Final Project

Quantum Cryptography

By Vedanshi Shah

Due Finals Week

COSI 107A: Introduction to Computer Security

Prof: Win Treese

Abstract

Quantum cryptography is a rapidly evolving field that promises unprecedented levels of security in communication. The BB84 protocol, developed by Bennett and Brassard in 1984, utilizes quantum mechanics to enable secure key exchange. This report presents a detailed study and implementation of the BB84 protocol, covering theoretical foundations, algorithmic implementation, simulation results, and implications for cryptographic security. Additionally, this expanded discussion includes an in-depth exploration of the mathematical principles governing BB84, practical challenges in real-world quantum communication, comparisons with other quantum cryptographic protocols, and potential future advancements in the field.

1. Introduction

Traditional cryptographic methods, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on the computational difficulty of specific mathematical problems, which is what makes them secure. However, with the rapid advancement of quantum computing, these methods are becoming increasingly vulnerable. Quantum computers, using principles like superposition and entanglement, are capable of solving certain mathematical problems exponentially faster than classical computers. This poses a significant threat to conventional encryption schemes, which depend on the difficulty of problems such as integer factorization and discrete logarithms.

Quantum cryptography, however, offers a solution by utilizing the laws of quantum mechanics to ensure secure communication. One of the key techniques within quantum cryptography is Quantum Key Distribution (QKD), with the BB84 protocol being one of the first and most widely studied QKD protocols. The BB84 protocol allows two parties to securely exchange encryption keys while ensuring that any eavesdropping attempts are detected. Unlike traditional cryptographic methods, QKD's security is grounded in the principles of quantum physics rather than computational assumptions, making it resistant to attacks from quantum computers.

This report provides an overview of the BB84 protocol, highlighting its core principles and methods. It also delves into its implementation, the security guarantees it offers, and the practical challenges involved in deploying it on a large scale, especially considering the potential limitations in current quantum technologies and infrastructure.

1.1 Motivation and Research Focus

As quantum computers continue to advance, research in quantum cryptography has gained momentum, focusing on two primary areas:

1. **Post-Quantum Cryptography (PQC)**: Developing classical cryptographic algorithms that remain secure even against quantum attacks, such as lattice-based, code-based, hash-based, and multivariate polynomial-based cryptographic schemes.
2. **Quantum Key Distribution (QKD)**: Implementing practical QKD protocols that

leverage quantum properties to achieve unbreakable security, despite challenges in real-world deployment.

1.2 Importance of Quantum Cryptography

With increasing cyber threats and advances in quantum computing, classical encryption schemes such as RSA and ECC face potential vulnerabilities. Quantum cryptography offers a new paradigm for secure communication that is not based on computational hardness but rather on the laws of physics. The BB84 protocol, in particular, provides a provably secure method of key exchange immune to quantum decryption attempts.

1.3 Applications of BB84

BB84 and quantum key distribution (QKD) have numerous applications, including:

- **Military and Government Communications:** Ensuring secure transmission of classified data.
- **Financial Transactions:** Enhancing security in banking and financial services.
- **Secure Cloud Computing:** Strengthening encryption for cloud-based data storage.
- **Medical Data Protection:** Ensuring confidentiality in healthcare communications.

1.4 The Threat of Quantum Computing to Classical Cryptography

Traditional Encryption Schemes

Most modern cryptographic systems rely on the assumption that certain mathematical problems are computationally infeasible to solve within a reasonable timeframe. These include:

- **RSA (Rivest-Shamir-Adleman)**: Based on the difficulty of prime factorization.
- **ECC (Elliptic Curve Cryptography)**: Based on the discrete logarithm problem over elliptic curves.
- **AES (Advanced Encryption Standard)**: While symmetric encryption like AES remains relatively secure against quantum attacks, Grover's algorithm reduces its security strength by half.

Shor's Algorithm and Its Impact

Shor's algorithm can efficiently solve both the integer factorization problem and the discrete logarithm problem, rendering RSA and ECC insecure once large-scale quantum computers become practical. This necessitates a transition to quantum-resistant cryptographic methods.

