




[MS-CSEC](#) / [4. Fall 2024 \(4th Semester\)](#) / [Crypto and Communications](#) / [Assignment\\_3](#)  
/ [CaseStudy-QuantumCrypto.md](#) 

 **Cyb3rZ3d** Update CaseStudy-QuantumCrypto.md

c4478f5 · now  History

Ruben Valdez  
CSEC5323 | Cryptography and Secure Communication  
Friday's @ 4pm  
Prof. Robert Jones  
Assignment: Case Study- Quantum Cryptography



## Objective:

This assignment is designed to introduce students to the principles of quantum cryptography, specifically Quantum Key Distribution (QKD) and its applications in modern security. Students will gain an understanding of the core concepts, advantages, and challenges associated with quantum cryptography.

## Tasks:

### Research and Summary (25 points)

1. Research Quantum Key Distribution (QKD) and provide a summary that explains:
  - The basic principles behind QKD (10 points)

QKD uses quantum mechanics to securely share encryption keys. It relies on principles like the Heisenberg Uncertainty Principle, which makes eavesdropping detectable. If someone tries to intercept the quantum bits (qubits) during transmission, the system is disturbed, and the intrusion is revealed. The secure keys generated are then used in encryption algorithms.

- The differences between classical and quantum cryptography (10 points)

Security Basis: Classical cryptography depends on solving hard math problems. QKD relies on quantum physics, which prevents undetected eavesdropping. Eavesdropping Detection: Classical methods can't detect eavesdropping. QKD can instantly spot an intrusion. Implementation: Classical encryption works on standard hardware and software. QKD needs special hardware and dedicated channels. Scalability: Classical methods are cheaper and easier to scale. QKD has high costs and infrastructure needs.

- Real-world applications of QKD (5 points)
  - Government Use: Secures sensitive communication.
  - Banking: Protects financial data.
  - Quantum Satellites: Enables secure, long-distance communication.
  - Research: Drives advancements in secure quantum networks.

## 2. References:

- Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

<https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>

## Concept Application (20 points)

---

### 1. Explain how the BB84 protocol works. Your explanation should include:

- A step-by-step overview of how QKD is used to share a key securely (15 points)
  - a. Encoding (Alice):
    - Preparation (Alice's Encoding):
      - Alice generates a random sequence of bits.

- She encodes each bit into a photon using one of two polarization bases:
  - Rectilinear Basis (+): Horizontal ( $0^\circ$ ) or Vertical ( $90^\circ$ ) polarization.
  - Diagonal Basis (×):  $45^\circ$  or  $135^\circ$  polarization.

b. Transmission:

- Alice sends the sequence of polarized photons to Bob over a quantum channel.

c. Measurement (Bob's Reception):

- Bob measures each incoming photon using a randomly chosen basis (either + or ×).
- Due to the random choice of bases, Bob's measurements will match Alice's encoding basis approximately 50% of the time.

d. Sifting (Basis Comparison):

- Alice and Bob publicly communicate to compare the bases they used for each photon (without revealing the actual bit values).
- They retain only the bits where their bases matched, discarding the rest.

e. Key Generation:

- The remaining bits, where both parties used the same basis, form the raw key.

f. Error Checking:

- Alice and Bob compare a subset of the raw key to estimate the error rate.
- If the error rate exceeds a predetermined threshold, it may indicate eavesdropping, and the key is discarded.

g. Privacy Amplification:

- If the error rate is acceptable, Alice and Bob apply privacy amplification techniques to distill a shorter, secure final key.

- A discussion of the role of quantum states in ensuring security (5 points)

Quantum states are essential to the security of protocols like BB84 because they make eavesdropping detectable. Two key principles ensure this:

- a. No-Cloning Theorem: Quantum mechanics prohibits exact copies of unknown quantum states. This means an eavesdropper (Eve) cannot intercept and replicate photons without altering them, ensuring any attempt to copy the quantum states is detectable.
- b. Measurement Disturbance: Measuring a quantum state disrupts it, especially if the measurement basis differs from the original preparation basis. If Eve intercepts and measures the photons, she changes their states, introducing errors that Alice and Bob can identify during the key verification process.

