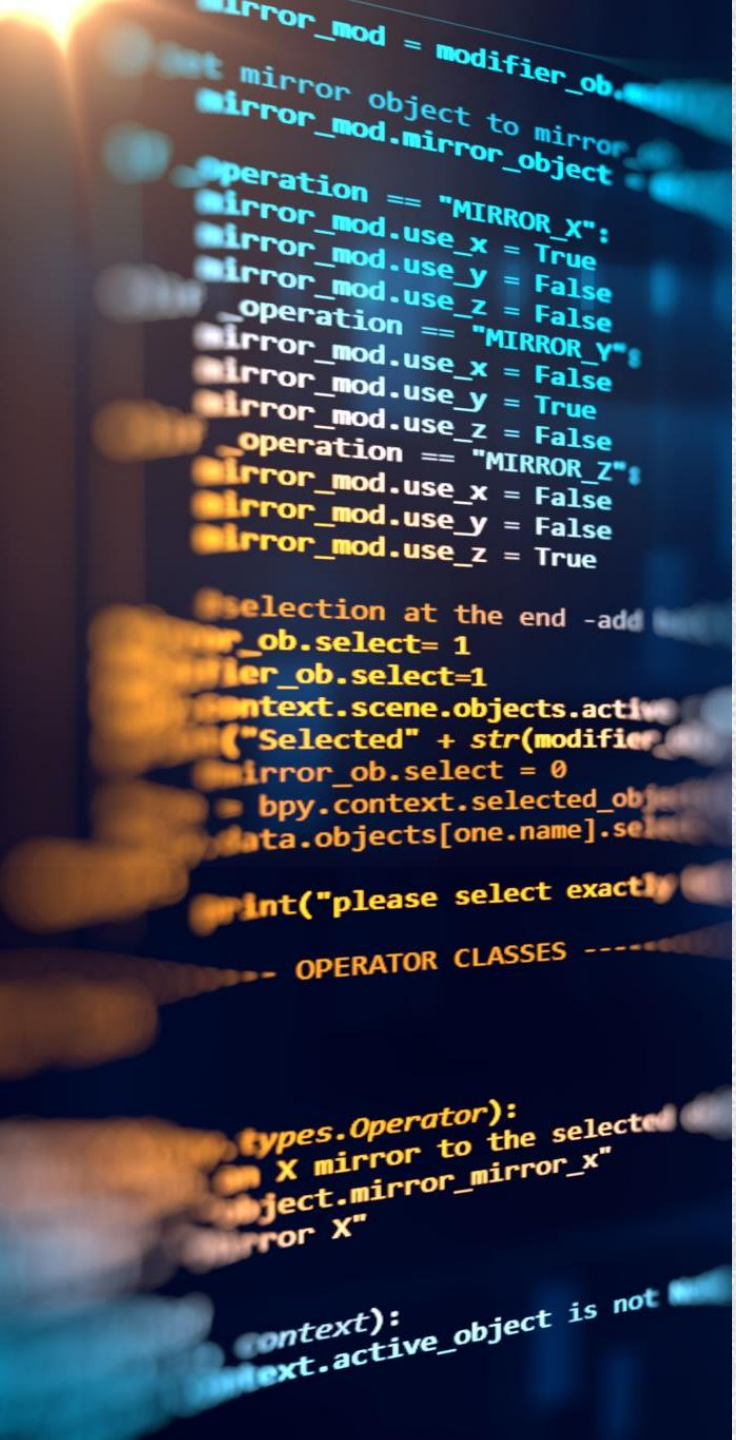
HYBRID QUANTUM-CLASSICAL SECURE COMMUNICATION

CPR E 681 Project Presentation

By Barkha Mathur and Yasaswini Tatikonda



QUANTUM COMPUTING – A SECURITY THREAT?

