Cybersecurity of a communication channel between quantum computers for the distribution of symmetric quantum keys.

D. A. Correa Ortiz
Engineering department
Pontificia Universidad Javeriana Cali
Cali, Valle del Cauca Colombia
dilancorrea@javerianacali.edu.co

S. Torres Rincón
Engineering department
Pontificia Universidad Javeriana Cali
Cali, Valle del Cauca Colombia
torrent@javerianacali.edu.co

ABSTRACT

This paper presents a study on the implementation of the BB84 protocol in traditional systems for quantum key distribution (QKD). The work focuses on the simulation of photon transmission and reception over a quantum channel, using information reconciliation algorithms such as LDPC. The security parameters are validated according to ETSI GS QKD 005 V1.1.1 [1] and ETSI GS QKD 008 V1.1.1 [2]. The results demonstrate the effectiveness of the proposed methods to ensure the security of quantum information transmission, providing a solid foundation for future research in quantum cybersecurity.

KEYWORDS

Quantum Cybersecurity, Quantum Key Distribution, BB84 Protocol, LDPC, ETSI GS QKD.

I INTRODUCTION

Quantum cryptography has emerged as a promising technology for securing communication, taking advantage of the fundamental properties of quantum mechanics. Unlike classical cryptography, which is based on the computational complexity of mathematical problems, quantum cryptography offers security based on unbreakable physical laws. Among the various protocols developed, the BB84 protocol stands out as the first and most widely studied quantum key distribution (QKD) scheme.

The BB84 protocol uses quantum particles, such as photons, to securely transmit information between two parties, typically named Alice and Bob. The security of the protocol is based on the no-cloning theorem, which prevents perfect copying of an unknown quantum state. This means that any attempt to eavesdrop on the communication channel will be detectable by the introduction of errors.

Information reconciliation is a critical component in QKD, necessary to correct discrepancies between Alice's and Bob's keys due to noise and measurement errors. Error correction codes, such as LDPC (Low-Density Parity-Check), are fundamental in this process, allowing efficient error detection and correction.

This work focuses on the implementation of the BB84 protocol in traditional systems, simulating the sending and receiving of photons through a quantum channel. In addition, information reconciliation algorithms, such as LDPC, are used to ensure the integrity of the final key. The validity of the implementation is verified according to ETSI GS QKD 005 V1.1.1 and ETSI GS QKD 008 V1.1.1, which set standards for the theoretical security and practical implementation of QKD.

II THEORETICAL FRAMEWORK

For this research, it is necessary to define some concepts related to technology and applied theory:

A QUANTUM CRYPTOGRAPHY

Quantum cryptography uses the principles of quantum mechanics to secure the transmission of information. Unlike classical methods, which rely on the computational difficulty of certain mathematical problems, quantum security is based on fundamental physical properties such as superposition and quantum entanglement. This makes it possible to detect any interception attempt due to the inevitable perturbation of quantum states [3].

B PROTOCOL BB84

The BB84 protocol, proposed by Bennett and Brassard in 1984, is one of the best known schemes for quantum key distribution (QKD). This protocol uses four polarized quantum states to represent bits of information. The selection of measurement bases is random, and the security of the protocol derives from the no-cloning principle, which states that an unknown quantum state cannot be copied without error [4].

C INFORMATION RECONCILIATION

In a QKD system, errors can arise due to device imperfections and channel noise. Information reconciliation is the process by which the participants in a quantum communication (Alice and Bob) correct these errors to obtain an identical key. Error correction codes, such as LDPC (Low-Density Parity-Check) codes, are crucial tools in this process. LDPC allows error correction with high efficiency, minimizing the amount of information to be exchanged publicly [5].

D LDPC ALGORITHM (LOW DENSITY PARITY CHECK)

LDPC codes are a class of error correction codes used in various digital communication applications, including information reconciliation in QKD. These codes are characterized by a low-density parity check matrix, which means that most of the matrix elements are zeros. This allows efficient coding and decoding, especially in channels with high error rate [6].

III GOALS

A GENERAL

Develop a simulated communication channel for symmetric key distribution supported by quantum computing and cybersecurity.

B SPECIFIC

- Perform a literature survey on quantum computing, Heisenberg's uncertainty principles, quantum key distribution protocols and implementations of these protocols.

- Design an algorithm that simulates a communication channel according to the BB84 protocol.

- Perform the implementation of the designed algorithm in the Python programming language.

- Validate the security parameters met by the implementation of the BB84 protocol algorithm according to ETSI GS QKD 005 V1.1.1 (2010-12).

IV RESULTS

The results obtained show that the use of LDPC algorithms in information reconciliation allows high secure transmission rates to be achieved, even in conditions of significant noise. The validation of the security parameters according to ETSI standards confirms the robustness of the system against potential attacks. In addition, limitations of the current approach were discussed and possible improvements for future implementations were suggested.

V CONCLUSION

The implementation of the BB84 protocol using LDPC algorithms for information reconciliation is a viable solution for secure quantum key distribution. This study provides a solid foundation for the development of more advanced quantum cybersecurity systems, highlighting the importance of following international standards to ensure information security.

References

[1] Group Specification, "ETSI GS QKD 005 V1.1.1 (2010-12)", Etsi.org. [En línea]. Disponible en: `https://www.etsi.org/deliver/etsi_gs/qkd/001_099/005/01.01.01_60/gs_qkd005v010101p.pdf` [Consultado: 29-may-2024].

[2] Group Specification, "ETSI GS QKD 008 V1.1.1 (2010-12)", Etsi.org. [En línea]. Disponible en: `https://www.etsi.org/deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf.` [Consultado: 29-may-2024].

[3] "¿Qué es quantum computing?," IBM. [En línea]. Disponible: `https://www.ibm.com/mx-es/topics/quantum-computing`. [Consultado: 24-Sep-2023]

[4] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," arXiv.org, 11-Sep-2014. [En línea]. Disponible: `https://arxiv.org/abs/1409.3525`. [Consultado: 30-Sep-2023]

[5] G. Brassard y L. Salvail, "Secret-key reconciliation by public discussion", en Advances in Cryptology — EUROCRYPT '93, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 410–423.

[6] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, y P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution", Phys. Rev. A, vol. 77, núm. 4, 2008.