Quantum-Secured Immutable Checkpoints with BB84 and SPHINCS+

Project Title:

Quantum-Secured Immutable Checkpoints with BB84 and SPHINCS+

Objective:

This project aims to develop a quantum-resistant security mechanism by integrating **BB84 Quantum Key Distribution (QKD)** with **SPHINCS+ post-quantum digital signatures**. The goal is to create immutable, verifiable checkpoints for secure communication and blockchain applications, ensuring resilience against both classical and quantum threats.

1. Introduction & Problem Statement

With the advent of quantum computing, traditional cryptographic schemes like RSA and ECC face potential vulnerabilities. Secure communication and blockchain systems require post-quantum cryptography to maintain integrity and confidentiality. This project addresses two key aspects:

1. **Key Distribution:** Using BB84 for quantum-secure key exchange.
2. **Digital Signatures:** Leveraging SPHINCS+ for post-quantum authentication and immutability.

2. Methodology

A. Quantum Key Distribution - BB84 Protocol

The BB84 protocol ensures secure key exchange between Alice and Bob by transmitting qubits in different bases. The steps include:

1. **Alice's Key Generation:** Alice randomly selects bits and encodes them in a quantum circuit.
2. **Bob's Measurement:** Bob chooses random bases and measures the transmitted qubits.
3. **Key Agreement:** They compare bases and retain matching bits to form a shared secret key.

This key will later be used to encrypt data or authenticate transactions.

B. Post-Quantum Digital Signatures - SPHINCS+

SPHINCS+ is a hash-based signature scheme resistant to quantum attacks. It is used to ensure the authenticity and integrity of messages in the system:

1. **Key Pair Generation:** A public-private key pair is created using pyspx.
2. **Signing Messages:** The private key signs critical messages or checkpoints.
3. **Verification:** The signature is verified using the public key.

C. Integration of BB84 and SPHINCS+

The quantum-generated key from BB84 will be used in combination with SPHINCS+ signatures to:

- **Secure blockchain transactions by signing blocks and ensuring immutability.**
- **Create quantum-secure authentication mechanisms for decentralized systems.**

3. Implementation Details

A. Required Technologies & Libraries

- **Python & Qiskit** for quantum circuit simulation.
- **pyspx** for SPHINCS+ post-quantum cryptography.
- **Qiskit AerSimulator** for simulating quantum key exchange.

B. Algorithm Breakdown

1. Generate a SPHINCS+ Key Pair

- Generate a random seed and derive a secure key pair.
- Store the public key for verification purposes.

2. Quantum Key Distribution with BB84

- Simulate a quantum circuit with Alice and Bob exchanging qubits.
- Measure and extract a shared quantum-secure key.

3. Sign a Message with SPHINCS+

- Use the private key to sign a message.
- Store the signed checkpoint for verification.

4. Verify the Signature

- Ensure the authenticity and integrity of signed messages.
- If the signature is valid, accept the transaction/checkpoint.

5. Apply the Quantum Key for Secure Communication

- Use the BB84 key for encrypting/decrypting sensitive data.
- Apply hybrid cryptographic techniques to enhance security.

4. Use Cases & Potential Applications

1. Blockchain & Immutable Checkpoints

- Secure on-chain transactions using quantum-secure keys and signatures.
- Ensure data immutability by signing each block using SPHINCS+.

2. Secure Communications & Authentication

- Enhance encryption protocols with quantum-generated keys.
- Implement quantum-secure authentication mechanisms for users.

3. Post-Quantum Cybersecurity

- Strengthen security protocols in IoT, healthcare, and financial systems.
- Prepare systems for the quantum computing era.

5. Expected Outcomes & Future Work

Expected Results:

- A functional hybrid cryptographic framework combining **BB84 & SPHINCS+**.
- A prototype demonstrating **quantum-secure key exchange & authentication**.
- Proof of concept for **blockchain integration with post-quantum security**.

Future Improvements:

- Implement real-world quantum hardware for improved security.
- Explore multi-party key distribution for decentralized networks.
- Optimize performance for large-scale applications.

6. Conclusion

This project provides a **post-quantum, quantum-enhanced security solution** by combining BB84 quantum key distribution with SPHINCS+ signatures. It ensures **secure key exchange, authentication, and immutable checkpoints** in blockchain and cybersecurity applications.