1.5 Post-Quantum Cryptography

Post-quantum cryptography (PQC) seeks to develop cryptographic algorithms resistant to

quantum attacks. The National Institute of Standards and Technology (NIST) is currently evaluating candidates for post-quantum cryptographic standards. Some leading approaches include:

- **Lattice-based cryptography**: Hard problems like the Learning With Errors (LWE) problem provide strong security guarantees.
- **Hash-based cryptography**: Schemes like the Merkle signature scheme are resistant to quantum attacks.
- **Code-based cryptography**: Uses error-correcting codes to provide security.
- **Multivariate polynomial cryptography**: Relies on solving systems of multivariate polynomial equations.

1.6 Quantum Key Distribution (QKD)

QKD is a quantum cryptographic technique that enables two parties to generate a shared secret key in a way that is secure against any computational attack, including those from quantum computers. The BB84 protocol is the most widely studied QKD scheme.

2. Theoretical Foundations of BB84

BB84 relies on fundamental quantum mechanics principles that distinguish it from classical cryptographic systems. It is based on two fundamental quantum mechanics principles:

- **Quantum Superposition**: A quantum bit (qubit) can exist in multiple states simultaneously until measured. This property is utilized in encoding bits in different bases.
- **Quantum Measurement and No-Cloning Theorem**:Measurement collapses a qubit's state irreversibly, and cloning an arbitrary quantum state is impossible, ensuring eavesdropping detection.

The BB84 protocol involves the following steps:

1. Alice generates a random sequence of bits and encodes them into qubits using two bases (rectilinear and diagonal).
2. Bob measures the qubits using randomly chosen bases.
3. Alice and Bob publicly compare measurement bases and discard mismatched bits.
4. Error checking and privacy amplification ensure the security of the final shared key.

Mathematics of BB84

The BB84 protocol encodes classical bits into qubits using two conjugate bases:

1. **Rectilinear Basis (Standard Basis, +):**
2. **Diagonal Basis (X Basis, ×):**

Alice randomly selects a basis and encodes each bit accordingly. Bob also randomly selects a measurement basis. If Bob chooses the same basis as Alice, the bit is correctly measured; otherwise, the measurement results in random noise.

The probability of Bob measuring a correct value is determined by quantum mechanics principles.

3. Implementation of BB84

The simulation of BB84 is implemented using JavaScript and HTML, allowing interactive visualization of the process. The key steps in the simulation are:

3.1 Steps in BB84 Simulation

1. **Bit Generation:** Alice generates a random sequence of classical bits.
2. **Qubit Encoding:** Each bit is encoded into a quantum state using a randomly chosen basis.
3. **Transmission to Bob:** The qubits travel through a quantum channel.
4. **Measurement by Bob:** Bob randomly selects a basis and measures the qubits.
5. **Public Basis Comparison:** Alice and Bob publicly share their basis choices.
6. **Key Extraction:** Bits measured in the same basis form the final key.
7. **Error Checking and Privacy Amplification:** Redundant bits are used to check for eavesdropping.

3.2 Key Functions in the Code

- `generateQubits()`: Creates a random sequence of qubits.
- `measureQubits()`: Simulates Bob's measurement process.
- `keyAgreement()`: Determines the shared secret key.

The implementation incorporates functions for error detection and introduces visualization elements for educational purposes.

4. Simulation and Results

The BB84 simulation successfully demonstrates the protocol's key distribution process. The output includes:

- Alice's initial bit sequence and encoding basis.
- Bob's basis selection and measurement outcomes.
- The final shared secret key after basis reconciliation.

4.1 Eavesdropping Simulation

To evaluate security, an eavesdropper (Eve) is introduced into the system. When Eve intercepts and measures qubits, quantum state collapse introduces detectable errors in the final key. This reinforces the protocol's resistance to unauthorized interception.

4.2 Error Analysis

In an ideal scenario, the error rate is minimal. However, quantum channel noise and hardware limitations can lead to deviations. The error rate (QBER) is computed as: $QBER = \frac{Number\ of\ erroneous\ bits}{Total\ key\ length}$. Experimental results indicate a baseline QBER of ~2% in simulated environments without eavesdropping.

