol. 2, no. 1, p. 16025, Nov. 2016.

[14] C. Ding, S.Wang,Y.Wang, Z.Wu, J. Sun, andY. Mao, ‘‘Machine-learning based detection for quantum hacking attacks on continuous-variable quantum-key-distribution systems,’’ *Phys. Rev. A, Gen. Phys.*, vol. 107, no. 6, Jun. 2023, Art. no. 062422.

[15] Y. Dulek, A. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, ‘‘Secure multiparty quantum computation with a dishonest majority,’’ in *Advances in Cryptology—EUROCRYPT 2020*. Zagreb, Croatia: Springer, May 2020, pp. 729–758.

[16] A. K. Ekert, ‘‘Quantum cryptography based on Bell’s theorem,’’ *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[17] D. Fischer, ‘‘Quantum diffie–hellman key exchange,’’ Cryptol. ePrint Arch., Paper 2021/1279, 2021.

[18] D. Harlow and P. Hayden, ‘‘Quantum computation vs. firewalls,’’ *J. High Energy Phys.*, vol. 2013, no. 6, Jun. 2013, Art. no. 85, doi:10.1007/JHEP06(2013)085.

[19] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, ‘‘Choosing parameters for NTRUEncrypt,’’ Cryptol. ePrint

Arch., Paper 2015/708, 2015.

[20] B. Huttner, R. Alléaume, E. Diamanti, F. Fröwis, P. Grangier, H. Hübel,V. Martin, A. Poppe, J. A. Slater, T. Spiller, W. Tittel, B. Tranier, A. Wonfor, and H. Zbinden, ‘‘Long-range QKD without trusted nodes is not possible with current technology,’’ *npj Quantum Inf.*, vol. 8, no. 1, Sep. 2022, Art. no. 108, doi: 10.1038/s41534-022-00613-4.

[21] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, ‘‘Risk analysis of trojan-horse attacks on practical quantum key distribution systems,’’ *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 168–177, May 2015.

[22] W.Kozlowski and S.Wehner, ‘‘Towards large-scale quantum networks,’’ in *Proc. 6th Annu. ACM Int. Conf. Nanosc. Comput. Commun. (NANOCOM)*, Dublin, Ireland, Sep. 2019, pp. 1–7.

[23] T. Li and Z.-Q. Yin, ‘‘Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator,’’ *Sci. Bull.*, vol. 61, no. 2, pp. 163–171, Jan. 2016.

[24] N. Lütkenhaus and M. Jahma, ‘‘Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack,’’ *New J. Phys.*, vol. 4, pp. 44.1–44.9, Jul. 2002.

[25] J. P. Mattsson, B. Smeets, and E. Thormarker, ‘‘Quantum-resistant cryptography,’’ 2021, *arXiv:2112.00399*.

[26] D. McMahon, ‘‘Quantum noise and error correction,’’ in *Quantum Computing Explained*. Wiley, 2008, pp. 251–278.

[27] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, ‘‘Implementation of quantum key distribution network simulation module in the network simulator NS-3,’’ *Quantum Inf. Process.*, vol. 16, no. 10, p. 253, Oct. 2017.

[28] H. A. Al-Mohammed, A. Al-Ali, E. Yaacoub, U. Qidwai, K. Abualsaud, S. Rzewuski, and A. Flizikowski, ‘‘Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios,’’ *IEEE Access*, vol. 9, pp. 136994–137004, 2021.

[29] M. A. Mukhtar, M. K. Bhatti, and G. Gogniat, ‘‘Architectures for security: A comparative analysis of hardware security features in Intel SGX and ARM TrustZone,’’ in *Proc. 2nd Int. Conf. Commun., Comput. Digit. Syst. (C-CODE)*, Mar. 2019, pp. 299–304.

[30] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ‘‘‘Plug and play’ systems for quantum cryptography,’’ *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, 1997.

[31] (Jul. 2022). *NIST Announces First Four Quantum- Resistant Cryptographic Algorithms*. [Online].Available:https://www.nist.gov/news-events/news/2022/07/nist-announces-firstfour-quantum-resistant-cryptographic-algorithms

[32] A. I. Nurhadi and N. R. Syambas, ‘‘Quantum key distribution (QKD) protocols: A survey,’’ in *Proc. 4th Int. Conf. Wireless Telematics (ICWT)*, Nusa Dua, Indonesia, Jul. 2018, pp. 1–5.