- Most of today's internet security (like HTTPS, email encryption, etc.) depends on math problems that are hard for classical computers (like factoring big numbers in RSA).
- But **quantum computers** can solve those problems **fast**—especially with algorithms like:
- **Shor's algorithm**: breaks RSA and ECC.
- **Grover's algorithm**: weakens AES by cutting its strength in half.
- So once powerful quantum computers arrive, much of our current security becomes useless.

MOST PROPOSED FIXES RELY ON:

Quantum Key Distribution (QKD), like the BB84 protocol.

But QKD usually needs expensive **quantum hardware** and doesn't work well in common software setups.

PROBLEM DEFINITION

- Quantum algorithms break classical encryption assumptions.
- QKD promises theoretical security .
- Existing systems have limited usability, accessibility, and adversarial modeling.

PROJECT GOALS

Simulate BB84 protocol using Qiskit.

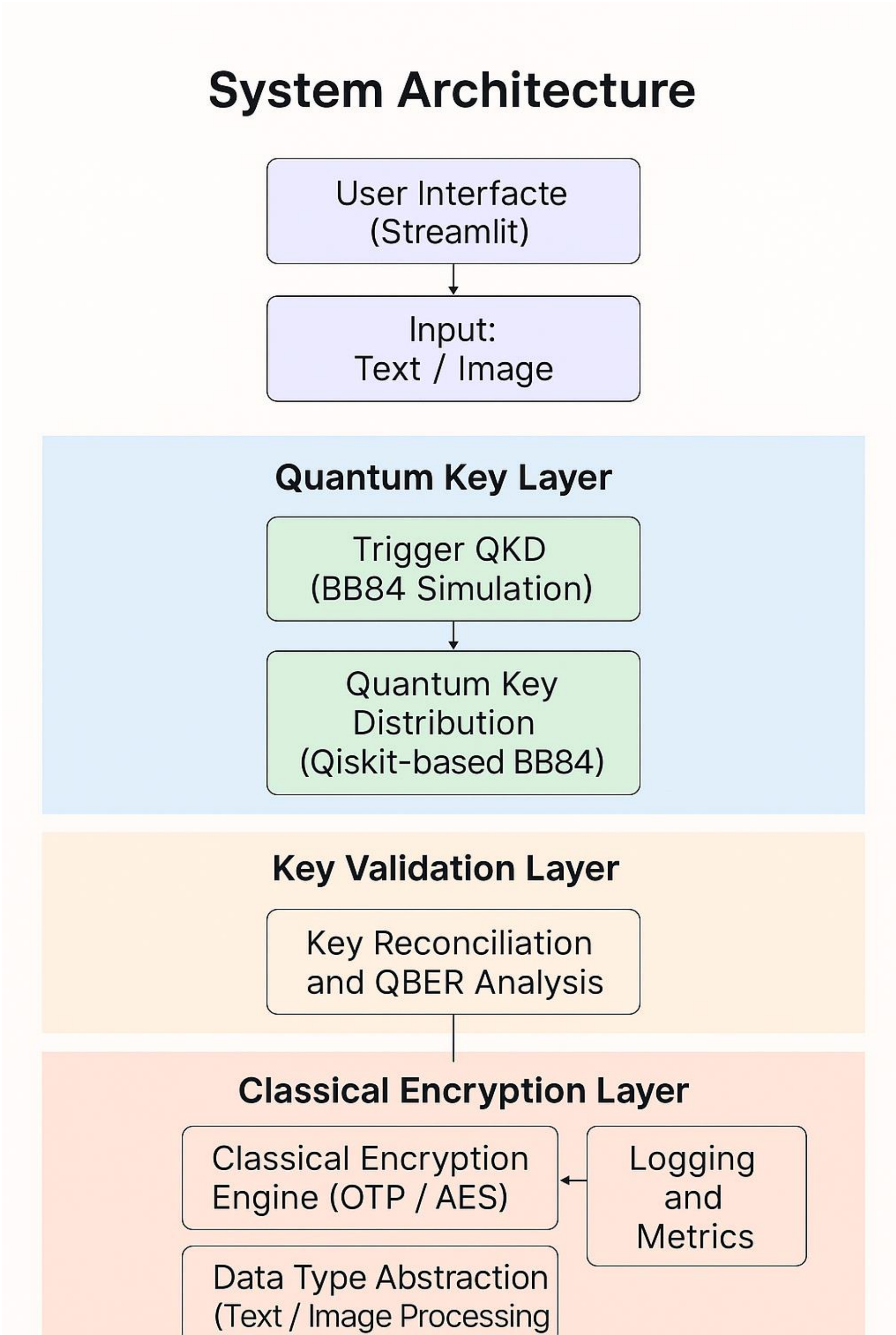
Integrate quantum keys into OTP and AES encryption.