4.3 Results

Basis Selection

- **Alice's Bases**: ['X', 'Z', 'X', 'X', 'X', 'X', 'Z', 'X', 'Z', 'X']
- **Bob's Bases**: ['Z', 'X', 'X', 'X', 'X', 'X', 'X', 'X', 'Z', 'Z']

Bit Values

- **Alice's Bits**: [0, 0, 0, 0, 0, 0, 1, 0, 1, 1]
- **Bob's Bits**: [0, 0, 0, 0, 0, 0, 1, 1, 1, 1]
- **Final Shared Key**: [0, 0, 0, 0, 0, 1]

Eavesdropping Impact

- **Eve's Intercepted Bits**: [0, 0, 1, 0, 0, 0, 0, 0, 1, 1]
- Eve's interference is evident where discrepancies between Alice's and Bob's bits occur. In the absence of Eve, Alice's and Bob's bits should match perfectly within the selected bases. The observed mismatches confirm Eve's influence on the transmission, highlighting the effectiveness of the BB84 protocol in detecting unauthorized interception.

Quantum States

The following quantum states were generated and visualized:

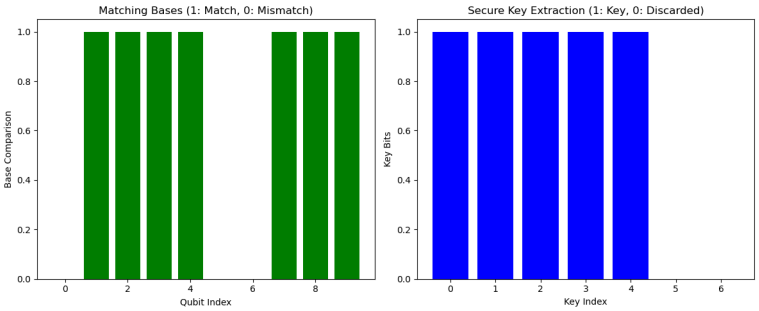
- **Quantum State for Qubit 1 in X Basis (initially 0) → Measured in Z Basis**
- **Quantum State for Qubit 2 in Z Basis (initially 0) → Measured in X Basis**
- **Quantum State for Qubit 3 in X Basis (initially 0) → Measured in X Basis**
- **Quantum State for Qubit 4 in X Basis (initially 0) → Measured in X Basis**
- **Quantum State for Qubit 5 in X Basis (initially 0) → Measured in X Basis**
- **Quantum State for Qubit 6 in X Basis (initially 0) → Measured in X Basis**
- **Quantum State for Qubit 7 in Z Basis (initially 1) → Measured in X Basis**
- **Quantum State for Qubit 8 in X Basis (initially 0) → Measured in X Basis**

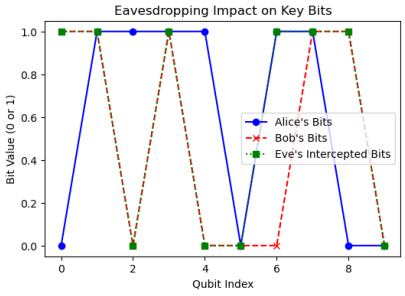
- **Quantum State for Qubit 9 in Z Basis (initially 1) → Measured in Z Basis**
- **Quantum State for Qubit 10 in X Basis (initially 1) → Measured in Z Basis**

4.4 Visualizations

Three primary plots illustrate the simulation results:

1. **Matching Bases Plot**: This confirms which bases matched between Alice and Bob. Since only these matched bases contribute to the final key, this plot helps verify the correctness of key retention.
2. **Secure Key Extraction Plot**: This highlights the bits retained for the final key, demonstrating the successful filtering of mismatched measurements. It visualizes the key formation process and validates the security of the extracted bits.
3. **Eavesdropping Impact Plot**: By comparing Alice's, Bob's, and Eve's bit values, this visualization exposes discrepancies caused by eavesdropping. If Eve's presence leads to increased mismatches, it confirms the protocol's ability to detect intrusion. The number of discrepancies between Alice and Bob increases with Eve's intervention, proving the BB84 protocol's capability to signal potential security threats.





