ISSN 2278-3091

Volume 13, No.4, July - August 2024

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse021342024.pdf

https://doi.org/10.30534/ijatcse/2024/021342024

Security Analysis of the BB84 Protocol in IoT Networks

Zied Guitouni[1], Sirine Maize[2], Mounir Zrigui[2], Mohsen Machhout[1]

[1] Electronics and Microelectronics Laboratory, Faculty of Sciences Monastir (FSM), Tunisia

[2] Research Laboratory in Algebra, Numbers theory and Intelligent Systems, FSM, Tunisia

guitouniziedyahoo.fr

Received Date : June 5, 2024 Accepted Date: July 14, 2024 Published Date: August 06, 2024

ABSTRACT

The Internet of Things (IoT) has experienced rapid growth, resulting in a proliferation of interconnected devices in domains such as smart homes, cities, and healthcare applications. Ensuring secure communication within IoT networks is crucial for protecting privacy and data. The BB84 protocol, a quantum key distribution (QKD) protocol, shows promise in enhancing IoT communication security. This paper presents a comprehensive security analysis of the BB84 protocol in IoT networks, examining key aspects including entropy, execution time, quantum bit error rate (QBER), and cryptographic key generation efficiency. The analysis aims to evaluate the protocol's resilience against potential attacks and its suitability for securing IoT communications. We delve into the evaluation of entropy levels in the key generation process to ensure strong cryptographic properties. We also examine the correlation between execution time and QBER to determine the protocol's efficiency and ability to counter timing-based attacks. Additionally, we analyze the efficiency of the keys generated by the BB84 protocol, taking into consideration factors such as key size, generation rate, and computational overhead. These evaluations allow us to assess the protocol's suitability for resource-constrained IoT devices.

Key words: Internet of Things, Quantum Key Distribution, BB84 Protocol, Security Analysis, Cryptographic Key Generation

1. INTRODUCTION

The explosive growth of the Internet of Things (IoT) has paved the way for a multitude of interconnected devices spanning diverse domains [1]. including smart homes, cities, industrial automation, and healthcare applications. These IoT networks facilitate the collection, processing, and exchange of vast amounts of data, often containing sensitive or critical information. Consequently, ensuring the security and privacy of communication within IoT networks has become of paramount importance.

One promising approach to achieve secure IoT communications is through the utilization of quantum key distribution (QKD) protocols, such as the renowned BB84 protocol. Developed by Charles H. Bennett and Gilles Brassard in 1984 [2], the BB84 protocol leverages the principles of quantum mechanics to establish secure cryptographic keys between two parties, even in the presence of an eavesdropper. The BB84 protocol possesses inherent security properties, including the detection of any attempts at eavesdropping, making it an attractive option for safeguarding IoT networks against various security threats.

However, the successful deployment of the BB84 protocol in IoT environments poses unique challenges. These challenges arise from the resource-constrained nature of IoT devices, the large scale and heterogeneity of IoT networks, and the specific attack vectors prevalent in these environments. Therefore, a comprehensive security analysis of the BB84 protocol in the context of IoT networks is necessary to understand its strengths, vulnerabilities, and potential optimizations.

This paper aims to provide a thorough security analysis of the BB84 protocol in IoT networks, focusing on key aspects including entropy, correlation execution time, Quantum Bit Error Rate (QBER), and the efficiency of the keys generated. By examining these factors, we can assess the protocol's robustness against potential attacks and evaluate its suitability for securing IoT communications. Additionally, the analysis will consider the impact of resource limitations and scalability issues on the protocol's implementation in IoT environments.

The paper will delve into the evaluation of entropy levels in the key generation process, ensuring that a sufficient amount of randomness is achieved to maintain strong cryptographic properties. Furthermore, the correlation execution time between the sender and receiver will be examined to determine the protocol's efficiency and resilience against timing-based attacks.