[33] Y. Pelet, I. V. Puthoor, N. Venkatachalam, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, Ž. Samec, M. Stipčević, R. Ursin, E. Andersson, J. G. Rarity, D. Aktas, and S. K. Joshi, ‘‘Unconditionally secure digital signatures implemented in an eight-user quantum network,’’ *New J. Phys.*, vol. 24, no. 9, Sep. 2022, Art. no. 093038.

[34] B. Qi, C.-H.-F. Fung, H.-K. Lo, and F.-X. Ma, ‘‘Time-shift attack in practical quantum cryptosystems,’’ *Quantum Inf. Comput.*, vol. 7, nos. 1–2, pp. 73–82, Jan. 2007.

[35] S. Ren, Y. Wang, and X. Su, ‘‘Hybrid quantum key distribution network,’’ *Sci. China Inf. Sci.*, vol. 65, no. 10, Oct. 2022, Art. no. 200502.

[36] J. Rabbie, K. Chakraborty, G. Avis, and S. Wehner, ‘‘Designing quantum networks using

preexisting infrastructure,'' *npj Quantum Inf.*, vol. 8, no. 1, p. 5, Jan. 2022.

[37] M. Roetteler, M. Naehrig, K. M. Svore and K. Lauter, ''Quantum resource estimates for computing elliptic curve discrete logarithms,'' in *Advances in Cryptology—ASIACRYPT 2017*. Hong Kong, China: Springer, Dec. 2017, pp. 241–270. 128808 VOLUME 11, 2023 S. Bajrić: Enabling Secure and Trustworthy Quantum Networks

[38] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. V. Meter, ''Attacking the quantum Internet,'' *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–17, 2021.

[39] V. Scarani and C. Kurtsiefer, ''The black paper of quantum cryptography: Real implementation problems,'' *Theor. Comput. Sci.*, vol. 560, no. 1, pp. 27–32, Dec. 2014.

[40] P. Sharma, K. Choi, O. Krejcar, P. Blazek, V. Bhatia, and S. Prakash, ''Securing optical networks using quantum-secured blockchain: An overview,'' *Sensors*, vol. 23, no. 3, p. 1228, Jan. 2023.

[41] V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee, ''A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols,'' *Quantum Inf. Process.*, vol. 15, no. 11, pp. 4681–4710, Nov. 2016.

[42] *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, Official Call for Proposals*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Dec. 2016. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantumcrypto/documents/call-for-proposals-final-dec-2016.pdf

[43] K. Sutradhar and H. Om, ''An efficient simulation for quantum secure multiparty computation,'' *Sci. Rep.*, vol. 11, no. 1, p. 2206, Jan. 2021.

[44] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, ''Resource-efficient verification of quantum computing using Serfling's bound,'' *npj Quantum Inf.*, vol. 5, no. 1, Apr. 2019, Art. no. 27.

[45] R. Trényi and M. Curty, ''Zero-error attack against coherent-one-way quantum key distribution,'' *New J. Phys.*, vol. 23, no. 9, Sep. 2021, Art. no. 093005.

[46] Q. Wang, D. Wang, C. Cheng, and D. He, ''Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices,'' *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 193–208, Jan. 2023.

[47] W. K. Wootters and W. H. Zurek, ''A single quantum cannot be cloned,'' *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[48] B. Yan et al., ''Factoring integers with sublinear resources on a superconducting quantum processor,'' 2022, *arXiv:2212.12372*.

[49] Y. Zhao, C.-H.-F. Fung, B. Qi, C. Chen, and H.-K. Lo, ''Quantum hacking:

Experimental demonstration of time-shift attack against practical quantumkey- distribution systems,'' *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042333.

[50] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng and J.-W. Pan, ''Large scale quantum key distribution: Challenges and solutions,'' *Opt. Exp.*, vol. 26, no. 18, pp. 242–260, 2018.