Enable secure communication for text and images.

Implement adversarial simulations and performance benchmarking.

PROJECT PROTOTYPE

- **Simulates BB84 key exchange using Qiskit** (no quantum hardware needed).
- **Feeds quantum-generated keys into AES or OTP encryption**.
- **Let's users send text or images securely—even under eavesdropping attacks**.
- **Detects attacks** using Quantum Bit Error Rate (QBER) and blocks compromised keys.
- **Runs in a web app interface (Streamlit)** for accessibility and demos.



SYSTEM ARCHITECTURE

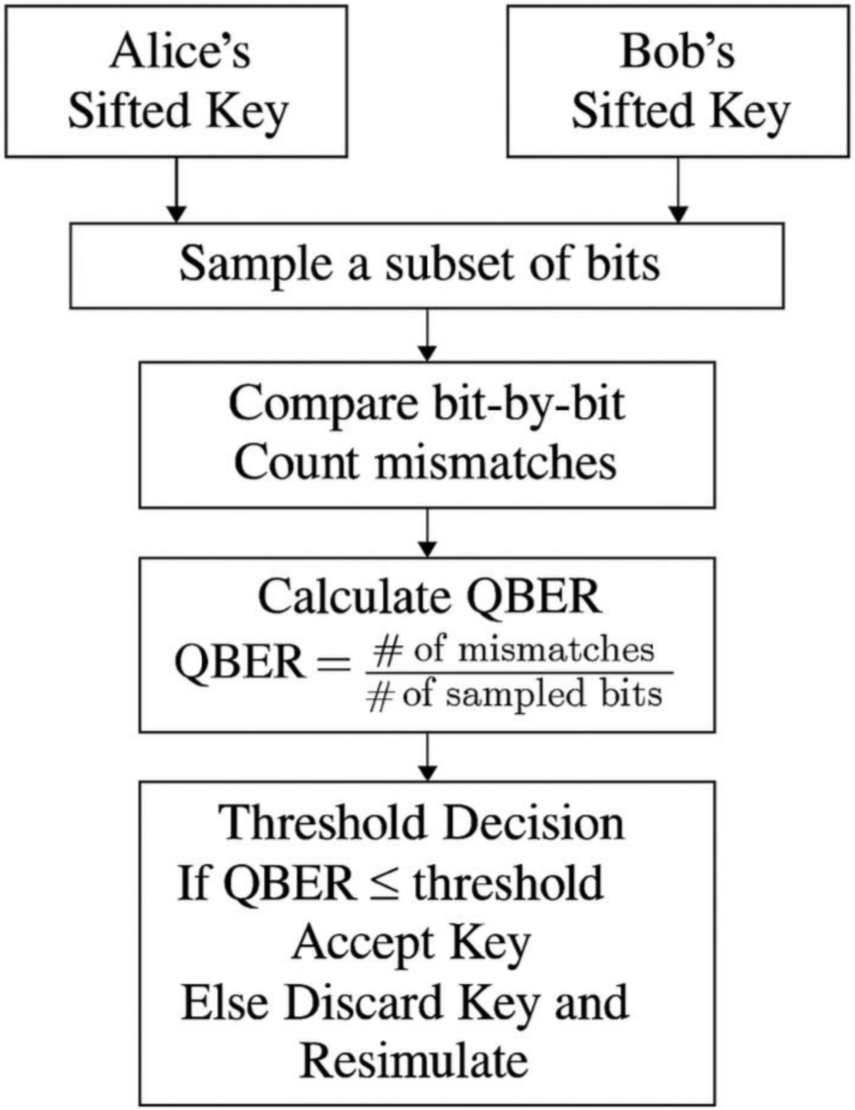
- Quantum Key Distribution via BB84 (Qiskit).
- Classical Encryption Engine: OTP and AES.
- Streamlit-based UI for input, encryption, visualization.
- Adversarial simulation module to test QBER impact.