Another crucial element of the security analysis will be the assessment of the QBER, which measures the error rate in the transmission of quantum bits. By quantifying the QBER, we can evaluate the vulnerability of the BB84 protocol to eavesdropping attempts and assess its effectiveness in maintaining secure communication channels within IoT networks.

Moreover, the efficiency of the keys generated by the BB84 protocol will be analyzed, considering factors such as the key size, generation rate, and computational overhead. This evaluation will help determine the protocol's suitability for resource-constrained IoT devices, ensuring that it can be effectively implemented in practical IoT network scenarios.

This paper aims to provide valuable insights into the security characteristics of the BB84 protocol in IoT networks. By identifying the strengths and weaknesses of the protocol, we can propose potential optimizations and enhancements to enhance its performance and adaptability to the unique requirements of IoT environments.

The rest of this paper is structured as follows: Section 2 provides an overview of the related work regarding the integration of QKD protocols with IoT systems. In Section 3, a detailed explanation of the BB84 protocol is presented, delving into its key generation and distribution process. Additionally, the challenges associated with implementing QKD in IoT networks are discussed. In Section 4, a comprehensive security analysis of the BB84 protocol in the context of IoT networks is conducted. Finally, in Section 5, the paper concludes, summarizing the key findings and implications derived from the analysis.

2. RELATED WORKS

Several studies have explored the integration of QKD with IoT systems to strengthen their security measures. Anilkumar et al. [3] demonstrated the feasibility of implementing the BB84 protocol, a QKD method, in IoT applications. The authors emphasized the potential of the BB84 protocol in providing robust security for IoT devices and communication. Abdulkader [4] proposed an integrated approach that combines quantum cryptography with block ciphers to secure IoT systems, offering a comprehensive solution for safeguarding IoT devices and their communication. Devi and Kalaivani [5] developed an enhanced version of the BB84 protocol tailored for secure communication in wireless body sensor networks used in medical IoT applications. Their work focused on adapting the BB84 protocol to meet the specific requirements of the medical IoT domain, enhancing its resilience and suitability for transmitting sensitive healthcare data. Srikrishnan et al. [6] investigated the practical implementation aspects of a QKD algorithm for securing communication in IoT networks. They evaluated the performance of QKD-based security solutions and explored their feasibility in real-world IoT scenarios. Edwards et al. [7] assessed the potential benefits and challenges of incorporating QKD in secure satellite-integrated IoT networks, considering the distributed nature of such architectures. Neeraj and Singhrova [8] conducted a comprehensive review of various QKD-based techniques and their applicability in IoT security. They highlighted the advantages and limitations of different approaches, providing insights into the diverse range of strategies available. Adu-Kyere et al. [9] developed a Python-based modeling and simulation tool for the BB84 protocol in QKD for IoT, enabling researchers to evaluate the performance and behavior of QKD systems in simulated IoT environments. Krithika and Kesavmurthy [10] explored the integration of QKD with existing IoT protocols and architectures, focusing on securing IoT networks. Dhar et al. [11] proposed a novel approach that combines blockchain and quantum cryptography to enhance IoT device security, leveraging the strengths of both technologies.

Additionally, Su [12] conducted a simple analysis of the security properties of the widely-used BB84 protocol, offering insights into its theoretical security aspects. Rao and Sreeja [13] emphasized the importance of quantum cryptography in addressing the security challenges faced by IoT networks, highlighting the need to explore QKD as a means of enhancing IoT security.

These studies collectively demonstrate the growing interest in and exploration of QKD as a viable solution for securing communication in IoT systems. However, further research is required to address practical challenges, such as resource constraints, scalability, and interoperability, to seamlessly integrate QKD with IoT architectures.

In this paper, we present a comprehensive security analysis of the BB84 protocol in IoT networks. We evaluate key factors such as entropy, correlation execution time, quantum bit error rate (QBER), and the efficiency of the generated cryptographic keys. Through extensive experiments and evaluations, our research aims to assess the protocol's robustness and suitability for securing communication in IoT environments.

