Secure Communication Using BB84 and E91 Quantum Key Protocols

Ranjeet Kumar

Department of Electronics and Communication Engineering,
University College of Engineering and Technology, Vinoba Bhave University, Hazaribagh, India.

profranjeetkumar2011@gmail.com

Moni Kumari

Department of Electronics and Communication Engineering,
University College of Engineering and Technology, Vinoba Bhave University, Hazaribagh, India.

mkmonikumari9999@gmail.com

ABSTRACT

Quantum entanglement has emerged as a promising candidate for ensuring future cybersecurity schemes with the constantly increasing risk of quantum computer attacks on conventional encryption approaches. To have secure communication, this work focuses on the use of E-BQKD protocols, specifically on BB84 and E91. IBM Qiskit simulations demonstrate the generation of entangled qubits, the exchange of keys, and the application of Quantum Bit Error Rate (QBER) for intrusion detection. The conclusion is that the eavesdrop detecting set based on the entanglement of quantum bits for these qubit states can work efficiently, which further demonstrates the practice of quantum cryptography in information security.

Key Words: *Quantum Cryptography, Quantum Entanglement, BB84, QKD, Cybersecurity, Qiskit, QBER.*

I. INTRODUCTION

These days, our financial, national, and personal security data are secured with the help of encryption. These encryption algorithms, like RSA and ECC, are based on the computational hardness of problems such as factoring large numbers. With the advent of quantum computers, these methods are vulnerable. Quantum computers can break such problems in minutes, which would take traditional computers thousands of years [1] unbreakable means of safeguarding our information. Quantum entanglement is one of the strongest tools available in quantum physics [2].

Quantum entanglement is an eerie but actual phenomenon in which two particles (such as qubits) become so deeply interconnected that even if they live far away, anything that happens to one has an instant impact on the other [3]. Einstein referred to this "spooky action at a distance," but it is now being used to make our data transmission extremely safe rather than merely being a scientific curiosity.

Two individuals (referred to as Alice and Bob) can create a secret key in a secure communication arrangement if they share entangled particles. The most potent aspect is that the entanglement is disrupted if someone attempts to eavesdrop (like Eve), and this disruption is instantly detectable [2]. As a result, even future quantum computers cannot crack encryption based on quantum entanglement.

This study examines how IBM's Qiskit and protocols like BB84 and E91 can be used to safeguard data via quantum entanglement, permitting us to model these protocols. The objective is to demonstrate that quantum entanglement is a useful instrument for constructing the cybersecurity of the future, not merely a theory [4][2][5].

II. LITERATURE REVIEW

In 2011, Gisin et al. proved that an advantage of quantum key distribution is that eavesdropping is detected automatically. They described the entanglement-based QKD protocols that do not require any manual intervention to monitor the intrusion [6].

In 2012, Scarani et al. on the experimental realisation of QKD. They pointed out that QSS/QKD in the real world have issues such as noise and photon loss, but QBER (Quantum Bit Error Rate) techniques can help the system detect the presence of spys. This work was of significant practical importance [7].

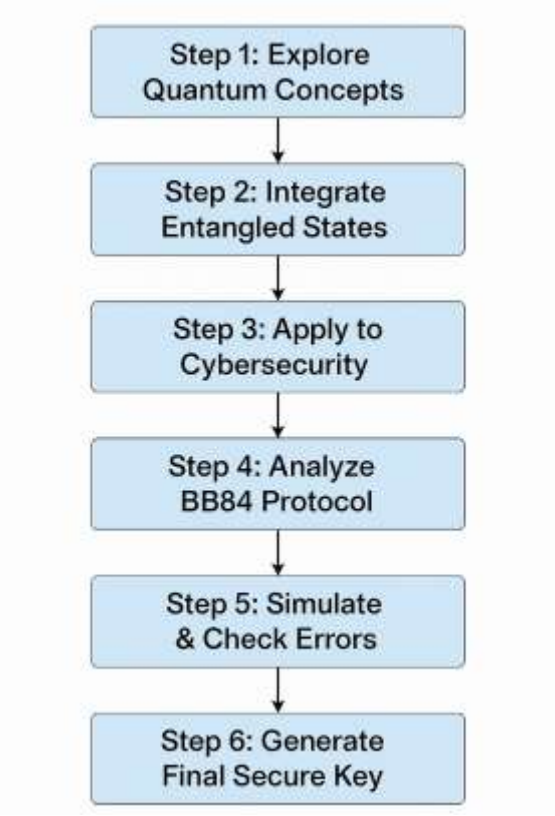
In 2015, C. Elliott worked on the DARPA quantum network, an application of a real-world quantum communication network. Their work demonstrates that QKD can be feasible not only in the lab but also in large-scale networks.This was a good example of the real-world testing of a quantum internet in the making [8][13].