BB84 PROTOCOL OVERVIEW

Generate	Generate random bits and bases (Alice and Bob).
Simulate	Simulate qubit transmission and measurement.
Perform	Perform basis comparison and key sifting.
Calculate	Calculate QBER to detect eavesdropping.

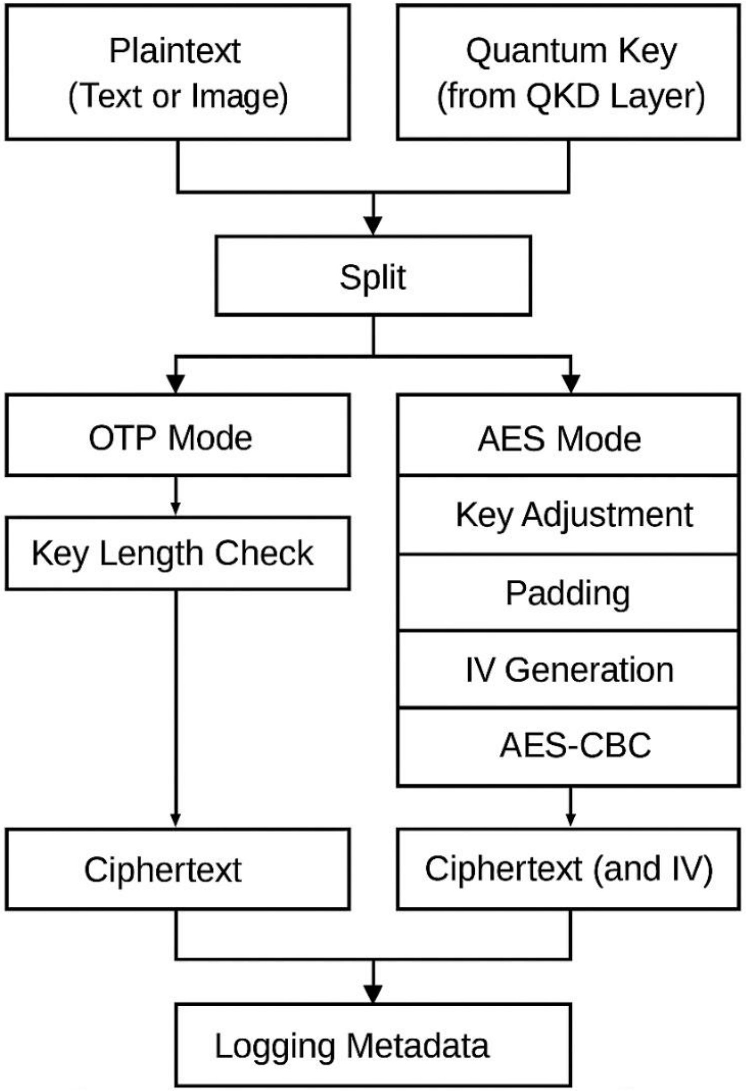
ENCRYPTION INTEGRATION

- OTP for perfect secrecy (bitwise XOR).
- AES-128 in CBC mode with padding and IV.
- Quantum key adapted for encryption compatibility.
- Supports text and image formats.