3. BAKGROUND

In this section, we provide an overview of the BB84 QKD protocol and discuss the challenges involved in implementing QKD in IoT networks.

3.1 Overview of the BB84 Protocol

The BB84 protocol, developed by Charles H. Bennett and Gilles Brassard in 1984, is a seminal quantum key distribution (QKD) protocol. QKD protocols leverage the principles of quantum mechanics to enable two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages [2].

The key generation and distribution process in the BB84 protocol involves the encoding of random bits of information onto the polarization states of single photons, which are then sent from the sender (Alice) to the receiver (Bob). Bob randomly chooses one of two possible measurement bases to measure the received photons, and then Alice and Bob publicly discuss the measurement bases used, without revealing the actual bit values. They then discard the bits where they used different measurement bases, leaving them with a shared sequence of bits, known as the raw key. Alice and Bob then estimate the error rate in the raw key and use classical error correction techniques to remove any errors, resulting in a corrected key. Finally, they apply privacy amplification techniques to remove any information that may have been obtained by an eavesdropper, resulting in the final shared secret key.

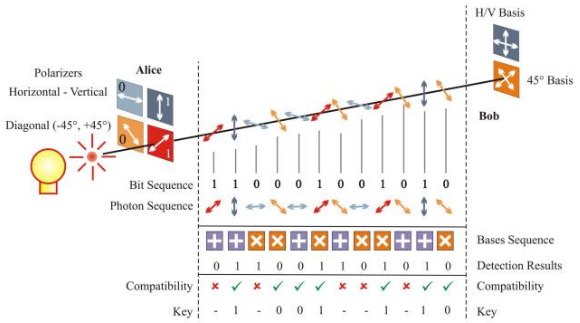

Figure 1: Key exchange process in the BB84 protocol

Figure 1 illustrates the key exchange process in the implementation of the BB84 protocol using photon polarization. This diagram provides a visual representation of the steps involved in establishing a secure key between the sender and receiver in the protocol [14]. This Figure depicts the sender generating random qubits encoded with different polarization states, such as horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A). These qubits are then transmitted to the receiver through a quantum channel.

The security of the BB84 protocol relies on the principles of quantum mechanics, specifically the no-cloning theorem and the uncertainty principle. Any attempt by an eavesdropper (Eve) to intercept and measure the transmitted photons will inevitably disturb the quantum state, which can be detected by Alice and Bob, allowing them to abort the key exchange and prevent the eavesdropper from obtaining the secret key.

3.2 Challenges of BB84 Implementation in IoT Networks

Implementing the BB84 protocol in IoT networks presents several challenges that must be overcome to ensure successful deployment and enhance security.

One significant challenge is the resource limitations of IoT devices. These devices often have limited computational power, memory, and energy capacity. To tackle this issue, it is crucial to find efficient algorithms and protocols that optimize resource usage. By doing so, we can ensure the feasibility of key generation and distribution processes on resource-constrained IoT devices.

Scalability is another critical aspect to consider. IoT networks can encompass a vast number of devices, ranging from simple sensors to powerful gateways. Securing such large-scale and heterogeneous networks requires scalable solutions. The BB84 protocol needs to effectively handle the challenges associated with large-scale deployments, including efficient key distribution and management across numerous devices.

Device heterogeneity adds another layer of complexity. IoT networks consist of devices with different capabilities, communication protocols, and security requirements. It is essential for the BB84 protocol to be adaptable enough to accommodate the diverse range of devices in an IoT network. This includes addressing interoperability issues and ensuring that the protocol can be implemented on various types of devices.

Wireless communication is a common method for IoT devices to transmit data, utilizing technologies like Wi-Fi, Bluetooth, or Zigbee. However, this introduces additional security vulnerabilities, such as eavesdropping and unauthorized access. To maintain the confidentiality and integrity of the transmitted quantum bits, the BB84 protocol should incorporate robust encryption and authentication mechanisms.

