

A Comparison of Quantum Cryptography Protocols for Securing Internet of Things Devices

Karlo N. Rendic

Mamaroneck High School, 1000 Boston Post Road, Mamaroneck, NY, 10543, USA; knrendic@gmail.com

Mentor: Eric Sakk

ABSTRACT: Internet of Things devices have become a staple of our society, whether that be possessions that you have in your household, such as NEST Smart Thermostats, or industrial and military products that are more widely applicable. Regardless of the context, these items must be secured promptly, given the ever-evolving field of quantum computing. Current cryptographic methods in IoTs rely on fundamental cryptographic principles, adopting an algorithmic approach to implement key distribution between an IoT device and a trusted medium. Research has suggested a new approach to ensure the confidentiality, integrity, and availability (CIA Triad) of data transmitted between devices: Quantum Key Distribution (QKD). Such protocols include Bennett and Brassard 84 (BB84) and Ekert 91 (E91), both of which use quantum principles to secure the key being transmitted. These two protocols can help secure IoTs. This paper analyzed both fundamental Quantum Protocols and examined their implementation in a realistic Implantable Medical Device (IMD) setting. It is found that, although both protocols have advantages, BB84 is the more optimal protocol due to a lower Quantum Bit Error Rate (QBER) over distances of 10 meters than E91, although E91 has a higher detection rate of eavesdroppers.

KEYWORDS: IoT, Quantum Cryptography, BB84, E91.

■ Introduction

IoT devices transmit highly sensitive data daily and are implemented throughout our lives; however, existing security methods may become insufficient over the next 5-10 years as quantum computing advances. Many IoT security protocols rely on classical cryptographic techniques, such as RSA and elliptic curve cryptography, being more algorithm-based. Quantum computing, however, is specifically designed to solve hard problems such as these efficiently, posing a threat to this widely utilized system.^{3,7} However, due to their overall limited power and constraints regarding usable circuitry, the optimization of implementing QKDs is limited. The reason that quantum techniques have been proposed as a solution for key distribution is that anyone eavesdropping on a communication channel will affect the photon distribution or photon status. This is due to the Heisenberg uncertainty principle, where a measurement cannot be made without noticeably affecting the system. Researchers have found methods of applying quantum cryptography, where they present a security blockchain intrusion detection system (IDS) for industrial IoT networks, demonstrating how this can be optimized into industrial environments.^{2,4} The issue with this, however, is that industrial IoTs have significantly fewer constraints regarding a multitude of sources compared to IMDs; this thereby limits the applicability of implementation into practical usages.

The main identified issues regarding the feasibility of these implementations have been broad, including items such as data leakage and other attacks that are often overlooked.³ To defend against attacks such as these, as aforementioned, implementing QKDs has been considered. Some attacks, however, such as long-term device non-updating, cannot be avoided; on the

other hand, eavesdropping can be prevented.³ Eavesdropping, in particular, is a key aspect of the protection that protocols BB84 and E91 protect against—E91 through photon entanglement and BB84 through photon polarization.³ This paper will directly look at the feasibility, along with the practicality of implementing the two aforementioned methods in IMD, such as Pacemakers and Injectable Insulin pumps; IoTs that need the utmost security. These two protocols have been selected due to their foundational applications into other QKDs, with BB84 being simpler, easier to accomplish, and E91 being more complex, safer, but more energy-constrained. BB84 relies on the transmission of quantum bits (qubits) encoded into different polarization bases, where, when intercepted allow the detection of eavesdropping by enabling the sender to detect it by using measurement properties of the quantum states of the qubits.³ E91 utilizes quantum entanglement and Bell Inequality violations, where, when intercepted, the sender can utilize Bell's inequality to see if there is a violation; meaning no interception due to quantum properties, while when there is no violation, it means there are no quantum properties—meaning interception.³

■ Methods

Programming tools:

To implement this simulation, we used a Python-based model that leveraged the Matplotlib and NumPy APIs for mathematical calculations and plotting, respectively. This enables us to determine the total amount required for the 1000-bit transmission while also providing an estimate of the demands on the IMDS when implementing these two protocols under varying atmospheric conditions.