FLOW DIAGRAM – QUANTUM BIT ERROR RATE

- It is essential to verify the integrity of the resulting key and detect any evidence of eavesdropping.
- Calculating the Quantum Bit Error Rate (QBER), reflects discrepancies between Alice's and Bob's sifted keys.
- The QBER serves as both a performance indicator and a security checkpoint.

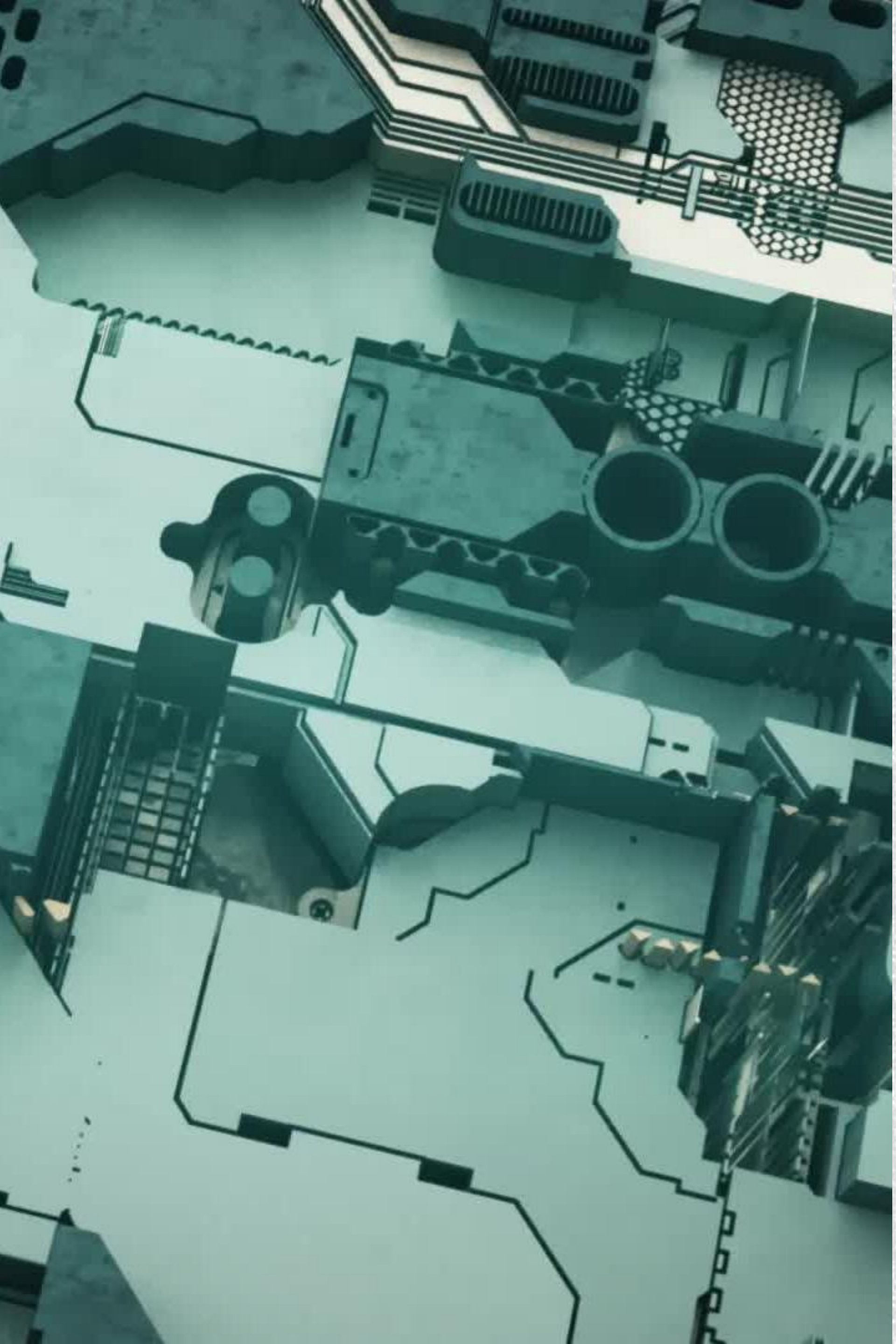


DUAL MODE ENCRYPTION PIPELINE

- Once a validated symmetric key has been established via BB84 and QBER analysis, the system proceeds to the encryption phase.
- This step utilizes either the One-Time Pad (OTP) or the Advanced Encryption Standard (AES), as selected by the user.
- The goal of this layer is to demonstrate how quantum-generated keys can be integrated with classical encryption protocols in a flexible and secure manner.

ADVERSARIAL MODELING

- Eve intercepts and measures qubits randomly.
- Simulates passive and active attacks.
- System computes QBER to detect interference.
- Threshold-based key validation ensures security.