Security threats pose a significant risk to IoT networks. Eavesdropping, man-in-the-middle attacks, and denial-of-service attacks are among the various threats that can compromise the BB84 protocol's security and the confidentiality of the shared secret key. Mitigating these threats requires implementing countermeasures such as advanced authentication schemes and intrusion detection systems.

Efficient key management is crucial in IoT networks. Key generation, storage, distribution, and revocation must be carefully designed to ensure the security and integrity of the keys. The BB84 protocol should seamlessly integrate with existing key management systems or provide robust key management mechanisms tailored to IoT environments.

By addressing these challenges, we can pave the way for the successful implementation of the BB84 protocol in IoT networks. This will enhance the security of these networks by ensuring the confidentiality of communication and protecting against potential threats.

4. SECURITY ANALYSIS OF BB84 IN IoT NETWORKS

In this section, we will discuss the threats and attack vectors in IoT networks, as well as evaluate the security of the BB84 protocol in IoT

4.1 *Threats and Attack Vectors in IoT Networks*

IoT networks face various security threats that can compromise the effectiveness of the BB84 protocol. These threats include:

- *Eavesdropping*: The distributed and wireless nature of IoT networks makes them vulnerable to eavesdropping attacks, where adversaries intercept the communication between IoT devices to gain unauthorized access to sensitive information [15]. This poses a significant concern for the BB84 protocol as eavesdroppers may attempt to measure the transmitted photons, disrupting the quantum state and potentially obtaining information about the secret key.
- *Man-in-the-Middle Attacks*: In a man-in-the-middle attack, adversaries intercept the communication between two IoT devices and impersonate both parties, enabling them to monitor and manipulate the data exchange. Such attacks can compromise the key distribution process of the BB84 protocol, as adversaries may inject their own photons or manipulate the basis reconciliation and sifting steps [16].
- *Denial-of-Service Attacks*: IoT networks are susceptible to denial-of-service (DoS) attacks, where adversaries attempt to disrupt or disable the normal operation of IoT devices or the entire network. In the context of the BB84 protocol, a DoS attack could target the resources required for key generation and distribution, such as computational power, memory, or communication channels, rendering the protocol inoperable [17].

4.1 Evaluation of BB84 Security in IoT Networks

- *Correlation Variation*: The security of the BB84 protocol can be affected by the correlation between transmitted photons or generated secret key bits. In an IoT environment, factors such as device heterogeneity, environmental conditions, and resource constraints may introduce variations in this correlation. Analyzing correlation variation is essential to ensure the overall security of the protocol [18].

Figure 2 depicts the variation of correlation between adjacent pixels in the 1000 keys generated by the BB84 protocol for IoT networks.

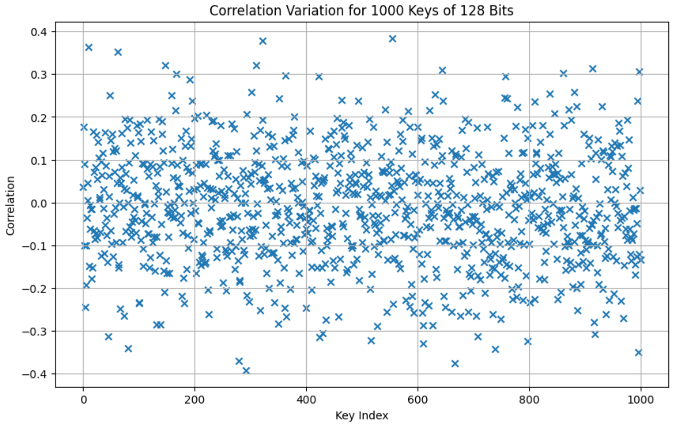

Figure 2: Correlation Variation in the BB84 protocol

According to Figure 2, the correlation values range from a minimum of -0.39 to a maximum of 0.38, indicating both positive and negative correlations.