Cryptographic Protocols Tested:

Two distinct cryptographic protocols were used to perform the tests: E91 and BB84. BB84 is a quantum cryptographic protocol that uses quantum mechanics to establish a shared key between a sender and a receiver, while ensuring that an eavesdropper is detected. Information is encoded in two distinct bases, as seen in Figure 1, rectilinear (Z) or diagonal (X). This property allows a sender to detect when a photon's base is measured, as it measures the photons; it creates a discrepancy, allowing any eavesdropper to be detected, creating a quantum bit error (QBE).³ A large number of these errors then lead to an increased QBER, demonstrating eavesdropping.

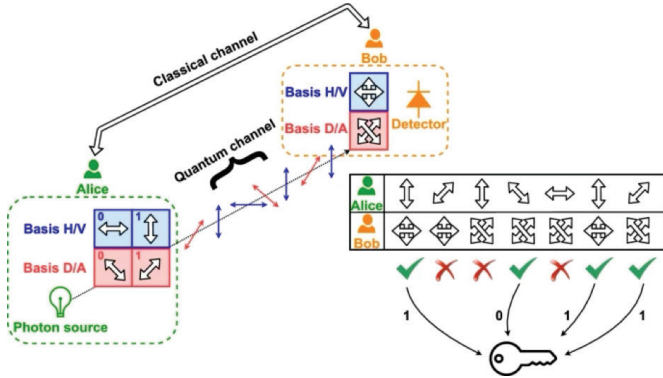


Figure 1: Working Diagram for BB84 Protocol, used along with text for interpretation.⁸

E91, although based on the fundamentals of quantum mechanics, is similar to that of BB8, but it does work using different protocols. As seen in Figure 2, E91 uses Bell's inequality: by sending entangled photons, it can detect eavesdropping. When an entangled photon is looked at, you can utilize Bell's Inequality Theorem to see if it violates the principles of it, then if it does that means that the Entangled Photon still has quantum properties meaning it is not looked at; however, in the opposite case where it doesn't violate it, eaves dropping is present, leading to a more accurate reading than that of BB84.³ (See Figure 2)

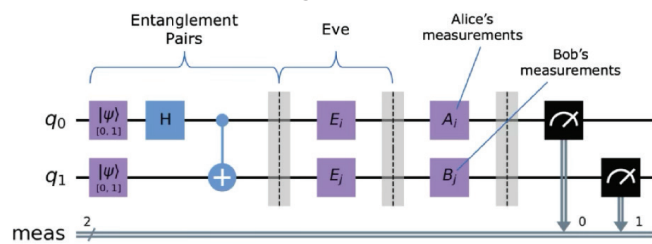


Figure 2: Working Diagram for E91 Protocol, used along with text for interpretation.⁹

Device Models:

The devices that were modeled in this study include IMDs, which include IoTs such as pacemakers and injectable insulin pumps, both extremely resource-constrained. These models utilize realistic constraints to closely copy the conditions under which real IMDs operate. Atmospheric impedance was also utilized in the model, as it affects the energy required to transmit the keys over a distance of 10 meters. We used the wavelength of infrared photons (1550 nm) as a baseline for both of the models—BB84 and E91—which therefore accounts

for a more realistic approach to the sending of photons, as most already applicable IoTs, such as Televisions (TVs), utilize this in the communication between remotes and themselves. In this simulation, only a fraction of the original qubits truly reach the receiver, as most are lost, requiring a larger amount of energy utilized to send the same number of qubits, which is our goal of 1000 qubits to create a sufficiently complex key.

Model for Atmospheric Attenuation: Probability of a photon being lost over a distance. α = atmospheric attenuation coefficient and d = transmission distance. Used in BB84 and E91. However, in E91, both pairs need to survive, so that is accounted for by

$$p(\text{survive}) = (1 - p_{\text{atm}})^2.$$

$$p_{\text{atm}} = 1 - e^{-\alpha d}$$

Required Amount of Photons Sent by Sender: To make sure that the receiver receives a target number of usable photons. Used in BB84.

$$N_0 = \frac{N_{\text{target}}}{(1 - p_{\text{atm}})(1 - p_{\text{Eve}})}$$

Calculation For Total Energy Used:

Planck's Relation: used to model infrared photons, where h = Planck constant, c = speed of light, λ = wavelength, in which case wavelength is 1550 nm to simulate infrared photons. Used in both simulations. Used in both to calculate the amount of energy required. (Doubled due to pairs of photons in E91).

$$E_{\text{total}} = N_0 E_0$$

Matching Basis for BB84 + E91: Only retains the matching basis to form the key.

$$K = \{i \mid B_A^{(i)} = B_B^{(i)}\}$$

QBER Threshold: Used in both simulations to test QBER and to check if it passes a threshold.