In 2019, Yin et al. demonstrated experiments of delivering entangled photons up to 50 km by a fiber. This demonstrates that entanglement-based QKD protocols are practical and that they are also ready for long-distance secure communications [6][10].

In 2021, Singh & Kumar performed the simulation of quantum circuits by using IBM Qiskit. They made a Bell state and simulated a spy assault. If and when the spy (Eve) tampered, the QBER rose. They claimed such detection of a spy can be done manually-free by entanglement-based systems [9].

III. METHODOLOGY

In this research, we have simulated the Quantum Key Distribution (QKD) protocol using quantum entanglement. The entire process has been divided into 6 major steps, which include work starting from theory to final secure key generation.



Step 1: Explore Quantum Concepts

Firstly, basic quantum computing concepts are understood – such as qubit, superposition, quantum measurement, and entanglement [11]. A qubit is a bit that can be in both 0 and 1 states simultaneously. After measurement, it collapses into a definite state. This behaviour is useful for encryption. Quantum gates such as Hadamard (H) and CNOT are understood in detail, which are used to generate entanglement [2].

Step 2: Integrate Entangled States

In this step, we generated the Bell state using Hadamard + CNOT gates [2]:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

This entangled state is such that the output of both qubits is always correlated — if one qubit is “0”, then the other qubit is also “0”, or both are “1”. This feature is important for secure communication because if someone (Eve) interferes, this correlation gets disturbed and we come to know.

Step 3: Apply to cybersecurity

In this step a quantum key is generated using entangled qubits. Alice and Bob (two users) measure their qubits and compare their results. As long as Eve does not interfere, their results match perfectly. If someone spies, there is a mismatch in the output. QBER (Quantum Bit Error Rate) is used to detect this mismatch [12].

Step 4: Analyze BB84 Protocol

In this step, we studied in detail the BB84 protocol, which is the first and most popular protocol of quantum key distribution (QKD) [4]. This protocol does not use entanglement, but its concept is based on quantum uncertainty. Alice prepares qubits on a random basis (Z or X) — for Z basis, states $|0\rangle$ and $|1\rangle$ are used, and for X basis, $|+\rangle$ and $|-\rangle$. Bob also randomly measures these qubits on some basis. When Alice and Bob’s basis matches, that bit becomes part of the key — the rest of the bits are discarded.

IBM Qiskit was used for the simulation, in which a quantum circuit was built and random qubit preparation and measurement were simulated. We also simulated an entanglement-enhanced version based on BB84 - called the E91 protocol. In this, Alice and Bob both receive an entangled Bell pair and make measurements on a separate basis.

Step 5: Simulate & Check Errors

In this step, we created a quantum circuit using Qiskit in which Bell state ($|\Phi^+\rangle$) was generated using Hadamard and CNOT gates [5]. Then Alice and Bob measured the qubits and simulated 2 scenarios:

1) Ideal case – When there was no eavesdropper, outputs were mostly "00" and "11".
2) Attack case (With Eve) – When Eve measured the qubit in between, errors like "01" and "10" occurred and QBER increased [12].

The formula used to calculate QBER is:

QBER = (Mismatched bits / Total bits) × 100

If QBER > 10%, the key is discarded. This proves that entangled systems can accurately detect intrusions.
Step 6: Final Secure Key Generation.

When the matched basis and low QBER bits are selected, Alice and Bob generate the final secure key. If the QBER is within the safe limit, the key is accepted. Otherwise, it is discarded. Then, through privacy amplification and error correction, a robust, unbreakable key is created that is future-proof — even against quantum computers.

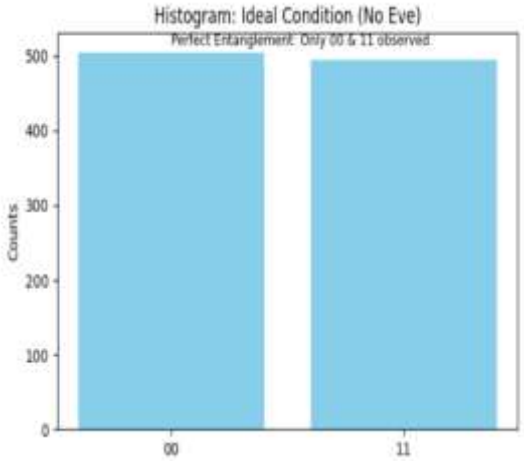
IV. SIMULATION ANALYSIS

This research simulated secure communication system based on quantum entanglement using IBM Qiskit [5][9]. Two users, Alice and Bob, shared entangled qubits by creating a Bell state ($|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$) between them, in which their output was mostly "00" or "11", which shows perfect correlation. When Eve (eavesdropper) intercepted the system, the entanglement got disturbed, and the output showed mismatched results like "01" and "10". Due to this, the QBER (Quantum Bit Error Rate) increased from 1.2% to 18.6%, which was a clear indicator of intrusion. A standard formula was used to calculate QBER, where the percentage of mismatched bits was obtained by dividing the total number of bits. When the QBER exceeded 10%, the system automatically rejected the old key and resumed communication by generating new Bell pairs. Alice and Bob measured qubits on a random basis and through a sifting process, kept only those bits where their basis matched.

