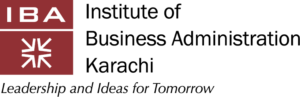


Project Proposal

Quantum Key Distribution Using the BB84 Protocol: A Simulation-Based Approach





Mohammad kamil (29464)

Discord: kamilshaheen

Git: mkamil92

Email: m.kamil.29464@khi.iba.edu.pk

**Abstract**

Data communication systems acquire new protection methods through quantum computing technology. Quantum Key Distribution operates as a practical quantum mechanics application because it permits secure key sharing to enable two parties establish encrypted communications. The project implements modeling of the BB84 protocol because this fundamental QKD protocol has received the greatest recognition among researchers. A secure quantum communication system uses quantum measurement methods with superposition principles to present all cryptographic operations in the model.

**Introduction**

The continuous expansion of quantum computing technology has created a crucial need for quantum-secure communication because traditional cryptographic approaches prove insufficient. Quantum computers will render mathematical complexity-dependent key exchanges vulnerable because they can break the encryption. The implementation of QKD combines quantum mechanics physical principles to create a system that protects communication from both detection and prevention of unauthorized access. The BB84 protocol created by Bennett and Brassard in 1984 [1] introduced the first essential protocol through which qubits pass randomly chosen bases. The measurement procedure reveals if any unauthorized modification happens in the communication channel. The BB84 protocol simulation delivers this research endeavor to illustrate quantum-secure communication operation and its working mechanisms.

**Literature Review**

Quantum key distribution started as theoretical research before researchers dedicated their efforts to developing practical implementations for early field applications. It became the fundamental framework which academic researchers and industrial developers continue to use for building secure communication systems. According to [2] QKD offers provable security grounded in physics, unlike classical cryptography which depends on computational hardness assumptions. Another paper[3] provided a comprehensive overview of practical QKD protocols, reinforcing BB84’s relevance as a pedagogical and experimental model.

In recent developments, [4] demonstrated a satellite-based quantum communication network that employed BB84-like schemes for secure key sharing over long distances.It emphasized the value of BB84 simulations in educational settings, noting that hands-on modeling helps students understand basis mismatches, measurement errors, and eavesdropping detection. These studies highlight both the theoretical importance and applied relevance of simulating BB84 in controlled environments, which this project seeks to do.

**Project Details**

In this project I’m focusing on simulating the BB84 quantum key distribution protocol to understand how secure keys can be shared using the principles of quantum mechanics. In this method, a sender (Alice) transmits qubits encoded using random bases, and a receiver (Bob) measures them using his own randomly chosen bases. After the transmission, both parties compare their bases over a public channel and keep only the bits where their choices matched. This shared key can then be used for encryption.

The project will also simulate an eavesdropper (Eve) trying to intercept the communication. Since any measurement in quantum systems can disturb the qubit, Eve’s interference introduces errors in the key. The protocol includes a step to estimate this error rate, and if it’s too high, the key is discarded to maintain security.

The entire simulation will be done using Python and Qiskit, built step by step to show each stage of the protocol clearly. The code will include random bit generation, basis selection, qubit preparation, measurement, and error analysis. Each part will be organized and explained to help others follow and learn from the process. Visualizations will be added to show measurement results and error rates.

So it will not only aims to simulate the protocol but also presents it in a way that helps others understand how quantum cryptography works in practice.

**Methodology**

In this project I’ll be following methodology step-by-step simulation of the BB84 protocol which runs through Python with Qiskit. The project starts by creating randomly generated bits and basis encoding for the sender Alice. An appropriate set of quantum gates transforms the bits into qubit states before transmission to receiver (Bob) who measures the qubits using randomly selected bases. The bases from both sides will be assessed through a classical channel until they match which will result in forming the final key. An extra part of the project will create conditions that represent an eavesdropper attempting to intercept and measure qubits before they reach Bob. Security thresholds will be used to analyze error rates that result from the key measurement process.

In this methodology I’ll be considering the following steps in order to develop it:

* Generate random bits and bases for Alice
* Encode bits into qubits using Hadamard and X gates based on the basis choice
* Simulate Bob’s measurement using independently chosen random bases
* Implement classical comparison of Alice and Bob’s bases to filter out mismatches
* Construct the final shared key from the matching basis positions
* Simulate eavesdropping by introducing Eve, who measures and resends qubits
* Analyze the error rate and determine if the key is safe or should be discarded
* Visualize the process using measurement histograms and bit comparisons

**Expected Outcomes**

The developed model will function as a complete implementation of the BB84 protocol which demonstrates secure key distribution alongside eavesdropping detection mechanisms. The project will deliver essential knowledge on the security benefits that quantum communication systems provide through unconditional protection. The final product aims to create an operational simulation model which allows education institutions to teach quantum communication concepts while performing threat simulations through simplified methods.

**Work Plan/Milestones**

|  |  |
| --- | --- |
| **Milestone** | **Tasks** |
| Milestone 1 | Background Research study, basic implementation of Alice–Bob communication, presentation |
| Milestone 2 | Add Eve simulation, implement error rate analysis, and improve visuals, exercises |
| Final Milestone | Final optimization, polish documentation, and prepare complete submission |

**References**

[1] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, 7-11.

[2] Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, *8*(8), 595-604.

[3] Scarani, V., Bechmann-Pasquinucci, H., Cerf M., Lütkenhaus, & Peev, (2009). The security of practical quantum key distribution. *Reviews of modern physics*, *81*(3), 1301-1350.

[4] Aji, A., Jain, K., & Krishnan, P. (2021, October). A Survey of Quantum Key Distribution (QKD) network simulation platforms. In *2021 2nd Global Conference for Advancement in Technology (GCAT)* (pp. 1-8). IEEE.