Experimental Procedure:

Using a Python program with the application programming interface of numpy, matplotlib, and seaborn, we ran two versions of the simulation, both sending a 1000-qubit-long key. In both, these photons are sent to a receiver, with increasing rates of atmospheric attenuation, along with eavesdropper strength. In the BB84 simulation, the sender encodes a random sequence of bits into photon polarization states according to randomly selected bases; the receiver measures each photon and keeps the corresponding bases. Eavesdropping is then introduced through "eavesdropper strength," which then allows an adversary to intercept and measure the photons being sent, which causes QBE, therefore increasing QBER. Then, using the raw key and the received true key, QBER is calculated; if it exceeds the designated threshold of 11%, the key is subsequently discarded.

The E91 protocol builds on the same framework; however, it utilizes entangled photon pairs. Then the sender and receiver measure their entangled photons with the randomly chosen bases, and only keep those that still contain quantum mechanics. Just as in BB84, the QBER is then calculated regarding the original sent key to the key that is truly used, where the

threshold for discarding a key is the same as in BB84 – 11 %. Just as BB84, this program also accounts for fluctuation values of atmospheric attenuation, looking at different atmospheric conditions, calculated using an atmospheric attenuation coefficient (α), ranging from clean air, 0.1, to contaminated air, 0.30.

■ Results

BB84:

The results of the BB84 simulation demonstrate the capabilities of BB84 regarding atmospheric conditions; they do not include eavesdropping conditions. In Figure 3, for the case of an adversary, the QBER of BB84 is zero when the adversary is absent (assuming no atmospheric attenuation). This then alters to a QBER of 0.26% when an adversary is introduced, due to the hypothesized disturbance of the quantum states when an adversary tries to read the qubits. Figure 4 reinforces this, as it demonstrates a direct relationship between the adversary's interception strength and QBER: increasing the strength subsequently also increases the QBER, with a max QBER of 0.25 when at full strength, just as the previous bar graph. Figure 5 demonstrates a final quantitative idea: as the attenuation coefficient increases, the number of photons that the sender must send to deliver one thousand photons starts to grow exponentially. This occurs because the higher atmospheric loss causes more photons to be lost, or their path is altered due to other particles in the air. The maximum value of photons required is twenty-five thousand to send one thousand qubits at an atmospheric attenuation coefficient of 0.3.

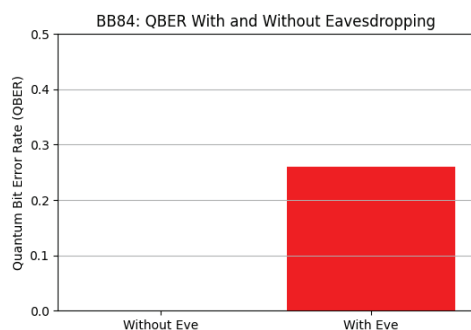


Figure 3: Simulated comparison of Quantum Bit Error Rate with and without adversary (Eve) (1.0 Strength) when using the BB84 cryptographic protocol.

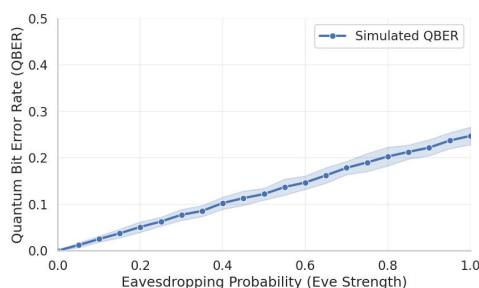


Figure 4: Simulated Comparison of the Eavesdropper Interception Probability v.s. QBER in BB84.