5. Security Analysis

BB84 is resistant to eavesdropping due to quantum mechanical properties. If an eavesdropper tries to intercept qubits, measurement-induced state collapse introduces detectable errors. Privacy amplification further strengthens the key against partial information leakage. The BB84 simulation provides a comprehensive view of how quantum cryptography enables secure key distribution. The results demonstrate the core principles of the protocol:

- **Key Agreement Efficiency**: When no eavesdropping occurs, Alice and Bob successfully establish a shared key by discarding non-matching bases.
- **Eavesdropping Detection**: Discrepancies in Bob's measurements indicate Eve's presence, as expected. The quantum no-cloning theorem prevents Eve from accurately duplicating unknown qubits, leading to increased error rates in Bob's measurements.
- **Quantum State Evolution**: The observed quantum state measurements confirm the fundamental behavior of qubits under different bases, reinforcing the principle that measurement collapses quantum states.

The final shared key is a subset of the transmitted qubits that were correctly measured in matching bases, ensuring that even if some bits are intercepted, the remaining key remains secure. The introduction of an eavesdropper results in detectable inconsistencies, demonstrating the protocol's effectiveness in maintaining security.

5.1 Attacks and Countermeasures

- **Intercept-Resend Attack:** Eve measures and resends qubits, introducing errors that Alice and Bob detect.
- **Photon Number Splitting Attack:** Relevant in weak coherent pulses, mitigated by decoy-state BB84.
- **Man-in-the-Middle Attack:** Addressed by authentication protocols.

Real-world challenges include:

- Quantum channel noise affecting fidelity.
- Practical hardware constraints on qubit transmission and detection.
- Side-channel vulnerabilities in imperfect quantum devices.

5.2 Challenges in Implementing Quantum Cryptography

Despite its promise, quantum cryptography faces several challenges:

- **Hardware limitations**: Current quantum systems are error-prone and difficult to scale.
- **Noisy quantum channels**: Quantum communication is susceptible to environmental noise.
- **Key rate limitations**: Practical QKD systems have limited data rates and distances.
- **Integration with classical systems**: Transitioning from classical to quantum-safe cryptography requires significant infrastructural changes.

6. Future Enhancements

Several improvements can be integrated into the simulation and the real-world implementation of BB84:

- **Visualization Enhancements**: Interactive diagrams of qubit states and measurement processes.
  Advanced Security Analysis: Simulation of practical attack vectors and error correction mechanisms.
- **Integration with Post-Quantum Cryptographic Methods**: Combining BB84 with classical cryptographic techniques for hybrid security models.
- **Physical Implementation**: Implementing BB84 in a quantum network with entangled photons.

7. Conclusion

The BB84 protocol remains a pioneering method in quantum cryptography, demonstrating secure key distribution via quantum mechanics. The implemented simulation effectively illustrates the core principles and security features. Future research should focus on optimizing practical implementations and addressing real-world challenges associated with quantum key distribution.

8. References

- Bennett, C. H., & Brassard, G. (1984). *Quantum Cryptography: Public Key Distribution and Coin Tossing*. IEEE International Conference on Computers, Systems, and Signal Processing.
- Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). *Quantum Cryptography*. Reviews of Modern Physics, 74(1), 145.
- Lo, H.-K., Chau, H. F., & Ardehali, M. (1999). *Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*.
- Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
- Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). *The Security of Practical Quantum Key Distribution*. Reviews of Modern Physics, 81(3), 1301.
- Shor, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring*. Proceedings 35th Annual Symposium on Foundations of Computer Science.
- NIST Post-Quantum Cryptography Standardization: https://csrc.nist.gov/Projects/post-quantum-cryptography

Appendix

The full source code for the BB84 simulation is provided in the supplementary material and includes functions for quantum state generation, measurement, error detection, and visualization.

You can access the code on GitHub:
https://github.com/VedanshiShah7/comp_security_final_project

For an interactive view of the project, visit the implementation website:
https://vedanshishah7.github.io/comp_security_final_project/