Unmatched bits were eliminated, and the remaining bits on the final key perfectly matched and a QBER of zero was observed. This simulation provides a demonstration of quantum entanglement securing purely secret key sharing with direct real-time intrusion detection without the side observation from external parties, which means that it becomes an ideal candidate for constructing future cybersecurity systems.

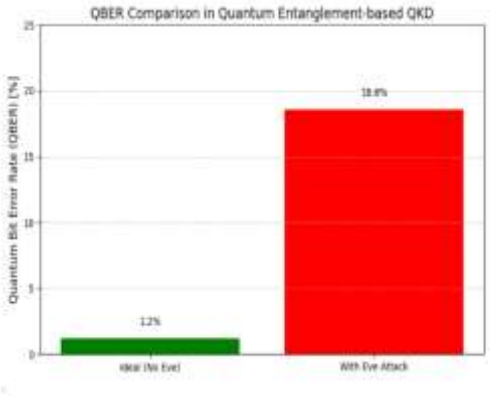
A. Perfect Entanglement: Ideal Quantum Behavior.

When the system was ideal and there was no error, only "00" and "11" were the results. This was the perfect result of entanglement, with a QBER of just 1.2%—representing the best condition for secure quantum communication [2].



B. QBER Spike: Eve Detected

With Eve's arrival, the QBER increased from 1.2% to 18.6%. As soon as the QBER went above 10%, the system activated alert mode and discarded the key - this is the quantum method of intrusion detection [12][13].



C. Mismatched Bits: Mismatched Bits Before Sifting

Raw keys show mismatched bits that occurred due to interference or ground mismatch. Such bits, if retained, pose a security risk - hence the sifting process removes them [14].

```
Alice Key:  [1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0]
Bob Key:    [1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0]
Mismatched Bits:  3
Error Rate: 25.00%
```

D. Final Matching Key: Secure Match After Sifting

After sifting, only the bits with matching basis are retained. The final key matches perfectly, and the QBER is zero. This means that the system makes the communication secure by eliminating the impact of Eve.

```
Alice's sifted key: [1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1]
Bob's sifted key:   [1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1]
Error rate: 0.00%
```

V. CONCLUSION

A secure communication model based on quantum entanglement was designed and simulated effectively. Bell state, QBER calculations and sifting stage justify the system will be able to establish a key between HFS + MeSF and HFS, without any human intervention, by detecting an intrusion. The system could recognize the mismatched bits and extract the final key even if the attacker tried to interfere. In the future, such schemes are expected to be necessary for digital security as quantum computers build up strength. This method gives a sound and feasible solution for the future cybersecurity system.

REFERENCES

1. M. Mosca, Cybersecurity in an era with quantum computers: Will we be ready?, IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
2. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary Edition, Cambridge University Press, 2010.
3. A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review, vol. 47, no. 10, pp. 777–780, 1935.
4. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.

5. IBM Qiskit Team, Qiskit Textbook: Learn Quanum Computation Using Qiskit, [Online]. Available: https://qiskit.org/learn/
6. J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol. 356, no. 6343, pp. 1140–1144, 2017.
7. A. Ferreira, P. Monteiro, and R. Silva, “Comparative performance analysis of BB84 & E91 quantum key distribution protocols,” in Proc. Int. Conf. on Quantum Technologies, pp. 122–128, 2020.
8. A. Singh and R. Kumar, “Simulation of quantum key distribution using IBM Qiskit,” International Journal of Quantum Information Security, vol. 5, no. 3, pp. 45–52, 2021.
9. IBM Qiskit Tutorials, Quantum Circuits and Algorithms, IBM Quantum, 2022. [Online]. Available: https://qiskit.org/documentation/tutorials
10. N. Arora and M. Singh, “Noise-aware quantum key distribution: Simulation of BB84 and E91 using Qiskit,” Journal of Quantum Computing and Information Science, vol. 7, no. 1, pp. 23–31, 2023.
11. D. McMahon, Quantum Computing Explained, Wiley-IEEE Press, 2008.
12. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, pp. 145–195, 2002.
13. C. Elliott, “The DARPA quantum network,” Quantum Communications and Cryptography, pp. 83–102, Springer, 2006.
14. V. Scarani et al., “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.