## 2. References:

- Quantum Key Distribution, BB84 - simply explained | Quantum 1x1

[https://youtu.be/8hNQyTdNil4?si=7OSQNkQgshV\\_OYYH](https://youtu.be/8hNQyTdNil4?si=7OSQNkQgshV_OYYH)

- Quantum Key Distribution and BB84 Protocol

<https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5>

# Challenges and Future Directions (15 points)

---

- Write a brief essay (300-400 words) discussing:
  - The challenges in implementing quantum cryptographic systems in practice (e.g., cost, infrastructure) (10 points)
  - How quantum computing could impact existing cryptographic techniques in the future (5 points)

**ESSAY:**

Quantum cryptography, particularly Quantum Key Distribution (QKD), is a revolutionary approach to secure communication. By leveraging the principles of quantum mechanics, it offers the potential for theoretically unbreakable encryption. However, despite its promise, implementing quantum cryptographic systems faces significant challenges in practice. Additionally, the advent of quantum computing introduces new risks to existing cryptographic techniques, necessitating advancements in both fields.

[MS-CSEC / 4. Fall 2024 \(4th Semester\) / Crypto and Communications](#)

 [main](#) [Assignment\\_3](#) ↑ Top  
/ **CaseStudy-QuantumCrypto.md**

**Preview**

Code

Blame

180 lines (102 loc) · 11 KB

Raw



enterprises. Furthermore, the infrastructure requirements for QKD systems are substantial. They often necessitate dedicated hardware and communication channels, such as leased optical fibers or free-space optical links. These requirements not only increase costs but also make integration with existing communication networks difficult.

Another limitation of QKD is its range. Photon loss in optical fibers restricts the effective distance of QKD to a few hundred kilometers. Extending this range requires quantum repeaters, which are still in experimental stages and not widely available. Additionally, QKD systems frequently rely on trusted relay nodes to extend communication distances. These nodes, while solving some distance issues, introduce vulnerabilities to insider attacks, increasing overall security risks.

The security of QKD is also heavily dependent on implementation. While the theoretical principles of quantum mechanics ensure security, practical systems are prone to errors and vulnerabilities. Poorly engineered components can introduce flaws, and the sensitivity of quantum systems to external disturbances makes them challenging to validate and deploy reliably.

Looking toward the future, quantum computing poses a significant threat to existing cryptographic systems. Algorithms like Shor's algorithm allow quantum computers to break widely used cryptographic schemes, such as RSA, ECC, and Diffie-Hellman, by solving complex mathematical problems exponentially faster than classical computers. This would compromise the security of nearly all current digital communication.

To mitigate this threat, researchers are actively developing post-quantum cryptographic algorithms. These algorithms are designed to resist attacks from both classical and quantum computers. Organizations like the National Institute of Standards and Technology (NIST) are leading efforts to standardize quantum-resistant cryptographic solutions, ensuring secure communication in the face of advancing quantum technologies.

In conclusion, while quantum cryptography offers immense potential for secure communication, its implementation faces significant hurdles, including cost, infrastructure demands, and practical vulnerabilities. Simultaneously, the rise of quantum computing necessitates the urgent development of quantum-resistant cryptography to safeguard existing systems. Overcoming these challenges will require continued research, innovation, and collaboration across the fields of quantum mechanics and cybersecurity.

### ***References:***

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Retrieved from <https://ieeexplore.ieee.org>

National Institute of Standards and Technology (NIST). (n.d.). Post-quantum cryptography project. Retrieved from <https://csrc.nist.gov/projects/post-quantum-cryptography>

National Security Agency (NSA). (n.d.). Quantum key distribution synopsis. Retrieved from <https://nsa.gov>

Pan, J. W., et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. Nature. Retrieved from <https://www.nature.com>

Quantum Untangled. (n.d.). Quantum key distribution and BB84 protocol. Medium. Retrieved from <https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5>

IBM Quantum. (n.d.). Quantum computing basics. Retrieved from <https://quantum-computing.ibm.com>

## **Practical Scenario Analysis (15 points)**

---

- Consider the following scenario:

- A company wants to implement a secure communication channel between two remote offices using QKD. Identify the primary challenges the company may face and propose solutions to address them. Your response should be around 200 words.

### ***Response:***

If a company wants to set up Quantum Key Distribution (QKD) for secure communication between two remote offices, they will face some key challenges:

- **Infrastructure Problems:** QKD needs special fiber-optic cables or free-space channels. Over long distances, the signal weakens, and free-space channels can be disrupted by bad weather.
- **High Costs:** Setting up QKD requires expensive equipment like single-photon detectors and maintaining it adds more expenses.
- **Distance Limits:** QKD doesn't work well over long distances without special devices called quantum repeaters, which are still being developed.
- **Security Risks:** To make QKD work over long distances, trusted relay stations are used, but these can be targeted by insider threats.

Solutions:

- Use quantum satellites to cover long distances without relying on cables.
- Combine QKD with traditional encryption to save on costs and make the system more flexible.
- Partner with existing QKD providers to reduce setup and maintenance costs.
- Use post-quantum encryption alongside QKD to stay secure while the technology improves.