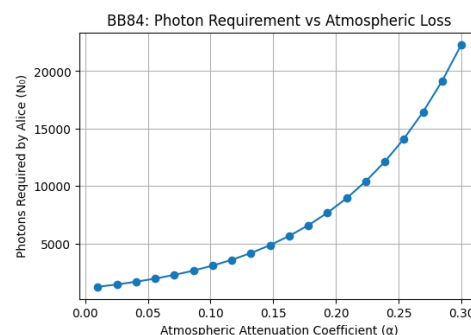


Figure 5: Atmospheric Attenuation Coefficient (α) v.s. Photons Required to Send One Thousand to the Receiver in BB84.

E91:

The results of the E91 simulation, although demonstrating similar patterns to those of the BB84 protocol, show different quantitative values, those of a large caliber. Similar to BB84, when there is no adversary present, the QBER is zero. When this changes to a full-strength adversary, the QBER jumps to 0.5, double that of BB84. In Figure 6, this jump is also seen, where the values of QBER are significantly higher than those of BB84, although both do have a direct relationship between Eavesdropper Strength and QBER, as seen in Figure 7. Another significant change is the difference in photon pairs required to send one thousand over the atmosphere compared to that of BB84, seen in Figure 8. These values are doubled due to the reason that both photons are required to survive the transaction, and if one doesn't, that qubit must be discarded, and that would be registered as a QBE, further increasing the QBER. Otherwise, the graph also increases exponentially as the Atmospheric Attenuation Coefficient increases, just as in BB84.

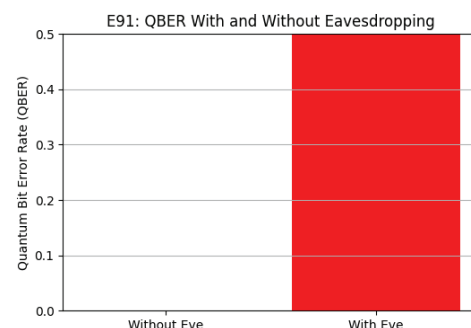


Figure 6: Simulated comparison of Quantum Bit Error Rate with and without adversary (Eve) (1.0 Strength) when using the E91 cryptographic protocol.

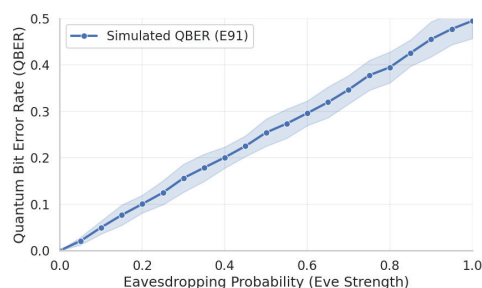


Figure 7: Simulated Comparison of the Eavesdropper Interception Probability v.s. QBER in BB84.

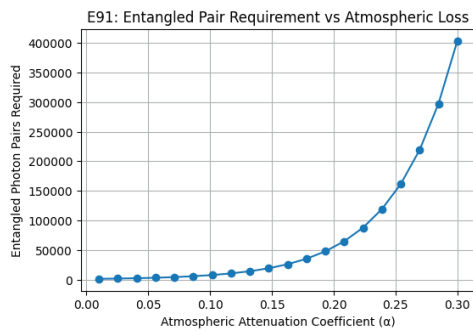


Figure 8: Atmospheric Attenuation Coefficient (α) v.s. Photons Required to Send One Thousand to the Receiver in E91.

■ Discussion

From our study, it is concluded that although our hypothesis was partially correct, as BB84 is feasible for implementations over IoT networks and E91 is not, it is true that these QKDs could have been more optimized for specific needs, for IMDs. Considering the alignment that is required with these protocols, and with many other technologies that tend to send photons, such as these, which require direct alignment, this is not applicable within certain IoT frameworks. These protocols, specifically that of BB84 due to its smaller photon loss rate, would be more practical in Industrial IoTs and stand-alone IoTs that don't require movement, such as Pacemakers and Injectable Insulin Pumps.⁵ Although both protocols are sufficient for detecting eavesdropping regarding the sharing of encryption keys, this is not pertinent due to the required alignment. It is helpful to understand that these protocols are applicable in the frameworks, just not in widely regarded frameworks, such as those mentioned and per se "Smart Home" appliances.