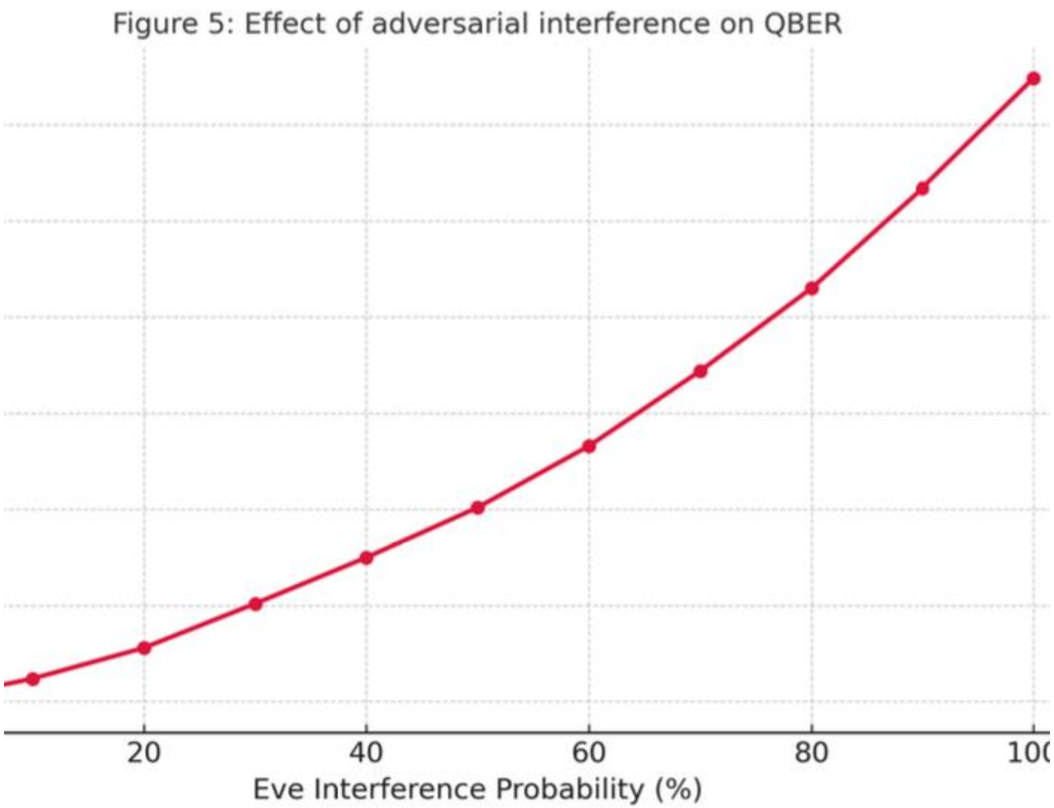


EXPERIMENTAL SETUP

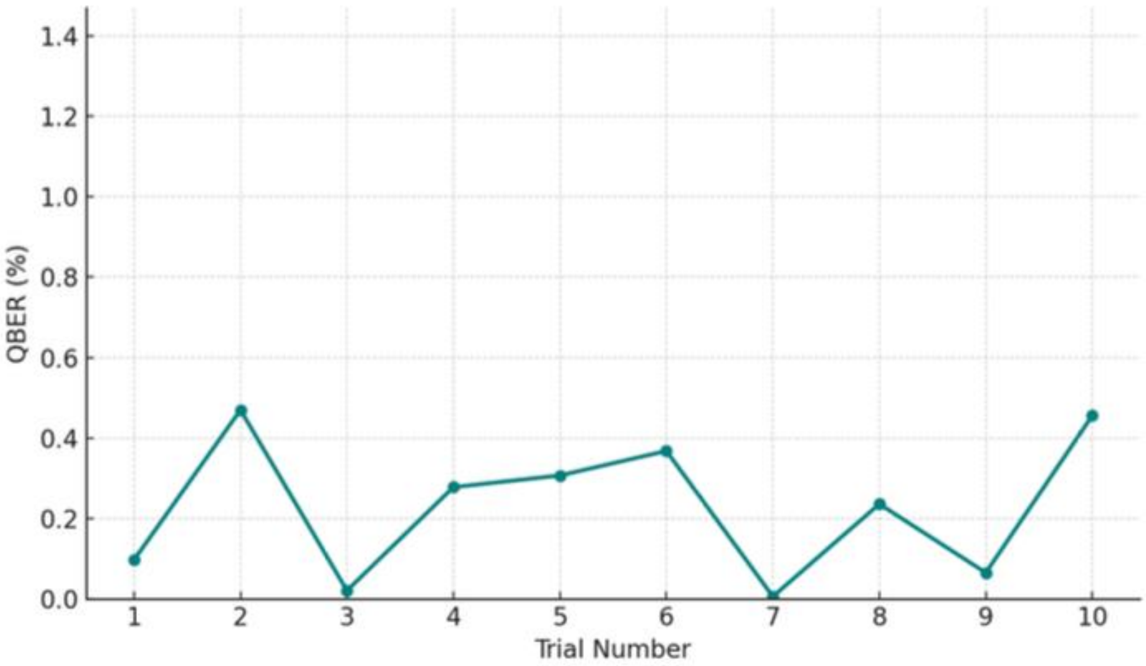
- Conducted on standard machine, no quantum hardware.
- Runs repeated for multiple configurations.
- Text/image encrypted under both normal and attack conditions.
- Performance and QBER tracked.

RESULTS AND OBSERVATIONS

- Correct key exchange: QBER < 0.5% (no attack).
- Eavesdropping raises QBER > 30%, triggers key rejection.
- AES faster for large messages; OTP ideal for short texts.
- Image encryption maintains fidelity post-decryption.