Positive correlations suggest a higher similarity between adjacent pixels, implying consistent patterns among neighboring pixels within the keys. This similarity enhances the reliability and integrity of data transmission in IoT networks. Conversely, negative correlations signify a higher dissimilarity between adjacent pixels, potentially introducing vulnerabilities. Addressing these dissimilarities is crucial to ensure the robustness and security of the generated keys.

The average correlation equal -0.01 indicates a relatively weak overall correlation between adjacent pixels. This suggests that, on average, there is little similarity or dissimilarity between neighboring pixels in the generated keys.

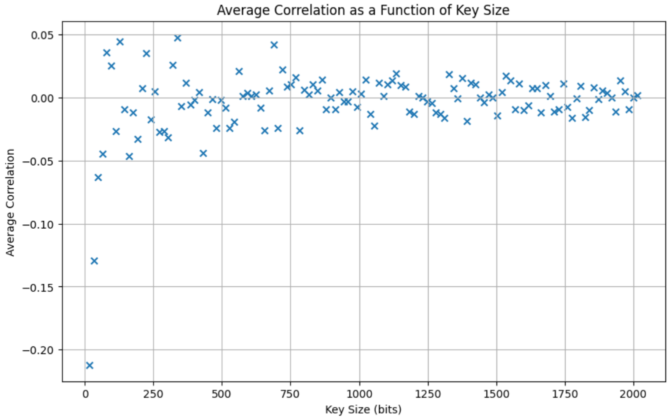

Figure 3: Average Correlation Variation For Various key Sizes

Figure 3 presents the average correlation variation for various key sizes ranging from 16 to 2024. The results show that the minimum average correlation is -0.21, indicating a relatively low similarity between adjacent pixels in the smallest key size. The maximum average correlation is 0.05, suggesting a slightly higher similarity in the largest key size. Overall, the average correlation across all key sizes is close to zero at -0.00, indicating little to no similarity or dissimilarity between adjacent pixels in the generated keys. These findings highlight the protocol's ability to produce keys with low average correlations, regardless of the key size. This contributes to the security and reliability of key generation in IoT networks, ensuring the confidentiality and integrity of data transmission.

- *Entropy Variation*: One crucial aspect in the security analysis of the BB84 protocol in IoT networks is the potential variation in entropy. Entropy measures the randomness and unpredictability of the generated secret key. IoT devices often have limited sources of true random number generation, which can reduce the entropy in the secret key and make it more vulnerable to attacks. The quality of random number generation directly impacts the security of the BB84 protocol and needs careful evaluation, especially in resource-constrained IoT devices [19].

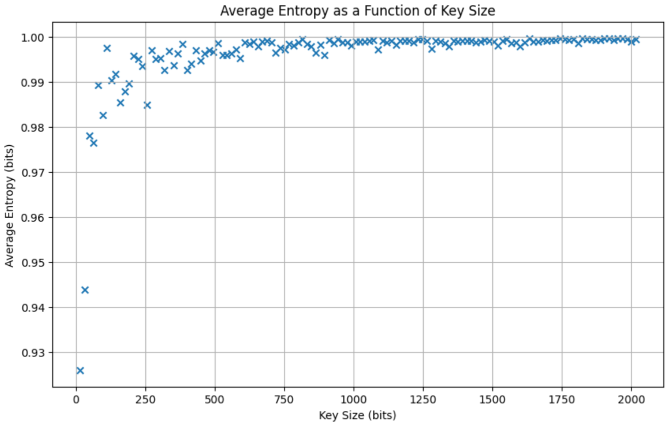

Figure 4: Average Entropy Variation For Various key Sizes

Figure 4 depicts the average entropy variation of 1000 keys generated by the BB84 protocol for different key sizes.

The minimum average entropy of 0.93 bits in the smallest key size suggests a relatively lower level of randomness. This could pose security concerns for IoT networks, as lower entropy keys are more vulnerable to attacks.