■ Conclusion

In this paper, we have examined two distinct QKD protocols, BB84 and E91, and, based on our resource-constrained models, concluded that the more stable protocol for IoT applications to be implemented in the near future would be BB84. This is the case because it loses less energy when transmitted through the atmosphere due to atmospheric attenuation, while still maintaining a stable detection rate of eavesdroppers, with a QBER greater than 0.25. This value has been chosen because it is easy to discern whether there has been an eavesdropper, and it is not so low as to be negligible. To reach this conclusion, we have used a Python simulation to ensure that both protocols work as expected and are feasible to implement in a world dominated by IoT devices.

Future Work:

Many items are missing from today's implementations of BB84 and E91. One might look to improve both BB84 and E91 by testing these protocols with other security methods, such as AES, to help create a compromise and get the best of both protocols. This can be further improved by developing a method to send photons in a wider beam, helping extend the range while also increasing the angle of alignment

that is required for these protocols, and implementing other post-quantum cryptography methods.^{6,7} Other protocols, more complex ones, could also be tested to see their applicability in IoT frameworks as well. Finally, as long as improved engineering comes along in the next 5 - 10 years, using these procedures may become a very real solution to address post-quantum security issues associated with classical key distribution.

■ Acknowledgments

I would like to express sincere gratitude toward my mentor, Dr.Sakk, and all the time he put in to help me with my research paper. This paper would not have been possible without him.

■ References

1. Dhar, S.; Khare, A.; Dwivedi, A. D.; Singh, R. Securing IoT Devices: A Novel Approach Using Blockchain and Quantum Cryptography. *Internet Things* **2024**, *25*, 101019. <https://doi.org/10.1016/j.iot.2023.101019>.
2. Chawla, D.; Kumari, S.; Rathore, R. S.; Mehra, P. S.; Das, A. K.; Kumar, N. Quantum Blockchain for Internet of Things: A Systematic Review, Proposed Solutions, and Challenges. *Comput. Electr. Eng.* **2025**, *126*, 110524. <https://doi.org/10.1016/j.compeleceng.2025.110524>.
3. Yang, Y.; Lin, Y.; Xiao, J.; *et al.* Feasibility Discussion of Quantum Cryptography for Internet of Things Security: A Literature Review. *Opt. Quantum Electron.* **2025**, *57*, 264. <https://doi.org/10.1007/s11082-025-08168-2>.
4. Hussain, N.; Li, S.; Hussain, A.; *et al.* Quantum-Aware Secure Blockchain Intrusion Detection System for Industrial IoT Networks. *Sci. Rep.* **2025**. <https://doi.org/10.1038/s41598-025-31985-0>.
5. Liu, A.; Zhang, Q.; Xu, S.; Feng, H.; Chen, X.-B.; Liu, W. QBIoT: A Quantum Blockchain Framework for IoT with an Improved Proof-of-Authority Consensus Algorithm and a Public-Key Quantum Signature. *Comput. Mater. Contin.* **2024**, *80*, 1727–1751. <https://doi.org/10.32604/cmc.2024.051233>.
6. Khan, A. A. Securing IoT Communication with the Integration of Quantum Cryptography and Machine Learning. *Int. J. Intell. Syst. Appl. Eng.* **2024**, *12* (3), 4435–4445.
7. Balogh, S.; Gallo, O.; Ploszek, R.; Špaček, P.; Zajac, P. IoT Security Challenges: Cloud and Blockchain, Post-Quantum Cryptography, and Evolutionary Techniques. *Electronics* **2021**, *10* (21), 2647. <https://doi.org/10.3390/electronics10212647>.
8. Caputo, C.; Simoni, M.; Cirillo, G. A.; *et al.* A Simulator of Optical Coherent-State Evolution in Quantum Key Distribution Systems. *Opt. Quantum Electron.* **2022**, *54*, 689. <https://doi.org/10.1007/s11082-022-04041-8>.
9. Pedone, I.; Atzeni, A.; Canavese, D.; Liroy, A. Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment. *IEEE Access* **2021**, *9*, 115270–115291. <https://doi.org/10.1109/ACCESS.2021.3102313>.
10. Pedone, I., Atzeni, A., Canavese, D., & Liroy, A. (2021). Toward a complete software stack to integrate quantum key distribution in a cloud environment. *IEEE Access*, *9*, 115270–115291. <https://doi.org/10.1109/ACCESS.2021.3102313>

■ Author

Karlo Rendic is an 11th-grade student with a strong interest in problem-solving and analytical thinking. He spends much of his time coding, solving math problems, or working on his next big project.