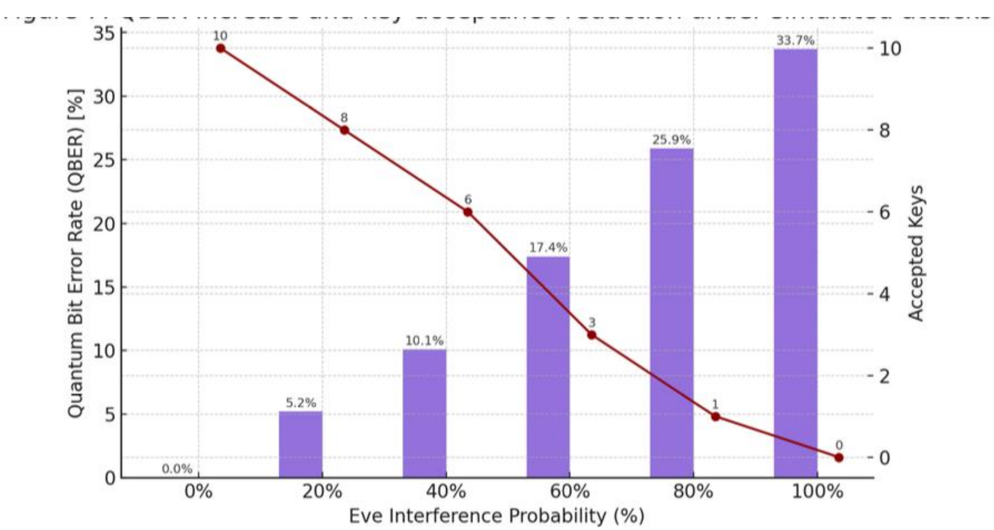


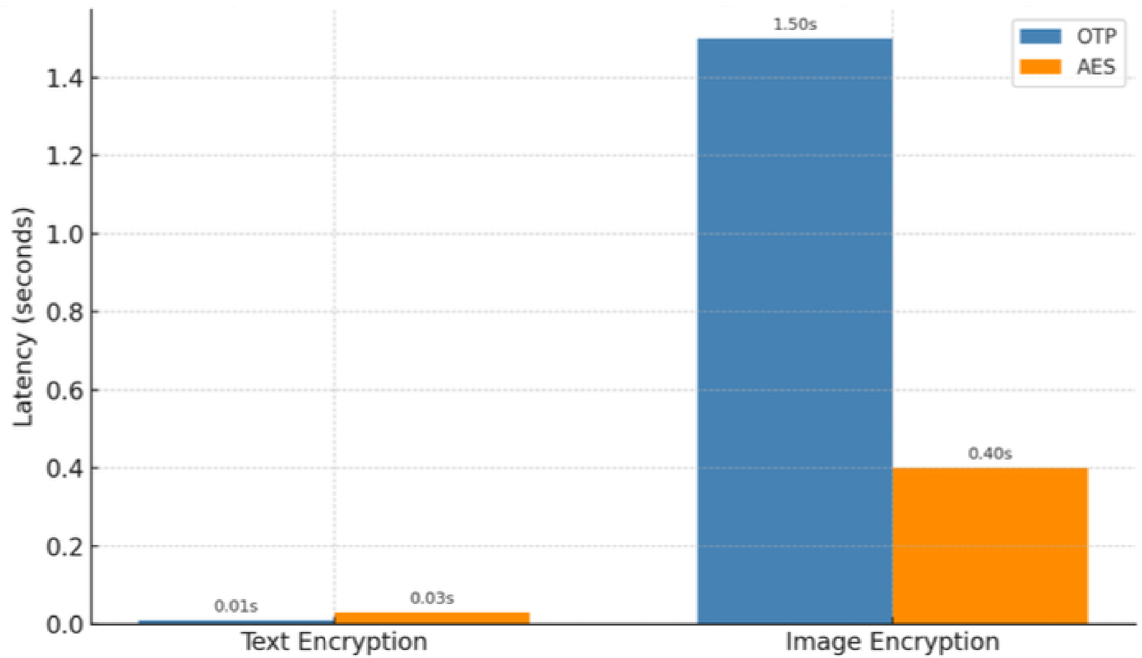
EFFECT OF ADVERSARIAL INTERFERENCE ON QBER



QBER OBSERVED ACROSS 10 BBB4 TRIALS WITHOUT ADVERSARIAL INTEREFERENCE

QBER INCRAESE AND KEY ACCEPTANCE REDUCTION UNDER SIMULATED ATTACKS





LATENCY COMPARISON FOR TEXT AND IMAGE ENCRYPTION USING OTP AND AES

FUTURE WORK

- Integrate hardware-based QKD systems.
- Expand to new data types (audio, PDF, video).
- Enhance UI with multi-user support, session history.
- Evaluate in distributed and real-time settings.

CONCLUSION

- Hybrid approach ensures quantum-resilient secure communication.
- Accessible via software, educational and practical use.
- Real-time adversarial modeling and performance profiling.
- Foundation for scalable post-quantum cryptographic platforms.