On the other hand, the maximum average entropy of 1.00 bits in the largest key size indicates a higher level of randomness. Keys with higher entropy provide stronger security, making it harder for unauthorized access or decryption.

- *QBER Variation*: The Quantum Bit Error Rate (QBER) is a critical metric in the BB84 protocol, reflecting the error rate in the generated secret key [20]. In an IoT environment, the QBER may vary due to factors such as device heterogeneity, environmental conditions, and communication channel characteristics. Analyzing QBER variation is essential to ensure the reliability and security of the protocol.

The QBER is calculated as the ratio of incorrect bits in the reconciled key K_r compared to the true states T:

$$QBER = \frac{1}{L}\sum_{i=1}^{L} I(K_{r,i} \neq T_i) \qquad (1)$$

Where I is the indicator function that is 1 if the condition is true and 0 otherwise.

Figure 5 provides a representation of the average QBER values for varying key lengths. The Average QBER equal 50.04% across the different key lengths indicates the average error rate observed during the key generation and transmission process for these specific key lengths. These results provide insights into the overall reliability and security of the system when using different key lengths.

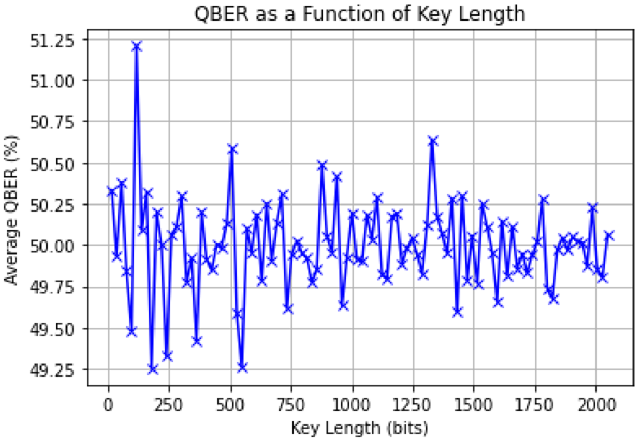

Figure 5: Average QBER Variation For Various key Sizes

In the context of IoT networks, these findings are significant. The selection of an appropriate key length is crucial for ensuring the security and effectiveness of the encryption process in IoT applications. A higher QBER can introduce risks to the confidentiality and integrity of data transmitted within IoT networks.

- *Efficiency Variation*: The efficiency of the BB84 protocol, including the key generation rate, communication overhead, and resource utilization, needs evaluation in the context of IoT networks. The resource constraints and heterogeneity of IoT devices may impact the protocol's efficiency, which can affect its suitability and practicality for deployment in IoT environments.

We can calculate efficiency using a simple formula:

$$Efficiency\left(E\right) = \left(Work\ output\ /\ Work\ input\right) \times 100\% \quad (2)$$

In the context of our analysis, we can determine the efficiency of the key distribution process by dividing the length of the key by the number of used bits and multiplying it by 100% [20].

To evaluate the efficiency of BB84, we can refer to Figure 6, which shows the variation of average efficiency for 1000 generated keys based on the key length.

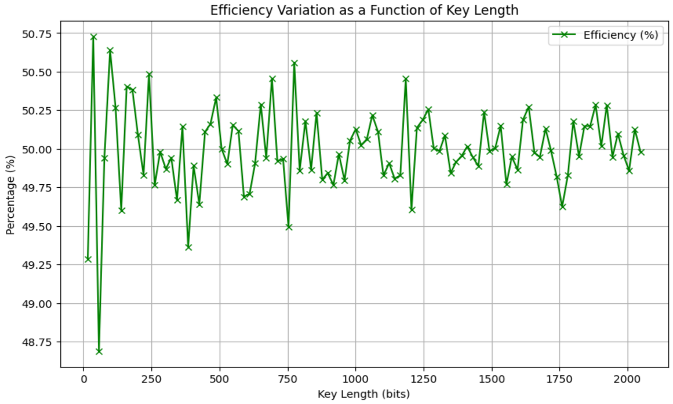

Figure 6: Average Entropy Variation For Various key Sizes

The maximum efficiency of 50.75% indicates the highest level of resource utilization and output achieved during key distribution, showcasing methods or configurations with optimal efficiency.

Conversely, the minimum efficiency of 48.62% represents instances where certain methods or configurations showed lower efficiency, potentially leading to suboptimal resource utilization.

The average efficiency of 50.00% for different key sizes has a significant impact on the IoT networks security. This indicates that, on average, half of the resources allocated for key distribution in IoT networks are effectively utilized.

- *Execution Time Evaluation*: The time required to execute the key generation and distribution process of the BB84 protocol is another important factor in IoT networks. Resource-constrained IoT devices may have limited computational capabilities, which can impact the protocol's execution time and potentially introduce vulnerabilities or performance issues.

Figure 7 provides a representation of the average execution time as a function of key lengths. The findings of Figure 7 demonstrate that the minimum execution time recorded was 0.06 ms, while the maximum execution time observed was 0. 22 ms. These results represent the efficient and rapid execution of key-related operations within IoT networks. The minimum execution time of 0.06 ms indicates that the system can perform these tasks quickly and with minimal delay, ensuring smooth operation.

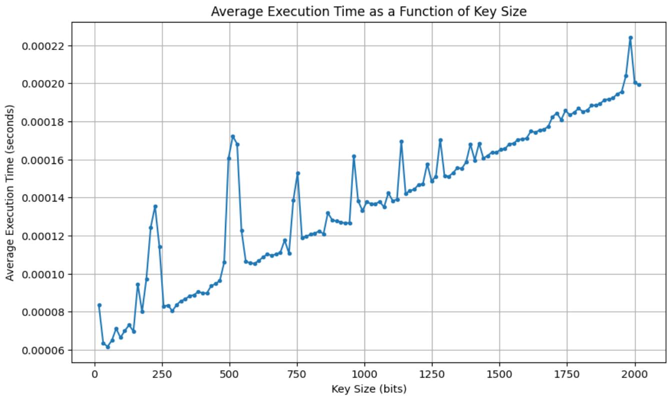

Figure 7: Execution Time Variation For Various key Sizes

The maximum execution time of 0.22 ms represents the upper limit of the time required for key-related operations. This slightly longer duration may be influenced by factors such as computational complexity or network limitations within the IoT environment.

5. CONCLUSION

This paper presented a comprehensive security analysis of the BB84 protocol in the context of IoT networks. The analysis evaluated key aspects such as entropy, execution time, QBER, and the efficiency of cryptographic key generation. The evaluation of entropy levels in the key generation process showed that the BB84 protocol can achieve a sufficient amount of randomness to maintain strong cryptographic properties. The analysis of correlation execution time between the sender and receiver indicated the protocol's efficiency and resilience against timing-based attacks. The assessment of QBER quantified the error rate in the transmission of quantum bits, allowing for the evaluation of the protocol's effectiveness in maintaining secure communication channels within IoT networks and its ability to detect eavesdropping attempts. Furthermore, the analysis of the efficiency of the generated keys, considering factors like key size, generation rate, and computational overhead, demonstrated the protocol's suitability for resource-constrained IoT devices and its ability to be effectively implemented in practical IoT network scenarios.

REFERENCES

1. H A. Al-Mohammed and E. Yaacoub **On The Use of Quantum Communications for Securing IoT Devices in the 6G Era**, in 2021 IEEE International Conference on Communications Workshops (ICC Workshops), June 2021.
2. Bennett, C. H.; Brassard, G. **Quantum cryptography: Public key distribution and coin tossing**, in IEEE International Conference on Computers, Systems and Signal Processing, New York, Bangalore, India, 1984, pp. 175–179.
3. C. Anilkumar, S. Lenka, N. Neelima, and S. V. E. **A Secure Method of Communication Through BB84 Protocol in Quantum Key Distribution**, Scalable Comput. Pract. Exp., vol. 25, no. 1, pp. 25–33, 2024.
4. Z. A. Abdulkader. **A Secure IoT System Using Quantum Cryptography with Block Cipher**, J. Appl. Sci. Eng., vol. 24, no. 5, pp. 771–776, 2021.
5. A. Devi V. and V. Kalaivani. **Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications**, Pers Ubiquit Comput, vol. 27, pp. 875–885, 2023.
6. A. Srikrishnan, A. Raaza, and B. E. Abishek. **Internet of Things (Iot) Network Security using Quantum Key Distribution Algorithm**, in International Journal of Engineering Trends and Technology, vol. 70, no. 2, pp. 19-23, Feb. 2022.
7. Edwards, A., Law, Y. W., Mulinde, R., & Slay, J. **Evaluation of Quantum Key Distribution for Secure Satellite-integrated IoT Networks**, Proceedings of the 18th International Conference on Cyber Warfare and Security, Maryland USA, 2023.
8. Neeraj and A. Singhrova. **Quantum key distribution-based techniques in IoT, The Scientific Temper**, vol. 14, no. 3, pp. 1008-1013, 2023.
9. A. Adu-Kyere, E. Nigussie and J. Isoaho. **Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3**, Sensors, vol. 22, no. 16, pp. 6284, 2022.
10. S. Krithika and T. Kesavmurthy. **Securing IOT Network through Quantum Key Distribution**, International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 6S4, pp. 693-697, April 2019.
11. Dhar, S., Khare, A., Dwivedi, A. D., & Singh, R.. **Securing IoT devices: A novel approach using blockchain and quantum cryptography**. Internet of Things, vol 25, Article 101019, 2024.
12. H.-Y. Su. **Simple analysis of security of the BB84 quantum key distribution protocol**, Quantum Information Processing, vol. 19, pp. 169, 2020.
13. A. S. Rao and S. S. Sreeja. **The Vital Role of Quantum Cryptography in IoT Network Security**, Eur. Chem. Bull., vol. 12, no. 9, pp. 573–587, 2023.
14. V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang. The **Impact of Quantum Computing on Present Cryptography**, Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, pp. 405–414, 2018.
15. H.-N. Dai, H. Wang, H. Xiao, X. Li, and Q. Wang. **On Eavesdropping Attacks in Wireless Networks**, in 2016 IEEE International Conference on Computational Science and Engineering, IEEE International Conference on Embedded and Ubiquitous Computing, and International Symposium on Distributed Computing and Applications to Business, Engineering and Science, Aug. 2016, pp. 138-143
16. Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. . **Internet of Things and the Man-in-the-Middle Attacks – Security and Economic Risks**. MEST Journal, vol 5, no 2, 15-25, 2017.
17. J. G. Almaraz-Rivera, J. A. Cantoral-Ceballos, and J. F. **Botero. Enhancing IoT Network Security: Unveiling the Power of Self-Supervised Learning against DDoS Attacks**, Sensors, vol. 23, no. 21, p. 8701, Oct. 2023
18. Zhu, H., Zhao, C., Zhang, X., & Yang, L . **A novel iris and chaos-based random number generator,** Computers & Security, 36, 40-48, 2013.
19. Y. Choi, Y. Yeom, and J.-S. Kang. **Practical Entropy Accumulation for Random Number Generators with Image Sensor-Based Quantum Noise Sources**, Entropy, vol. 25, no. 7, p. 1056, Jul. 2023
20. Alharith A. Abdullah and Yasser H. Jassem. **Enhancement of Quantum Key Distribution Protocol BB84**, Journal of Computational and Theoretical Nanoscience, vol. 16, pp. 1-17, 2019